DEPARTMENT OF COMPUTER SCIENCE

AN INTRUSION RECOVERY SECURITY FRAMEWORK IN WIRELESS SENSOR NETWORKS

DOCTOR OF PHILOSOPHY DISSERTATION

Iouliani Stavrou

February, 2014

DEPARTMENT OF COMPUTER SCIENCE

AN INTRUSION RECOVERY SECURITY FRAMEWORK IN WIRELESS SENSOR NETWORKS

Iouliani Stavrou

A Dissertation Submitted to the University of Cyprus in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

February, 2014

APPROVAL PAGE

Doctor of Philosophy Dissertation

AN INTRUSION RECOVERY SECURITY FRAMEWORK IN WIRELESS SENSOR NETWORKS

Presented by

Iouliani Stavrou

Research Supervisor

_____

Dr. Andreas Pitsillides

Committee Member

_____

Dr. Constantinos Pattichis

Committee Member

_____

Dr. Vasos Vassiliou

Committee Member

_____

Dr. Christos Douligeris

Committee Member

_____

Dr. Antonio Liotta

University of Cyprus

February, 2014

DECLARATION OF DOCTORAL CANDIDATE

The present doctoral dissertation was submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy of the University of Cyprus. It is a product of original work of my own, unless otherwise mentioned through references, notes, or any other statements.

Iouliani Stavrou

……..

ΠΛΑΙΣΙΟ ΑΝΑΚΤΗΣΗΣ ΕΠΗΡΕΑΖΟΜΕΝΩΝ ΛΕΙΤΟΥΡΓΙΩΝ ΑΠΟ ΕΠΙΘΕΣΕΙΣ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΜΕ ΑΙΣΘΗΤΗΡΕΣ

Ιουλιανή Σταύρου

Πανεπιστήμιο Κύπρου, 2014

Τα ασύρματα δίκτυα αισθητήρων έχουν αποκτήσει αξιοσημείωτο ερευνητικό ενδιαφέρον κατά τη διάρκεια των τελευταίων ετών. Τα ασύρματα δίκτυα αισθητήρων μπορούν να υποστηρίξουν τη λειτουργία υποδομών ζωτικής σημασίας, όπως είναι οι υποδομές για υποστήριξη της υγείας, στρατιωτικών θεμάτων, αντιμετώπιση καταστροφών, κλπ. Μόλις οι αισθητήρες εντοπίσουν ένα κρίσιμο περιστατικό ενημερώνουν το κέντρο ελέγχου ώστε να ληφθούν κατάλληλες ενέργειες για την αντιμετώπιση του. Κατά τη διάρκεια που το κέντρο ελέγχου ενημερώνεται για τα περιστατικά τα οποία έχουν ανιχνευτεί, είναι ζωτικής σημασίας οι αισθητήρες να διατηρήσουν τη λειτουργία τους και να συνεχίσουν να αποστέλλουν τις παρατηρήσεις τους στο κέντρο ελέγχου. Ωστόσο, κακόβουλες δραστηριότητες μπορούν να επηρεάσουν τη λειτουργία του δικτύου και τη λήψη αποφάσεων. Έτσι, η ασφάλεια είναι μια σημαντική προϋπόθεση, προκειμένου να εξασφαλιστεί μια αξιόπιστη διαδικασία λήψης αποφάσεων. Για την εξασφάλιση της ασφάλειας, πρέπει να χρησιμοποιηθούν κατάλληλοι μηχανισμοί ασφαλείας για την προστασία της λειτουργίας του δικτύου αισθητήρων και την αντιμετώπιση των κακόβουλων δραστηριοτήτων.

Μια στρατηγική ασφάλειας συνήθως αποτελείται από τρία επίπεδα: την πρόληψη, ανίχνευση επιθέσεων και την ανάκτηση των επηρεαζόμενων λειτουργιών του δικτύου. Στο παρόν στάδιο, οι περισσότερες από τις ερευνητικές έρευνες σε ασύρματα δίκτυα αισθητήρων εστιάζονται στην πρόληψη και την ανίχνευση επιθέσεων. Η ανάκτηση των επηρεαζόμενων λειτουργιών του ασύρματου δικτύου αισθητήρων είναι επίσης ένα σημαντικό κομμάτι της παροχής ασφάλειας που δεν έχει λάβει την ίδια προσοχή. Οι μηχανισμοί πρόληψης δεν είναι κατ' ανάγκην άψογες λύσεις και η προστασία του δικτύου μπορεί να τεθεί σε κίνδυνο από

εισβολείς. Εάν η λειτουργία του δικτύου με αισθητήρες επηρεαστεί, τότε θα πρέπει να αποκατασταθεί, προκειμένου να διατηρηθεί η αξιόπιστη λειτουργία του. Το γεγονός ότι οι εισβολείς μπορεί να εκτελέσουν διάφορες επιθέσεις και να επιμείνουν με τη στρατηγική επίθεσή τους, καθιστά την ανάγκη για επικέντρωση στις πτυχές αποκατάστασης ακόμα μεγαλύτερη. Στο παρόν στάδιο, οι λύσεις αποκατάστασης λειτουργιών που επηρεάζονται από επιθέσεις στα ασύρματα δίκτυα αισθητήρων, επικεντρώνεται κυρίως στις στατικές στρατηγικές επίθεσης, για αυτό και επίμονοι/προσαρμοστικοί εισβολείς δεν αντιμετωπίζονται αποτελεσματικά.

Σε αυτή τη διδακτορική διατριβή, θα διερευνηθούν πτυχές ανάκτησης των επηρεαζόμενων λειτουργιών από επιθέσεις σε ασύρματα δίκτυα αισθητήρων, με έμφαση στην ανάκτηση της διαθεσιμότητας, της επιβίωσης και της αξιοπιστίας των αισθητήρων και την ενίσχυση της αντοχής τους ενάντια σε ένα στατικό ή/και επίμονο/προσαρμοστικό εισβολέα που έχει πάρει στην κατοχή του αισθητήρες και έχει γίνει μέρος του δικτύου. Η διατριβή προτείνει ένα νέο πλαίσιο ασφάλειας ανάκτησης επηρεαζόμενων λειτουργιών σε ασύρματα δίκτυα αισθητήρων, το οποίο αποτελείται από τον προσδιορισμό των απαιτήσεων ανάκτησης, μια νέα λύση ανάκτησης η οποία καθοδηγείται από μια νέα πολιτική ανάκτησης και μια νέα μέθοδο αξιολόγησης. Η προτεινόμενη λύση ανάκτησης έχει σχεδιαστεί έχοντας τρεις βασικούς στόχους: (α) να ανακτήσει τις επηρεαζόμενες λειτουργίες του ασύρματου δικτύου με αισθητήρες, (β) να περιορίσει την πηγή των επιθέσεων, και (γ) να ενισχύσει την ανθεκτικότητα του δικτύου όταν οι επιθέσεις συνεχίζονται. Ένα βασικό χαρακτηριστικό του προτεινόμενου πλαισίου είναι η χρήση κατευθυντικών κεραιών για να δημιουργηθούν ελεγχόμενα μονοπάτια δρομολόγησης και επικοινωνίας και να αποκλειστούν οι κακόβουλοι κόμβοι. Το πλαίσιο προωθεί διαφορετικά επίπεδα ανάκαμψης μέσω μιας πολιτικής ασφάλειας που συντονίζει την εφαρμογή των μέτρων αποκατάστασης προκειμένου να αντιμετωπιστούν οι στατικοί ή/και επίμονοι/προσαρμοστικοί εισβολείς. Τέλος, η προτεινόμενη μέθοδος αξιολόγησης καθορίζει τα κριτήρια για την αξιολόγηση και τη σύγκριση της απόδοσης των

λύσεων ανάκαμψης σε ασύρματα δίκτυα αισθητήρων. Η αξιολόγηση περιλαμβάνει κριτήρια, όπως η παράδοση πακέτων, η καθυστέρηση στην παράδοση, η ενέργεια, ο αριθμός των κόμβων που έχουν επηρεαστεί, και ο αριθμός των πακέτων που έχουν υποκλαπεί. Η μέθοδος αξιολόγησης χρησιμοποιείται για να αξιολογήσει και να συγκρίνει την προτεινόμενη λύση έναντι των τυπικών λύσεων αποκατάστασης σε ασύρματα δίκτυα αισθητήρων για να διαπιστωθεί αν τηρούνται οι λειτουργικές απαιτήσεις, όπως η διαθεσιμότητα, η ικανότητα επιβίωσης, η αξιοπιστία, η ανθεκτικότητα, και η ανταπόκριση. Τα αξιολόγηση δείχνει ότι η υιοθέτηση του προτεινόμενου πλαισίου, με κατευθυντικές κεραίες, σε ένα πλαίσιο ανάκτησης στα ασύρματα δίκτυα αισθητήρων είναι αποτελεσματική. Η προτεινόμενη λύση έχει αποδειχθεί ότι αντιμετωπίζει αποτελεσματικά στατικές και επίμονες στρατηγικές επίθεσης, ελαχιστοποιεί τον αντίκτυπο επιθέσεων και βοηθά στο να ανακτηθεί η διαθεσιμότητα, η ικανότητα επιβίωσης, η αξιοπιστία και η ανθεκτικότητα του δικτύου σε περίπτωση επηρεασμού. Οι τυπικές λύσεις αποκατάστασης από επιθέσεις έχουν αποδειχθεί ικανοποιητικές για την αντιμετώπιση κυρίως στατικών επιθέσεων, συχνά με ένα σημαντικό αντίτιμο όσον αφορά τη διαθεσιμότητα κόμβων και τη δυνατότητα παράδοσης πακέτων.

AN INTRUSION RECOVERY SECURITY FRAMEWORK IN WIRELESS SENSOR NETWORKS

Iouliani Stavrou

University of Cyprus, 2014

Wireless sensor networks (WSNs) have gained remarkable research attention over the last several years. WSNs are being considered to support the operation of critical infrastructures, such as healthcare, military and disaster relief, on which our modern world is increasingly dependent upon. As soon as critical events are propagated by the WSN to the control center, appropriate actions need to be taken to address the reported incidents. During this time, it is vital that the WSN maintains its operation and continues propagating observations to the control center. However, malicious activity, which targets the compromisation of the network's operation during critical events observation, cannot be precluded. Thus, security is an important requirement in order to ensure a reliable decision-making. Security mechanisms are required to protect the sensor network's operation and address compromisation.

A security strategy is usually comprised of three layers: prevention, intrusion detection and intrusion recovery. Currently, most of the research investigations in WSNs focus on prevention and intrusion detection. Intrusion recovery in WSNs is also an essential part of security provisioning that has not received the same attention. Prevention mechanisms are not flawless solutions and protection can be compromised by adversaries. If the sensor network's operation is compromised, it has to be restored in order to maintain its reliable operation. The fact that the adversaries can perform different attacks and persist with their attack strategy makes the need to also focus on recovery aspects even greater. Currently, intrusion recovery solutions in WSNs are mainly focused on static attack strategies, thus persistent/adaptive adversaries are not effectively addressed.

In this thesis, we investigate intrusion recovery aspects in WSNs, focusing on recovering the availability, survivability and reliability of sensor nodes and enhancing their resilience

against a static or a persistent/adaptive adversary that has compromised nodes and become a part of the network. An intrusion recovery security framework in WSNs is proposed consisting of the specification of intrusion recovery requirements, a new intrusion recovery countermeasure driven by a new recovery policy and an evaluation method. The proposed intrusion recovery countermeasure is designed with three main objectives: (a) recover the compromised WSN operation, (b) confine the attack source, and (c) enhance the network's resilience when attack continues. A core feature for the proposed countermeasure framework is the utilization of directional antennas to create controlled communication paths and to physically exclude malicious nodes. The framework promotes recovery escalation through a security policy that coordinates recovery applicability in order to address static and persistent/adaptive adversaries. Finally, the proposed evaluation method defines the security evaluation features and related metrics that should be considered to assess and compare the performance of intrusion recovery countermeasures in WSNs. The performance evaluation includes the networking and security metrics, such as packet delivery, delay, energy, number of compromised nodes, number of eavesdroped packets and malicious nodes on eavesdropping, together with operational requirements, such as availability, survivability, reliability, resilience, responsiveness, and self-healingness. The evaluation method is utilized in order to evaluate and compare the proposed solution against typical intrusion recovery solutions (blacklisting and rerouting, low duty cycle and channel surfing) in WSNs. Results demonstrate that the adoption of the proposed framework, with directional antennas, is beneficiary in an intrusion recovery context in WSNs. The proposed countermeasure has been shown to address static and persistent attack strategies, minimize the attack outcome and recover the network's availability, survivability, reliability and resilience in case of compromisation, without significant tradeoff. Typical intrusion recovery solutions have been shown to mainly address static attacks, often with a significant tradeoff in terms of nodes' availability and packet delivery capability, in addition to reduced operational objectives.

ACKNOWLEDGEMENTS

I would like to express my gratitude to everyone who helped and supported me throughout my Ph.D experience.

First and foremost, I would like to express my gratitude to my supervisor, Professor Dr. Andreas Pitsillides. This thesis would not have been possible without his guidance and constructive feedback, throughout every stage of the Ph.D process. I thank him for all the opportunities he has given me over the years to work in his team and be a part of the Network's Research Laboratory. He has been always positive and supportive at difficult times, at both an academic and a personal level. His advices, constant support and understanding have been invaluable, for which I am deeply grateful.

I would also like to thank Dr. Vasos Vasiliou and Dr. Costas Pattichis for their valuable comments and suggestions. Their feedback has helped me highlight different aspects of the proposed work when finalizing the thesis content.

Moreover, I would like to thank all the members of my family for their continuous support throughout the years. They have endured my absence from many family gatherings without any complaints while I was working on my Ph.D. To them, I promise to visit them more often and stay by their side when they need my support.

Last, but certainly not least, I would like to thank Dimitris, my husband and life partner. This has been a long journey for both of us. His patience, love and understanding have been immeasurable. Without his unconditional love and support I would have not pursued my dreams. There are really no words to express the depth of my gratitude and love. To him, I dedicate this thesis and I promise to make up for the lost time.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AP	Access Point
AODV	Adhoc On-demand Distance Vector
CBR	Constant Bit Rate
DoS	Denial of Service attack
EC	Evaluation Criterion
EO	Evaluation Objective
ICT	Information Communication Technology
IDS	Intrusion Detection System
LOS	Line of Sight
MAC	Medium Access Control
MoAO	Management of Antenna Operation
NLOS	Non Line of Sight
SF	Selective forwarding attack
SIR	Signal to Interference Ratio
WSN	Wireless Sensor Network

Chapter 1

Introduction

1.1 Problem statement

Wireless sensor networks (WSNs) are increasingly becoming integrated in every aspect of the citizens' lifes [1], revolutionizing the Information and Communication Technologies (ICT) area, forming the Future Communications and Internet services [2], introducing new opportunities, better communication channels and an enhanced quality of provided services. WSNs are being considered to support the operation of critical infrastructures [3, 4, 5] such as medical, military, disaster and relief and transport in order to support their operation and offer reliable services to citizens.

Sensor nodes are usually deployed in a predetermined geographic area where observations are of special interest, forming a WSN. The fundamental tasks [3, 5] performed by sensor nodes include sensing the environment, establishing communication with neighbor nodes and forwarding their reports to the sink node. The sink is then responsible to disseminate observations to the control center for further processing and decision-making. A number of issues [6] can risk the operation and related tasks of a WSN such as the open nature of

wireless communication, the unrestricted deployment of the WSNs and the limited capabilities of sensor nodes in terms of communication, storage and energy. Adversaries can benefit from the aforementioned reasons as they can launch a number of attacks [6, 7] against the sensor network and compromise its operation. An application that utilizes a WSN to support its objectives can be greatly affected if the WSN's services are compromised, even causing an unexpected and harmful operation. Protecting the WSN from malicious activities is deemed necessary in order to promote a WSN application's reliable operation. The growing number of critical applications that are envisaged to become highly depended on WSNs has led the research community to investigate the fundamental security issues and challenges in WSNs, in an effort to propose security solutions [6, 7, 8] and protect the WSN operation.

In a security context, there are two overall strategies. There is the security strategy of the WSN that aims to protect its operations and on the other hand there is the attack strategy of the adversary that aims to compromise the WSN's operation. As the attacks progress, there is the need for the security strategy of the network to adapt in order to cope with the circumstances. Therefore, it is essential that the WSN utilizes a security strategy [9, 10, 11] consisting of three layers (Figure 1): prevention, intrusion detection and intrusion recovery. These three layers comprise a spherical security approach with each layer compensating the other. Defense can be considered as the first layer of security as it targets to protect the network from intruders and nodes from attacks' compromisation. Defense mechanisms [6, 8] address external adversaries more effectively than when considering attackers that have compromised sensor nodes and have gained access to the network. When protective measures are not adequate and fail to prohibit adversaries from compromising the network, intrusion detection mechanisms help in detecting the malicious activity in order to promote recovery actions. Intrusion detection [6, 8] is the second layer, while intrusion recovery can be perceived as the third layer of a security strategy. Intrusion recovery is triggered when intrusion detection has identified compromisation of the network's confidentiality, integrity, authentication, availability or reliability and it targets to restore the network to a stable state.

All three layers are required in order to successfully maintain the network in an operational mode. Currently, researchers have designed a number of WSN-related security solutions [8, 12] in an effort to address security problems, mostly focusing their investigations on the defense and intrusion detection layers. Research in the area of intrusion recovery has received less attention; however, it is equally important as the other security layers. This thesis investigates intrusion recovery aspects in WSNs and contributes an intrusion recovery framework in an effort to restore the compromised WSN operation and maintain operability of the network under static or persistent/adaptive attack conditions.

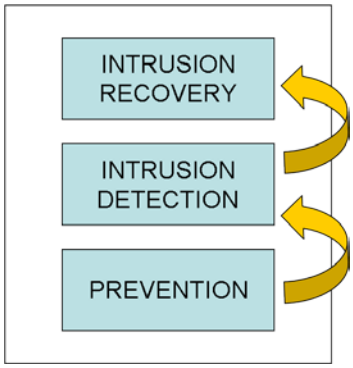

Figure 1: Security strategy layers

1.2 Research motivation

Wireless sensor networks may support the operation of mission-critical applications [3, 4, 5]. In these mission-critical environments network and data compromisation is unacceptable since these environments are depended on timely and reliable information to provide their services. The fact that security is of paramount importance in critical WSN infrastructures and must be well addressed in order to protect the network and its data and maintain operability of the network under attack conditions, has motivated this research work in the context of mission-critical WSN applications. As soon as critical events are propagated by the WSN to the control center, appropriate actions need to be taken to address the reported incidents. During this time, it is vital that the WSN maintains its services and continues propagating

observations to the control center and/or response units. Thus, any malicious activity should be appropriately addressed so that the attack outcome is nullified or at least minimized. Moreover, this research addresses adversaries that have gained access to the WSN and have become a part of the network. This type of adversary poses a greater threat for critical applications and is a challenge for the design of security solutions. Overall, the main objective is to maintain network operability in mission critical applications when security incidents occur.

One of the most important security requirements for mission-critical applications is availability [12]. Critical infrastructures are highly depended on the availability of resources in order to fulfill their operational objectives. Sensor nodes have to be available to sense the environment, be able to communicate with other nodes and report their observations to the sink/control center. WSN applications rely on data availability to function correctly and promote appropriate decision-making. Path redundancy solutions [12] represent one of the fundamental key security research areas that have been designed to enhance the data availability and data delivery reliability and resilience, and hence keep the network operational. This research work investigates path redundancy aspects, in an effort to pursue solutions to promote the availability – reliability – resilience and survivability of a mission-critical WSN. Throughout our research in the area of path redundancy, we have made a number of observations regarding the strengths/benefits as well as the vulnerabilities of path redundancy solutions. Most of the contributions in this area focus on providing alternative route paths to the sink to ensure that at least one path exists to bypass malicious nodes and compromised routes, and deliver packets to the intended destination. The level of data availability and packet delivery reliability and resilience that can be achieved, and hence the level of operability of the application, is depended on many factors, ranging from the network topology, the path redundancy strategy, the number of malicious nodes and their location, to the attack type. Most of the proposed so far research efforts, e.g. [13, 35, 67, 68, 69, 70], address the selective forwarding attack by using alternative paths and bypassing the nodes that

actively drop packets. Although the selective forwarding attack can be successfully addressed by path redundancy, the malicious nodes are not prohibited from launching other attacks such as eavesdropping [6, 7, 8] and Denial of Service (DoS) [14, 15]. Moreover, compromised nodes may risk the multipath routing procedure, affect its operation and diminish the benefits gained.

Furthermore, other recovery solutions that have been proposed in WSNs to recover the network's operability are the blacklisting [42,43], key revocation [22, 45, 46, 47], low duty cycle [14, 15, 17, 48, 49, 50, 51, 52], reprogramming [59, 60, 61] and channel surfing [52, 55, 56, 57, 58] measures. All the aforementioned recovery solutions, including path redundancy, require that sensor nodes have to be able to communicate and forward information in order to achieve their recovery objectives. The aforementioned tasks greatly depend on the communication link availability in order to be executed successfully. If the link availability is compromised, then fundamental WSN services may function partially, or may not even function at all, jeopardizing the operation of critical infrastructures that rely on the WSN. Recovering the communication link availability, after it has been compromised, is critical as all major services such as routing, reporting and security depend on the ability of nodes to establish communication paths and forward their observations through multiple hops to the sink node. Currently, most of the research efforts in WSNs are focusing on prevention and intrusion detection solutions. Investigations in these areas have been extensive, and thus the problems/challenges in each area are well identified and understood, thus researchers know how to approach them, and a number of solutions have been designed to address them (section 2.1.5). Recovery investigations have received less attention and therefore the problems and challenges that exist are not well identified, and thus there is no clear view of the elements that constitute the problem and how to solve it. This makes the need to focus on the recovery area and design new intrusion recovery solutions even more important. Intrusion recovery is as much important as prevention and intrusion detection procedures as it aims to restore network services in case of compromisation, in order to allow the sensor network to regain a

stable operational state. We are therefore motivated to seek new solutions in the intrusion recovery area in an effort to aid sensor nodes to restore link and data availability. In particular, restoring link and data availability is challenging as it often depends on the attack type. Malicious nodes launch different security attacks in order to compromise the network's ability to communicate and affect the availability, survivability, reliability and resilience of the sensor network.

In this dissertation, we investigate the recovery from typical security attacks that can be deployed to affect the network's communication capability, focusing on the selective forwarding [6, 7, 8], eavesdropping [6, 7, 8] and DoS attacks [6, 8, 14, 15]. A malicious node can follow a static or a persistent/adaptive attack strategy to achieve its objectives. A static attack strategy consists of the execution of a specific attack against the WSN. As part of a persistent attack strategy, a malicious node can persist with a specific attack, change the attack's dynamics (i.e. increase transmission power), react based on conditions (i.e. overhearing) and/or adapt its strategy by executing a combination of security attacks. In order to address the attacks' outcome, nodes deploy appropriate recovery measures. To mitigate both static and persistent/adaptive attack strategies, the rationale of the intrusion recovery actions should be twofold. Firstly to restore the network to a normal operation and secondly to prohibit/minimize any further malicious passive or active activity against the recovered network services. Existing intrusion recovery solutions (section 2.2.1) focus mainly on the former objective. A big challenge in the design of intrusion recovery countermeasures is how to exclude the malicious nodes from the communication and isolate them so that they are prohibited from affecting the network, especially after recovery is applied. By reviewing the literature on intrusion recovery in WSNs we have observed that proposed intrusion recovery countermeasures have been designed in the context of omni-directional networks. The property of omni-directional antennas [16] to transmit and receive equally to/from all directions does not facilitate the successful isolation of malicious nodes, allowing malicious nodes to pick up transmitted data easier and also reach legitimate nodes and affect their

services, i.e. by launching a DoS attack [14, 15]. On the other hand, the property of directional antennas [16] to transmit and receive to/from specific directions, and therefore potentially exclude the direction of malicious nodes or minimize their effect, makes it a promising approach towards supporting intrusion recovery aspects. Currently, directional antennas in WSNs have hardly been investigated in an intrusion recovery context (section 2.2.2). We are thus motivated to investigate directional antennas as a means to control the communication links established between nodes and therefore promote intrusion recovery objectives.

Our research is further motivated by the need to support the operation of diverse WSN applications. Applications have diverse operational objectives [1, 3, 4] and may need to focus on different intrusion recovery requirements (discussed in section 3.4). Overestimating intrusion recovery requirements can lead to unnecessary utilization of recovery countermeasures. This could lead to extra and unnecessary cost (e.g. in terms of energy consumption, packet delivery, etc.) that is incurred from the recovery actions. Also, if intrusion recovery requirements are depreciated, then restoration countermeasures that are applied may not effectively recover the network services. The fact that applications have diverse operational objectives and intrusion recovery requirements creates the need for recovery adaptability to cope with different environments; a feature that is not addressed adequately by the research community. Moreover, the fact that adversaries may modify their attack dynamics to evade recovery and continue to attack the network drives the need for a dynamic intrusion recovery approach. The lack of adaptability and appropriate coordination of recovery actions can lead to insufficient utilization of recovery services, without been able to fully restore a compromised WSN service. Thus, adaptability is needed to coordinate different restoration actions and achieve restoration objectives. Coordination can also help in balancing resource consumption incurred from the recovery activities by deploying the appropriate recovery action that is required to address a specific attack strategy. Recovery adaptability is included in our study in an effort to address persistent and adaptive adversaries; existing intrusion recovery countermeasures mostly address a static attack strategy. An adaptable

intrusion recovery strategy should take into consideration different metrics (i.e. intrusion recovery requirements, attack type) in order to successfully restore the sensor network's operation. This research work will pursue recovery escalation and propose appropriate intrusion recovery levels in an effort to aid users to identify the intrusion recovery requirements that should be supported by their WSN and promote the network's availability, survivability, reliability and resilience. This is achieved by having an intrusion recovery policy (section 3.8) that applies intrusion recovery actions according to the situation.

1.3 Thesis contributions

This thesis addresses intrusion recovery aspects in mission-critical WSNs and proposes a new intrusion recovery framework (INCURE). Currently, in the context of intrusion recovery, design and evaluation guidelines are limited. The proposed intrusion recovery framework is envisioned to support each phase of the development of an intrusion recovery countermeasure, covering the complete sphere of requirements specification, design, implementation and evaluation. Three main components are proposed to constitute the INCURE framework and promote its objectives by specifying: (a) the intrusion recovery requirements that need to be supported by an intrusion recovery solution, (b) a new intrusion recovery countermeasure and a new recovery policy, and (c) a new evaluation method. The thesis contributions are:

(I) Analysis of intrusion recovery requirements

In order to design effective intrusion recovery countermeasures, covering diverse operational and intrusion recovery objectives, it is necessary to clearly identify what needs to be achieved with an intrusion recovery solution. Specifying intrusion recovery security

requirements is not a trivial process, especially since diverse applications may need to address different recovery objectives. Throughout the literature, researchers identify in their work aspects of security requirements in WSNs and establish appropriate security mechanisms to address these requirements. Typically a list of security requirements includes: confidentiality, integrity, authentication and availability [6, 7, 8, 17]. However, intrusion recovery needs to focus on a different set of security requirements: availability, reliability, resilience and survivability. These requirements are currently not adequately addressed in the context of restoration activities in WSNs. Studying appropriate intrusion recovery security requirements will permit researchers to gain a better understanding of the intrusion recovery elements they should focus on. In this thesis, we do not just provide another overview of security requirements but we identify the specific security requirements (section 3.4) that need to be addressed by intrusion recovery countermeasure designs.

(II) Proposal of a new intrusion recovery countermeasure and recovery policy

A new intrusion recovery countermeasure (section 3.7), called INCURE countermeasure, is proposed to support the intrusion recovery requirements specified in this thesis. The operation of the proposed countermeasure achieves three main attributes: (a) recovery of compromised WSN operation, (b) confinement of the attack source and (c) enhancement of the network's resilience when an attack continues. The rationale of the new countermeasure is not only to restore what has been compromised but also to minimize the attack initialization and to prohibit further network compromisation. The solution addresses static and persistent/adaptive adversaries that have compromised sensor nodes and gained access to the WSN. This type of adversaries pose a great challenge when it comes to security as they can compromise the network easier when compared to external threats. The proposed intrusion recovery countermeasure utilizes directional antennas to promote its intrusion recovery design objectives and address persistent adversaries. INCURE takes advantage of the directional transmission characteristics of directional antennas to create controlled communication paths

and to physically exclude malicious nodes. This thesis is mainly focused on intrusion recovery aspects, when considering typical attacks (selective forwarding, eavesdropping and DoS) that can compromise the network's communication ability. INCURE is evaluated and compared against typical intrusion recovery countermeasures implemented in omni-directional WSNs, including blacklisting and rerouting, low duty cycle and channel surfing. The proposed countermeasure has been shown to address static and persistent attack strategies and recover the network's availability, survivability, reliability and resilience in case of compromisation without any significant tradeoff. Typical intrusion recovery countermeasures have been shown to mainly address static attack strategies, often with a significant tradeoff. Blacklisting and rerouting can address the selective forwarding attack and recover nodes' packet delivery capability. The low duty cycle countermeasure can address the DoS attack and recover the network's survivability with a significant tradeoff in terms of nodes' availability and packet delivery reliability, greatly affecting decision-making. The channel surfing can address the DoS and eavesdropping attacks as long as malicious nodes do not execute a persistent attack strategy. In this thesis it is also shown that the measure of blacklisting and rerouting further increases the network's recovered performance when implemented by INCURE, as INCURE minimizes interference, packet drops and retransmissions and enables the network to achieve a stable operation. INCURE addresses a DoS attack without affecting the nodes' availability and packet delivery ability, thus it can reliably support the decision-making. Moreover, INCURE shows an increased resilience against the eavesdropping attack and malicious nodes that attack based on an overhearing case.

The operation of INCURE is driven by a new intrusion recovery security policy (section 3.8) that addresses adversaries that deploy a static or a persistent intrusion strategy. The policy aims to address a static intrusion strategy where a specific attack is executed by compromised nodes or a persistent intrusion strategy where a compromised node executes a combination of selective forwarding, eavesdropping and DoS attacks in an effort to affect the availability of sensor nodes. The recovery policy coordinates recovery actions, taking into consideration

different intrusion recovery requirements and attack conditions. The aim is to promote the availability, survivability, reliability and resilience of a WSN. The policy's operation and design is easily extendable and can promote the integration of new and/or existing intrusion recovery actions. Moreover, three intrusion recovery layers are proposed to aid users identify the intrusion recovery requirements that should be supported by their WSN and utilize the policy accordingly.

(III) Design of a new intrusion recovery evaluation method

Another major contribution of this thesis (Chapter 4) is the design of a new intrusion recovery evaluation method. The proposed method defines the security evaluation aspects and related evaluation metrics that should be considered to assess the performance of intrusion recovery countermeasures in WSNs. Our aim is twofold:

a) Support researchers into evaluating and fine-tuning their designs. The evaluation process of intrusion recovery countermeasures is challenging. In the literature, the evaluation of intrusion recovery in WSNs is not consistently investigated. In order to evaluate intrusion recovery solutions, one has to identify which are the most appropriate elements that need to be considered for their assessment. The method proposed in this thesis guides researchers into selecting appropriate intrusion recovery requirements and thus assessing the performance of their solution more thoroughly under a specific intrusion recovery context. The objective is for the evaluation to indicate if specific intrusion recovery requirements are met and if the restoration level that is achieved along with the associated cost is acceptable to recover from security attacks. Based on the evaluation results, researches can update their designs appropriately.

b) Promote the comparison of intrusion recovery countermeasures. Often, researchers use different sets of evaluation criteria [12] to evaluate the performance of their solution in terms

of security requirements. The absence of a common set of evaluation criteria prohibits even superficially the comparison with other designs. Our method promotes a set of fundamental evaluation criteria with the aim of utilizing them in the evaluation and comparison of intrusion recovery countermeasures in WSNs.

1.4 Publication list

This section provides a list of publications stemming out of this thesis. The dissemination of the thesis contributions and results was supported by ASPIDA project (KINHT/0506/03), funded by Cyprus Research Promotion Foundation.

- Stavrou, E. and Pitsillides, A. Security Evaluation Methodology for Intrusion Recovery Protocols in Wireless Sensor Networks, 15th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, *MSWiM' 12*, October 21–25, 2012, Paphos, Cyprus

- Stavrou, E. and Pitsillides, A. Vulnerability assessment of intrusion recovery countermeasures in wireless sensor networks, 16th IEEE Symposium on Computers and Communications (ISCC), pp. 706-712, June 28 - July 1, 2011, Kerkyra, Greece

- Stavrou, E. and Pitsillides, A. Combating persistent adversaries in wireless sensor networks using directional antennas, 18th International Conference on Telecommunications (ICT), pp. 433-438, May 8 – 11, 2011, Ayia Napa, Cyprus

- Stavrou, E. and Pitsillides, A. A Survey on Secure Multipath Routing Protocols in WSNs, Computer Networks Journal, Elsevier, 2010, vol. 54, no. 13, pp. 2215- 2238

- Stavrou, E., Pitsillides, A., Hadjichristofi, G., and Hadjicostis, C. Security in future mobile sensor networks - Issues and Challenges, International Conference on Security and Cryptography, July 26-28, 2010, Athens, Greece

Under submission

- Stavrou, E. and Pitsillides, A. An INtrusion reCovery secUrity framework in wiReless sEnsor networks – INCURE
- Stavrou, E. and Pitsillides, A. Intrusion Recovery in WSNs: A survey
- Stavrou, E. and Pitsillides, A. Intrusion Recovery evaluation framework in WSNs

1.5 Thesis organization

This thesis is organized into six chapters. Chapter 2 provides background information on the thesis concepts and presents existing work on intrusion recovery countermeasures in WSNs. Aspects of security in WSNs are presented as part of the background information, briefly covering: the need for security in WSNs, the main efforts towards protecting the operation of WSN applications and the current need for intrusion recovery in WSNs. Chapter 3 presents the concept behind the design of the proposed intrusion recovery framework in WSNs (INCURE), the design objectives and the actual framework, including the specification of intrusion recovery requirements and the recovery countermeasure. Chapter 4 discusses the evaluation method that is proposed to assess intrusion recovery countermeasures in WSNs and Chapter 5 analyses the performance evaluation results and investigates if the adoption of directional antennas is beneficial in an intrusion recovery context. INCURE is then compared against typical intrusion recovery solutions implemented in omni WSNs. An assessment is performed to conclude on the adequacy of the proposed/typical intrusion recovery solutions to address a static and/or persistent attack strategy and to identify if there is any tradeoff that

incurs from the recovery measures. Finally, Chapter 6 concludes the thesis and proposes future work directions.

Chapter 2

Background & State of the Art

This chapter introduces the reader to the fundamental security aspects in WSNs and then analyzes the state of the art related to this thesis' subject and objectives.

2.1 Security in WSNs

2.1.1 Critical WSN applications

WSNs are becoming an essential component in every major sector of society [1]. Applications are utilizing WSNs to support many diverse sectors (Figure 2), including military, healthcare, disaster and relief, transportation, construction, agriculture, business and industrial sectors. Sensors are utilized to perform functions [3, 5] such as event detection, periodic measurements and actuators' control, in support of applications' objectives.

A number of WSN applications perform critical operations [3, 4, 5] that need to be well protected, otherwise the applications may fail to fulfill their mission [17]. Therefore, security [6, 7, 8] is a crucial issue that needs to be addressed in WSN applications in order to protect

their operation. Examples of critical WSN applications [3, 4, 5] include: surveillance applications where sensor networks can be utilized for perimeter, border, battlefield monitoring, etc; environmental WSN applications which can help in pollution monitoring and in chemical and biological detection; medical applications which utilize WSNs for monitoring the vital signs of patients and control drug administration in hospitals; smart WSNs for monitoring the power grid and smart home infrastructures, including energy consumption/production monitoring and provide control of related equipment; disaster and relief in which WSN applications support many areas ranging from wildfire detection to avalanche victims' rescue.

When a critical event is detected by sensor nodes, observations are forwarded to the control center for decisions to be taken and appropriate actions to be triggered. During this time, it is crucial for the WSN to maintain network communication and promote data propagation to the control center. In this way, the control center is aware of the situation and can adapt its decisions accordingly. Any compromisation of the WSN operations during this time can jeopardize the responder units' actions and may even endanger human life.

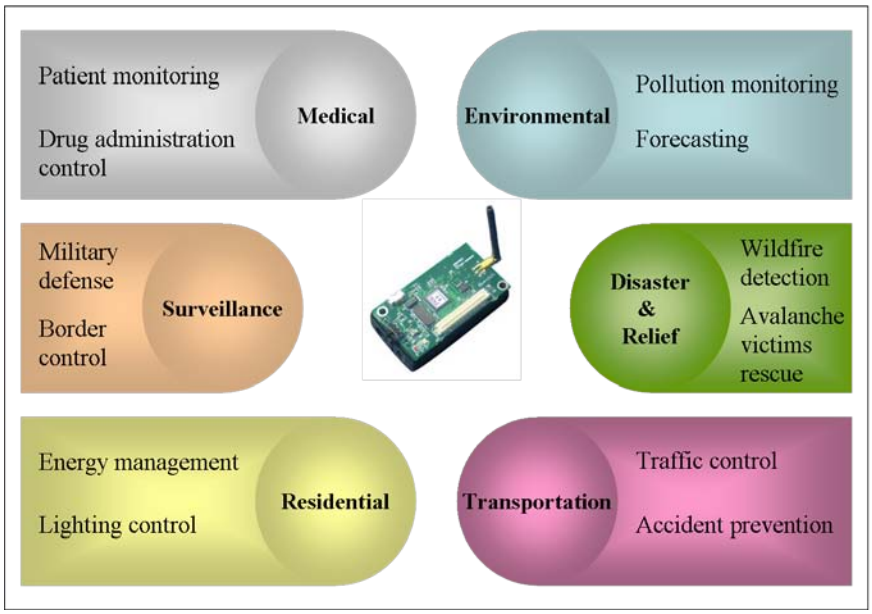

Figure 2: WSNs application space

2.1.2 Security challenges in WSNs

A number of security challenges [6, 7] exist in WSNs that can lead to the network's compromisation if not addressed properly. An adversary can compromise its operation and prohibit nodes to detect malicious activities in the WSN environment. Research efforts concentrate on addressing and overcoming the security challenges in WSNs through the design of appropriate security mechanisms. Prior to designing and developing security solutions, it is important to understand the security challenges in the WSNs in an effort to maximize security and minimize compromisation. A number of security challenges are outlined next.

2.1.2.1 Security attacks

A number of attacks [6, 7, 8, 14, 15] can be launched against a WSN and disrupt its operation. An adversary executes an attack if he has the means to do so (e.g. he participates in the active path) and according to the outcome he tries to achieve.

2.1.2.1.1 Spoofed, altered or replayed routing information

By spoofing, altering or replaying [6, 7, 8] routing information the attacker can confuse the sensor nodes in a number of ways, such as forcing them to create routing loops, establish route paths towards malicious nodes, drop traffic and partition the network communication. The attack outcome can prohibit observation of critical events and delay countermeasures from the response center.

2.1.2.1.2 Selective forwarding

One of the adversary's objectives is to include himself in an active packet flow path in order to steal passing by information and affect routing with malicious activities. In a selective forwarding attack [6, 7, 8] the adversary may choose not to forward certain packets and drop them in order to affect routing decisions and monitoring of the environment. A variation of this attack is when the adversary drops all the received packets without forwarding them, creating a "blackhole" in the network.

2.1.2.1.3 Sinkhole attack

The goal of a sinkhole attack [6, 7, 8] is to lure traffic towards the adversary that participates in the network communication. Once the adversary succeeds with the sinkhole attack, he can initiate other attacks such as the selective forwarding. The adversary can create a sinkhole by making a compromised node attractive to its neighbors. This is done by advertising high quality routes, i.e. short routes, to the destination. The neighbors that receive these advertisements will then forward all their data destined to the sink through the malicious node. Sensor networks are susceptible to these attacks due to the multihop communication pattern they use.

2.1.2.1.4 Sybil attack

The Sybil attack [6, 7, 8] involves a malicious node that presents multiple identities to the network. This means that the adversary appears to be at multiple locations and thus it can be selected more than once by neighboring nodes, compromising a number of functions such as topology maintenance, multipath routing, localization etc.

2.1.2.1.5 Wormholes

A wormhole attack [6, 7, 8] allows an adversary to tunnel packets received in one part of the network to another part of the network. The packets are then propagated in the network affecting routing decisions and the application's operation. The adversary can create a number of issues through a wormhole attack and can force sensor nodes into performing unnecessary actions; distant nodes are convinced that they are neighbors and exchange information, routing maintenance is initiated unnecessarily in different parts of the network creating confusion and making it hard for the network to converge to a stable routing state, security associations are created between non-neighboring nodes, etc. Every unnecessary action performed by sensor nodes, especially in a communication context (transmitting, receiving), consumes nodes' energy resources and minimizes the network's lifetime.

2.1.2.1.6 Hello flood attack

A number of routing protocols use hello packets to aid nodes in discovering their neighbors. When a node receives a hello packet it assumes that the node that transmitted the packet is within its range and therefore considers it as its neighbor. The adversary can convince every node in the network that it is their neighbor by transmitting with high power. The attack [6, 7, 8] will force packets to be lost if nodes try to forward packets through nodes that perceive as their neighbors but in fact they are not in their transmitting range.

2.1.2.1.7 Acknowledgment spoofing

Communication protocols may utilize acknowledgments to denote a successful packet reception. A receiving node sends an acknowledgment to the sender if it has received the

transmitted packet. If the sender does not receive the acknowledgment, it may assume that the packet was not received and thus retransmits it. The adversary may spoof an acknowledgment [7, 8] convincing the sender that a weak link is strong or that a dead node is alive. The outcome of this attack is to fool nodes to continue using bad quality links, on the ground that the packets are successfully delivered. In fact, packets are lost and never reach the destination. This will affect the decision making and the application's objectives.

2.1.2.1.8 Denial of Service

With a Denial of Service attack [6, 7, 8, 14, 15] the adversary target is to deny the network to perform its expected operation. The adversary tries to prohibit the nodes' communication by overwhelming the network with a large volume of traffic that cannot be handled by sensor nodes, consuming network bandwidth and reducing nodes' energy. A DoS attack can severely degrade the network's performance as the large volume of traffic that is often involved in the attack leads to an increased number of packet collisions, packet retransmissions, packet loss, packet delivery delays, forces nodes to stay in receive mode and prohibit them to send their observations in a timely manner.

2.1.2.2 Environment

The deployment environment, the communication medium and the sensor nodes' characteristics [5, 6, 17] may also risk the WSN operation.

2.1.2.2.1 Hostile/ unattended environment

Sensor networks are often deployed in remote or hostile environments (i.e. battlefields) [5, 6, 17] where they may be physically accessed by an adversary. An adversary could capture a sensor node, destroy it or even introduce his own malicious nodes inside the network. The adversary's objective is to compromise the WSN operation and prohibit nodes from supporting their operational objectives. Different levels of node compromisation can occur [18]. Any sensitive information that may be collected could be used for malicious purposes, for example, stolen cryptographic material can be used to initiate communication with legitimate nodes.

2.1.2.2.2 Insecure wireless medium

Wireless communication is susceptible to eavesdropping [6, 7, 8]. An adversary who is physically located within the transmission range of the sensor nodes can overhear network communication. Captured packets can be read by the adversary if they are not well protected and traffic analysis can be performed to discover the location of critical sensor nodes, as e.g. the sink.

2.1.2.2.3 Personnel

Human resources [19] can pose a threat to the operation of the WSN if not taken into consideration and addressed properly by security procedures. Terminated or disgruntled personnel may deliberately misuse the system and information and help third parties to easily compromise the sensor network. Moreover, security misconfigurations on the WSN that happen due to a lack of security education or negligence by the involved personnel can also lead to vulnerabilities that can be exploited by adversaries.

2.1.2.3 Sensor node limitations

2.1.2.3.1 Energy

Energy [5, 17] is considered to be an outmost value resource in a WSN. Usually batteries are used as a source of energy making it difficult to replace or recharge them, especially when the WSN is deployed in remote or hostile areas. This could lead to situations where sensor nodes are disabled due to energy depletion, affecting the connectivity and operation of the network. Energy is consumed during sensing, communication and data processing operations with energy consumption been greater during communication [5]. Security is constrained due to energy limitations since security mechanisms often introduce a (usually significant) processing and communication overhead [8] between the nodes, for example, more messages must be exchanged for key management purposes, leading to higher energy consumption levels.

2.1.2.3.2 Memory

Typical sensor nodes have very limited memory and storage capacity [5, 17]. Table 1 lists the resources of typical commercial WSN platforms. A typical sensor node, i.e. Micaz, has an 8MHz processor with 128 KB of instruction memory, 4 KB of RAM and 512 KB of external flash memory. The limited capability for memory affects the storage of security-related data, i.e. cryptographic keys. For example, according to the encryption scheme used, each sensor node may need to know a number of keys for each other node in the network to secure communication. However, the large number of sensor nodes requires a lot of memory, which may not be provided.

Table 1: WSN commercial platforms

Platform	**MCU**	**Radio chip**	**RAM**	**Program memory**
WiSMote	MSP430F5437	CC2520	16KB	256KB
Ubimote2	MSP430F2618	CC2520	8KB	116KB
MICAz	ATmega128L	CC2420	4KB	128KB
Tmote Sky	MSP430 F1611	CC2420	10KB	48KB
Jennic	RISC	JN5121	96KB	64KB

2.1.3 Typical security requirements

Security requirements [6, 7, 8, 17] provide information on what we are trying to protect. Studying the security requirements permits developers to apply appropriate security techniques to ensure the protection and safety of the WSN and its data. This section analyzes the main security requirements (confidentiality, integrity, authentication, and availability), as discussed in the literature. These security requirements constitute fundamental objectives based on which every sensor application should adhere in order to guarantee an appropriate level of security.

2.1.3.1 Confidentiality

The confidentiality requirement [6, 8, 12, 17] ensures that sensitive information is well protected and not revealed to unauthorized third parties. The confidentiality objective is required in WSNs to protect information exchanged between nodes from disclosure. An adversary that participates in the network or eavesdrops on the communication can obtain critical information such as observed data and routing information. Based on the sensitivity of

the data stolen, an adversary may cause severe damage since he/she can use the sensing data for many illegal purposes, i.e. sabotage, blackmail etc.

2.1.3.2 Integrity

There is the danger that information could be altered when exchanged over insecure networks. A lack of integrity controls could result in many problems since the consequences of using inaccurate or false information could be disastrous. Many sensor applications such as pollution and healthcare monitoring rely on the integrity [6, 8, 12, 17] of the information to function with accurate outcomes; it is unacceptable to measure the magnitude of the pollution caused by chemicals waste and discover later that the information provided was improperly altered. Therefore, there is a strong need to make sure that information is traveling from one end to the other without being intercepted and modified in the process.

2.1.3.3 Authentication

Authentication techniques verify the identity of the participants in a communication, distinguishing in this way legitimate users from intruders [6, 8, 12, 17]. In the case of sensor networks, it is essential for each sensor node and sink node to have the ability to verify that the data received was really sent by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. Sensitive applications rely on the trustworthiness of the communicating entities to provide their services. However, if authentication is compromised, decision-making may be affected and erroneous and harmful decisions may be made.

2.1.3.4 Availability

Availability [6, 8, 12, 17] ensures that services and information can be accessed at the time that are required. In sensor networks there are many risks that could result in loss of availability such as denial of service attacks and energy depletion. The lack of availability may affect the operation of many critical applications like those in the healthcare sector that require a continuous operation that could even result in the loss of life. Therefore, it is critical to find ways to restore compromised sensor nodes and allow the network to continue its operation.

2.1.4 Threat models

This section analyzes aspects of the threat models that need to be considered in the design of security mechanisms in WSNs, categorized in terms of threat models and adversarial objectives.

2.1.4.1 Categorization

Threat models [7, 8, 12] are usually categorized according to the adversary's ability to constitute an internal or external threat. If the adversary is not part of the network, then he can act as an unauthorized entity and he is considered an external threat. If the adversary compromises sensor nodes and turns them malicious, then he can be authorized to participate in the network and malicious nodes will be perceived as legitimate entities. In a security context, internal adversaries pose a greater threat than external adversaries. Internal adversaries may access sensitive information [19] such as encryption keys, trust management data, routing control information, install malicious code, etc. External threats are easier to address as security mechanisms such as cryptography often prohibit the successful execution of security attacks.

Another category of threat models which needs to be considered when designing security mechanisms involves the adversary's knowledge and motivation. There are arbitrary and novice adversaries that have a basic knowledge of security issues and they launch a static intrusion attack strategy, involving the execution of a single security attack, as a means of experimentation. Often, they do not understand the extent of damage they can cause. This category of adversaries is not considered to pose a high risk for the WSN operation. However, persistent adversaries can severely damage a WSN. This category involves adversaries that have advanced programming skills and their main motivation is to compromise the network's operation [20]. They have dedicated objectives to prohibit or stall the observation and the identification of critical events. To achieve their objectives, adversaries target the availability, reliability and resiliency of the sensor network.

Security designs need to take into consideration both threat models in order to design appropriate security mechanisms that will suppress internal or external malicious activities that may be triggered by adversaries deploying a static or a persistent attack strategy. This thesis considers an adversary that has compromised sensor nodes, turned them malicious and executes a static or a persistent attack strategy. A static attack strategy consists of the execution of a specific attack against the WSN. As part of a persistent attack strategy, a malicious node can persist with a specific attack changing the attack's dynamics (i.e. increase transmission power), react based on conditions (i.e. overhearing) and/or adapt its strategy by executing a combination of security attacks. The terms "persistent", "adaptive" and/or "reactive" malicious nodes are used interchangeable in the thesis to refer to the case where a persistent attack strategy is deployed by malicious nodes.

2.1.4.2 Adversarial objectives

The need for securing a WSN increases, as there are a number of attacks that can be launched by an adversary against the WSN. Therefore, it is very important to investigate an adversary's malicious objectives [12], especially in the case of a persistent adversary, in order to gain a better understanding of his motives, what he is actually trying to achieve and in what way. Such an understanding will be useful when designing security mechanisms to limit potential damage during an attack or even stall a security incident from the early beginning. The main attack outcomes are:

- Events not reported or delayed: Sensor nodes observe their environment according to the application's objectives, establish communication with neighbor nodes and forward observation of events through multiple hops to the sink. Reporting of events mainly depends on the ability of nodes to communicate and propagate received packets towards the sink. The adversary launches attacks, for example a DoS, to prohibit or delay the propagation of events to the sink [6, 8, 12, 17]. Network partitioning can be achieved as the malicious node compromises sensor nodes whose location is considered critical e.g. they link different areas that otherwise, would not have been able to establish communication. Decision making will be affected as observations are not received or delayed rendering them useless. By having areas at which reporting cannot be established between sensor nodes, the adversary can act maliciously without been caught.

- Route compromisation: WSNs can be implemented in remote and even hostile environments where they may operate unattended for a long period of time. Since physical security cannot be established, an adversary can capture a node and turn it into a malicious node or even introduce his own nodes into the network. The malicious node can affect the routing process by modifying the routing paths. Compromising the routing paths can also be done when the adversary eavesdrops on the communication, and captures and modifies the packets exchanged between nodes. These actions can lead to

different outcomes such as routing loops, construction of non-optimized routes, dead-end routes, inclusion of malicious nodes within routing paths, etc [6, 8, 12].

- Network congestion: An adversary who steers traffic towards a specific area may overflow that part of the network causing congestion at nodes [6, 8, 12, 17]. If nodes are not able to handle the extra traffic, they may drop packets. This situation may cause great loss and even delay in delivering packets, or even a total network disruption due to node energy depletion. Dropping packets containing sensitive data e.g. crypto keys, observation data etc, at highly congested nodes may affect critical applications that depend on the timely and reliable delivery of the data. Furthermore, delays in the network can affect mechanisms that use synchronization to function, disrupting the communication between nodes that are required to be synchronized.

- Energy exhaustion: Energy is often very limited in WSNs. Assuming that the batteries are the main source of energy, their replacement or recharging is often not practical since sensors can be deployed in remote and unreachable locations. Energy consumption occurs during the communication and processing at a node. The adversary targets to increase the energy consumption [8, 12, 17] at a considerable rate, in order to drain the batteries and disable the node from participating in the network. In the meantime, the adversary may have stolen the node's identity and sensitive data e.g. crypto keys, impersonating it and acting maliciously against the network.

- Routing database divergence: The adversary tries to prevent the routing protocol from converging to a stable state [7, 12]. Having a malicious node flooding the network with route discovery requests will trigger the routing procedure over and over again, creating more traffic, delays, instability of the routing tables etc. All these could lead to a collapse of the network.

2.1.5 Security controls: Prevention & Intrusion detection

Security spans into different research areas [6, 7, 8, 12, 17], supporting diverse functionalities and security requirements. Currently, most of the research efforts are concentrated towards two research directions: prevention and intrusion detection.

Prevention mechanisms act proactively with the objective of preventing security attacks that will allow the adversary to gain access to the network, steal and manipulate information. A number of key research security areas [6, 7, 8, 12, 17] are categorized under the prevention direction. One of the fundamental prevention areas focuses on the efficient usage of cryptographic schemes to authenticate and encrypt the transmitted data. The utilization of cryptographic schemes is supplemented with appropriate key management schemes, i.e. [21, 22] that establish the procedures related to the generation, exchange and update of encryption keys. Regarding cryptographic schemes [8, 17], the simplest option is to use a globally shared key among all the sensor nodes in the network to prevent adversaries from reading data. However, if the adversary manages to compromise a legitimate node and steal the shared key, then he will be able to masquerade as any node and launch other attacks. Other solutions have adopted more sophisticated cryptographic schemes, i.e. asymmetric cryptography, probabilistic key distribution, etc., however, often with a higher overhead and consumption of nodes' resources. Other prevention-related solutions are categorized under the areas of: secure localization, secure data aggregation, trust management and secure routing. These security areas usually support some form of cryptographic operations to promote their objectives. Secure localization [23] focuses on how the sensors can securely determine their location, even in the presence of adversaries. Secure data aggregation [24] aims to safeguard the aggregated data, prevent the compromisation of aggregators and protect the communication between sensor nodes and aggregators. Trust management schemes [25] build and manage trust relationships between sensors based on reputation values in order to forward packets through more secure areas. Secure routing [8, 12, 17] is another fundamental research area

that is concerned with the protection of the routing operation. Routing is the fundamental operation in WSNs that facilitates the establishment of communication paths between sensor nodes and the packet delivery. Most of the security key areas such as secure data aggregation, secure localization, key management, etc., rely on routing schemes to exchange data and support their operation.

As mentioned earlier, the efforts in the prevention security area aim in prohibiting an attack from been executed successfully and in protecting the WSN's operation. When protective measures are not adequate and fail to prohibit adversaries from compromising the network, it is important to identify misbehavior and the services that have been compromised. The intrusion detection research area is concerned with the design and deployment of mechanisms that target to detect malicious activity in the network in order to allow the sensor nodes to address the situation. Several mechanisms have been proposed by the research community to address intrusion detection aspects. Intrusion detection follows two main approaches [8, 26, 27, 28]: local-based or cooperative-based.

A local-based IDS, i.e. [29, 30, 31, 32], involves a single node that performs intrusion detection locally and detects a compromisation. For example, Marti et al. [30] proposed a reputation-based scheme composed of a watchdog and a path-rater module in order to determine whether intermediate nodes are indeed forwarding the received packets. The watchdog node overhears the communication to verify if its neighbor node has forwarded the packet. Based on the result, the pathrater rates each path and chooses a path to avoid misbehaving nodes. Lee and Choi have also designed another scheme [31] using the concept of a neighbor watch system (NWS) to detect maliciously packet dropping nodes in sensor networks. The idea of the NWS is to check if the neighbor of a node has really forwarded the relaying packet to its neighbor. This means that decisions are taken locally by sensor nodes without referring to the sink or other neighboring nodes.

Cooperative-based IDS, i.e. [33, 34, 35, 36, 37], perform intrusion detection cooperatively through a number of nodes, that communicate to decide whether an intrusion has occurred or just to inform each other about the incident. Wang et al. [33] proposed a cooperative detection technique where the nodes around a suspected node collaborate with each other to reach an agreement on whether the suspect is malicious. A similar approach is proposed by Lee and Choi [35] where the detection is decided by the sink node. Their protocol addresses the selective forwarding attack and detects the malicious nodes that advertise inconsistent routing information by having a neighbor report system. When a node advertises inconsistent information, its neighbor nodes report its identity to the base station. Then, the base station informs the entire network so that sensor nodes will revoke the associated cryptographic keys and exclude the malicious node from the network. Another cooperative-based IDS is proposed by Buchegger et al. [34] where a reputation-based scheme is deployed to promote detection of malicious nodes. Once a node detects a malicious node it sends warning messages to other nodes in the network to alert them. Nodes evaluate the warning messages they receive and they decrease the reputation of a node if a number of trusted nodes have reported the node as malicious.

Once an attack is detected, the network needs to respond appropriately in order to restore the compromised services. This means that intrusion detection mechanisms need to trigger recovery actions based on the detection findings in order to try to overcome the compromisation. In the case of local intrusion detection, it is expected that intrusion recovery is applied locally when an incident is identified. Cooperative intrusion detection is expected to promote cooperative recovery in the sense that more nodes apply a recovery countermeasure to address the same security incident. Currently, recovery aspects in WSNs have not been actively investigated in the context of intrusion detection research.

2.1.6 The need for intrusion recovery

Prevention mechanisms are not flawless solutions and, thus, protection can be compromised by adversaries. The compromised services have to be restored in order to maintain a reliable and correct operation. This objective is very important to critical WSN applications that rely on sensor nodes observations and their communication ability to support their objectives and decision-making. This means that sensor nodes have to be available to monitor their environment and communicate with the rest of the network to propagate observations to the decision center. If the nodes' services get compromised, they have to be restored to promote a stable performance and operation as required by the application. This is an extremely urgent task to achieve, especially for critical applications, i.e. [38, 39, 40, 41], where continuous briefing is required on the situation until response units reach the area and/or countermeasures are applied. Thus, the WSN recovery should not be taken lightly but rather it should receive the attention it demands by the research community.

As mentioned earlier, intrusion detection needs to trigger recovery once an attack/compromisation is detected. The state of the art in intrusion detection research area focuses mostly on detection activities, following two main approaches. One approach investigates only detection activities without considering recovery features at all. The other approach considers that once malicious activity is identified, then some very basic form of recovery is provided. However, these approaches are not adequate to address different attacks and recover the WSN from compromisation. The fact that the adversaries have the means in terms of knowledge and tools [20] to perform different attacks in order to compromise nodes' operation, makes the need to focus on recovery even greater. Currently, mostly static attack strategies are addressed in WSNs, neglecting investigations towards adversaries that have compromised sensor nodes, have turned them malicious and execute a persistent and adaptive attack strategy.

In a security context, there are two overall strategies that need to be taken into consideration: the security strategy of the WSN and the attack strategy of the adversary. The former strategy targets to protect the network's operation while the latter strategy focuses on compromising the WSN's operation. The security strategy of the network needs to adapt as the attacks progress in order to cope with the security incidents. Therefore, it is imperative that the WSN follows a holistic security approach [9, 10, 11] based on the triptych prevention – intrusion detection – intrusion recovery. These three components comprise a spherical security strategy with each component compensating the other. Prevention can be thought as the first line of defense. If the adversary compromises protection then the second line of security, intrusion detection, is called to handle the situation. Upon detecting the compromisation, intrusion recovery is triggered acting as the third line of security in order to restore the operation. An escalation of the security approach is required in order to offer a broad range of security services, proactively and reactively. Each component is equally important and significant in the security process, thus its operation needs to be well studied to promote appropriate solutions. The prevention and intrusion detection research areas have been extensively investigated and promising mechanisms have been proposed. Attention should now shift to the recovery area which has so far been largely neglected. Investigations will aid the researchers to design recovery countermeasures against different attack strategies in order to regain compromised services and restore normal network operation. Research in the prevention and intrusion detection areas is foreseen to continue, however, researchers should take into consideration the need for recovery and should address potential cooperation requirements, promoting new contributions in all security areas.

2.2 Related work

2.2.1 Intrusion recovery countermeasures

Intrusion recovery countermeasures in WSNs have been mainly developed for simple adversarial environments where adversaries are not persistent with their attack strategy. The following sections overview existing intrusion recovery countermeasures in WSNs, discussing the security benefits and weaknesses of each approach.

