Situation Aware Intrusion Recovery Policy in WSNs

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) have been gaining tremendous research attention the last few years as they support a broad range of applications in the context of the Internet of Things. WSN-driven applications greatly depend on the sensors' observations to support decision-making and respond accordingly to reported critical events. In case of compromisation, it is vital to recover compromised WSN services and continue to operate as expected. To achieve an effective restoration of compromised WSN services, sensors should be equipped with the logic to take recovery decisions and self-heal. Self-healing is challenging as sensors should be aware of a variety of aspects in order to take effective decisions and maximize the recovery benefits. So far situation awareness has not been actively investigated in an intrusion recovery context. This research work formulates situation aware intrusion recovery policy design guidelines in order to drive the design of new intrusion recovery solutions that are operated by an adaptable policy. An adaptable intrusion recovery policy is presented taking into consideration the proposed design guidelines. The evaluation results demonstrate that the proposed policy can address advanced attack strategies and aid the sensors to recover the network's operation under different attack situations and intrusion recovery requirements.**

Keywords—WSN, resilience, persistent adversary, survivability, adaptability, intrusion recovery, situation aware intrusion recovery, intrusion recovery policy

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have evolved the last few years, supporting a broad range of critical infrastructures in the context of the Internet of Things (IoT) [1, 2]. WSNs find applicability in critical areas such as healthcare, smart grid, disaster relief and ambient living. The fact that critical operations depend on the sensors' observations to deliver reliable services, makes their protection a high priority. A variety of factors can threaten the operation of the sensor network, lead to the network's compromisation and affect the decision-making process. Such factors [3] include characteristics of the deployment environment, e.g. remote deployment location, characteristics of the sensor nodes, e.g. available resources and characteristics of the adversary, e.g. knowledge and motivation.

In the case where compromisation occurs, it is crucial for the WSN to be able to self-heal, restore compromised services and continue operating to support its objectives. Self-healing is challenging as it is a continue process that should promote two objectives; restore what is has been compromised and also prohibit malicious nodes from compromising again restored operations [4]. A variety of intrusion recovery solutions have been proposed in WSNs [5-12] assuming a casual adversary that will not persist with his/her attack strategy. These solutions are not adequate to address the new challenges that emerge as adversaries are getting more experienced and determined to succeed in their compromisation attempts. Intelligent adversaries have the appropriate knowledge to execute an advanced attack strategy to work around defenses. Therefore, the tasks of recovering and maintaining a level of operability during attack execution, in the context of persistent adversaries, become challenging.

Sensors should be equipped with the logic to respond in a prompt way to compromisation attempts in an effort to restore the operations that have been affected. In order to promote such a logic, sensors should be aware of the situation so they can respond accordingly. In the context of intrusion recovery, situation awareness [13] is required on different aspects that will drive sensors' recovery attempts. Sensors should be aware of the application's security priorities, of how an attack situation evolves, of the intrusion recovery actions that can be applied to address the attack strategy and of how the attack and recovery strategies can impact the sensors' operation. In order to promote a self-healing capability, an appropriate situation aware intrusion recover policy should be designed, taking into consideration all the aforementioned aspects that formulate the situation that the WSN needs to handle.

Situation awareness in the context of intrusion recovery has not been actively investigated by the research community. This research work formulates the situation awareness aspects that need to be considered in relation to intrusion recovery and contributes situation aware intrusion recovery policy design guidelines and an applicable policy. The key feature of the policy is that it enables the sensors to be aware of the attack situation as it evolves and allow them to make recovery decisions by been aware of the application's security requirements and of the applicable recovery solutions. Section II discusses related work. Section III specifies the aspects that should drive the situation awareness process. Section IV presents the proposed situation awareness intrusion recovery policy design guidelines. Section V demonstrates the applicability of the proposed policy design guidelines and section VI provides the relevant evaluation analysis. Section VII constitutes conclusions.

II. Related Work

A number of security attacks [10, 11] can be executed against a WSN in an effort to affect the sensor nodes communication capability. Such attacks include the blackhole, selective forward, sinkhole, wormhole, eavesdropping and denial of service (DoS) attacks. In order for the blackhole and selective forward attacks to be effective, the malicious node has to be part of the active route path. The key feature of the blackhole and selective forward attacks is that the malicious node decides whether it will forward a received packet or it will discard it, aiming to disrupt the information flow that is destined for the destination/control center. Attacks such as eavesdropping are less intrusive, as the primary task of a malicious node is to overhear communication in order to support the malicious intents, e.g. steal packets, identify sensors' presence. A DoS is a highly intrusive attack that can be implemented by a malicious node. A typical case of a DoS is having a malicious node continuously transmitting packets with a high rate in an effort to affect the network's availability, communication and operability.

