WSN operability during persistent attack execution

Eliana Stavrou
Computing Department
UCLan Cyprus
Larnaca, Cyprus
estavrou@uclan.ac.uk

Andreas Pitsillides
Department of Computer Science
University of Cyprus
Nicosia, Cyprus
andreas.pitsillides@ucy.ac.cy

***Abstract*—Wireless Sensor Networks (WSNs) are utilized in a number of critical infrastructures, e.g. healthcare, disaster and relief. In sensitive environments, it is vital to maintain the operability of the network in an effort to support the decision-making process that depends on the sensors' observations. The network's operability can be maintained if observations can reach the specified destination and also if the sensors have adequate energy resources. The operability is negatively affected by security attacks, such as the selective forward and the denial of service (DoS), that can be executed against the WSN. The attacks' impact greatly depends on the attackers' capabilities such as their knowledge and the number of malicious nodes they hold. Currently, the research community focuses on addressing casual attackers that don't persist with their attack strategy. However, the proposed solutions cannot address persistent attackers that continue with their attack execution after the network has applied appropriate recovery countermeasures. Designing an adaptive recovery strategy is challenging as a number of issues need to be taken into consideration such as the network's density, the number of malicious nodes and the persistent attack strategy. This research work formulates a persistent attack strategy and investigates the integration of different recovery countermeasures in WSNs. The evaluation results demonstrate that an adaptive recovery strategy can enhance the network's recovery benefits, in terms of increased packet delivery and decreased energy consumption, and prolong its operability. Moreover, the observations made are envisioned to encourage new contributions in the area of adaptive intrusion recovery in WSNs.**

Keywords—WSN, resilience, recovery, persistent adversary, survivability, adaptability, intrusion recovery

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have become an essential component of the cyberspace, supporting a variety of applications in the context of smart spaces [1]. Sensors are utilized in many smart environments (i.e. healthcare, surveillance, industrial, transportation) where security is considered a critical requirement. Cyberspace, and the emerging Internet of Things (IoTs), create many opportunities for delivering new services to a word-wide scale but also provide the resources (knowledge, tools) to adversaries to deliver more advanced attack strategies. Adversaries can become more persistent with their malicious objectives, thus compromisation can occur even if security measures are already implemented by a WSN. Security efforts should focus on enhancing the resilience of sensors' operation during attack occurrences and thus promoting their operability.

Some of the main assets that need to be protected in WSNs are the sensed data and the energy source. Critical applications rely on the sensed data [2] to support their services and the decision-making. To be able to relay data to the control center, sensors have to be available to communicate. Communication [2] is greatly dependent on the energy sources and on the sensors' ability to access the wireless channel to transmit/receive data. There are a number of security attacks [3, 4] in WSNs, e.g. blackhole, selective forward, DoS, that can disrupt sensors' communication. Intrusion recovery measures should address compromisation and recovery of the network's operation. So far, the research focus was mainly on designing intrusion recovery solutions i.e. [4-8] to combat non-persistent adversaries. Non-persistent adversaries execute an attack but do not continue with the attack execution when the network implements recovery countermeasures. These solutions are not effective in addressing adversaries that implement a persistent attack strategy which includes the continuation of an attack and/or the execution of different attacks. Thus, it is not adequate to only act proactively to protect the operation of a WSN, but it is equally important to be prepared for the existence of an intelligent attacker that will adjust his/her attacks to work around recovery countermeasures.

The focus of this research work is to formulate a persistent attack strategy and then investigate the integration of different recovery measures in WSNs that can address such a strategy. The aim is to setup an adaptive recovery strategy that will promote the reliability and the survivability of the network during an adaptive attack execution. The idea is to enable the sensors to respond to the attacks that affect their communication capabilities and retain a level of operability that will allow the network to deliver information to the intended destination, i.e. a control center. However, designing an adaptive recovery strategy in WSNs is challenging as a number of issues [5] need to be considered such as the network's density and the number of malicious nodes that trigger recovery countermeasures. This research work investigates how the aforementioned issues affect the recovery benefits in an effort to provide observations that could lead to the design of new recovery solutions that can maximize recovery benefits under the assumption of a persistent attacker. Section II presents the typical intrusion recovery solutions that are proposed in WSNs, section III presents the attacker profile and section IV discusses the rationale of the proposed investigations. Section V provides the evaluation analysis in terms of packet delivery and energy consumption. Section VI constitutes conclusions.