2.2.1.1 Blacklisting malicious nodes

The simplest typical recovery countermeasure is the blacklisting method [42, 43]. Sensor nodes blacklist detected malicious nodes and do not accept or forward any kind of communication from/to nodes listed in the blacklisting cache. Packets received from blacklisted nodes are dropped. A variation of blacklisting a node is proposed in [44] where the protocol blacklists insecure locations. Blacklisting is often promoted by reputation-based trust schemes, e.g. [30, 42], where the utilization of next hops depends on their reputation value. The reputation value reflects the good or bad behaviour of a node over time and drives the applicability of the blacklisting measure. A low reputation value (as defined by the application/solution) indicates a misbehaved node that is penalized by not been selected for routing by its neighbors. Blacklisting can effectively address the selective forwarding and blackhole attacks and restore the availability and packet delivery reliability of the WSN. These attacks are effective if the adversary can participate on active route paths. With the blacklisting method, sensor nodes stop selecting malicious nodes as the next hop towards the sink and, thus, prohibit the adversary to launch the aforementioned attacks. The sinkhole and wormhole attacks are also addressed. Once the malicious node that launched the attack is detected and blacklisted, nodes stop accepting and forwarding packets from blacklisted nodes. For example, if the detected malicious node advertises a high quality route towards the sink, it will not be considered by the node if the malicious node is blacklisted and the attack will be

suppressed. If the adversary executes the aforementioned attacks, then the network can recover its operation by using the blacklisting method. However, the adversary can still receive broadcasted packets and eavesdrop on the communication if configured on a promiscuous mode. This means that malicious nodes can execute other attacks, such as traffic analysis, spoofing, replaying routing information, etc. In terms of a DoS, the attack cannot be fully addressed. In a DoS attack the nodes can prohibit the propagation of unnecessary malicious packets in the network by not forwarding them. However, the adversary can compromise a node in its vicinity by overflowing it with packets and forcing it to drop packets, depleting its energy, causing packet collisions at the nodes and prohibiting them from propagating critical events, forcing the node to stay in receive mode and not transmit packets, etc. This countermeasure is mainly proposed in the context of selective forwarding and blackhole attacks. When considering dynamic and persistent adversaries, the blacklisting countermeasure on its own cannot prohibit the adversaries from continuing their malicious efforts to compromise the network.

2.2.1.2 Cryptographic keys revocation

A number of cryptographic protocols [8, 17] have been proposed to protect the confidentiality, integrity and authentication of the communication. If the adversary manages to compromise sensor nodes, he can steal sensitive information such as the cryptographic keys that are stored on the nodes. This means that malicious nodes can continue taking part in the communication, reading and altering information and affecting the operation of the WSN. To address compromised cryptographic keys and restore the confidentiality, integrity and authentication of the communication, key revocation protocols [22, 45, 46, 47] have been proposed. These protocols revoke the compromised cryptographic keys in order to prohibit the malicious node to be perceived as a legitimate network entity. Revoked keys are no longer used and therefore malicious communication is prohibited from spreading in the network.

Although this recovery countermeasure can aid the network to restore the confidentiality, integrity and authentication of the communication, it cannot address attacks that target the availability and reliability of the network such as a denial of service (DoS) attack [14, 15]. Cryptographic keys can be established using different communication patterns. For example, global keys, pairwise keys, and group keys can be established. This means that once a key is revoked and depending on the context (communication pattern) it is used, it may need to be updated. One of the key security research areas discussed in section 2.1.5 is key management. A number of key management protocols exist that define the procedures to update and exchange the encryption keys. Therefore, nodes have to be available and able to communicate in order to establish the handshaking and update the encryption keys as defined by the utilized key management protocol. However, attacks like the DoS can affect the operation of the key management mechanisms by not allowing nodes to receive/exchange cryptographic information and thus prohibit the network from establishing new cryptographic keys. This means that portions of the nodes that cannot update the encryption key will not be able to participate in the communication. Also, every time the key management procedure is invoked increases the communication overhead and the energy consumption in order to support its objectives. Thus, in the case where the network has to initiate the key management a number of times to address an attack outcome, it executes a costly operation that can affect the survivability and availability of the network.

2.2.1.3 Low duty cycle

An active attack such as a DoS can be devastating for the operation of WSNs, because the malicious nodes can greatly affect the availability of nodes, the resilience and reliability of the network. Intrusion recovery countermeasures such as blacklisting and key revocation cannot prohibit a DoS attack from compromising the network and the decision making process. To address this attack and protect the nodes' energy, nodes try to avoid the attack during its

execution, by deploying a low duty cycle strategy [14, 15, 17, 48, 49, 50, 51, 52]. Sensor nodes utilize a low duty cycle to go to sleep in an effort to turn the DoS attack ineffective. With this approach, the attack is ineffective during the time that nodes are utilizing the low duty cycle. The low duty cycle solution can protect the energy consumption and thus the network's lifetime when considering attack conditions. However, this approach may affect the network's packet delivery capability and decision-making since nodes are turned unavailable during the low duty cycle countermeasure. Currently, there is not much research performed in the context of a low duty cycle solution under attack conditions. Traditionally, the low duty cycle [53] has been proposed by researchers as a measure for energy conservation in WSNs. However, most of the proposed protocols have not considered security aspects and can be exploited by an adversary in order to launch a denial of sleep attack [15] and prohibit sensor nodes from entering a low duty cycle. The low duty cycle approach looks promising to address DoS attacks, although that there are significant tradeoffs that need to be taken into consideration. In this thesis, we take into consideration the benefits and tradeoffs of the low duty cycle approach for the design of a new intrusion recovery countermeasure that can utilize the concept of low duty cycle with a new perspective and address its tradeoffs.

Similar to the concept of the low duty cycle strategy is the protocol proposed by Wood et al. [54] called JAM. To recover from jamming attacks the authors propose the detection and mapping of the jammed area in order to avoid this area for routing, by rerouting around the jammed area. However, the events that are triggered in the area covered by nodes that are under attack may not be forwarded to destination. This can affect the decision making and response to critical events. Moreover, the sensor nodes that are compromised by the attack can be forced to a state of increased energy consumption, during the attack execution, affecting their survivability. Also, if the adversary adjusts the transmission power it can increase the affected area. In the case where a significant portion of the nodes are affected, the network performance can be severely degraded and services may turn unavailable.

2.2.1.4 Channel surfing

One of the objectives of the malicious nodes is to prevent sensor nodes from communicating. Therefore, nodes have to exclude the malicious node from the network in such a way as to prohibit the malicious communication from reaching sensor nodes and prohibit attacks such as DoS. Channel surfing [52, 55, 56, 57, 58] is a recovery countermeasure that can accomplish the aforementioned objectives and exclude the malicious nodes from the network communication, turning security attacks ineffective. At the deployment phase or during runtime, nodes are configured to use a specific frequency to communicate. To address an adversary that executes an attack against the network, utilizing the network's frequency, nodes switch to a new frequency after the attack is detected. In this way, nodes communicate over a different frequency, leaving the malicious node operating on the default frequency and turning the attack ineffective. However, this countermeasure does not prohibit a persistent adversary from trying to eavesdrop on the communication. If the malicious node is reprogrammed to scan available frequency channels and discovers the new frequency, then the countermeasure will be suppressed and the adversary can continue successfully attacking the network.

2.2.1.5 Reprogramming

Once an adversary compromises sensor nodes, it can turn them useless in terms of legitimate functionality. As malicious nodes increase in the network, they decrease the network's resources in terms of sensor nodes and they can risk the network's operation. Deploying intrusion recovery countermeasures such as blacklisting, channel surfing, etc., may temporarily address security attacks. However, malicious nodes still exist and can continue being a threat as they can participate in the network's communication and affect its operation. Researchers have proposed to reprogram [59, 60, 61] the malicious node into the correct

operation as another means of recovering the network resources. Such an operation is considered complicated and costly that may not be easy or efficient to perform on-line, especially as malicious nodes increase. Reprogramming requires that the application code is transmitted to the malicious node, increasing the network communication and the energy consumption. Neighbor nodes share the task and the load of sending the application code to the compromised node. In order for the reprogramming to be successful, there are two main conditions: (1) the malicious application code cannot intercept the reprogramming procedure and (2) the sensor nodes can access the wireless channel to communicate and forward the application code to the compromised node. Attacks such as DoS can prohibit the reprogramming intrusion recovery countermeasure.

2.2.1.6 Path redundancy

Special focus has been given by the research community to recover the availability and reliability of information. In the context of sensitive WSN applications, establishing and maintaining the availability and the reliability of the information is considered vital for an application to serve its objectives successfully. Routing [5] is one of the fundamental WSN operations that establishes communication paths between sensor nodes and supports forwarding data from a source to the destination node. The common practice in WSNs is to establish single path routing [62, 63] between the source and destination nodes. However, failure of nodes along the path would mean failure of the path and loss of data. Furthermore, if routing is compromised then the entire WSN is endangered. Researchers have designed protocols to support path redundancy [12, 63] to enhance the availability and the reliability and, thus, the resilience of the network.

A number of secure multipath routing protocols, i.e. [13, 25, 31, 35, 64, 65, 66, 67, 68, 69, 70], have been developed to address specific security problems and attacks in the routing

process. Although each protocol has its own objectives, the protocols' operation is driven by two main components: the multipath routing strategy and the security measures that are deployed to further protect the network's operation. The multipath routing strategy defines issues such as the criteria based on which the alternative paths are established and used and it is of great interest in the context of intrusion recovery aspects as it supports the restoration services provided by the multipath routing protocols.

From the existing literature on secure multipath routing protocols in WSNs, a set of routing-related criteria have been identified [12] to constitute the multipath routing strategy based on which network routing is established:

- Number of paths

In a multipath routing protocol, more than one path [25, 66, 71] is established for communication. This means that packets have a better chance to reach the destination in comparison to single path routing. However, this also enhances the adversary's chance to compromise data because multipath can make data available at multiple locations.

- Path type

There are two kinds of alternative paths that can be used in the path establishment procedure, braided [35, 72, 73] and disjoint [21, 74, 75] paths. Braided paths include common nodes between the paths while disjoint paths do not share any common nodes. This means that if a common node is compromised in the braided paths, all paths that include that node will be affected. However, if disjoint paths are used, a compromised node can only affect at most the path that includes it. Therefore, disjoint paths have a higher security and reliability level than braided paths but they are also more difficult to setup.

- Path selection mode

A number of path selection strategies can be used in multipath routing, such as the following:

- Round robin transmission [35], which uses all paths, one path each time.
- Redundant transmission [71, 74], which uses all alternative paths at the same time.
- Single path [25, 31] that turns into multipath when an event occurs.

The path selection mode should be selected based on the application's objectives, the security requirements and the sensor nodes capabilities.

- Packet transmission mode

There are three types of packet transmission modes.

- Single mode [35], where a different packet is sent along each alternative path.
- Copy mode [71], where multiple copies of the same packet are sent over the alternative paths.
- Split mode [66, 74], where a packet is splitted in fragments using an appropriate threshold secret sharing algorithm [76] and the fragments are sent to the destination over the alternative paths. The destination has to receive all the packets or a certain number of packets (the number is defined by the coding algorithm) in order to reconstruct the original packet. This mode makes it more difficult for the adversary to compromise communication because he has to steal the appropriate fragments, over the different paths that are forwarded, in order to reproduce the original packets.

The way the multipath routing strategy is utilized by the routing protocols affects the level of recovery that can be achieved in terms of data availability and packet delivery reliability and resilience.

Proposed protocols follow two design approaches, tolerance-driven intrusion recovery and attack-driven intrusion recovery. A tolerance-driven intrusion recovery path redundancy countermeasure approach, i.e. [71], proactively applies appropriate actions before any incident has occurred. The aim of this approach is to tolerate undetected attacks in an effort to allow the network to retain the availability and reliability of information, even if some portion of the network is compromised. Intrusion tolerance promotes recovery objectives in the sense that it can tolerate undetected attacks, minimize the risk of service loss and retain the operability of the network. An attack-driven intrusion recovery path redundancy countermeasure approach, i.e. [25, 31], deploys a countermeasure once an attack is detected with the aim of minimizing the damage caused by the attack and preventing further compromisation. Each design approach utilizes a different configuration of the multipath routing strategy in order to achieve its objectives.

In the intrusion tolerance approach, the path selection mode may follow one of the following strategies: round robin or redundant transmission. The round robin path selection mode utilizes the single mode transmission where a different packet is sent along each alternative path. The latter mode uses all alternative paths at the same time utilizing either the copy or the split packet transmission. The rationale of the intrusion tolerance is to achieve having at least an alternative path that is not compromised by an adversary in order to tolerate undetected attacks and promote packet delivery at the destination through unaffected routes. In the attack-driven intrusion recovery approach, a single path is utilized and once malicious activity is detected the routing turns into multipath in order to recover compromised WSN services.

The level of information availability and reliability that can be recovered by path redundancy countermeasures depends on a number of factors. There are a number of attacks that cannot be prohibited with redundant routing; however, redundant routing successfully addresses the selective forwarding attack. Most of the researchers address the selective forwarding attack by using alternative paths and bypassing the node that actively drops packets. However, attacks such as a DoS, eavesdropping and altering cannot be prohibited since if a malicious node still has neighbors in its vicinity or is near an active path, it can continue compromising the network. For example, when a redundant routing strategy is utilized it introduces data redundancy in the network. With more data been available at multiple locations, an adversary has more opportunities to intercept the communication and launch other attacks, i.e. replay attack. As malicious nodes increase in the network, they can compromise more active route paths and turn the path redundancy countermeasure ineffective. Moreover, a number of attacks can be launched against the routing and compromise the route discovery procedure. This kind of compromisation can give the adversary control over the alternative path establishment and manipulate it in a way that he can participate on route paths or even prohibit the discovery of alternative paths. Moreover, the packet reliability and delivery resilience depend on the attack executed by the malicious nodes. With the tolerance-driven intrusion recovery approach the selective forwarding attack is not prohibited but rather tolerated. Often, this approach works without the need of detecting malicious nodes i.e. [77]. This means that with this approach the selective forwarding attack is not entirely addressed since malicious nodes may be included in future communication and continue misbehaving. With the attack-driven intrusion recovery approach the malicious nodes are excluded from routing tables so that they will no longer participate in active route paths. However, attacks such as a DoS are not well addressed and when executed they can affect the multipath operation by prohibiting sensor nodes from communicating. The path type (braided or disjoint) considered by the routing protocol also affects the reliability level. Braided paths have common nodes between the different paths. Compromising a common node can lead to the compromisation of a number of paths, therefore risking the data delivery to the intended

destination. On the other hand, disjoint paths do not include any common nodes, so compromising a single node can only affect the path that contains that node and, thus, the data delivery probability is increased.

Path redundancy can promote the availability of information depending on the attack conditions. However, the information availability and reliability level that can be achieved is greatly depended on the link availability. In order for path redundancy to achieve its objectives, sensor nodes have to be able to communicate and forward information. The challenge is for the network to be able to construct and operate alternative route paths, even at the presence of malicious nodes and promote the information availability and reliability. This can be achieved by ensuring multiple node (and thus link) availability, leading to increased node participation in the discovery and utilization of alternative routing. This thesis pursues such a solution in order to support WSN operations that require nodes' availability to successfully deliver their intended functionality, such as path redundant routing.

A comparison of the applicability and limitations of the aforementioned intrusion recovery solutions is presented in Table 2 (section 2.3).

2.2.2 Prevention security protocols utilizing directional antennas

The aforementioned recovery countermeasures have been proposed in the context of omni-directional WSNs. Directional antennas have received little or no attention for supporting intrusion recovery services in WSNs (a brief overview of some fundamental concepts of wireless communications and of directional antennas appears in APPENDIX A). Most of the investigations on directional antennas in WSNs have focused on the design of MAC protocols [78, 79, 80, 81, 82, 83, 84]. Although directional antennas have been utilized to increase the communication range, reduce packet collisions, etc, they have not been

substantially considered for supporting security objectives in WSNs. The security benefits of directional antennas have only been briefly investigated in wireless and sensor networks with most of the efforts concentrating on defense aspects.

Hu and Evans [85] use directional antennas and neighbor cooperation to prevent wormhole attacks in ad hoc networks. Sensor nodes use the directional antennas to obtain direction information and discover their neighbors. Legitimate neighbor relationships are established through verifier nodes. In this way, nodes can verify whether a connection is established from a non-neighbor node and therefore can identify the wormhole attack. Lazos and Poovendran [23, 86] have proposed a similar approach in their secure localization scheme to detect wormhole attacks. Their scheme utilizes locators equipped with directional antennas that aid sensors to determine their location based on the intersection of the areas covered by the beacons transmitted by multiple locators. The sector uniqueness property aids in the detection of a wormhole attack.

Lakshmanan et al. [87] prohibit eavesdroppers from accessing the WLAN communication using different strategies. Directional antennas and secret sharing are used on the access points (APs) in order to focus transmission on specific regions that legitimate clients reside and minimize the eavesdropper's ability to access all shares and decrypt the message. However, if the eavesdropper moves to an active attack, such as a DoS, he can prohibit a legitimate node from accessing all the shares. Another strategy proposed by the authors requires the APs to use controlled jamming in order to cause interference to eavesdroppers so that they will not be able to decode information. The challenge here is to cause no or negligible interference to legitimate clients, otherwise legitimate communication will be affected.

Sheth et al. [88] follow a similar approach as the work in [87] to address the eavesdrop attack. They propose to equip APs with directional antennas and control the transmit power so that they can confine coverage to clients within the overlapping region created by the APs'

transmission. Using secret sharing the clients can recover the transmitted packets if they receive the packet fragments sent from all APs.

Directional antennas are also utilized to protect the network from the Sybil attack, where a malicious node sends multiple messages claiming different sender identities. Tangpong et al. [89] detect the Sybil attack based on the physical location of each node. Nodes are equipped with directional antennas and know their own location. At a packet reception, a node knows the section at which the packet was received, thus it can determine the direction of the incoming packet. Each sender includes a location claim at the transmitted packet. Upon receiving a packet, the receiver authenticates and verifies the location of the sender. The sender's location claim has to reside in the correct sector of the receiver and the distance between the two nodes has to be less than a bound distance in order for the receiver to accept the packet. The nodes exchange their observations periodically in order to identify the identities owned by the malicious node.

Suen and Yasincac [90] follow a similar concept as in [89] in order to address the sinkhole attack. Specifically, the authors consider the signal direction, signal strength and nodes collaboration to identify the transmitter's location. Each node is equipped with directional antennas and knows its own location. A node can calculate the transmitter's location with the help of trusted neighbors that receive the transmitted signal. Location information can assist nodes with peer identification to detect the case where a node claims to be at different locations at the same time or where multiple nodes claim to be at the same location at the same time.

Piro et al. [91] propose each node to monitor all transmissions it receives over many time intervals in order to detect a Sybil attacker. The node keeps track of the different identities heard during the interval. Then, the node analyzes the data to find identities that appear together often and that appear apart rarely. These identities are likely utilized by a malicious

node. The authors propose to extend their scheme with directional antennas to consider the signal direction in order to facilitate the attack detection and increase the accuracy of their scheme.

2.3 Concluding remarks

This chapter presented fundamental security issues in WSNs covering: the security challenges that WSNs face; the typical security requirements that are addressed in WSNs; the threat models that need to be considered when designing security mechanisms in WSNs and the research efforts made towards prevention and intrusion detection aspects in WSNs. Moreover, the need for intrusion recovery in WSNs was analyzed and then the state-of-the-art related to intrusion recovery in WSNs was presented. Finally, special attention was directed towards directional antennas and their usage to support security objectives in WSNs. Our analysis of current research efforts has indicated that directional antennas have been briefly investigated in wireless and sensor networks, at which they are mainly utilized in a defense context.

The following table (Table 2) indicates the applicability of each intrusion recovery solution towards specific attacks and its main limitations.

Table 2: Typical intrusion recovery countermeasures applicability and limitations comparison

		Type of attack							Attack strategy		
		x indicates effectively addressed							If addressed indicated by Y, otherwise by N		
		Selective forwarding	Blackhole	DoS	Eavesdropping	Sybil	Wormhole	Sinkhole	Static	Adaptive	Main limitations
Intrusion recovery solutions	Blacklisting & Rerouting	x	x				x	x	Y	N	Cannot prohibit malicious nodes from launching active attacks and affecting nodes in their coverage range. If the malicious nodes are next to an active path then they can greatly affect the packet delivery and decision making. Eavesdropping cannot be prohibited. Interference while rerouting can cause retransmissions, packet delivery delays and more energy consumption.
	Key revocation				x	x			Y	N	Can protect the information from been disclosed but cannot hide communication occurrence. Eavesdropping cannot be prohibited. The malicious nodes can prohibit the revocation process and the updating of new cryptographic keys. Sensor nodes that have been prohibited from updating their keys maybe excluded from communication.
	Low duty cycle			x	x				Y	Y with high tradeoff	Recovers network's survivability and minimizes eavesdropping but greatly affects packet delivery and decision making.

	Channel surfing			x	x	x			Y	N	Cannot address intelligent malicious nodes that scan available channels to discover communication. In the case of intelligent malicious nodes, eavesdropping cannot be prohibited. Persistent and adaptive malicious nodes can prohibit the applicability of the mechanism and prohibit sensors from negotiating a new channel to communicate.
	Reprogramming	x	x	x	x	x	x	x	Y if malicious nodes do not interrupt the process	Y if malicious nodes do not interrupt the process	Very expensive operation in terms of communication overhead and energy consumption. Should be used as malicious nodes increase. The malicious nodes can prohibit applicability of reprogramming.
	Path redundancy	x	x				x	x	Y	N	The multipath routing strategy affects the recovery level that can be achieved. Cannot prohibit compromisation of the network's communication. Data availability can be affected. Eavesdropping cannot be prohibited.

The main deficiencies (summarized in Table 2) of existing solutions and open issues in the intrusion recovery area in WSNs were specified through the state-of-the-art review and are summarized below:

- Applying recovery does not mean that the malicious nodes have disappeared. They continue to exist in the network and can continue their compromisation attempts. In the case of persistent/adaptive malicious nodes re-compromisation can occur, even if recovery has already been applied.
- Intrusion recovery solutions mainly address a static intrusion attack strategy, focusing on a specific security attack, thus, they are vulnerable against persistent and adaptive adversaries.

- Resilience against the eavesdropping attack is low and thus initialization of new attacks on an overhearing case cannot be minimized.
- The network's availability is greatly affected when persistent and adaptive adversaries are considered. Decision-making that is depended on the WSN's observations can be affected if the network's availability is compromised.
- In the case of the low duty cycle mechanism, there is a high tradeoff for recovering from active attacks such as a DoS. The survivability of the network is recovered at the expense of the network's availability and packet delivery capability.
- Intrusion recovery solutions have been proposed in the context of omni-directional networks. The fact that the communication can be established from/to any direction with the same gain cannot effectively isolate malicious nodes in a way that the risk of compromisation can be eliminated, or at least severely minimized.

A new approach needs to be taken towards intrusion recovery in WSNs in order to address the deficiencies of existing solutions and open issues in the area. The efforts should be concentrated on recovering the network from compromisation and empowering the nodes ability to withstand persistent and adaptive malicious nodes in order to continue to communicate and support the decision-making process. Directional antennas are identified in the thesis as potentially an effective tool in the recovery of a compromised sensor network.

Chapter 3

INCURE framework

This chapter presents the concept behind the INCURE framework design [12, 92, 93, 94], specifies the intrusion recovery requirements that should be addressed by intrusion recovery countermeasures and discusses the objectives related to the formulation of new intrusion recovery solutions. Finally, this chapter analyzes the components and the operation of the proposed framework.

3.1 The concept

This thesis proposes a new intrusion recovery framework that is envisioned to support each phase of the development of a new intrusion recovery countermeasure, covering the complete sphere of requirements specification, design, implementation and evaluation. Currently, as discussed in the previous chapter, in the context of intrusion recovery, design and evaluation guidelines are limited. Before moving into the design of new intrusion recovery solutions, it is essential to have a clear view of what needs to be achieved by an intrusion recovery countermeasure. The framework specifies the intrusion recovery requirements and the recovery objectives that need to be promoted by new intrusion recovery solutions. The former indicate what operational aspects need to be recovered in case of

compromisation. The latter indicate directions as to what needs to be addressed and in what way in order for recovery to be made possible and to support effectively the intrusion recovery requirements. Based on these specifications, a new intrusion recovery countermeasure that aims to recover the WSN in case of compromisation and an intrusion recovery policy that manages recovery actions according to the incident are proposed. The framework also specifies a new evaluation method (Chapter 4) that aims to guide researchers when assessing/comparing their intrusion recovery countermeasures.

In Chapter 2, an analysis of existing intrusion recovery countermeasures and their deficiencies were presented. It was observed that an adversary that has compromised several sensor nodes and turned them malicious is a great challenge to address as he can use the malicious nodes to launch security attacks against the WSN in order to compromise and manipulate its operation. When a node has been compromised by a malicious node, there is the need to restore its operation in order to support the WSN services (i.e. network communication, event reporting, etc.) and return network operation and performance to a stable state. Existing intrusion recovery solutions apply measures in order to restore the WSN's operation under the assumption of a specific attack. However, the case of adversaries that deploy an adaptive intrusion strategy is not well addressed. In such a case, the network can be again compromised, greatly affecting the availability of the network communication and the decision-making. Moreover, the resilience of current solutions against eavesdropping is low, and, thus, an attack initialization based on an overhearing case cannot be minimized. If the compromised nodes are in the transmission range of other sensors, they can receive network communication and initialize security attacks such as a DoS and affect sensor nodes that are located in their transmission range. Also, there is a high tradeoff associated with specific solutions such as the low duty cycle (section 2.2.1.3) where the network's survivability is recovered at the expense of the network's availability and packet delivery capability. A new approach needs to be taken towards recovery in order to address the

aforementioned issues. Efforts should concentrate on isolating malicious nodes from the rest of the network in a way that the outcome of any malicious activity is minimized.

Restoration activities need to move along two design objectives: a) recover what has been compromised and b) prohibit further network compromisation. The network's security and recovery protection can be re-enforced through the isolation of malicious nodes. Isolation of malicious nodes can be achieved by prohibiting malicious nodes from a) transmitting towards sensors and b) receiving network communication. Physical isolation is proposed in the thesis in an effort to physically bypass malicious nodes and prohibit them from communicating with the sensor network. The benefit of directional antennas to transmit/receive to/from particular directions is utilized in the proposed countermeasure to promote the intrusion recovery objectives. The use of directional antennas aims to promote the creation of controlled communication paths leading to the malicious nodes' physical exclusion from the network communication. In this way rendering ineffective whatever actions the malicious nodes undertake. The following table (Table 3) presents a summary of the limitations of existing intrusion recovery solutions and indicates how the usage of directional antennas is expected to address their deficiencies.

Table 3: INCURE versus typical intrusion recovery countermeasures comparison

Recovery solutions	Main limitations of typical intrusion recovery countermeasures	INCURE potential benefits
Blacklisting & Rerouting	Cannot prohibit malicious nodes from launching active attacks and affecting nodes in their coverage range. If the malicious nodes are next to an active path then they can greatly affect the packet delivery and decision making. Eavesdropping cannot be prohibited.	Less interference while updating active route paths, less retransmissions, energy consumption and packet delivery delay. Can minimize the outcome of active attacks launched by malicious nodes on near-by nodes. Isolates malicious nodes making

	Interference while rerouting can cause retransmissions, packet delivery delays and higher energy consumption.	attacks ineffective.
Key revocation	Can protect the information from been disclosed but cannot hide communication occurrence. Eavesdropping cannot be prohibited. The malicious nodes can prohibit the revocation process and the updating of new cryptographic keys. Sensor nodes that have been prohibited from updating their keys maybe excluded from communication.	Can hide communication's occurrence and minimize eavesdropping. Can support the updating of cryptographic keys during active attacks.
Low duty cycle	Recovers network's survivability and minimizes eavesdropping but greatly affects packet delivery and decision making.	Can recover the network's survivability and the packet delivery.
Channel surfing	Cannot address intelligent malicious nodes that scan available channels to discover communication. In the case of intelligent malicious nodes, eavesdropping cannot be prohibited. Persistent and adaptive malicious nodes can prohibit the applicability of the mechanism and prohibit sensors from negotiating a new channel to communicate.	Can address adaptive malicious nodes and achieve higher resilience against the eavesdropping attack.
Reprogramming	Very expensive operation in terms of communication overhead and energy consumption. Should be used as malicious nodes increase. The	Can support reprogramming tasks by promoting nodes' availability and communication.

	malicious nodes can prohibit applicability of reprogramming.	
Path redundancy	The multipath routing strategy affects the recovery level that can be achieved. Cannot prohibit compromisation of the network's communication. Data availability can be affected. Eavesdropping cannot be prohibited.	Can promote data availability while retaining network communication during active attacks.

An adversary's intrusion strategy can include more than one attack (section 2.1.4.1), challenging the design of security mechanisms. Due to the attack dynamics, recovery cannot be static and has to cope with the attacks dynamically as they are executed. This adaptability of recovery needs to be coordinated and managed based on the situation in order to achieve an enhanced recovery level and balance recovery, compromisation and overheads. A security policy [95, 96, 97, 98, 99] can coordinate different security actions based on different conditions, and therefore the design of an appropriate intrusion recovery security policy is mandatory.

The design of a security solution is followed by the evaluation phase [100, 101] that aims to assess its performance. An evaluation method (Chapter 4) is proposed with the objective of aiding researchers into assessing the performance of their intrusion recovery countermeasure. Based on the results, researchers can update their designs accordingly.

3.2 Methodology

This section briefly describes the adopted methodology of work for the proposed intrusion recovery framework. The methodology consists of three phases (identify, design, evaluate) as shown in Figure 3.

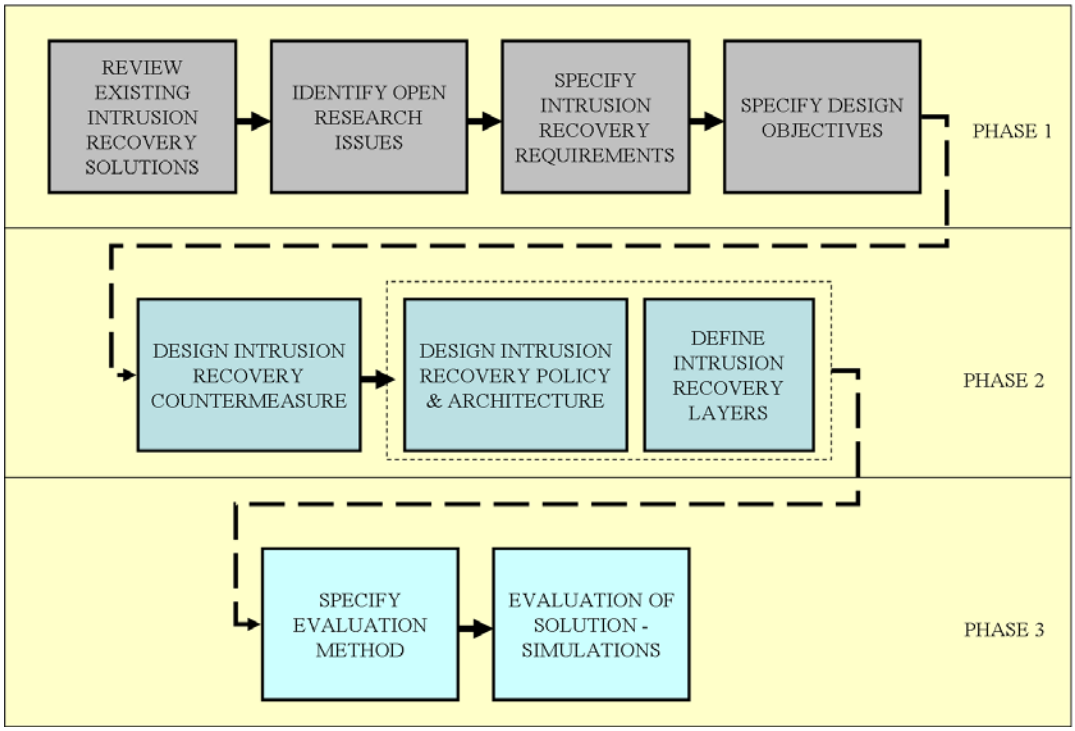

Figure 3: Design methodology

In phase 1, we reviewed existing intrusion recovery design approaches [12, 92] (section 2.2) and identified the open research issues in the area (section 2.3). Then, we defined our intrusion recovery requirements (section 3.4) and design objectives (section 3.5) that need to be taken into consideration when designing intrusion recovery countermeasures. The design of the proposed framework and its components are based on the specifications made in phase 1.

In phase 2, the proposed countermeasure and associate security policy are designed (section 3.7). An appropriate policy architecture (section 3.8) is designed to support and manage the operation of the proposed components. Moreover, three intrusion recovery layers (section 3.8.2.1) are proposed specifying different intrusion recovery requirements that need to be supported by a WSN. Our aim is the proposed layers to serve as a guide to the users to identify the intrusion requirements of their WSN application. The target is the recovery policy to be deployed by the WSN according to the users' needs.

In phase 3, we defined the evaluation method (Chapter 4) that drives the assessment of the proposed countermeasure (Chapter 5). The method specifies the security evaluation elements and related evaluation metrics that should be considered to assess the performance of intrusion recovery countermeasures in WSNs.

3.3 Overview of INCURE's main components

The proposed intrusion recovery framework consists of three main components: the specification of intrusion recovery requirements and objectives (sections 3.4 and 3.5), a new intrusion recovery countermeasure (section 3.7) and a respective security policy (section 3.8), and an evaluation method (presented in Chapter 4). A policy architecture (presented in section 3.8) manages the enforcement of the security policy and the operation of the proposed countermeasure.

Prior to the design of a new intrusion recovery countermeasure, the *intrusion recovery requirements and objectives* are defined to drive the design and evaluation efforts. This is considered an essential step in the development of new solutions in order to take into consideration the aspects that need to be recovered by the new restoration mechanisms and also directions as to how recovery under different attack conditions can be achieved.

The core idea of the proposed *intrusion recovery countermeasure* is to provide controlled routing and prohibit/enable communication with nodes in order to suppress security attacks by using antennas that have less antenna gain in the direction of the adversary. Controlled routing is achieved by controlling the activation/de-activation of the antenna beams on each node based on security conditions, and therefore dynamically changing the physical connections established between sensor nodes and malicious nodes. By enabling and using antennas that have deep nulls or less antenna gain in the direction of the adversary, the proposed intrusion

recovery countermeasure prohibits or minimizes the possibility that malicious nodes compromise legitimate nodes and thus successfully launch security attacks.

The proposed *intrusion recovery policy* component aims to achieve recovery adaptability and support different intrusion recovery requirements. Three intrusion recovery layers are proposed specifying different intrusion recovery requirements. The layers can be used by users as a guide to identify the intrusion recovery requirements that should be supported by their WSN and utilize the recovery policy accordingly. The recovery policy coordinates recovery actions, taking into consideration different intrusion recovery requirements and attack conditions. The aim is to achieve a dynamic intrusion recovery strategy that enables nodes to address persistent/adaptive adversaries by adapting their recovery.

Figure 4 presents INCURE's main components and their interactions. Prior to deployment, the intrusion recovery requirements of the WSN are specified and they drive the configuration of the intrusion recovery security policy. The intrusion recovery policy coordinates the applicability of the proposed countermeasure in order to address attacks. After the initial configurations are established and set on the sensor nodes, the network can be deployed. The network starts by establishing routing paths and forwarding packets from sources to destination. Under normal operation, no intrusion recovery actions are taken. In the event of an attack, the proposed framework cooperates with an appropriate intrusion detection system (the IDS exact operation is out of the scope of this research work) that will detect and report the security incident to sensor nodes. As soon as an intrusion is detected, the intrusion recovery module that resides on the sensor nodes is triggered. The intrusion recovery module is responsible for deploying the intrusion recovery policy, including: (i) coordinating and applying the intrusion recovery according to the reported security incident and (ii) managing the activation/deactivation of the antenna beams on each sensor node in order to control the routing operation and the communication between nodes. In the case where an attack

continues, the nodes carry on with their intrusion recovery strategy in order to re-address the attack.

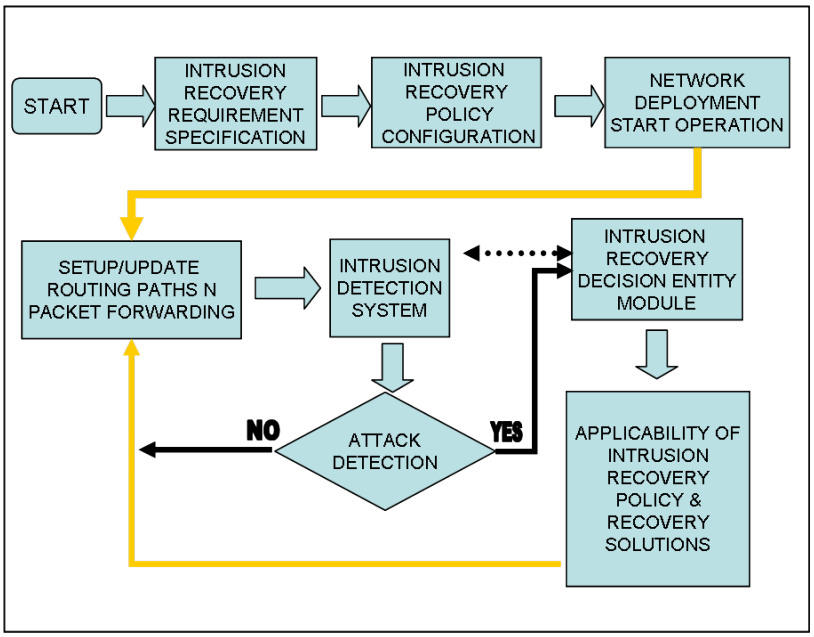

Figure 4: INCURE high level framework components and interactions

The following sections present in greater detail the main components of the INCURE framework.

3.4 Intrusion recovery requirements

In order for intrusion recovery countermeasures to be effective, it is essential to clearly identify what they are trying to protect and what needs to be achieved with a restoration mechanism. The intrusion recovery requirements will be defined in terms of appropriate security requirements that will also drive the assessment of intrusion recovery effectiveness to restore the network's normal operation. The intrusion recovery security requirements specification should not be considered a trivial process. Usually, in security studies a typical list of security requirements is considered [6, 7, 8, 17] and analyzed when designing secure protocols. This typical list includes integrity, confidentiality, authentication and availability.

However, the intrusion recovery needs to focus on a different set of security requirements. Currently, this is not adequately addressed in the context of restoration activities in WSNs. Studying the appropriate intrusion recovery requirements will permit researches to gain a better understanding of the intrusion recovery aspects they should focus on. Furthermore, the intrusion recovery requirements will drive the specification of the elements that need to be well protected. Table 5 (in Chapter 4) depicts the WSN services that are expected to be recovered when an intrusion recovery solution supports a specific intrusion recovery requirement. The requirements considered in this thesis are listed below:

Requirement 1 (R.1): Availability

The most important security requirement to be addressed by intrusion recovery countermeasures is *availability*. Availability [1, 8, 12] ensures that the services and information can be accessed at the time required. In order to ensure availability, fundamental services in a WSN in the form of sensing, communicating and reporting, must remain operational. The communication capability of sensor nodes is a prerequisite in order to support security requirements such as confidentiality, authentication and integrity. For example, if a sensor is prohibited from communicating with its neighbors to report an event, authentication cannot be established, thus it is turned ineffective and prohibited from contributing to the communication protection. Therefore, the ability to communicate is a critical WSN service that needs to be recovered in case of compromisation. Communication and reporting can become unavailable due to a number of reasons [7, 14, 15, 17, 102]: during attacks nodes cannot access the wireless channel for long time periods; attacks force nodes to stay in receive mode and thus cannot transmit packets; packet collisions occur at the receiver; packet drops happen due to buffer overflowing; nodes are desynchronized with security mechanisms; and energy depletion occurs. Also, it must be noted that availability of communication also affects the level of restoration that can be achieved. If a node is prohibited from communicating with the rest of the network's nodes, any intrusion recovery

countermeasure that involves nodes' transmission capabilities can be turned ineffective. Thus, intrusion recovery countermeasures main focus should be on addressing the aforementioned attack outcomes and restoring the availability of nodes in an efficient and effective manner. The availability requirement is interrelated with a number of other security requirements: survivability, resilience, self-healingness, reliability and responsiveness. These are discussed next.

Requirement 2 (R.2): Survivability

Survivability [12, 19] refers to the ability of nodes to remain alive after a security attack has been launched and to continue functioning, supporting the fundamental WSN services. The survivability of nodes is enhanced by their capability to balance energy consumption during an attack. Usually, sensor nodes use batteries [5] as their main source of energy. Security attacks often target to deplete the nodes' batteries in an attempt to turn them unavailable. Intrusion recovery countermeasures should aid the nodes to preserve their energy resources during an attack. This can be achieved by isolating the malicious nodes in such a way as to minimize the attack outcome related to energy depletion. Moreover, attack avoidance is a critical element of the intrusion recovery functionality to protect energy consumption and maximize the network's lifetime. Intrusion recovery mechanisms can help the network to save energy during an attack. Furthermore, they can also act the other way around with regard to malicious nodes, forcing them to deploy new attacks to compromise the network and therefore consume their own resources.

Requirement 3 (R.3): Reliability

Reliability [12] should be also considered to ensure that the network can perform and maintain its packet delivery operation. A number of threats exist that can compromise the operation of a WSN as discussed in section 2.1.2. If the packet delivery capability of the

network is affected, critical events may not be reported and therefore decision making cannot be supported successfully. Intrusion recovery should promote a reliable network operation [12], meaning that packet delivery capability should be successfully restored after a compromisation in order to allow data to be delivered to the destination. This will support a reliable decision-making as reported events will indicate if an action needs to be taken to support the operational objectives.

Requirement 4 (R.4): Resilience

Resilience is another important intrusion recovery security requirement [1, 12]. Once intrusion recovery countermeasures are applied and network's availability and operation are restored, it is essential to be able to resist new attacks that aim to interrupt the recovered WSN's services. The recovered network can resist more effectively to attacks if the source of threat is isolated so it is prohibited from continuing to attack the network or at least the attack outcome is minimized. In the case where compromisation occurs again, appropriate intrusion recovery countermeasures should be applied again, in order to re-establish service restoration.

Requirement 5 (R.5): Responsiveness

Attacks can increase the packet delivery delay affecting the timely decision making and response to critical events. During the observation of critical events, the main responsibility of a WSN is to propagate the observations to the control center in a timely manner. It is essential for intrusion recovery countermeasures to consider responsiveness [17] requirement and aid the network to converge to a stable and normal state. It is important to ensure that the network can perform its tasks well when recovery is applied to address security attacks and that the malicious nodes are prohibited from affecting the network's responsiveness when they persist/adapt their intrusion strategy. This can be achieved if intrusion recovery countermeasures can effectively minimize attack outcome (i.e. packet loss, retransmissions,

transmission delays, etc.) or prohibit successful execution of attacks. The rationale behind the need for effective restoration is that it can minimize attack duration time. In this way, the network's packet delivery capability can be restored and packet delivery delays due to attack occurrence can be minimized. Therefore, decision making can be restored as quickly as possible.

Requirement 6 (R.6): Self-healingness

The resilience and availability of the network can be further improved through an adaptive recovery process that can be achieved through a *self-healing* [12] intrusion recovery approach. Resilience and self-healingness can be most effective if the potential threats and the operational aspects which have to be protected and recovered in case of compromisation are identified. Thus a multi-level intrusion recovery approach is proposed to offer different levels of recovery based on the security incident. In this way, an appropriate level of robustness can be achieved.

3.5 Objectives of intrusion recovery countermeasures

Intrusion recovery is an essential feature of a security strategy [9, 10, 11]. In the context of WSNs, intrusion recovery investigations are limited and they need to be extended in order to promote robust restoration services under different attack conditions. Since intrusion recovery in WSNs is an open area, there is an increased demand for new intrusion recovery countermeasures, especially for critical infrastructures. This section identifies five objectives (1-5) related to the formulation of new intrusion recovery countermeasures. These objectives drive the INCURE framework specification.

Objective 1: Address persistent adversaries

As sensor networks are evolving and find applicability in many applications [1, 2, 3, 4, 5] supporting many social and business aspects and performing simple to critical tasks, so do adversaries in terms of compromisation knowledge and tools [20]. Adversaries with dedicated objectives to compromise a network do not get discouraged from potential security measures adopted by the sensor network to tackle the attacks. The situation gets worse in the case where the adversaries have compromised sensor nodes, turned them malicious and have gained network access. By compromising sensors, the adversary can launch security attacks easier and affect the network operation. Persistent adversaries may deploy different security attacks with the objective of compromising the WSN operation, even after the network has recovered its services that have been previously affected by malicious activity. By considering persistent adversaries, robust recovery solutions can be designed from the beginning, in order to establish an effective restoration service.

Moreover, in order to cope with persistent adversaries, intrusion recovery should not be static. Recovery can be influenced by many factors, such as the number and location of malicious nodes, the attack type, etc. As adversaries adapt their intrusion strategy in order to compromise the WSN, the intrusion recovery countermeasure should follow the same approach. Proposed countermeasures should be flexible and should be able to adapt their actions according to the applied intrusion strategy. The objective is to enhance security and force adversaries to substantially increase their attack efforts to compromise the WSN and therefore consume their resources. In order to support the aforementioned objective, intrusion recovery countermeasures should consider different criteria in order to adapt their actions accordingly. Such criteria that can drive the recovery strategy include the intrusion recovery requirements and the type of implemented attacks. Intrusion recovery countermeasures should be designed with the characteristic of recovery escalation. If an attack cannot be fully suppressed, we aim to offer delayed degradation of restoration and performance.

Objective 2: Address elevated security policy and coordination support

It is not necessary, nor recommended, to apply strong and potentially resource consuming intrusion recovery countermeasures if there are simpler and lighter recovery mechanisms that can cope with a security problem. This property is derived from the observation that different recovery strategies may incur different trade-offs in terms of recovery, compromisation, resource overhead and performance. The recovery strategy should apply the appropriate actions based on the situation and balance the aforementioned trade-off.

The recovery adaptability has to be coordinated in order for the most relevant actions to be applied to the current situation, elevated in accordance with the severity and need for stronger actions. This can be achieved through an appropriate security policy that will consider the current situation and apply the intrusion recovery countermeasure. Currently, most of the proposed security policies in WSNs focus on the selection of appropriate prevention mechanisms [96, 97, 98, 99] to provide a certain security level (low, medium, high). Intrusion recovery solutions should support an intrusion recovery oriented security policy that will provide sensor nodes with the intelligence of recovery so that they will dynamically react under different attack conditions in order to restore compromised services.

Objective 3: Address restoration, attack confinement and recovery resilience

Although the WSN can apply a recovery countermeasure, i.e. [14, 22, 30, 31, 42, 43, 45, 46, 55, 59, 71], and restore its operation, it does not mean that the threat is eliminated or the attack source is prevented from launching more advanced attacks. In order to re-enforce recovery and network security, proposed solutions should be designed with the objectives of restoring compromised operation, confining the attack source in a way that it will be prohibited from communicating with sensor nodes thus promoting recovery resilience.

Objective 4: Address attack initialization

Often, a malicious node acts conservatively to save energy resources and thus first identifies the presence of legitimate nodes before launching an attack [15, 102]. Therefore, recovery should reduce a node's exposure to malicious nodes to minimize attack initialization and confine the attack source in order to eliminate or minimize compromisation outcome. New intrusion recovery countermeasures should be designed with the objective of minimizing attack initialization and hardening the malicious efforts to compromise the network.

Objective 5: Address recovery of WSN network communication service

One of the fundamental services of sensor nodes is network communication [5, 8]. Network communication supports nodes' cooperation and promotes reporting to the decision-making center. If the nodes' communication ability is affected, decision-making can be compromised. Moreover, security and intrusion recovery mechanisms usually require network communication to support their operations and fulfill their objectives. Intrusion recovery countermeasures should focus on recovering the WSN's communication services in case of compromisation. To achieve this objective, physical security should be investigated as a potential component of the countermeasures' recovery strategy design.

3.6 Assumptions and operational state of INCURE

This section describes the network, threat and security models that are considered by INCURE.

3.6.1 Network model

An IEEE 802.15.4 [103] sensor network is considered. Sensor nodes monitor their surrounding environment and report to the sink if they have detected the occurrence of a specified event. The sensor nodes are static and have the same capabilities in terms of transmission range, battery and processing power. The sink is considered robust with enhanced resources in terms of memory, computational power and energy. The WSN application requires a continuous and reliable operation in order to support the decision-making and allow for quick reaction to observed events. The operation of the network is considered critical and therefore justifies intrusion recovery countermeasures, to varying degrees.

3.6.2 Threat model

This research work considers adversaries that have access to a number of compromised sensor nodes, have turned them malicious and have gained access to the network. Malicious nodes retain the same capabilities as legitimate nodes in terms of energy, storage and processing power. Since security attacks may arise at any given time, in any network location, with static or adaptable attack dynamics, they pose a threat to the WSN operation. This category of adversaries has dedicated objectives aiming to compromise the network's operation. They aim to disrupt the operation during malicious activity in order to prohibit observation and identification of critical events that will allow decision making. To achieve their malicious objectives they target to compromise the nodes' operation and affect the availability, survivability, reliability and resilience of the sensor network. They try to do so by persisting and adapting their intrusion strategy, aiming to compromise sensor node communication and turn WSN services unavailable. Malicious nodes retain their original position and are reprogrammed to launch different attacks (e.g. selective forwarding,

eavesdropping and DoS) in an attempt to prohibit nodes from communicating with the sink. The malicious nodes aim to force nodes to drop packets destined for the sink, prohibit access to the wireless medium for an extended period of time, force nodes to remain in the receive state through a constant stream of malicious incoming packets and thus consume their energy.

3.6.3 Security model

Recovery mechanisms should not be static in order to be effective against a dynamic attack strategy, thus they should demonstrate an equivalent dynamic behavior. The proposed intrusion recovery framework aims to demonstrate an adaptable behavior. The existence of an Intrusion Detection System (IDS) is assumed, e.g. [29, 30, 31, 32, 33, 34, 35, 36, 37], that detects malicious behavior and interacts with the intrusion recovery module to inform the sensor nodes of the malicious activity. This assumption is essential in order to make it possible to investigate the feasibility of the proposed intrusion recovery concept and assess the effectiveness of the proposed intrusion recovery countermeasure to restore the network's operation after an attack is detected. It is obvious that if the IDS fails to detect and inform nodes about the malicious activity, then no recovery actions will be taken, since legitimate nodes will not perceive any change to the network status. The objective of this research work is to contribute towards intrusion recovery aspects. In the case of passive attacks such as the selective forwarding attack, sensor nodes cooperate, i.e. [27, 28, 29, 30, 31], to inform the network of the misbehavior. In this case, intrusion recovery is applied by all the nodes that are informed about the event. In the case of the DoS attack, intrusion recovery is performed locally, i.e. [29, 30, 31, 32], by each sensor.

3.7 Intrusion recovery countermeasure

This section presents the proposed intrusion recovery countermeasure in terms of the deployed antenna model, the routing and the intrusion recovery operations.

3.7.1 Antenna model

Each sensor node is equipped with multiple directional antennas that cover the 360° region around the node (Figure 5). Antennas are numbered from 1 to N in an anti-clockwise fashion and use the same antenna pattern. A switching module allows nodes to control the switching of every antenna element, thus achieving on purpose controlled routing. More than one antenna can be active during transmission. This means that if all antennas on the node are switched on, it can transmit in an omni-directional fashion. During reception, only one of the antenna beams is selected which has the best signal-to-interference-ratio (SIR) over the others. During a single beam antenna switch, there is a switching time delay in the order of nanoseconds; a typical value of 250 nanoseconds is considered [104]. Typical power consumption is considered to be in the order of 30 μW [105] per switching.

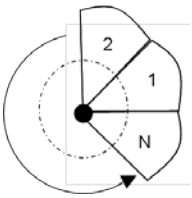

Figure 5: N-beam antenna model

3.7.2 Routing operation

The utilization of multiple directional antennas on each node in order to establish controlled routing requires appropriate management in terms of neighbor discovery, antenna

beam caching, antenna beam selection for transmission/reception and packet forwarding (Figure 6 outlines the routing and intrusion recovery operations). This section describes each of the aforementioned aspects.

3.7.2.1 Neighbor discovery and antenna beam caching

In order to support the operation of the proposed intrusion recovery countermeasure it is necessary for each node to identify which antenna beam communicates with each of its neighbors. This information is required so that a node can control an antenna's activation/de-activation operation and revoke the communication with specific nodes (such as malicious nodes). An antenna is characterized as *active* if it is considered for transmission/reception operations, thus it is utilized in the routing operation. An antenna that gets blacklisted and is not utilized for transmission/reception, thus does not participate in routing in order to address a security incident, is characterized as *deactivated*. A hibernation timer specifies the activation time of an antenna that got deactivated in order to turn an attack ineffective. As soon as the hibernation timer is over, the deactivated antenna can be utilized for transmission/reception and participate in routing, thus its status is reset to active. The purpose of the hibernation time is to aid nodes to avoid an attack during its execution and thus prohibit malicious nodes from affecting the network's operation and performance. An appropriate antenna cache is maintained on each sensor node having a record for each of the deployed antenna elements. Each antenna element is characterized by an antenna ID number, a field indicating the antenna's current status and a hibernation timer:

<antenna_id><antenna_status> <hibernation timer>

At the beginning of the network's deployment, nodes exchange HELLO packets in order to announce their presence and initialize their neighbors' table. At the reception of a signal, each

receiving node enters a fast antenna switching mode, selects the antenna that has the best SIR and receives the packet. New neighbors can also be discovered through the packet forwarding procedure. An appropriate neighbors-antennas cache is specified to record the neighbors and respective communicating antennas beam. The cache records the following fields:

<neighbor_node_id> <antenna_beam_id>

3.7.2.2 Packet forwarding procedure

INCURE establishes on demand routing, for example like in [106, 107, 108, 109, 110, 121], in order to support the network's packet forwarding operation. In the case where a sensor identifies an event of interest and needs to inform the sink node, it initiates a route discovery by broadcasting RREQ packets, in order to establish a route path towards the sink and forward observations. When a RREQ packet arrives at the sink, the sink unicasts a RREP packet traversing the (reverse) path from which the RREQ packet was forwarded towards the sink. As soon as the source node receives the RREP, it forwards data packets towards the sink node over the established route. When not transmitting or receiving packets, a node has all of its active antennas enabled. When a node receives a packet, it initiates a fast switching mode and selects the antenna that has the best SIR in order to receive the packet. Then, it records the sender's ID and the receiving antenna ID element in the neighbors-antennas cache. If an ACK is required, the node transmits the ACK packet. When a node finishes receiving a packet, it enables all active antenna beams. In the case of broadcasted packets the node enables all active antennas and transmits the packet. If a node has data packets to transmit to the sink, it first consults its routing table to find the next hop towards the destination. Then, the node reviews its neighbors-antennas cache to find the appropriate antenna element to switch to, and transmits the packet.

3.7.3 Intrusion recovery operation

The operation of the intrusion recovery countermeasure is managed by an appropriate intrusion recovery module deployed on sensor nodes. Intrusion recovery should utilize an adaptable approach in order to address persistent/adaptive adversaries and successfully restore WSN's compromised operation. In order to support such a dynamic behavior there is the need to coordinate recovery actions to respond to different malicious activities. The coordination of intrusion recovery actions can be established by defining and enforcing an appropriate intrusion recovery security policy. The proposed policy (section 3.8) will enforce specific intrusion recovery rules and provide a structured approach to guide sensor nodes as to the recovery strategy they should adopt. The intrusion recovery module residing on each node is responsible to coordinate and deploy the intrusion recovery policy and manage the operation of the intrusion recovery countermeasure. When an attack is detected (Figure 6), the intrusion recovery module residing on each node is responsible to apply recovery according to the specified intrusion recovery policy. The target of this entity is to react against an adaptable attack strategy and recover the compromised WSN.

In order to support the intrusion recovery actions, an appropriate blacklisting cache must be defined on each node so that malicious nodes can be blacklisted. Each record in the cache includes the following fields:

<malicious_id> <receiving_antenna_id> <attack_type>

When a malicious node is detected, the node blacklists it by recording the malicious node id, the respective antenna id that communicates with the malicious node and the attack type in the blacklist cache. INCURE utilizes this information to manage which of the antennas participate in routing in order to address a security attack. A blacklisted antenna is deactivated as specified by the intrusion recovery policy in order to prohibit any kind of communication

to/from the malicious node. Once an antenna beam is enabled, the node assesses the network status and continues its operation accordingly. In the case where an attack is still executed, the node continues utilizing the specified intrusion recovery countermeasure according to the proposed intrusion recovery policy. The respective security policy (section 3.8.2.3) controls the INCURE's operation, under different attack conditions and takes into consideration specific intrusion recovery requirements.

As previously mentioned (section 3.6.3), the thesis focus is on intrusion recovery aspects and the objective of the investigations is to assess if a recovery solution can effectively restore compromised operations, after an attack is detected. Therefore, an ideal IDS is considered that detects when a security attack is executed and interacts with the intrusion recovery module that resides on sensor nodes in order to trigger the appropriate recovery action. This ideal approach is essential to be taken in order to focus on assessing the effectiveness of a solution to recover compromised operations. In a real setup, the operation of the IDS can affect the applicability of the recovery actions if: (a) a security attack is not detected. In this case, it is obvious that recovery measures will not be taken, and (b) an alarm is raised by the IDS when no attack has taken place (false positive). In such a case, nodes will unnecessarily apply recovery actions, deactivate antennas and break connectivity with some of their neighbours. To handle such a case, nodes should collaborate with their neighbours to increase their confidence in deciding if an attack is indeed executed and then apply recovery. Furthermore, if the WSN deployment considers an IDS that is known to have a high false positive rate, then we should consider adjusting the deactivation strategy and using shorter deactivation periods to regain nodes' connectivity. These are aspects that will be investigated as part of the future work.

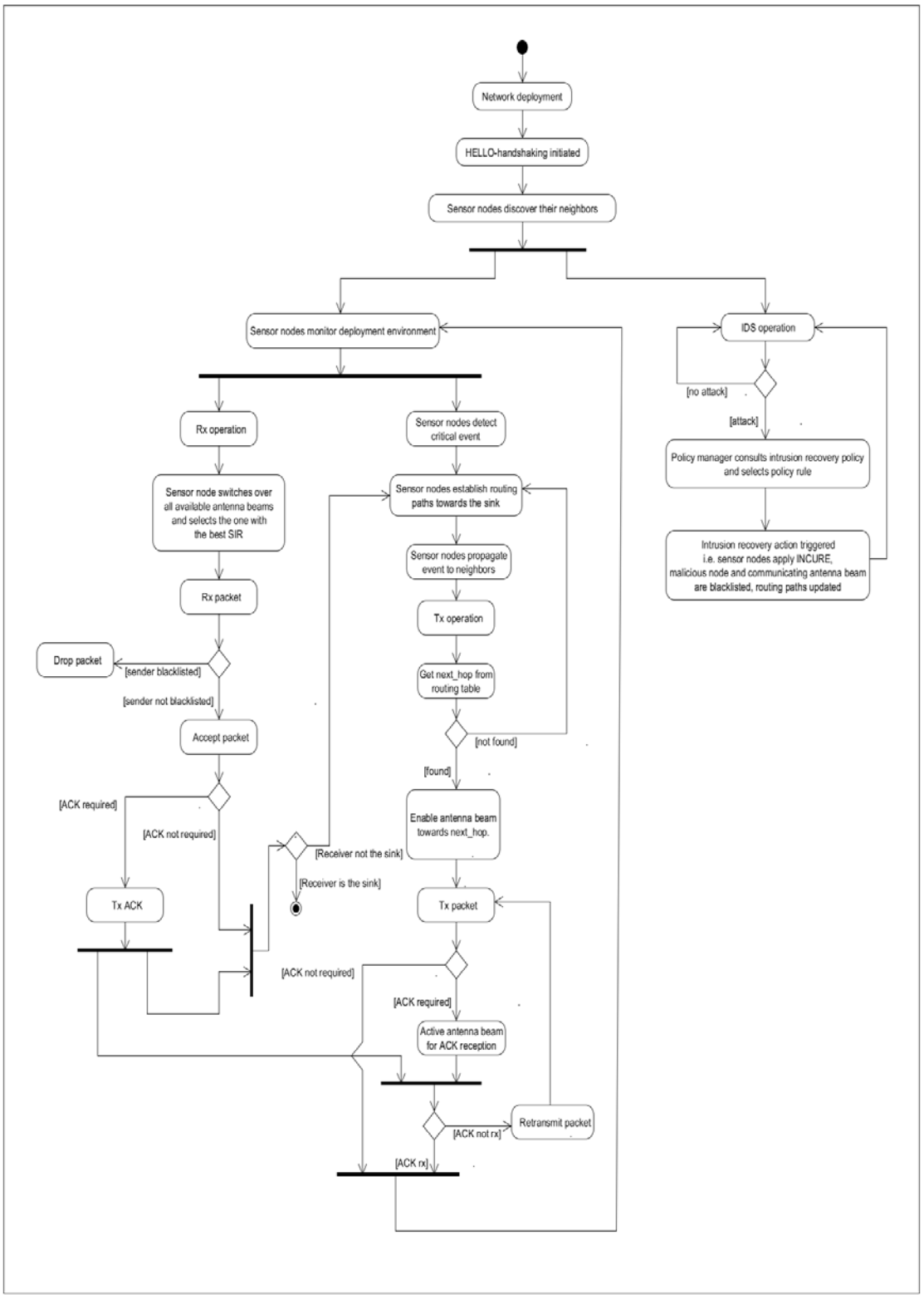

Figure 6: INCURE activity diagram

3.8 Intrusion recovery policy

This section presents the proposed intrusion recovery policy, its components and the framework under which the policy is specified and adopted. The design of the policy framework follows the main policy design principles utilized in WSNs, e.g. [95, 96, 97, 98, 99], regarding the specification of policy layers and components. Typically, three policy layers are utilized covering low, moderate and high importance security objectives. Each layer proposes security actions that need to be taken based on the context (i.e. prevention, trust-management, etc.) that the policy is proposed. Furthermore, the policy operation is usually supported by an appropriate policy architecture that considers a configuration and a decision/enforcement entity to respectively configure and deploy the policy. The configuration entity is usually utilized by end users and its responsibility is to gather the users' requirements in order for the policy to be appropriately configured. The sensor nodes usually host the decision/enforcement entity that, based on specific situations, decides which of the supported security actions that are included in the policy, should be deployed. The thesis utilizes the same design principles to specify the policy architecture (section 3.8.1) and the intrusion recovery layers (section 3.8.2.1). It is worth mentioning that this is the first intrusion recovery policy designed for the needs of WSNs and of critical infrastructures.

