A Distributed Energy-Aware Trust Management System for Secure Routing in Wireless Sensor Networks

Yannis Stelios, Nikos Papayanoulas, Panagiotis Trakadas,
Sotiris Maniatis, Helen C. Leligou, and Theodore Zahariadis

TEI of Chalkis, Dept. of Electrical Engineering, Psahna, Greece
Tel.: +30-2228099550
{jstellios,nicolappj,trakadasp,smaniatis,leligou,
zahariad}@teihal.gr

Abstract. Wireless sensor networks are inherently vulnerable to security attacks, due to their wireless operation. The situation is further aggravated because they operate in an infrastructure-less environment, which mandates the cooperation among nodes for all networking tasks, including routing, i.e. all nodes act as "routers", forwarding the packets generated by their neighbours in their way to the sink node. This implies that malicious nodes (denying their cooperation) can significantly affect the network operation. Trust management schemes provide a powerful tool for the detection of unexpected node behaviours (either faulty or malicious). Once misbehaving nodes are detected, their neighbours can use this information to avoid cooperating with them either for data forwarding, data aggregation or any other cooperative function. We propose a secure routing solution based on a novel distributed trust management system, which allows for fast detection of a wide set of attacks and also incorporates energy awareness.

Keywords: Wireless sensor networks, trust management, secure routing.

1 Introduction

Wireless Sensor Networks (WSN) offer efficient solutions in a great variety of application domains such as military fields, healthcare, homeland security, industry control, intelligent green aircrafts and smart roads. Although security is a key user requirement, which can be specified in a list of detailed security requirements, (see [1] - [3]), which include node verification, user authorization, data confidentiality, data integrity and freshness, privacy, secure localization and trusted resource allocation, its satisfaction proves to be a difficult task mainly due to the limited node and network resources. Well established security solutions designed for infrastructure based networks, cannot be applied in wireless sensor networks due to the limited memory space, processing power and energy (battery powered) as well as due to the absence of a trusted third party. The end result is that new solutions to defend against security attacks are needed [3].

In this infrastructure-less environment, nodes rely on the cooperation among each other for forwarding their packets to the sink node. A wide set of attacks addresses the

F. Granelli et al. (Eds.): MOBILIGHT 2009, LNICST 13, pp. 85–92, 2009.

routing procedure specifically. For example, in the blackhole attack, a node exhibits selfish behaviour and refuses to forward its neighbours traffic [3]. The situation can be further aggravated if it additionally advertises routes passing through it, alluring traffic. Another set of attacks is based on the modification of packets (either data or routing), which can disrupt the routing procedure driving nodes to route traffic incorrectly or falsifying the data that will finally reach the sink node. Other types of attacks include the Sybil attack, where a node pretends to possess certain characteristics which it does not really possess, and wormhole attack where more than one nodes collude in order to get the transmitted data or just to disrupt the routing procedure.

To combat such behaviours, an approach borrowed from human societies has been proposed (see [2]): 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. In other words, a trust management system is implemented. While key-based techniques can be used to provide data integrity, a trust model is mostly used for higher layer decisions such as routing [4], [5] and data aggregation [6], but also cluster head election [7] and, more surprisingly, for key distribution [8]. We propose a novel trust model which defends against routing attacks including black-hole, grey-hole, integrity-modification and confidentiality-authentication. Trust is then combined with energy awareness and location information to perform secure routing decisions.

In the rest of the paper, we first briefly report the related work found in the literature on trust models, while in section 3 we detail our innovative trust model and the secure routing protocol. In section 4, we evaluate the efficiency of our secure routing algorithm as a function of malicious nodes. Conclusions are drawn in the final section 5.

2 Trust Models for Sensor Networks - Related Work

Trust is the confidence of a node s_i that a node s_j will perform as expected i.e. on the node's s_j 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. The aim is to improve security and thus increase the throughput, the lifetime and the resilience of a sensor network even in the presence of adversaries.