Typical solutions that have been proposed as an effort to address the blackhole and selective forward attacks include blacklisting the malicious node and updating the active route paths to exclude the blacklisted nodes and successfully route packets to the intended destination, e.g. [5,6]. In the case where a non-intrusive attack is considered, such as eavesdropping, it is challenging to detect and address it. With regards to a DoS attack, the WSN can implement a low duty cycle [7] or a channel surfing strategy [8,9]. In the context of the intrusion recovery solutions that have been proposed so far in WSNs, e.g. [5-12], a single type of a security attack is mainly addressed. This means that the proposed solutions cannot effectively address an attacker that adapts his intrusion attack strategy after recovery measures have been applied. An adaptable attack strategy is a challenging feature to address and requires adaptability to be applied by the intrusion recovery strategy implemented by the WSN. Such a feature can be promoted by an appropriate security policy that will guide sensors to react based on different conditions. With regards to security policies in WSNs, designs have mostly focused on prevention aspects [14-17].

III. Situation Awareness in an Intrusion Recovery Context

In order to incorporate situation awareness into intrusion recovery solutions, knowledge is required on three main directions as depicted in Fig.1:

- *Attack situation*. This includes the type of the executed attack, its frequency and also a plausible attack strategy that is relevant to the WSN operation.
- *Intrusion recovery situation*. This includes what countermeasures are applicable under specific attack conditions. Also, the advantages and disadvantages of the available intrusion recovery countermeasures should be considered in an effort to select the appropriate solution that can maximize the recovery benefits.
- *Intrusion recovery priorities.* The intrusion recovery requirements that can be promoted by each solution should be considered and prioritized based on the application's needs. Different applications may require to promote specific intrusion recovery benefits and therefore the intrusion recovery strategy should be adapted accordingly.

The sensor network should be aware of the aforementioned directions in order to decide on the intrusion recovery actions that should be applied based on the current situation.

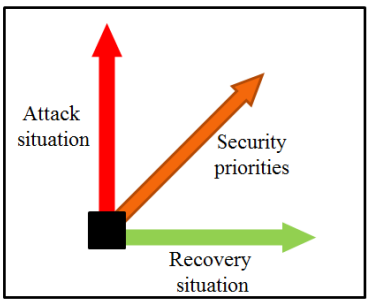

Fig. 1: Situation awareness directions

IV. Situation Aware Intrusion Recovery Policy Design

This section investigates the aspects that formulate a situation awareness intrusion recover process and proposes intrusion recovery policy design guidelines. The new design approach is driven by a number of activities that drive the intrusion recovery decision making. The decision making process can be used by the research community to formulate new recovery solutions in WSNs. Fig. 2 presents the proposed activities.