3.8.1 High-level policy architecture

Figure 7 presents INCURE's policy high level architecture. The architecture consists of two policy-related entities; the policy configuration entity and the policy manager. The former entity operates on the user level while the latter entity operates on the sensor level. Figure 8 presents more details related to the policy activities that are implemented at a user and at a sensor level.

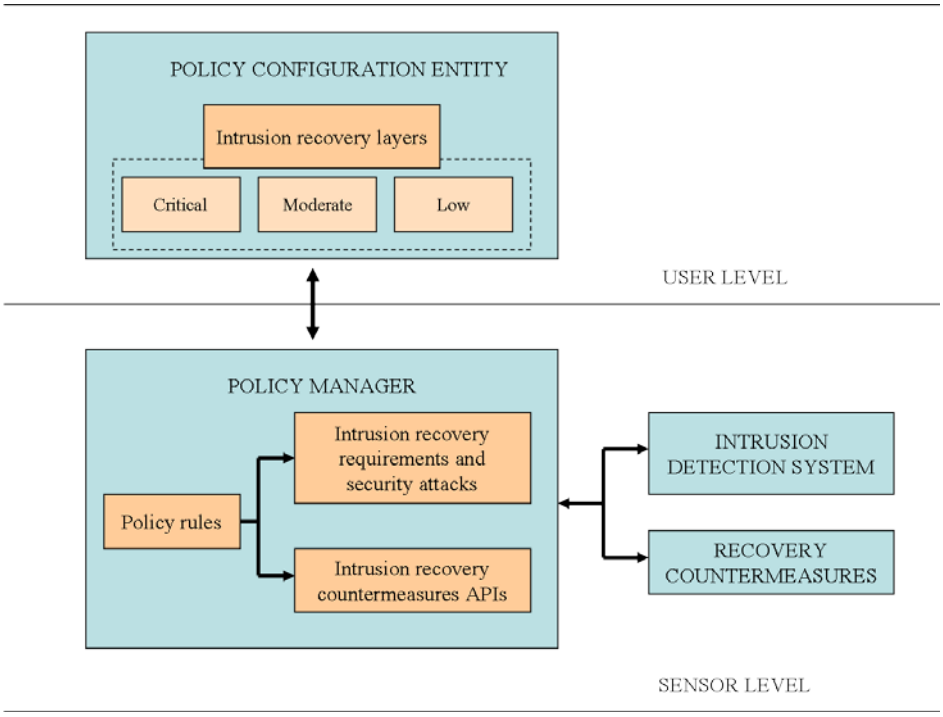

Figure 7: INCURE high level policy architecture

3.8.1.1 Policy configuration entity

The policy configuration entity is used by users, prior to the WSN's deployment, to select the intrusion recovery requirements and configure the policy on sensor nodes. Users select the intrusion recovery layer (section 3.8.2.1) that reflects the intrusion recovery requirements of their WSN. Then, the policy configuration entity interacts with the policy manager to configure the intrusion recovery policy deployed on sensors. When the sensor nodes configuration phase is finished, the WSN can be deployed at the area of interest.

3.8.1.2 Policy manager entity

The policy manager is deployed on sensor nodes to configure, coordinate, manage and enforce the recovery policy in the event of a detected security attack. The policy manager interacts with the following entities to fulfill its objectives: the policy configuration entity, the intrusion detection system (IDS) and the actual intrusion recovery countermeasures. When the

user selects an intrusion recovery layer and configures related parameters if any, the policy configuration entity interacts with the policy manager in order to configure the appropriate settings on the node. The policy manager holds the intelligence of the policy details and it is responsible for the policy's enforcement. In the event of an attack detection, the IDS interacts with the policy manager to inform about the incident in order to coordinate the recovery actions enforced by the node. Then, the policy manager selects the intrusion recovery actions according to the configurations and triggers recovery.

The policy manager entity deploys appropriate intrusion recovery policy rules in order to support different intrusion recovery requirements that indicate what needs to be recovered in case of compromisation. Moreover, the policy takes into consideration different attacks that should be addressed with the objective of supporting an adaptive recovery approach. The policy rules associate the attacks and intrusion recovery requirements with specific recovery actions to achieve restoration of compromised operations. A policy rule is triggered based on the reported security incident and then applies the respective intrusion recovery mechanism. The policy manager controls the applicability of INCURE countermeasure which is then appropriately enforced by sensor nodes in order to aid the network to address an attack compromisation. In the case where the policy needs to update its current settings or consider a new intrusion recovery countermeasure, the policy manager functionality needs to be updated accordingly.

3.8.2 Policy – related tasks

This section presents the tasks that need to be performed to support the INCURE policy architecture.

The objective of the policy architecture is to support different intrusion recovery requirements, aid the user select the appropriate intrusion recovery layer that is relevant to the deployed WSN and define the intrusion recovery policy that will be deployed by sensor nodes. The proposed intrusion recovery policy aims to address persistent and adaptive adversaries through an adaptive recovery approach. Adaptability is achieved by utilizing intrusion recovery according to the intrusion recovery requirements and the reported security incident.

In order to realize the functionality and support the operation of the policy module, different activities have to be implemented. The activities involve two main types of stakeholders, namely developers and end users, and are as follows:

1. Intrusion recovery layers definition and deployment (developer side)
2. Intrusion recovery security policy definition and deployment (developer side)
3. Intrusion recovery layer selection (user side)
4. Intrusion recovery policy configuration on sensor nodes based on user's selection (developer side)
5. Policy enforcement (developer side)

Figure 8 displays the main activities related to the operation of the proposed intrusion recovery policy module.

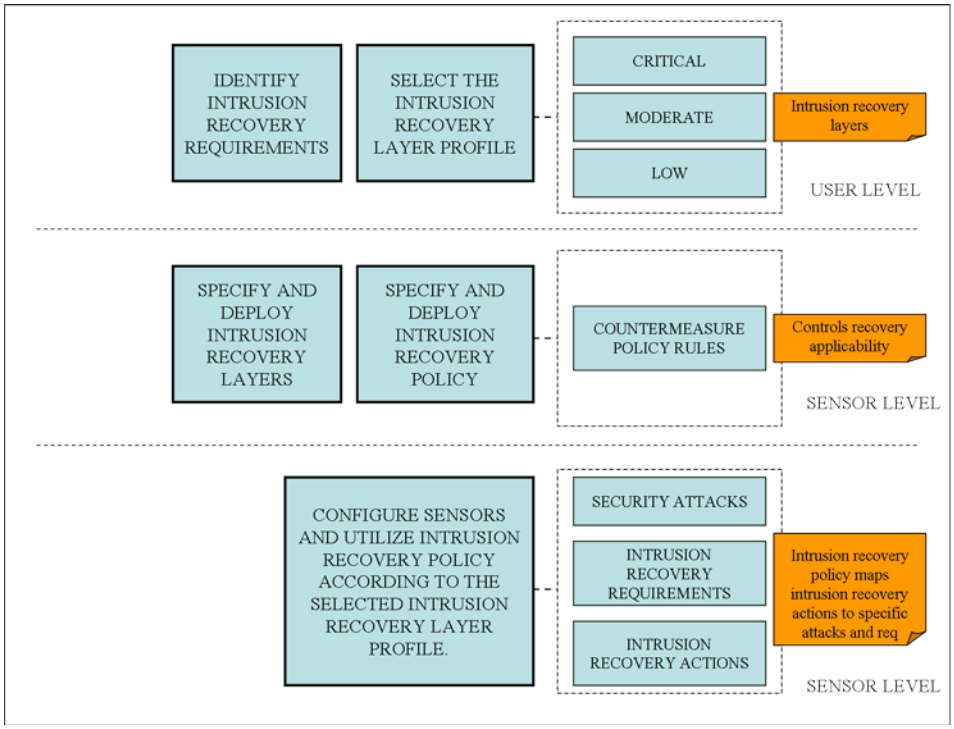

Figure 8: Policy-related activities

As depicted in Figure 8, the intrusion recovery layers/intrusion recovery requirements (section 3.8.2.1) and the respective intrusion recovery policy (section 3.8.2.3) are specified and deployed on sensor nodes. The intrusion recovery policy specifies the rules for recovery utilization, in order to support different intrusion recovery requirements under different attack conditions, and thus fulfill the objectives of the intrusion recovery layer as selected by the user. Prior to the WSN's deployment, the user has to identify the intrusion recovery requirements that should be supported by the WSN and select the layer (section 3.8.2.2) that reflects his requirements. The selected intrusion recovery layer will then be used to configure the appropriate settings on the sensor nodes in order to utilize the intrusion recovery countermeasures and address compromisation. Figure 9 illustrates the activities sequence and the stakeholders' responsibility/functionality.

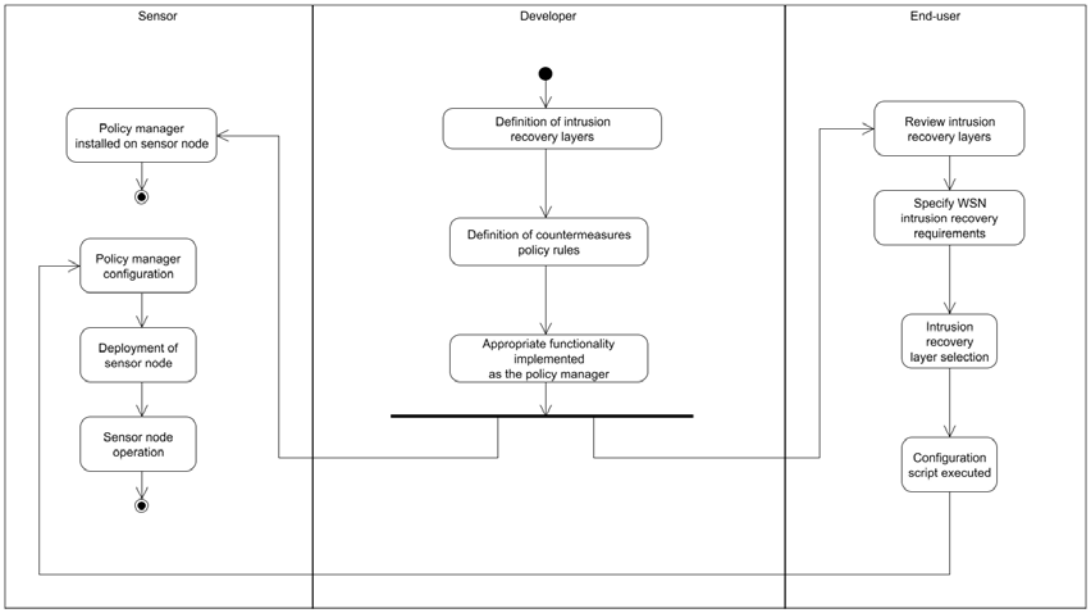

Figure 9: Policy-related stakeholders

The following sections provide more details regarding each of the aforementioned activities.

3.8.2.1 Intrusion recovery layers specification

As discussed in section 3.4, it is essential to identify the intrusion recovery requirements that should be supported by a WSN in order for appropriate restoration mechanisms to be deployed/designed and promote the specified requirements. Thus, it is imperative to acknowledge what operational aspects of the WSN are important and require to be recovered in case of compromisation, in order to offer effective and successful restoration services. By not identifying what is important for the WSN operation, recovery efforts may not succeed in restoring the appropriate compromised services. Moreover, it needs to be taken into consideration that different WSNs may need to support different intrusion recovery requirements based on their operational objectives and the attack conditions. Thus, adaptability of intrusion recovery should be pursued to address the different intrusion recovery needs and promote restoration to varying degree. The framework promotes adaptive intrusion recovery, driven by the WSN's intrusion recovery requirements. To facilitate users

identify the intrusion recovery requirements that should be supported by their WSN, three intrusion recovery layers are specified covering different intrusion recovery elements. Each intrusion recovery layer is defined taking into consideration three main directions: the data sensitivity, the intrusion recovery requirements and the security attacks that need to be addressed (Figure 10). The data sensitivity indicates how valuable the WSN data is to the application and the degree of data reliance required by the decision-making process, the intrusion recovery requirements specify what operational aspects need to be recovered in case of compromisation and the security attacks that should be considered indicate whether a persistent adversary needs to be addressed. The specifications made by each layer will drive the deployment of appropriate intrusion recovery solutions in order to fulfill each layer's recovery needs.

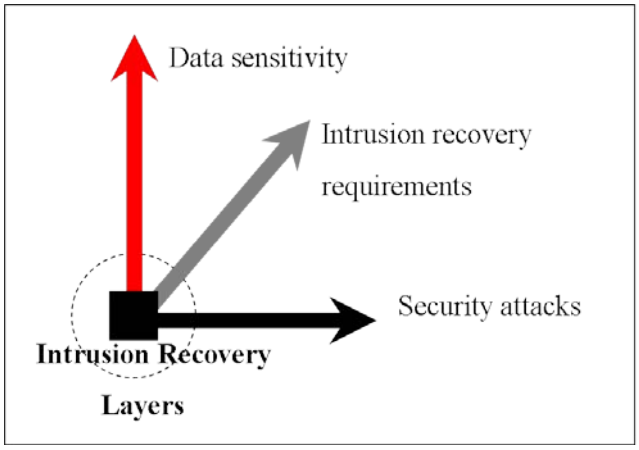

Figure 10: Directions of intrusion recovery layers specification

The following three generic intrusion recovery layers are proposed, covering diverse intrusion recovery security requirements:

1. Critical

All intrusion recovery requirements (Requirement 1-6) are of equal importance under this recovery layer. All efforts concentrate on making it hard to impossible for the adversary to

compromise the WSN's operation or recovery. WSN applications requiring this layer of intrusion recovery support critical operations. Such critical operations include healthcare monitoring [38], military surveillance [39], avalanche rescue [40], etc. The sensitivity of these applications requires high availability of WSN's fundamental services in order to support the decision making. The applicability of intrusion recovery countermeasures needs to be promoted in order to ensure a successful recovery operation. This layer aims to minimize compromised nodes (Requirement 1) from passive and active attacks and restore a stable network state (Requirement 5). A persistent adversary is addressed, considering that his attack strategy can be adaptive and consist of combined security attacks. Recovery needs to adapt (Requirement 6) according to the attack strategy to support a self-healing network behavior. The network's lifetime (Requirement 2) needs to be protected to the highest level during attack occurrences. If the WSN's functionality is compromised, it can endanger mission-critical operations and even endanger human lives. Packet loss needs to be prohibited (Requirement 3). Moreover, the WSN applications listed under this layer may handle very sensitive information that needs to be maintained secret and its occurrence to be hidden. Disclosure of information could have a number of negative impacts. For example, it may seriously damage: an organization's reputation, the security at a national/regional/organizational/individual level, etc. Eavesdropping should be prohibited to the maximum level possible (Requirement 4) as a recovery measure to traffic analysis, cryptanalysis and attack occurrence prohibition. Attack sources are confined in a strict manner in order to ensure to a high level that attacks are prohibited from occurring on an overhearing case and affecting communication.

2. Moderate

This layer focuses on a subset of the intrusion recovery requirements based on the WSN's functionality. Reliability (Requirement 3), data availability (Requirement 1) and self-healingness (Requirement 6) are pursued. Important operational aspects that need to be

recovered are packet delivery and reliable decision making. Applications from this layer require recovery from passive packet dropping attacks. Packet loss can be tolerated in case of infrequent active attacks, without the need for further recovery actions. Data sensitivity is of moderate level. Exchanged data should be protected. Some form of data protection, i.e. cryptography [8, 17, 103], is sufficient without the need to hide the communication occurrence. Data may be disclosed in some format eventually. Compromisation or loss of data could cause embarrassment to an organization, without any further negative impacts. This layer recovers compromised WSN operation from passive and infrequent active attacks, considering an adversary that deploys passive attacks and does not execute active attacks persistently. Such WSN application examples include structural monitoring [111], environmental monitoring [112] and people management systems [113].

3. Low

This is the lowest layer of intrusion recovery, applied by WSN applications with no critical or important operations. Attacks are infrequent, or even nonexistent, thus the WSN can tolerate them. Usually security defense is sufficient, i.e. integrity controls [103]. Some basic form of intrusion recovery may be applied or not be considered at all. Data sensitivity is not a concern. Often, data can be collected only for analytical reasons. WSN applications listed under this layer make the data available in the public domain. The disclosure or loss of data does not have an adverse effect on either the WSN or short-term decision-making. Application examples include agriculture production [114] and bird observation [115].

The intrusion recovery layers discussed above refer to an indicative list of WSN application examples. However, it has to be clearly stated that a WSN application categorization depends on the context it is utilized. For example, an animal observation application can be utilized for statistical reasons, thus it can be listed under the low intrusion recovery layer. If it is used to monitor endangered wildlife and there is a high risk of

compromisation, i.e. by illegal hunters, it can be considered for example under the critical layer.

3.8.2.2 Intrusion recovery layer selection process

Providing security, and more specifically recovery, is not a trivial process. Each WSN application under consideration can give emphasis on different aspects that need to be recovered in case of compromisation. Prior to the WSN deployment and operation, its intrusion recovery requirements need to be specified. This will allow the selection of the intrusion recovery layer, and the evaluation of whether the intrusion recovery countermeasure is effective in supporting the selected requirements. Figure 11 can be used by users to select the layer that best meets their intrusion recovery needs.

Each intrusion recovery layer specifies and supports a set of intrusion recovery features, taking into consideration the proposed intrusion recovery requirements as discussed in section 3.4. In order to select an intrusion recovery layer, the user has to review each of the proposed intrusion recovery layers and select the one that best reflects the WSN's intrusion recovery requirements. The following guidelines are provided in order to aid the selection of an intrusion recovery layer. The user must first identify the threat model that he is considering in the deployed environment, whether he is considering a simple or a persistent adversary. Then the sensitivity of the data needs to be considered. The data sensitivity concerns the effect an attack outcome may have on the WSN's operation and on the data that are handled by the WSN. Finally the user has to consider the intrusion recovery requirements that should be supported by the deployed WSN. In terms of availability, the user has to define if sensor nodes need to be available, with minimum interruptions as possible, or if the WSN can tolerate loss of nodes' communication. This will identify if a high link availability level needs to be achieved. The availability is affected by the attack strategy. Thus, the user has to decide

the WSN's resilience level against specific attacks. The user should consider whether the WSN can tolerate passive and/or active attacks. In terms of packet delivery reliability, the user has to specify if the WSN can tolerate packet loss or not. In terms of survivability, the user has to consider if the WSN can tolerate the energy consumption that occurs during an attack execution. The user needs to select the appropriate intrusion recovery layer, based on his requirements.

	CRITICAL	MODERATE	LOW
Threat model	Active/passive attacks Adversary persists with attacks	Passive attacks/ Infrequent active attacks	Nonexistent/ Infrequent attacks
Data sensitivity and importance to decision-making	Data maintained secret; hide data occurrence High reliance on data	Data needs to be protected; no need to hide their occurrence Disclosure has no major impact on decision-making	Data available in public domain
Network availability	Minimum interruptions	Can tolerate communication loss up to a threshold	No concern
Packet delivery reliability	No tolerance to packet loss	Can tolerate packet loss from infrequent active attacks	No concern
Resilience to eavesdropping	Prohibit attack initialization based on overhearing	Protect content from disclosure	No concern
Survivability	Minimize attack outcome that targets energy depletion	Can tolerate energy consumption due to infrequent active attacks	No concern
Self-healingness	Nodes apply recovery to address persistent attacks	Nodes apply recovery to address passive attacks	No concern

Figure 11: Intrusion recovery layer selection map

3.8.2.3 Policy rules specification

Intrusion recovery should utilize an adaptable approach in order to address static and/or persistent/adaptive adversaries and successfully restore WSN's compromised operation. In order to support such a dynamic behavior there is the need to coordinate recovery actions to

respond to different malicious activities. The coordination of intrusion recovery actions can be established by defining and enforcing an appropriate intrusion recovery security policy (Table 4). The proposed policy will enforce specific intrusion recovery rules and provide a structured approach to guide sensor nodes as to the recovery strategy they should adopt. The intrusion recovery module residing on each node is responsible to coordinate and deploy the intrusion recovery policy and manage the operation of the intrusion recovery countermeasure. When an attack is detected, the intrusion recovery module residing on each node is responsible to apply recovery according to the specified intrusion recovery policy. The target of this entity is to react against an adaptable attack strategy and recover the compromised WSN.

The policy takes into consideration different intrusion recovery requirements and security conditions for the applicability of intrusion recovery actions. The proposed policy defines recovery actions towards two directions, typical active (i.e. DoS) and passive (i.e. selective forwarding, eavesdropping) attacks. Table 4 presents the security attacks and the conditions under which a recovery action is triggered. The policy's aim is to address malicious nodes that launch a static and/or a persistent/adaptive attack strategy. In the case of a static attack strategy, a malicious node executes a specific attack against the WSN. The policy indicates the actions that need to be applied in order to address the static attack. A set of actions of general applicability are defined with the aim of providing a basic level of recovery. The general applicability actions applied by the security policy include: the detected malicious node and the associated antenna id that is utilized to communicate with the malicious node are blacklisted; the malicious node is removed from the routing table; routing paths are updated in order to exclude a malicious node, if it is detected on an active route path. The general applicability actions on their own are most efficient when applied to handle security incidents that involve simple and non-persistent attacks, such as the selective forwarding attack that can be turned ineffective as soon as the basic recovery is applied. In the case where a persistent/adaptive attack strategy is launched (meaning that the malicious node will persist with an attack, adapt the attack's dynamics or deploy a combination of attacks to compromise

the WSN's operation), the policy takes into consideration different conditions with the aim to: (a) dynamically adapt recovery based on malicious activity, (b) minimize the attack opportunities a malicious node can have to affect the network's operation, thus maintain a stable recovered network performance, and (c) turn attacks ineffective and make it hard or even impossible for malious nodes to continue compromising the WSN with a persistent/adaptive attack strategy. The aforementioned objectives are supported by utilizing directional antennas and managing their operation as proposed by INCURE in order to create controlled communication paths and isolate the malicious node from the WSN. The proposed policy specifies the applicability of the rules related to the operation of antennas during routing, aiming to aid the network to propagate critical events to the control center and allow for decision-making and further corrective measures to be taken, during an attack execution. Specifically, managing the antennas' operation is considered to:

(a) Prohibit attack initialization in the case where a malicious node is eavesdropping on the communication. If a malicious node is not aware of the communication occurrence, it may not launch an attack such as a DoS if it perceives that there are no neighbors at its vicinity.

(b) Enhance the general applicability actions against compromisation and the recovery benefits that can be achieved. In the case where a malicious node participates on an active route path and compromises the network's operation (as in the case of the selective forwarding attack), the WSN updates to new active route paths in order to exclude it and recover from the attack. In the case where only the general applicability actions are considered for recovering from the aforementioned security incident, the malicious node can deceive nodes to consider it as a next hop option during the establishment of the new route paths, leading to the continuation of the selective forwarding attack. This situation can occur if for example a malicious node executes a Sybil attack [6, 7, 8] by presenting multiple identities to the network with the aim to be reselected as a next hop towards the sink node. However, if the malicious node is isolated from

the network, it is prohibited from acknowledging and taking part in the establishment of the new route paths.

(c) Address a DoS attack by prohibiting malicious signals to be received at nodes and thus promote the network's survivability, availability and reliability.

A task related to the management of the antennas' operation, is to activate the antennas that got deactived, with the aim to avoid an attack during its execution, and assess the network status. If an attack is still valid, then nodes continue applying recovery as the policy specifies. Otherwise, nodes can participate in the network communication as usual. Integration of other recovery actions can be realized by extending the proposed security policy. This can be achieved by implementing the new recovery actions on the sensor nodes and then updating the functionality of the policy manager that is responsible for triggering a recovery action (section 3.8.1.2).

Table 4: Intrusion recovery security policy specification

INTRUSION RECOVERY POLICY			
	Security attack	Condition	Actions
Passive	Selective forwarding	No recovery required	Not applicable
		Recover packet delivery reliability. Non-persistent malicious nodes are considered.	Apply general applicability actions (*) and bypass malicious node.
		Prohibit continuation of the selective forwarding attack in the case of a persistent malicious node.	Apply general applicability actions (*). Deactivate antenna towards malicious node. Hibernation(time)
		Prohibit attack initialization based on an overhearing case	Reference eavesdropping recovery actions.

	Eavesdropping	Non-persistent adversary assumed. No need to hide the communication occurrence. Data may be disclosed in some format eventually.	Not applicable
		Prohibit attack initialization. Disclosure/loss of information could negatively impact application.	Apply general applicability actions (*). Deactivate antenna towards malicious node. Hibernation(time)
Active	Denial of Service	No recovery required	Not applicable
		Infrequent active attacks are considered. Packet loss can be tolerated.	Apply general applicability actions (*) and drop packets received from malicious node. If the attack occurrences > threshold, then follow next recovery rule.
		Address persistent adversaries. Network's survivability, availability and reliability need to be protected to the highest degree during attack occurrence.	Deactivate antenna towards malicious node. Hibernation(time)
(*)General applicability actions		Blacklist malicious node and respective receiving antenna beam, exclude from routing table, repair paths if malicious node on active route path.	

3.9 Concluding remarks

This chapter presented the INCURE framework that supports each phase of the development of a new intrusion recovery countermeasure. Three main components were proposed as part of the framework, which promote the requirements specification, design, implementation and evaluation of new intrusion recovery solutions. Specifically, this chapter covered the intrusion recovery requirements that need to be supported by an intrusion recovery countermeasure and the design objectives that have to be taken into consideration when designing new solutions. Based on the specifications, the design of a new countermeasure was presented. The proposed countermeasure utilized directional antennas to promote the intrusion recovery requirements and turn malicious activity ineffective. The operation of the countermeasure was driven by a new recovery policy that allows a WSN to dynamically adapt the applied recovery and address static and/or persistent attack strategies. Moreover, the procedure that needs to be followed by researchers in order to apply appropriate recovery, according to the WSN's intrusion recovery requirements, was described. Three intrusion recovery layers were proposed to support the objectives of the aforementioned procedure. The layers served as a guide to users to identify the intrusion recovery requirements of their WSN application. Finally, a new evaluation method was proposed as part of the INCURE framework. Chapter 4 presents the intrusion recovery evaluation method that drives the assessment of the proposed countermeasure, which is presented in Chapter 5.

Chapter 4

Intrusion recovery evaluation method

Intrusion recovery countermeasures in WSNs are developed in order to restore sensors' compromised operation and aim to allow the network to continue its operation in a secure manner, and promote reliable decision-making. The design phase of intrusion recovery countermeasures is only one step of the development process [100, 101]. One has to also evaluate the performance of the solution towards its recovery objectives, if the compromised operation can be restored and also assess if the associated cost (if any) is acceptable when recovering from security attacks.

The operations that need to be recovered in case of compromisation in a WSN are generally not investigated consistently. In order to evaluate intrusion recovery solutions, one has to identify what needs to be restored in case of compromisation and assess if a solution can restore it. Furthermore, by reviewing the literature on the area of security and intrusion recovery countermeasures in WSNs [12], it has been observed that researchers use different sets of criteria to evaluate the performance of their countermeasure in terms of security requirements, which hinders the comparison with other countermeasures proposed by others.

Currently, the lack of an all encompassing intrusion recovery related design and evaluation guideline has aggravated the design, evaluation and comparison process of intrusion recovery countermeasures in WSNs. Therefore, there is a need to establish an evaluation method in order to a) define the intrusion recovery requirements that should be considered to assess the security and performance of intrusion recovery countermeasures in WSNs, b) support researchers into evaluating and fine-tuning their designs and c) promote intrusion recovery countermeasures comparisons.

This chapter proposes an evaluation method [116] to aid the evaluation and comparison of intrusion recovery countermeasures in WSNs. The method (Figure 12) defines and gives guidelines towards three directions. First, it defines and analyzes a set of intrusion recovery requirements that should be considered in the evaluation process in order to assess the capability of a solution to recover the compromised WSN. Second, it defines appropriate evaluation criteria and maps them to the specified intrusion recovery requirements. Finally, the method guides researchers towards the evaluation phases they should adopt to assess the performance of their intrusion recovery countermeasure in WSNs.

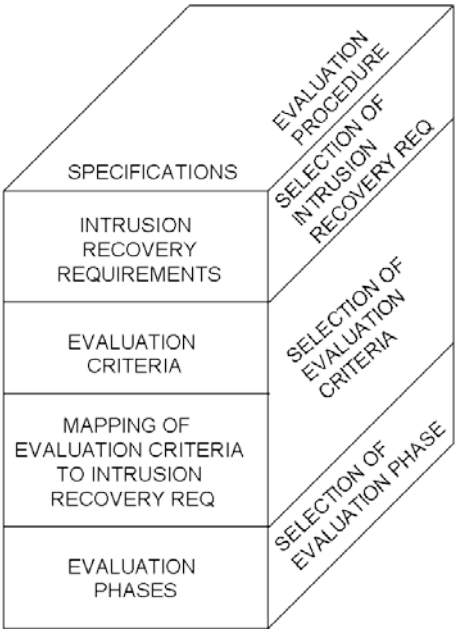

Figure 12: Intrusion recovery evaluation approach

4.1 Evaluation procedure

In order to proceed with the evaluation or comparison of intrusion recovery countermeasures, it is essential to decide what needs to be assessed according to the WSN's intrusion recovery requirements. This section guides the user to decide what intrusion recovery requirements he needs to consider for the evaluation. The selection of the intrusion recovery requirements will then drive the selection of the appropriate evaluation criteria that should be utilized for the evaluation. The activity diagram (Figure 13) presents the steps that can be followed in order to utilize the proposed evaluation selection procedure. An explanation of the process is presented in the following sections.

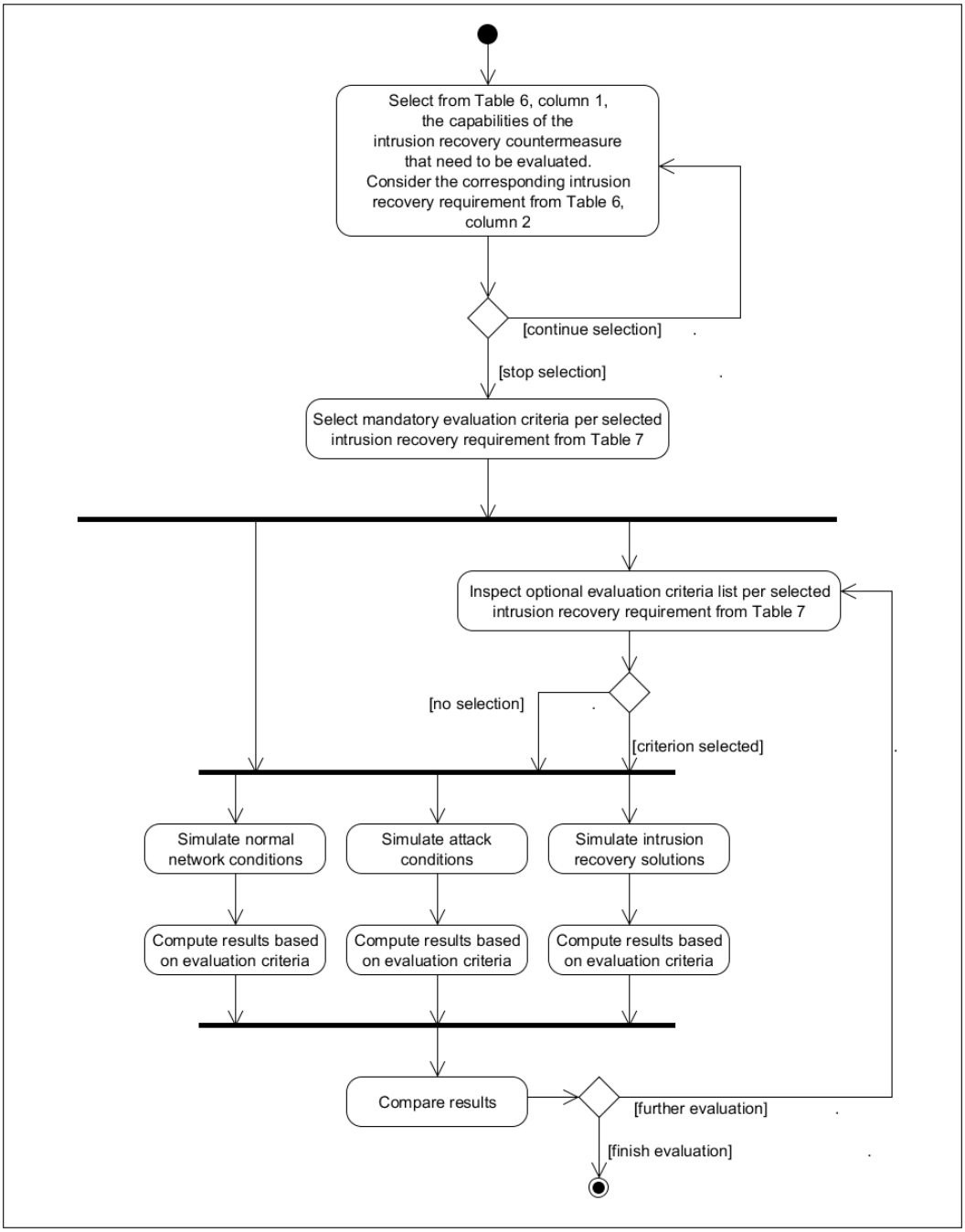

Figure 13: Evaluation methodology activity diagram

4.1.1 Definition of intrusion recovery requirements for evaluation

The main evaluation purpose is to assess whether an intrusion recovery countermeasure adhered to specific intrusion recovery requirements and has achieved its objectives to restore

the operation that has been compromised. The fact that WSN applications have diverse operational objectives and may give emphasis on different intrusion recovery requirements, makes assessment a challenging task to perform [12]. This occurs since the intrusion recovery requirements are often not well defined, thus neglecting evaluating important intrusion recovery functionality of a countermeasure. In order to achieve a comprehensive intrusion recovery evaluation, it is imperative to clearly identify what intrusion recovery requirements an intrusion recovery countermeasure considers supporting after a compromisation has occurred. The intrusion recovery requirements that should be considered in the evaluation of intrusion recovery countermeasures will drive the evaluation process.

The main tasks [5, 17] of sensor nodes include sensing the environment, communicating with other sensors and reporting the observations made to the control center/sink. If any of these tasks is compromised by an adversary, the WSN's operation can be jeopardized. Security and intrusion recovery operations that depend on sensors' communication are also at risk. Table 5 indicates the operational WSN services that can be recovered when a specific security requirement is supported by intrusion recovery countermeasures. The definition of each intrusion recovery requirement (R.1 – R.6) is provided in section 3.4.

In terms of sensing and processing, a sensor node monitors its environment if it has enough energy to perform these tasks. Since sensor nodes often use batteries [5, 17] as their main source of energy, batteries depletion leads to failure in sensing the environment. Energy depletion also leads in communication and reporting failure. Intrusion recovery countermeasures need to be assessed as to their survivability (R.2) [19] capabilities. Survivability assessment includes evaluating the ability of the adversary to achieve energy depletion and also the capability of the intrusion recovery countermeasures to prohibit the energy consumption due to the attacks.

One of the most important tasks of a WSN can be considered the nodes' communication ability. If sensors are prohibited from communicating, then reporting of observations cannot be achieved and decision-making can be compromised and turned ineffective. This means that any compromisation that occurs at the communication level has to be restored. Assessment should take into consideration the need for packet and link communication availability (R.1). This means that a recovery countermeasure needs to be evaluated as to its ability to restore the communication link and the compromised nodes operation. Reliable decision-making is depended on the ability of the WSN to report the observations to the decision entity/control center. If the operation of the WSN is compromised and observations are not reported, then correct decision-making cannot be promoted. Reliability (R.3) assessment in the context of intrusion recovery means to evaluate whether the ability of the network for packet delivery can be restored in case of compromisation.

Restoring compromised services does not mean that the adversary will stop attacking the network. It is crucial that the intrusion recovery measures aid compromised services to recover and provide the sensor nodes the means to resist new attacks aiming to interrupt the recovered WSN operation. Evaluation should consider the resilience (R.4) level that can be achieved by the deployed intrusion recovery countermeasures when the network is under attack. Such an assessment will indicate the attack strength and whether the adversary can affect the network's resilience. The results could be used to improve the intrusion recovery countermeasure under evaluation.

Intrusion recovery would be very effective if sensor nodes are equipped with the logic of applying intrusion recovery countermeasures according to the situation. Demonstrating a self-healing (R.6) behavior will allow sensor nodes in remote and/or hostile areas to recover from compromisation and continue their operation without the need of human intervention. The self-healing capability of an intrusion recovery countermeasure should be assessed to conclude on its ability to address different attack situations. The evaluation should also

consider the responsiveness (R.5) capability of the recovery measures and assess whether they can aid the network to perform its tasks when recovery is applied to address security attacks. During the observation of critical events, the main responsibility of a WSN is to propagate the observations to the control center in a timely manner. It is important to consider how the network's responsiveness is affected during security attacks or when recovery actions are applied, and whether recovery measures can prohibit malicious nodes increasing the network's response time while achieving a stable operational state.

Table 5: Recovered WSN services based on intrusion recovery security requirements

Intrusion recovery security requirements	**Recoverable operational WSN services when a requirement is met**		
	Sensing	**Communicating**	**Reporting**
R.1: Availability	x	x	x
R.2: Survivability	x	x	x
R.3: Reliability			x
R.4: Resilience		x	x
R.5: Responsiveness		x	x
R.6: Selfhealingness		x	x

4.1.2 Intrusion recovery requirements selection for evaluation

The evaluation will assess the intrusion recovery countermeasures' capability to address security attacks, recover compromised network operation and prohibit attack occurrence. In the evaluation process, one has to first identify the capabilities of his/her countermeasure that need to be evaluated. The capabilities of a countermeasure express the intrusion recovery requirements that need to be supported by the countermeasure, based on which the evaluation will indicate if the countermeasure's objectives are met. The following list defines a number of statements that are related to specific intrusion recovery requirements. One should choose

the statements that are valid from Table 6 (column 1), taking into consideration the operation of the countermeasure under evaluation. The selected statements will indicate the intrusion recovery requirements (Table 6, column 2) that need to be considered and which will drive the evaluation process.

Table 6: Intrusion recovery requirements selection for evaluation

Intrusion recovery requirement selection for evaluation	
Assess Intrusion Recovery Countermeasures' Capability to:	**Reguirement selection**
• Recover from service interruptions. • Restore compromised nodes and communication links.	R.1: Availability
• Minimize energy consumption. • Incur reasonable energy consumption due to recovery measures.	R.2: Survivability
• Enable packets to reach destination. Support reliable decision making.	R.3: Reliability
• Prohibit adversary to compromise network operation, after recovery is applied. Minimize eavesdropping on communication.	R.4: Resilience
• Respond to critical events by propagating observations to the control center in a timely manner.	R.5: Responsiveness

• Prohibit malicious nodes from affecting the network's response time to deliver packets to the control center.	
• Address different attack strategies and respond dynamically according to case.	R.6: Self-healingness

4.1.3 Evaluation criteria selection

The proposed evaluation method maps each intrusion recovery requirement (Table 6) to one or more evaluation criteria (section 4.1.3.1). The appropriate criteria should be utilized, based on the selected intrusion recovery requirement (from Table 6) that needs to be considered in the evaluations. Table 7 presents the proposed mapping between the intrusion recovery requirements and evaluation criteria; it should be referenced in order to choose the appropriate evaluation criteria based on the requirements selected from the previous step. The selected criteria should be used in order to assess if the countermeasures under evaluation adhere to the intrusion recovery requirements represented by the selected criteria. Evaluation criteria are either tagged as mandatory or optional. Each intrusion recovery requirement considers at least one mandatory criterion required to be utilized for countermeasures' assessment and/or comparison. Other optional criteria may be utilized, if they exist. Mandatory criteria are essential in order to assess the main objective of a specific evaluation aspect. Optional criteria are complementary to the evaluation and can be utilized if required to further explain the performance of the WSN and the deployed intrusion recovery countermeasures. The grey-shaded cells in Table 7 indicate mandatory evaluation criteria while the white-shaded cells represent the optional evaluation criteria.

Table 7: Evaluation criteria selection

	Intrusion recovery requirements for evaluation						
Evaluation criteria (EC)	**R.1 Availability**	**R.2 Survivability**	**R.3 Reliability**	**R.4 Resilience**		**R.5 Responsiveness**	**R.6 Self-healingness**
				Eavesdrop	**Other attacks**		**Consider a variety of attacks**
EC.1: Compromised nodes (due to attack)	x			x	x		x
EC.2: Compromised nodes (due to recovery)	x						
EC.3: Energy consumption		x			x		x
EC.4: Routing overhead		x					
EC.5: Retransmissions		x					
EC.6: Path length		x					
EC.7: Packet delivery		x	x		x	x	x
EC.8:Eavesdropped packets				x			x
EC.9: Number of malicious nodes on eavesdropping				x			
EC.10: End-to-end packet delivery delay						x	x
Note: Mandatory evaluation criteria in grey-shaded cells, Optional evaluation criteria in white-shaded cells							

4.1.3.1 Definition of evaluation criteria

Sections 4.1.1 and 4.1.2 have discussed the intrusion recovery requirements that need to be considered in the evaluation in order to decide if a specific intrusion recovery solution is able to restore compromised WSN services. For each intrusion recovery requirement, there is the need to identify the evaluation criteria that should be considered in a potential experiment/simulation scenario. This section describes the evaluation criteria (EC) and their objectives in order to categorize them under a specific intrusion recovery requirement. The evaluation will reveal the effectiveness of a solution to address attacks and the ability of the adversary to successfully attack the network after recovery measures are applied.

4.1.3.1.1 Number of compromised nodes (due to attack) (EC.1)

The number of compromised nodes will evaluate the ability of the intrusion recovery to address an attack and restore compromised nodes operation, its robustness level and the compromisation capabilities of the adversary. In the case of the:

- *selective forwarding attack*, the compromised nodes are calculated by counting the one-hop nodes i downstream of the malicious nodes which are prohibited from communicating with the sink as indicated by the following formula:

$$EC.1: COMPR\_NODES(SLF) = \frac{\sum_{i=1}^{N} i \in active\_path \quad (source \rightarrow dest) \quad \wedge \quad next\_hop(SLF\_MN)}{N}$$

where *N* is the number of nodes and SLF_MN is a malicious node that executes the selective forwarding attack and is a next hop neighbor of node i.

- *eavesdropping attack*, compromised nodes are considered the nodes i that are tapped by the malicious nodes and give the advantage to the adversary to launch other attacks, i.e. DoS attack. The following formula should be considered for the calculation:

$$EC.1: COMPR\_NODES(EAV) = \frac{\sum_{i=1}^{N} EAV(i)}{N}$$

where *N* is the number of nodes and

  - EAV(i) = 1, if node's i transmission can be eavesdropped by a malicious node
  - EAV(i) =0, if node's i transmission cannot be eavesdropped by a malicious node

- *DoS attack*, compromised nodes are considered the ones that can be reached by the nodes executing the attack.

$$EC.1: COMPR\_NODES(DoS) = \frac{\sum_{i=1}^{N} DoS(i)}{N}$$

where *N* is the number of nodes and

  - DoS(i) = 1, if a node i is affected by the DoS attack
  - DoS(i) =0, if a node i is not affected by the DoS attack

4.1.3.1.2 Number of compromised nodes (due to recovery) (EC.2)

Intrusion recovery countermeasures should be assessed whether they compromise the nodes' operation during the effort to recover from compromisation. The proposed recovery solutions should be assessed as to whether they incur compromised nodes and if the network's

operation is affected. During the applicability of the intrusion recovery actions, a node i is considered to be compromised by a recovery countermeasure, if it has deactivated all its antennas or if all its neighbors have deactivated their antenna beams towards the node. The following formula calculates the nodes i that are affected by recovery:

$$EC.2: COMPR\_NODES(REC) = \frac{\sum_{i=1}^{N} affected(i)}{N}$$

where *N* is the number of nodes and affected(i) = i : (∀antenna(i):DEACTIVATED || ∀antenna(nb→i): DEACTIVATED, nb is a neighbor of node i). Consider:

- affected(i) = 1, if a node i is isolated due to the recovery measures
- affected(i) =0, if a node i is not isolated due to the recovery measures

4.1.3.1.3 Energy consumption (EC.3)

This criterion will assess if an intrusion recovery countermeasure can minimize the energy consumption that occurs during an attack that targets to affect the survivability of nodes. Also, it can assess if a persistent adversary can continue affecting the network's energy consumption after an intrusion recovery countermeasure is applied. The following formula calculates the mean energy consumption from all the sensor nodes, measured in Joules:

$$EC.3: Energy = \frac{\sum_{i=1}^{N} E_c^i}{N}$$

where *N* is the number of nodes and *Ec* (in Joules) is the energy consumed at each node *i*. Ec counts the energy consumed for packet transmission, packet reception, sleep, idle state and antenna switching.

4.1.3.1.4 Routing control overhead (EC.4)

Routing control packets are usually exchanged to support the objectives of the routing phases and intrusion recovery mechanisms respectively. It is important to count the routing control overhead produced when an attack occurs or when recovery is deployed. This will indicate if the recovery solution is effective in minimizing/prohibiting the attack outcome, by minimizing the routing overhead that is incurred. If routing communication is increased it will affect the energy consumption. Therefore, it is necessary to study if the communication overhead is at an acceptable level in order to support the survivability of the network. The following formula counts the total routing control packets that are transmitted by each sensor node i:

$$EC.4: ROUTE\_CTRL\_OVER = \sum_{i=1}^{N} routing\_ctrl\_pkts(i)$$

4.1.3.1.5 Retransmissions (EC.5)

Due to the nature of the wireless medium and the adversary's ability to launch a variety of attacks such as a DoS [14, 15], packet loss can occur in the network, forcing the nodes to retransmit packets, disrupting the routing, security and observation operations. Retransmissions lead to energy consumption and packet delivery delays, therefore they should be minimized. Once intrusion recovery countermeasures are applied, it is anticipated that security attacks will be prohibited from affecting the network. Evaluation will indicate if recovery countermeasures can minimize packet retransmissions in the face of security attacks. This will also reveal the resilience level against security attacks that can be achieved by a recovery countermeasure. The following formula calculates the total packet retransmissions that occur by counting the times r that each packet i was retransmitted.

$$EC.5: PKT\_RETR = \sum_{i=1}^{k} \sum_{r=1}^{h} retransmitted\_packet(i)$$

4.1.3.1.6 Packet delivery (EC.6)

The packet delivery criterion will indicate if the network can restore its packet delivery capability and reliably deliver packets to the destination in the presence of attacking adversaries. The following formula is utilized to calculate the packet delivery ratio (PDR):

$$EC.6: PDR = \frac{P_{rx}}{P_{tx}}$$

where P*rx* is the total number of packets delivered to the sink and P*tx* is the total number of packets transmitted by all source nodes.

4.1.3.1.7 Path length (EC.7)

As the path length increases, the packets traverse more hops to reach the destination. This incurs more energy consumption and increased packet delivery delays. One should consider assessing if an intrusion recovery countermeasure leads to longer path lengths and decide if it is acceptable in terms of energy consumption and delay. The chance of an adversary to compromise the communication is also increased. As the packet is forwarded by more nodes, the adversary has a better chance to be among the forwarding nodes or he can even have more opportunities to attack while the packet is traversing the network. Therefore, it is important to

consider if the incurred path length has an acceptable trade-off between security and compromisation.

$$EC.7 : PATH\_LEN = \frac{\sum_{p=1}^{PN} path\_hops(p)}{PN}$$

where path_hops is the number of hops in a given path p from source to destination and PN are the total paths established in the current evaluation.

4.1.3.1.8 Eavesdropped packets (EC.8)

The adversary can eavesdrop on the communication and launch a number of attacks using the captured packets, such as traffic analysis, replay attack, etc. The number of eavesdropped packets will show the ability of the adversary to overhear communication and the ability of the countermeasures to minimize eavesdropping. This criterion will assess if an intrusion recovery countermeasure can promote a resilient network operation against the eavesdropping attack. The following formula calculates the total eavesdropped packets P_{eav} that are overheard by each malicious node *m*:

$$EC.8 : EAV\_PKTS = \sum_{m=1}^{MN} \boldsymbol{P}_{eav}(\mathrm{m})$$

where MN is the total number of malicious nodes.

4.1.3.1.9 Number of malicious nodes on eavesdropping (EC.9)

The number of malicious nodes that can eavesdrop also indicates how effective an intrusion recovery solution is in isolating malicious nodes. Moreover, this criterion helps

assessing the risk level that exists in the case where the malicious nodes decide to launch new attacks. The following formula calculates the number of malicious nodes that eavesdrop on the communication:

$$\text{EC.9}: \text{EAV\_MALICIOUS\_NODES} = \sum_{m=1}^{MN} EAV\_MN(m)$$

where MN is the number of malicious nodes and EAV_MN is a malicious node that can eavesdrop on the WSN's communication.

4.1.3.1.10 End to end packet delivery delay (EC.10)

The timely arrival of routing control and data packets ensures the successful operation of the network, the provision of intrusion recovery services and support of decision-making processes. However, since communication in WSNs may be affected by a number of elements, transmitted packets may experience delays to reach the intended destination. The average end-to-end packet delivery delay (E2E_PDD) will indicate if recovery measures can aid the network to converge fast to a stable state, allowing it to continue its operation. The delay evaluation metric, measured in milliseconds, is calculated using the following formula:

$$\text{EC.10}: \text{E2E\_PDD} = \frac{\sum_{i=1}^{\text{Pr}} (Pt_r^i - Pt_g^i)}{\text{Pr}}$$

where the difference between the packet generation time Pt_g at the source and packet reception Pt_r at the sink of packet i is considered. Pr refers to the total number of packets successfully received at the destination. Lost packets are considered having "infinite" delay and therefore are not considered in the delay calculations, following the approach proposed in

[117]. This is necessary in order to be able to compute and make valid observations about the average end-to-end packet delivery delay.

Table 7 maps the evaluation criteria to specific intrusion recovery security requirements in order to evaluate if a specific capability of a countermeasure meets its purpose. The following section discusses the evaluation phases that should be utilized in the assessment. The selected evaluation criteria should be used in each evaluation phase in order to assess a recovery countermeasure.

4.1.4 Evaluation phases definition

In order to conclude on the effectiveness of an intrusion recovery countermeasure to minimize an attack outcome, its behaviour should be assessed under normal network conditions (phase 1), when security attacks are executed (phase 2) and when intrusion recovery is applied (phase 3). The following three evaluation phases should be utilized:

- *Normal*. The network should be assessed under normal network conditions. This will constitute the initial reference case where all other phases will be compared against.
- *Security attack*. In the case where malicious activity is considered, further information must be defined:
  - Attack type. List what attacks are considered.
  - Number of malicious nodes. Define the percentage of nodes in the network that act maliciously.
  - Adversary transmission range. Define the malicious nodes' transmission range in comparison to the legitimate nodes respective settings.

- *Intrusion recovery*. Consider the recovery countermeasures that are applied to address specific security attacks.

4.2 Concluding remarks

This chapter proposed an intrusion recovery evaluation method in order to promote the assessment and comparison of intrusion recovery countermeasures. First, the intrusion recovery requirements that should be considered in the evaluation of intrusion recovery countermeasures were specified. Then a number of evaluation criteria were defined and associated with specific intrusion recovery requirements. The aim of the proposed method was to help the user identify the intrusion recovery requirements and the related evaluation criteria he/she should consider in order to assess the capabilities of his/her countermeasure. The evaluation method drives the assessment of the INCURE countermeasure. Chapter 5 presents the performance evaluation results.

Chapter 5

Performance evaluation

The proposed directional antennae based intrusion recovery framework is evaluated in an IEEE 802.15.4 network using ns2 [118] simulations and also compared to typical intrusion recovery solutions implemented in omni-directional antennae WSNs. The following sections present the evaluation metrics, the evaluation process, the simulation scenarios and configurations and the analysis of the simulation results.

5.1 Evaluation objectives

This section defines the evaluation objectives (EO) that will drive the evaluation scenarios specification and configuration (section 5.2) and the result's analysis phase (section 5.3).

This research work considers a WSN supporting critical operations, thus recovery services are needed to varying degree to restore the compromised WSN and support decision-making. Decision-making can be affected by the unavailability (either partially or fully) of the sensors' observations. Malicious nodes aim to affect decision-making by trying to disrupt the network's operation in order to prohibit observation, identification and handling of critical events. To achieve their malicious objectives, they launch different security attacks in order to

compromise the network's ability to communicate and affect the availability, survivability, reliability and resilience of the sensor network. Typical security attacks that can be deployed to affect the network's communication capability are the selective forwarding and DoS attacks. A malicious node is considered to either follow a static or persistent/adaptive attack strategy to achieve its objectives. In order to address the attacks' outcome, nodes deploy appropriate recovery measures. A static attack strategy consists of the execution of a single attack, while a persistent attack strategy starts with an attack and adapts accordingly as nodes apply recovery in order to address compromisation.

The evaluation objectives are specified below:

EO.1. Assess the effectiveness of the proposed intrusion recovery countermeasure to restore the WSN's operation when considering: (a) a static (section 5.3.1.2) and (b) a persistent attack strategy (section 5.3.1.4) that is utilized taking into consideration both line of sight (section 5.3.1) and shadowing conditions (section 5.3.2). The effectiveness of typical intrusion recovery solutions implemented in omni-directional WSNs will also be assessed and compared to the proposed solution. The evaluation also aims to investigate if the proposed/typical intrusion recovery solutions applied against a static attack strategy are adequate to address a persistent/adaptive attack strategy and to identify if there are any deficiencies. Moreover, the assessment will identify if there is any tradeoff that incurs from the recovery measures, or benefits that empower the WSN to address malicious nodes that execute either a static or persistent/adaptive attack strategy.

EO.2. Evaluate the effectiveness of INCURE/typical solutions to recover the compromised WSN (sections 5.3.1.4.5 and 5.3.2.1.1). In order to facilitate the performance evaluation of this work, the intrusion recovery evaluation method

(Chapter 4) is been applied to identify the intrusion recovery requirements and related evaluation metrics that need to be considered:

a. Availability (R.1). Assess if recovery can minimize the ability of malicious nodes to compromise the communication ability and operation of nodes and also if there is any tradeoff related to compromised nodes that incurs from the recovery measures.
b. Survivability (R.2). Evaluate if the attack outcome related to energy depletion can be minimized and also assess in what way the recovery may affect the energy consumption.
c. Resilience (R.3). Assess if recovery measures can empower nodes to restore and retain their communication and packet delivery ability when malicious nodes execute a static/persistent attack strategy. Also, evaluate if the DoS attack initialization based on an overhearing case can be minimized.
d. Reliability (R.4). Investigate if the packet delivery capability can be restored in case of compromisation.
e. Responsiveness (R.5). Observe how a network responds during security attacks and when recovery actions are applied. Evaluate if the network's responsiveness can be restored, taking into consideration the network's packet delivery capability along with the network's response time to deliver observations to the control center.
f. Self-healingness (R.6). Assess if recover measures can aid a network to restore its compromised operation while addressing different attack situations.

This research work utilizes the mandatory evaluation criteria (Table 7, page 100) that are related to the selected intrusion recovery requirements in order to perform the evaluation, as proposed in section 4.1.3, that is: compromised nodes (due to the attack (EC.1) / due to recovery (EC.2)), packet delivery ratio (EC.7), energy consumption (EC3), number of eavesdropped packets (EC.8) and average end-to-end packet

delivery delay (EC.10). A detailed discussion related to each evaluation criterion is provided in section 4.1.3.1.

EO.3. Evaluate the memory overhead (section 5.3.3) and the cost (section 5.3.4) of INCURE's main components.

The following section presents the simulation scenarios that are utilized to support the aforementioned evaluation objectives.

5.2 Simulation scenarios

This section presents the specification and configuration of simulation scenarios.

5.2.1 Specification

Simulation scenarios have been defined towards two directions in order to support the evaluation objectives: (a) a static attack strategy and (b) a persistent attack strategy. In order to address each attack strategy, the WSN deploys appropriate intrusion recovery countermeasures. The simulation scenarios specified (attack and recovery related) are deployed by the following two networks: (a) the INCURE network where nodes are equipped with directional antennas and utilize the proposed countermeasure and/or the typical intrusion recovery actions of blacklisting and rerouting and (b) a network that deploys typical intrusion recovery solutions using omni-directional antennas in WSNs. Scenarios deployed by the first network are referred to as INCURE scenarios while scenarios deployed by the second network are referred as OMNI scenarios. A normal network operation is first simulated and used as an initial reference for comparison when the INCURE and OMNI networks are under attack.

As discussed in section 5.1, malicious nodes' main objective is to affect the network's communication and thus prohibit decision-making. Typical security attacks that are deployed to affect the network's communication are the selective forwarding and DoS attacks. Malicious nodes deploy a static attack strategy where the selective forwarding (section 5.3.1.2.1) or a DoS attack (section 5.3.1.2.2) is executed against the WSN. Two simulation scenarios are defined as part of the static attack strategy, one scenario for each of the aforementioned attacks, in order to investigate how each attack can affect the operation of the network. Typical intrusion recovery countermeasures are then deployed by the WSN to address each attack. In the case of the selective forwarding attack, legitimate nodes blacklist malicious nodes that execute the attack, stop forwarding/receiving packets towards/from them and reroute traffic in the case where the malicious nodes participate on active route paths. A simulation scenario is created as part of the recovery strategy of nodes in addressing the selective forwarding attack. The aforementioned scenarios (attack and recovery related) are deployed by both INCURE and OMNI networks. Nodes participating in the INCURE or OMNI network deploy the aforementioned typical recovery actions in order to address the selective forwarding attack. Results show that both networks can successfully restore the normal operation of the sensor network when they deploy typical recovery countermeasures for the selective forwarding attack, with INCURE achieving a better network performance in terms of packet delivery and energy consumption. In the case of the DoS attack, two simulation scenarios are specified, a scenario concerning the INCURE network and another one for the OMNI case, where nodes deploy different intrusion recovery countermeasures to address the attack. INCURE nodes manage the operation of their antennas towards the malicious nodes as specified in section 3.7 while OMNI nodes deploy a low duty cycle as discussed in section 2.2.1.3. Evaluation shows that INCURE recovers the availability, resilience, reliability and survivability of the network with no significant tradeoff, while OMNI is able to recover the survivability of the network at the expense of nodes' availability and packet delivery capability. Furthermore, in the case of the INCURE network,

investigations (section 5.3.1.3) are performed to assess if the measure of managing the deactivation of antennas when security incidents occur is beneficiary (over the case where only typical intrusion recovery actions are utilized) when deployed to recover from the selective forwarding attack while considering a persistent/reactive attack strategy. Results show that recovery is further enhanced when INCURE nodes manage the operation of their antennas to recover from compromisation, instead of utilizing only the typical measures of blacklisting and rerouting. The rest of the discussion concerns the adoption of a persistent attack strategy (section 5.3.1.4) by the malicious nodes.