Depending on the distribution of the trust establishment functionality in the network, the trust models can be distinguished in centralized and distributed. In the centralized case, (an example of which can be found in [10]), a head node, which is assumed to be trusted, undertakes the responsibility to decide the nodes' trustworthiness, based either on trust data it has collected on its own, or on trust data received by other nodes. The advantage of this approach is that the head node can be selected to be the most powerful node in order to be able to monitor the behaviour of all others, alleviating the need for monitoring from the rest network nodes. However, it represents a single point of failure. Alternative trust architecture can be formed organizing the network in clusters and assigning the monitoring functionality to the cluster heads ([6], [7], [11]). In this case, the trustworthiness of each node is taken into account for the selection of the cluster head. In the purely distributed case, (like the one presented in [12]), each node monitors the behaviour of its neighbours and based on the collected

measurements, it calculates their trustworthiness, which is then taken into account when routing decisions are made. In this case, the trust establishment functionality is uniformly distributed all over the network, and so does the implementation cost.

Different behaviour aspects can be monitored in a wireless sensor networks. Monitoring a certain behaviour aspect enables the detection of different security attacks. For example, each time node s_1 (see fig. 1) selects node s_3 for forwarding its packet, it enters the promiscuous mode in order to check whether node s_3 successfully forwarded it. After a number of cooperations, comparing the successfully forwarded packets to the number of packet s_1 sent to s_3, the source node (node s_1) can assess the sincere execution of the routing protocol while a systematic failure reveals a selfish and/or malicious node acting as a blackhole. Temporary failures due to channel errors will slightly affect the success over failure ratio when enough interactions have taken place. For each behaviour, based on the collected measurements either a trust value can be derived (in many cases a ratio of success over failure e.g. [10]), or distinct trust levels can be distinguished [13]).

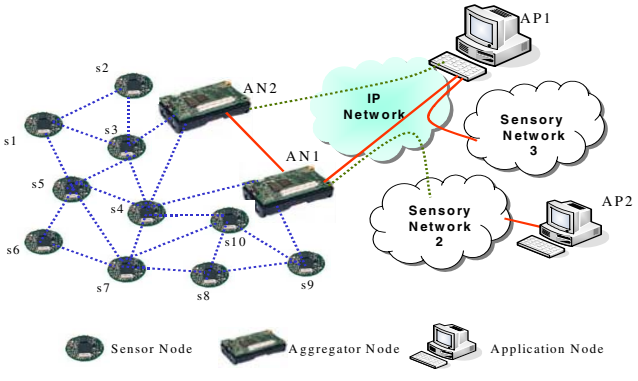

Fig. 1. Aggregator Nodes (ANs) collect data from the sensor nodes (si) and communicate with application nodes (AP) which provide the desired services

The detection of an unexpected behaviour based only on direct measurements with an adequate confidence requires the collection of an important number of evidences (samples). This procedure can be accelerated taking advantage of the neighbours' experiences. In other words, each node (say s_1 in Figure 1) may calculate its neighbour's (for example, node s_3) trust value either based on its own observations (direct evidence) [12] or combine it with information obtained from other nodes (for example nodes s_2, s_5). The information provided by s_2 and s_5 is called reputation or indirect evidence [13]. In this concept, every node can build a relation with its neighbours, based on the collection of actions (events) performed by other nodes in the neighbourhood. It is worth stressing that the trust information exchange can be exploited by adversaries to ruin the routing functionality of the network (as supported in [14]). Sharing information makes the system vulnerable to false reports (bad-mouthing attack), i.e. there are specific attacks targeting the reputation exchange protocol.

3 A Novel Energy-Aware Trust Model

In this section, we propose a novel distributed trust model suitable for the demanding and highly unreliable environments of wireless sensor networks (WSN). This trust model brings two important innovations: first, it defends against a wide set of attacks by monitoring multiple behaviour aspects (and not just a few as most trust models in the literature do) second, it incorporates energy-awareness which allows for better load balancing and higher resilience against the attacks. Moreover, a routing cost function incorporating trust, energy and location information is derived to guide routing decisions. The proposed trust model is a decentralized trust scheme, suitable for typical sensor network architecture (as the one shown in Figure 1).