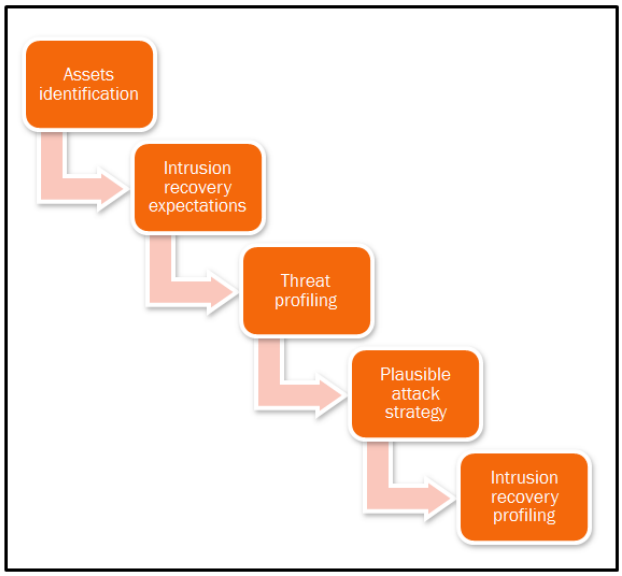

Fig. 2: Situation aware decision making activities

A. Assets Identification

In order to formulate an effective situation aware intrusion recovery policy, the assets that need to be recovered in case of compromisation should be clearly specified. The main assets that are of great value in a WSN are the *sensed data* and the *energy source*. WSN-driven applications rely on the sensed data to support their services and the decision-making process. For example, if observations regarding a critical event, e.g. fire, are reported by the sensor network to a control center, an appropriate decision is taken such as sending a response team to mitigate the fire. To be able to relay data to the control center, sensors have to be available to communicate. Communication is greatly dependent on the energy source and on the sensors' ability to access the wireless channel to transmit/receive data. Batteries are often utilized by sensors as their main energy source, therefore if battery depletion occurs, this will lead to the sensors' unavailability. Moreover, if the sensors are prohibited from accessing the wireless channel, e.g. due to on-going communication in their vicinity, this can stall the control center from been informed of a critical event that occurred. Therefore, the *communication capability* of the sensors should also be considered as an asset that needs to be recovered in case of compromisation. Without this capability, the sensor network will not be in position to propagate its observations and support decision-making.

By being aware of the main assets that need to be recovered in case of compromisation, appropriate intrusion recovery solutions can be formulated. Based on the assets that have been specified, sensors should be able to recover from attacks that target the battery's depletion in an effort to make them unavailable. Moreover, they should apply recover actions to recover from attacks that affect their packet delivery capability.

B. Intrusion Recovery Expectations

As soon as the main assets that are of value of the WSN-driven application are specified, the intrusion recovery expectations of the solution to be designed should be considered. The expectations should be identified in the context of the network's operation and then drive the specification of appropriate security requirements that should be achieved through the proposed solutions. It is important to realize that different applications may focus on recovering different security requirements, therefore, prioritizing them based on the applications' objectives is an element that should be part of the situation awareness process.

The principle expectation should be to recover the network's operation in case of compromisation. Taking into consideration that a WSN is often implemented in remote locations where human intervention cannot be easily and/or promptly applied, it would be beneficial if sensors could self-heal. A self-healing capability will allow sensors to respond promptly to compromisation and potentially minimize the attack surface, thus minimizing the negative consequences on the network's operation. In order to self-heal, sensors should be able to adapt their decisions based on the priorities set on the security requirements that should be achieved. In an intrusion recovery context, self-healingness can be supported by the following security requirements:

- Survivability. This 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. This can be achieved if the energy consumption that occurs due to the attacks can be minimized and/or eliminated.
- Reliability. Intrusion recovery should promote a reliable network operation, meaning that packet delivery capability should be successfully restored after a compromisation in order to allow data to be delivered to the destination.
- Resilience. Once intrusion recovery countermeasures are applied and the network's operation is restored, it is essential to be able to resist new attacks that aim to interrupt the recovered WSN's services.

C. Threat Profiling

In the quest of designing a situation aware intrusion recovery solution, it is necessary to specify the threat that the WSN would be expected to deal with. Profiling the threat should aim in understanding the adversary's intent, opportunities and capabilities.

An adversary can be characterized as *internal* if he is able to compromise sensors and turn them malicious or if he can insert his own malicious nodes that can be conceived as part of the network. If he is not able to participate in the network, he is perceived as an *external* threat. Internal attackers are by far more dangerous as they can be included in routing paths, thus they may affect the network's communication as they are supposed to forward packets to the next hop. Also they have direct access to neighboring nodes' observations. Furthermore, an attacker can be characterized as *casual* or *persistent* based on his compromisation objectives. A casual attacker is a person who has basic programming skills and knowledge to execute a single attack. His compromisation objectives are assumed to be superficial and mainly focus on testing his capabilities. Therefore, in this case the attacker does not have strong motivations to damage the network. In the case where the network recovers, a casual attacker is not expected to continue with new compromisation efforts. However, a persistent attacker is expected not to be discouraged by the intrusion recovery actions that are applied by sensors. His motivation is to prohibit sensors from propagating critical observations to a control center so that reliable decision-making cannot be made. A persistent adversary has excellent knowledge of how protocols and technologies work and he is capable of adapting his intrusion strategy while the network recovers. Such an attacker poses a great threat to the network. In the case where a persistent attacker gets access in the network, recovery becomes even more challenging.