In the context of a persistent attack strategy (Figure 14, page 117), malicious nodes start with a security attack and as the network applies recovery, malicious nodes adapt their strategy in an effort to continue compromising the network's operation. As discussed in section 3.5, malicious nodes often act conservatively to save their energy resources [15, 102]. Thus, they deploy a security strategy that can meet the objectives of the operation of affecting nodes while minimizing the energy they have to spend in order to attack the network. Malicious nodes start with the selective forwarding attack, as it is a passive attack that does not need malicious nodes to spend a lot of energy in comparison to active attacks such as a DoS attack. As soon as recovery measures are applied by nodes in order to turn the selective forwarding attack ineffective, malicious nodes continue their efforts to affect the network's operation. In the context of malicious nodes' efforts to spend little energy for their compromisation attempts, they first identify the presence of legitimate nodes before launching an attack. Thus, persistent/reactive malicious nodes execute a DoS attack in case they can eavesdrop on the network's communication. The evaluation demonstrates that the proposed scheme minimizes the adversary's ability to overhear and prohibit malicious reactive actions. A continuous DoS attack is then considered in the case where the malicious nodes decide to aggressively attack the network, independently of whether they can overhear or not. The proposed scheme showcases the ability of INCURE to minimize the attack outcome related to compromised nodes, packet delivery and energy consumption in comparison to the typical

intrusion recovery countermeasure of low duty cycle in omni WSNs. It is also demonstrated that the OMNI network has to deploy more recovery actions (channel surfing) in an attempt to address the continuous DoS attack and increase the network's performance. Even so, compromisation in OMNI case is again achieved despite channel surfing having been deployed, thus the network's operation continue to be affected, as the malicious nodes reconnaissance the network and adapt their actions to continue with the attack. Then it is assumed that the malicious nodes persist with their intrusion strategy in an effort to succeed in compromising INCURE's and OMNI's operation. The malicious nodes extend the DoS attack, by increasing their transmission power, with the aim of increasing the affected coverage area. Both the networks continue their recovery strategy (INCURE versus the OMNI low duty cycle) in order to mitigate the extended attack. The assessment demonstrates that INCURE can minimize the compromisation of network's availability, survivability, reliability and resilience when compared to the OMNI case. Moreover, the evaluation demonstrates that INCURE yields considerably less tradeoff in terms of compromising nodes' availability when compared to the OMNI low duty cycle recovery countermeasure. Overall, the proposed countermeasure addresses adversaries that implement a static or persistent attack strategy and supports intrusion recovery requirements more effectively than typical intrusion recovery countermeasures in WSNs.

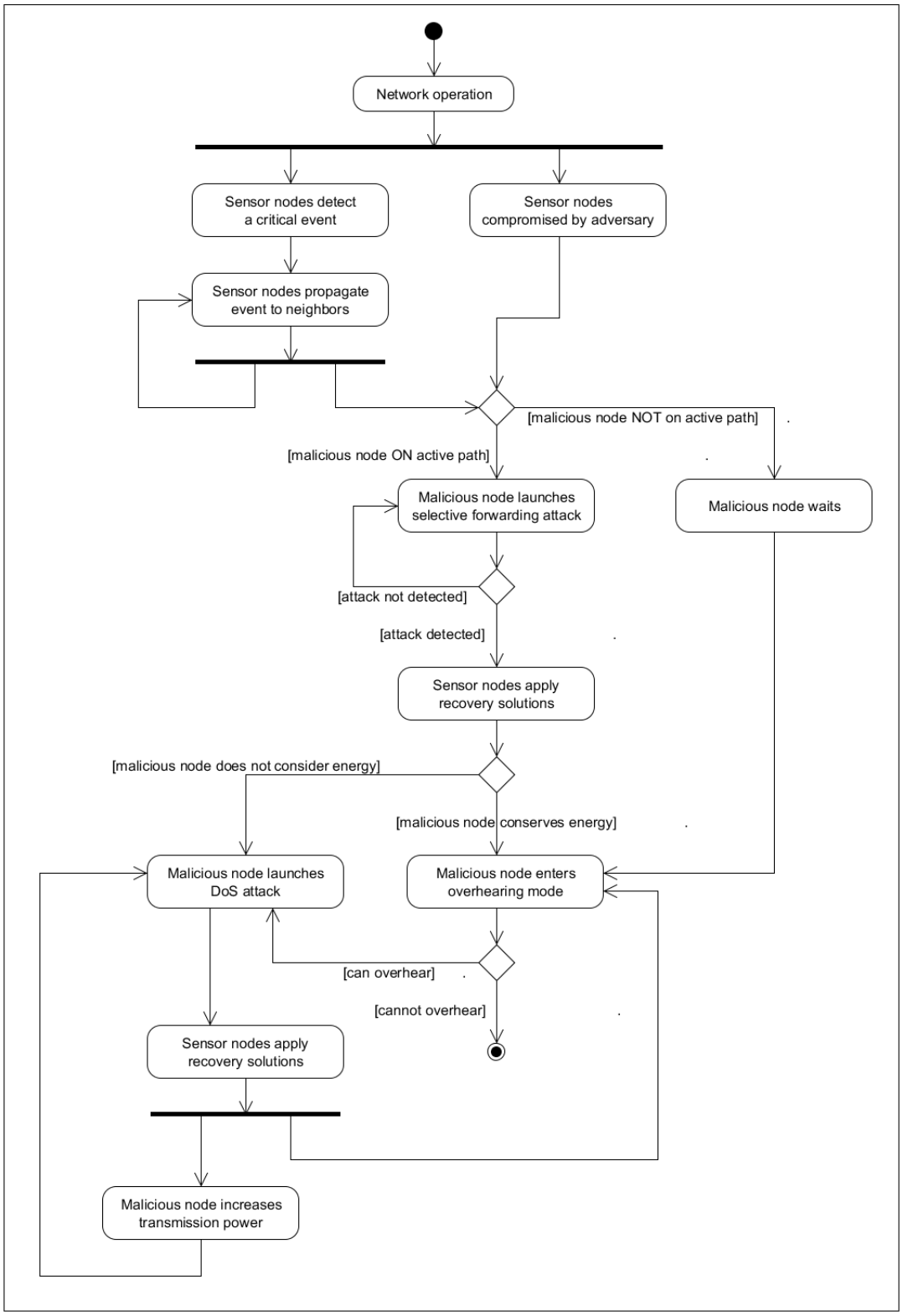

Figure 14: Simulation scenarios flow activity diagram

5.2.2 Configuration

This section presents the configurations considered in the evaluation. The proposed framework is evaluated under line of sight (LOS) and non-line of sight (NLOS) radio conditions. Sender nodes generate constant bit rate (CBR) traffic with a rate of 2 packets per second and a packet size of 70 bytes [3, 41, 119], under the assumption of a detected event. Moreover, 5% and 10% randomly selected malicious nodes are considered [18, 102, 120]. In order to facilitate the intrusion recovery actions, an IDS process is simulated by each sensor node to identify an attack execution. Overall, 6240 simulations have been performed and analyzed, computing average values on selected evaluation metrics and 95% confidence intervals. According to the simulation setup/scenario that is executed, the total size of the files produced by each averaged simulation setup and its related results analysis, ranges from 500MB to 10GB. When the performance evaluation is finished, formatted reports of the results are saved for further processing. Details of the simulation framework are presented in APPENDIX B.

INCURE is implemented in the context of the popular AODV [121] routing protocol for illustration purposes and utilizes patch directional antennas as in [122]. It is worth pointing out that in [122] it is also demonstrated that it is feasible to equip sensor nodes with directional antennas. Figure 15 presents the utilized antenna pattern. The receiver's sensitivity is considered to be -90 dBm in both networks. The transmission range for both INCURE and OMNI antennas is set to be the same. This is achieved by transmitting more power in the omni-directional network to compensate for the antenna gain of the INCURE network. This is done in order to compare in a fair manner the proposed countermeasure against typical intrusion recovery countermeasures that use omni-directional antennas. The plane earth loss propagation model in ns2 is utilized for the path loss calculations in LOS scenarios and the log-normal shadowing model for non LOS scenarios. Initial energy is 100 Joules. Power consumption was based on a CC2400 WSN transceiver [123].

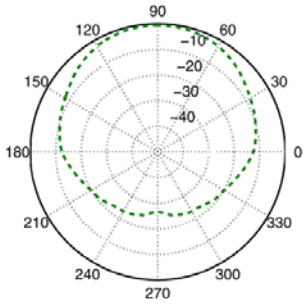

Figure 15: INCURE antenna pattern

Three different topologies are simulated: (a) a grid topology 1000x1000 m, (b) a random sparse topology 750x750 m and (c) a random dense topology 550x550 m. These topologies were selected to achieve different levels of connectivity, from minimally-connected (3 to 4 neighbors) to moderately-connected (8 to 12 neighbors) [54]. In every case, the network consists of 100 nodes. In the case of the grid topology, both INCURE and OMNI networks have the same node density of 3.6. INCURE nodes are placed on the grid with each antenna beam facing the cross neighbors in order to transmit and receive with the maximum gain from each antenna beam towards each neighbor. The proposed countermeasure utilizes directional antennas to control the exposure of the nodes and minimize the opportunities of malicious nodes to compromise a node's operation. Based on the selected antenna pattern and the number of antennas utilized, INCURE achieves different node densities than OMNI in the case of random topologies. In random topologies OMNI yields a higher node density than equivalent INCURE scenarios as the omni-directional nature of transmission allows a node to discover all neighbors that are in its coverage. In random topologies, nodes are uniformly distributed over the deployment area. The antenna model utilized in the thesis yields an average node density of 4.1 for the random sparse 750x750 topology and 7.5 for the random dense 550x550 topology. OMNI yields 6.5 and 11.7 node densities for the equivalent topologies.

5.3 Simulation results

This section presents the analysis of the simulation results when the adversary deploys a static or persistent/adaptive attack strategy. Each attack/recovery-related INCURE/OMNI setup/scenario (section 5.2.1) has been simulated over 30 random topologies and presented results have been averaged over the set of the 30 simulation runs. The evaluation figures are listed in APPENDIX C. Each simulation scenario is assessed based on the selected evaluation metrics as discussed in section 5.1. For the analysis of each evaluation metric, an increase/decrease percentage is utilized in order to compare each INCURE/OMNI simulation scenario under evaluation with a reference (R) scenario that is specified at the point where the analysis is presented. The reference scenario represents a previous network state and it is utilized in the analysis to facilitate the comparison with the new network state, resulted from the current simulation scenario under evaluation, and thus conclude on the countermeasures' effectiveness to address a security attack. Specifically, the aim of the analysis is to observe whether attacks have affected the operation of the network and whether recovery actions have restored the compromised network operation. Appropriate evaluation tables are presented at each analysis section displaying the relevant results obtained from the simulation scenario (S) under evaluation and the reference (R) scenario. A separate column at each evaluation table indicates the increase/decrease (I/D) percentage results, as compared to the referene scenario. A "+%" notation indicates an increase performance percentage while a "-%" notation means a decrease performance percentage of the simulation scenario (S) in comparison to the reference (R) scenario. Moreover, a comparison between INCURE versus OMNI is peformed, indicating which network (INCURE or OMNI) has a gain over the other. The term "gain" has a different meaning for each evaluation metric. In terms of packet delivery, a x% gain of network A over B means that network A has x% more packet delivery than B. In terms of energy consumption, packet delivery delay, compromised nodes and eavesdropped packets, a x% gain of network A over B means that network A has achieved x% less energy consumption/packet delivery delay/compromised nodes/eavesdropped packets than network

B. When INCURE has a gain over OMNI, this is indicated by an "(I)" notation in the evaluation tables. Otherwise, a "(O)" notation is presented to indicate OMNI gain over INCURE.

The main focus of this thesis is a persistent attack strategy, which can severely damage the WSN if not appropriately addressed, especially for mission-critical applications. The analysis related to a persistent adversary considers both LOS (section 5.3.1) and NLOS (shadowing section 5.3.2) radio conditions. For evaluation purposes we also consider a static attack strategy to show that typical intrusion recovery measures are adequate to address only a simple adversary. When a static intrusion strategy turns into persistent/reactive, we first demonstrate (section 5.3.1.3) the importance of managing the operation of antennas by INCURE nodes in order to increase the recovery benefits over the case where INCURE deploys only typical recovery measures. For the static attack strategy and INCURE investigations when a static intrusion strategy turns into persistent only LOS radio conditions are considered as we expect to have a similar behaviour when considering NLOS conditions.

5.3.1 Line-of-sight conditions (LOS)

This section analyzes the results when LOS radio conditions are considered.

5.3.1.1 Normal network conditions

In order to extract conclusions regarding the networks' performance, according to the different recovery actions that will be applied to address the security attacks, comparisons will be made with a reference to the results that are produced when both OMNI and INCURE networks operate under different conditions, starting with normal conditions. Thus, normal network conditions will constitute the initial reference scenario.

As it can be observed in Table 8, the INCURE case achieves 94%, 89% and 97% packet delivery when considering a random sparse (750x750), dense (550x550) and grid sparse (1000x1000) topology respectively under normal network state. The lower packet delivery observed in the dense topology is due to a higher number of collisions and packet drops that occur due to the higher node density. The OMNI scenarios demonstrate about 9% less packet delivery when compared to the INCURE sparse topologies and 19% compared to the dense topology respectively (86%, 74%, 89%). The packet delivery in the INCURE network is higher as it takes advantage of the directional antennas' ability to focus on specific transmission and reception directions, reducing packet loss, retransmissions and overhearing.

Table 8: LOS Normal network conditions – Packet delivery %

Packet delivery %	Topologies		
	Sparse	Dense	Grid
INCURE (I)	93.6	88.7	97
OMNI (O)	85.7	74.3	89.4
Gain	**9.2% (I)**	**19.3% (I)**	**8.5% (I)**

End-to-end packet delivery delay is affected by a number of factors, such as neighbor density, path discovery delays and path length, overhearing, collisions, retransmission attempts, queuing delays, etc. Since directional networks allow for sectorized operation, the path quality can be improved, for example by reducing retransmissions, overhearing and increasing the nodes' access to the wireless medium. Good path quality can decrease packet delivery delays considerably. In terms of average end-to-end packet delivery delay (Table 9), INCURE grid network outperforms the equivalent OMNI case. Both networks have the same node density on the grid topology. INCURE grid features an average delay of 87 milliseconds whereas OMNI grid yields an average delay of 247 milliseconds (around 182% more). INCURE routing on the grid topology converges easier than the OMNI grid network and also reduces retransmissions around 61% when compared to the OMNI case. Both of the networks present their lowest packet delivery delay on the random dense topology. The lower delay in

the dense topology is achieved as the higher node density allows nodes to have more options for next-hop routing and therefore establish shorter paths to destination. INCURE random dense case features an average delay of 51 milliseconds whereas OMNI yields an average delay of 33 milliseconds (around 35% less). INCURE has a lower node density than OMNI and establishes routing over longer paths, thus the higher packet delivery delay. The same observation applies on the random sparse topologies as INCURE achieves a lower node density than OMNI. INCURE random sparse has a 107 milliseconds delay where OMNI has 58 milliseconds delay. OMNI presents the greatest delay on the grid topology while INCURE case on the random sparse topology. The low neighbor density on the grid and the fixed communication grid pattern make it harder to discover and establish the route paths in the OMNI case when compared to the random topologies. INCURE presents its highest packet delivery delay on the random sparse topology as it is harder to discover and establish the route paths when compared to the other topologies.

Table 9: LOS Normal network conditions – Packet delivery delay

Packet delivery delay (ms)	Topologies		
	Sparse	Dense	Grid
INCURE (I)	107.1	51.2	87.3
OMNI (O)	57.6	33.1	246.8
Gain	**46.2% (O)**	**35.3% (O)**	**64.6% (I)**

Furthermore, since INCURE reduces packet retransmissions and overhearing, it presents a better performance in terms of energy consumption in comparison to the OMNI case. As Table 10 presents, INCURE decreases the energy consumption about 60%, 62% and 66% in random sparse, random dense and grid sparse topologies respectively when compared to the OMNI case. INCURE grid sparse presents the lowest energy consumption in comparison to the INCURE random sparse and dense networks. This occurs as the grid topology has a lower neighbor density and therefore communication and overhearing from the neighbor nodes is much less, yielding less energy consumption than the other topologies.

Table 10: LOS Normal network conditions – Energy consumption

Energy consumption (mJ)	Topologies		
	Sparse	Dense	Grid
INCURE (I)	120.4	121.4	101.9
OMNI (O)	297.7	317.2	302
Gain	**59.5% (I)**	**61.7% (I)**	**66.2% (I)**

5.3.1.2 Static attack strategy

This section evaluates the case where malicious nodes execute a static attack strategy as discussed in section 5.2.1 in order to prohibit the network from propagating observations to the control center. A grid topology is considered to facilitate analysis of observations. First the case where the malicious nodes that participate on active route paths and deploy the selective forwarding attack is considered. INCURE and OMNI networks deploy typical recovery actions as a countermeasure to the selective forwarding attack; they blacklist active malicious nodes, they stop receiving/forwarding packets from/to malicious nodes and they update the affected route paths. Moreover, another case is considered; the case where a DoS attack is deployed by malicious nodes as part of their static attack strategy. In order to recover from the attack, INCURE nodes manage their antennas's operation towards the malicious nodes as specified in section 3.7 while OMNI nodes deploy a low duty cycle as discussed in section 2.2.1.3.

5.3.1.2.1 Selective forwarding attack and recovery

The success of the selective forwarding attack depends on the location of the malicious nodes towards the active packet flow, the number of malicious nodes and the density of the network. Malicious nodes must be located in one of the active route paths in order to successfully launch the attack and drop data packets.

In terms of the number of compromised nodes (Table 11, Figure 29 – page 237), both OMNI and INCURE grid demonstrate similar results. As malicious nodes increase in the network and participate in more active routing paths, they can compromise more sensor nodes from communicating and prohibit them from successfully forwarding packets to the sink. The number of compromised nodes is low as the selective forward attack is not intensive as other attacks, i.e. DoS, affecting only the communication between a single pair of nodes, the malicious node and the associated downstream node participating on an active route. Effectively, all the nodes along the affected path could be considered as compromised, since they could not reach the sink through the utilized path.

Table 11: LOS selective forwarding attack – Compromised nodes (%)

Compromised nodes (%)		Topology (network size =100 nodes)
	malicious nodes	Grid
INCURE (I)	5%	3.3%
	10%	4%
OMNI (O)	5%	2.9%
	10%	3.9%
Gain	**5%**	**0.4% (O)**
	10%	**0.1% (O)**

Packet delivery (Table 12, Figure 30 – page 238) is also affected by the selective forward attack. In the grid topology, the number of malicious nodes that participate in active paths at both OMNI and INCURE cases is equivalent, thus packet delivery is similarly decreased. As malicious nodes increase in the network they have more chances to be selected as forwarding points and therefore successfully launch the selective forward attack, reducing the network's packet delivery capability even greater. Overall, the INCURE network retains a higher packet delivery compared to the OMNI case.

Table 12: LOS selective forwarding attack – Packet delivery increase/decrease % from LOS normal network conditions (R) scenario

Packet delivery decrease %		Topology		
		Grid		
	malicious nodes	R (%)	S (%)	I/D
INCURE (I)	5%	97	50.8	-47.6%
	10%		39.6	-59.1%
OMNI (O)	5%	89.4	48.2	-46.1%
	10%		38.4	-57%
Gain	**5%**		**5.4 % (I)**	
	10%		**3.1% (I)**	

In terms of the energy consumption, energy (Table 13, Figure 31 – page 238) is reduced in both INCURE and OMNI cases. This is due to the fact that the packets that are dropped by the malicious nodes result in less packet forwarding in the network, less overhearing, less packet collisions and retransmissions. Therefore, sensor nodes can save energy. As compromised nodes increase, energy consumption is reduced even more. INCURE network shows a reduction of 32% from its normal energy consumption and OMNI of 31% in the grid topology in the case of 5% malicious nodes. When considering 10% malicious nodes, INCURE drops its energy consumption down by 42% while OMNI drops it by 40%. Overall, INCURE presents about 67% less energy when compared to the OMNI case.

Table 13: LOS selective forwarding attack – Energy consumption increase/decrease % from LOS normal network conditions (R) scenario

Energy consumption decrease %		Topology		
		Grid		
	malicious nodes	R (mJ)	S (mJ)	I/D
INCURE (I)	5%	101.9	69.4	-31.8%
	10%		59.6	-41.5%
OMNI (O)	5%	302	207.8	-31.1%
	10%		179.8	-40.4%
Gain	**5%**		**66.6% (I)**	
	10%		**66.8% (I)**	

The average end-to-end packet delivery delay (Table 14, Figure 32 – page 238) is affected by the packets successfully delivered to the sink node. When the selective forward attack is launched, a large amount of data packets are not delivered to the sink and therefore are not considered for the packet delay calculations as discussed in section 4.1.3.1.10. The packet delivery delay in the case of the selective forwarding attack is greatly affected by the path quality over which the remaining packets are routed. In the grid topology, OMNI demonstrates a significant delay of 428 milliseconds when considering 10% malicious nodes. This occurs as the packets that are successfully delivered utilize long path routes and experience more collisions and retransmissions, thus increasing the delay. INCURE presents a lower delay, 83 milliseconds, as there is less interference, packet drops and retransmissions than the OMNI case.

Table 14: LOS selective forwarding attack – Packet delivery delay increase/decrease % from LOS normal network conditions (R) scenario

Packet delivery delay increase/decrease %		Topology		
		Grid		
	malicious nodes	R (ms)	S (ms)	I/D
INCURE (I)	5%	87.3	73.5	-15.8%
	10%		83	-4.9%
OMNI (O)	5%	246.8	305.3	+23.7%
	10%		427.9	+73.3%
Gain	**5%**		**76% (I)**	
	10%		**80.6 % (I)**	

As soon as the attack is acknowledged, both networks apply typical intrusion recovery countermeasures, blacklisting and excluding the detected malicious nodes from active route paths. Inactive malicious nodes continue to be assumed as legitimate nodes. The recovery measures are effective in both networks and when applied, previously compromised nodes are no longer affected (Figure 29 – page 237). Moreover, the recovery actions themselves do not compromise any nodes either.

Packet delivery (Table 15, Figure 30 – page 238) is successfully restored in both INCURE and OMNI networks as malicious nodes are removed from active route paths. INCURE restores 81% and 78% packet delivery when considering 5% and 10% malicious nodes respectively on the grid topology. OMNI recovers 72% and 68% packet delivery for the equivalent scenarios. As the networks address more active malicious nodes they demonstrate a higher ability to increase their packet delivery. The proposed protocol maintains a higher overall packet delivery (12% - 15%) when compared to the equivalent OMNI scenarios. The INCURE network appears to be more effective in updating to new active paths and therefore presents an enhanced packet delivery capability. Nonetheless, both networks can effectively address the selective forwarding attack with the INCURE network outperforming the OMNI case.

Table 15: LOS selective forwarding recovery – Packet delivery increase/decrease % from LOS selective forwarding attack (R) scenario

Packet delivery increase %		Topology		
		Grid		
	malicious nodes	R (%)	S (%)	I/D
INCURE (I)	5%	50.8	80.9	+59.2%
	10%	39.6	78	+97%
OMNI (O)	5%	48.2	72.1	+49.5%
	10%	38.4	67.9	+76.8%
Gain	**5%**		**12.2% (I)**	
	10%		**14.8% (I)**	

In terms of average end-to-end packet delivery delay (Table 16, Figure 32 – page 238) both networks show increased packet delivery delay while updating to new route paths. OMNI grid topology increases packet delivery delay by 53% and 31% when considering 5% and 10% malicious nodes in comparison to the OMNI reference scenario. INCURE grid case increases packet delivery delay by 15% and 47% when considering 5% and 10% malicious nodes in comparison to its equivalent reference scenario. The route maintenance process is triggered more times as more active route paths are compromised due to the selective

forwarding attack. This means that new route paths need to be established in order to avoid the malicious nodes, and therefore increase the packet delivery delay. The INCURE grid outperforms the equivalent OMNI scenario in terms of average packet delivery delay. The proposed countermeasure can reduce delay up to 73% when compared to the OMNI grid network.

Table 16: LOS selective forwarding recovery – Packet delivery delay increase/decrease % from LOS normal network conditions (R) scenario

Packet delivery delay increase %		Topology		
		Grid		
	malicious nodes	R (ms)	S (ms)	I/D
INCURE (I)	5%	87.3	100.2	+14.7%
	10%		128.4	+47%
OMNI (O)	5%	246.8	377.1	+52.7%
	10%		324.3	+31.4%
Gain	**5%**		**73.4% (I)**	
	10%		**60.4% (I)**	

As packet delivery increases due to the recovery actions, so does the energy consumption (Table 17, Figure 31 – page 238). INCURE increases its energy consumption by 43% and 78% when considering 5% and 10% malicious nodes. For the equivalent scenarios, OMNI presents a lower energy consumption increase percentage (36% and 40%). The higher increase percentage at the INCURE case happens due to higher network communication that occurs as it recovers 12% and 15% more packet delivery than OMNI. Overall, INCURE performs better than the OMNI, with up to 65% less energy consumption.

Table 17: LOS selective forwarding recovery – Energy consumption increase/decrease % from LOS selective forwarding attack (R) scenario

Energy consumption increase %		Topology		
		Grid		
	malicious nodes	R (mJ)	S (mJ)	I/D
INCURE (I)	5%	69.4	99.5	+43.3

	10%	59.6	106.3	+78.3
OMNI (O)	5%	207.8	281.7	+35.5
	10%	179.8	251.8	+40
Gain	**5%**		**64.6 (I)**	
	10%		**57.7 (I)**	

5.3.1.2.1.1 Concluding remarks

Both networks are able to address the selective forwarding attack successfully and restore the network's performance (Table 18) by utilizing typical recovery actions. Although the nodes' availability that has been compromised by the selective forwarding attack is restored by both networks, INCURE outperforms OMNI in terms of packet delivery, energy consumption and packet delivery delay. The typical measure of blacklisting and rerouting to exclude malicious nodes from active route paths leads to an increased communication. In the OMNI case the increased communication leads to higher interference, packet loss and retransmissions, than the INCURE case that updates to new route paths with less effort in terms of network communication. Thus, OMNI restores a lower network performance when compared to the INCURE. A visual analysis of INCURE's gain over OMNI when considering 10% malicious nodes is presented in Figure 16.

Table 18: LOS selective forwarding attack recovery – Overall gain of INCURE versus OMNI

Gain of INCURE over OMNI		Topology	
	malicious nodes	Grid	Comments
Compromised nodes due to recovery	5%	0%	All compromised nodes are recovered by INCURE and OMNI recovery
	10%	0%	
Packet delivery	5%	12.2% (I)	More % of packet delivery than OMNI
	10%	14.8% (I)	
Energy consumption	5%	64.6% (I)	Less % of energy consumption than OMNI
	10%	57.7% (I)	
Packet delivery delay	5%	73.4% (I)	Less % of packet delivery delay than OMNI
	10%	60.4% (I)	

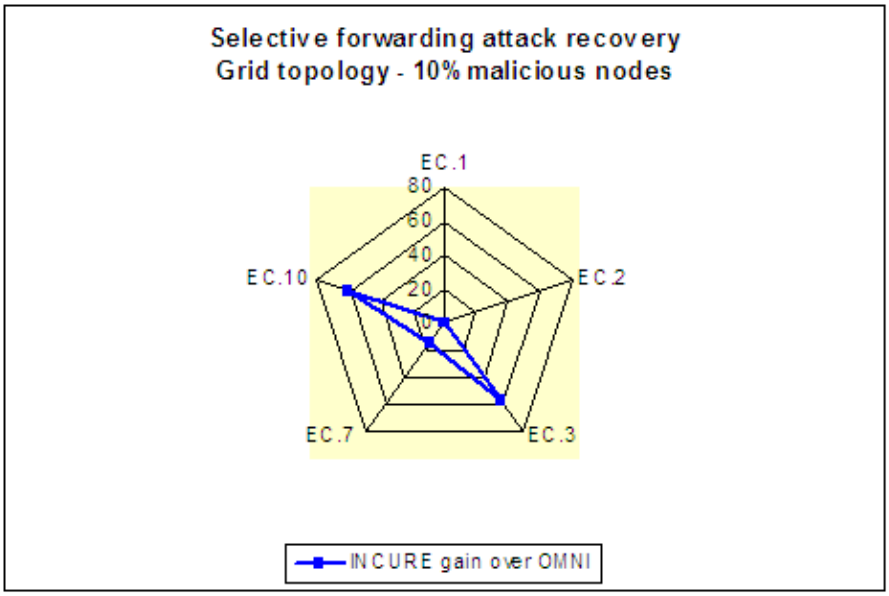

Figure 16: Static attack strategy – selective forwarding attack recovery INCURE gain

5.3.1.2.2 DoS attack and recovery

A continuous DoS attack is executed where malicious nodes persistently send packets with the aim of forcing nodes to increased energy consumption, blocking the network communication and prohibiting nodes from forwarding their packets. As it can be observed, as the number of malicious nodes increases, so does the number of compromised nodes (Table 19, Figure 29 – page 237). The DoS attack compromises a significantly larger number of nodes in comparison to the selective forward attack as a malicious node can affect neighbor nodes in a more brute way. The malicious nodes compromise a similar amount of nodes (about 18% and 36% when considering 5% and 10% malicious nodes) at both INCURE and OMNI networks as they establish communication with the same set of neighbouring nodes.

Table 19: LOS DoS attack – Compromised nodes (%) due to DoS attack

Compromised nodes (%)		Topology (network size =100 nodes)
	malicious nodes	Grid
INCURE (I)	5%	18%
	10%	35.4%
OMNI (O)	5%	18.7%

	10%	36.7%
Gain	**5%**	**0.7% (I)**
	10%	**1.3% (I)**

As the nodes' operation is affected from the DoS attack, the network's performance is degraded for both networks. The packet delivery capability of nodes decreases (Table 20, Figure 30 – page 238) for both networks since there are malicious nodes that are located near nodes on active route paths, thus they can affect their operation. Both networks decrease their packet delivery with OMNI presenting a higher decrease percentage, about 30% and 41% when considering 5% and 10% malicious nodes. Overall, INCURE presents about 12% more packet delivery than OMNI as it decreases interference, packet drops and retransmissions.

Table 20: LOS DoS attack – Packet delivery increase/decrease % from LOS normal network conditions (R) scenario

Packet delivery decrease %		Topology		
		Grid		
	malicious nodes	R (%)	S (%)	I/D
INCURE (I)	5%	97	69.7	-28.1%
	10%		58.9	-39.2%
OMNI (O)	5%	89.4	63	-30%
	10%		52.6	-41.1%
Gain	**5%**		**10.6% (I)**	
	10%		**12% (I)**	

The DoS also forces the nodes to extra energy consumption (Table 21, Figure 31 – page 238), affecting the network's survivability. INCURE appears to have a higher energy consumption increase percentage than OMNI as it achieves more packet delivery (about 12%), thus more packets are forwarded by nodes, leading to an increased network communication. Moreover, in INCURE there are more malicious nodes nearby active route paths causing more packet drops and retransmissions than in the OMNI case, contributing further to INCURE nodes' energy consumption. Overall INCURE presents much less energy consumption than OMNI (48% and 38% when considering 5% and 10% malicious nodes).

Table 21: LOS DoS attack – Energy consumption increase/decrease % from LOS normal network conditions (R) scenario

Energy consumption increase %		Topology		
		Grid		
	malicious nodes	R (mJ)	S (mJ)	I/D
INCURE (I)	5%	101.9	315.4	+209.5% [1]
	10%		513.7	+404.1% [1]
OMNI (O)	5%	302	606.3	+100.7%
	10%		830.7	+175%
Gain	**5%**		**47.9% (I)**	
	10%		**38.1% (I)**	
Note	[1]	Achieves more packet delivery than OMNI		

In terms of packet delivery delay (Table 22, Figure 32 – page 238), both networks increase the packet delivery delay as the malicious nodes forces the network to packet drops and packet retransmissions. Overall, INCURE presents significantly less delay than OMNI. When considering 5% and 10% malicious nodes, INCURE delivers packets with an average end-to-end delay of 181 and 110 milliseconds respectively. OMNI presents a delay of 399 and 386 milliseconds for the equivalent scenarios.

Table 22: LOS DoS attack – Packet delivery delay increase/decrease % from LOS normal network conditions (R) scenario

Packet delivery delay increase %		Topology		
		Grid		
	malicious nodes	R (ms)	S (ms)	I/D
INCURE (I)	5%	87.3	180.8	+107.1%
	10%		110.1	+26.1%
OMNI (O)	5%	246.8	399.4	+61.8%
	10%		386.3	+56.5%
Gain	**5%**		**54.7% (I)**	
	10%		**71.4% (I)**	

As soon as the DoS attack is detected, nodes apply their recovery measures to address the attack. INCURE nodes deactivate the antennas towards the adversary while OMNI nodes apply a low duty cycle. These measures affect the network's performance in different ways. In terms of packet delivery (Table 23, Figure 30 – page 238), INCURE recovers the network's packet delivery capability while OMNI recovery cannot as the low duty cycle affects the availability of nodes. INCURE increases its packet delivery by 15% and 27% when compared to the DoS attack scenario while OMNI decreases it by 8% and 16% and considering 5% and 10% malicious nodes respectively. Overall, INCURE achieves 38% and 69% more packet delivery than OMNI case in the presence of 5% and 10% malicious nodes.

Table 23: LOS DoS recovery – Packet delivery increase/decrease % from LOS DoS attack (R) scenario

Packet delivery increase/decrease %		Topology		
		Grid		
	malicious nodes	R (%)	S (%)	I/D
INCURE (I)	5%	69.7	80.2	+15%
	10%	58.9	75	+27.3%
OMNI (O)	5%	63	58.1	-7.7%
	10%	52.6	44.4	-15.5%
Gain	**5%**		**38% (I)**	
	10%		**68.9% (I)**	

As mentioned previously, the low duty cycle recovery measure that is applied by OMNI nodes affects the availability (Table 24, Figure 29 – page 237) of nodes considerably, up to 20% and 41% when considering 5% and 10% malicious nodes respectively. INCURE does not yield any tradeoff in terms of nodes' availability when recovery is applied.

Table 24: LOS DoS recovery – Compromised nodes (%) due to recovery from LOS DoS attack (R) scenario

Compromised nodes (%)		Topology (network size =100 nodes)
	malicious nodes	Grid

INCURE (I)	5%	0%
	10%	0%
OMNI (O)	5%	20.1%
	10%	40.9%
Gain	**5%**	**20.1% (I)**
	10%	**40.9% (I)**

Concerning the network's survivability, both networks appear to reduce the energy consumption (Table 25, Figure 31) that occurs due to the DoS attack. INCURE demonstrates a higher ability to decrease its energy consumption when compared to the DoS attack scenario, up to 61% and 74% less consumption in the case of 5% and 10% malicious nodes. OMNI presents a 42% and 38% energy consumption decrease percentage for the equivalent scenarios. The lower decrease percentage at OMNI occurs as nodes experience more interference, packet collisions and retransmissions, thus there is more network communication than in the INCURE case. INCURE achieves 65% and 74% less energy consumption than OMNI when considering 5% and 10% malicious nodes.

Table 25: LOS DoS recovery – Energy consumption increase/decrease % from LOS DoS attack (R) scenario

Energy consumption decrease %		Topology		
		Grid		
	malicious nodes	R (mJ)	S (mJ)	I/D
INCURE (I)	5%	315.4	122.3	-61.2%
	10%	513.7	131.8	-74.3%
OMNI (O)	5%	606.3	352.6	-41.8%
	10%	830.7	512.1	-38.3%
Gain	**5%**		**65.3% (I)**	
	10%		**74.2% (I)**	

In terms of packet delivery delay (Table 26, Figure 32 – page 238), OMNI demonstrates an increase delay percentage of 8% and 11% as nodes that are turned unavailable due to the low duty cycle recovery measure cannot participate in the routing process, thus route paths need to be updated accordingly in order to reroute traffic through the updated routes. INCURE

appears to decrease its packet delivery delay in the case of 5% malicious nodes as nodes apply recovery and prohibit malicious nodes that are near active route paths to affect packet delivery. In the case of 10% malicious nodes, INCURE increases its packet delivery delay by 13% as it recovers a higher increase percentage of packet delivery and also there are more malicious nodes located on active route paths, thus nodes have to update to new route paths incurring extra delay.

Table 26: LOS DoS recovery – Packet delivery delay increase/decrease % from LOS DoS attack (R) scenario

Packet delivery delay increase/decrease %		Topology		
		Grid		
	malicious nodes	R (ms)	S (ms)	I/D
INCURE (I)	5%	180.8	117.3	-35.1%
	10%	110.1	124.5	+13%
OMNI (O)	5%	399.4	432.2	+8.2%
	10%	386.3	429.2	+11.1%
Gain	**5%**		**72.8% (I)**	
	10%		**71% (I)**	

5.3.1.2.2.1 Concluding remarks

Both INCURE and OMNI are able to address the DoS attack. However, OMNI yields a significant tradeoff (Table 27) in terms of compromising node's availability in order to decrease the energy consumption that occurs due to the attack. Moreover, although OMNI can recover the survivability of the network, it affects nodes' packet delivery capability considerably. INCURE recovers nodes' availability, survivability and packet delivery without any significant tradeoff, achieving a considerably improvement of performance over OMNI (Figure 17).

Table 27: LOS DoS attack recovery – Overall gain of INCURE versus OMNI

Gain of INCURE over OMNI		Topology	
	malicious nodes	Grid	Comments
Compromised nodes	5%	20.1% (I)	Less % of compromised nodes due to recovery than OMNI
	10%	40.9% (I)	
Packet delivery	5%	38% (I)	More % of packet delivery than OMNI
	10%	68.9% (I)	
Energy consumption	5%	65.3% (I)	Less % of energy consumption than OMNI
	10%	74.2% (I)	
Packet delivery delay	5%	72.8% (I)	Less % of packet delivery delay than OMNI
	10%	71% (I)	

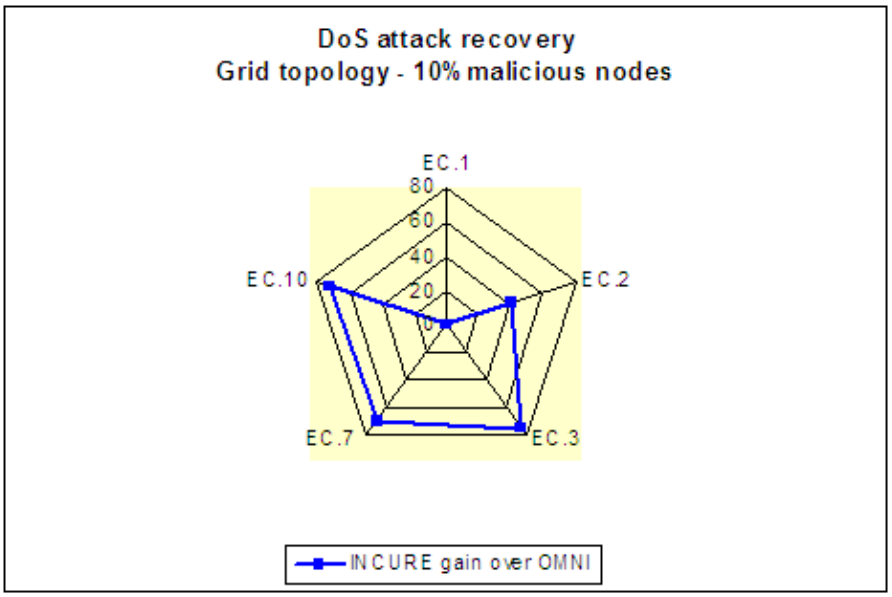

Figure 17: Static attack strategy – DoS attack recovery INCURE gain

5.3.1.3 INCURE setup against a static attack strategy that turns into persistent/reactive

This section investigates if the INCURE network should manage the antennas' deactivation operation (over the case where only the typical INCURE recovery actions of blacklisting and rerouting are utilized as discussed in section 5.3.1.2.1) in order to recover from the selective forwarding attack while considering persistent/reactive malicious nodes that act upon overhearing communication.

With regards to reactive adversaries, an adversary of this type is assumed to move to another action, if for example, it has not received any traffic for a specified time interval. Malicious nodes enter eavesdropping mode with the objective of tapping legitimate communication and then use overheard packets to launch other attacks, i.e. replay attack, DoS, traffic analysis and so on. If a node can be tapped, it is considered as compromised. Eavesdropping is in general an attack hard to detect if previously the adversary has not made any illegal activity that could be detected. In this scenario it is assumed that the selective forwarding attack was preceded, active malicious nodes were detected and compromised nodes (due to the selective forwarding attack) were recovered before the eavesdropped attack was executed.

In the case of a static intrusion strategy, INCURE recovers from the selective forwarding attack (section 5.3.1.2.1) by utilizing the typical recovery actions of blacklisting malicious nodes, updating the route paths and rerouting traffic over the new active paths, turning the selective forwarding attack ineffective. As it was observed in the case of the DoS attack (section 5.3.1.2.2), INCURE nodes effectively recover from the DoS attack by managing the deactivation of antennas that communicate with the malicious nodes in order to exclude them from the communication and minimize the attack outcome. With the antenna deactivation action nodes aim to prohibit the reception of malicious signals and thus continue their operation, supporting decision making. In the case of reactive malicious nodes, if the management of antenna deactivation is applied further to the typical INCURE recovery actions of blacklisting and rerouting, when recovering from the selective forwarding attack, it is expected that it will minimize the possibility of triggering reactive adversaries when they overhear communication. The typical measure of updating the route paths, in order to exclude the malicious nodes that are included in the active route paths, leads to increased network communication, giving more opportunities to malicious nodes to eavesdrop and trigger a DoS attack. By managing the deactivation of antennas towards detected malicious nodes, the idea is to make legitimate nodes stop forwarding packets in the direction of the adversary,

minimizing eavesdropping, and also increase the network's communication resilience in the case where malicious nodes decide to execute a DoS attack, whether they can overhear or not.

This section evaluates if the measure of antenna deactivation when a selective forwarding malicious node is detected is beneficiary over the case where only typical INCURE recovery actions are utilized, in order to address a reactive adversary.

When active selective forwarding malicious nodes are detected, the active route paths need to be updated to reroute traffic and avoid having malicious nodes participate on active route paths. Table 28 presents the comparison of the results when the INCURE network manages the antennas's operation versus the case where only the typical recovery actions are utilized to address the attack. Both cases can restore the network's packet delivery capability. In the case of 5% malicious nodes, both cases recover a similar packet delivery fraction. The case where only typical recovery actions are utilized presents slightly more packet delivery (0.7%) than the case of applying antenna deactivation. This occurs as the network communication is rerouted over route paths that experience less packet collisions and retransmissions, thus the utilization of typical actions present less packet delivery delay (37%) and energy consumption (7.6%). In the presence of 10% malicious nodes, the case where nodes manage the antennas' deactivation operation updates to new route paths on which previously inactive malicious nodes have been selected to participate on the updated paths and have become active selective forwarding nodes, meaning that some portion of the communication is dropped by the malicious nodes. Once the new active malicious nodes are detected, the network continues applying the recovery measures and updating again its active paths to reroute network communication in order to address the selective forwarding attack. Due to this, there is more network communication traversing the network when compared to the case where only typical INCURE recovery actions are applied, increasing collisions, retransmissions and delay. Thus, the case of utilizing only typical intrusion recovery actions

appears to have recovered a higher packet delivery fraction, with less delivery delays but higher energy consumption as more packets are delivered to the destination.

Table 28: LOS selective forwarding recovery – Overall performance % of INCURE(MoAO - management of antennas' operation) versus typical INCURE (T) from LOS selective forwarding attack scenario

Overall evaluation			Topology		
			Grid		
	INCURE	Malicious nodes	R	S	**I/D**
Compromised nodes (%) [1] due to recovery	TYPICAL (T)	5%		0%	**0%**
		10%		0%	**0%**
	MoAO	5%		0%	**0%**
		10%		0%	**0%**
Gain		5%		0%	
		10%		0%	
Packet delivery (%)	TYPICAL (T)	5%	50.8	80.9	**+59.2% [2]**
		10%	39.6	78	**+96.9% [3]**
	MoAO	5%	50.8	80.3	**+58%**
		10%	39.6	73.1	**+84.5%**
Gain		5%		0.7% (T)	
		10%		6.7% (T)	
Energy consumption (mJ)	TYPICAL (T)	5%	69.4	99.5	**+43.3%**
		10%	59.6	106.3	**+78.3%**
	MoAO	5%	69.4	107.8	**+55.3%**

		10%	59.6	104.8	**+75.8%**
Gain		5%		7.6% (T)	
		10%		1.4% (MoAO)	
Packet delay (ms)	TYPICAL (T)	5%	87.3	100.2	**+14.7%**
		10%	87.3	128.4	**+47%**
	MoAO	5%	87.3	158.8	**+81.9%**
		10%	87.3	171.9	**+96.9%**
Gain		5%		36.9% (T)	
		10%		25.3% (T)	
Note	[1]	Compromised nodes due to the attack are recovered by both cases. There are no compromised nodes from the recovery actions.			
	[2]	Reroutes through new paths that experience less collisions and retransmissions			
	[3]	Less malicious nodes become active, executing the selective forwarding attack			

After recovery is applied to address the selective forwarding attack, a reactive malicious node enters an overhearing mode and executes a DoS attack when it can eavesdrop on the network communication. As Table 29 presents, in the case where nodes apply the antenna deactivation action, malicious nodes eavesdrop on 2% and 13% less nodes when compared to the case where nodes apply only the typical INCURE recovery actions. This occurs as nodes that deactivate antennas stop forwarding packets towards the direction of the malicious nodes, thus minimize their eavesdrop capability. Eavesdropped packets are decreased by 66% and 72% when compared to the case where nodes apply the typical recovery actions. By minimizing eavesdropping, a reactive malicious node is most likely to be prohibited or stalled from executing a new attack, i.e. DoS, based on overhearing. In the case where only the typical INCURE recovery actions are applied, more malicious nodes eavesdrop on the communication and are triggered to launch the DoS attack, decreasing the packet delivery capability of the network considerably (up to 22% when considering 10% malicious nodes). If the antenna deactivation action is applied, a fraction of 2% and 24% more packet delivery is

achieved when considering 5% and 10% malicious nodes and compared to the case where typical actions are applied. Due to the fact that the management of antenna deactivation prohibits malicious signals to reach sensor nodes, the energy consumption is much less (33% and 53% with 5% and 10% malicious nodes respectively) than in the case where typical recovery actions are applied. The packet delivery delay appears to decrease at both cases as fewer packets are considered in the calculations due to the DoS attack, and which are routed over shorter paths and experience less retransmissions.

Table 29: LOS DoS attack per eavesdropping case – Overall gain of INCURE(MoAO - management of antennas' operation) versus typical INCURE (T) from LOS selective forwarding recovery scenario

Overall evaluation			Topology		
			Grid		
	INCURE	Malicious nodes	R	S	**I/D**
Compromised nodes (%) due to eavesdropping	TYPICAL (T)	5%		6.1%	**6.1%**
		10%		21.6%	**21.6%**
	MoAO	5%		4%	**4%**
		10%		9.1%	**9.1%**
Gain		5%		2.1% (MoAO)	
		10%		12.5% (MoAO)	
Eavesdropped packets (#)	TYPICAL (T)	5%		268	
		10%		1204	
	MoAO	5%		92	
		10%		342	
Gain		5%		65.6% (MoAO)	

		10%		71.5% (MoAO)	
Packet delivery (%)	TYPICAL (T)	5%	80.9	78.7	**-2.7%**
		10%	78	61.1	**-21.6%**
	MoAO	5%	80.3	80.4	**+0.1%**
		10%	73.1	75.7	**+3.5%**
Gain		5%		2.1% (MoAO)	
		10%		23.8% (MoAO)	
Energy consumption (mJ)	TYPICAL (T)	5%	99.5	164.4	**+65.2%**
		10%	106.3	335.3	**+215.4%**
	MoAO	5%	107.8	109.1	**+1.2%**
		10%	104.8	156.5	**+49.3%**
Gain		5%		33.6% (MoAO)	
		10%		53.3% (MoAO)	
Packet delay (ms)	TYPICAL (T)	5%	100.2	95.9	**-4.3%**
		10%	128.4	83.7	**-34.8%**
	MoAO	5%	158.8	151.1	**-4.8%**
		10%	171.9	131	**-23.7%**
Gain		5%		36.5% (T)	
		10%		36.1% (T)	

5.3.1.3.1 Concluding remarks

The typical measures of blacklisting and rerouting in the INCURE network, without applying appropriate management of the operation of antennas, is effective if malicious nodes launch the selective forwarding attack without continuing their intrusion attempts after the attack is addressed by the WSN. This means that a malicious node executes the selective

forwarding attack once and does not deploy any other malicious activities when the network recovers from the attack. In the case of such a simple threat model, where malicious nodes do not persist with their attacks, the typical measures of blacklisting and rerouting can be considered adequate to address the selective forwarding attack. However, as discussed in section 3.6.2, the adversaries that have dedicated objectives to compromise the network's operation, in order to prohibit observation and identification of critical events that will allow decision making, persist with their intrusion strategy. Therefore, to achieve their malicious objectives they deploy activities beyond a simple threat model. In this case, the measures of blacklisting and rerouting only cannot aid the network to address a persistent/reactive malicious node. When sensor nodes manage the operation of their antennas as discussed in section 3.7, they can address persistent/reactive adversaries more effectively when compared only to typical reocvery measures, decreasing the capability of malicious nodes to eavesdrop and execute new attacks, thus, achieving better network performance. In this thesis, we are concerned about adversaries that deploy a persistent attack strategy. Therefore, the rest of the analysis considers that the INCURE nodes apply appropriate management of the operation of antennas to address the security attacks.

5.3.1.4 Persistent, adaptive or reactive attack strategy

Adversaries that have dedicated objectives to prohibit or stall observation and identification of critical events and affect decision making [20] can persist with their attack strategy to continue compromising the WSN, even if the network has restored its operation from previous compromisation efforts. In the case where the network is deploying a static intrusion recovery approach, it may not be adequate to address persistent adversaries. It is essential to consider persistent/adaptive attack strategies, not only static, in order to design recovery solutions that are robust in the case where malicious nodes change their attack dynamics. This section evaluates whether INCURE countermeasure and OMNI typical

intrusion recovery countermeasures can address the case where a static attack strategy turns into persistent, adaptive or reactive attack strategy.

5.3.1.4.1 Selective forwarding attack and recovery

In the case of a passive attack such as the selective forward attack, the network's performance is affected in all scenarios. As discussed in section 5.3.1.2.1, the success of this attack depends upon many factors such as the location of the malicious nodes towards the active packet flow, the number of malicious nodes and the density of the network. Malicious nodes must be located in one of the active route paths in order to successfully launch the attack and drop data packets.

In terms of the number of compromised nodes (Table 30), both OMNI and INCURE grid and random networks demonstrate similar results. As the number of malicious nodes that participates in active route paths increases, malicious nodes can prohibit more nodes from routing their data towards the sink. However, as the network's density is increased, malicious nodes have fewer chances to be selected as forwarding points and therefore they compromise fewer nodes when compared to the sparse topologies. Also, it is observed that communication on the grid is evenly distributed throughout the network when compared to the random sparse topology, increasing the malicious nodes chances to be located on active route paths and compromise communication. In the case where 10% of nodes turn malicious they can compromise at most 4% of the nodes (one-hop nodes downstream the malicious node). As discussed in section 5.3.1.2.1, the selective forwarding attack yields a low percentage of compromised nodes in comparison to attacks such as a DoS. This occurs as the selective forwarding attack affects only the communication between the malicious node and the downstream node that forwards data through the malicious node.

Table 30: LOS Selective forwarding attack – Compromised nodes (%)

Compromised nodes %		Topology		
		Sparse (Figure 33 – page 239)	Dense (Figure 37 – page 240)	Grid (Figure 41 – page 241)
	malicious nodes	I/D	I/D	I/D
INCURE (I)	5% [1]	+2.2%	+0.9%	+3.3%
	10% [1]	+3.1%	+1.9%	+4%
OMNI (O)	5%	+1.8%	+0.8%	+2.9%
	10%	+2.5%	+1.5%	+3.9%
Gain	**5%**	**0.4% (O)**	**0.1% (O)**	**0.4% (O)**
	10%	**0.6% (O)**	**0.4% (O)**	**0.1% (O)**
Note	[1]	In INCURE there are more malicious nodes participating on active route paths		

Packet delivery (Table 31) is also affected by the selective forward attack in different ways. The random sparse INCURE network presents a decrease percentage of 27% and 43% from its normal packet delivery when considering 5% and 10% malicious nodes while the random sparse OMNI network's decrease percentage is 26% and 34%. This is due to the fact that in INCURE more active routing paths are affected by the attack as more malicious nodes participate in active data flows. The same observation applies in the random dense topology, where INCURE packet delivery is reduced by 10% and 29% when considering 5% and 10% malicious nodes respectively. The equivalent OMNI dense scenario shows a reduction percentage of 11% and 20% in the case of 5% and 10% malicious nodes when compared to the OMNI reference scenario. In the grid topology, the number of malicious nodes that participate in active paths at both OMNI and INCURE cases is equivalent, thus packet delivery presents a similar decreased percentage. When the network is sparse, sensor nodes have fewer neighbors to select from as the next hop to the sink. This means that malicious nodes have more chances to participate in one of the active route paths, therefore more paths

can be affected by the attack. As the network gets denser, nodes have more neighbors to choose from and therefore malicious nodes have fewer chances to be selected as forwarding points. Moreover, as malicious nodes increase in the network they have more chances to be selected as forwarding points and therefore successfully launch the selective forward attack, reducing the network's packet delivery capability even greater. Overall, it was found that the INCURE network retains a higher packet delivery compared to the OMNI case.

Table 31: LOS Selective forwarding attack – Packet delivery increase/decrease % from LOS normal network conditions (R) scenario

Packet delivery decrease %		Topology								
		Sparse (Figure 34 – page 239)			Dense (Figure 38 – page 240)			Grid (Figure 42 – page 242)		
	malicious nodes	R (%)	S (%)	I/D	R (%)	S (%)	I/D	R (%)	S (%)	I/D
INCURE (I)	5%	93.6	68	-27.3%	88.7	79.6	-10.2%	97	50.8	-47.6%
	10%		53.8	-42.5%		62.8	-29.2%		39.6	-59.1%
OMNI (O)	5%	85.7	63.1	-26.3%	74.3	65.9	-11.3%	89.4	48.2	-46.1%
	10%		56.9	-33.6%		59.7	-19.6%		38.4	-57%
Gain	**5%**		**7.7% (I)**			**20.7% (I)**			**5.4% (I)**	
	10%		**5.7% (O)**			**5.2% (I)**			**3.1% (O)**	

In terms of the energy consumption, both INCURE and OMNI cases reduce energy consumption (Table 32). The decrease of energy consumption occurs due to the fact that there is less traffic traversing the network as the attack causes packets to be dropped, resulting in less overhearing, less packet collisions and retransmissions. As compromised nodes increase, energy consumption is reduced even more. INCURE network shows a reduction of 22% from its normal energy consumption and OMNI 18% in the random sparse topology in the case of

5% malicious nodes. When considering 10% malicious nodes, INCURE random sparse drops its energy consumption down 30% while OMNI drops it to 25%. This occurs since in INCURE more nodes are compromised and therefore less traffic is forwarded between nodes. In the dense topology, both networks present a minimum energy consumption decrease percentage as malicious nodes participate in fewer active paths and result in blocking less network communication. The grid topology was found to yield the greatest energy consumption decrease percentage in both networks in comparison to the random sparse and dense topologies as there are more compromised nodes, thus, affecting the packet delivery even greater. However, the INCURE setup still maintains a lower overall energy consumption in all cases, with INCURE presenting the least energy consumption on the grid when compared to the OMNI (about 67% less energy).

Table 32: LOS Selective forwarding attack – Energy consumption increase/decrease % from LOS normal network conditions (R) scenario

Energy consumption decrease %		Topology								
		Sparse (Figure 35 – page 239)			Dense (Figure 39 – page 241)			Grid (Figure 43 - page 242)		
	malicious nodes	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D
INCURE (I)	5%	120.4	93.8	-22.1%	121.4	113.8	-6.3%	101.9	69.4	-31.9%
	10%		83.9	-30.3%		103.2	-15%		59.6	-41.5%
OMNI (O)	5%	297.7	243.9	-18.1%	317.2	296.5	-6.5%	302	207.8	-31.1%
	10%		224.6	-24.5%		278	-12.3%		179.8	-40.4%
Gain	**5%**		**61.5% (I)**			**61.6% (I)**			**66.6% (I)**	
	10%		**62.6% (I)**			**62.9% (I)**			**67% (I)**	

The average end-to-end packet delivery delay (Table 33) is affected by the packets successfully delivered to the sink node. As discussed in section 5.3.1.2.1, the selective

forwarding attack causes a large number of packets to be dropped and therefore they are not considered for the packet delay calculations as discussed in section 4.1.3.1.10. Also, it needs to be taken into consideration that the packet delivery delay is greatly affected by the path quality over which the packets are routed. In the grid sparse topology, OMNI demonstrates a significant delay of 428 milliseconds when considering 10% malicious nodes. This occurs as the packets that are successfully delivered utilize long path routes and experience more collisions and retransmissions, thus increasing the delay. The same observation applies for the INCURE case when considering the random sparse topology and 10% malicious nodes, where a delay of 125 milliseconds is presented.

Table 33: LOS Selective forwarding attack – Packet delivery delay increase/decrease % from LOS normal network conditions (R) scenario

Packet delivery delay increase / decrease %		Topology								
		Sparse (Figure 36 – page 240			Dense (Figure 40 – page 241)			Grid (Figure 44 – page 242)		
	malicious nodes	R (ms)	S (ms)	I/D	R (ms)	S (ms)	I/D	R (ms)	S (ms)	I/D
INCURE (I)	5%	107.1	113.4	+5.8%	51.2	52.3	+2.1%	87.3	73.5	-15.8%
	10%		125	+16.7%		58.8	+14.8%		83	-4.9%
OMNI (O)	5%	57.6	63.2	+9.7%	33.1	30.8	-6.9%	246.8	305.3	23.7%
	10%		63.5	+10.2%		30.2	-8.7%		427.9	73.3%
Gain	**5%**		**44.2% (O)**			**41.1% (O)**			**75.9% (I)**	
	10%		**49.2% (O)**			**48.6% (O)**			**80.6% (I)**	

In order to address the selective forwarding attack, each network applies its intrusion recovery measures in order to exclude the detected malicious nodes from active route paths. In

the case where a malicious node is not located on an active path, it is considered as inactive as the attack cannot be executed. Both networks are able to restore the compromised nodes and the applied recovery measures do not affect the availability of any node.

As the INCURE and OMNI networks apply their recovery measures and remove the malicious nodes from active route paths, the packet delivery (Table 34) is successfully restored. INCURE restores up to 85% and up to 79% packet delivery when considering 5% and 10% malicious nodes respectively on the random dense topology. OMNI recovers 70% and 66% packet delivery for the equivalent scenarios. As the networks address more active malicious nodes they show a higher ability to increase their packet delivery. The proposed protocol maintains a higher overall packet delivery (8% - 20%) when compared to the equivalent OMNI scenarios. The INCURE network appears to be more effective in updating to new active paths and therefore presents an enhanced packet delivery capability. Nonetheless, both networks can effectively address the selective forwarding attack with the INCURE network outperforming the OMNI case.

Table 34: LOS Selective forwarding recovery – Packet delivery increase/decrease % from LOS selective forwarding attack (R) scenario

Packet delivery increase %		Topology								
		Sparse (Figure 34 – page 239)			Dense (Figure 38 – page 240)			Grid (Figure 42 – page 242)		
	malicious nodes	R (%)	S (%)	I/D	R (%)	S (%)	I/D	R (%)	S (%)	I/D
INCURE (I)	5%	68	83.3	+22.5%	79.6	84.6	+6.2%	50.8	80.3	+58.1%
	10%	53.8	74	+37.5%	62.8	78.5	+25%	39.6	73.1	+84.6%
OMNI (O)	5%	63.1	77.1	+22.1%	65.9	70.3	+6.6%	48.2	72.1	+49.5%
	10%	56.9	75	+31.8%	59.7	65.9	+10.3%	38.4	67.9	+76.8%
Gain	**5%**		**8.0% (I)**			**20.3% (I)**			**11.3% (I)**	
	10%		**1.4% (O)**			**19.1% (I)**			**7.6% (I)**	

In terms of average end-to-end packet delivery delay (Table 35) the INCURE dense topology shows a similar delay percentage as the equivalent reference results. The active route paths are updated in a timely manner and delay is affected insignificantly. The same observation applies when considering the OMNI dense case. However, both networks increase the packet delivery delay when considering the random sparse topology due to the low node density since more effort is required to update the route paths. OMNI random sparse topology increases packet delivery delay by 26% and 34% when considering 5% and 10% malicious nodes in comparison to the OMNI reference scenario. INCURE random sparse case increases packet delivery delay by 14% and 28% when considering 5% and 10% malicious nodes in comparison to its equivalent reference scenario. OMNI retains a lower overall packet delivery delay than INCURE in the random topologies as it achieves a higher node density that allows it to discover shorter route paths. In the case of the grid network, both networks show a significant increase in the packet delivery delay. The route maintenance process is triggered more times on the grid as more active route paths have been compromised due to the selective forwarding attack and need to be updated in order to avoid using the malicious node for routing. Due to this, the packet delivery delay is increased. Moreover, the fixed node density and the grid communication pattern make the network connectivity to be more sensitive to routing changes. Thus, it is harder for nodes to update the active paths and leads to a much higher number of packet loss and retransmissions. All these, further increase the delay on the packet delivery capabilities of the network. The INCURE grid sparse topology outperforms the equivalent OMNI scenario in terms of average packet delivery delay. The proposed countermeasure can reduce delay up to 58% when compared to the OMNI grid network.