II. RELATED WORK

Intrusion recovery solutions in WSNs mainly address a single type of a security attack. Typical attacks [3,4] that are executed in WSNs, aiming to disrupt the communication, are blackhole/selective forwarding, eavesdropping and denial of service (DoS) attacks. A blackhole/selective forwarding attack can be implemented by malicious nodes that participate in the network communication and are chosen to forward packets to the destination/control center. When a malicious node receives packets, it can drop them or selectively decide which packets to discard. The main objective of this type of attack is to affect propagation of data to the control center. Eavesdropping is an attack that aims to overhear communication in an effort to either identify sensors existence in the vicinity of the malicious node and/or steal packets. A DoS attack is implemented by continuously sending a number of packets through the wireless channel, affecting the communication and availability of the nodes. The blackhole/selective forward attack is addressed by blacklisting the malicious node and rerouting traffic [5,6,13] over a route path that does not contain the malicious node(s). Eavesdropping is difficult to address, especially if the malicious node is considered an internal part of the network and does not execute an active attack (e.g. DoS) that will indicate its presence. A DoS attack can be addressed by a low duty cycle [4] or a channel surfing strategy [7,8].

III. ATTACKER PROFILE

It is essential to identify and understand the characteristics [9] of potential attackers, in an effort to realize their objectives and capabilities and implement appropriate countermeasures to address the implemented attacks. There are two types of attackers: internal and external. Internal attackers are considered those that have either successfully inserted their own malicious nodes into the network or they have compromised legitimate nodes and turned them malicious. On the other hand, external attackers possess malicious nodes that are not considered part of the network. Internal attackers are more dangerous than external because they are perceived as trusted elements of the network and can participate in the routing paths. Due to this, designing recovery solutions to address internal attacker is more challenging than taking into consideration external attackers.

Furthermore, an attacker can be characterized as casual or persistent based on the attack strategy that is applied. A casual attack strategy is considered to be deployed by an attacker with relevant knowledge to execute a single attack in an effort to disrupt the network's communication. In this case the attacker has loose motivations to damage the network. However, a persistent attacker has strong motivations to affect the network's communication, for example, in order to prohibit sensors to report a critical event (e.g. fire). Therefore, a persistent attacker is not discouraged by the recovery measures and continues his/her attack strategy, in order to continue affecting the network's operation and maximizing the negative impact, posing a higher threat for the operability of the network. This type of attacker, has sufficient knowledge to execute a variety of attacks while the network applies recovery measures to address them.

In this research work, an internal and persistent attacker is assumed.

IV. RATIONALE OF ATTACK AND INTRUSION RECOVERY STRATEGY

In this section, the rationale of the attack and the intrusion recovery integration investigations is presented. So far, research works focused on proposing countermeasures to address a specific security attack. A persistent attack strategy has not been actively investigated in omni-directional WSNs. Therefore, the integration (and potential benefits) of different intrusion recovery solutions has not been evaluated.

The network's operability is mainly depended on the sensors' ability to communicate [2] with each other and propagate observations to a control center that will further process the data and take actions, if necessary. The sensors' communication ability [2] is depended on the sensors' available energy resources and on their ability to access the wireless channel to transmit/receive data. Typical security attacks that can affect the network's communication ability are the selective forwarding and the DoS attacks. As already mentioned in section II, blacklisting and rerouting is usually deployed to recover from the selective forwarding attack. A low duty cycle and channel surfing are potential solutions that can address a DoS attack.