D. Plausible Attack Strategy

Sensors should be aware of the attack situation and self-heal accordingly. This means that sensors should have knowledge about the attacks that can occur so they can decide on the appropriate countermeasure(s) that should be applied. The attacks that should be considered, need to be relevant to the assets that have been identified as important and need to be

recovered in case of compromisation. Based on the assets that have been specified at section A, potential attacks that can be part of an adversary's strategy include the selective forward, blackhole, sinkhole, wormhole, denial of service (DoS) and eavesdropping. Energy consumption can be greatly affected by a DoS attack and make sensors unavailable. Packet delivery is degraded with the selective forward, blackhole, sinkhole, wormhole and DoS as well. If a number of sensors cannot communicate due to energy depletion, this can affect the network communication. With eavesdropping, a malicious node can perform reconnaissance activities in an effort to identify if there are near-by sensors. A variety of attack strategies can be formulated, based on the selected combination of attacks. This needs to be taken into consideration when investigating potential recovery strategies in an effort to consider relevant and effective recovery countermeasures. Depending on whether the malicious nodes are considered an external or an internal threat as discussed at section C, specific attacks can be executed as depicted in Fig.3:

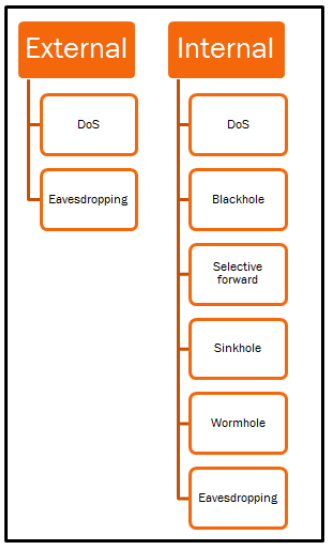

Fig. 3: Attacks categorization based on attacker's profile

E. Intrusion Recovery Profiling

Taking into consideration the attacks that may be included in the attacker's strategy, the relevant intrusion recovery countermeasures should be applied by the sensor nodes. Sensors can apply existing countermeasures, in addition to new intrusion recovery solutions that can be designed. Currently, the following intrusion recovery solutions have been identified:

- Blacklisting and rerouting. This is the typical and simplest recovery countermeasure. Sensor nodes blacklist detected malicious nodes and do not accept or forward any kind of communication from/to nodes listed in the blacklisting cache. They update affected route paths to exclude the participation of detected malicious nodes.
- Low duty cycle. Sensor nodes utilize a low duty cycle to go to sleep in an effort to address the DoS attack and protect their energy source from depletion. 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.
- Channel surfing. At the deployment phase or during runtime, sensors are configured to use a specific frequency to communicate. If an attack is detected, sensors switch to a new frequency in an effort to isolate the malicious nodes and turn the attacks ineffective.
- Multipath routing. Redundant paths are calculated in advance so they can be utilized when an attack is detected. Initially, a single path is utilized and once malicious activity is detected the routing turns into multipath in order to recover compromised WSN services.

Fig. 4 maps the intrusion recovery countermeasures, that can be considered by future intrusion recovery policy designs, to the relevant attacks that can be addressed.

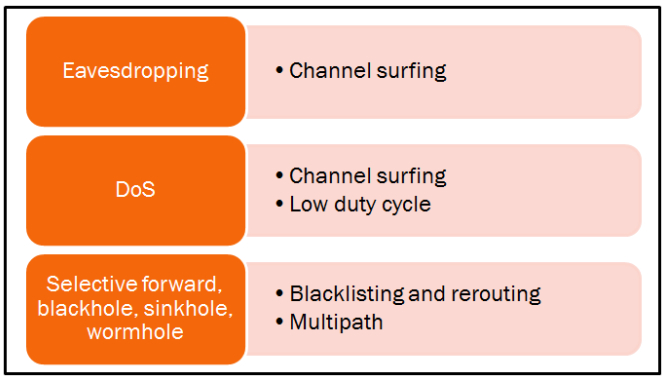

Fig. 4: Attacks and relevant intrusion recovery countermeasures

F. Situation Aware Intrusion Recovery Decision Making

Sensors should hold the decision making engine in order to select and apply recovery actions depending on the situation in terms of the attack execution, the persistency of the malicious nodes, the available recovery countermeasures and their benefits, and the application's security priorities. As the attack situation evolves, sensors should adapt accordingly taking into consideration the aforementioned information. Fig. 5 categorizes countermeasures based on the attack that can be addressed and based on the intrusion recovery requirements that can be promoted. This classification should drive the intrusion recovery decision-making process.

As it can be observed from Fig. 5, there may be more than one countermeasure mapped to a specific attack. Also, a specific countermeasure may address more than one intrusion recovery requirement. The decision on which countermeasure should be implemented should be based on conditions set by the designer of the solution in an effort to maximize the recovery benefits and minimize the attack window. This means that the designer should have a good understanding of how a countermeasure works and of its strong and weak operational features.