Table 35: LOS Selective forwarding recovery – Packet delivery delay increase/decrease % from LOS normal network conditions (R) scenario

Packet delivery delay increase / decrease %	Topology		
	Sparse (Figure 36 – page 240)	Dense (Figure 40 – page 241)	Grid (Figure 44 – page 242)

	malicious nodes	R (ms)	S (ms)	I/D	R (ms)	S (ms)	I/D	R (ms)	S (ms)	I/D
INCURE (I)	5%	107.1	121.6	+13.5%	51.2	58.2	+13.7%	87.3	158.8	+82% [1]
	10%	107.1	136.8	+27.7%	51.2	54.8	+7%	87.3	171.9	+97% [1]
OMNI (O)	5%	57.6	72.5	+25.8%	33.1	35.2	+6.3%	246.8	377.1	+52.8%
	10%	57.6	76.9	+33.5%	33.1	31.1	-6%	246.8	324.3	+31.4%
Gain	**5%**		**40.4% (O)**			**39.5% (O)**			**57.8% (I)**	
	10%		**43.7% (O)**			**43.2% (O)**			**46.9% (I)**	
Note	[1]	More active route paths are affected by the attack on INCURE grid when compared to OMNI grid case								

As packet delivery increases due to the recovery actions, so does the energy consumption (Table 36). Both INCURE and OMNI grid topology yields the highest energy consumption increase percentage, with INCURE grid presenting (overall) the lowest energy consumption in comparison to the random topologies. The high increase percentage is due to a large number of control packets traversing the network in an effort to discover new route paths. The increased network communication leads to much more overhearing, collisions and retransmissions. The lowest energy consumption increase percentage is observed at the INCURE dense case. The high node density with the combination of the INCURE recovery measures benefits the network as it leads to a lower number of packet retransmissions and control packets, allowing it to converge to new routing paths easier. OMNI case also presents its lowest energy consumption increase percentage at the random dense topology. This is due to the fact that the existence of fewer compromised nodes triggers the recovery and updating of active route paths less often. Overall, the INCURE appears to perform better than the OMNI network, with up to 62% less energy consumption.

Table 36: LOS Selective forwarding recovery – Energy consumption increase/decrease % from LOS selective forwarding attack (R) scenario

Energy consumption increase %		Topology								
		Sparse (Figure 35 – page 239)			Dense (Figure 39 – page 241)			Grid (Figure 43 – page 242)		
	malicious nodes	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D
INCURE (I)	5% [1]	93.8	111.5	+18.8%	113.8	117.3	+3%	69.4	107.8	+55.3%
	10% [1]	83.9	111.9	+33.3%	103.2	115.4	+11.8%	59.6	104.8	+75.8%
OMNI (O)	5%	243.9	272.5	+11.7%	296.5	300	+1.1%	207.8	281.7	+35.5%
	10%	224.6	278.2	+23.8%	278	292.1	+5%	179.8	251.8	+40%
Gain	**5%**		**59.0% (I)**			**61% (I)**			**61.7% (I)**	
	10%		**59.7% (I)**			**60.4% (I)**			**58.3% (I)**	
Note	[1]	INCURE recovers more packet delivery than OMNI								

5.3.1.4.1.1 Concluding remarks

INCURE and OMNI are able to address the selective forwarding attack successfully and restore the network's performance. The restoration level that can be achieved depends on a number of aspects. A higher number of active malicious nodes can affect more nodes, thus, more nodes have to apply recovery countermeasures, increasing the routing overhead and communication. Increased communication can negatively affect the network as it can lead to higher packet loss and retransmissions. Moreover, the quality of the recovered route paths and the node density can affect the networks' performance. A higher density network can aid the sensors to converge to shorter route paths, thus decrease packet delivery delays. Also, malicious nodes have less chances to become active when the node density is higher, thus a dense network is less affected by a selective forwarding attack.

Both networks are able to restore the nodes' availability, with INCURE showcasing an overall higher performance in most of the cases in terms of packet delivery, energy consumption and packet delivery (Table 37). As discussed in section 5.3.1.2.1, the measure of blacklisting and rerouting leads to an increased communication. In the OMNI case the increased communication leads to higher interference, packet loss and retransmissions. INCURE appears to be able to handle the increased communication due to the blacklisting and rerouting, as it can update to new route paths with fewer efforts in terms of network communication and retain a higher network performance when compared to OMNI. Figure 18 presents a visual snapshot of INCURE's gain over OMNI when considering 10% malicious nodes in the grid topology.

Table 37: LOS selective forwarding attack recovery – Overall gain of INCURE versus OMNI

Overall Gain – LOS selective forwarding attack recovery		Topology		
	malicious nodes	Sparse	Dense	Grid
Compromised nodes due to recovery	5%	0%	0%	0%
	10%	0%	0%	0%
Packet delivery	5%	8% (I)	20.3% (I)	11.3% (I)
	10%	1.4% (O)	19.1% (I)	7.6% (I)
Energy consumption	5%	59% (I)	61% (I)	61.7% (I)
	10%	59.7% (I)	60.4% (I)	58.3% (I)
Packet delivery delay	5%	40.4% (O)	39.5% (O)	57.8% (I)
	10%	43.7% (O)	43.2% (O)	46.9% (I)

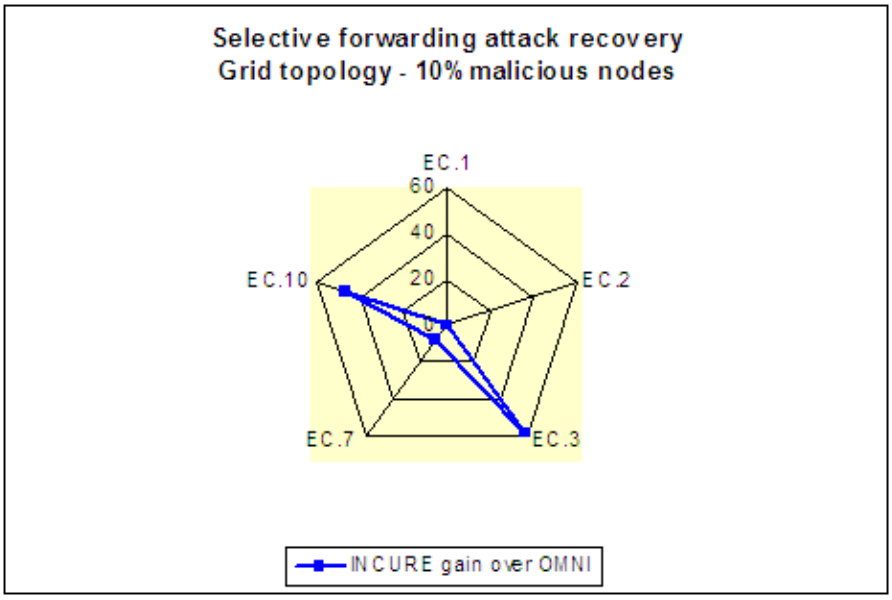

Figure 18: Persistent attack strategy – selective forwarding recovery gain

5.3.1.4.2 Reactive adversary

As it was discussed in section 5.3.1.3, reactive adversaries launch a DoS attack based on an overhearing case. This section considers a scenario where the selective forwarding attack is executed, active malicious nodes are detected and compromised nodes due to the attack are recovered before the eavesdropped attack is executed. The success of the eavesdropping attack under the specified scenario depends on the applicability of the intrusion recovery actions against active malicious nodes. If inactive malicious nodes exist, then the eavesdropping is more effective which justifies the increase of compromised nodes (due to tapping) as malicious nodes increase (Table 38).

As it can be observed, INCURE grid yields the lowest number of compromised nodes (Table 38), 4% and 9% when considering 5% and 10% malicious nodes respectively. OMNI grid increases compromised nodes by 14% and 21% when compared to the INCURE grid topology (18%, 30%). The previously recovered grid communication benefits the INCURE network in isolating malicious nodes effectively and therefore addressing the eavesdrop

attack. The dense topology yields the highest number of compromised nodes at both OMNI and INCURE cases. This occurs due to the high node density that appears in the dense network, thus malicious nodes can overhear communication from more neighbor nodes. INCURE random dense shows 9% and 19% compromised nodes when considering 5% and 10% malicious nodes. OMNI dense presents 22% and 36% more compromised nodes in comparison to the equivalent INCURE scenarios. In the case of random sparse networks, INCURE presents 6% and 15% compromised nodes while OMNI case shows 27% and 48% compromised nodes, when considering 5% and 10% malicious nodes respectively.

Table 38: LOS eavesdropping attack – Compromised nodes % from LOS selective forwarding attack recovery (R) scenario

Compromised nodes %		Topology		
		Sparse (Figure 33 – page 239)	Dense (Figure 37 – page 240)	Grid (Figure 41 – page 241)
	malicious nodes	I/D	I/D	I/D
INCURE (I)	5%	+6.4%	+8.6%	+4%
	10%	+15%	+18.9%	+9.1%
OMNI (O)	5%	+26.8%	+30.5%	+18.2%
	10%	+47.5%	+54.7%	+30%
Gain	**5%**	**20.4% (I)**	**21.9% (I)**	**14.2% (I)**
	10%	**32.5% (I)**	**35.8% (I)**	**20.9% (I)**

By aiding the network to isolate malicious nodes, their eavesdropped capability is considerably decreased, as presented in the INCURE scenario. Eavesdropping is reduced in the INCURE network by 97%, 80% and 83% when considering the grid, dense and sparse cases with 5% malicious nodes and compared to the equivalent OMNI scenarios (Table 39). Although the selective forwarding attack is addressed in the OMNI scenarios by just updating the active paths and avoiding the active malicious nodes, the eavesdropping attack cannot be

effectively addressed. The malicious nodes are not prohibited from eavesdropping on the communication due to the omni-directional nature of transmission. On the other hand, the directional transmission limits the communication at specific regions. Therefore, communication between nodes is established in a more constrained/controlled manner and can prohibit malicious nodes from eavesdropping communication from their respective neighbors.

Table 39: LOS eavesdropping attack – Eavesdropped packets (#) from LOS selective forwarding attack recovery (R) scenario

Eavesdropped packets (#)		Topology		
		Sparse (Figure 45 – page 243)	Dense (Figure 45 – page 243)	Grid (Figure 45– page 243)
	malicious nodes	Number of eavesdropped packets	Number of eavesdropped packets	Number of eavesdropped packets
INCURE (I)	5%	484	427.8	92
	10%	918.2	1192	342
OMNI (O)	5%	2827.1	2129.2	2727
	10%	4496.4	4658.6	4356
Gain	**5%**	**82.8% (I)**	**80% (I)**	**96.6% (I)**
	10%	**79.5% (I)**	**74.4% (I)**	**92.1% (I)**

Minimizing eavesdropping is essential as it helps the network to prohibit traffic analysis on captured packets and potentially reveal sensitive data. Moreover, by limiting the ability of the malicious nodes to eavesdrop, reactive adversaries are prohibited from launching other attacks, such as the DoS, based on an overhearing case. As Table 40 depicts, packet delivery is affected when reactive malicious nodes launch a DoS attack. Packet delivery is decreased more in the case of 10% malicious nodes. This occurs as there are more undetected malicious nodes that the nodes have not taken recovery actions against them. Therefore, they can eavesdrop on the communication and reactively trigger the DoS attack. The OMNI network

cannot minimize eavesdropping as effectively as the INCURE case, therefore it has more malicious nodes tapping on the network communication able to launch the DoS attack. Due to this, packet delivery is greatly affected in the OMNI network as it yields 56%, 44% and 50% in random sparse, random dense and grid sparse topologies respectively, a fraction which is 26%, 33% and 27% less when compared to the previously recovered results and considering 10% malicious nodes. OMNI's packet delivery capability is further degraded in the dense topology as the attack can affect more nodes due to the higher node density. INCURE is affected as well, however with a lower reduction percentage; packet delivery percentages of 72% and 69% are observed in the random sparse and dense topologies when considering 10% malicious nodes, which are 3% and 12% respectively less than the previous results. Results demonstrate that low density networks are greatly affected in the OMNI case while INCURE is more resilient. This is due to the fact that the malicious nodes in the OMNI case take benefit of the low density and affect the connectivity of the network. INCURE isolates detected malicious nodes in such a way that minimizes their ability to affect connectivity and the network's packet delivery capability. The INCURE grid retains the recovered packet delivery as there are more detected malicious nodes that are effectively isolated and thus are prohibited from launching new attacks. Overall, the INCURE network retains higher packet delivery than the OMNI case, ranging from 28% (random sparse case, 10% malicious nodes) to 58% (dense topology, 10% malicious node) more packets successfully delivered to the sink.

Table 40: LOS DoS attack per eavesdropping case – Packet delivery increase/decrease % from LOS selective forwarding recovery (R) scenario

Packet delivery increase / decrease %		Topology								
		Sparse (Figure 34 – page 239)			Dense (Figure 38 – page 240)			Grid (Figure 42 – page 242)		
	malicious nodes	R (%)	S (%)	I/D	R (%)	S (%)	I/D	R (%)	S (%)	I/D
INCURE	5%	83.3	82.1	-1.4%	84.6	79.2	-6.3%	80.3	80.4	+0.1%

	10%	74	71.5	-3.3%	78.5	69.3	-11.7%	73.1	75.7	+3.5%
OMNI (O)	5%	77.1	68	-11.8%	70.3	58	-17.5%	72.1	59.3	-17.7%
	10%	75	55.6	-25.8%	65.9	44.1	-33.1%	67.9	49.5	-27.1%
Gain	**5%**		**20.7% (I)**			**36.5% (I)**			**35.5% (I)**	
	10%		**28.6% (I)**			**57.1% (I)**			**53% (I)**	

Packet delivery delay (Table 41) is also increased in most of the cases as the DoS increases packet loss, retransmissions, routing overhead, access time to the channel, etc. The attack is most effective if the malicious node is near an active route. At the dense topology, both networks present the lowest delay as the packets continue to be delivered over short paths to the sink. INCURE presents a delay reduction at the grid topology as it updates to more efficient routing paths. On the other hand, OMNI presents an increase delay percentage of 29% and 23% considering 5% and 10% malicious nodes respectively at the grid. This occurs as malicious nodes are still neighbors of active nodes, although they have been excluded from active route paths, thus can compromise their neighbors' operation. In the sparse topology, the DoS attack takes benefit of the low node density, affecting the connectivity of both INCURE and OMNI networks and increasing the packet delivery delay. OMNI increases delay by 39% and INCURE by 24% when considering 10% malicious nodes.

Table 41: LOS DoS attack per eavesdropping case – Packet delivery delay increase/decrease % from LOS selective forwarding attack recovery (R) scenario

Packet delivery delay increase / decrease %		Topology								
		Sparse (Figure 36 – page 240)			Dense (Figure 40 – page 241)			Grid (Figure 44 – page 242)		
	malicious nodes	R (ms)	S (ms)	I/D	R (ms)	S (ms)	I/D	R (ms)	S (ms)	I/D
INCURE (I)	5%	121.6	157.2	+29.2%	58.2	65.8	+13.1%	158.8	151.1	-4.8%
	10%	136.8	169.2	+23.6%	54.8	50.3	-8.2%	171.9	131	-23.7%

OMNI (O)	5%	72.5	97.5	+34.5%	35.2	39.5	+12.2%	377.1	487.8	+29.3%
	10%	76.9	106.6	+38.6%	31.1	38.1	+22.5%	324.3	397.7	+22.6%
Gain	**5%**		**38% (O)**			**40% (O)**			**69% (I)**	
	10%		**37% (O)**			**24.3% (O)**			**67% (I)**	

Energy consumption (Table 42) is also affected by the reactive malicious nodes. INCURE outperforms significantly the OMNI case in terms of yielding less energy consumption. The proposed work reduces energy consumption from 64% (random dense, 10% malicious) to 79% (grid, 10% malicious) when compared to the equivalent OMNI scenarios. INCURE demonstrates the least energy consumption increase percentage at the grid and the highest increase percentage at the random dense network. In the dense network, malicious nodes have more chances to eavesdrop on the communication, thus react with a new attack and affect more nodes. On the grid, the lower node density in combination with the topology and the recovery measures lessen the eavesdropping ability of the malicious nodes and therefore prohibit reactive malicious actions that have a negative impact on the network's performance.

Table 42: LOS DoS attack per eavesdropping case – Energy consumption increase/decrease % from LOS selective forwarding attack recovery (R) scenario

Energy consumption increase %		Topology								
		Sparse (Figure 35 – page 239)			Dense (Figure 39 – page 241)			Grid (Figure 43 – page 242)		
	malicious nodes	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D
INCURE (I)	5%	111.5	175.6	+57.5%	117.3	220.2	+87.7%	107.8	109.1	+1.2%
	10%	111.9	269.5	+140.8%	115.4	311.3	+169.7%	104.8	156.5	+49.3%
OMNI (O)	5%	272.5	592.5	+117.4%	300	662.8	+121%	281.7	512.3	+81.8%
	10%	278.2	846	+204%	292.1	856.4	+193.1%	251.8	743.3	+195.1%
Gain	**5%**		**70.3% (I)**			**66.7% (I)**			**78.7% (I)**	
	10%		**68.1% (I)**			**63.6% (I)**			**79% (I)**	

5.3.1.4.2.1 Concluding remarks

Recovery in INCURE can effectively address both selective forwarding and eavesdropping attacks. As more active malicious nodes are addressed in the case of the selective forwarding recovery scenario, INCURE minimizes the ability of malicious nodes to eavesdrop (Figure 19) on the network's communication and to react by continuing their attack strategy. Therefore, INCURE can minimize the negative impact on compromised nodes, packet delivery and energy consumption, when the DoS attack is executed based on an overhearing case. On the other hand, although the OMNI recovery actions can address the selective forwarding attack, they cannot effectively defend against the eavesdrop attack nor protect the network from malicious nodes' compromisation capabilities, showcasing a significant performance degradation.

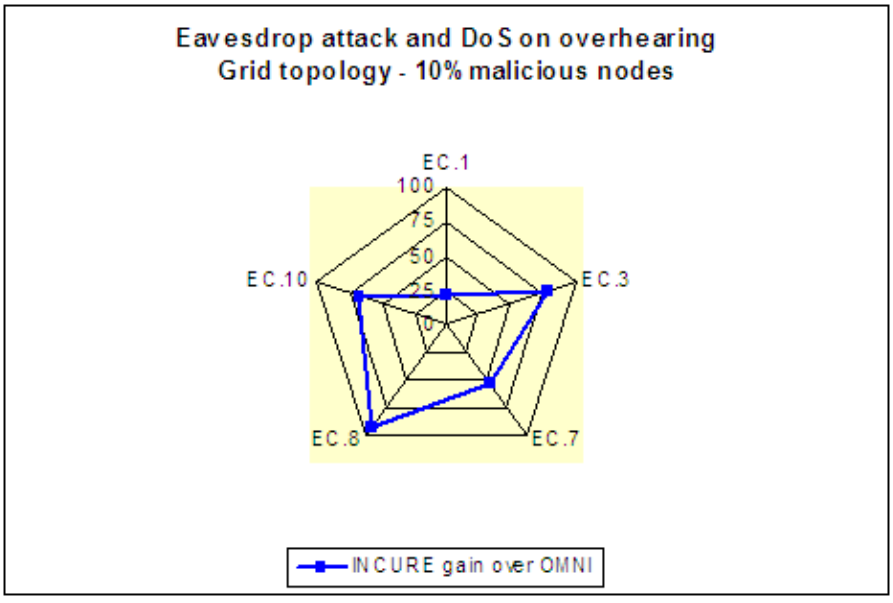

Figure 19: Persistent attack strategy – eavesdrop and DoS on overhearing performance gain

5.3.1.4.3 Continuous DoS attack and recovery

As the passive attacks are addressed by the appropriate intrusion recovery countermeasures, the adversary adapts his intrusion strategy and implements a DoS attack, whether it can overhear or not. Malicious nodes execute a continuous DoS attack, persistently sending packets with the aim of forcing nodes to increased energy consumption, blocking the network communication and prohibiting nodes from forwarding their packets. As the number of malicious nodes increases, so does the number of compromised nodes (Table 43). When malicious nodes execute a DoS attack, they can compromise a significant larger number of nodes in comparison to the case where they execute a selective forward attack. This occurs as a malicious node can affect neighbor nodes in a more brute way when a DoS attack is executed. Moreover, as the node density increases, compromised nodes increase as well since there are more nodes in the vicinity of the malicious nodes that can be affected. INCURE yields the lowest amount of compromised nodes on the grid, 9% when considering 5% malicious nodes and a greater number on the random dense with 36% when having 10% malicious nodes. For the equivalent scenarios, OMNI yields 18% and 63% compromised nodes (that is 9% and 27% more than INCURE). This is due to the fact that previously more active selective forwarding malicious nodes have been detected on the grid, triggering recovery countermeasures. When INCURE recovery countermeasure is applied, the malicious signals are prohibited from reaching legitimate nodes and compromising them. On the other hand, OMNI networks allow signals to be received from all directions and therefore malicious nodes can take advantage of this property to affect more nodes. Also, as it can be observed from Table 43, there are more compromised nodes when considering a continuous attack than when considering a reactive adversary who attacks based on an overhearing case (Table 38). This is somehow expected as in a continuous attack all malicious nodes execute the attack, independently of whether they can eavesdrop or not.

Table 43: LOS DoS attack – Compromised nodes % from LOS selective forwarding recovery (R) scenario

Compromised nodes %		Topology		
		Sparse (Figure 33 – page 239)	Dense (Figure 37 – page 240)	Grid (Figure 41 – page 241)
	malicious nodes	I/D	I/D	I/D
INCURE (I)	5%	+11.3%	+20%	+9.3%
	10%	+20%	+35.8%	+16.4%
OMNI (O)	5%	+30.1%	+36.2%	+18.4%
	10%	+49.1%	+63.2%	+36.3%
Gain	**5%**	**18.8% (I)**	**16.2% (I)**	**9.1% (I)**
	10%	**29.1% (I)**	**27.4% (I)**	**19.9% (I)**

The DoS also negatively affects the packet delivery (Table 44) in both INCURE and OMNI networks. As DoS nodes increase the packet delivery is decreased. Both networks show the highest packet delivery decrease percentage (compared to selective forward attack recovered scenario) at the dense topologies, due to the higher node density and a higher number of (previously) undetected malicious nodes. INCURE presents a packet delivery percentage of 63% and the OMNI 46% at the dense topology when there are 10% malicious nodes. Moreover, INCURE demonstrates a higher resilience at low node densities in comparison to the OMNI case. INCURE packet delivery decrease percentage ranges from 5% to 13% at the random and grid sparse topologies, whereas OMNI shows a decrease percentage between 17% and 25%. This occurs as INCURE's operation is effective in minimizing the adversary's ability to affect the network's connectivity, especially on the grid case. Overall, INCURE presents more packet delivery (from 13% to 36%) than the OMNI case.

Table 44: LOS DoS attack – Packet delivery increase/decrease % from LOS selective forwarding recovery (R) scenario

Packet delivery decrease %		Topology								
		Sparse (Figure 34 – page 239)			Dense (Figure 38 – page 240)			Grid (Figure 42 – page 242)		
	malicious nodes	R (%)	S (%)	I/D	R (%)	S (%)	I/D	R (%)	S (%)	I/D
INCURE (I)	5%	83.3	72.8	-12.6%	84.6	76.1	-10%	80.3	74.5	-7.2%
	10%	74	67.3	-9%	78.5	62.9	-19.8%	73.1	69.1	-5.4%
OMNI (O)	5%	77.1	64.3	-16.6%	70.3	57.4	-18.3%	72.1	59.5	-17.4%
	10%	75	56.8	-24.2%	65.9	46.1	-30%	67.9	50.9	-25%
Gain	**5%**		**13.2% (I)**			**32.5% (I)**			**25.3% (I)**	
	10%		**18.4% (I)**			**36.4% (I)**			**35.7% (I)**	

In terms of energy consumption (Table 45), INCURE grid presents the lowest consumption in comparison to the random sparse and dense topologies as fewer nodes are affected by the attack and thus the attack impact is minimized. As attacks get more severe, for example when malicious nodes increase in the network and execute the attack, energy is increased even more. The same observation applies as the network gets denser. Both networks present the highest energy consumption at the dense networks. INCURE outperforms the OMNI case as there is about 71%, 51% and 60% less energy consumption at the grid, dense and sparse networks respectively when compared to the equivalent OMNI scenarios and considering 5% malicious nodes.

Table 45: LOS DoS attack – Energy consumption increase/decrease % from LOS selective forwarding attack recovery (R) scenario

Energy consumption increase %	Topology		
	Sparse (Figure 35 – page 239)	Dense (Figure 39 – page 241)	Grid (Figure 43 – page 242)

	malicious nodes	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D
INCURE (I) [1]	5%	111.5	251.4	+125.4%	117.3	356.7	+204%	107.8	146.6	+35.9%
	10%	111.9	340.6	+204.3%	115.4	518.5	+349.3%	104.8	219.8	+109.7 %
OMNI (O)	5%	272.5	626.8	+130%	300	726	+142%	281.7	503.7	+78.8%
	10%	278.2	805.2	+189.4%	292.1	883.1	+202.3%	251.8	716.1	+184.3 %
Gain	**5%**		**59.8% (I)**			**50.8% (I)**			**70.8% (I)**	
	10%		**57.6% (I)**			**41.2% (I)**			**69.3% (I)**	
Note	[1]	INCURE presents more packet delivery (from 13% to 36%) than the OMNI case								

Packet delivery delay (Table 46) is also affected by the continuous DoS attack. INCURE presents a delay of 174, 57 and 192 milliseconds when considering the random sparse, random dense and grid topologies respectively with 10% malicious nodes. The delay is increased by 27% (random sparse), 3% (random dense) and 12% (grid) when there are 10% malicious nodes and compared to the scenario where the network recovers from the selective forwarding attack. For the same recovered case, OMNI increases its delay by 26%, 14% and 16% when considering the random sparse, dense and grid topologies. OMNI yields around 96% more delay on the grid topology when compared to the INCURE case. At the random topologies INCURE presents a higher overall packet delivery delay as OMNI achieves a higher node density that allows it to route packets over shorter route paths, but also it presents a lower packet delivery percentage than INCURE.

Table 46: LOS DoS attack – Packet delivery delay increase/decrease % from LOS selective forwarding recovery (R) scenario

Packet delivery delay increase %	Topology		
	Sparse (Figure 36 – page 240)	Dense (Figure 40 – page 241)	Grid (Figure 44 – page 242)

	malicious nodes	R (ms)	S (ms)	I/D	R (ms)	S (ms)	I/D	R (ms)	S (ms)	I/D
INCURE (I)	5%	121.6	159	+30.7%	58.2	64.3	+10.4%	158.8	183.2	+15.3%
	10%	136.8	173.5	+26.8%	54.8	56.5	+3.1%	171.9	191.8	+11.5%
OMNI (O)	5%	72.5	104.6	+44.2%	35.2	51.9	+47.4%	377.1	452	+19.8%
	10%	76.9	96.9	+26%	31.1	35.4	+13.8%	324.3	376.8	+16.1%
Gain	**5%**		**34.2% (O)**			**19.2% (O)**			**59.4% (I)**	
	10%		**44.1% (O)**			**37.3% (O)**			**49% (I)**	

As soon as the DoS attack is detected, affected INCURE nodes recover as specified by the intrusion recovery policy. OMNI nodes enter a low duty cycle mode as an equivalent measure to avoid the DoS attack.

In the random sparse and dense INCURE cases, no nodes are compromised (Table 47) due to the recovery actions when considering 5% malicious nodes. For the same topologies, INCURE compromises a small amount of nodes when considering 10% malicious nodes. In the random sparse case, INCURE recovery compromises 1% of the nodes in 10% of the simulations and for the random dense topology it compromises 1% of the nodes in about 6% of the simulation runs. OMNI recovery in the sparse case compromises 35% and 59% nodes when 5% and 10% malicious nodes are present. OMNI recovery in dense topology yields 46% and 78% compromised nodes in the presence of 5% and 10% malicious nodes. A similar observation is made on the grid topology where INCURE does not compromise any nodes and OMNI compromises 20% and 41% of the nodes when having 5% and 10% malicious nodes. As it can be observed, as malicious nodes increase, and thus recovery is applied by more nodes in the network, OMNI case is significantly affected by the recovery measures taken. On the contrary, INCURE recovery is applied without a significant tradeoff between recovery and compromised nodes.

Table 47: LOS DoS recovery – Compromised nodes % from recovery measures

Compromised nodes %		Topology		
		Sparse (Figure 33 – page 239)	Dense (Figure 37 – page 240)	Grid (Figure 41 – page 241)
	malicious nodes	I/D	I/D	I/D
INCURE (I)	5%	0%	0%	0%
	10%	+0.11%	+0.06%	0%
OMNI (O)	5%	+35.3%	+46%	+20.2%
	10%	+59.3%	+78%	+40.8%
Gain	**5%**	**35.3% (I)**	**46% (I)**	**20.2% (I)**
	10%	**59.2% (I)**	**77.94% (I)**	**40.8% (I)**

Although both networks address the DoS attack and minimize the compromised nodes, packet delivery is not recovered in all the cases. The recovery measures in OMNI greatly affect the packet delivery as the nodes that deploy the low duty cycle are unavailable for routing, thus routes to destination are difficult to be established. Table 48 shows a decrease in packet delivery in OMNI yielding a 40% and 34% fraction (which is around 30% and 27% reduction from the previous scenario) when considering the sparse and dense cases respectively, and 10% malicious nodes. Also, OMNI grid is affected even more as packet delivery is decreased by a 42% percentage when considering 10% malicious nodes. Overall, the packet delivery in the OMNI case is affected due to its recovery measures. In INCURE, the networks' packet delivery capability is recovered. As malicious nodes are increased, more nodes apply the INCURE recovery measure. At the random sparse and grid topologies it is more difficult to re-establish routing paths, thus the low packet delivery increase percentage, around 3% when considering 10% malicious nodes. At the dense case, INCURE presents a higher increase packet delivery percentage up to 12% due to the higher node density that

allows the network to retain its connectivity more effectively. Overall, INCURE shows a recovered packet delivery ranging from 69% to 81%.

Table 48: LOS DoS recovery – Packet delivery increase/decrease % from LOS DoS attack (R) scenario

Packet delivery increase / decrease %		Topology								
		Sparse (Figure 34 – page 239)			Dense (Figure 38 – page 240)			Grid (Figure 42 – page 242)		
	malicious nodes	R (%)	S (%)	I/D	R (%)	S (%)	I/D	R (%)	S (%)	I/D
INCURE (I)	5%	72.8	77	+5.7%	76.1	80.3	+5.5%	74.5	81.2	+8.9%
	10%	67.3	69.4	+3.1%	62.9	70.6	+12.2%	69.1	71.5	+3.4%
OMNI (O)	5%	64.3	54	-16%	57.4	44.6	-22.2%	59.5	45.2	-24%
	10%	56.8	39.8	-29.9%	46.1	33.6	-27.1%	50.9	29.6	-41.8%
Gain	**5%**		**42.5% (I)**			**80% (I)**			**79.6% (I)**	
	10%		**74.3% (I)**			**110.1 % (I)**			**141.5 % (I)**	

Also, energy consumption (Table 49) is decreased as the attack is addressed by both networks. As the networks apply their recovery countermeasures on more malicious nodes, prohibiting them to compromise nearby neighbors, they present less energy consumption. INCURE achieves up to 72% less energy consumption when compared to the DoS scenario, while OMNI can reduce its energy consumption up to 58%. INCURE case outperforms OMNI as it yields from 58% (sparse, 5% malicious node) to 66% (grid, 10% malicious nodes) less energy consumption when compared to the OMNI equivalent scenarios. It is worth mentioning that INCURE achieves saving its energy resources due to the fact that the attack outcome on sensor nodes is minimized. INCURE promotes the network survivability while restoring the packet delivery capability. At the OMNI case, the high reduction is achieved as a large number of sensor nodes become unavailable in order to address the attack, and therefore

minimize the energy consumption. However, OMNI tradeoffs the packet delivery capability with the network survivability.

Table 49: LOS DoS recovery – Energy consumption increase/decrease % from LOS DoS attack (R) scenario

Energy consumption decrease %		Topology								
		Sparse (Figure 35 – page 239)			Dense (Figure 39 – page 241)			Grid (Figure 43 – page 242)		
	malicious nodes	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D
INCURE (I)	5%	251.4	128.1	-49%	356.7	138.1	-61.2%	146.6	111.1	-24.2%
	10%	340.6	120.6	-64.5%	518.5	146	-71.8%	219.8	101.3	-53.9%
OMNI (O) [1]	5%	626.8	308	-50.8%	726	336.5	-53.6%	503.7	279.3	-44.5%
	10%	805.2	346.1	-57%	883.1	385.8	-56.3%	716.1	298.3	-58.3%
Gain	**5%**		**58.4% (I)**			**58.9% (I)**			**60.2% (I)**	
	10%		**65.1% (I)**			**62.1% (I)**			**66% (I)**	
Note	[1]	Tradeoffs packet delivery with network survivability								

In terms of end-to-end packet delivery delay (Table 50), recovery measures increase the delay as route paths are updated to recover the packet delivery capability of the network. OMNI presents an overall lower packet delivery delay at the random topologies when compared to the INCURE case. This occurs as OMNI recovers less packet delivery than INCURE and also it achieves a higher node density at the random topologies that allows it to create shorter route paths. However, INCURE dense achieves a lower increase delay percentage when compared to the OMNI scenarios. This occurs as the low duty cycle mode deployed by the OMNI case prohibits the network from converging easily to new route paths, increasing the delay. On the grid, where both networks achieve the same node density, INCURE presents up to 66% less packet delivery delay when compared to the OMNI grid

case. A snapshot of INCURE's gain over OMNI for the grid topology is presented in Figure 20.

Table 50: LOS DoS recovery – Packet delivery delay increase/decrease % from LOS DoS attack (R) scenario

Packet delivery delay increase / decrease %		Topology								
		Sparse (Figure 36 – page 240)			Dense (Figure 40 – page 241)			Grid (Figure 44 – page 242)		
	malicious nodes	R (ms)	S (ms)	I/D	R (ms)	S (ms)	I/D	R (ms)	S (ms)	I/D
INCURE (I)	5%	159	175.9	+10.6%	64.3	67	+4.1%	183.2	192.5	+5%
	10%	173.5	188.3	+8.5%	56.5	65.6	+16.1%	191.8	162.5	-15.2%
OMNI (O)	5%	104.6	107.3	+2.5%	51.9	59.1	+13.8%	452	406.9	-10%
	10%	96.9	104.2	+7.5%	35.4	43.1	+21.7%	376.8	473.2	+25.5%
Gain	5%		**38.9% (O)**			**11.8% (O)**			**52.6% (I)**	
	10%		**44.6% (O)**			**34.2% (O)**			**65.6% (I)**	

As discussed previously, the low duty cycle countermeasure in the OMNI network addresses the DoS attack, greatly affecting the availability of the network and increasing the risk of compromising the decision making process that depends on the delivered information. In an effort to address the DoS attack and recover the network's performance, OMNI nodes deploy more recovery actions. The channel surfing countermeasure [52, 55, 56, 57, 58] is deployed by OMNI nodes. Following we evaluate the appropriateness of the channel surfing countermeasure in WSNs to address adaptive/persistent adversaries.

The case where the OMNI network has deployed the low duty cycle in order to address the continuous DoS attack is considered. After sensor nodes have deployed the low duty cycle and observed that the attack continues when they resume their operation, they switch to a new

frequency in order to address the attack, decrease low duty cycle's side effects and restore the network's performance. When the frequency switch is deployed, leaving the malicious nodes operating in the default frequency channel, the attack is turned ineffective and the network can continue its operation. It can be observed in the OMNI case that there are no compromised nodes (Table 51) due to the attack or due to the recovery. This helps the network to restore its packet delivery capability by 31%, 20% and 48% in the sparse, dense and grid topologies respectively with 10% malicious nodes. OMNI can recover a packet delivery percentage of 40% to 60%, considering both 5% and 10% malicious nodes cases. As it can be observed from Table 51, OMNI yields a higher packet delivery increase percentage at the grid when considering 10% malicious nodes as it recovers a higher number of nodes that have been previously compromised due to the low duty cycle mode. As the packet delivery is increased, so does the energy consumption (up to 48%). End-to-end packet delivery delay varies; in the sparse networks the packet delivery delay is highly increased due to the large amount of communication that occurs as the low node density makes it harder to update to new route paths as sensor nodes are awaken and try to establish network communication. In the dense network the sensor nodes establish efficient routing paths and forward packets to destinations more effectively, thus delay is retained at low levels.

Table 51: LOS DoS recovery channel surfing– OMNI overall evaluation increase/decrease % from LOS DoS recovery low duty cycle (R)

OMNI channel surfing overall evaluation		Topology								
		Sparse			Dense			Grid		
	malicious nodes	R	S	**I/D**	R	S	**I/D**	R	S	**I/D**
Compromised nodes (%) due to attack [1]	5%	0	0	**0%**	0	0	**0%**	0	0	**0%**
	10%	0	0	**0%**	0	0	**0%**	0	0	**0%**

Packet delivery (%) [2]	5%	54	59.7	**+10.5%**	44.6	50.9	**+14.1%**	45.2	54.7	**+21%**
	10%	39.8	52.1	**+30.9%**	33.6	40.4	**+20.2%**	29.6	43.9	**+48.3%**
Packet delay (ms) [3]	5%	107.3	141.3	**+31.6%**	59.1	69	**+16.7%**	406.9	425.3	**+4.5%**
	10%	104.2	129.2	**+23.9%**	43.1	49.5	**+14.8%**	473.2	365	**-22.8%**
Energy consumption (mJ) [4]	5%	308	366.5	**+18.9%**	336.5	396.4	**+17.8%**	279.3	335	**+19.9%**
	10%	346.1	460.2	**+32.9%**	385.8	570.1	**+47.7%**	298.3	409.6	**+37.3%**
Note	[1]	Figure 46 (page 243), Figure 50 (page 244), Figure 54 (page 246)								
	[2]	Figure 47 (page 243), Figure 51 (page 245), Figure 55 (page 246)								
	[3]	Figure 49 (page 244), Figure 53 (page 245), Figure 57 (page 247)								
	[4]	Figure 48 (page 244), Figure 52 (page 245), Figure 56 (page 246)								

As the malicious nodes in the OMNI scenarios cannot overhear anything, they adapt their strategy and they scan available frequency channels for network communication. If they can overhear nodes' communication, they stop scanning and use the discovered frequency channel to continue the DoS attack. The OMNI case cannot prohibit malicious nodes discovering the new frequency and therefore the network's performance degrades once more (Table 52). The attack increases the network's energy consumption, increases compromised nodes and affects the packet delivery. The channel surfing countermeasure utilized in WSNs appears to be ineffective in the case of adaptive and persistent adversaries. OMNI nodes required more recovery efforts to be deployed in order to cope with the DoS attack, without been able to prohibit malicious nodes from continue compromising the WSN.

Table 52: LOS DoS recovery channel surfing and reactive malicious nodes– OMNI overall evaluation increase/decrease % from LOS DoS recovery channel surfing (R)

OMNI channel surfing overall evaluation		Topology								
		Sparse			Dense			Grid		
	malicious nodes	R	S	**I/D**	R	S	**I/D**	R	S	**I/D**

Compromised nodes (%) [1]	5%	0	25	**+25%**	0	28	**+28%**	0	15.1	**+15.1%**
	10%	0	46	**+46%**	0	50	**+50%**	0	27	**+27%**
Packet delivery (%) [2]	5%	59.7	57	**-4.5%**	50.9	48.6	**-4.5%**	54.7	51.3	**-6.2%**
	10%	52.1	47.9	**-8%**	40.4	36.5	**-9.6%**	43.9	38.4	**-12.5%**
Packet delay (ms) [3]	5%	141.3	120.1	**-15%**	69	65.5	**-5%**	425.3	408.6	**-3.9%**
	10%	129.2	124.4	**-3.7%**	49.5	49.4	**-0.2%**	365	380.3	**+4.1%**
Energy consumption (mJ) [4]	5%	366.5	372.2	**+1.5%**	396.4	405.2	**+2.2%**	335	345.6	**+3.1%**
	10%	460.2	475.3	**+3.2%**	570.1	608.1	**+6.6%**	409.6	434	**+5.9%**
Note	[1]	Figure 46 (page 243), Figure 50 (page 244), Figure 54 (page 246)								
	[2]	Figure 47 (page 243), Figure 51 (page 245), Figure 55 (page 246)								
	[3]	Figure 49 (page 244), Figure 53 (page 245), Figure 57 (page 247)								
	[4]	Figure 48 (page 244), Figure 52 (page 245), Figure 56 (page 246)								

5.3.1.4.3.1 Concluding remarks

Regarding INCURE recovery, it has been shown previously that it has successfully addressed the continuous DoS attack. In terms of compromised nodes (Table 53), INCURE did not have any significant tradeoff due to its recovery actions and continues to preserve the availability of sensor nodes. Since the attack is effectively addressed as malicious nodes are prohibited from affecting nodes, active route paths cannot be compromised easily. Therefore, the network retains a stable performance (Table 53) in terms of packet delivery, energy consumption and end-to-end packet delivery delay, without the need for any further actions.

Table 53: LOS DoS recovery – INCURE versus OMNI overall evaluation

Overall evaluation			Topology		
			Sparse	Dense	Grid
Compromised nodes (%) due to recovery	INCURE (I)	5%	0%	0%	0%
		10%	0.11%	0.06%	0
	OMNI (O) – Low duty cycle	5%	35.3%	46%	20.2%
		10%	59.3%	78%	40.8%
	OMNI (O) – Channel surfing	5%	0%	0%	0%
		10%	0%	0%	0%
Packet delivery (%)	INCURE (I)	5%	77%	80.3%	81.2%
		10%	69.4%	70.6%	71.5%
	OMNI (O) – Low duty cycle	5%	54%	44.6%	45.2%
		10%	39.8%	33.6%	29.6%
	OMNI (O) – Channel surfing	5%	59.7%	50.9%	54.7%
		10%	52.1%	40.4%	43.9%
Energy consumption (mJ)	INCURE (I)	5%	128.1	138.1	111.1
		10%	120.6	146	101.3
	OMNI (O) – Low duty cycle	5%	308	336.5	279.3
		10%	346.1	385.8	298.3
	OMNI (O) – Channel surfing	5%	366.5	396.4	335
		10%	460.2	570.1	409.6
Packet delivery delay (ms)	INCURE (I)	5 %	175.9	67	192.5
		10 %	188.3	65.6	162.5
	OMNI (O) – Low duty	5 %	107.3	59.1	406.9
		10 %	104.2	43.1	473.2
	OMNI (O) – Channel surfing	5%	141.3	69	425.3
		10%	129.2	49.5	365

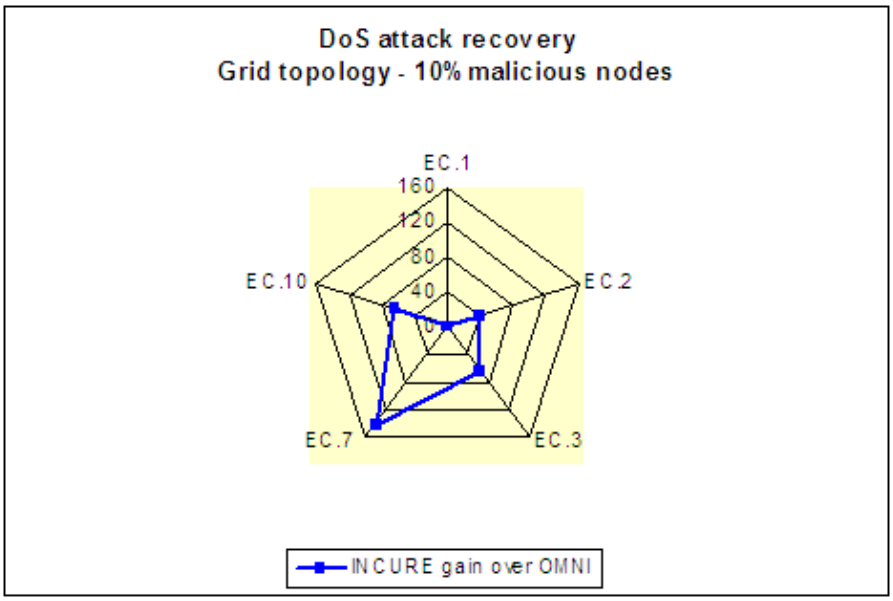

Figure 20: Persistent attack strategy – DoS recovery gain over OMNI low duty cycle

5.3.1.4.4 Persistent adversary

If the malicious nodes do not receive any communication they may assume that recovery measures are active and therefore they persist with their compromisation efforts by adapting their intrusion strategy. They increase their transmission power in an attempt to affect more nodes. As malicious nodes attack the network, the nodes continue applying their recovery measures. As it can be observed from Table 54, a large portion of the network is affected by the OMNI recovery itself when compared to the INCURE case. INCURE recovery compromises 6%, 9% and 2% of the nodes due to the recovery action when considering the sparse, dense and grid topologies with 10% malicious nodes. OMNI compromises from 80% to 86% of the nodes when 10% malicious nodes are considered.

Table 54: LOS DoS extended attack – Compromised nodes due to recovery (%)

Compromised nodes %		Topology		
		Sparse (Figure 33 – page 239)	Dense (Figure 37 – page 240)	Grid (Figure 41 – page 241)
	malicious nodes	I/D	I/D	I/D
INCURE (I)	5%	+2%	+1.4%	+0.1%
	10%	+6.2%	+8.9%	+2.1%
OMNI (O)	5%	+73%	+75.7%	+56.5%
	10%	+84%	+86%	+80%
Gain	**5%**	**71% (I)**	**74.3% (I)**	**56.4% (I)**
	10%	**77.8% (I)**	**77.1% (I)**	**77.9% (I)**

As it can be observed from Table 55, packet delivery is reduced as the extended DoS attack affects the network and also some of the recovery actions have turned unavailable a number of sensor nodes. Overall INCURE retains a much higher packet delivery, ranging from 52% to 75%. INCURE is affected more at the sparse and dense topologies in comparison to the grid case as more nodes are compromised by the attack, affecting network's connectivity. Grid provides a better resilience, thus a lower packet delivery percentage is observed. OMNI presents a packet delivery percentage from 30% to 47%, indicating that the recovery has a similar effect as the DoS attack. This occurs as the attack has compromised a considerable amount of nodes, severely compromising the ability of the network for packet delivery. Recovery measures in OMNI compromise a large number of sensor nodes as the DoS attack and thus the network's capabilities in terms of packet delivery are considerably decreased as in the DoS attack case.

Table 55: LOS DoS extended attack – Packet delivery increase/decrease % from LOS DoS recovery (R) scenario

Packet delivery decrease %		Topology								
		Sparse (Figure 34 – page 239)			Dense (Figure 38 – page 240)			Grid (Figure 42 – page 242)		
	malicious nodes	R (%)	S (%)	I/D	R (%)	S (%)	I/D	R (%)	S (%)	I/D
INCURE (I)	5%	77	60	-22%	80.3	66.2	-17.5%	81.2	75.3	-7.2%
	10%	69.4	51.9	-25.2%	70.6	52.9	-25%	71.5	64.6	-9.6%
OMNI (O)	5%	54	46.9	-13.1%	44.6	42.6	-4.5%	45.2	40.5	-10.3%
	10%	39.8	38.3	-3.7%	33.6	33.5	-0.3%	29.6	29.3	-1%
Gain	**5%**		**27.9% (I)**			**55.3% (I)**			**85.9% (I)**	
	10%		**35.5% (I)**			**57.9% (I)**			**120.4 % (I)**	

The extended DoS attack forces the networks to consume more energy (Table 56), reducing their lifetime. In the random topologies, OMNI seems to have a much lower increase percentage than the INCURE case; however this is due to the large number of sensor nodes that are turned unavailable due to the recovery and thus cannot participate in any of the communication activities. Overall, INCURE presents around 31%, 51% and 63% less energy consumption than OMNI in the sparse, dense and grid topologies respectively with 10% malicious nodes. In INCURE, grid provides a higher level of resilience against compromisation (Figure 21), thus it presents the lowest energy consumption increase percentage due to the extended DoS. As the network becomes denser, resilience is reduced; however INCURE delays malicious nodes from degrading resources in comparison to the OMNI case.

Table 56: LOS DoS extended attack – Energy consumption increase/decrease % from LOS DoS recovery scenario

Energy consumption increase %		Topology								
		Sparse (Figure 35 – page 239)			Dense (Figure 39 - page 241)			Grid (Figure 43 – page 242)		
	malicious nodes	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D	R (mJ)	S (mJ)	I/D
INCURE (I)	5%	128.1	295.7	+130.8%	138.1	330.3	+139.1%	111.1	166.7	+50%
	10%	120.6	328.3	+172.2%	146	365.5	+150.3%	101.3	184.1	+81.7%
OMNI (O)	5%	308	484.7	+57.3%	336.5	475.3	+41.2%	279.3	429	+53.5%
	10%	346.1	478.8	+38.3%	385.8	748.2	+93.9%	298.3	503.6	+68.8%
Gain	**5%**		**38.9% (I)**			**30.5% (I)**			**61.1% (I)**	
	10%		**31.4% (I)**			**51.1% (I)**			**63.4% (I)**	

5.3.1.4.4.1 Concluding remarks

Malicious nodes can extend their intrusion strategy by changing the dynamics of an attack as in the DoS case where they increase their transmission power to affect more nodes. The OMNI low duty recovery measure yields a considerable tradeoff in terms of compromised nodes in order to address the attack and prohibit the malicious nodes from consuming a large amount of the network's energy. Although the attack is addressed, the large number of nodes that are turned unavailable affects the packet delivery capability of nodes, and thus the decision-making can be affected also or even prohibited. INCURE addresses the extended attack with much less tradeoff in terms of compromised nodes, thus the network is affected much less when compared to the OMNI case and continues to support decision-making, a task that is vital for mission-critical applications.

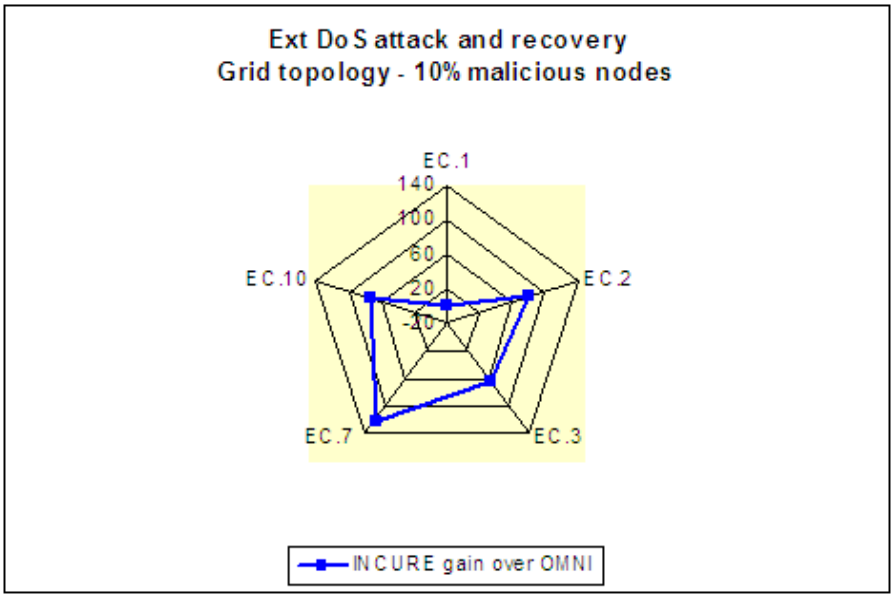

Figure 21: Persistent attack strategy – ext DoS and recovery gain

5.3.1.4.5 Overall evaluation remarks for LOS

This section summarizes the evaluation results for LOS and discusses the effectiveness of INCURE/typical intrusion recovery solutions in WSNs towards the intrusion recovery evaluation aspects (availability, survivability, reliability, resilience, responsiveness and self-healingness) that are defined in section 5.1.

In terms of availability, we are interested to assess if recovery can minimize the ability of malicious nodes to compromise nodes and their operation. Also, it is important to evaluate the tradeoff related to compromised nodes that may incur from the recovery measures. Such compromised nodes are considered those that either disabled all their antennas or all their neighbors disable their antennas towards them. As indicated by Table 57, both networks present the best results in the random sparse and grid topologies in comparison to the dense case when considering the number of nodes that can be compromised by eavesdropping or a DoS attack. INCURE random topologies yield an insignificant tradeoff of 1% compromised nodes due to recovery when there are 10% malicious nodes, while they recover 20% and 36%

compromised nodes during a DoS attack at the sparse and dense topologies respectively. With regards to the grid topology, INCURE recovers the compromised nodes that are affected by the attack without affecting the operation of nodes. When an extended DoS attack is executed, at most 2% of the INCURE nodes are compromised due to the recovery countermeasures on the grid topology when considering 10% malicious nodes. At the random topologies and as the network gets denser, recovery yields a higher tradeoff in terms of compromised nodes in order to address the extended DoS attack; up to 6% in random sparse and 9% in random dense as malicious nodes increase. Overall, INCURE is more effective in minimizing the ability of malicious nodes to compromise the WSN after recovery is applied. Also, it presents a negligible tradeoff in terms of compromised nodes due to the recovery measures. On the other hand, the low duty cycle countermeasure implemented in the OMNI case affects the availability of quite a number of nodes in the effort to address the DoS attack and minimize its impact on the network's energy depletion. OMNI compromises up to 78% of the nodes with the low duty cycle measure, affecting considerably the network′ s packet delivery capability.

Table 57: Availability evaluation – LOS Compromised nodes

AVAILABILITY (Ref. Table 24)		
Compromised nodes %	Topology	
	Grid	
Static attack strategy	Malicious nodes	
	5%	10%
Due to DoS recovery		
INCURE-LOS	0	0
OMNI-LOS	20.1	40.9

AVAILABILITY (Ref. Table 38, Table 43, Table 47, Table 54)			
Compromised nodes %	Topology		
	Sparse	Dense	Grid
Persistent attack strategy	Malicious nodes		

	5%	10%	5%	10%	5%	10%
Due to eavesdrop						
INCURE-LOS	6.4	15	8.6	18.9	4	9.1
OMNI-LOS	26.8	47.5	30.5	54.7	18.2	30
Due to DoS						
INCURE-LOS	11.3	20	20	35.8	9.3	16.4
OMNI-LOS	30.1	49.1	36.2	63.2	18.4	36.3
Due to DoS recovery						
INCURE-LOS	0	0.11	0	0.06	0	0
OMNI-LOS	35.3	59.3	46	78	20.2	40.8
Due to ext DoS recovery						
INCURE-LOS	2	6.2	1.4	8.9	0.1	2.1
OMNI-LOS	73	84	75.7	86	56.5	80

In terms of survivability, the evaluation aims to indicate if recovery countermeasures can minimize the attack outcome related to energy depletion (Table 58) and also assess in what way the energy consumption is affected when recovery is applied. Both networks decrease their energy consumption when malicious nodes execute the selective forwarding attack. The decrease of energy consumption occurs as fewer packets are traversing the network as the malicious nodes on active route paths drop the received packets. Moreover, as nodes forward fewer packets, there is less overhearing, collisions, packet drops and retransmissions, thus less energy spent for network communication. As malicious nodes increase, thus have more chances to participate on active route paths and execute the selective forwarding attack, energy consumption appears to decrease even more. The malicious nodes also have more chances to be selected as next hops in sparse networks. As INCURE and OMNI networks recover from the selective forwarding attack and restore the networks' packet delivery capability, the energy consumption increases. INCURE restores a higher percentage of packet delivery than OMNI, thus appears to have a higher increase percentage of energy consumption. When the malicious nodes execute a DoS attack, nodes are forced to increased energy consumption. The energy consumption that occurs due to the DoS attack is increased

even more if malicious nodes are near by active route paths (as in the case of INCURE static attack strategy), causing packet drops and retransmissions. In the case of a persistent attack strategy, where malicious nodes execute a DoS based on overhearing, INCURE can minimize the attack outcome related to energy depletion when compared to the OMNI case. This occurs as the INCURE is able to minimize eavesdropping considerably, thus less malicious nodes trigger the DoS on overhearing and affect the network's energy consumption. On the grid, INCURE minimizes the overhearing more when compared to the other topologies and the OMNI respective scenarios, thus it presents the lowest increase percentage of energy consumption; when considering 10% malicious nodes on the grid, INCURE presents an increase percentage of energy consumption up to 49% while OMNI yields a percentage of 195% more energy consumption. When the networks apply their measures to address the continuous DoS attack in the persistent attack strategy case, they are able to decrease the energy consumption that occurs due to the attack. OMNI appears to achieve a higher decrease percentage than INCURE as it restores much less packet delivery. Overall, INCURE achieves less energy consumption than OMNI.

Table 58: Survivability evaluation – LOS Energy consumption increase/decrease %

SURVIVABILITY (Ref. Table 13, Table 17, Table 21, Table 25)		
Energy consumption increase/decrease %	Topology	
	Grid	
Static attack strategy	Malicious nodes	
	5%	10%
SF attack		
INCURE-LOS	-31.8	-41.5
OMNI-LOS	-31.1	-40.4
Recover from SF attack		
INCURE-LOS	+43.3	+78.3
OMNI-LOS	+35.5	+40
DoS attack		
INCURE-LOS	+209.5	+404.1

OMNI-LOS	+100.7	+175
Recover from DoS attack		
INCURE-LOS	-61.2	-74.3
OMNI-LOS	-41.8	-38.3

SURVIVABILITY (Ref. Table 32, Table 36, Table 45, Table 49)						
Energy consumption increase/decrease %	Topology					
	Sparse		Dense		Grid	
Persistent attack strategy	Malicious nodes					
	5%	10%	5%	10%	5%	10%
SF attack						
INCURE-LOS	-22.1	-30.3	-6.3	-15	-31.9	-41.5
OMNI-LOS	-18.1	-24.5	-6.5	-12.3	-31.1	-40.4
Recover from SF attack						
INCURE-LOS	+18.8	+33.3	+3	+11.8	+55.3	+75.8
OMNI-LOS	+11.7	+23.8	+1.1	+5	+35.5	+40
DoS on overhearing						
INCURE-LOS	+57.5	+140.8	+87.7	+169.7	+1.2	+49.3
OMNI-LOS	+117.4	+204	+121	+193.1	+81.8	+195.1
Continuous DoS						
INCURE-LOS	+125.4	+204.3	+204	+349.3	+35.9	+109.7
OMNI-LOS	+130	+189.4	+142	+202.3	+78.7	+184.3
Recover from DoS attack						
INCURE-LOS	-49	-64.5	-61.2	-71.8	-24.2	-53.9
OMNI-LOS	-50.8	-57	-53.6	-56.3	-44.5	-58.3
Ext DoS and recovery						
INCURE-LOS	+130.8	+172.2	+139.1	+150.3	+50	+81.7
OMNI-LOS	+57.3	+38.3	+41.2	+93.9	+53.5	+68.8

In terms of resilience (Table 59), the evaluation aims to indicate if recovery measures can minimize the initialization of the DoS attack that occurs based on an overhearing case. Recovery measures are also evaluated if they can empower nodes to restore and retain their communication and packet delivery ability after recovery is applied. When the malicious

nodes execute a static attack strategy, INCURE presents a higher resilience than OMNI in terms of recovering the network's packet delivery capability. As active route paths are updated to address the selective forwarding attack and exclude the malicious nodes that participate on active route paths, communication is increased leading to collisions, packet drops and retransmissions. INCURE nodes can update to new route paths with less communication effort and achieve a higher increase percentage of packet delivery (up to 97% compared to 77% at OMNI case) as the directional communication incurs less interference, collisions, and packet retransmissions than the omni-directional communication. In the case of recovering from a DoS attack, INCURE recovers its packet delivery by a 27% increase percentage while the low duty cycle implemented by OMNI nodes affects the network's ability to communicate considerably; OMNI decreases its packet delivery by 16%. When considering a persistent attack strategy, INCURE shows a significant gain over OMNI with regards to minimizing the ability of malicious nodes to eavesdrop on the communication (up to 97% less eavesdropped packets than the OMNI case) and compromise nodes (up to 36% less nodes compromised). The higher resilience of INCURE against eavesdropping permits the nodes to address the case of reactive malicious nodes that execute a DoS attack based on overhearing. Since less malicious nodes are triggered to execute the attack compared to the OMNI case, INCURE achieves to minimize the attack outcome on the network's energy consumption and packet delivery.