In order to promote the objectives of this research work, an appropriate and realistic attack strategy is formulated, along with a relevant recovery strategy. The following objectives of a persistent adversary have been considered for the formation of the attack strategy:

- Act unnoticed, for as long as possible
- Save energy resources on malicious nodes
- Priority to affect nodes that participate in routing paths
- Progressively respond to a continuous self-healing network with a persistent/continuous attack, affecting as many nodes a possible; no consideration for saving energy resources on the malicious nodes

The attacker is assumed to gradually enable the malicious nodes to execute the attacks so he/she can delay suspicion. To be able to act undercover and prolong the possibility for detection, malicious nodes are first assumed to implement a selective forward attack. When a malicious node is participating on an active route path, it can drop data packets and prohibit their propagation. With this attack, malicious nodes could be considered by the rest of the network as malfunctioning and not perceived as malicious. If detection measures are implemented, the sensor network can converge to new routing paths to avoid the "malfunctioning" nodes. Since recovery measures will be implemented, the selective forwarding attack will turn ineffective. The attacker is not discouraged by the recovery measures and further actions are taken by the malicious nodes to continue affecting the network's communication. Since batteries [2] are the typical energy source in WSNs, the attacker would like to safeguard the malicious nodes' energy so he/she could have more opportunities to attack the sensors. Therefore, his/her attack

strategy could be configured appropriately to consume only the minimum necessary energy. An attack that can actively disrupt the network's communication is a DoS. Malicious nodes can transmit a large number of packets to cause packet collisions, retransmissions, energy consumption, etc. All these can greatly affect the network's reliability, availability and survivability. Since a DoS is a resource demanding attack, the attacker could use it only when there are nodes near the compromised nodes. So, the malicious nodes enter a promiscuous mode in an attempt to overhear communication, a fact that will indicate that there are sensor nodes in their vicinity. When they overhear communication, they initiate a DoS attack. If the attacker decides to maximize the attack's impact, he/she can configure the malicious nodes to enforce a more persistent behavior, that is for all the malicious nodes to execute a DoS attack. The sensor network continues with the recovery measures and implements a low duty cycle in an attempt to withstand the DoS attack and recover a level of operability that will allow sensors to propagate observations to the appropriate authorities and support decision-making. If the malicious nodes still continue to affect communication when the sensor nodes operate in the low duty cycle, the network applies a channel surfing countermeasure to update to a new channel frequency and hence exclude the malicious nodes from the communication. Since an intelligent attacker is assumed, in this case the malicious nodes enter a scanning phase to identify the new frequency channel. As far as we know, the aforementioned example adaptable intrusion and recovery strategies are the first to be proposed in the context of WSNs. Our objective is to raise awareness of this type of intelligent persistent attacks and hence formulate adaptive intrusion recovery strategies. The proposed intrusion recovery strategies should take into consideration the adversary's persistency, and aid the WSN to selfheal and continue applying recovery measures in an effort to withstand the attacks and eliminate or minimize the impact. Overall, the aim would be to maintain a level of operability that would allow the sensors to propagate their observations and support decision-making.

V. NETWORK'S OPERABILITY WITH INTRUSION RECOVERY ADAPTABILITY

The ns2 simulator has been utilized to facilitate investigations. An IEEE 802.15.4 network has been simulated consisting of sensor nodes that are equipped with an omni-directional antenna. Sender nodes generate constant bit rate (CBR) traffic with a rate of 2 packets per second and a packet size of 70 bytes, following reactive routing, under the assumption of a detected event. A dense (550x550m) and a sparse (750x750m) network topology have been specified, consisting of 100 nodes each. Moreover, 5% and 10% randomly selected malicious nodes are considered. Initial energy is 100 Joules. Power consumption is based on a CC2400 WSN transceiver and LOS radio conditions are considered. Each experiment is repeated 30 times and the presented results have been averaged over the set of the 30 simulation runs. More details can be found in [11].

This research work focuses on investigating the network's performance in terms of packet delivery and energy consumption [12]. The operability of the WSN under a persistent adversary can be achieved if the packer delivery can be recovered and the energy consumption due to the attacks can be kept low. Recovering the packet delivery can support taking decisions reliably. Decreasing the energy consumption due to the attacks means that the network's survivability can be enhanced.