Fig. 6 presents the decision making flowchart that should drive the operation of the situation awareness intrusion

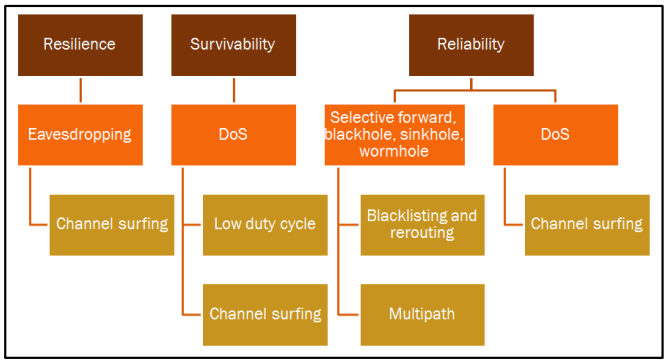

Fig. 5: Intrusion recovery requirements, attacks and countermeasures

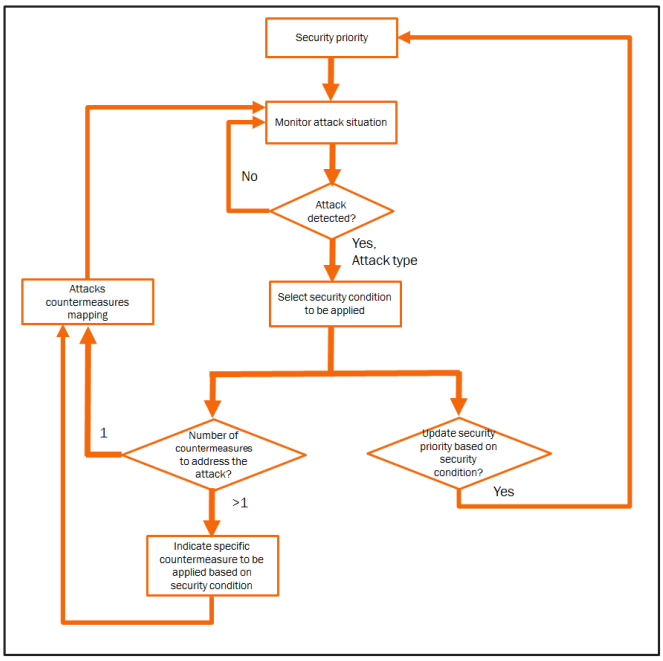

Fig. 6: Intrusion recovery decision making flowchart

recovery policy. The decision making process first considers the security priority set by the policy designer. The security priority is the driving factor of the recovery countermeasures to be applied. As discussed in section B, the intrusion recovery expectations should consider restoring the survivability, reliability and/or resilience of sensors in case of compromisation. Policy designers should initially select a security priority (survivability, reliability, resilience) to drive the decision making process. As soon as an attack is detected by the sensor network, its type is considered by the sensors so that the relevant countermeasure could be applied. As discussed in section E, each recovery countermeasure has specific operational features that the policy designer should be aware of in an effort to promote the selected security priority.

Depending on the application's objectives, the detected attack, the attacker's profile and the characteristics (strengths, weaknesses) of the relevant intrusion recovery countermeasures, the application's security priority may need to change as attacks evolve. In order to update the security priority, appropriate *security conditions* need to be specified considering the aforementioned elements. The rationale of the need to update the security priority comes from the realization that as an attack evolves, an application may need to focus on the recovery of different operability aspects (compared to the initial selected security priority) that have been compromised by the attack. For example, initially a WSN application may focus on recovering the reliability of the network. However, as attacks get more persistent, greatly affecting the network's operability, recovering the network's survivability may be more important, thus it should become the primary objective. This means that adaptability of recovery will be promoted to deal with different attack situations.

The fact that more than one options, in terms of intrusion recovery countermeasures, might exist in order to address a specific attack is both challenging but also beneficial for the network as it can support a diverse recovery approach. Selecting an appropriate intrusion recovery countermeasure to address an attack is challenging as sensors need to be equipped with the logic to select a solution. This logic can be established if sensors are aware of the following information: a) a mapping between attacks and countermeasures (as presented in Fig. 5) and b) what countermeasure to select in case there is more than one option. The security conditions that are mentioned earlier should guide the sensors as to the selection that should be made.

The proposed situation awareness intrusion recovery process, that is presented in section IV, can be easily extended to support more security requirements, security attacks and relevant countermeasures, if required by the WSN application. If such a case occurs, the proposed process will still be utilized in the same way, the difference is that more options will exist under the proposed situation aware intrusion recovery activities. The following section presents a case study to demonstrate how the proposed intrusion recovery design guidelines can be utilized.