Table 59: Resilience evaluation – LOS increase/decrease % of performance of INCURE over OMNI

RESILIENCE (Ref. Table 15, Table 25)			
Packet delivery increase/decrease %	Topology		
	Sparse	Dense	Grid
Static attack strategy	Malicious nodes		
	5%	10%	
Packet delivery – Recover from SF attack			

INCURE-LOS	+59.2	+97
OMNI-LOS	+49.5	+76.8
Packet delivery – Recover from DoS attack		
INCURE-LOS	+15	+27.3
OMNI-LOS	-7.7	-15.5

RESILIENCE (Ref. Table 38, Table 39, Table 40, Table 42)						
Increase/decrease %	Topology					
	Sparse		Dense		Grid	
Persistent attack strategy	Malicious nodes					
	5%	10%	5%	10%	5%	10%
Eavesdropped packets						
INCURE-LOS % gain over OMNI-LOS (in terms of less eavesdropped packets)	+82.8	+79.5	+80	+74.4	+96.6	+92.1
Compromised nodes due to eavesdropping						
INCURE-LOS % gain over OMNI-LOS (in terms of less % of compromised nodes)	+20.4	+32.5	+21.9	+35.8	+14.2	+20.9
Energy consumption on DoS based on overhearing						
INCURE-LOS	+57.5	+140.8	+87.7	+169.7	+1.2	+49.3
OMNI-LOS	+117.4	+204	+121	+193.1	+81.8	+195.1
Packet delivery on DoS based on overhearing						
INCURE-LOS	-1.4	-3.3	-6.3	-11.7	+0.1	+3.5
OMNI-LOS	-11.8	-25.8	-17.5	-33.1	-17.7	-27.1

In terms of reliability, the assessment aims to indicate if the network's packet delivery capability can be restored when nodes apply recovery. As it can be observed in Table 60 both INCURE and OMNI networks can recover the packet delivery when recovering from a selective forwarding attack. However, in the case of recovering from a DoS attack, the OMNI case cannot restore the packet delivery as nodes enter a low duty cycle mode and are turned unavailable. OMNI grid presents the highest decrease percentage of packet delivery due to the

low duty cycle measure. This occurs as the grid topology is sensitive to connectivity disruptions due to the low neighbor density that limits the ability of the network to maintain stable routing as more nodes turn unavailable due to an attack or the recovery countermeasures. Overall, INCURE recovers the network's communication and packet delivery ability as it isolates malicious nodes more effectively, allowing the network to protect its connectivity for as long as possible as the attack strategy continuous.

Table 60: Reliability evaluation – LOS Packet delivery increase/decrease %

RELIABILITY (Ref. Table 15, Table 23)		
Packet delivery increase/decrease %	Topology	
	Grid	
Static attack strategy	Malicious nodes	
	5%	10%
Recover from SF attack		
INCURE-LOS	+59.2	+97
OMNI-LOS	+49.5	+76.8
Recover from DoS attack		
INCURE-LOS	+15	+27.3
OMNI-LOS	-7.7	-15.5

RELIABILITY (Ref. Table 34, Table 48, Table 55)						
Packet delivery increase/decrease %	Topology					
	Sparse		Dense		Grid	
Persistent attack strategy	Malicious nodes					
	5%	10%	5%	10%	5%	10%
Recover from SF attack						
INCURE-LOS	+22.5	+37.5	+6.2	+25	+58.1	+84.6
OMNI-LOS	+22.1	+31.8	+6.6	+10.3	+49.5	+76.8
Recover from DoS attack						
INCURE-LOS	+5.7	+3.1	+5.5	+12.2	+8.9	+3.4
OMNI-LOS	-16	-29.9	-22.2	-27.1	-24	-41.8

Ext DoS and recovery						
INCURE-LOS	-22	-25.2	-17.5	-25	-7.2	-9.6
OMNI-LOS	-13.1	-3.7	-4.5	-0.3	-10.3	-1

Table 61 presents results related to the responsiveness requirement. Responsiveness evaluation will indicate if the network can perform its tasks when recovery is applied to address security attacks. We are interested in observing the network's packet delivery capability along the network's response time to deliver observations to the control center, under attack conditions and when recovery is applied. Overall, INCURE achieves better responsiveness than OMNI, whether we are considering security attacks or recovery. INCURE achieves a higher resilience to attacks, prohibiting malicious nodes that persist with their intrusion strategy from severely affecting the network's responsiveness. Thus, INCURE nodes are able to respond effectively and propagate their observations to the control center. OMNI can only improve the network's responsiveness when considering the selective forward attack. However, OMNI cannot effectively address a persistent intrusion strategy and thus the network's responsiveness, in terms of packet delivery, is greatly affected. The networks' response time to deliver observations to the control center is affected by the packets successfully delivered. The path quality over which the delivered packets are routed affects the packet delivery delay. Moreover, the attack type influences delay in different ways. Delay is increased when nodes recover from the selective forwarding attack as active route paths are updated to exclude malicious nodes and turn the attack ineffective. In most of the cases, OMNI presents a higher increase percentage of delay from its reference scenario than what INCURE presents when recovering from the selective forwarding attack, as the packets successfully delivered experience more collisions and retransmissions. In the dense topology, OMNI presents less increase percentage of delay compared to INCURE as it achieves a higher node density that allows it to discover shorter route paths. Even so, INCURE recovers considerably more packet delivery than OMNI. In terms of a DoS attack, the packet delivery delay is increased as malicious nodes force the networks to packet drops and retransmissions.

INCURE presents a lower increase percentage of delay than OMNI as it prohibits malicious nodes from greatly affecting node's operation. Thus, the network's responsiveness, in terms of packet delivery and response time, is higher in comparison to OMNI.

Table 61: Responsiveness evaluation – LOS Packet delivery fraction and delivery delay increase/decrease %

RESPONSIVENESS (Ref. Table 15, Table 16, Table 23, Table 26)			
Packet delivery and delay increase/decrease %		Topology	
		Grid	
Static attack strategy		Malicious nodes	
		5%	10%
SF attack recovery			
Packet delivery	INCURE-LOS	+59.2	+97
	OMNI-LOS	+49.5	+76.8
Packet delivery delay	INCURE-LOS	+14.7	+47
	OMNI-LOS	+52.7	+31.4
DoS attack recovery			
Packet delivery	INCURE-LOS	+15	+27.3
	OMNI-LOS	-7.7	-15.5
Packet delivery delay	INCURE-LOS	-35.1	+13
	OMNI-LOS	+8.2	+11.1

RESPONSIVENESS (Ref. Table 34, Table 35, Table 40, Table 41, Table 44, Table 46, Table 48, Table 50, Table 55)							
Packet delivery and delay increase/decrease %		Topology					
		Sparse		Dense		Grid	
Persistent attack strategy		Malicious nodes					
		5%	10%	5%	10%	5%	10%
SF attack recovery							
Packet delivery	INCURE-LOS	+22.5	+37.5	+6.2	+25	+58.1	+84.6
	OMNI-LOS	+22.1	+31.8	+6.6	+10.3	+49.5	+76.8
Packet delivery delay	INCURE-LOS	+13.5%	+27.7%	+13.7%	+7%	+82%	+97%
	OMNI-LOS	+25.8%	+33.5%	+6.3%	-6%	+52.8%	+31.4%
DoS on overhearing							

Packet delivery	INCURE-LOS	-1.4%	-3.3%	-6.3%	-11.7%	+0.1%	+3.5%
	OMNI-LOS	-11.8%	-25.8%	-17.5%	-33.1%	-17.7%	-27.1%
Packet delivery delay	INCURE-LOS	+29.2%	+23.6%	+13.1%	-8.2%	-4.8%	-23.7%
	OMNI-LOS	+34.5%	+38.6%	+12.2%	+22.5%	+29.3%	+22.6%
Continuous DoS							
Packet delivery	INCURE-LOS	-12.6%	-9%	-10%	-19.8%	-7.2%	-5.4%
	OMNI-LOS	-16.6%	-24.2%	-18.3%	-30%	-17.4%	-25%
Packet delivery delay	INCURE-LOS	+30.7%	+26.8%	+10.4	+3.1	+15.3	+11.5
	OMNI-LOS	+44.2%	+26%	+47.4	+13.8	+19.8	+16.1
DoS attack recovery							
Packet delivery	INCURE-LOS	+5.7	+3.1	+5.5	+12.2	+8.9	+3.4
	OMNI-LOS	-16	-29.9	-22.2	-27.1	-24	-41.8
Packet delivery delay	INCURE-LOS	+10.6%	+8.5%	+4.1%	+16.1%	+5%	-15.2%
	OMNI-LOS	+2.5%	+7.5%	+13.8%	+21.7%	-10%	+25.5%
Ext DoS attack and recovery							
Packet delivery	INCURE-LOS	-22	-25.2	-17.5	-25	-7.2	-9.6
	OMNI-LOS	-13.1	-3.7	-4.5	-0.3	-10.3	-1
Packet delivery delay	INCURE-LOS	+130.8%	+172.2%	+139.1%	+150.3%	+50%	+81.7%
	OMNI-LOS	+57.3%	+38.3%	+41.2%	+93.9%	+53.5%	+68.8%

In terms of self-healingness, a dedicated table summarizing results is omitted as the evaluation metrics utilized for the self-healingness requirement have been covered by the other intrusion recovery requirements and their respective evaluation tables (Table 57 - Table 61). Both INCURE and OMNI demonstrate a self-healing ability, addressing different attack situations as malicious nodes adapt their attack strategy in an effort to compromise the networks' operation. However, INCURE is able to self-heal with a small tradeoff in terms of compromised nodes due to recovery while achieving an overall stable network performance. OMNI self-heals well in terms of survivability, however, with a high overhead in terms of network's availability and reliability.

5.3.2 Shadowing

This section considers a deployment scenario where shadowing occurs due to objects in the environment that obstruct the propagation path between the transmitting and receiving nodes. Shadowing leads to reduced received signal power when compared to the LOS case. The log-normal shadowing model is a classic path loss propagation model that is utilized by researchers in order to evaluate their protocols' performance when shadowing conditions are considered. As discussed in section APPENDIX A, the development of a shadowing model is typically based on field measurements which derive the path loss exponent and standard deviation parameters of the respective shadowing model. This evaluation is not intended to cover all possible environments and conditions. It aims to assess scenarios characterized by the specific path loss exponent and standard deviation. An obstructed scenario is considered to be simulated with a path loss exponent of 3.0 and a standard deviation of 4.0 [103, 124, 125, 126, 127, 128]. The objective of this assessment is to investigate the proposed countermeasure's and typical recovery solutions' applicability and how these are affected when considering the variance of the path loss, induced by the shadowing effect and its variability, at a transmitter – receiver pair. First, normal network conditions are simulated. Then, comparisons are made when recovery is applied in order to address the selective forwarding, eavesdropping and DoS attacks.

Initially, both random and grid topologies have been considered. Simulation results have shown that shadowing conditions can affect the networks as a number of sensors cannot establish routing paths to the sink, as the average path loss is increased by 20 dB (when compared to the respective LOS scenarios) affecting node connectivity and leading to low network performance. Different solutions are proposed in the literature in order to overcome the increased path loss due to the shadowing, such as deploying more sensor nodes [5] or increasing the transmission power [129]. It is assumed that before a real WSN is deployed, simulations and/or field measurements will be performed to aid network designers to adjust

the network operating conditions accordingly, in order to achieve good network performance. Since initial simulations have indicated poor network performance, the transmission power increase solution is applied to account for the 20 dB loss due to the shadowing effect. Sensor nodes are configured to transmit 20 dB more from their equivalent LOS scenarios. Although the power was adjusted to compensate for the increase in the average path loss, the shadowing loss variability is not adjusted and is expected to influence the network evaluation accordingly. INCURE nodes transmit with -4 dBm while OMNI nodes transmit with 12dBm in order to achieve an equivalent setup. In the case of the OMNI network a high power sensor node needs to be considered, i.e. [130], however, the power consumption is much higher than low power sensors. A transmit power consumption of 85mA [130] is considered at OMNI case in comparison to the 14mA consumption considered [131] at the INCURE case. The high power sensor in [130] also utilizes higher energy consumption for reception (30mA). Low power sensors as in [131] utilize much lower energy consumption for reception (19mA). It is obvious that low power sensors outperform the high power sensors in terms of energy consumption. Following, we present the evaluation results relevant to the 750x750, 550x550 and 1000x1000 topologies. The reported results are averaged over 30 simulation runs for each attack/recovery-related INCURE/OMNI setup/scenario (section 5.2.1).

5.3.2.1 Persistent, adaptive or reactive attack strategy

In the case of the 750x750 topology, when shadowing and normal network conditions are considered, the packet delivery (Table 62) is decreased 1.5% for INCURE scenarios when compared to the equivalent LOS scenarios where an unobstructed propagation path between a transmitting and receiving nodes was considered. OMNI yields 1% more packet delivery for the same scenario. In the case of the 550x550 topology, INCURE yields 83% (5% less from the LOS scenario) and OMNI 80% (6% more from the LOS scenario) packet delivery. In the case of the grid topology, INCURE achieves 81% packet delivery which is 16% less than then

equivalent LOS scenario. OMNI decreases its packet delivery by only 2% on the grid, yielding a total of 87%. The variation on packet delivery occurs as the randomness factor of the shadowing model affects network communication differently. Some of the sensors have lost connectivity with their neighbors affecting the establishment and utilization of the routing paths. Moreover, there are nodes that have established communication with distant nodes due to smaller path losses because of the variability of the shadowing model. There are cases where a decrease of neighbors at a node can benefit the network. Often, a large number of neighbors can lead to more overhearing and energy consumption, more packet loss and retransmissions, affecting the network's performance. Fewer neighbors at nodes, reducing a dense area, may help the network to increase its performance (as in the case of OMNI 550x550 topology). However, fewer neighbors in sparse areas may negatively affect the network performance as nodes may not converge easily to routing and establish stable network connections (as in the case of INCURE 1000x1000 topology). Connectivity disruptions also affect the packet delivery delay (Table 62). For example, packet delivery delay may be increased if nodes have to retransmit a large number of lost packets or forward packets over long route paths. INCURE 1000x1000 case and the OMNI 750x750 case yield more packet delivery delay when compared to the equivalent LOS case as connectivity disruptions lead to more efforts to converge to stable routing affecting delay. In the case of INCURE 550x550 topology, there is less packet delivery delay when compared to the equivalent LOS case as active route paths experience less overhearing, collisions and retransmissions. In the case of OMNI 550x550 case, the packet delivery delay is slightly increased as some of the active paths utilize longer routes as node connections are lost due to the shadowing. The OMNI 1000x1000 case shows a lower packet delivery delay level when compared to the LOS case. This occurs as the connectivity disruption on the grid due to the shadowing benefits the OMNI network in terms of fewer collisions, retransmissions, overhearing and routing overhead, aiding the network to converge and maintain a stable routing operation when compared to the LOS case. As the transmission power was previously

increased in order to re-enforce the network performance, the energy consumption is significantly higher in the OMNI network than the energy consumption for the INCURE case.

Table 62: NLOS normal network conditions - normal network conditions scenario

Overall evaluation		Topology		
		Sparse	Dense	Grid
Compromised nodes (%)	INCURE (I)	0%	0%	0%
	OMNI (O)	0%	0%	0%
Gain		**0%**	**0%**	**0%**
Packet delivery (%)	INCURE (I)	92.1	83	81.2
	OMNI (O)	86.9	80.1	87
Gain		**5.9% (I)**	**3.6% (I)**	**7.1% (O)**
Energy consumption (mJ)	INCURE (I)	101.3	113.1	123.2
	OMNI (O)	727.8	744.8	617.8
Gain		**86% (I)**	**84.8% (I)**	**80% (I)**
Packet delay (ms)	INCURE (I)	66.9	32.2	213
	OMNI (O)	85.4	36.6	209.5
Gain		**21.6% (I)**	**12% (I)**	**1.6% (O)**

During the occurrence and propagation of critical observations by the sensor nodes, the malicious nodes execute the selective forwarding attack. As long the malicious nodes can participate on active route paths the attack can be successful. Compromised nodes (Table 63) exist in both networks as the malicious nodes compromise their ability to send data towards the sink with the selective forwarding attack. Moreover, as malicious nodes increase, they have more chances to affect the network operation. The packet delivery capability of both

networks is decreased (Table 63). INCURE 750x750 yields a packet delivery decrease percentage of 20% and 34% and the OMNI 750x750 decreases by 21% and 44% when compared to their equivalent reference scenarios and considering 5% and 10% malicious nodes. In the INCURE case, there are slightly less malicious nodes participating in active paths when compared to the LOS scenarios. The same observation applies in the case of OMNI with 5% malicious nodes. In the case of 550x550 topologies, malicious nodes have fewer chances to be selected as the next hop due to higher density and thus they affect less the packet delivery capability of the network. Both INCURE and OMNI show a packet delivery decrease percentage of about 10% when considering 5% malicious nodes. In the case of 10% malicious nodes, OMNI has a higher decrease percentage of packet delivery as there are more active malicious nodes performing the selective forwarding attack. At the grid topology, compromised nodes have been slightly increased when compared to the LOS case as some of the malicious nodes have increased their chances to be selected as next hops. This occurs as some of the neighbors of malicious nodes discover fewer neighbors due to the extra shadowing loss and thus increase the chances of malicious nodes to participate on active route paths. The packet delivery (Table 63) is significantly decreased at the grid OMNI and INCURE cases as malicious nodes launch the selective forwarding attack. As the packet delivery is decreased due to the attack, the energy consumption (Table 63) that is reported is less as well. Moreover, the selective forwarding attack affects the end-to-end packet delivery delay (Table 63). The end-to-end packet delivery delay is depended on the route paths that are utilized by the packets successfully delivered to the sink. For example, the packet successfully delivered to the sink may use longer route paths or experience more retransmissions when compared to another scenario. Due to the aforementioned reasons, the reported end-to-end packet delivery delay is shown to either increase or decrease from the respective reference scenarios.

Table 63: NLOS selective forwarding attack – Overall performance increase/decrease % from NLOS normal network conditions (R) scenario

Overall evaluation			Topology								
			Sparse			Dense			Grid		
			R	S	**I/D**	R	S	**I/D**	R	S	**I/D**
Compromised nodes (%) due to attack [1]	INCURE (I)	5%	0%	1.8%	+1.8%	0%	0.8%	+0.8%	0%	3.2%	+3.2%
		10%	0%	2.7%	+2.7%	0%	1.5%	+1.5%	0%	4.1%	+4.1%
	OMNI (O)	5%	0%	1.7%	+1.7%	0%	0.7%	+0.7%	0%	3.1%	+3.1%
		10%	0%	3.1%	+3.1%	0%	1.8%	+1.8%	0%	3.9%	+3.9%
Gain		**5%**		**0.1% (O)**			**0.1% (O)**			**0.1% (O)**	
		10%		**0.4% (I)**			**0.3% (I)**			**0.2% (O)**	
Packet delivery (%) [2]	INCURE (I)	5%	92.1	73.5	-20.2%	83	75.2	-9.3%	81.2	43.7	-46.1%
		10%	92.1	61	-33.7%	83	64.8	-21.9%	81.2	32.3	-60.2%
	OMNI (O)	5%	86.9	68.8	-20.8%	80.1	72	-10.1%	87	45.3	-47.9%
		10%	86.9	48.6	-44%	80.1	59.1	-26.2%	87	36.5	-58%
Gain		**5%**		**6.8% (I)**			**4.4% (I)**			**3.6% (O)**	
		10%		**25.5% (I)**			**9.6% (I)**			**13% (O)**	
Energy consumption (mJ) [3]	INCURE (I)	5%	101.3	90.7	-10.4%	113.1	107.7	-4.7%	123.2	84.8	-31.1%
		10%	101.3	88.1	-13%	113.1	104.7	-7.4%	123.2	71.4	-42%
	OMNI (O)	5%	727.8	616.6	-15.2%	744.8	670.5	-9.9%	617.8	432.4	-30%
		10%	727.8	510.7	-29.8%	744.8	606.2	-18.6%	617.8	358.3	-42%
Gain		**5%**		**85.2% (I)**			**83.9% (I)**			**80.3% (I)**	
		10%		**82.7% (I)**			**82.7% (I)**			**80% (I)**	
Packet delay (ms) [4]	INCURE (I)	5%	66.9	58.9	-11.9%	32.2	29.7	-7.7%	213	305.2	+43.2%
		10%	66.9	53.7	-19.7%	32.2	29.1	-9.6%	213	411	+92.9%

	OMNI (O)	5%	85.4	79.1	-7.3%	36.6	32.3	-11.7%	209.5	288	+37.4%
		10%	85.4	94.1	+10.1%	36.6	32	-12.5%	209.5	248.3	+18.5%
Gain		**5%**		**25.5% (I)**			**8% (I)**			**5.6% (O)**	
		10%		**42.9% (I)**			**9% (I)**			**39.5% (O)**	
Note	[1]		Figure 58 (page 249), Figure 63 (page 250), Figure 68 (page 252)								
	[2]		Figure 59 (page 249), Figure 64 (page 251), Figure 69 (page 252)								
	[3]		Figure 60 (page 249), Figure 65 (page 251), Figure 70 (page 253)								
	[4]		Figure 61 (page 250), Figure 66 (page 251), Figure 71 (page 253)								

The compromised network operation is restored as soon as the networks apply their recovery measures. Packet delivery (Table 64) is increased in all cases. Both networks present a higher packet delivery increase percentage at the grid case since there more active route paths affected by the attack and recovered by each network. However, both networks overall present the least packet delivery at the grid case as shadowing affects nodes connectivity considerably. INCURE presents 59% packet delivery and OMNI 67% at the grid when considering 10% malicious nodes (Figure 22). OMNI shows more packet delivery than INCURE as the average node connectivity is less at the INCURE case, 2.8, where OMNI retains an average node connectivity of 3.1. At the other topologies, INCURE presents a higher packet delivery than OMNI as there are less retransmissions and routing overhead. Compromised nodes (Table 64) are recovered and no further nodes are compromised due to the recovery measures. Energy consumption (Table 64) is increased in all cases as route paths are updated to exclude the active malicious nodes. The same observation applies for the packet delivery delay as sensors update the active route paths to exclude the active malicious nodes. Both networks retain a lower end-to-end packet delivery delay at the 550x550 case (Table 64) since there are less affected route paths that need to be recovered when compared to the other cases.

Table 64: NLOS selective forwarding recovery – Overall performance increase/decrease % from NLOS selective forwarding attack (R) scenario

Overall evaluation			Topology								
			Sparse			Dense			Grid		
			R	S	**I/D**	R	S	**I/D**	R	S	**I/D**
Compromised nodes (%) [1] due to recovery	INCURE (I)	5%		0%	0%		0%	0%		0%	0%
		10%		0%	0%		0%	0%		0%	0%
	OMNI (O)	5%		0%	0%		0%	0%		0%	0%
		10%		0%	0%		0%	0%		0%	0%
Gain		**5%**		**0%**			**0%**			**0%**	
		10%		**0%**			**0%**			**0%**	
Packet delivery (%) [2]	INCURE (I)	5%	73.5	85.9	+16.8%	75.2	81.3	+8.1%	43.7	67.8	+55.1%
		10%	61	80	+31.1%	64.8	77.4	+19.4%	32.3	58.8	+82%
	OMNI (O)	5%	68.8	81.1	+17.8%	72	76.8	+6.6%	45.3	69.4	+53.2%
		10%	48.6	73.1	+50.4%	59.1	73.2	+23.8%	36.5	67.5	+84.9%
Gain		**5%**		**5.9% (I)**			**5.8% (I)**			**2.3% (O)**	
		10%		**9.4% (I)**			**5.7% (I)**			**14.7% (O)**	
Energy consumption (mJ) [3]	INCURE (I)	5%	90.7	106.5	+17.4%	107.7	117.6	+9.2%	84.8	122.2	+44.1%
		10%	88.1	115.4	+30.9%	104.7	119.9	+14.5%	71.4	109.2	+52.9%
	OMNI (O)	5%	616.6	669.4	+8.5%	670.5	676.7	+1%	432.4	562.1	+29.9%
		10%	510.7	582.6	+14%	606.2	641.9	+5.8%	358.3	538.7	+50.3%
Gain		**5%**		**84% (I)**			**82.6% (I)**			**78.2% (I)**	
		10%		**80.1% (I)**			**81.3% (I)**			**79.7% (I)**	
Packet delay (ms) [4]	INCURE (I)	5%	58.9	75.4	+28%	29.7	31.7	+6.7%	305.2	301.6	-1.2%
		10%	53.7	71.1	+32.4%	29.1	33	+13.4%	411	215.1	-47.6%

	OMNI (O)	5%	79.1	109.6	+38.5%	32.3	32.9	+1.8%	288	382.1	+32.6%
		10%	94.1	82.2	-12.6%	32	31	-3.1%	248.3	231.9	-6.6%
Gain		**5%**		**31.2% (I)**			**3.6% (I)**			**21% (I)**	
		10%		**13.5% (I)**			**6% (O)**			**7.2% (I)**	
Note	[1]	Figure 58 (page 249), Figure 63 (page 250), Figure 68 (page 252)									
	[2]	Figure 59 (page 249), Figure 64 (page 251), Figure 69 (page 252)									
	[3]	Figure 60 (page 249), Figure 65 (page 251), Figure 70 (page 253)									
	[4]	Figure 61 (page 250), Figure 66 (page 251), Figure 71 (page 253)									

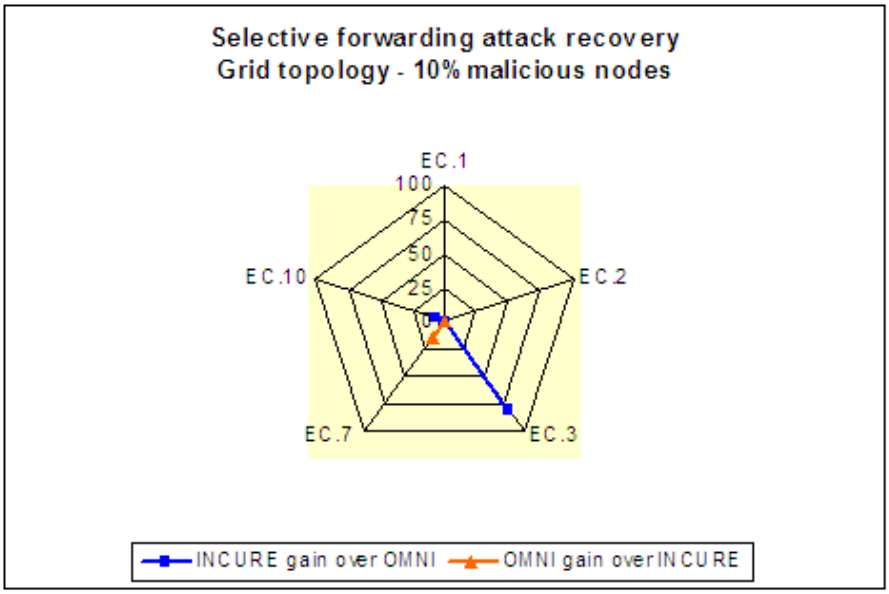

Figure 22: Persistent attack strategy NLOS – selective forwading recovery gain

After recovery measures are applied, the malicious nodes eavesdrop on the network communication and if they can overhear, they deploy a DoS attack. The eavesdropping capability of the malicious nodes is decreased (Table 65) in most of the scenarios when compared to the equivalent LOS scenario. The extra shadowing loss, compared to LOS scenarios, affects the ability of the malicious nodes to receive some of the signals since the transmitted signals do not reach the malicious receivers due to the path loss. INCURE decreases more the ability of the malicious nodes to overhear when compared to the equivalent OMNI scenarios (Figure 23). The malicious nodes have more chances to overhear

when the node density is higher (Table 65). Both networks present the highest decrease packet delivery percentage at the 550x550 case (Table 65) as eavesdropping is more effective in comparison to the other topologies. Therefore, there are more malicious nodes at the INCURE and OMNI 550x550 case launching the DoS attack when compared to the other topologies. Due to the higher number of active malicious nodes and due to the higher node density, there are more sensors affected at the 550x550 topology (Table 65) when compared to the other topologies. There are 17% and 33% compromised nodes due to eavesdropping attack at INCURE, and 30% and 53% at OMNI when considering 5% and 10% malicious nodes respectively. The grid presents the least number of compromised nodes as the node density is very low, thus malicious nodes affect fewer nodes. OMNI demonstrates more compromised nodes in all cases when compared to the INCURE as the omni-directional transmission promotes overhearing, thus there are more active malicious nodes launching the DoS attack and affecting nodes' operation. INCURE presents from 13% to 26% less compromised nodes when compared to the OMNI case. Overall, end-to-end packet delivery delay (Table 65) is increased as packet loss and retransmissions occur. The energy consumption (Table 65) is considerably increased in all cases as the DoS attack leads to a large number of packets to be retransmitted, occurs more overhearing and network communication.

Table 65: NLOS DoS triggered by eavesdropping – Overall increase/decrease % performance from NLOS selective forwarding recovery (R) scenario

Overall evaluation			Topology								
			Sparse			Dense			Grid		
			R	S	**I/D**	R	S	**I/D**	R	S	**I/D**
Compromised nodes (%) due to eavesdropping [1]	INCURE (I)	5%	0%	8.2%	+8.2%	0%	17.2%	+17.2%	0%	2.5%	+2.5%
		10%	0%	17.2%	+17.2%	0%	32.8%	+32.8%	0%	5.4%	+5.4%
	OMNI (O)	5%	0%	25.6%	+25.6%	0%	30.3%	+30.3%	0%	15.9%	+15.9%
		10%	0%	42.9%	+42.9%	0%	52.9%	+52.9%	0%	29.5%	+29.5%

Gain		**5%**		**17.4% (I)**			**13.1% (I)**			**13.4% (I)**	
		10%		**25.7% (I)**			**20.1% (I)**			**24.1% (I)**	
Eavesdropped packets (#) [2]	INCURE (I)	5%		523			782			159	
		10%		984			1765			293	
	OMNI (O)	5%		2842			2063			2021	
		10%		4189			4485			3287	
Gain		**5%**		**81.5% (I)**			**62% (I)**			**92.1% (I)**	
		10%		**76.5% (I)**			**60.6% (I)**			**91% (I)**	
Packet delivery (%) [3]	INCURE (I)	5%	85.9	82.7	-3.7%	81.3	73.9	-9.1%	67.8	65.5	-3.3%
		10%	80	73.3	-8.3%	77.4	63	-18.6%	58.8	56.4	-4%
	OMNI (O)	5%	81.1	72.6	-10.4%	76.8	65.1	-15.2%	69.4	52.9	-23.7%
		10%	73.1	56.4	-22.8%	73.2	48.2	-34.1%	67.5	46.4	-31.2%
Gain		**5%**		**13.9% (I)**			**13.5% (I)**			**23.8% (I)**	
		10%		**29.9% (I)**			**30.7% (I)**			**21.5% (I)**	
Energy consumption (mJ) [4]	INCURE (I)	5%	106.5	197.3	+85.2%	117.6	321.2	+173.1%	122.2	139.1	+13.8%
		10%	115.4	310.8	+169.3%	119.9	466.6	+289.1%	109.2	162.1	+48.4%
	OMNI (O)	5%	669.4	1178.7	+76%	676.7	1274.5	+88.3%	562.1	905.5	+61%
		10%	582.6	1492.6	+156.1%	641.9	1672.4	+160.5%	538.7	1185.8	+120.1 %
Gain		**5%**		**83.2% (I)**			**74.7% (I)**			**84.6% (I)**	
		10%		**79.1% (I)**			**72% (I)**			**86.3% (I)**	
Packet delay (ms) [5]	INCURE (I)	5%	75.4	81.2	+7.6%	31.7	40	+26.1%	301.6	280.3	-7%
		10%	71.1	95.8	+34.7%	33	39.4	+19.3%	215.1	243.9	+13.3%
	OMNI (O)	5%	109.6	154	+40.5%	32.9	36	+9.4%	382.1	371	-3%
		10%	82.2	91.4	+11.1%	31	45.2	+45.8%	231.9	318.4	+37.3%
Gain		**5%**		**47.2% (I)**			**10% (O)**			**24.4% (I)**	

		10%		4.5% (O)			12.8% (I)			23.3% (I)	
Note	[1]	Figure 58 (page 249), Figure 63 (page 250), Figure 68 (page 252)									
	[2]	Figure 62 (page 250), Figure 67 (page 252), Figure 72 (page 253)									
	[3]	Figure 59 (page 249), Figure 64 (page 251), Figure 69 (page 252)									
	[4]	Figure 60 (page 249), Figure 65 (page 251), Figure 70 (page 253)									
	[5]	Figure 61 (page 250), Figure 66 (page 251), Figure 71 (page 253)									

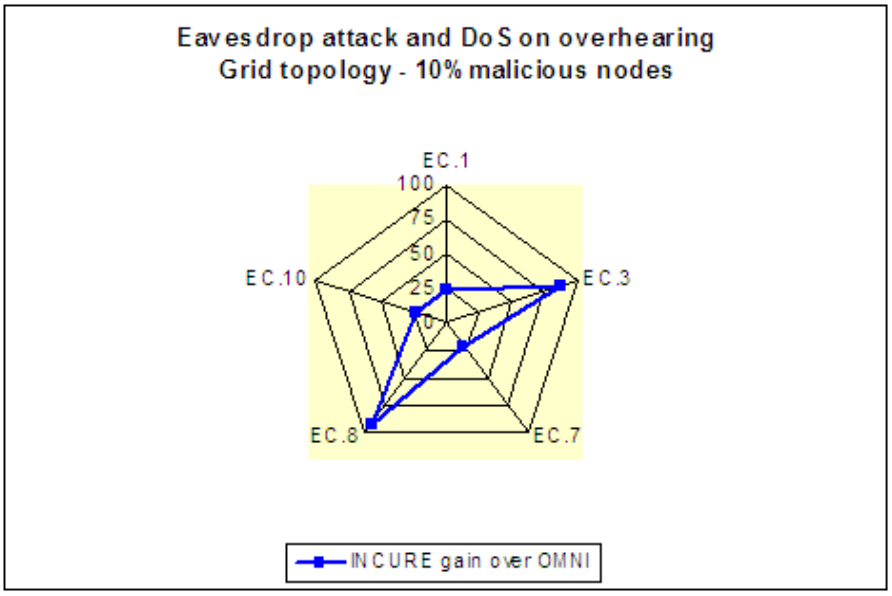

Figure 23: Persistent attack strategy NLOS – eavesdrop and DoS on overhearing performance gain

The malicious nodes adapt their attack strategy and deploy a continuous DoS attack, affecting the networks' operation. The effect of the DoS attack happens at different granularities, depending on the ability of the malicious nodes to affect active route paths. This ability is affected by the path loss between each link. As depicted in Table 66, packet delivery is decreased more as malicious nodes increase. Both networks present the least packet delivery at the grid as the low network connectivity that occurs due to shadowing, is affecting network's performance more due to the DoS attack. INCURE yields 62% and 52% and OMNI 57% and 45% packet delivery when considering 5% and 10% malicious nodes respectively at the grid case. Previously, INCURE demonstrated a packet delivery of 75% and 69% and

OMNI 60% and 51% packet delivery when considering 5% and 10% malicious nodes at the grid LOS case. The higher node density at the grid LOS case helped the networks to retain a higher packet delivery percentage during the DoS attack. The DoS attack compromises the operation of a number of nodes at both networks. Both networks present the highest number of compromised nodes at the 550x550 case (Table 66) as the node density is higher when compared to the other topologies, thus malicious nodes can affect more nodes. The grid presents the least number of compromised nodes (Table 66) as the node density is much less when compared to the other topologies. OMNI presents more compromised nodes when compared to INCURE as the higher density that is achieved at OMNI cases permits the malicious nodes to compromise the operation of more nodes. INCURE presents from 6% to 22% less compromised nodes when compared to OMNI. Overall, the increase percentage of compromised nodes is lower at the shadowing cases when compared to the equivalent LOS scenarios. This occurs as some of the malicious nodes have fewer neighbors due to shadowing, thus they affect less nodes when compared to the LOS case. The energy consumption (Table 66) is also increased as malicious nodes increase in the network and affect more nodes. At the OMNI case the network communication is very expensive in terms of energy consumption [130] as it requires considerably more transmission and reception power as discussed previously, than the INCURE case. Due to this, the DoS outcome in terms of energy consumption is more severe in the OMNI case, thus affecting more the survivability of the network. Moreover, the end-to-end packet delivery delay (Table 66) is affected as the attack causes packet drops at the receivers, breaking communication links and forcing a large number of packets to be retransmitted.

Table 66: NLOS DoS attack – Overall performance increase/decrease % from NLOS selective forwarding recovery (R) scenario

Overall evaluation	Topology		
	Sparse	Dense	Grid

			R	S	**I/D**	R	S	**I/D**	R	S	**I/D**
Compromised nodes (%) due to attaclk [1]	INCURE (I)	5%	0%	13.5%	+13.5%	0%	25.4%	+25.4%	0%	6.8%	+6.8%
		10%	0%	21.7%	+21.7%	0%	39.4%	+39.4%	0%	12.7%	+12.7%
	OMNI (O)	5%	0%	25.1%	+25.1%	0%	31.7%	+31.7%	0%	16.4%	+16.4%
		10%	0%	43.2%	+43.2%	0%	58.8%	+58.8%	0%	30.7%	+30.7%
Gain		**5%**		**11.6% (I)**			**6.3% (I)**			**9.6% (I)**	
		10%		**21.5% (I)**			**19.4% (I)**			**18% (I)**	
Packet delivery (%) [2]	INCURE (I)	5%	85.9	79.5	-7.4%	81.3	68.3	-15.9%	67.8	62.4	-7.9%
		10%	80	67.2	-16%	77.4	64.3	-16.9%	58.8	52.1	-11.3%
	OMNI (O)	5%	81.1	70.2	-13.4%	76.8	62.8	-18.2%	69.4	57	-17.8%
		10%	73.1	54	-26.1%	73.2	46.9	-35.9%	67.5	44.7	-33.7%
Gain		**5%**		**13.2% (I)**			**8.7% (I)**			**9.4% (I)**	
		10%		**24.4% (I)**			**37.1% (I)**			**16.5% (I)**	
Energy consumption (mJ) [3]	INCURE (I)	5%	106.5	263.9	+147.7%	117.6	413	+251.1%	122.2	177.2	+45%
		10%	115.4	365.8	+216.9%	119.9	578.3	+382.3%	109.2	225.7	+106.6 %
	OMNI (O)	5%	669.4	1226.2	+83.1%	676.7	1305.3	+92.8%	562.1	907.9	+61.5%
		10%	582.6	1434.8	+146.2%	641.9	1650	+157%	538.7	1168.9	+116.9 %
Gain		**5%**		**78.4% (I)**			**68.3% (I)**			**80.4% (I)**	
		10%		**74.5% (I)**			**64.9% (I)**			**80.6% (I)**	
Packet delay (ms) [4]	INCURE (I)	5%	75.4	128.1	69.8%	31.7	35	10.4%	301.6	277	-8.1%
		10%	71.1	118.9	67.2%	33	33.9	2.7%	215.1	281.7	30.9%
	OMNI (O)	5%	109.6	138.4	26.2%	32.9	49.7	51%	382.1	414.8	8.5%
		10%	82.2	94.9	15.4%	31	39.5	27.4%	231.9	352.8	52.1%
Gain		**5%**		**7.4% (I)**			**29.5% (I)**			**33.2% (I)**	
		10%		**20.1% (O)**			**14.1% (I)**			**20.1% (I)**	

Note	[1]	Figure 58 (page 249), Figure 63 (page 250), Figure 68 (page 252)
	[2]	Figure 59 (page 249), Figure 64 (page 251), Figure 69 (page 252)
	[3]	Figure 60 (page 249), Figure 65 (page 251), Figure 70 (page 253)
	[4]	Figure 61 (page 250), Figure 66 (page 251), Figure 71 (page 253)

As soon as the DoS attack is detected, INCURE and OMNI countermeasures are applied. Both solutions allow the network to address the DoS and minimize the energy consumption (Table 67) that occurs due to the attack. Although the low duty cycle at the OMNI case can prolong the network lifetime by prohibiting the malicious nodes to force unnecessary energy consumption, the solution affects the availability of nodes (Table 67). The loss of availability is not desirable in critical WSNs as the packet delivery is considerably decreased. As results demonstrate with the OMNI case, critical events will not be propagated or will be delayed. The INCURE countermeasure incurs minor compromisation of the availability of nodes due to the recovery operation. It is observed that up to 1% of the nodes are compromised when considering 10% malicious nodes. This occurs in 16% of the simulation runs. INCURE yields an insignificant amount of compromised nodes due to the recovery at all cases whereas in the equivalent LOS cases only the random topologies with 10% malicious nodes present compromised nodes. This occurs as the low node density, due to increased path loss, increases nodes' chances to get isolated, due to recovery measures. Moreover, some of the malicious nodes have affected distant nodes, thus recovery is deployed by more nodes. The packet delivery (Table 67) is affected at different granularities as the sensors deploy recovery measures. OMNI decreases its packet delivery at all cases as the low duty cycle affects the operation of many sensor nodes. INCURE increases its packet delivery at the random topologies but decreases it at the grid. Shadowing has affected nodes connectivity at the grid and the lower node density prohibits the network from converging to stable active paths, when compared to the equivalent LOS case. Overall, INCURE retains a higher packet delivery percentage at all cases when compared to the OMNI scenarios. INCURE achieves a recovered packet delivery percentage from 52% to 83% while OMNI presents a percentage of 35% to

59%. Figure 24 presents a snapshot of INCURE's gain over OMNI when considering the grid topology. The end-to-end packet delivery delay (Table 67) is also affected at different granularities. INCURE overall decreases the packet delivery delay as the DoS attack is addressed and new stable active route paths are established to forward packets. The same observation applies at the case of OMNI grid and 550x550 topologies. At the 750x750 topology, OMNI requires more effort to update the active route paths and therefore presents an increase of end-to-end packet delivery delay.

Table 67: NLOS DoS recovery – Overall performance increase/decrease % from NLOS DoS attack (R) scenario

Overall evaluation			Topology								
			Sparse			Dense			Grid		
			R	S	**I/D**	R	S	**I/D**	R	S	**I/D**
Compromised nodes (%) due to recovery [1]	INCURE (I)	5%		0.1%	+0.1%		0.06%	+0.06%		0.03%	+0.03%
		10%		0.16%	+0.16%		0.13%	+0.13%		0.06%	+0.06%
	OMNI (O)	5%		31.5%	+31.5%		42.2%	+42.2%		19.3%	+19.3%
		10%		53.8%	+53.8%		73%	+73%		37.9%	+37.9%
Gain		**5%**		**31.4% (I)**			**42.1% (I)**			**19.2% (I)**	
		10%		**53.6% (I)**			**72.8% (I)**			**37.8% (I)**	
Packet delivery (%) [2]	INCURE (I)	5%	79.5	82.6	+3.8%	68.3	72.2	+5.7%	62.4	59.6	-4.4%
		10%	67.2	72	+7.1%	64.3	67	+4.1%	52.1	52.3	+0.3%
	OMNI (O)	5%	70.2	59.4	-15.3%	62.8	51.9	-17.3	57	43.1	-24.3%
		10%	54	39.4	-27%	46.9	36.3	-22.6	44.7	34.5	-22.8%
Gain		**5%**		**39% (I)**			**39.1% (I)**			**38.2% (I)**	
		10%		**82.7% (I)**			**84.55 (I)**			**51.5% (I)**	

Energy consumption (mJ) [3]	INCURE (I)	5%	263.9	128.8	-51.1%	413	139	-66.3%	177.2	125.9	-28.9%
		10%	365.8	138.8	-62%	578.3	145.1	-74.9%	225.7	110.7	-50.9%
	OMNI (O)	5%	1226.2	771.6	-37%	1305.3	828.3	-36.5%	907.9	529.7	-41.6%
		10%	1434.8	677.4	-52.7%	1650	780.2	-52.7%	1168.9	724.2	-38%
Gain		**5%**		**83.3% (I)**			**83.2% (I)**			**76.2% (I)**	
		10%		**79.5% (I)**			**81.4% (I)**			**84.7% (I)**	
Packet delay (ms) [4]	INCURE (I)	5%	128.1	102.7	-19.8%	35	34.1	-2.5%	277	279.2	+0.7%
		10%	118.9	92.6	-22.1%	33.9	35.8	+5.6%	281.7	269.5	-4.3%
	OMNI (O)	5%	138.4	159.6	+15.3%	49.7	49.4	-0.6%	414.8	334.3	+19.4%
		10%	94.9	103.9	+9.4%	39.5	44.3	+12.1%	352.8	318.5	-9.7%
Gain		**5%**		**35.6% (I)**			**30.9% (I)**			**16.4% (I)**	
		10%		**10.8% (I)**			**19.1% (I)**			**15.3% (I)**	
Note	[1]	Figure 58 (page 249), Figure 63 (page 250), Figure 68 (page 252)									
	[2]	Figure 59 (page 249), Figure 64 (page 251), Figure 69 (page 252)									
	[3]	Figure 60 (page 249), Figure 65 (page 251), Figure 70 (page 253)									
	[4]	Figure 61 (page 250), Figure 66 (page 251), Figure 71 (page 253)									

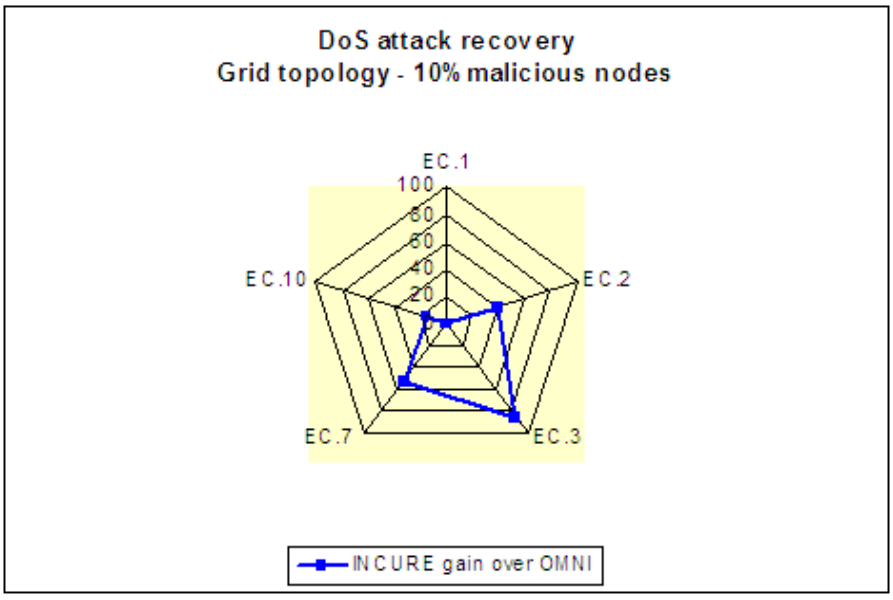

Figure 24: Persistent attack strategy NLOS – DoS attack recovery gain

In the case where an extended DoS attack is executed, the attack outcome happens again at different granularities based on the ability of the malicious nodes to reach sensor nodes, an ability which is affected by the extra path loss of shadowing. Due to this, the malicious nodes that launch the extended DoS affect fewer nodes when compared to the equivalent LOS case. Therefore, fewer nodes apply the recovery measures, presenting less compromised nodes due to recovery when compared to the LOS case. Packet delivery (Table 68) is decreased at all cases as malicious nodes affect more nodes and the affected nodes deploy recovery measures. INCURE achieves higher packet delivery at all cases when compared to the equivalent OMNI scenarios. INCURE presents 48% to 70% packet delivery whereas OMNI yields 32% to 52%. Overall, INCURE retains a higher performance gain over OMNI (Figure 25). The energy consumption (Table 68) is increased at all cases as the malicious nodes increase communication in the network and sensors apply recovery measures to address the attack.

Table 68: NLOS extended DoS and recovery – Overall performance increase/decrease % from NLOS DoS recovery (R) scenario

Overall evaluation			Topology								
			Sparse			Dense			Grid		
			R	S	**I/D**	R	S	**I/D**	R	S	**I/D**
Compromised nodes (%) due to recovery [1]	INCURE (I)	5%	0.1%	1.2%	+1.1%	0.06%	0.7%	+0.6%	0.03%	0.1%	+0.07%
		10%	0.16%	3.8%	+3.6%	0.13%	6%	+5.8%	0.06%	0.2%	+0.14%
	OMNI (O)	5%	31.5%	60%	+28.5%	42.2%	66.7%	+24.5%	19.3%	48.4%	+29.1%
		10%	53.8%	80.8%	+27%	73%	85.9%	+12.9%	37.9%	75%	+37.1%
Gain		**5%**		**58.8% (I)**			**66% (I)**			**48.3% (I)**	
		10%		**77% (I)**			**79.9% (I)**			**74.8% (I)**	
Packet delivery (%) [2]	INCURE (I)	5%	82.6	69.7	-15.6%	72.2	64.3	-10.9%	59.6	53.8	-9.7%
		10%	72	58.1	-19.3%	67	55.3	-17.4%	52.3	47.5	-9.1%

	OMNI (O)	5%	59.4	52.1	-12.2%	51.9	47.9	-7.7%	43.1	39.7	-7.9%
		10%	39.4	37.1	-5.8%	36.3	35.8	-1.3%	34.5	31.8	-7.8%
Gain		**5%**		**33.7% (I)**			**34.2% (I)**			**35.5% (I)**	
		10%		**56.6% (I)**			**54.4% (I)**			**49.3% (I)**	
Energy consumption (mJ) [3]	INCURE (I)	5%	128.8	254.9	+97.9%	139	290.1	+108.7%	125.9	162.3	+28.9%
		10%	138.8	303.7	+118.8%	145.1	339.6	+134%	110.7	179.8	+62.4%
	OMNI (O)	5%	771.6	1095.1	+41.9%	828.3	1146.2	+38.3%	529.7	739.2	+39.5%
		10%	677.4	922.6	+36.1%	780.2	919.6	+17.8%	724.2	1196.1	+65.1%
Gain		**5%**		**76.7% (I)**			**74.6% (I)**			**78% (I)**	
		10%		**67% (I)**			**63% (I)**			**84.95 (I)**	
Packet delay (ms) [4]	INCURE (I)	5%	102.7	114	+11%	34.1	37.4	+9.6	279.2	290.6	+4%
		10%	92.6	89.3	-3.5%	35.8	34.9	-2.5%	269.5	262.4	-2.6%
	OMNI (O)	5%	159.6	140.6	-11.9%	49.4	50.8	+2.8%	334.3	339	+1.4%
		10%	103.9	97.6	-6%	44.3	43	-2.9%	318.5	300.5	-5.6%
Gain		**5%**		**18.9% (I)**			**26.3% (I)**			**14.2% (I)**	
		10%		**8.5% (I)**			**18.8% (I)**			**12.6% (I)**	
Note	[1]	Figure 58 (page 249), Figure 63 (page 250), Figure 68 (page 252)									
	[2]	Figure 59 (page 249), Figure 64 (page 251), Figure 69 (page 252)									
	[3]	Figure 60 (page 249), Figure 65 (page 251), Figure 70 (page 253)									
	[4]	Figure 61 (page 250), Figure 66 (page 251), Figure 71 (page 253)									

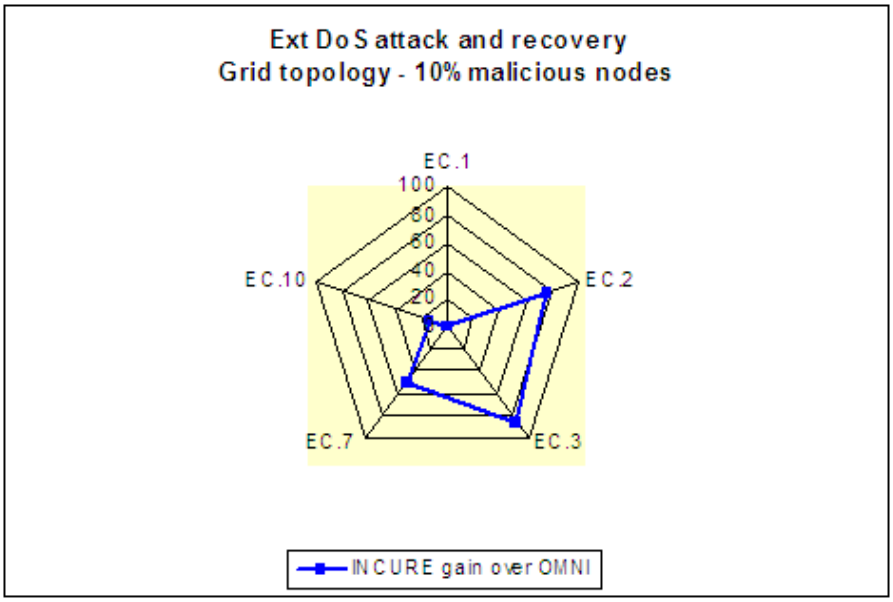

Figure 25: Persistent attack strategy NLOS: ext DoS and recovery gain

5.3.2.1.1 Overall evaluation remarks for NLOS

The analysis has indicated that in the case of NLOS INCURE and OMNI present a similar behavior at both LOS and shadowing cases (NLOS). INCURE can recover compromised WSN operation and re-enforce network performance better in comparison to typical intrusion recovery countermeasures implemented in OMNI networks, when considering an increased and variable path loss due to shadowing conditions. The ability to self-heal and recover the availability of the sensor nodes (Table 69), the survivability of the network (Table 70), the reliability (Table 72), the network's responsiveness (Table 73) and the ability to recover and maintain resilience (Table 71) to attacks are demonstrated by INCURE countermeasure.

INCURE minimizes eavesdropping more than the OMNI case. Overall, INCURE can reduce the eavesdropping of packets up to 92% and the compromised nodes up to 26% when compared to the OMNI case (Table 71). In a number of cases, the eavesdrop ability of malicious nodes is decreased due to shadowing conditions and compared to the LOS case. There are some cases where the variable path loss allows a malicious node to communicate

with distant nodes, increasing eavesdropping. The same observation applies when malicious nodes launch a DoS attack. As malicious nodes affect more nodes (Table 69), recovery is applied by more nodes, restoring the network performance at different granularities. OMNI successfully addresses the selective forwarding attack and restores network performance. The recovery measures deployed by OMNI nodes to address the DoS attack decrease the energy consumption (Table 70) that is forced by the attack. However, packet delivery (Table 72) is decreased in all cases as OMNI low duty cycle recovery affects the network's operation. INCURE restores the network's packet delivery (Table 72) operation in most of the cases when considering the selective forward and DoS attacks. At the grid, INCURE is affected more when compared to the other topologies and the LOS case. The DoS attack and INCURE recovery affect the network's performance at the grid topology as the lower node density that occurs due to shadowing prohibits nodes from discovering new active paths. Although the DoS attack is addressed and energy consumption is decreased, the packet delivery is also decreased. Packet delivery is depended on the network connectivity and on the ability of the nodes to discover/update routing paths easily in order to forward their observations to the control center. Moreover, the networks' packet delivery delay (Table 73) is affected at different granularities as it greatly depends on the nodes connectivity and the path quality. Lower density topologies require more effort to update route paths and forward observations to the control center. Shorter route paths allow the network to deliver observations faster.

Network connectivity is affected due to shadowing and due to the recovery actions, thus there are cases where nodes require more effort to converge to routing and establish stable packet delivery. Furthermore, a number of actions can be taken to re-enforce the benefits of INCURE countermeasure. First, we consider that an assessment of the environment at which the WSN will be deployed needs to be performed using simulations and/or field measurements. This will allow users to evaluate the path loss that this is expected to occur in the deployment environment and thus help them to choose operating conditions accordingly. Through simulations, users can evaluate how the attackers' capabilities can be re-enforced or

degraded under different operational conditions, and also evaluate the extend at which the INCURE can address them at the specific deployment environment. Simulation results will indicate to users the benefits and tradeoffs of the different recovery actions they plan to deploy. Furthermore, simulation results will also indicate if complementary solutions need to be considered in order to re-enforce and optimize the recovery benefits, i.e. utilize sensor platforms with higher capabilities, deploy more sensor nodes, etc.

Table 69: Availability evaluation – NLOS Compromised nodes %

AVAILABILITY (Ref. Table 65,Table 66,Table 67,Table 68)						
Compromised nodes %	Topology					
	Sparse		Dense		Grid	
Persistent attack strategy	Malicious nodes					
	5%	10%	5%	10%	5%	10%
Due to eavesdrop						
INCURE-NLOS	8.2	17.2	17.2	32.8	2.5	5.4
OMNI-NLOS	25.6	42.9	30.3	52.9	15.9	29.5
Due to DoS						
INCURE-NLOS	13.5	21.7	25.4	39.4	6.8	12.7
OMNI-NLOS	25.1	43.2	31.7	58.8	16.4	30.7
Due to DoS recovery						
INCURE-NLOS	0.1	0.16	0.06	0.13	0.03	0.06
OMNI-NLOS	31.5	53.8	42.2	73	19.3	37.9
Due to ext DoS recovery						
INCURE-NLOS	1.2	3.8	0.7	6	0.1	0.2
OMNI-NLOS	60	80.8	66.7	85.9	48.4	75

Table 70: Survivability evaluation – NLOS Energy consumption increase/decrease %

SURVIVABILITY (Ref. Table 63, Table 64, Table 65,Table 66,Table 67,Table 68)			
Energy consumption increase/decrease %	Topology		
	Sparse	Dense	Grid
	Malicious nodes		

Persistent attack strategy	5%	10%	5%	10%	5%	10%
SF attack						
INCURE-NLOS	-10.4	-13	-4.7	-7.4	-31.1	-42
OMNI-NLOS	-15.2	-29.8	-9.9	-18.6	-30	-42
Recover from SF attack						
INCURE-NLOS	+17.4	+30.9	+9.2	+14.5	+44.1	+52.9
OMNI-NLOS	+8.5	+14	+1	+5.8	+29.9	+50.3
DoS on overhearing						
INCURE-NLOS	+85.2	+169.3	+173.1	+289.1	+13.8	+48.4
OMNI-NLOS	+76	+156.1	+88.3	+160.5	+61	+120.1
Continuous DoS						
INCURE-NLOS	+147.7	+216.9	+251.1	+382.3	+45	+106.6
OMNI-NLOS	+83.1	+146.2	+92.8	+157	+61.5	+116.9
Recover from DoS attack						
INCURE-NLOS	-51.1	-62	-66.3	-74.9	-28.9	-50.9
OMNI-NLOS	-37	-52.7	-36.5	-52.7	-41.6	-38
Ext DoS and recovery						
INCURE-NLOS	+97.9	+118.8	+108.7	+134	+28.9	+62.4
OMNI-NLOS	+41.9	+36.1	+38.3	+17.8	+39.5	+65.1

Table 71: Resilience evaluation – NLOS overall increase/decrease % performance

RESILIENCE (Ref. Table 65)						
Increase/decrease %	Topology					
	Sparse		Dense		Grid	
Persistent attack strategy	Malicious nodes					
	5%	10%	5%	10%	5%	10%
Eavesdropped packets						
INCURE-NLOS % gain over OMNI-NLOS (in terms of less eavesdropped packets)	+81.5	+76.5	+62	+60.6	+92.1	+91
Compromised nodes due to eavesdropping						
INCURE-NLOS % gain over OMNI-NLOS (in terms of less % of compromised nodes)	+17.4	+25.7	+13.1	+20.1	+13.4	+24.1

Energy consumption on DoS based on overhearing						
INCURE-NLOS	+85.2	+169.3	+173.1	+289.1	+13.8	+48.4
OMNI-NLOS	+76	+156.1	+88.3	+160.5	+61	+120.1
Packet delivery on DoS based on overhearing						
INCURE-NLOS	-3.7	-8.3	-9.1	-18.6	-3.3	-4
OMNI-NLOS	-10.4	-22.8	-15.2	-34.1	-23.7	-31.2

Table 72: Reliability evaluation – NLOS Packet delivery increase/decrease %

RELIABILITY (Ref. Table 64, Table 67, Table 68)						
Packet delivery increase/decrease %	Topology					
	Sparse		Dense		Grid	
Persistent attack strategy	Malicious nodes					
	5%	10%	5%	10%	5%	10%
Recover from SF attack						
INCURE-NLOS	+16.8	+31.1	+8.1	+19.4	+55.1	+82
OMNI-NLOS	+17.8	+50.4	+6.6	+23.8	+53.2	+84.9
Recover from DoS attack						
INCURE-NLOS	+3.8	+7.1	+5.7	+4.1	-4.4	+0.3
OMNI-NLOS	-15.3	-27	-17.3	-22.6	-24.3	-22.8
Ext DoS and recovery						
INCURE-NLOS	-15.6	-19.3	-10.9	-17.4	-9.7	-9.1
OMNI-NLOS	-12.2	-5.8	-7.7	-1.3	-7.9	-7.8

Table 73: Responsiveness evaluation – NLOS Packet delivery fraction and delivery delay increase/decrease %

RESPONSIVENESS (Ref. Table 64, Table 65,Table 66,Table 67,Table 68)						
Packet delivery and delay increase/decrease %	Topology					
	Sparse		Dense		Grid	
Persistent attack strategy	Malicious nodes					
	5%	10%	5%	10%	5%	10%

SF attack recovery							
Packet delivery	INCURE-NLOS	+16.8	+31.1	+8.1	+19.4	+55.1	+82
	OMNI-NLOS	+17.8	+50.4	+6.6	+23.8	+53.2	+84.9
Packet delivery delay	INCURE-NLOS	+28%	+32.4%	+6.7%	+13.4%	-1.2%	-47.6%
	OMNI-NLOS	+38.5%	-12.6%	+1.8%	-3.1%	+32.6%	-6.6%
DoS on overhearing							
Packet delivery	INCURE-NLOS	-3.7%	-8.3%	-9.1%	-18.6%	-3.3%	-4%
	OMNI-NLOS	-10.4%	-22.8%	-15.2%	-34.1%	-23.7%	-31.2%
Packet delivery delay	INCURE-NLOS	+7.6%	+34.7%	+26.1%	+19.3%	-7%	+13.3%
	OMNI-NLOS	+40.5%	+11.1%	+9.4%	+45.8%	-3%	+37.3%
Continuous DoS							
Packet delivery	INCURE-NLOS	-7.4%	-16%	-15.9%	-16.9%	-7.9%	-11.3%
	OMNI-NLOS	-13.4%	-26.1%	-18.2%	-35.9%	-17.8%	-33.7%
Packet delivery delay	INCURE-NLOS	+69.8%	+67.2%	+10.4%	+2.7%	-8.1%	+30.9%
	OMNI-NLOS	+26.2%	+15.4%	+51%	+27.4%	+8.5%	+52.1%
DoS attack recovery							
Packet delivery	INCURE-NLOS	+3.8	+7.1	+5.7	+4.1	-4.4	+0.3
	OMNI-NLOS	-15.3	-27	-17.3	-22.6	-24.3	-22.8
Packet delivery delay	INCURE-NLOS	-19.8%	-22.1%	-2.5%	+5.6%	+0.7%	-4.3%
	OMNI-NLOS	+15.3%	+9.4%	-0.6%	+12.1%	+19.4%	-9.7%
Ext DoS attack and recovery							
Packet delivery	INCURE-NLOS	-15.6	-19.3	-10.9	-17.4	-9.7	-9.1
	OMNI-NLOS	-12.2	-5.8	-7.7	-1.3	-7.9	-7.8
Packet delivery delay	INCURE-NLOS	+11%	-3.5%	+9.6	-2.5%	+4%	-2.6%
	OMNI-NLOS	-11.9%	-6%	+2.8%	-2.9%	+1.4%	-5.6%

5.3.3 Memory overhead evaluation

This section aims to evaluate the main memory requirements of the INCURE countermeasure. The memory overhead analysis will define the number of bytes required for data storage by the INCURE countermeasure at runtime. Taking into consideration the resource-constrained characteristics of sensor nodes, the analysis will indicate if the required

amount of memory is acceptable for typical sensor nodes that have limited memory, such as 4KB RAM [131] or 10 KB RAM [132].