Initially a normal network operation is simulated and serves as the initial reference point for the rest of the attack and recovery scenarios. The sparse topology demonstrates an 85.7% versus a 74.3% packet delivery that is presented by the dense topology. 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. Based on the persistent attack strategy that is considered in this research work, malicious nodes that have become part of a route path implement a selective forward attack. The selective forward attack affects the network's performance in all scenarios. 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. As figure 1 demonstrates, as malicious nodes in the network increase, the packet delivery decreases. A higher number of malicious nodes means that they have more chances to be selected to participate in routing and therefore affect more active route paths. The packet delivery is decreased by 26% and by 33.6% when considering 5% and 10% malicious nodes respectively in the sparse topology. In the dense case, the packet delivery is decreased by 11.3% and 19.6% respectively. Furthermore, the selective forward attack is more effective in the case of sparse topologies compared to the dense topologies. In a higher density network, a malicious node has fewer chances to be selected to route paths and therefore can affect less the network's ability to propagate observations to the destination. As it can be observed, the packet delivery is about 14% less in the sparse topology compared to the dense one, when considering 10% malicious nodes. Also the energy consumption (fig. 2) is decreased since there are less packets propagated in the network. The sparse topology demonstrates up to 12% less energy consumption than the dense topology.

As soon as the network detects the selective forward attack, sensor nodes blacklist the malicious nodes and update the routing paths to exclude them from the communication. As the networks address more active malicious nodes, they show a higher ability to increase their packet delivery (fig. 1). The sparse topology presents a higher increase percentage (fig. 3 and 4), up to 31.8%, compared to the dense topology that goes up to 10.3%. As previously mentioned, in the dense topology malicious nodes have fewer chances to route packets compared to the sparse topology. However, as the network applies recovery measures and updates routing paths, undetected malicious nodes in the dense topology increase their chance to route packets. Therefore, while the dense network excludes previously detected malicious nodes from the communication and tries to recover, the updated routing paths continue to be affected by the undetected malicious nodes that are now selected to forward observations to the destination.

When the network is able to recover from the selective forward attack, the malicious nodes are excluded from the

routing paths. This situation does not discourage the attacker since he/she can execute another attack in an effort to continue affecting the operability of the network. Since one of the attacker's objectives is to save energy resources, the malicious nodes eavesdrop first on the network's communication to identify if there are active nodes in their vicinity. If they detect communication, they execute a DoS attack by continuously sending route control packets. The packet delivery is affected more in the dense network where it is decreased by 33% compared to a 26% decrease that occurs in the sparse network when 10% malicious nodes are considered. This is due to the high node density that appears in the dense network, thus malicious nodes can overhear communication from more neighbor nodes and therefore affect more nodes by initiating the DoS attack. The attack is causing packet drops, retransmissions, triggers the route path maintenance procedure a number of times and therefore the energy consumption is increased in all cases. In an effort to maximize the attack's impact, the attacker is assumed to instruct all malicious nodes to execute the DoS attack. The sparse topology is affected more than the dense topology in terms of communication. The sparse topology decreases by 5% its packet delivery, compared to 1% that is observed in the dense topology. This occurs because more malicious nodes are executing the DoS in the sparse topology as previously they have been inactive since they weren't overhearing anything. Therefore, they didn't attack based on an overhearing case as in the case that occurred in the dense topology where more malicious nodes were eavesdropping traffic. The network implements a low duty cycle to address the DoS attack. The packet delivery capability of the network is affected as the malicious nodes increase and also based on their location (if they are located near active route paths). While the DoS attack is implemented by fewer malicious nodes, the packet delivery (fig. 3) decreases by 22% and by 16% in the case of dense and sparse topologies respectively, when considering 5% malicious nodes. The impact of the DoS attack is higher in the dense network as more nodes implement the low duty cycle as the neighborhood density is higher in the vicinity of the malicious nodes. Also, a number of the nodes that have applied the recovery measure in the dense network are located in the active route paths, therefore the route maintenance procedure is triggered to update the paths. This is difficult to achieve as a number of nodes are unavailable to participate in the update of the active paths, causing a higher number of packet loss and retransmissions. However, as the number of malicious nodes increases from 5% to 10%, the communication capability is greater affected in the sparse topology. The lower density neighborhood does not favor the low duty cycle recovery measure as it gets harder for the nodes to update the active paths compared to the dense network. The packet delivery (fig. 4) is decreased by 30% and by 27% in the sparse and dense topology respectively, when considering 10% malicious nodes. Although the low duty cycle measure affects the packet delivery, it safeguards the energy resources of sensor nodes and therefore it still enhances the operability of the network by promoting its survivability. The energy consumption is decreased by 56% and by 57% in the dense and sparse topology, when considering 10% malicious nodes.