V. Case Study Scenario

An appropriate situation aware intrusion recovery policy has been formulated, taking into consideration the proposed design guidelines. A critical WSN-driven application is considered, where a persistent adversary is able to compromise existing sensors and turn them malicious. Therefore, he has become an internal threat that aims to affect the network's packet delivery capability and to deplete the sensors' batteries. Initially, the network's security priority is set as to recover the reliability in case of compromisation. The following conditions have been specified:

If selective forward attack detected & persistent adversary assumed -> update security priority to survivability and set low duty cycle as the applicable recovery action against a DoS (condition 1)

If DoS attack detected & low duty cycle previously applied & attack frequency continuous -> update security priority to reliability and set channel surfing as the applicable recovery action against a DoS (condition 2)

If DoS attack detected & channel surfing previously applied & attack frequency continuous -> update security priority to

survivability and set low duty cycle as the applicable recovery action against a DoS (condition 3)

The rationale of the specified conditions is that a persistent adversary would like to postpone the attack detection, therefore he may try to initially implement attacks such as the selective forward. The malicious nodes that implement the attack may be perceived as malfunctioned nodes and therefore stall the attack's detection. In the case that such an attack is detected, the sensors blacklist the malicious nodes and update the active route paths to exclude them from the communication. This is the only solution for the relevant attack that has been considered by the case study recovery policy. Multipath is considered to require a more complicate approach, i.e. discover and maintain multiple routing paths, and is not considered to be part of the policy at the moment. Since a persistent adversary is assumed, it is anticipated that he will move forward to execute a more active attack, such as a DoS, in an effort to deplete the energy sources and continue compromising the network's operation. In such a case, the recovery priority is updated to survivability. It is also considered that the low duty cycle affects the packet delivery capability of the network. Therefore, if the adversary insists with his attack strategy, the network will focus again on recovering reliability and thus deploy a channel surfing countermeasure in an effort for observations to reach the intended destination. However, in the case where the adversary is able to identify the new frequency and continue with the attack, the priority should be to protect the network's energy sources. Taking into consideration the recovery benefits of the relevant countermeasures, the low duty cycle should be applied in an effort to prolong the network's lifetime. The following section demonstrates through ns2 simulations the effectiveness of the intrusion recovery policy by empowering sensors with a self-healing capability.

VI. Performance Evaluation

The evaluation is performed using the ns2 simulator. The simulation scenario considers an IEEE 802.15.4 network, 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 [4].

Based on the security priorities set in section V, the network's performance in terms of packet delivery and energy consumption will be investigated [18]. The rationale of the investigations is that the WSN operability can be recovered, assuming a persistent adversary, if the packer delivery can be restored and the energy consumption due to the attacks can be kept low. A reliable decision making can be made if the packet delivery is recovered. Moreover, the network's survivability can be maintained if the energy consumption is decreased.

A normal network operation is first simulated in order to serve as a reference point for the rest of the simulated scenarios. A percentage of 85.7% packet delivery is achieved by the sparse topology while the dense topology presents a 74.6%. The dense topology demonstrates a lower packet delivery capability due to a higher number of collisions and packet drops that occur due to the higher node density. Based on the case study scenario presented in section V, the malicious nodes execute a selective forward attack, affecting the operability of the network. The attack's outcome varies depending on a number of 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 Fig. 7 demonstrates, the packet delivery decreases as the number of malicious nodes in the network increases. As the number of malicious nodes increases, this 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 up to 33.6% and up to 19.6% in the sparse and dense topologies respectively when considering 10% malicious nodes. As it is observed, the selective forward attack is more effective in the case of the sparse topology. The packet delivery is about 14% less in the sparse topology compared to the dense one, when considering 10% malicious nodes. This occurs as the opportunities of a malicious node to be selected in routing paths decrease as the network's density increases. Therefore, a malicious node affects less the network's ability to propagate observations to the destination. Moreover, the energy consumption (Fig. 8) 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.

The sensor network monitors its operation in order to identify malicious activities. When the selective forward attack is detected, the appropriate countermeasure is deployed. According to the case study scenario, sensor nodes blacklist the malicious nodes and update the routing paths to exclude them from the communication in order to address the selective forward attack. As indicated in Fig. 7, the network demonstrates a higher ability to increase its packet delivery as more active malicious nodes are detected and excluded from the route paths. The sparse topology presents a higher increase percentage (Fig. 9 and 10), 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.

