Efficient detection of routing attacks in Wireless Sensor Networks

Theodore Zahariadis, Panagiotis Trakadas , Sotiris Maniatis, Panagiotis Karkazis, Helen C. Leligou, Stamatis Voliotis
Dept. of Electrical Engineering, Technological Educational Institute of Chalkis,
Psahna Evias, 34400, Greece, Tel: +302228099641
E-mail: {zahariad, ptrakadas, smaniatis, karpa, leligou, svoliotis}@teihal.gr

***Abstract*— A lot of effort has been spent in securing the routing procedure in Wireless Sensor Network (WSNs) since this is accomplished in a cooperative way and is vital for the communication of the sensors with the base station which collects the sensed data. The communication over wireless links in combination with the ad hoc organization introduces vulnerabilities. Each node monitors the behaviour of its neighbours in order to check whether they behave maliciously or not. Nodes with low trustworthiness are then avoided during routing decisions which are based on location and trust information. The efficiency of the proposed approach in defending against black-hole, grey-hole and integrity attacks is evaluated using computer simulations.**

Keywords-component Wireless sensor network, security, trust models

I. INTRODUCTION

Security plays an important role in the deployment and penetration of wireless sensor network which offer flexible and low cost solutions. The security requirements (see [1]- [2]), include node verification, user authorization, data confidentiality, data integrity and freshness, privacy, and secure localization. Unfortunately, security solutions designed for legacy networks are not applicable to wireless sensor networks, due to their specific characteristics. The wireless sensor systems operate in an unattended manner while they are characterized by limited resource both network and node. Namely, the energy, the computational power and the memory capacity is [1] very limited in sensor nodes, imposing strict limitation in the implementation of security mechanisms. The end result is that new solutions to defend against security attacks are needed.

A wide set of security attacks address the routing procedure. Representative examples include the black-hole and grey-hole attacks where a node exhibits selfish behaviour and refuses to forward all /part of the traffic received from its neighbours. The situation can be further aggravated if it additionally advertises routes passing through it, alluring traffic. To combat such behaviours, an approach borrowed from human societies has been proposed: nodes establish trust relationships between each other and base their routing decisions not only on geographical or pure routing information, but also on their expectation (trust) that their neighbours will sincerely cooperate. While key-based techniques can be used to provide data integrity, a trust model is mostly used for higher layer decisions such as routing [3], and key distribution [4].

Trust is the confidence of a node ni that a node nj will perform as expected i.e. on the node's nj cooperation. To evaluate the trustworthiness of its neighbours, a node monitors their behaviour (direct observations) but may also communicate with other nodes to exchange their opinions. The methods for obtaining trust information and defining each node's trustworthiness are referred to as trust models. All these schemes aim to improve security and thus increase the throughput, the lifetime and the resilience of a sensor network.

In the rest of the paper, we first detail our innovative trust model while its performance is evaluated in section 4 and conclusions are drawn in the final section 5.

II. THE TRUST MODEL

In this section, we propose a trust model suitable for the demanding and highly unreliable ad-hoc personal and wireless sensor networks (WSN). Our trust model is flexible and thus applicable to a variety of sensor network architectures while it protects against a wide set of attacks. The concept is to create on each sensor a trust repository (Trust Table), which will maintain and handle trust and reputation information about each neighbouring node. In the Trust Table values regarding a number of events is stored; based on these values, an overall cost function is calculated and drives the selection of the forwarding node.

The proposed trust model is a fully distributed trust scheme unlike the one presented in [5] where trust establishment is realized in a centralized manner. Each node is responsible for computing its own trust value per relation in the network, collecting events from direct relations. One of the most important aspects of trust management schemes is the process of data collection. Therefore, it is essential to point out, what type of can provide a useful feedback to the system, towards the proper decision. Trading-off security and implementation cost, we have selected a set of metrics that reveal the cooperation willingness of the nodes as regards routing. In more detail, the behaviour aspects to monitor are:

The work presented in this paper was partially supported by the EU-funded FP7 211998 AWISSENET project

- Packet forwarding: To protect against black-hole and grey-hole attacks a node should be evaluated regarding its willingness and sincerity in the routing procedure cooperation. This can be checked either through overhearing, or based on link layer acknowledgements.