3.1 Trust Metrics

One of the most important aspects of trust management schemes is the process of data collection. The direct trust value of a neighboring node can be determined by its multi-attribute, time-varying trust value depending on a set of events. We have selected a set of metrics that reveal the cooperation willingness of the nodes as regards routing. In more detail, each sensor monitors its neighbours as regards:

- Packet forwarding: To protect against black-hole and grey-hole attacks, every node should be evaluated regarding its willingness and sincerity in forwarding the received packets, cooperating in the routing procedure. This can be checked either through overhearing, or based on link layer acknowledgements, i.e. the source node checks whether its neighbour has forwarded the message.
- Network layer ACK: We also suggest that for each transmitted packet, the source node evaluates its next hop neighbour based on the reception (or not) of the relevant network layer ACK from the Base Station. The reception of the Net-ACK is evidence that the next hop node or any other node in the path is not colluding with another adversary in order to disrupt the network operation. In other words, the correct reception of the network layer ack ascertains that the message has reached a higher layer node in the proposed architecture, providing trust info for the whole path.
- Integrity: For the proper operation of the WSN, it is important that the nodes do not intentionally falsify both the data and the control messages. To avoid such malicious behaviours, each node overhears the wireless medium so that it receives the forwarded message. Then it processes it to check its integrity, i.e. that it is not altered violating the communication protocol rules.
- Authentication – Confidentiality. A node can collect trust information about neighbouring nodes during interactions regarding the proper use of the applied security measures. For example, a node might use a mechanism to authenticate the message of a neighbouring node or the base station. Furthermore, integrity measures and confidentiality measures (e.g. elliptic curve cryptography) can be applied for the communication between neighbouring nodes. Consequently, the proper use of these security mechanisms is considered as input for trust value computation.
- Remaining energy. To avoid the node with high trust value die out early, (which would possibly result in low connectivity), the node's remaining energy is considered as a trust value component. For the collection of this information, each node sends its

remaining energy value piggybacked in the periodically exchanged HELLO message and/or in every interaction (exchanged packet). This way energy awareness becomes an inherent feature of the trust model.

Although other application-aware trust metrics have been proposed in the literature, the implementation of such sophisticated functionality would exceed the sensor node capabilities. In this view, to enhance the flexibility of the model, since its implementation is based on embedded system software, we strongly propose the development of a security toolbox, which incorporates the trust model. The full set of metrics can be implemented in this software component and each time it is used in a specific sensor type, the configuration can change so that the trust model takes into account fewer metrics than the complete design. The level of security achieved depends on the number and type of behaviours monitored while it should also be stressed that the desired level of security strongly depends on the application.

3.2 Trust Quantification

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:

$$T_i^{A,B} = \frac{S_i^{A,B}}{S_i^{A,B} + F_i^{A,B}} \ , \tag{1}$$

where S_i and F_i stand for the number of successful and failed co-operations respectively. (Each node is responsible for computing its own trust value per neighbour in the network, collecting events from direct interactions. The S_i and F_i values for all neighbours and all the above described events are maintained in a trust repository.) As regards the remaining energy, this is calculated as

$$T_{RE} = V_{now}/V_{initial} \ , \tag{2}$$

where V_{now} and $V_{initial}$ stand for the remaining energy levels reported at the last and initial message received.

Furthermore, if the trust model is used to perform routing decisions, we propose to incorporate in the total node trust value, its distance to the base station, in order to form a unique routing cost function guiding the node selection and thus address trust and routing information together. In this case, the value of the "trust" metric related to the distance to the base station can be computed as follows:

$$T_d = 1-(d_i/\Sigma d_i) \ , \tag{3}$$

where d_i is the distance of neighbour i to the base station while Σdi stands for the sum of the distances of all its neighbours to the base station. To calculate the total direct trust value, all the trust values are summed up in a weighted manner (W_i represents the significance of i-th trust metric) based on the following equation:

$$DT^{A,B} = (\sum W_i * T_i^{A,B}) \ . \tag{4}$$

The node that is assigned the highest total trust value will be selected for forwarding. If no malicious nodes exist in the network, the node closest to the base station will be chosen.