The INCURE countermeasure utilizes specific data implementation structures to support its operation. Each sensor node maintains the following three caches as explained in section 3.7:

a) Antenna cache

The antenna cache lists information related to the antennas contained on each node. Three fields are specified for each entry in the cache: antenna identification id, antenna status and hibernation timer. Each cache entry is of 4 bytes size.

b) Neighbors cache

The neighbor cache holds information about each neighbor that the node communicates with. Each entry is of 2 bytes size and consists of the fields: neighbor identification id and antenna id.

c) Blacklist cache

The blacklist cache lists the malicious nodes and related information. The cache maintains three fields per entry: a malicious identification id, antenna id and attack type. Each entry is of 3 bytes size.

The memory overhead depends on the number of antennas utilized on each sensor node, the neighbors' number and the number of malicious nodes. An indicative memory overhead is calculated taking into consideration the simulations at the random dense topology when there

are 10% malicious nodes. The antenna cache requires a memory overhead of 16 bytes (4 bytes x 4 antenna elements). The neighbour cache is calculated for a 7 node neighbour density, yielding a memory overhead of 14 bytes (2 bytes x 7 neighbours). The blacklist cache considers 10 records for the malicious nodes, thus its size yields another 30 bytes memory overhead (3 bytes x 10 malicious nodes). The total memory size required under the aforementioned scenario is 60 bytes. This yields an acceptable memory overhead of 1.46% when considering 4KB RAM and 0.58% overhead when considering 10KB RAM.

5.3.4 Cost analysis

Applications deploy WSNs of different sizes, usually ranging from some tens to some hundreds sensor nodes, depending on the applications' objectives and requirements. Typical sensor node cost is presented in Table 74 [133].

Table 74: Cost per node

Mote platform	Cost (US $)
Rene	100
Micaz	99
IRIS	115
TelosB	99

The proposed solution utilizes a switched beam antenna model, supporting the operation of multiple directional antennas instead of a typical single omni-directional antenna. This yields a cost overhead per sensor unit. As per [134], authors have built a sensor prototype with two directional antennas instead of the use of a single omni-directional antenna, which has

increased the total cost of the sensor unit by only 3%. Following we give an indicative cost analysis of the main components required to deploy a sensor node with multiple antennas.

It is assumed that two main components will contribute towards the extra cost when compared to an omni-sensor. These costs are related to the antenna and to the RF switch cost. If we assume that the antenna is a patch antenna as in [122], one can calculate the cost of this antenna by considering the cost of an FR-4 fiberglass board. The typical cost of an FR-4 sheet of dimensions 30cm x 60cm is about 10 USD (retail price) [135]. Since the antennas developed in [122] are of dimensions 56 x 56 mm, a 30cm x 60cm FR-4 sheet can produce around 50 antennas, bringing the individual antenna cost down to 0.20 USD (retail price). This suggests that the antenna cost for a 4-antenna sensor is approximately 1.0 USD. With regards to the RF switch cost, typical RF switches can cost some tens of cents [136] as large quantities will be utilized. The overall typical cost for a 4-antenna sensor is not expected to exceed 4 USD.

As demonstrated previously, the proposed countermeasure yields many benefits in terms of intrusion recovery aspects when compared to typical intrusion recovery solutions in omni-directional WSN networks. Critical WSN applications can utilize the benefits gained by INCURE to support their operational objectives when the network is under attack during propagation of critical observations. Thus, a cost overhead can be acceptable if there is a significant benefit gained by a specific solution.

5.4 Overall performance concluding remarks

This chapter defined the evaluation objectives and scenarios utilized in the evaluation process. Simulation scenarios have been specified covering static and persistent/adaptive attack strategies. The analysis of results presented the performance evaluation of the INCURE

countermeasure and compared it against typical recovery countermeasures in WSNs proposed in the literature. The recovery benefits of INCURE to restore the availability, reliability, survivability and responsiveness of sensor nodes, while yielding a low tradeoff in terms of compromised nodes due to recovery measures, are demonstrated in all cases, except when addressing the DoS attack in the grid topology with NLOS radio conditions. The network connectivity is quite low (< 3) at the grid topology as the shadowing has affected nodes connectivity. INCURE restores the availability of nodes (9% to 36%) and decreases the energy consumption from 24% to 72% due to the DoS attack in the grid topology with NLOS radio conditions. However, the packet delivery capability cannot be easily restored as the low node density prohibits nodes from converging to stable active paths while recovering from the DoS attack, decreasing up to 4% the packet delivery capability of the network. In such a case, a number of actions can be taken to re-enforce the benefits of INCURE countermeasure i.e. utilize sensor platforms with higher capabilities, deploy more sensor nodes, etc. Overall, the analysis demonstrated that INCURE recovery outperforms typical recovery countermeasures. In the case of a static attack strategy and LOS radio conditions, INCURE re-enforces the typical recovery measures of blacklisting and rerouting while addressing a selective forwarding attack and recovers packet delivery up to 81% compared to the OMNI case that recovers up to 72%. When considering a DoS attack launched by malicious nodes that deploy a static attack strategy, INCURE nodes manage the operation of their antennas and recover the availability, survivability, resilience and responsiveness of the network without any tradeoff in terms of compromised nodes due to its recovery measures. INCURE recovers up to 80% packet delivery while reducing by 74% the energy consumption due to the DoS attack. The OMNI low duty cycle yields a tradeoff of 20% to 41% of compromised nodes and reduces the packet delivery up to 16% (achieving a total up to 58%) in order to reduce by 42% the energy consumption that occurs due to the DoS attack. The OMNI low duty cycle measure tradeoffs the network's survivability with the availability, reliability and responsiveness. However, in mission-critical environments, it is vital to support decision making, a task that requires all operational objectives (availability, reliability, survivability and responsiveness) to be

recovered in case of compromisation. When considering a persistent/adaptive attack strategy, INCURE effectively recovers the compromised WSN by managing the operation of antennas and minimizing the ability of malicious nodes to affect sensor nodes. INCURE effectively addresses initialization of attacks based on an overhearing case. Results show that INCURE yields from 74% to 97% and 61% to 92% less eavesdropped packets when considering LOS and NLOS radio conditions respectively and compared to the OMNI case. By minimizing the ability of malicious nodes to eavesdrop and acknowledge network communication, INCURE prohibits them to react and launch other attacks after recovery measures are taken. INCURE achieves a packet delivery ranging from 69% to 82% and 56% to 83% when considering LOS and NLOS conditions and a reactive adversary. For the same scenarios, OMNI is affected more by the reactive malicious nodes yielding a packet delivery between 44% to 68% (LOS) and 46% to 73% (NLOS). In the case of a continuous DoS attack, INCURE yields an insignificant tradeoff of 1% in terms of compromised nodes due to its recovery actions while successfully recovering the network's availability, survivability, reliability and responsiveness. OMNI addresses the DoS attack and successfully decreases the energy consumption that occurs due to the attack up to 58% (versus 72% less energy consumption achieved by INCURE), however, it also decreases the packet delivery achieving a total of 30% to 54% in LOS (INCURE recovers from 69% to 81%) and 35% to 59% in NLOS (INCURE recovers from 52% to 83%) radio conditions. Furthermore, OMNI nodes have to deploy another recovery action, the channel surfing, in an effort to address the availability and reliability tradeoff that yielded from the low duty cycle while addressing the DoS attack. The channel surfing effectively recovers the network's performance when compared to the low duty cycle, however, it cannot prohibit a reactive adversary from recompromising the network's operation. On the other hand, INCURE has addressed the DoS attack without the need to deploy more recovery actions as the availability tradeoff, due to the recovery actions, is insignificant (1%). Furthermore, INCURE forces malicious nodes to change their attack dynamics in an effort to compromise the network, meaning that malicious nodes consume further their own energy. Thus, INCURE can also affect the survivability of malicious nodes.

When malicious nodes deploy an extended DoS by increasing their transmission power, INCURE yields a tradeoff up to 9% of compromised nodes due to its recovery actions while minimizing the ability of malicious nodes to severely affect the network's operation. INCURE achieves a packet delivery ranging from 52% to 75% in LOS and from 48% to 68% in NLOS radio conditions, allowing a mission-critical application to support the decision-making. On the other hand, the OMNI low duty cyle measure cannot promote the decision-making as the network's availability is greatly affected due to the recovery action (up to 86% compromised nodes), severely affecting the packet delivery capability of the network (29% to 47% LOS, 31% to 52% NLOS).

INCURE promotes the availability, resilience, reliability and survivability of the WSN, achieving an overall higher percentage of recovered performance when compared to typical recovery measures and supports the mission of critical applications when they are under attack by a an adversary that executes a static or a persistent attack strategy.

Chapter 6

Conclusions & Future work

In this thesis, the problem of intrusion recovery in WSNs, especially in the context of mission-critical applications, is addressed. The objective of this research work is twofold. The first objective considers recovering the WSN operation, when it is compromised by malicious nodes, in particular when considering an adaptive and persistent adversary. Once restoration is achieved, the second objective focuses on prohibiting the malicious node from compromising the previously recovered network. We focus on recovering the communication availability between nodes and at the same time on restoring and retaining the survivability, resilience and packet delivery reliability of the WSN.

A new intrusion recovery framework is proposed (INCURE) to address compromisation in WSNs. INCURE is supported by a number of novel features in terms of operation and evaluation aspects, outlined below.

In what follows, we provide our main findings and contributions and discuss possible future directions.

6.1 Main findings and contributions

Initially, we have identified that intrusion recovery investigations in WSNs, especially in the context of mission-critical WSNs, are limited and that they need to be extended in order to

promote robust restoration services under different attack conditions. Currently, investigations are focusing on simple threat models leading to vulnerabilities of the proposed solutions when considering an adaptive and persistent adversary. Intrusion recovery services are vital for mission-critical WSN applications in order to address compromised sensor nodes that deploy an adaptive and persistent attack strategy with the objective to affect the network during the observation and propagation of critical events. A major observation made through the thesis investigations is that typical intrusion recovery approaches in WSNs are vulnerable under different attack conditions as they were designed taking into consideration simple threat models. Therefore, they could not be effectively used to address adaptive and persistent attack strategies. Furthermore, existing intrusion recovery approaches were designed and deployed in omni-directional WSNs. Omni-directional networks transmit and receive signals equally to/from all directions, allowing malicious nodes to compromise the availability of sensor nodes more easily when compared to solutions that utilize directional antennas.

To address the aforementioned shortcomings, we have concentrated our efforts on minimizing the opportunities of the malicious nodes to compromise the availability of sensor nodes. The availability of sensors is a vital requirement that supports and promotes the fundamental operations of a WSN, particularly sensing, communicating and reporting. Thus, if availability is compromised, it is important to recover and retain it, for as long as possible, in order to permit the WSN to continue supporting its operational objectives. In order to recover and prohibit persistent malicious nodes from compromising sensors after recovery solutions are applied, effective isolation of malicious nodes must be achieved. We have pursued a different approach on the way the WSN isolates a malicious node in an effort to minimize its ability to affect sensors' operation. The proposed intrusion recovery countermeasure utilizes multiple directional antennas to create controlled routing and physically isolate malicious nodes from the network communication. Currently, directional antennas have hardly (if at all) been investigated in an intrusion recovery context in WSNs. The property of directional antennas to transmit and receive to/from specific directions can

support isolation of malicious nodes and promote our intrusion recovery objectives. INCURE specifies a novel approach to protect the operation of a WSN during the observation and propagation of critical events to the control center. Once a malicious node is detected, INCURE sensors manage their antenna beams operation, deactivate them appropriately towards the malicious nodes and control routing operation in order to isolate malicious nodes from the network communication and recover the compromised services. Nodes enable the deactivated antennas after a specified time window to assess the network condition and continue with recovery actions, if necessary. The proposed countermeasure minimizes the opportunities of reactive malicious nodes to launch an attack when they can overhear network communication and increases the resilience of recovered services against a persistent attack strategy.

The operation of the proposed intrusion recovery countermeasure is driven by a novel intrusion recovery policy in order to consider different attacks and accommodate different intrusion recovery requirements. Although our focus is on mission-critical WSN applications, we recognize that other WSN applications can benefit from INCURE if they require some level of recovery, thus we have considered them in the policy design. The policy considers different security attacks and intrusion recovery requirements in order to promote adaptability of the intrusion recovery strategy and selfhealingness of sensors as the attack strategy moves between different attack executions. This policy can be considered as the foundation based on which new intrusion recovery policies can extend it to accommodate more security attacks and intrusion recovery countermeasures. Moreover, throughout this thesis' investigations we have specified a number of design directions in an effort to inspire new solutions in the area. The proposed design directions were taken into consideration and have driven the design of INCURE framework.

Finally, we have proposed a new intrusion recovery evaluation method in order to assess and compare intrusion recovery countermeasures. Evaluation directions in the context of

intrusion recovery aspects in WSNs are limited which makes the assessment and comparison of intrusion recovery countermeasures very difficult. Within the evaluation framework we consider networking and security metrics, such as packet delivery, delay, energy, number of compromised nodes due to attacks (selective forwarding/eavesdropping/DoS) and number of eavesdroped packet, together with operational requirements, such as availability, survivability, reliability, resilience, responsiveness, and self-healingness. By promoting the proposed intrusion recovery evaluation framework we aim to provide important criteria based on which solutions should be evaluated, fine-tuned and compared.

INCURE is evaluated, taking into consideration: (a) a static and (b) a persistent/ adaptive attack strategy, and compared against typical intrusion recovery countermeasures in WSNs. Simulation results demonstrate that the proposed countermeasure improves the resilience of the network considerably, prohibiting reactive malicious nodes to attack based on an overhearing case and minimizing the attack outcome in case of adversaries that execute a static or persistent attack strategy. INCURE recovers the availability of compromised sensor nodes, up to 40% in the case of a DoS attack, and contributes to their survivability and packet delivery reliability with a small tradeoff of 1% compromised nodes due to the recovery measures. When an extended attack strategy is considered, INCURE presents a delayed degradation of performance and a tradeoff of up to 9% compromised nodes in order to minimize the attack outcome. Furthermore, at environments where we control the placement of sensor nodes, INCURE presents an increased resilient level and the best results in terms of isolating malicious nodes and restoring the network's operation. Encouraging results are also shown at random topologies. Overall, INCURE outperforms typical intrusion recovery countermeasures implemented in omni-directional WSNs in terms of recovering compromised nodes, packet delivery and survivability aspects.

As we stress out in this thesis, the intrusion recovery area is a fundamental part of a security strategy in WSNs. As advances in WSNs progress, the same observation applies for

the attack strategies that are executed against sensor nodes. This means that new designs should consider advanced threat models in order to promote resilient solutions. A spherical security approach is essential in order to provide holistic protection to a WSN. If prevention measures are not adequate and compromisation occurs, then intrusion detection and intrusion recovery must be applied to restore the WSN to a stable state and continue supporting the operational objectives of WSN applications.

6.2 Future work

This section discusses the future work we will pursue as an extension of the thesis contributions. Future work focuses on the enhancement of the proposed framework that can optimize the overall cost of the solution.

The idea of achieving nodes' availability recovery in WSNs by creating controlled routing paths and physically isolating malicious nodes sets the ground for many new ideas to rise. We have demonstrated the recovery benefits that can be achieved by utilizing multiple directional antennas to isolate compromised nodes that attack the network. The usage of multiple directional antennas incurs an extra cost per sensor unit. One can investigate the adoption of INCURE by a fraction of the sensors. Instead of equipping all the sensors with directional antennas, only a subset of the sensors will utilize directional antennas while the rest of the sensors can deploy typical omni-directional antennas. This semi-adoption of INCURE will yield less cost overhead. Therefore, one of the future plans is to investigate which of the sensor nodes should deploy directional or omni-directional antennas in order to achieve an acceptable intrusion recovery level. We will define and investigate a number of criteria in order to decide the way INCURE will be utilized by the sensors. An initial criterion could consider the location of sensor nodes. Sensors at specific locations that need to retain the network's operation can be equipped with directional antennas, thus in case of

compromisation, effective isolation and intrusion recovery can be achieved. Such locations, that are expected to be attractive to the adversaries, may include the area near the sink or specific critical areas that need to be closely monitored for critical status change of the monitored environment.

Moreover, to further enhance the intrusion recovery benefits of the aforementioned approach, we will define and investigate an intrusion recovery policy in omni-directional WSNs, following the approach of INCURE's intrusion recovery security policy. Such an intrusion recovery policy in omni-directional WSNs is not yet pursued. However, we foresee that such a policy will benefit intrusion recovery aspects in omni-directional WSNs also. The benefits can be further increased by the semi-adoption of INCURE as previously explained. The objective of this new policy will be to address adaptive and persistent adversaries by integrating new/existing solutions in WSNs proposed by the research community, assessing their operation under a common operational framework and proposing enhancements in order to maximize the recovery benefits. A first thought is to separate the network into different recovery zones, each zone deploying different intrusion recovery countermeasures, according to different criteria. Potential criteria could be the nodes' density, the location of malicious nodes, critical areas such as near the sink, etc. The objective of the recovery zones will be to improve the reliability and resilience of the network under the existence of an adaptive and persistent adversary, while trying to balance any potential recovery tradeoff.

APPENDIX A Communication aspects

In this section a brief overview of some fundamental concepts [16] of wireless communications and of antennas is presented.

A.1 Antenna classification

Antennas can be classified into two categories: omni-directional and directional. An omni-directional antenna radiates or receives energy equally to/from all directions. A directional antenna radiates or receives more energy in specific directions. Directional antennas can be mainly classified into two categories: switched beam and adaptive beamforming antenna systems. The selection and usage of a specific directional antenna by sensor nodes is driven by the constrained requirements in WSNs, such as the need for low energy consumption and hardware cost. Switched beam antenna systems have fixed antenna elements to transmit or receive from specific directions. Usually, one or more beams can be selected using simple RF switches. On the other hand, adaptive beamforming antenna systems use sophisticated signal processing algorithms to dynamically create a steerable radiation pattern, with the main beam pointed to any direction. Switched beam antenna systems are preferable for use in WSNs as they do not require expensive signal operations, therefore are simpler in terms of hardware and required processing power and have a lower cost in comparison to adaptive beamforming antennas.

A.2 Antenna fundamental concepts

The gain of an antenna is an important concept, and describes how much power is transmitted in the direction of peak radiation to that of a hypothetical isotropic antenna, which radiates equally in all directions. Antenna gain is used to quantify the directivity of an antenna. Directivity means that the antenna transmits or receives more energy to/from one particular direction when compared to other directions.

The gain of an antenna (1), measured in dB, in a particular direction $\vec{d}$ = (θ,φ) given by an elevation θ and azimuth φ is measured as

$$G(\vec{d}) = \eta\ D(\vec{d}) \quad (1)$$

where η is the efficiency of the antenna which accounts for losses and $D(\vec{d})$ is the ratio of the transmitted power in a given direction relative to the average power density over all directions transmitted by an isotropic antenna. The maximum gain taken over all directions is called the peak gain of the antenna.

An antenna is characterized by an associated antenna pattern (Figure 26) [137]. An antenna pattern is the specification of the different gain values in each direction in space. A directional antenna pattern typically has a main lobe (also called main beam) of peak gain and a number of side lobes of smaller gain. The side lobe in the opposite direction (180^o) from the main lobe is called the back lobe. The beamwidth of a directional antenna is the angle subtended by the two directions on either side of the direction of the peak gain that are 3 dB lower in gain (known as the half-power beamwidth). Gain and beamwidth are related. Typically, the more directional the antenna, the higher is the gain and smaller is the beamwidth.

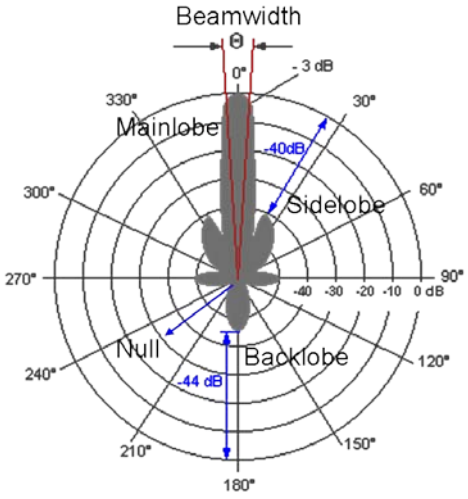

Figure 26: Antenna pattern example

A.3 Path loss propagation models

In a real environment, the transmission path between a transmitter and a receiver can vary from a direct and unobstructed line-of-sight (LOS) to one that is obstructed by various objects such as buildings and mountains. Signals arrive at the receiver through LOS, diffracted, transmitted through, reflected and scattered modes, causing signal fading. The path loss, measured in dB, is defined as the difference between the transmitted power and the received power. Different path loss propagation models have been proposed by researchers to predict the signal attenuation that occurs between a receiver and a transmitter separated by a distance. The following sections present three typical propagation models for path loss prediction utilized by researchers when evaluating their security protocols in WSNs:

A.3.1 Free space loss model

The free space or Friis propagation model assumes that there is only one clear and unobstructed LOS path between the transmitter and receiver. The following equation (2) calculates the received signal power (in watts) in free space at distance from the transmitter:

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \quad (2)$$

Where Pt is the transmitted signal power, Gt and Gr are the antenna gains of the transmitter and the receiver respectively, L is the system loss, lambda (λ) is the wavelength, and d is the distance between the two points (transmitter - receiver). From equation (2), it is derived that the received power decreases with the square of the distance d.

A.3.2 Plane Earth loss model

The Plane Earth (two ray ground) path loss model considers both the direct path and a ground reflection path between the transmitter and the receiver. The received power at distance d is predicted by the following equation (3):

$$P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L} \quad (3)$$

where Pt is the transmitted signal power, Gt and Gr are the antenna gains of the transmitter and the receiver respectively, L is the system loss and ht and hr are the heights of the transmitter and receiver antennas respectively. The model suggests a faster power loss as distance increases when compared to the free space loss propagation model.

A.3.3 Log-normal shadowing model

A more complex path loss propagation model is the log-normal model. The log-normal model is an empirical model that is derived from extensive field measurements. For this

reason, it is accurate for environments with the same characteristics as those where the measurements took place. The model considers shadowing from objects such as buildings that obstruct the propagation path between the transmitter and the receiver and cause fluctuation to the received signal power. The model considers that the existence of different objects in the environment can cause the received signal strength at two receiving points to be different, even at the same distance from a transmitter [16].

The shadowing model consists of two parts. The first one is known as the log-distance path loss model and predicts the mean received power at distance *d,* using a close-in distance d0 as a reference and a path loss exponent *n*. The path loss exponent *n* is empirically determined by field measurements and indicates the rate at which the path loss increases with distance. By increasing n, the average path loss is increased. The second part of the shadowing model represents the variation of the received power at a certain distance, denoted with X_σ. It is a Gaussian random variable with zero mean and standard deviation σ. The standard deviation is also obtained from field measurements. Typical path loss exponent and standard deviation values for WSNs path loss calculation in outdoor and indoor environments vary between n=2 to 4 and σ= 2 to 6 respectively [103, 124, 125, 126, 127, 128].

$$PL(d)\,[\text{dB}] = PL(d_0) + 10n\log(\frac{d}{d_0}) + X_\sigma \quad (5)$$

The deployment environment affects the network's performance. Thus, before a real WSN is deployed, simulations and/or field measurements should be performed in order to assess the network's performance. The results will aid the network designer to deploy solutions that address the specific propagation path loss conditions, thus supporting stable network performance. For example, deploy more sensor nodes in order to increase the network's density and assist routing functionality.

APPENDIX B Simulation framework

This section presents the deployed simulation framework in order to perform the evaluation of the proposed research work. The main components of the simulation framework are: the simulator tool utilized to simulate the selected scenarios, a number of personal computers responsible to run the simulations and utilities to analyze and plot the results.

B.1 Ns2 simulator

Network simulator (Ns2 - version 2.34) [118] has been selected as the network simulation tool to perform the assessment. Ns2 is an open source, discrete event simulator. Figure 27 presents the basic architecture of Ns2 [138]. The simulator takes as input argument a Tcl scripting file that initializes and configures the simulation. Once the simulation is executed, a simulation trace file is created containing information on the network events that have occurred, including packet transmissions and receptions, packet drops, remaining nodes' energy etc. The trace file is then used to analyze the behavior of sensor nodes and assess the performance of the simulated scenario.

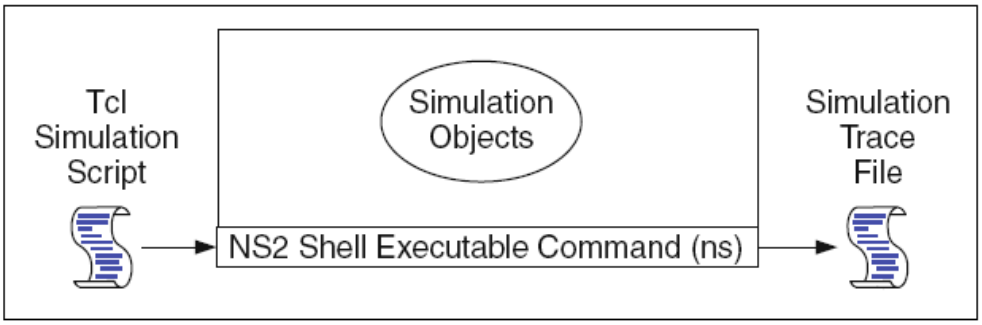

Figure 27: Ns2 architecture

B.2 Simulation process

The simulation framework consists of a number of tasks as depicted in Figure 28. First, the user configures the scenario configuration written as a TCL script (1). Then, the script is distributed over the NS2 simulator cluster to configure each machine (2) and start the simulation (3). Once a simulation is finished, a simulation trace file is generated (per machine) which is analyzed according to specific evaluation statistics (4). Results are forwarded (5) to the graph plotting manager in order to generate (6) the evaluation figures. Finally, the user can review (7) and process further (8) the evaluation results and related graphs. Following, the three major phases of the simulation framework (scenario configuration, simulation and results analysis, graph plotting) are analyzed in more detail.

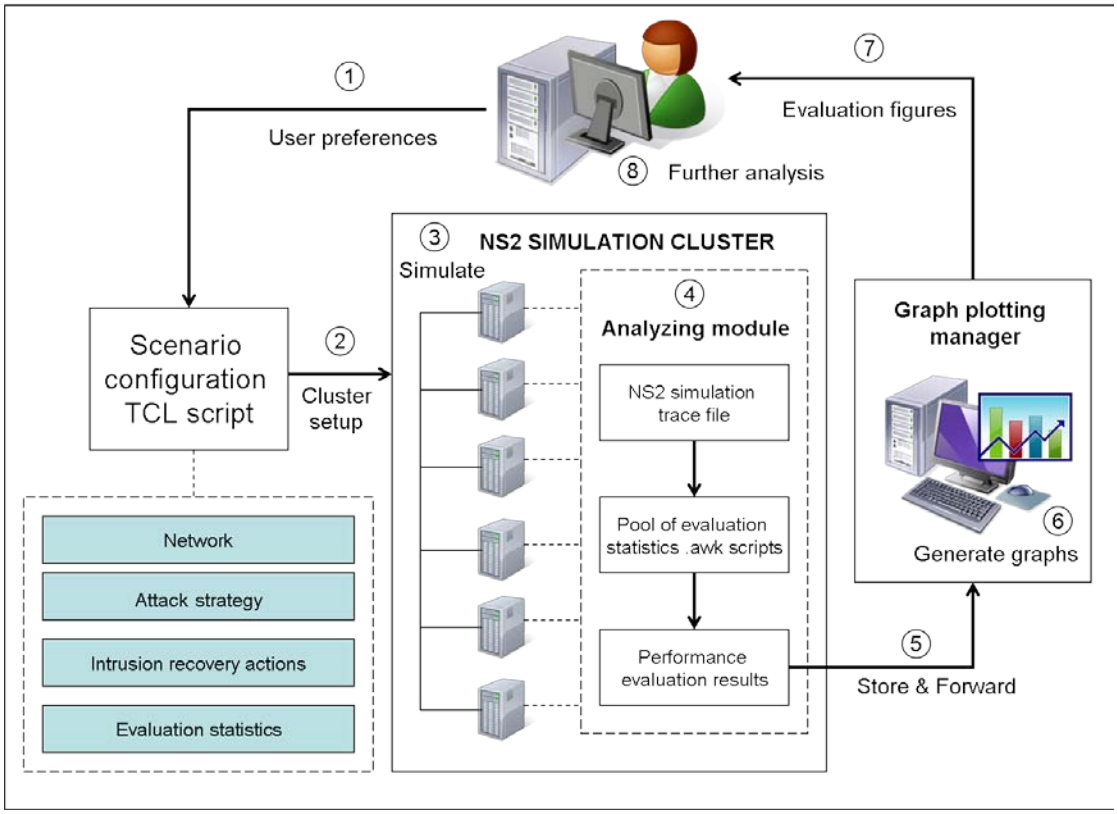

Figure 28: Simulation process

B.2.1 Scenario configuration phase

In this phase, the user must configure the scenario(s) that will be simulated with the ns2 simulator. The configuration procedure involves defining the values of input parameters required by the scenario and also selecting the evaluation statistics that will be utilized to assess the behavior of the proposed countermeasure under different network conditions.

The input parameters that need to be configured are grouped under three main categories:

- *Network configurations*. This category involves defining network-related aspects such as the network topology, the nodes capabilities, i.e. transmission power, antenna characteristics, energy resources, etc., the energy consumption that occurs due to different activities, i.e. packet transmission, and the routing protocol utilized by sensor nodes.

- *Attack strategy*. The scenarios that will simulate attack conditions need to define parameters such as the nodes that act maliciously, their capabilities, i.e. transmission power, and the attack type that they deploy. According to the attack type selected, there may be extra parameters that need to be configured. For example, in a DoS attack it is necessary to define the frequency of the attack and its duration.

- *Intrusion recovery actions*. In the case where the sensor nodes need to restore a compromised service, they have to deploy appropriate intrusion recovery actions. According to the selected intrusion recovery layer and the associated security attacks considered, the scenario is configured to utilize and configure the parameters of recovery actions.

Once the input scenario parameters have been configured, the user has to select the evaluation statistics (i.e. packet delivery, energy consumption, compromised nodes, etc.) that will be utilized to assess the performance of each simulation scenario.

B.2.2 Simulation and results analysis phase

The simulation framework deploys an Ns2-cluster, consisting of 6 quad-core machines with 4GB RAM and 2.4GHz Q6600 CPU that run the ns2 simulator for patch simulations. Once the scenario configuration phase is completed, the appropriate configurations are distributed over the cluster to configure a different simulation scenario on each machine and schedule the simulation execution. Each simulation yields an appropriate tracing file with a number of supplementary files related to the network's behavior and activity, when considering normal and attack network conditions, as specified by the simulation scenario.

Once the simulation is finished, analysis of results is performed locally at each machine using a number of evaluation scripts. The evaluation scripts are written in the AWK programming language. The awk [139] utility allows the user to extract data from input files, analyze them and produce formatted result reports.

B.2.3 Results plotting

When all necessary simulations have been finished, a script is executed to present results on appropriate figures.

APPENDIX C Evaluation figures

This section presents the evaluation figures that are utilized in Chapter 5 in order to perform the evaluation analysis. The criteria that have been utilized for the evaluation include: the network's energy consumption, the number of compromised nodes, the packet delivery fraction, the packet delivery delay and the number of eavesdropped packets.

C.1 Graph notations

Figures present evaluation results against each simulation scenario, referencing its id. The following simulation scenarios have been specified that correspond to the simulation id listed on the figures:

1. Normal network conditions
2. Selective forward attack
3. Intrusion recovery from selective forwarding (INCURE is utilized to address active malicious nodes. OMNI scenarios consider blacklisting malicious node and updating the routing paths in order to address the adversary.)
4. Eavesdropping and reactive DoS attack
5. Continuous DoS
6. Intrusion recovery from DoS (Nodes apply INCURE countermeasure. In OMNI scenarios, nodes deploy a low duty cycle.)
   6.A. In OMNI scenarios, nodes deploy a channel surfing countermeasure
   6.B. In OMNI scenarios, malicious nodes enter a channel switching mode, reconnaissance the network's status and continue with the DoS attack on overhearing
7. Extended DoS with increased transmission power. Recovery is applied as in 6

In the case of a static attack strategy, there is a single attack execution and nodes apply recovery to address it. In the case of a persistent attack strategy, each attack in each simulation scenario is cumulatively executed after the previous simulated activity is performed. For example, scenario 4 implements a DoS attack based on an overhearing case after recovering from the selective forwarding attack. Regarding the evaluation figures, legend INC(<R>,<5/10>) refers to INCURE, with R – Rate of malicious nodes, 5 - % malicious nodes, or 10 - % malicious nodes. OMN refers to the equivalent OMNI case.

C.2 Static attack strategy

This section presents the evaluation figures related to the static attack strategy.

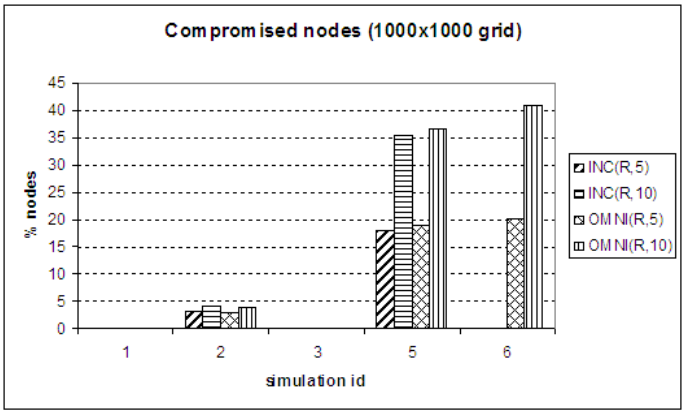

Figure 29: Compromised nodes – 1000x1000 LOS Static attack strategy

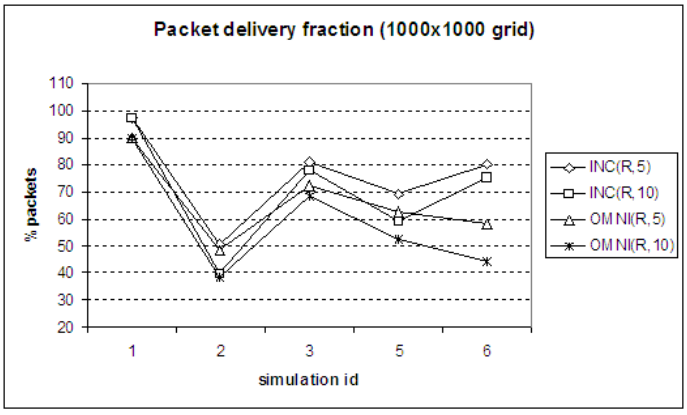

Figure 30: Packet delivery ratio – 1000x1000 LOS Static attack strategy

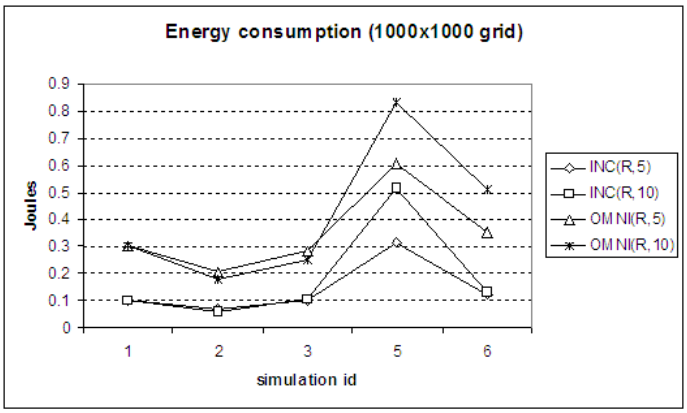

Figure 31: Energy consumption – 1000x1000 LOS Static attack strategy

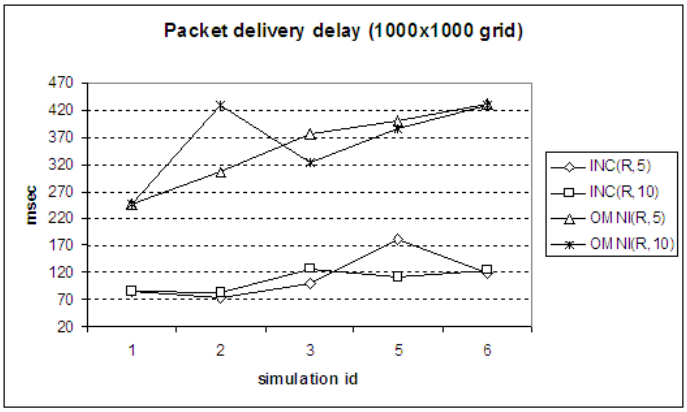

Figure 32: End-to-end packet delivery delay – 1000x1000 LOS Static attack strategy

C.3 Persistent attack strategy

This section presents the evaluation figures related to a persistent attack strategy, considering LOS and shadowing conditions.

C.3.1 LOS

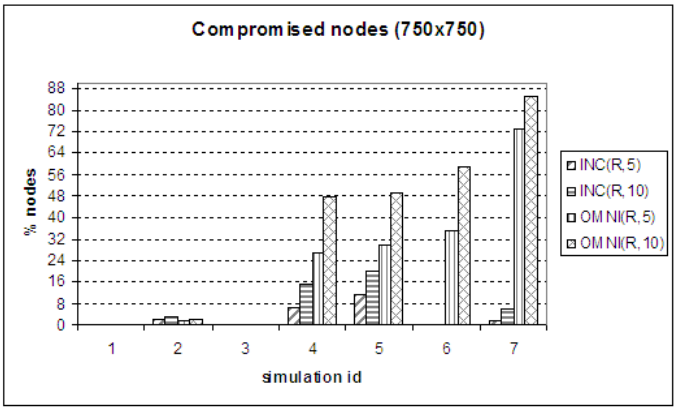

Figure 33: Compromised nodes – 750x750 LOS Persistent attack strategy

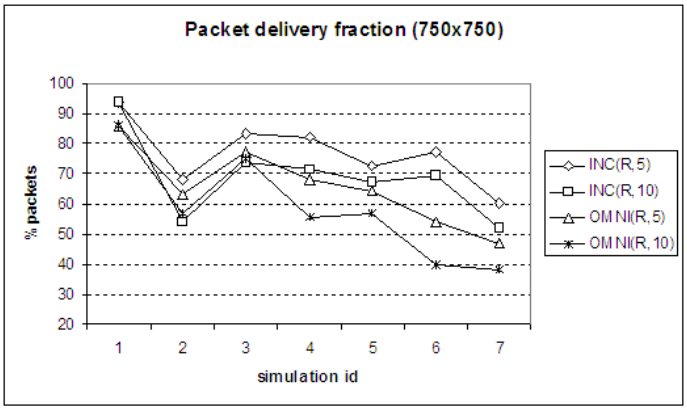

Figure 34: Packet delivery ratio – 750x750 LOS Persistent attack strategy

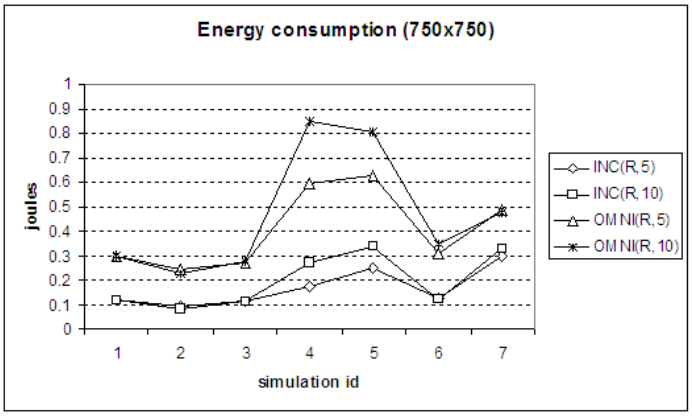

Figure 35: Energy consumption – 750x750 LOS Persistent attack strategy

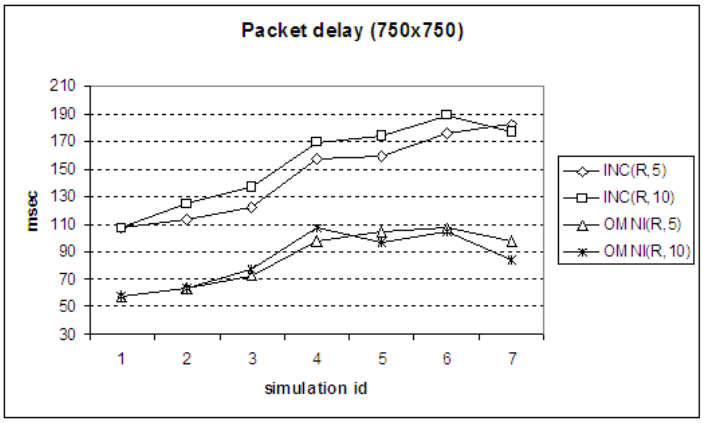

Figure 36: End-to-end packet delivery delay – 750x750 LOS Persistent attack strategy

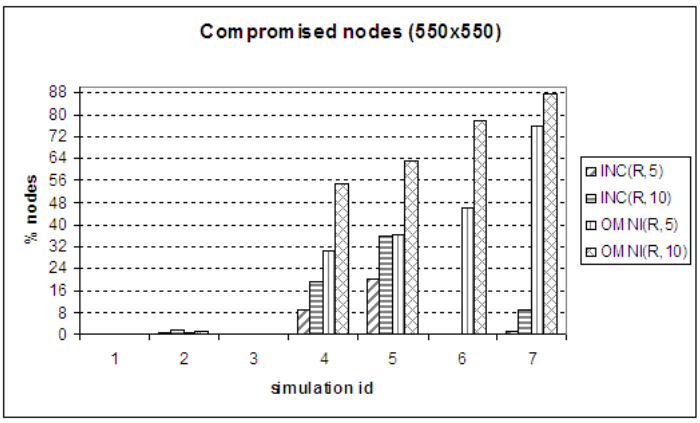

Figure 37: Compromised nodes – 550x550 LOS Persistent attack strategy

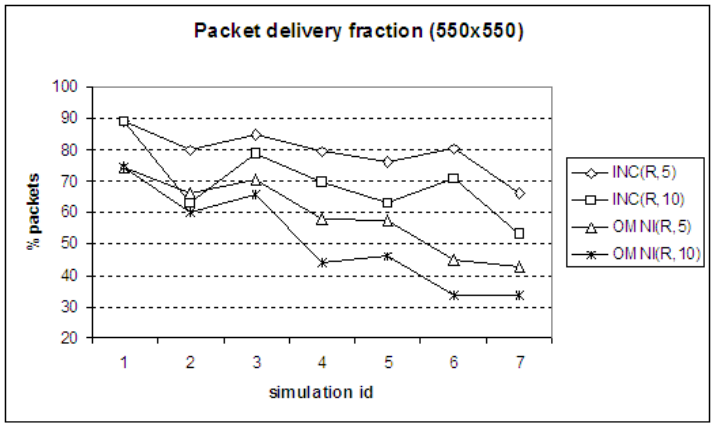

Figure 38: Packet delivery ratio – 550x550 LOS Persistent attack strategy

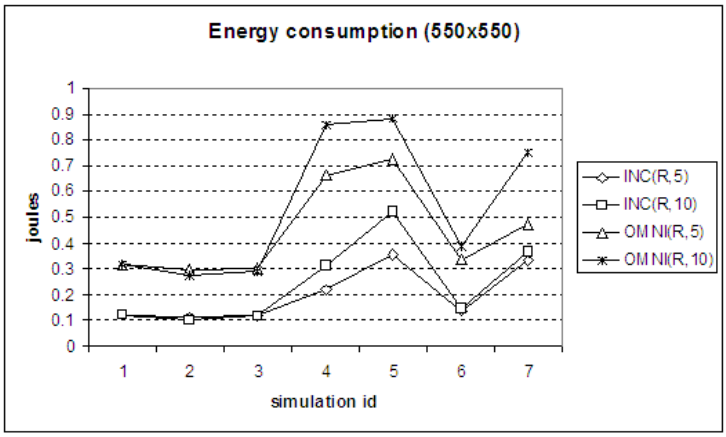

Figure 39: Energy consumption – 550x550 LOS Persistent attack strategy

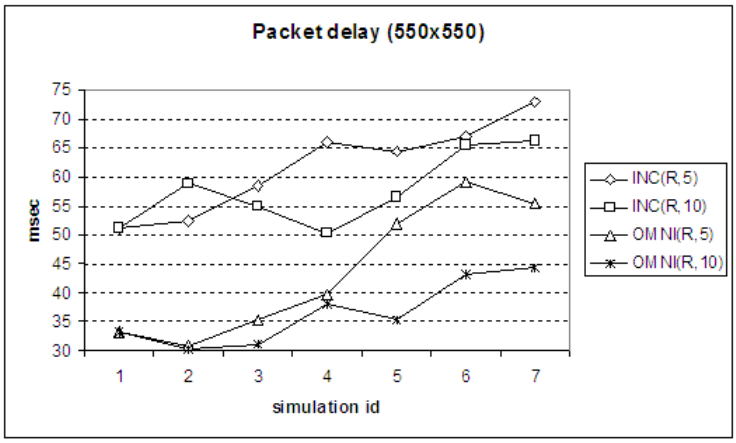

Figure 40: End-to-end packet delivery delay – 550x550 LOS Persistent attack strategy

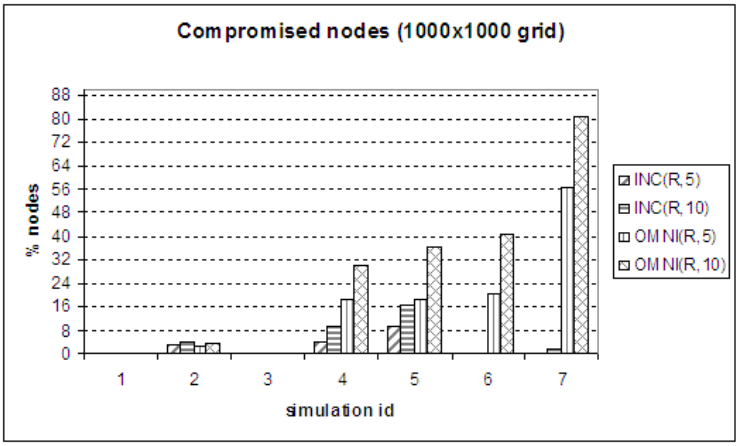

Figure 41: Compromised nodes – 1000x1000 LOS Persistent attack strategy

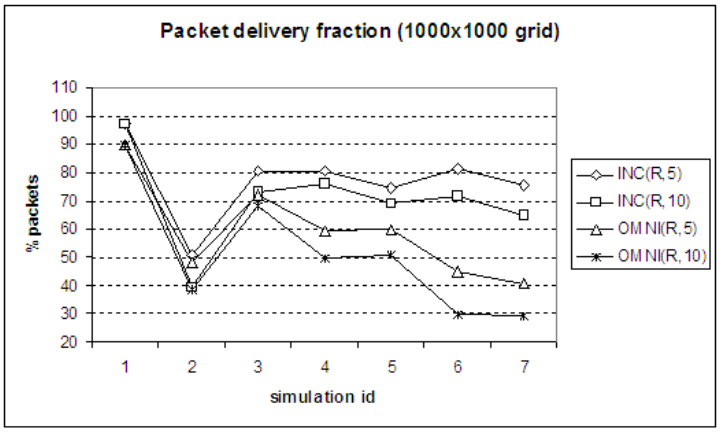

Figure 42: Packet delivery ratio – 1000x1000 LOS Persistent attack strategy

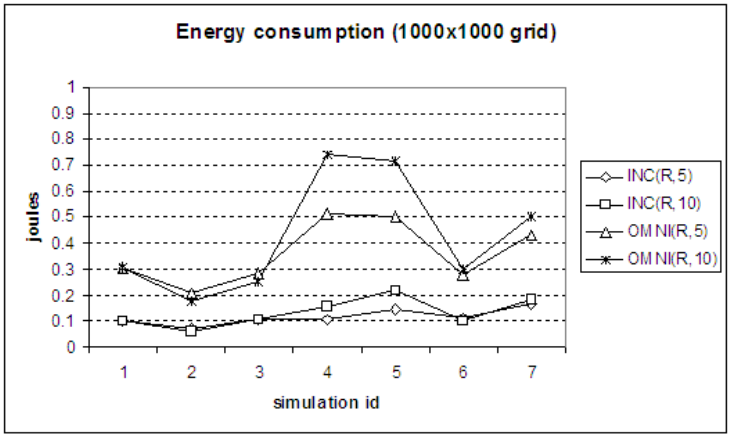

Figure 43: Energy consumption – 1000x1000 LOS Persistent attack strategy

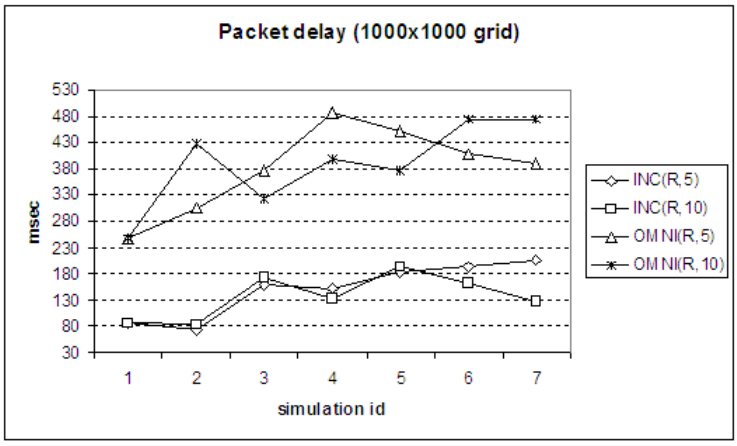

Figure 44: End-to-end packet delivery delay – 1000x1000 LOS Persistent attack strategy

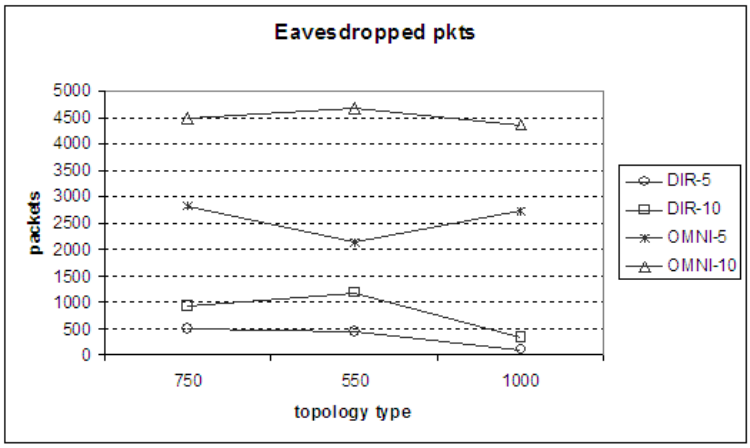

Figure 45: Total received packets on eavesdropping attack – LOS Persistent attack strategy

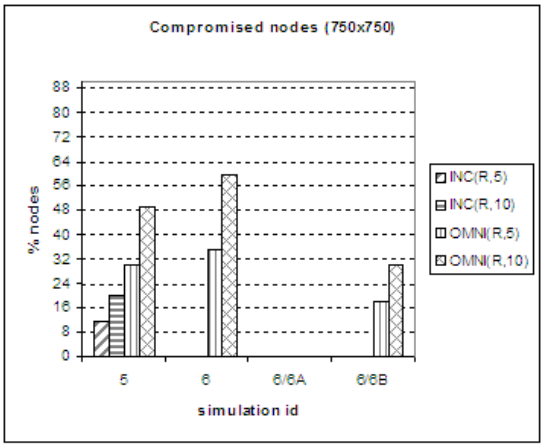

Figure 46: Channel surfing-Compromised nodes 750x750 LOS Persistent attack strategy

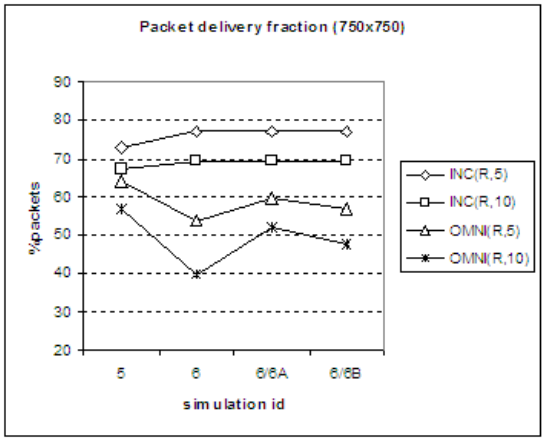

Figure 47: Channel surfing –Packet delivery 750x750 LOS Persistent attack strategy

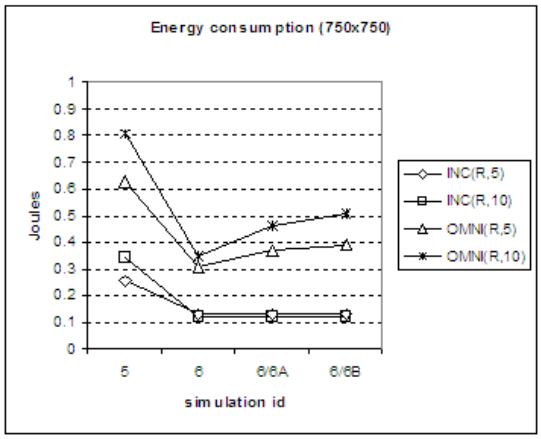

Figure 48: Channel surfing –Energy consumption 750x750 LOS Persistent attack strategy

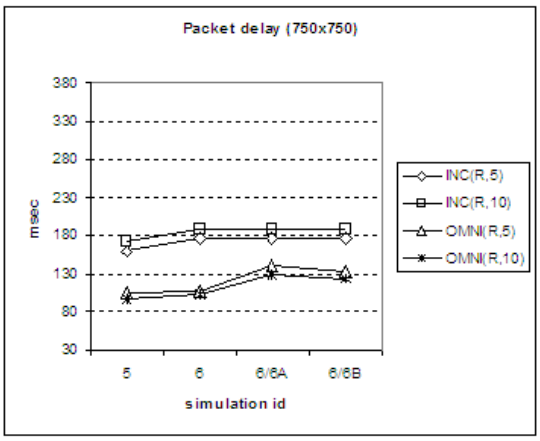

Figure 49: Channel surfing –Packet delay 750x750 LOS Persistent attack strategy

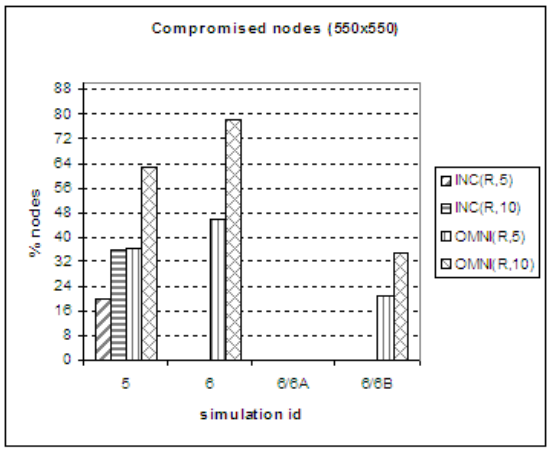

Figure 50: Channel surfing-Compromised nodes 550x550 LOS Persistent attack strategy

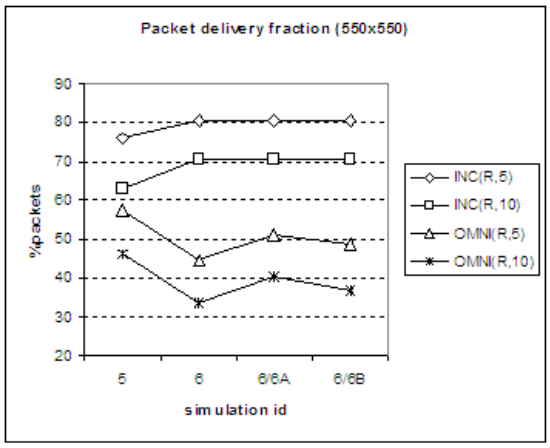

Figure 51: Channel surfing –Packet delivery 550x550 LOS Persistent attack strategy

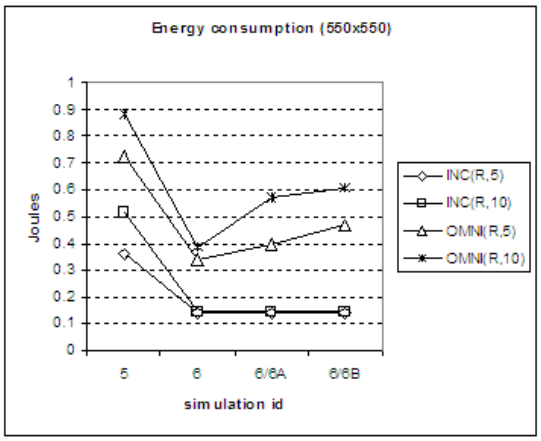

Figure 52: Channel surfing –Energy consumption 550x550 LOS Persistent attack strategy