As soon as the sensors apply the recovery measures, the selective forward attack becomes ineffective as the malicious nodes are excluded from the communication. This does not mean that sensors should be at rest, as the malicious nodes can deploy further attacks in an effort to compromise the recovered network operation. The malicious nodes enter a promiscuous

mode and they execute a DoS attack, per overhearing case, by continuously sending route control packets. The DoS attack is more effective in the dense network that demonstrates a decrease of packet delivery up to 33% compared to up to 26% decrease that occurs in the sparse network when 10% malicious nodes are considered. This occurs as the dense network provides more opportunities to malicious nodes to overhear communication, thus more malicious nodes initiate the DoS attack compared to the sparse case, affecting more neighboring nodes. The attack greatly affects the network's performance as a high number of packet drops and retransmissions occurs, triggering the route path maintenance procedure a number of times. This leads to increased energy consumption.

The malicious nodes can maximize the attack's outcome by executing the DoS attack, regardless whether they can overhear communication or not. In such a case, the malicious activities are more effective in the sparse topology. In terms of packet delivery, the sparse network presents a 5% decrease, compared to 1% that is observed in the dense topology. The sparse topology is affected more compared to the dense case, because there are more malicious nodes executing the DoS as previously they have been inactive since they weren't overhearing anything. In order to address the DoS attack, the network deploys a low duty cycle. Since a number of sensors become unavailable due to the low duty cycle, the packet delivery capability of the network is decreased. In the dense network there are more nodes affected by the attack and therefore more nodes implement the low duty cycle compared to the sparse topology. The packet delivery (Fig. 9) decreases by 22% and by 16% in the case of dense and sparse topologies respectively, when considering 5% malicious nodes. Furthermore, the impact of the DoS attack is higher in the dense network due to the location of the malicious nodes that is near active route paths. Therefore, the attack forces the route maintenance procedure to be triggered more times in order to update the paths. However, establishing new active route paths is challenging 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. It is also observed that as the number of malicious nodes increases from 5% to 10%, the communication capability is greater affected in the sparse topology. The low duty cycle does not favor recovery in the sparse network, compared to the dense network, as there are fewer nodes to consider in the routing process. This makes it difficult to establish stable routing paths. As Fig.10 presents, the packet delivery is decreased by 30% and by 27% in the sparse and dense topology respectively, when considering 10% malicious nodes. The low duty cycle measure affects the packet delivery, however, 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.

Since a persistent adversary is considered, it is expected that the malicious nodes will be persistent with the DoS attack. In such a case, sensors can apply the channel surfing solution to restore the network's packet delivery capability. With the