4 Performance Evaluation

The performance of the proposed trust management system has been evaluated through computer simulations. The JSim platform [15] has been used to model our approach. The simulated network topology includes 25 sensor nodes (n_0 to n_{24}) placed on a 5x5 grid. The adopted transport protocol operates in a request-response manner and implements retransmissions at the application level with a timeout set to 0.5s. The initial trust value for all neighbors has been set equal to 1. The modeled trust metrics include forwarding, network ACK, remaining energy, and distance to the Base Station. In all the tested scenarios, 4 connections are active.

To evaluate the efficiency of our model, we ran three scenario sets. In the first scenario set, the node distance is kept fixed (equal to 100m) while weights of the trust metrics were equal to: W_d (weight of distance to the sink node) = 0.5, W_e (weight of the remaining energy) = 0.1, W_f (weight of the forwarding metric) = 0.2, W_a (weight of the ack metric) = 0.2. Nodes performing the black-hole/grey hole attack drop all/randomly the received traffic. The obtained results are shown in Fig. 2.

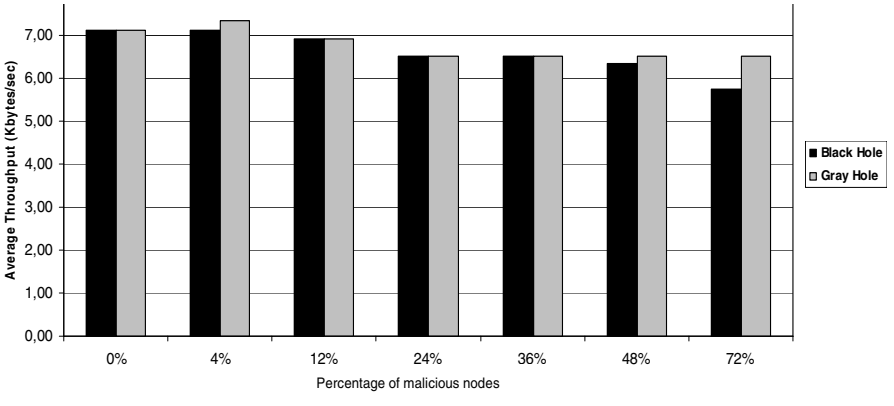

Fig. 2. Performance for different number of malicious nodes

The results show that the attackers are successfully detected and thus the throughput degradation compared to the case where no malicious node exists in the network is limited, even when malicious nodes represent the 72% of the network nodes. The detection of these attacks is based on the forwarding and net-ack trust metrics. Comparing black-hole to grey hole attacks, the impact of grey hole attack is less heavy and this is more evident when the malicious node reach high percentages.

We have run a second scenario set, where we modified the weights assigned to the trust metrics as follows: W_d = 0.2, W_e= 0.2, W_f = 0.5, W_a = 0.1. The results have shown that the impact of the modification of weights is almost negligible, since the

network is dense enough so that a trust-full neighbour is always found towards the destination. To further investigate the impact of the density of the network we have performed the third scenario set, where malicious nodes perform only black-hole attacks and the transmission range of each node is 260m. The average throughput for different distance values are shown in figure 3.

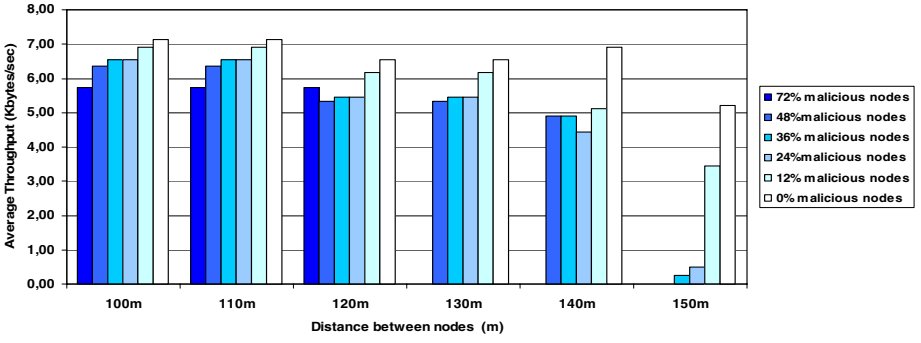

Fig. 3. Performance for different distance between neighbours

It is obvious that when the network is dense (i.e. low distance among nodes compared to the transmission range), this reflects to a high number of neighbours per node. As a result, a trusted neighbour can be found even when 72% of nodes are acting maliciously. The network operation becomes more vulnerable when the distance exceeds 150m. In this case less nodes exist in the neighbour list limiting the choices and thus the performance strongly depends on the number of attackers.