- Network layer ACK. We also suggest that each node should check whether it receives the network layer ACK from the Base Station, in order to make sure that the next hop node is not colluding with another adversary in order to disrupt the network operation. For every transmitted packet, the source node waits for a network ACK to check whether its message has reached a higher layer node in the proposed architecture. If this checks completes successfully, the trust of the selected node increases.

- Authentication – Confidentiality – Integrity. A node can collect trust information about neighbouring nodes during interactions regarding the proper use of the security measures applied. For example, a node might use a mechanism to authenticate the message of a neighbouring node or the base station. The proper use of these security mechanisms can be proved quite useful input events for trust value computation.

- Remaining energy. To avoid the node with high trust value die out early, the node's energy can be regarded as a restrictive factor and decrease its trust value. The relevant value can travel piggybacked in periodically exchanged BEACON message. This way energy awareness becomes an inherent feature of the trust model and saves the node from complex calculations which have been proposed in the literature in order to deduce the remaining energy of the node.

Coming to the quantification of trust, for each trust metric except the remaining energy, node A calculates a trust value regarding node B based on the following equation:

$$T_i^{A,B} = \frac{S_i^{A,B}}{S_i^{A,B} + F_i^{A,B}} \qquad (1)$$

where Si and Fi stand for the number of successful and failed co-operations respectively. As regards the remaining energy, this is calculated as the percentage of the initial energy of the node. Finally the direct trust is calculated as weighted sum of the trust values calculated per trust metric.

To perform routing decisions, we define a weighted routing cost function which is incorporates the trust information as well as the location information through the following equation:

$$W(T) * T^{A,B} + W(D) * D^B \qquad (3)$$

Where D^B is the distance metric equal to one minus the relevant distance between the destination and node B compared to the sum of distance of all one hop neighbours. In other words, the node that is closest to the destination maximizes DB. The node that maximizes the above sum which represents the routing cost function is selected for forwarding. A similar approach however capable of defending only black-hole and grey-hole attacks has been presented in [6].

III. Simulation Results

To investigate whether our secure routing protocol efficiently detects the malicious nodes we have modeled our trust-aware routing protocol using the JSIM platform [7] and we have run scenarios for different attacks and for a varying number of attacking nodes.

In all the scenarios in this section, 100 nodes were placed on a grid with hop distance equal to 100. The routing rule used was the weighted routing cost function which weights the trust and distance info equally (i.e. W(D)=W(T)=0.5 for this section). Also, no mobility was assumed to better concentrate on the detection of attacks.

We first examine the efficiency in detecting the black-hole, grey-hole and integrity attacks.

A. *Detecting black-hole nodes*

To investigate how efficient our secure routing approach in detecting black-hole attacks, we have run different scenarios where all nodes were performing black-hole attacks but the number of malicious nodes varies from run to run. The malicious nodes are spread all over the sensor network grid and we have activated 9 connections. The weight factors we used were set as shown in Table 1.

TABLE I. Weight values used for the calculation of direct trust

Metrics	Weight value
Forwarding	0.3
Network acknowledgement	0.2
Integrity	0.2
Authentication	0.1
Confidentiality	0.1
Energy	0.1

The results in terms of packet loss are shown in Figure 1. It is evident that our approach detects the malicious nodes acting as black-holes and packet loss less than 30% is observed even when 40% of the nodes are acting maliciously. It is worth stressing here that the number of malicious nodes that a network can efficiently defend (i.e. connectivity is not lost) depends also on the network density, since in more dense network more forwarding alternatives exist. The observed packet loss for grey-hole attacks is always higher than for black-hole attacks, since grey hole attackers drop part of the received traffic and thus, it takes some time to detect and avoid them.