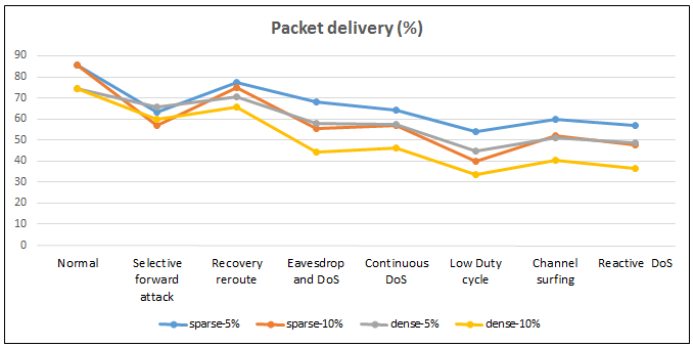

Fig. 7: Packet delivery

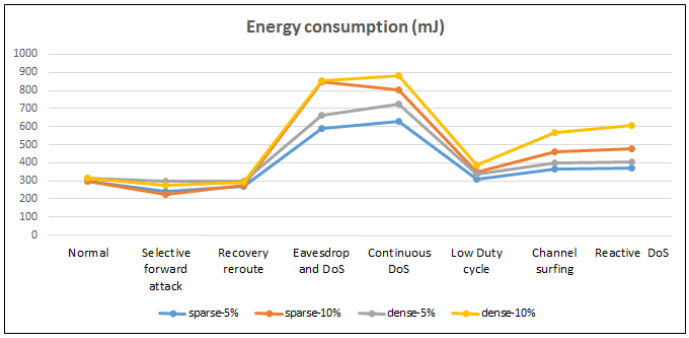

Fig. 8: Energy consumption

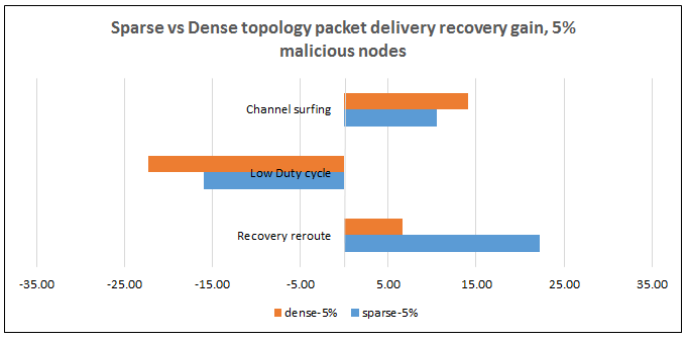

Fig. 9: Packet delivery % recovery gain with 5% malicious nodes

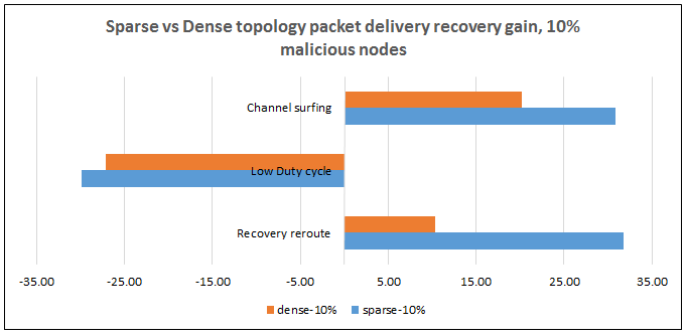

Fig. 10: Packet delivery % recovery gain with 10% malicious nodes

channel surfing, a different frequency can be utilized by the sensors in an effort to leave the malicious nodes operating at the default frequency and thus exclude them from the network communication. The applicability of the channel surfing is more effective in the case of the sparse topology. This occurs as sensors can update the frequency and establish stable routing

paths easier than the dense topology, presenting less packet collisions, packet retransmissions and packet loss. Thus, the sparse topology decreases energy consumption more, up to 15% less, compared to the dense network, when considering 10% malicious nodes. The sparse network favors an increased packet delivery capability, up to 31%, that is restored with the channel surfing measure. The dense topology presents an increase of the packet delivery up to 20.2%. Although sensors have applied measures to recover from compromisation, the threat still exists since the malicious nodes are present and can continue with their compromisation efforts. If the malicious nodes cannot eavesdrop any network communication, they scan available frequency channels in an effort to identify the presence of sensors and continue with the DoS attack. Once this occurs, the network performance is degraded once more. An overall 48% and 36.5% packet delivery is demonstrated by the sparse and dense topologies when considering 10% malicious nodes. As a response to the attack, the sensors 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.

As it is demonstrated, it is beneficial for the sensor network to deploy a situation aware intrusion recovery policy. The assessed policy was designed taking into consideration the proposed situation aware intrusion recovery guidelines. It is anticipated that a variety of policies can be formulated, taking into consideration the diversity in the WSN applications, the potential attacker profiles, the potential attacks and countermeasures. In order to achieve an effective evaluation, appropriate performance metrics need to be considered, driven by the security priorities set by the policy designers. The work at [18] can be utilized in order to select specific evaluation metrics that are proposed to assess security requirements in the context of intrusion recovery protocols.

VII. CONCLUSIONS

The utilization of a situation aware intrusion recovery policy can address a persistent adversary that adapts his attack strategy as the network applies recovery countermeasures. By taking into consideration information such as the attack type, the attack frequency, the intrusion recovery priorities and the countermeasures characteristics, the intrusion recovery decision-making can be accordingly adjusted in an effort to maximize the recover benefits and meet the application's intrusion recovery expectations. Designing intrusion recovery solutions is challenging, however, if sensors become intrusion recovery situation aware they will be able to respond to compromisation attempts and selfheal. The situation awareness intrusion recovery policy design guidelines constitute the first attempt to investigate situation awareness in the context of intrusion recovery in WSNs. As a future work, the policy guidelines will be further elaborated in order to drive the formulation of new intrusion recovery solutions. Moreover, a proof-of-concept implementation will be pursued.

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

[3] 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.

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

[5] 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.

[6] 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.

[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, International Conference on Security in Pervasive Computing (SPC), pp. 104-118.

[10] 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.

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

[12] 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.

[13] Barford, P. et al. 2009. Cyber SA: Situational Awareness for Cyber Defense, Advances in Information Security, Springer, 46, pp. 3-13.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.