5 Conclusions

In the unmanaged environment of WSNs, the list of security attacks addressing the routing procedure is very long. Although cryptography and strong authentication schemes are powerful tools to safeguard packet integrity and node authenticity, they do not detect the (large set of) routing attacks such as selfish behaviours, blackholes, and bad mouthing. The establishment of trust relationships among nodes, exactly as happens in human societies, based on behaviour monitoring, is a usefull and effective tool. The choice of the behaviours to monitor is directly associated with the attacks that can be detected and against which protection is aimed. We proposed an efficient and scalable trust model incorporating energy awareness (which is a key issue for long network lifetime). Our model was shown to efficiently detect the malicious nodes and retain connectivity even when malicious nodes represent the 72% of the existing nodes. The performance of our scheme for different network densities has also been investigated and reported. Our future work includes the extension of our model to also incorporate indirect trust information.

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

References

1. Giruka, V.C., Singhal, M., Royalty, J., Varanasi, S.: Security in wireless sensor networks. Wireless Comm. Mob. Comput. 8, 1–24 (2008)
2. Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., Jamalipour, A.: A survey of routing attacks in mobile ad hoc networks. IEEE Wireless Comm., 85–91 (2007)
3. Karlof, C., Wagner, D.: Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. In: IEEE Int. Workshop on Sensor Network Protocols and Applications, pp. 113–127 (2003)
4. Li, H., Singhal, M.: A Secure Routing Protocol for Wireless ad hoc Networks. In: 39th Hawaii International Conf. on system Sciences (2006)
5. Rezgui, A., Eltoweissy, M.: TARP: A Trust-Aware Routing Protocol for Sensor-Actuator Networks. In: IEEE Int. Conf. on Mobile Adhoc and Sensor Systems (2007)
6. Hur, J., Lee, Y., Yoon, H., Choi, D., Jin, S.: Trust evaluation model for wireless sensor networks. In: Advanced Comm. Tech. Conference, ICACT 2005, pp. 491–496 (2005)
7. Crosby, G.V., Pissinou, N.: Cluster-based Reputation and Trust for Wireless Sensor Networks. In: Consumer Communications and Networking Conference, CCNC (2007)
8. Lewis, N., Foukia, N.: Using Trust for Key Distribution and Route Selection in Wireless Sensor Networks. In: IEEE Globecom 2007 (2007)
9. Mahoney, G., Myrvold, W., Shoja, G.C.: Generic Reliability Trust Model. In: 3rd Annual Conference on Privacy, Security and Trust (2005)
10. Tanachaiwiwat, S., Dave, P., Bhindwale, R., Helmy, A.: Location-centric Isolation of Misbehavior and Trust Routing in Energy-constrained Sensor Networks. In: IEEE Int. Conf. on Performance, Computing, and Communications (2004)
11. Ghazaleh, N., Kang, K.D., Liu, K.: Towards Resilient Geographic Routing in Wireless Sensor Networks. In: 1st ACM Workshop on QoS and Security for Wireless and Mobile Networks (2005)
12. Pirzada, A., McDonald, C.: Trust Establishment In Pure Ad-hoc Networks. Wireless Personal Comm. 37, 139–163 (2006)
13. Marias, G., Tsetsos, V., Sekkas, O., Georgiadis, P.: Performance evaluation of a self-evolving trust building framework. In: 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (2005)
14. Sun, Y.L., Han, Z., Ray Liu, K.J.: Defense of Trust Management Vulnerabilities in Distributed Networks. IEEE Communications Magazine 25, 112–119 (2008)
15. `http://www.j-sim.org/`
16. Karp, K., Kung, H.T.: GPSR: Greedy Perimeter Stateless Routing for WirelessNetworks. In: MobiCom 2000 (2000)