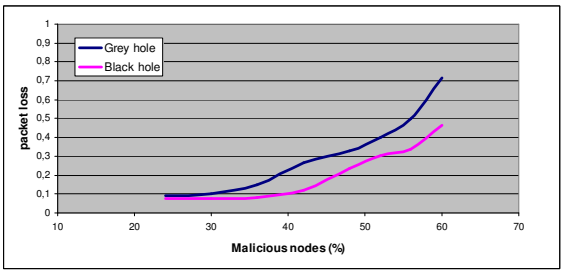

Figure 1. Packet loss for varying number of malicious nodes in the network

B. *Detecting grey-hole attacks*

Nodes that perform grey-hole attack refuse to forward part of the received traffic thus confusing their neighbours. The trust value of a grey-hole attacker drops less sharply than for a node performing black-hole attack, since some successful interaction happen among the total number of attempted interactions. For this reason, grey-hole attack detection is more difficult than the black-hole attack detection (as also shown in the previous section) which prompted us to thoroughly investigate the performance of our secure routing approach in the existence of grey-hole attackers.

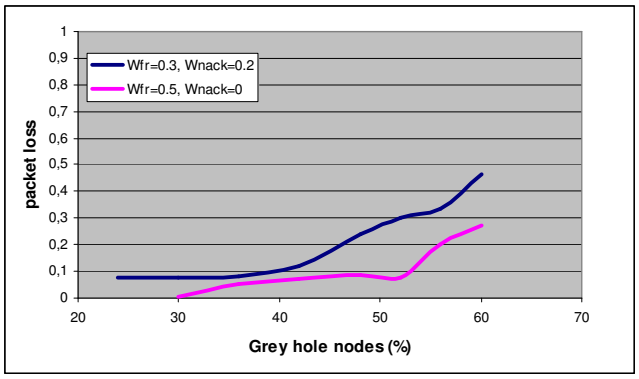

Figure 2. Packet loss as a function of grey hole nodes in the network for different weight factors

Another interesting investigation issue is the impact of the weight values on the performance in terms of packet loss. The detection of both black-hole and grey-hole attacks is based on the forwarding and network ack metrics. Based on the forwarding metric, the node gathers information about the sincerity in the routing protocol execution for all its one –hop neighbours while based on the network ack metric it obtains trust information regarding the whole path and the network situation rather than for its immediate neighbours.

To study the impact of the weight factors we have performed two scenario sets: one with W_{fr}=0.3 and W_{nack}=0.2 and another with W_{fr}=0.5 and W_{nack}=0. The rest weight values were as shown in the previous table. There is no need to change the other weight factors, since they are related to attacks not introduced in this scenario set. The results have been included in Figure 2. The first important result is that both curves follow the same tendency: packet loss increases as the number of malicious nodes increases and good performance (less than 10% loss) is observed for up to 40% of malicious nodes in the network. The second important conclusion is that in all cases, better performance, i.e. lower packet loss, is exhibited when the forwarding metric is assigned higher value. However, before reducing the weight of the network ack metric, we should bare in mind that the main purpose of this metric is not the detection of the grey-hole attack but the detection of colluding nodes attack. For example, if the first node in the path forwards the path to a colluding adversary, the forwarding trust metric will remain high and the source node will never get suspicions about its neighbour. Taking into account the network layer acknowledgement would reveal this kind of attack.

For the same scenario sets, the observed number of grey-hole attacks is shown in Figure 3. The number of attacks reveals the difficulty in detecting the malicious nodes since it reflects the failed attempts. Since the failed attempts consume node and network resources, we should try to fine tune the approach to minimize them.

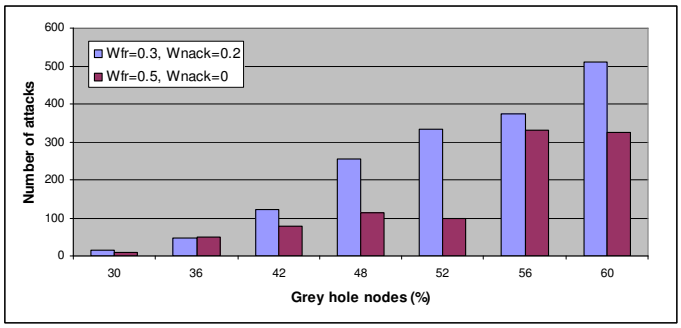

Figure 3. Attacks for different number of malicious (grey-hole) nodes and weight factors

Observing the figure it is clear that lower number of attacks is observed for the same weight factors and cases that packet loss is also improved. The performed attacks augment with the number of malicious nodes and higher number of attacks is observed when the weight factors are balanced between forwarding and network ack.