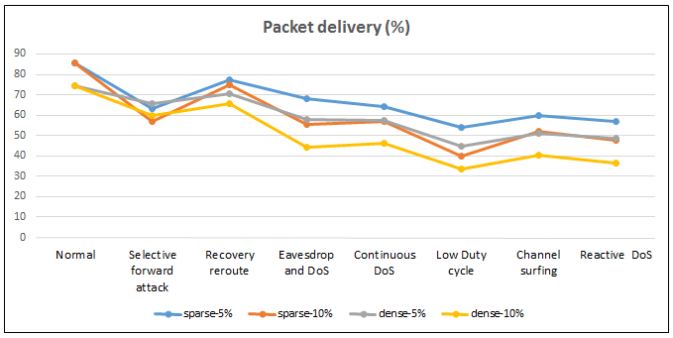

Fig. 1: Packet delivery versus attack evolution

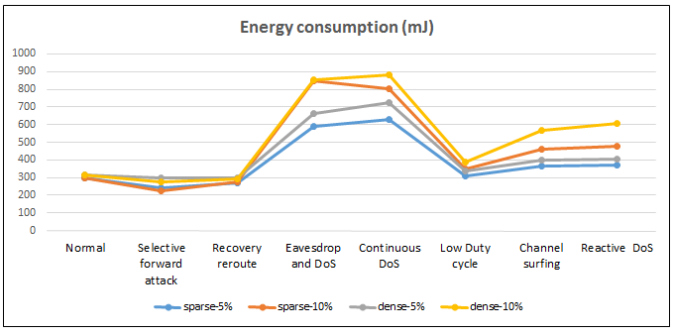

Fig. 2: Energy consumption versus attack evolution

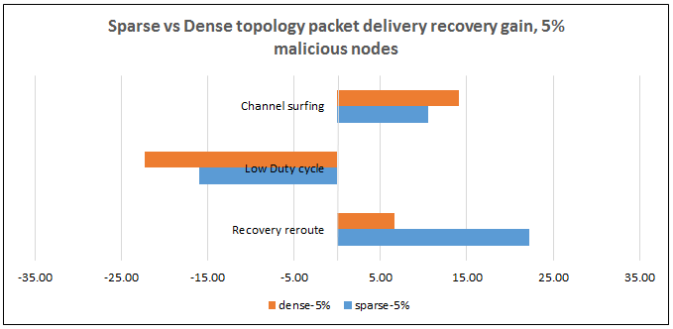

Fig. 3: Packet delivery % recovery gain with 5% malicious nodes

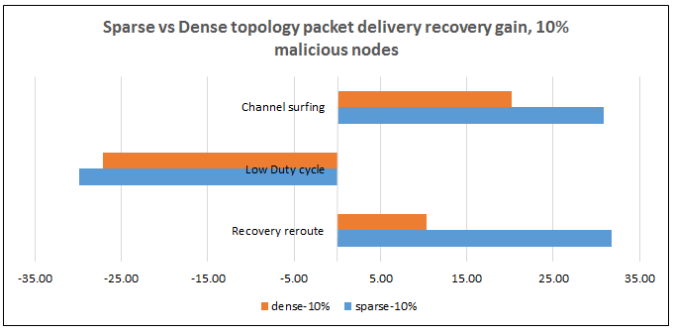

Fig. 4: Packet delivery % recovery gain with 10% malicious nodes

If the malicious nodes persist with the DoS attack, the network can implement another recovery measure, the channel surfing, in an effort to recover the network's reliability. The sensors switch to a different frequency and exclude the malicious nodes from the communication. The sparse network favors the adoption of the channel surfing as it can update the