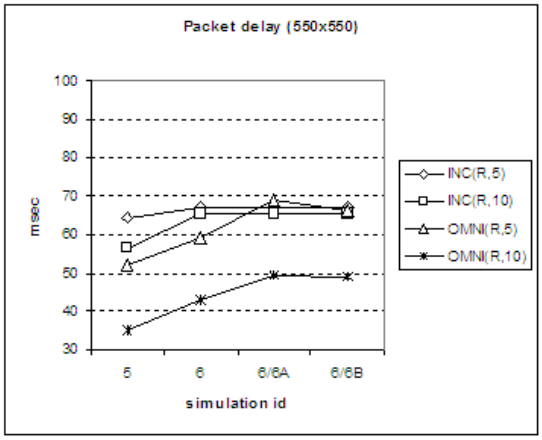

Figure 53: Channel surfing –Packet delay 550x550 LOS Persistent attack strategy

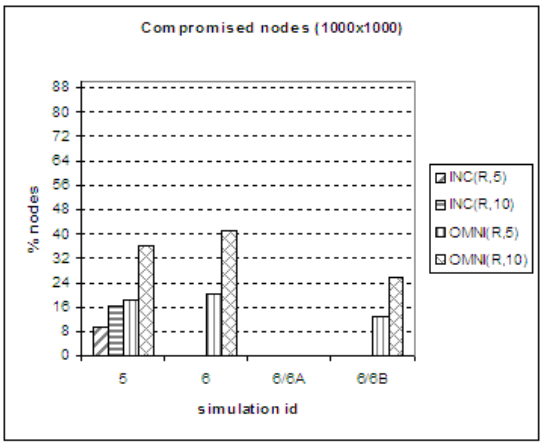

Figure 54: Channel surfing - Compromised nodes 1000x1000 LOS Persistent attack strategy

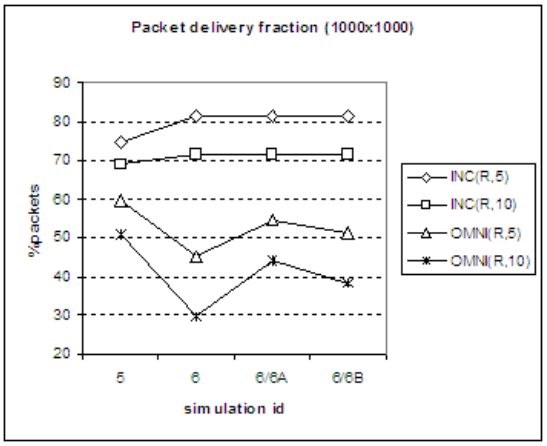

Figure 55: Channel surfing–Packet delivery 1000x1000 LOS Persistent attack strategy

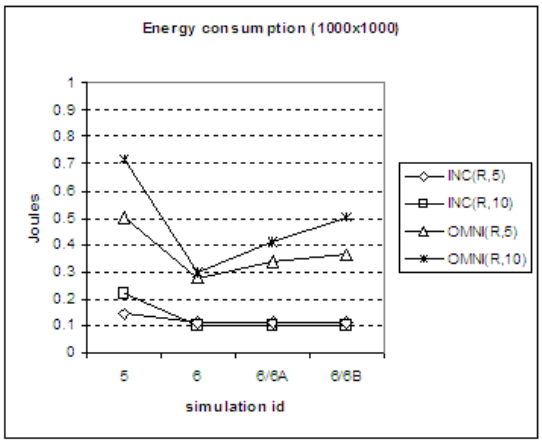

Figure 56: Channel surfing –Energy consumption 1000x1000 LOS Persistent attack strategy

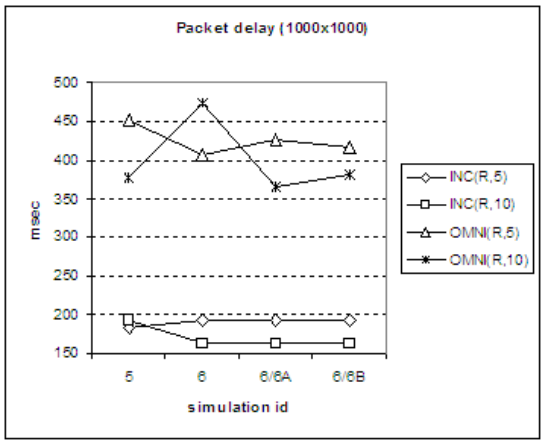

Figure 57: Channel surfing –Packet delay 1000x1000 LOS Persistent attack strategy

Confidence Intervals LOS scenarios						
Compromised Nodes (%) - INCURE						
	550x550		750x750		1000x1000	
Blackhole attack	0.427904	0.514149	0.413916	0.520974	0.397962	0.435574
Recovery	0	0	0	0.065333	0	0
Eavesdrop & Reactive DoS	3.752644	7.042062	2.748823	4.158832	0.932594	2.272429
Continuous DoS	2.878146	4.895793	2.020968	2.95386	2.060886	3.330056
Recovery	0.090788	0.097144	0.065333	0.116667	0	0
Ext DoS & Recovery	0.435574	1.660857	0.630402	1.21327	0	0.217778
Compromised Nodes (%) - OMNI						
Blackhole attack	0.376877	0.417457	0.579935	0.486042	0.408907	0.550776
Recovery	0	0	0	0	0	0
Eavesdrop & Reactive DoS	5.248081	4.767914	2.762923	2.559412	0.536562	0.872246
Continuous DoS	5.310145	4.932275	1.905357	3.390568	0.795647	1.155355
Recovery	3.710438	1.073468	1.034363	1.462358	0.272365	0.647761
Ext DoS & Recovery	5.601679	0.779104	5.972393	2.127929	3.803001	1.892918
Packet delivery (%) - INCURE						
Normal	4.40485	4.40485	3.169321	3.169321	2.286241	2.286241
Blackhole attack	6.702982	9.377256	7.602634	9.298372	8.522994	7.69023
Recovery	5.299965	5.123098	4.830986	6.253751	4.571493	6.142837
Eavesdrop & Reactive DoS	5.599918	6.070126	4.539554	5.241954	4.69028	5.46682
Continuous DoS	4.790362	5.946218	5.767404	5.164095	5.160719	5.912872
Recovery	5.210208	6.288884	5.057342	5.404484	4.201279	5.76257
Ext DoS & Recovery	4.876393	4.732756	3.760627	3.714147	4.319032	5.038305
Packet delivery (%) - OMNI						
Normal	6.33184	6.33184	4.497183	4.497183	3.447449	3.447449
Blackhole attack	6.751223	6.279165	8.496219	7.871937	7.754686	7.819888
Recovery	6.133798	7.227363	4.841585	5.023429	5.136804	5.580438

Eavesdrop & Reactive DoS	6.023049	5.718541	5.196439	5.287526	4.218973	3.677697
Continuous DoS	6.640892	5.899689	4.403161	5.960499	4.759304	4.333942
Recovery	5.366583	3.064015	4.915237	3.663211	4.682411	2.496538
Ext DoS & Recovery	4.884855	3.211142	3.842307	3.240856	3.596104	2.419072
Energy consumption (J) - INCURE						
Normal	0.013003	0.013003	0.015564	0.015564	0.01039	0.01039
Blackhole attack	0.011536	0.008607	0.009584	0.008269	0.008051	0.006381
Recovery	0.012202	0.01153	0.007973	0.009471	0.010863	0.009811
Eavesdrop & Reactive DoS	0.052589	0.081261	0.033603	0.045144	0.01096	0.028694
Continuous DoS	0.040592	0.070739	0.026805	0.032794	0.014384	0.034403
Recovery	0.010313	0.011597	0.010363	0.009976	0.008651	0.007346
Ext DoS & Recovery	0.01683	0.018075	0.011287	0.014284	0.007747	0.006342
Energy consumption (J) - OMNI						
Normal	0.036473	0.036473	0.031285	0.031285	0.028795	0.028795
Blackhole attack	0.031775	0.029922	0.029301	0.023686	0.022034	0.02279
Recovery	0.0298	0.028562	0.029432	0.027078	0.016886	0.017175
Eavesdrop & Reactive DoS	0.07294	0.122006	0.042442	0.061897	0.024048	0.034128
Continuous DoS	0.061855	0.124931	0.046776	0.058762	0.020821	0.029431
Recovery	0.024318	0.052141	0.022688	0.017414	0.014982	0.00991
Ext DoS & Recovery	0.045105	0.073719	0.048199	0.027346	0.023718	0.021483
End-to-end packet delivery delay (msec) - INCURE						
Normal	15.87877	15.87877	38.68512	38.68512	26.83937	26.83937
Blackhole attack	21.64811	27.82106	57.83618	161.1863	32.36291	45.27397
Recovery	22.98301	24.98266	40.27923	67.15207	64.64527	65.70827
Eavesdrop & Reactive DoS	25.50965	20.13698	80.11853	88.1359	59.11581	52.27822
Continuous DoS	26.08452	23.07444	63.52072	75.1052	65.81608	81.05333
Recovery	28.19108	24.8884	63.70885	82.7132	83.40928	43.54976
Ext DoS & Recovery	28.2558	28.5357	65.84999	79.04648	81.07473	38.14378
End-to-end packet delivery delay (msec) - OMNI						
Normal	10.61928	10.61928	21.45532	21.45532	68.38676	68.38676
Blackhole attack	10.74294	11.03752	31.17519	31.81995	110.7148	237.6802
Recovery	12.95607	10.71779	39.09867	29.31443	87.51009	107.9582
Eavesdrop & Reactive DoS	16.10058	14.32123	38.06344	37.17995	109.8244	115.0202
Continuous DoS	23.3747	12.47062	42.90686	40.57404	110.1273	102.2959
Recovery	22.7674	19.94039	50.74908	39.16947	112.279	195.3333
Ext DoS & Recovery	22.28602	21.26324	43.17277	35.64153	122.8475	195.3195

C.3.2 Shadowing

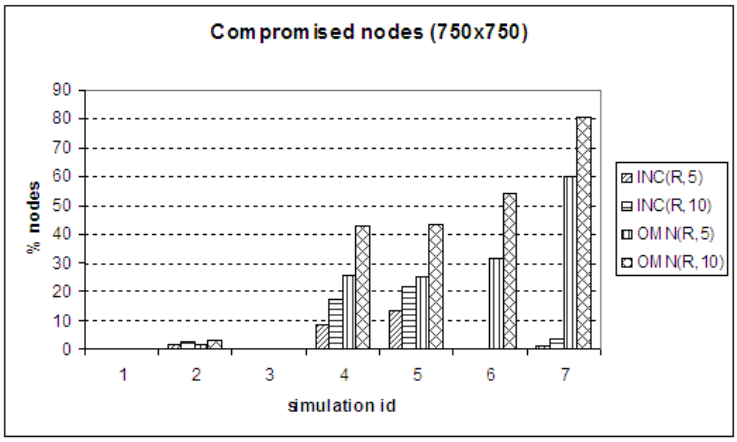

Figure 58: Compromised nodes – 750x750 NLOS Persistent attack strategy

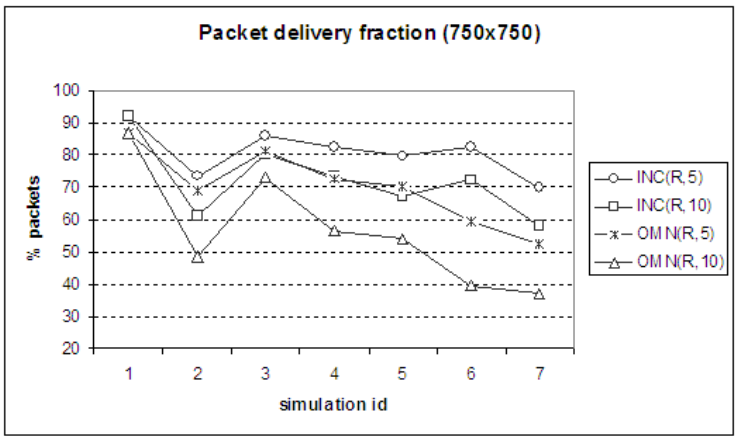

Figure 59: Packet delivery – 750x750 NLOS Persistent attack strategy

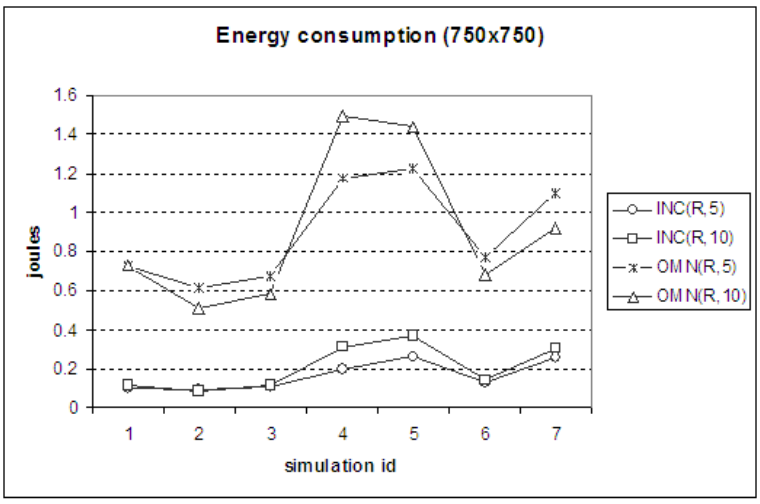

Figure 60: Energy consumption – 750x750 NLOS Persistent attack strategy

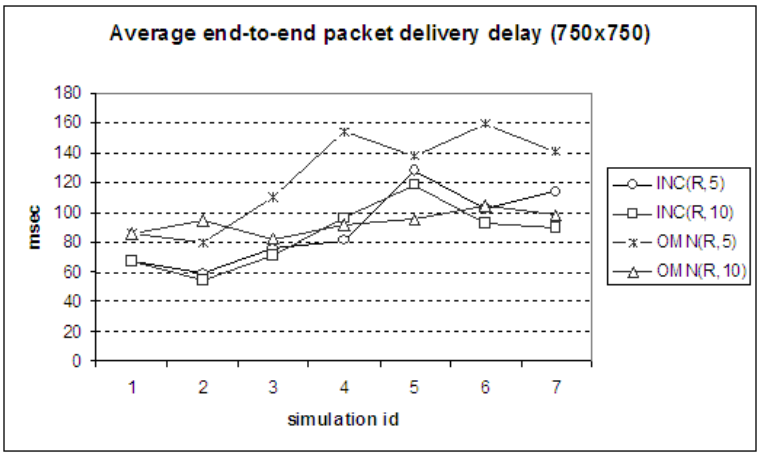

Figure 61: Packet delivery delay – 750x750 NLOS Persistent attack strategy

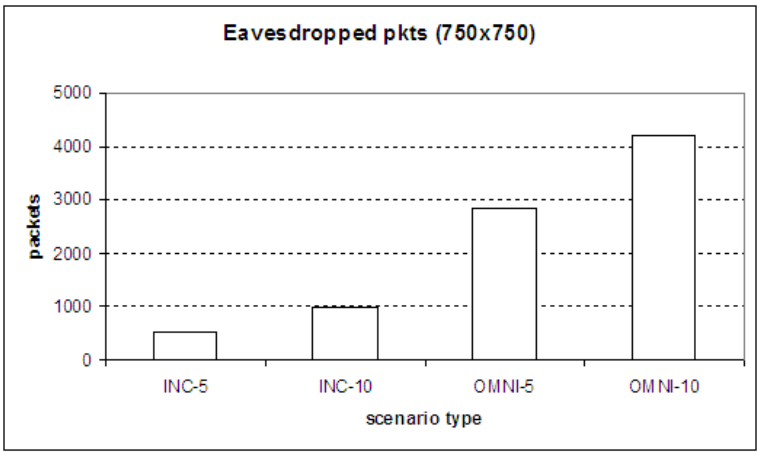

Figure 62: Eavesdropped packets – 750x750 NLOS Persistent attack strategy

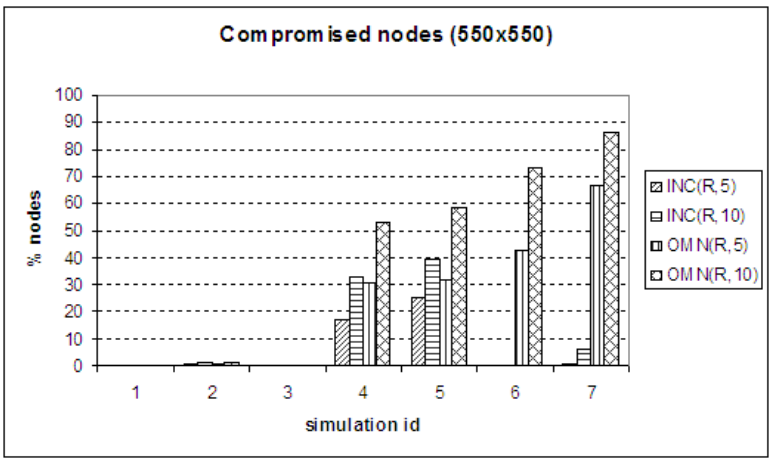

Figure 63: Compromised nodes – 550x550 NLOS Persistent attack strategy

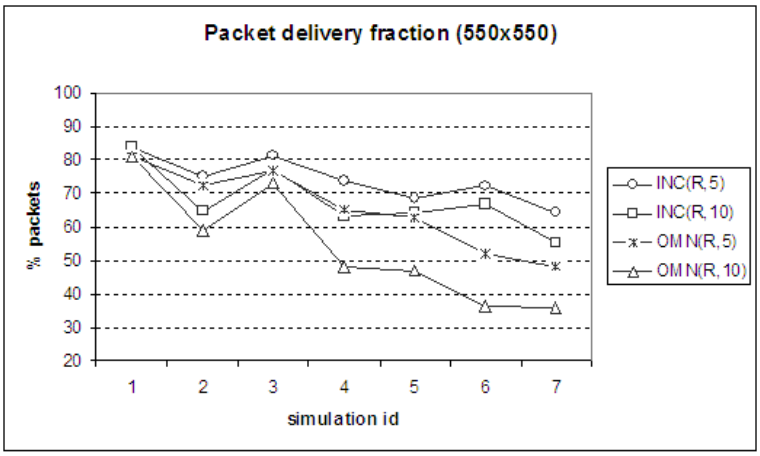

Figure 64: Packet delivery – 550x550 NLOS Persistent attack strategy

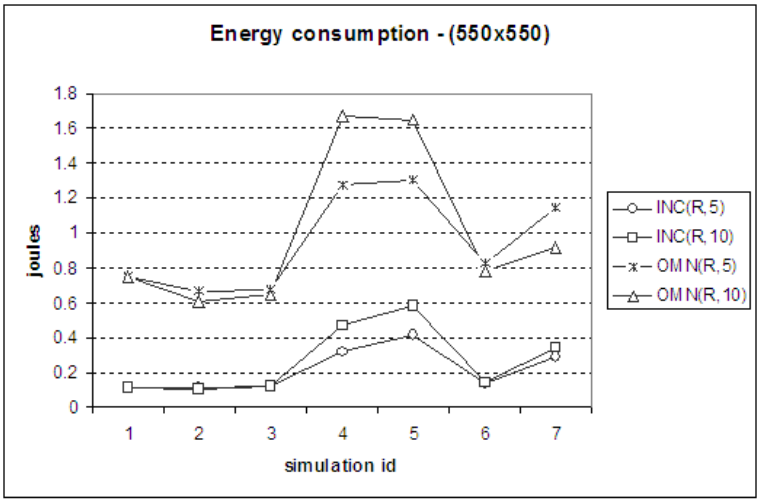

Figure 65: Energy consumption – 550x550 NLOS Persistent attack strategy

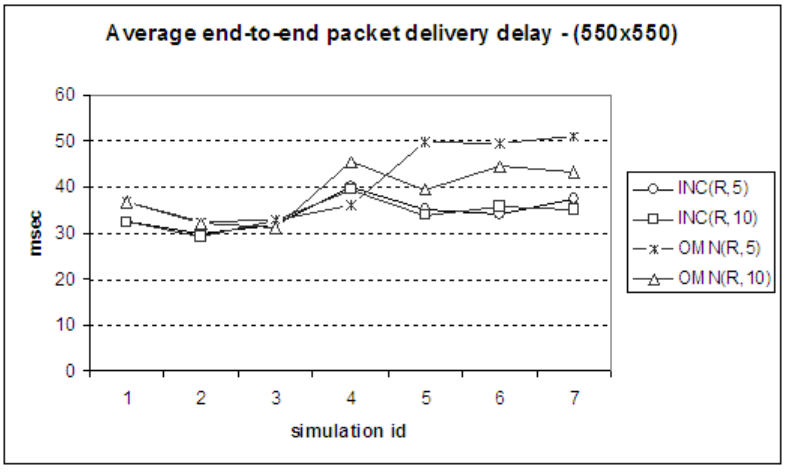

Figure 66: Packet delivery delay – 550x550 NLOS Persistent attack strategy

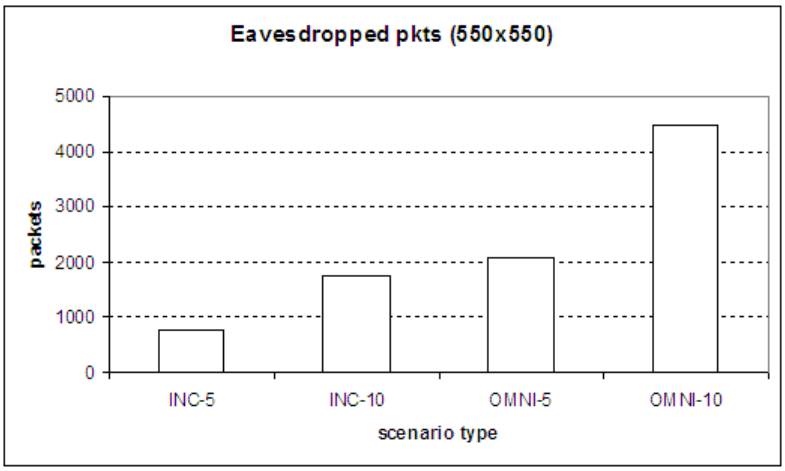

Figure 67: Eavesdropped packets – 550x550 NLOS Persistent attack strategy

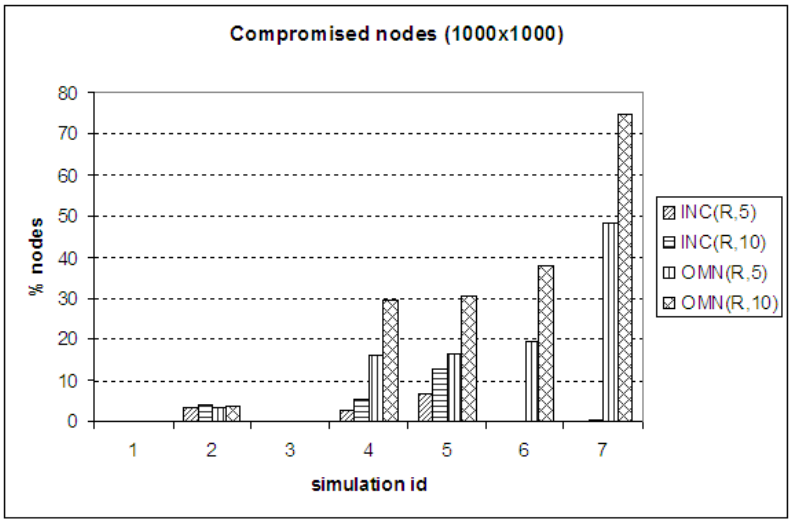

Figure 68: Compromised nodes – 1000x1000 NLOS Persistent attack strategy

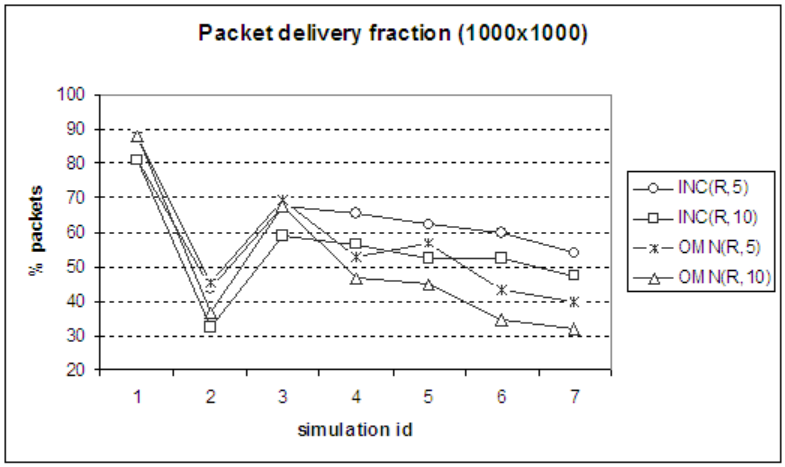

Figure 69: Packet delivery – 1000x1000 NLOS Persistent attack strategy

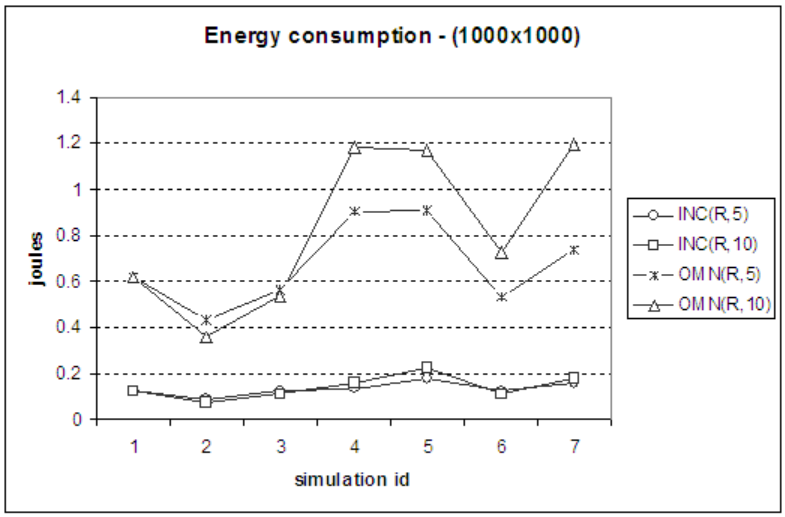

Figure 70: Energy consumption – 1000x1000 NLOS Persistent attack strategy

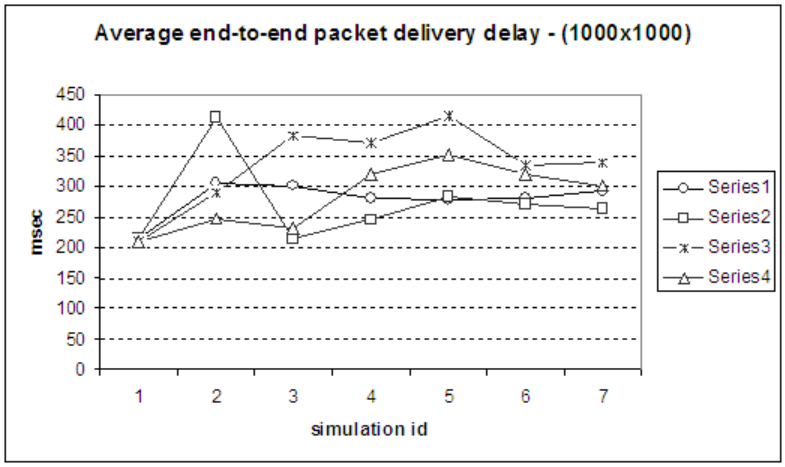

Figure 71: Packet delivery delay – 1000x1000 NLOS Persistent attack strategy

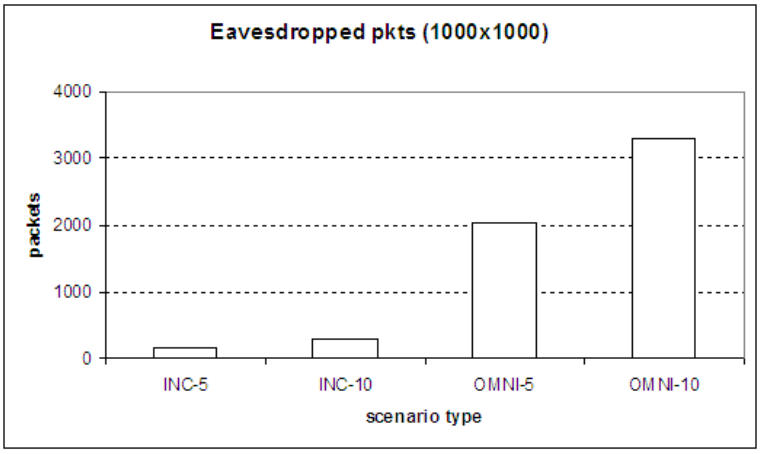

Figure 72: Eavesdropped packets – 1000x1000 NLOS Persistent attack strategy

Confidence Intervals NLOS scenarios						
Compromised Nodes (%) - INCURE						
	550x550		750x750		1000x1000	
Blackhole attack	0.413916	0.48589	0.500807	0.498598	0.413916	0.441615
Recovery	0	0	0	0	0	0
Eavesdrop & Reactive DoS	4.679609	6.588119	3.069804	4.50068	1.347919	2.360121
Continuous DoS	3.099293	5.308315	2.345012	3.677226	1.452005	1.883447
Recovery	0.090788	0.10854	0.109189	0	0.065333	0
Ext DoS & Recovery	0.437597	1.55556	0.464201	0.603126	0.109189	0.135641
Compromised Nodes (%) - OMNI						
Blackhole attack	0.386708	0.526594	0.372161	0.408907	0.421143	0.435574
Recovery	0	0	0	0	0	0
Eavesdrop & Reactive DoS	4.438242	3.406959	1.562169	2.676798	1.165944	1.234914
Continuous DoS	3.741508	3.777039	2.702627	3.340272	1.216602	1.281416
Recovery	3.326075	1.42189	0.993129	1.759949	1.116482	1.641378
Ext DoS & Recovery	3.888256	1.590601	5.241515	2.651494	2.806057	2.159815
Packet delivery (%) - INCURE						
Normal	8.208579	8.208579	3.622772	3.622772	9.209308	9.209308
Blackhole attack	8.725807	8.925389	6.969696	7.974248	8.903563	7.622335
Recovery	7.950186	7.844599	3.934804	5.110837	7.688591	8.185319
Eavesdrop & Reactive DoS	7.025384	8.267243	4.263218	4.785798	8.018563	8.375077
Continuous DoS	6.813776	7.591966	4.178398	5.109584	7.832404	7.102753
Recovery	7.001361	7.309268	3.825451	4.271868	7.941229	7.48125
Ext DoS & Recovery	6.249415	5.902016	4.181982	3.58163	7.026914	6.548864
Packet delivery (%) - OMNI						
Normal	6.594649	6.594649	7.208204	7.208204	7.365919	7.365919
Blackhole attack	6.415493	7.414776	8.387707	8.800046	7.107171	6.172158
Recovery	6.159841	5.835341	7.266651	6.778255	7.143991	7.046925
Eavesdrop & Reactive DoS	6.748748	5.530445	7.338521	6.839042	6.800008	6.136587
Continuous DoS	5.485456	4.908678	7.404795	6.652519	5.950307	6.229338
Recovery	5.635956	3.285595	6.285263	4.939403	5.169183	4.28155
Ext DoS & Recovery	4.984443	3.116572	5.598168	4.209079	4.277297	3.554353
Energy consumption (J) - INCURE						
Normal	0.013887	0.013887	0.008658	0.008658	0.011891	0.011891
Blackhole attack	0.012643	0.012411	0.010504	0.008265	0.009116	0.00732
Recovery	0.013328	0.01336	0.008685	0.009448	0.010152	0.009819
Eavesdrop & Reactive DoS	0.062246	0.083556	0.034469	0.058554	0.01534	0.028249
Continuous DoS	0.039261	0.071278	0.02364	0.043861	0.019341	0.026457
Recovery	0.011548	0.01276	0.009059	0.015359	0.007419	0.008105
Ext DoS & Recovery	0.016334	0.012654	0.010816	0.010125	0.007288	0.007238
Energy consumption (J) - OMNI						
Normal	0.109314	0.109314	0.092267	0.092267	0.058436	0.058436
Blackhole attack	0.093798	0.079871	0.068632	0.063116	0.052503	0.043998

Recovery	0.092394	0.075315	0.075933	0.062138	0.0589	0.05443
Eavesdrop & Reactive DoS	0.13809	0.201619	0.100152	0.109945	0.066006	0.073567
Continuous DoS	0.117932	0.216498	0.079293	0.129987	0.060838	0.063138
Recovery	0.08112	0.050613	0.053722	0.04416	0.042637	0.045538
Ext DoS & Recovery	0.118006	0.064261	0.085934	0.058996	0.042414	0.057206
End-to-end packet delivery delay (msec) - INCURE						
Normal	9.460335	9.460335	21.91873	21.91873	71.85776	71.85776
Blackhole attack	9.506773	9.587873	22.37099	29.36505	144.7459	218.8955
Recovery	9.587104	10.61505	21.92351	25.54256	115.2097	71.54499
Eavesdrop & Reactive DoS	15.06744	15.35677	27.85906	33.6996	115.7293	95.4908
Continuous DoS	11.64876	10.22978	43.59537	45.7812	84.8969	94.67553
Recovery	11.95651	12.20494	28.46514	31.35754	92.06648	86.37109
Ext DoS & Recovery	12.0254	11.29664	28.80128	32.16105	89.89244	95.3618
End-to-end packet delivery delay (msec) - OMNI						
Normal	9.330155	9.330155	35.87393	35.87393	85.72002	85.72002
Blackhole attack	9.396782	10.32154	37.45467	62.76846	133.062	131.3508
Recovery	9.392574	9.194828	45.14497	32.13095	133.0085	67.52898
Eavesdrop & Reactive DoS	10.25899	15.4426	49.40517	29.9493	133.4133	116.6955
Continuous DoS	32.88711	15.94625	53.91579	35.96463	125.9758	145.3243
Recovery	14.40205	18.56556	50.8658	49.53403	142.8735	149.6783
Ext DoS & Recovery	15.62075	18.56038	58.77367	50.04342	144.6706	151.0605

Bibliography

[1] Garcia-Hernandez, C. F., Ibarguengoytia-Gonzalez, P. H., Garcia-Hernandez, J. and Perez-Diaz, J. A. 2007. Wireless sensor networks and application: a survey, International Journal of Computer Science and Network Security (IJCSNS). 7, 3, 2007, pp. 264-273.

[2] E-sense, Capturing ambient intelligence for mobile communications through wireless sensor networks, IST-FP6-IP-027227, http://www.ist-e-sense.org/, 2006-2007.

[3] Kuorilehto, M., Hännikäinen, M., and Hämäläinen, T. D. 2005. A Survey of Application Distribution in Wireless Sensor Networks, EURASIP Journal of Wireless Comm. and Networking, vol. 4, pp. 774-788.

[4] Römer, K. and Mattern, F. 2004. The Design Space of Wireless Sensor Networks, IEEE Wireless Communications, vol. 11, pp. 54-61.

[5] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. 2002. Wireless Sensor Networks: A Survey, Computer Networks (Elsevier) Journal, vol. 38, no. 4, pp. 393-422.

[6] Padmavathi, G. and Shanmugapriya, D. 2009. A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, (IJCSIS) International Journal of Computer Science and Information Security, vol. 4, no. 1 & 2.

[7] Karlof, C., and Wagner, D. 2003. Secure routing in wireless sensor networks: Attacks and Countermeasures, In Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.

[8] Wang, Y., Attebury, G., and Ramamurthy, B. 2006. A survey of security issues in wireless sensor networks, IEEE Communications Surveys & Tutorials, 8 (2), pp. 2–23.

[9] Anjum, F., and Mouchtaris, P. 2007. Security for wireless ad hoc networks, Wiley-Interscience, 2007.

[10] Introduction to NISTIR 7628: Guidelines for smart grid cyber security, September 2010.

[11] Komninos, N., Vergados, D., and Douligeris, C. 2006. Layered security design for mobile ad hoc networks, Computers & Security, Elsevier, 25, pp. 121-130.

[12] Stavrou, E. and Pitsillides, A. 2010. A Survey on Secure Multipath Routing Protocols in WSNs, Computer Networks Journal (COMNET), 2010, 54, 13.

[13] Lee, S. and Choi, Y. 2006. A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks, Fourth ACM Workshop on Security of Ad hoc and Sensor Networks (SASN'06), pp. 59–70.

[14] Wood, A. D., and Stankovic, J. A. 2002. Denial of Service in Sensor Networks, IEEE Computer, 2002, 35, 10, pp. 54-62.

[15] Raymond, D.R., and Midkiff, S.F. 2008. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses, IEEE Pervasive Computing, 7, 1, 2008, pp. 74-81.

[16] Saunders, S., and Aragón-Zavala, A. 2007. Antennas and Propagation for Wireless Communication Systems, 2nd edition, Wiley, ISBN-10: 0470848790.

[17] Walters, J.P., Liang, Z., Shi, W. and Chaudhary, V. 2006. Wireless sensor network security: a survey, Book Chapter in Security in Distributed, Grid and Pervasive Computing, Auerbach Publications, CRC Press.

[18] Becher, A., Benenson, Z. and Dornseif, M. 2006. Tampering with motes: real-world physical attacks on wireless sensor networks, International Conference on Security in Pervasive Computing (SPC), pp. 104-118.

[19] Software Engineering Institute, Carnegie Mellon University, 2000. Survivable Network Analysis, ESC-TR-2000-013.

[20] Giannetsos, T., Dimitriou, T. and Prasad, N. R. 2010. Weaponizing Wireless Networks: An Attack Tool for Launching Attacks against Sensor Networks, Black Hat Europe 2010: Digital Self Defense.

[21] Chan, H., Perrig, A., and Song, D. 2003. Random key predistribution schemes for sensor networks, In Proceedings of the 2003 IEEE Symposium on Security and Privacy, pp. 197.

[22] Eschenauer, L., and Gligor, V. D. 2002. A key-management scheme for distributed sensor networks, 9th ACM conference on Computer and communications security, pp. 41–47.

[23] Lazos, L., and Poovendran, R. 2005. Serloc: Robust localization for wireless sensor networks, ACM Transactions on Sensor Networks, vol. 1, no. 1, pp. 73–100.

[24] Hu, L., and Evans, D. 2003. Secure Aggregation for Wireless Networks, Workshop Security and Assurance in Ad Hoc Networks.

[25] Ozdemir, S. 2007. Secure and reliable data aggregation for wireless sensor networks, 4th international conference on Ubiquitous computing systems, pp. 102–109.

[26] Brutch, P. and Ko, C. 2003. Challenges in intrusion detection for wireless ad-hoc networks, Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), pp. 368

[27] Anantvalee, T. and Wu, J. 2006. A Survey on Intrusion Detection in Mobile Ad Hoc Networks, Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D. -Z. Du (eds.), Springer, pp. 170-196.

[28] Sun, B., Osborne, L., Xiao, Y. and Guizani, S. 2007. Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks, IEEE Wireless Communications, vol. 14, no. 5, pp. 56-63.

[29] Loo, C.E., Ng, M.Y., Leckie, C. and Palaniswami, M. 2006. Intrusion detection for routing attacks in sensor networks. International Journal of Distributed Sensor Networks, vol. 2, no. 4, pp. 313-332.

[30] Marti, S., Giuli, T., Lai, K. and Baker, M. 2000. Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks, In Proceedings of the Sixth Annual International Conference on Mobile Communication and Networking, (MOBICOM), pp. 255 – 265.

[31] Lee, S. and Choi, Y. 2006. A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks, Proceedings of the fourth ACM workshop on security of ad hoc and sensor networks (SASN 06), pp. 59-70.

[32] Du, W., Fang, L. and Ning, P. 2006. LAD: Localization Anomaly Detection for Wireless Sensor Networks, Journal of Parallel and Distributed Computing, vol. 66, no. 7, pp. 874-886.

[33] Wang, G., Zhang, W., Cao, C. and Porta, T.L. 2003. On supporting distributed collaboration in sensor networks, In Proceedings of Military Communications Conference, (MILCOM), pp. 752-757.

[34] Buchegger, S. and Boudec, J., 2002. Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-hoc Networks), In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (MOBIHOC), pp.226-236.

[35] Lee, S. and Choi, Y. 2006. A secure alternate path routing in sensor networks, Computer Communications, Elsevier, vol. 30, no. 1, pp. 153-165.

[36] Trang, C. M., Kong, H-Y. and Lee, H-H. 2006. A Distributed Intrusion Detection System for AODV, Asia-Pacific Conference on Communications, 1-4.

[37] Krontiris, I., Benenson, Z., Giannetsos, T., Freiling, F. C. and Dimitriou, T. 2009. Cooperative Intrusion Detection in Wireless Sensor Networks, In EWSN '09: Proceedings of the 6th European Conference on Wireless Sensor Networks, Berlin, Heidelberg, 2009, Springer-Verlag, pp. 263-278.

[38] Aivaloglou, E., Mitseva, A., Skianis, C., Gritzalis, S., Waller., A. and Prasad., N. R. 2007 Scalable Security Management for Wireless Sensor Networks for Medical Scenarios, 10th International Symposium on Wireless Personal Multimedia Communications (WPMC), pp.1014-1018.

[39] Sang Hyuk Lee, Soobin Lee, Heecheol Song and Hwang Soo Lee. 2009. Wireless sensor network design for tactical military applications: Remote large-scale environments, IEEE Military Communications Conference (MILCOM), pp. 1-7.

[40] Michahelles, F., Matter, P., Schmidt, A. and Schiele, B. 2003. Applying Wearable Sensors to Avalanche Rescue. Computers and Graphics, 27, 6, pp.839–847.

[41] Wood, A., Virone, G., Doan, T., Cao, Q., Selavo, L., Wu, Y., Fang, L., He, Z., Lin, S. and Stankovic, J. 2006. ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring, Technical Report CS-2006-13, University of Virginia.

[42] Crosby, G. V., Pissinou, N., and Makki, K. 2006. Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks, International Journal of Network Security (IJNS), 2006.

[43] Hegazy, I., Safavi-Naini, R. and Williamson, C. 2010, Towards Securing MintRoute in Wireless Sensor Networks, IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010, Montreal, QC, Canada, pp.1-6.

[44] Tanachaiwiwat, S., Dave, P., Bhindwale, R., and Helmy, A. 2004. Location-centric Isolation of Misbehavior and Trust Routing in Energy-Constrained Sensor Networks", IEEE International Conference on Performance, Computing, and Communications, 2004, pp. 463 – 469.

[45] Dini, G., and Savino, I.M. 2006. An Efficient Key Revocation Protocol for Wireless Sensor Networks, Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks, pp. 450 – 452.

[46] Chan, H., Gligor, V., Perrig, A., and Muralidharan, G, 2005. On the distribution and revocation of cryptographic keys in sensor networks, IEEE Transactions on Dependable and Secure Computing, 2005, 2, 3, pp. 233–247.

[47] Hung, K.-S., Law, C.-F., Lui, K.-S., and Kwok, Y.-K. 2009. On Attack-Resilient Wireless Sensor Networks with Novel Recovery Strategies, In IEEE Wireless Communications & Networking Conference (WCNC), Budapest, Hungary, pp. 2272-2277.

[48] Raymond, D. R. 2008. Denial-of-Sleep Vulnerabilities and Defenses in Wireless Sensor Network MAC Protocols, Thesis, Virginia Tech University.

[49] Ashraf, F., Yih-Chun Hu and Kravets, R.H. 2011. Bankrupting the jammer, Sensor, 8th Annual IEEE Communications Society Conference on Mesh and Ad Hoc Communications and Networks (SECON), pp. 149-151.

[50] Ye, W., Heidemann, J. and Estrin, D. 2002. An energy-efficient MAC protocol for wireless sensor networks. INFOCOM, pp. 1567 - 1576.

[51] Raymond, D. R. and Midkiff, S. F. 2007. Clustered Adaptive Rate Limiting: Defeating Denial-of-Sleep Attacks in Wireless Sensor Networks, IEEE Military Communications Conference (MILCOM), pp. 1-7.

[52] Halder, S., Mobashir, M., Saraogi, R.K. and DasBit, S. 2011. A Jamming Defending Data-Forwarding Scheme for Delay Sensitive Applications in WSN, International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), pp. 1-5.

[53] Anastasi, G., Conti, M., Francesco, M. D., and Passarella, A. 2009. Energy Conservation in Wireless Sensor Networks: a Survey, Ad Hoc Networks, Elsevier, vol. 7, no. 3, pp. 537-568.

[54] Wood, A.D., Stankovic, J.A., and Son, S.H. 2003. JAM: a jammed-area mapping service for sensor networks, 24th IEEE Real-Time Systems Symposium, 2003.

[55] Xu, W., Trappe, W., and Zhang, Y. 2007. Channel Surfing: Defending Wireless Sensor Networks from Interference, 6th International Conference on Information Processing in Sensor Networks (IPSN07), pp.499-508, 2007.

[56] Xu, W., Wood, T., Trappe, W. and Zhang, Y. 2004. Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service, ACM workshop on Wireless security (WiSe), pp. 80 - 89.

[57] Misra, S., Agrawal, D. and Rayankula, A. 2008. Using Honeynodes along with Channel Surfing for Defense against Jamming Attacks in Wireless Networks, International Conference on Systems and Networks Communications (ICSNC '08), pp. 197-201.

[58] Justin Raj S.S., and Thilagavathy, D. 2012. Security threats and jamming attacks of multi channel wireless sensor networks, International Journal of P2P Network Trends and Technology (IJPTT), pp. 27 – 31.

[59] Strasser, M. and Vogt, H. 2006. Autonomous and Distributed Node Recovery in Wireless Sensor Networks, 4th ACM CCS Workshop on Security of Ad Hoc and Sensor Networks (SASN), Alexandria, Virginia, USA, pp. 113-122.

[60] Li, B., Doss, R., Batten, L.M. and Schott, W. 2009, Fast recovery from node compromise in wireless sensor networks, International Conference on New Technologies, Mobility and Security (NTMS), pp. 1-6.

[61] Jun-Zhao Sun. 2010. OS-based reprogramming techniques in wireless sensor networks: A survey, IEEE International Conference on Ubi-media Computing (U-Media), pp17-23.

[62] Al-Karaki, J.N., and Kamal, A.E.. 2004. Routing techniques in wireless sensor networks: a survey, IEEE Wireless Communications ,11 (6), pp. 6–28.

[63]Pantazis, N., Nikolidakis, S., and Vergados, D. 2012. Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey, IEEE Communications Surveys & Tutorials, no. 99, pp. 1-41.

[64] Zhao, L., and Delgado-Frias, J.G. 2006. Multipath routing based secure data transmission in adhoc networks, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2006), Montreal, Canada, June 19–21, 2006.

[65] Al-Wakeel, S.S., and Al-Swailemm, S.A. 2007. PRSA: a path redundancy based security algorithm for wireless sensor networks, in: IEEE Wireless Communications and Networking Conference (WCNC 2007), 2007.

[66] Ling, H., and Znati, T. 2005. End-to-end pairwise key establishment using multipath in wireless sensor network, in: Proceedings of the IEEE Global Communications Conference (GLOBECOM 2005), St. Louis, MO, November 2005.

[67] Abu-Ghazaleh, N., Kang, K., and Liu, K. 2005. Towards resilient geographic routing in WSNs, in: Proceedings of the First ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks, Montreal, Quebec, Canada, 2005, pp. 71–78.

[68] Nasser, N and Chen, Y. 2007. SEEM: secure and energy-efficient multipath routing protocol for wireless sensor networks, Computer Communications, Elsevier, vol. 30, issue 11-12, pp. 2401–2412.

[69] Zhao, L. and Delgado-Frias, J.G. 2006. Multipath routing based secure data transmission in adhoc networks, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2006), Montreal, Canada.

[70] Liao, C-Fu., Lu, Y-F., Pang, Ai-C. and Kuo, T-W. 2008. A secure routing protocol for wireless embedded networks, 14th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications.

[71] Deng, J., Han, R., and Mishra, s. 2002. INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks, Technical Report CUCS-939-02, Department of Computer Science, University of Colorado.

[72] Lu, F., Geng, L., Chia, LT., and Liang, YC. 2007. Secure multi-path in sensor networks, Proceedings of the 5th International Conference on Embedded Networked Sensor Systems (SenSys ‘07), 2007, pp. 413-414.

[73] Zhang, Y., Yang, J, and Vu, H. T. 2006. The Interleaved Authentication for Filtering False Reports in Multipath Routing based Sensor Networks, 20th International IEEE Parallel and Distributed Processing Symposium (IPDPS’06).

[74] Ma, R., Xing, L., and Michel, H. E. 2007. A New Mechanism for Achieving Secure and Reliable Data Transmission in Wireless Sensor Networks, Proc. of The 2007 IEEE Conference on Technologies for Homeland Security, Woburn, MA, May 16-17, 2007, pp. 274-279.

[75]Lou, W., and Kwon, Y. 2006. H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks, IEEE Transactions on Vehicular Technology, vol. 55, no. 4, July 2006, pp. 1320 – 1330.

[76] Shamir, A. 1979. How to share a secret, Communications of the ACM, vol. 22, no. 11, Nov. 1979, pp. 612-613.

[77] Deb, B., Bhatnagar, S., and Nath, B. 2003. ReInForM: Reliable Information Forwarding Using Multiple Paths in Sensor Networks. In Proceedings of the 28th Annual IEEE International Conference on Local Computer Networks (LCN'03), Bonn, Germany, 20–24 October 2003; pp. 406–415.

[78] Chiti, F., Ciabatti, M., Collodi, G., Di Palma, D., Fantacci, R., Manes, G., Manes, A., and Nelli, I. 2008. D-STAR MAC Protocol: A Cross Layer Solution for Wireless Sensor Networks Endowed with Directive Antennas, Wireless Personal Communications Journal, Springer, vol. 47, no. 1, pp. 15 - 26.

[79] Felemban, E., Vural, S., Murawski, R., Ekici, E., Lee, K., Moon, Y., and Park, S. 2010. SAMAC: A Cross-Layer Communication Protocol for Sensor Networks with Sectored Antennas, IEEE Transactions on Mobile Computing, vol. 9, no. 8, pp. 1072-1088.

[80] Zhang, S. and Datta, A. 2005. A Directional-Antenna Based MAC Protocol for Wireless Sensor Networks, International Conference on Computational Science and Its Applications, Singapore, Volume Part II, pp. 686 – 695.

[81] Dunlop, J. and Cortes, J. 2008. Co-Design of Efficient Contention MAC with Directional Antennas in Wireless Sensor Networks, International Wireless Communications and Mobile Computing Conference, pp. 383 – 388.

[82] Ko, Y., Shankarkumar, V., and Vaidya, N. 2000. Medium Access Control Protocols Using Directional Antennas in Ad Hoc Networks, IEEE INFOCOM, pp. 13-21.

[83] Ramanathan, R., Redi, J., Santivanez, C., Wiggins, D., and Polit, S. 2005. Ad Hoc Networking with Directional Antennas: A Complete System Solution, IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 496-506.

[84] Nasipuri, A., Ye, S., You, J., and Hiromoto, R. E. 2000. A MAC Protocol for Mobile Ad Hoc Networks Using Directional Antennas, IEEE Wireless Communications and Networking Conference, vol. 3, pp. 1212 – 1219.

[85] Hu, L., Evans, D. 2004. Using directional antennas to prevent wormhole attacks, in Network and Distributed System Security Symposium (NDSS), 2004.

[86] Lazos, L. and Poovendran, R. 2006. 13.High Resolution Localization for Wireless Sensor Networks, IEEE Journal on Selected Areas in Communications, Special Issue on Network Security, (JSAC), vol. 24, no. 2, pp. 233 – 246.

[87] Lakshmanan, S., Tsao, C-L., Sivakumar, R., and Sundaresan, K. 2008. Securing Wireless Data Networks against Eavesdropping using Smart Antennas, 28th International Conference on Distributed Computing Systems.

[88] Sheth, A., Seshan, S., and Wetherall, D. 2009. Geo-fencing: Confining Wi-Fi Coverage to Physical Boundaries, International Conference on Pervasive Computing, (Berlin, Heidelberg), pp. 274-290.

[89] Tangpong, A., Kesidis, G., Hsu, H-y. and Hurson, A. 2009. Robust Sybil detection for MANETS, 18th International Conference on Computer Communications and Networks, pp. 1-6.

[90] Suen, T. and Yasinsac, A. 2005. Peer identification in wireless and sensor networks using signal properties, IEEE International Conference on Mobile Adhoc and Sensor Systems.

[91] Piro, C., Shields, C. and Levine, B. N. 2006. Detecting the Sybil attack in mobile adhoc networks, IEEE/ACM SecureComm, pp. 1-11.

[92] Stavrou, E. and Pitsillides, A. Vulnerability assessment of intrusion recovery countermeasures in wireless sensor networks, 16th IEEE Symposium on Computers and Communications (ISCC), pp. 706-712, June 28 - July 1, 2011, Kerkyra, Greece

[93] Stavrou, E. and Pitsillides, A. 2011. Combating persistent adversaries in wireless sensor networks using directional antennas, 18th International Conference on Telecommunications (ICT), pp. 433-438, May 8 – 11, 2011, Ayia Napa, Cyprus

[94] Stavrou, E., Pitsillides, A., Hadjichristofi, G., and Hadjicostis, C. Security in future mobile sensor networks - Issues and Challenges, International Conference on Security and Cryptography, July 26-28, 2010, Athens, Greece

[95] Security Policy Roadmap - Process for Creating Security Policies, SANS Institute

[96] Claycomb, W. R., and Shin, D. 2011. A novel node level security policy framework for wireless sensor networks, Journal of Network and Computer Applications, Elsevier, 34, pp. 418–428.

[97] Claycomb, W., Lopes, R., and Shin, D. 2010. A Group-Based Security Policy for Wireless Sensor Networks, Proceedings of the 2010 ACM Symposium on Applied Computing, pp. 778 -785.

[98] Slijepcevic, S., Tsiatsis, V., and Zimbeck, S. 2002. On Communication Security in Wireless Ad-Hoc Sensor Networks, 11th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 139 - 144.

[99] de Oliveira, S., de Oliveira, T. R, and Nogueira, J. M. 2009. A Policy based Security Management Architecture for Sensor Networks, IFIP/IEEE International Symposium on Integrated Network Management, pp. 315 – 318.

[100] van Vliet, H. 2008. Software Engineering: Principles and Practice, Third edition, John Wiley & Sons.

[101] Software development process,
http://en.wikipedia.org/wiki/Software_development_process

[102] Bahl, N., Sharma, A. K. and Verma, H. K. 2012. On Denial of Service Attacks for Wireless Sensor Networks, International Journal of Computer Applications, vol. 43, no. 6.

[103] IEEE standard 802.15.4

[104] California Eastern Laboratories (CEL), PG2409T6X switch

[105] Hittite, HMC347 switch

[106] Backes, W. and Cordasco, J. 2010. MoteAODV – An AODV Implementation for TinyOS 2.0. Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices, Lecture Notes in Computer Science, vol. 6033, pp 154-169.

[107] Kulik, J., Heinzelman, W., and Balakrishnan,H. 2002. Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks, Wireless Networks Journal, vol. 8, pp. 169–185.

[108] Babbitt, A., Morrell, C., Szymanski, B. K., and Branch, J. W. 2008. Self-Selecting Reliable Paths for Wireless Sensor Network Routing, Computer Communication Journal, Elsevier, vol. 31, no. 16, pp. 3799-3809.

[109] Simón, R., Huggard, M., Goldrick, C. Mc. 2008. TinyHop - An End-to-End routing protocol for Peer-to-Peer communication in Wireless Sensor Networks, Middleware for network eccentric and mobile applications, pp. 5 – 9.

[110] ZigBee Architecture Overview, http://www.zigbee.org/zigbee/en/events/documents/April2006_ESC_Presentations/043120r11ZB_TAG-ZigBeeV1-0Architecture%5B1%5D.pdf

[111] Xiao, H., Lu, C. and Ogai, H. 2012. A Multi-hop Low Cost Time Synchronization Algorithm for Wireless Sensor Network in Bridge Health Diagnosis System, IEEE 18th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), pp. 392-395.

[112] Zheng, T., Qin, Y., Gao, D., Duan, J. and Zhang, H. 2010. A practical deployment of Intelligent Building Wireless Sensor Network for environmental monitoring and air-conditioning control, IEEE International Conference on Network Infrastructure and Digital Content, pp. 624-628.

[113] Yamazaki, T., Kayama, K. and Igi, S. 2007. Detection of People and Tracking Test Bed Using Multiple Sensors, International Conference on Multimedia and Ubiquitous Engineering, pp. 135-140.

[114] Burrell, J., Brooke, T. and Beckwith, R. 2004. Vineyard Computing: Sensor Networks in Agricultural Production. IEEE Pervasive Computing, Vol.3, No.1, pp. 38-45.

[115] Mainwaring, A., Polastre, J., Szewczyk, R., Culler, D. and Anderson, J. 2002. Wireless Sensor Networks for Habitat Monitoring. In ACM International Workshop on Wireless Sensor Networks and Applications (WSNA'02), Atlanta, GA.

[116] Stavrou, E. and Pitsillides, A. Security Evaluation Methodology for Intrusion Recovery Protocols in Wireless Sensor Networks, 15th ACM International Conference on Modeling,

Analysis and Simulation of Wireless and Mobile Systems, MSWiM' 12, October 21–25, 2012, Paphos, Cyprus

[117] IP Packet Delay Variation Metric for IP Performance Metrics http://www.ietf.org/rfc/rfc3393.txt

[118] The network simulator - ns2, http://www.isi.edu/nsnam/ns/

[119] Kang, W., Stankovic, J. A. and Son, S. H. 2008. On Using Weather Information for Efficient Remote Data Collection in WSN, 5th ACM Workshop on Embedded Networked Sensors (HotEmNets).

[120] Ramachandran, S. and Shanmugan, V. 2011. Impact of Sybil and Wormhole Attacks in Location Based Geographic Multicast Routing Protocol for Wireless Sensor Networks, Journal of Computer Science, vol. 7, pp. 973-979.

[121] Perkins, C., Royer, E. M., and Das, S. 2003. Ad hoc On-Demand Distance Vector (AODV) Routing, IETF RFC 3561.

[122] Giorgetti, G., Cidronali, A., Gupta., S.K.S., and Manes, G. 2007. Exploiting Low-Cost Directional Antennas in 2.4GHz IEEE 802.15.4 Wireless Sensor Networks, EUMW07: The 37th European Microwave Conference, 2007, Munich, Germany.

[123] CC2400 datasheet, http://www.ti.com/lit/ds/symlink/cc2400.pdf

[124] Dan, A., Halder, S. and DasBit, S. 2011. Localization with enhanced location accuracy using RSSI in WSN, IEEE 5th International Conference on Advanced Networks and Telecommunication Systems (ANTS), pp. 1-6.

[125] Musikanon, O. and Chongburee, W. 2012. ZigBee Propagations and Performance Analysis in Last Mile Network, International Journal of Innovation, Management and Technology, vol. 3, no. 4, pp. 353 – 357.

[126] Azim, M. A., Kibria, M. R. and Jamalipour, A. 2008. Designing an Application-Aware Routing Protocol for Wireless Sensor Networks, IEEE Global Telecommunications Conference (GLOBECOM).

[127] Di Marco, P., Fischione, C., Santucci, F. and Johansson, K. H. 2012. Modeling IEEE 802.15.4 networks over fading channels, Cornell University, 1209.3203.

[128] Liechty, L. C. 2007. Path Loss Measurements and Model Analysis of a 2.4 GHz Wireless Network in an Outdoor Environment, MSc Thesis, Georgia Institute of Technology.

[129] Debnath, D., Hossain, C. A., Islam, R., Tarique M. and Dutta, I. K. 2011. Minimizing Shadowing Effects on Mobile Ad hoc Networks, Journal of Selected Areas in Telecommunications, pp. 46- 51.

[130] LS Research, ProFLEX01 Transceiver Module datasheet, http://www.lsr.com/downloads/products/330-0001.pdf

[131] MICAz datasheet, http://www.openautomation.net/uploadsproductos/micaz_datasheet.pdf

[132] Tmote-sky datasheet, http://www.eecs.harvard.edu/~konrad/projects/shimmer/references/tmote-sky-datasheet.pdf

[133] Madan, V., and Reddy, SRN. 2012. Review of Wireless Sensor Mote Platforms, International Journal of Electrical, Electronics & Communication Engineering, vol.2, no. 2, pp. 50 – 55.

[134] Leang, D., and Kalis, A. 2004. Smart Sensor DVB sensor network development boards with smart antennas, International Conference on Communications, Circuits and Systems, ICCCAS, pp. 1476 – 1480.

[135] FR-4, http://www.g10fr4.com/g10_fr4_sheet_material.html

[136] uPG2030TK-A switch, http://eu.mouser.com/ProductDetail/CEL/UPG2030TK-A/?qs=sGAEpiMZZMuCmTIBzycWfH8S5%252b0z7Pdc5GHKpsU6doI%3d

[137] Wolff, C. Antenna characteristics, Available: http://www.radartutorial.eu/06.antennas/an05.en.html

[138] Issariyakul, T., and Hossain, E. 2008. Introduction to Network Simulator NS2, Springer.

[139] AWK, http://en.wikipedia.org/wiki/AWK