C. *Detecting integrity attacks*

To harm the normal and proper operation of a wireless sensor network, an adversary may alter either all the packet passing through it, or may differentiate its behaviour for control and data messages. Altering specific control messages may result in further damage ruining the connectivity. To defend against this type of attack, each node should overhear the wireless medium and compare the message it generated with the one that its one hop neighbour is forwarding. In case that the packet has been modified obviating the routing protocol rules, the source node should first avoid using this neighbour in the future for routing (which is achieved through the related trust metric) and second, attempt to re-send the packet towards the destination through another neighbour. As our focus is on the routing protocol, we are interested to check whether such nodes are avoided and how quickly the followed path is changed.

Exactly as happens for the previously discussed attacks, the malicious nodes are detected and avoided. However, this type of attacks does not result in packet loss but in modified packets reaching the base station. If we consider the modified packets as damaged packets, then the results would be no different than those obtained for the black-hole attack case.

A difference between the previous attacks and the integrity attack is that its detection is based on a single metric (the integrity metric) and not on two metrics as was the case for the

black-hole and grey-hole attacks. So, here we investigate the impact of the integrity metric weight factor on the number of observed attacks. This performance metric reveals how fast the trust aware routing protocol detects the malicious nodes and chooses alternative paths for the packet transfer. The results for the case where 48 malicious nodes issuing integrity attack exist in the network are included in Table 2.

TABLE II. OBSERVED ATTACKS FOR DIFFERENT WEIGHT FACTORS IN THE EXISTENCE OF 48 MALICIOUS NODES PERFORMING INTEGRITY ATTACKS

Weight factor	Number of attacks
0.1	746
0.3	61
0.5	39
0.7	42

As the integrity metric weight increases, the number of attacks decreases, since the direct trust value of the malicious nodes calculated by each source node decreases more sharply. It is worth stressing that no big difference is observed for 0.5 and 0.7 since each node in the path has to perform a number of interactions to obtain direct trust info. In other words, when the weight is 0.5 it is mainly the number of nodes involved in the paths that affect the number of attacks and not the weight factor. It is also worth stressing here that the distribution of the weight factor among the rest trust metrics does not influence the performance since they are associated with attacks which are not present in these simulation runs.

IV. CONCLUSION

A trust-aware location-based routing protocol has been presented. Its performance in detecting black-hole, grey-hole and integrity attacks has been investigated based on computer simulations and evaluated. It achieves less than 50% packet loss when more than 60% of malicious nodes exist in the network.

REFERENCES

[1] C. Giruka, M. Singhal, J. Royalty, S. Varanasi, “Security in wireless sensor networks”, Wireless Communications Mob. Comput. 2008; 8:1–24.

[2] Chris Karlof David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, Proc. of the IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127, May 2003

[3] H. Li, M. Singhal, “A Secure Routing Protocol for Wireless ad hoc Networks”, Proceedings of the 39th Hawaii International Conference on system Sciences, 2006.

[4] Nathan Lewis, Noria Foukia, “Using Trust for Key Distribution and Route Selection in Wireless Sensor Networks” IEEE Globecom 2007, 26-30 Nov. 2007

[5] Sapon Tanachaiwiwat, Pinalkumar Dave, Rohan Bhindwale, Ahmed Helmy “Location-centric Isolation of Misbehavior and Trust Routing in Energy-constrained Sensor Networks” IEEE International Conference on Performance, Computing, and Communications, 2004

[6] A.A. Pirzada and C. McDonald, “Trust Establishment In Pure Ad-hoc Networks”, Wireless Personal Communications Vol. 37, 2006, pp: 139–163

[7] http://www.j-sim.org/