frequency and converge to new routing paths easier than the dense topology in terms of less packet collisions, packet retransmissions and packet loss. This justifies the higher decrease of energy consumption, up to 15% less in the sparse topology compared to the dense case, when considering 10% malicious nodes. Furthermore, an increase of up to 31% packet delivery is observed in the sparse topology compared to an increase of 20.2% that occurs in the dense topology. The network may have been able to recover, but the malicious nodes are still in the network. As the malicious nodes 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 attack increases the network's energy consumption and affects the packet delivery once more. The sparse topology achieves an overall 48% packet delivery, when considering 10% malicious node. The dense topology presents an overall 36.5% packet delivery. The network can continue applying the low duty cycle and/or the channel surfing measure in order to establish communication over a different frequency channel and promote the network's operability.

VI. SUGGESTIVE STRATEGIES WITH INTRUSION RECOVERY ADAPTABILITY

A shown in section V, in order to address a persistent attack strategy, an adaptable intrusion recovery strategy is required. The evaluation results show that a blacklisting and rerouting measure, in order to address a selective forwarding attack, favors a sparse network in terms of increasing the packet delivery capability of the nodes and maintaining a higher overall delivery percentage compared to the dense network case. In the case of recovering from the DoS attack, a sparse topology can take benefit of a low duty cycle when there are fewer malicious nodes executing the attack. Otherwise, as malicious nodes increase and more nodes in the network are affected and apply a low duty cycle, the packet delivery in a sparse topology is affected more compared to the dense case. The channel surfing measure also favors a sparse network to recover its packet delivery capability, as the malicious nodes increase, and the low node density aids the network to update to the new frequency and converge easily to new routing paths. In terms of safeguarding the energy consumption, the low duty cycle presents the best defense against an active attack such as the DoS. However, this is at the expense of the packet delivery capability of the network. Blacklisting, rerouting and the channel surfing recovery measures increase the energy consumption but at the same time they promote the operability of the network in terms of delivering packets to the destination and supporting the decision-making process. Depending on the objectives and requirements set by the WSN application [1], the appropriate security recovery measures can be selected to address a persistent attack strategy.

VII. CONCLUSIONS

The utilization of an adaptive intrusion recovery strategy can aid the network to recover and prolong its operability against a persistent attacker. An adaptive recovery strategy promotes the network's self-heal capability under a variety of attack scenarios. In terms of operability, recovery efforts should concentrate in improving the packet delivery capability of the network and in decreasing the energy consumption that occurs due to an attack. Thus, a reliable decision-making and the network's survivability can be promoted. Designing an adaptive intrusion recovery strategy in WSNs is challenging as a number of issues need to be considered such as the network's density and the adversary's capabilities in terms of potential attacks foreseen to be executed and the number of malicious nodes that are under the control of the attacker. Moreover, the location of the malicious nodes need to be considered, for example, if they are located on an active route path or if they are neighbors to nodes participating in routing. As future work, the aforementioned aspects will be further investigated in an effort to maximize the recovery benefits that are demonstrated in this research work.

REFERENCES

[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] 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.

[3] 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.

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

[5] Lee, S. and Choi, Y. 2006. A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks, 4th ACM Workshop on Security of Ad hoc and Sensor Networks (SASN'06), pp. 59–70.

[6] Stavrou E, and Pitsillides, A. 2010. A Survey on Secure Multipath Routing Protocols in WSNs, Computer Networks Journal (COMNET), vol. 54, no. 13, September 2010, pp. 2215-2238.

[7] Halder, S., Mobashir, M., Saraogi, R.K. and DasBit, S. 2011. A Jamming Defending Data-Forwarding Scheme for Delay Sensitive Applications in WSN, Int. Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), pp. 1-5.

[8] Xu, W., Trappe, W., and Zhang, Y. 2007. Channel Surfing: Defending Wireless Sensor Networks from Interference, 6th Int. Conference on Information Processing in Sensor Networks (IPSN07), pp.499-508.

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

[10] Yinbiao, S. et al. 2014. Internet of Things: Wireless Sensor Networks, IEC WP IoT

[11] Stavrou, E. 2014. An intrusion recovery security framework in wireless sensor networks, PhD Dissertation, University of Cyprus.

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

[13] 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.