A Scalable Geographical Routing approach for Wireless Sensor Networks

Stamatis Voliotis, Theodore Zahariadis, Helen C. Leligou, Dimitrios Bargiotas, Panagiotis Trakadas, Panagiotis Karkazis
Electrical Engineering dept.
Technological Educational Institute of Chalkis
Psahna, Evias, Greece
{svoliotis, zahariad, leligou, bargiotas, trakadasp, karpa }@teihal.gr

Abstract— Efficient defense against security attacks is a challenging task in the wireless sensor network environment. Due to their infrastructure-less operation and the limited node and network resources, the applicability of legacy security solutions is disputable. The situation is further aggravated as the next generation wireless sensor network become larger and larger. To cope with the network dimensions we adopt the geographical routing principle which offers high scalability due to its localized operation. To efficiently defend against the routing attacks, a distributed trust model has been designed. Once trust information is available for all network nodes, the routing decisions can take it into account, i.e. routing can be based on both location and trust attributes. We propose a novel way of balancing trust and location information. Computer simulations show that the proposed routing rule (called ATSR) exhibits excellent performance in terms of delivery ratio, latency time and path optimality. ATSR adaptively weights location, trust and energy information, allowing the system designer to shift emphasis from security to path optimality, as shown by the simulation results.

Keywords-wireless sensor networks, routing, security, trust.

I. INTRODUCTION

As the range of wireless sensor network (WSN) application broadens and covers homeland, business area, urban and environmental monitoring solutions, the number of deployed sensors proliferates. In factories, sensor networks undertake a variety of tasks from production line monitoring to air, temperature and humidity monitoring and control, while state-of-the-art applications support the activity monitoring for energy consumption control purposes. In public urban environments, WSNs are mainly for security purposes while multiple WSNs may operate even inside a house/building to monitor conditions, to support health-care applications, security and HVAC system control.

WSNs offer flexible and low cost solutions, are easily installed and operated. However, the restricted node resources in terms of memory, processing capabilities and energy constrain the complexity of the functionality that can be implemented. On the other hand, they are inherently vulnerable to security attacks [1] due to their wireless operation in combination with the limited node resource that prohibits the implementation of mature security mechanisms designed for legacy wired and wireless system comprising of more powerful devices.

In all the aforementioned applications, wireless sensors are used to collect information and transmit it towards a node called base-station or sink, which is capable of data processing and can possibly further forward the data to specific application nodes. Routing in wireless sensor networks is performed in a cooperative way, i.e. each node relies on its neighbours to forward its packets towards the network sink. In other words, all sensor nodes participate in the routing procedure acting as routers. Unfortunately, malicious nodes may easily disrupt this procedure by simply refusing to forward the data packets of its neighbours issuing a so-called black-hole attack. The security attacks that address the routing procedure form a long list [2]. 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. A malicious node may also attack the packet integrity altering its content (integrity attack).

To combat such behaviours, an approach borrowed from human societies has been proposed [3]: nodes establish trust relationships between each other and base their routing decisions not only on pure routing information, but also on their expectation (trust) that their neighbours will sincerely cooperate. Trust is the confidence of a node A that a node B will perform as expected i.e. on the node's B 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. Thus, efficiency is expressed in terms of successful packet delivery ratios, as well as low (routing) overhead since this affects the consumed bandwidth, power, processing and memory resources which in turn defines the network's lifetime.

In the rest of the paper, we first detail our scalable trust model while its performance is evaluated in section 3 and conclusions are drawn in the final section 4.

II. THE ATSR PROTOCOL

To design a routing protocol that detects and avoids malicious nodes so that trusted nodes are preferred for routing purposes, we designed first a fully distributed trust model and we then defined the routing rules adopting the geographical approach which offers significant scalability advantages. The concept is to use geography for routing instead of measuring hops to avoid flooding the current state of all network nodes to create a map. This approach is less vulnerable to routing attacks and allows for efficient support of large sensor networks. Geographical routing is inherently immune against a set of attacks related to routing message propagation, node ID and attributes, which is of high importance for secure routing. Although these features are common for all geographical routing protocols such as the Greedy Perimeter Stateless Routing (GPSR) [4], the proposed Ambient Trust Sensor Routing (ATSR) bases the next hop neighbor selection not only on location coordinates but also on energy and trust based on a routing cost function. Energy awareness is necessary to avoid the node with high trust value die out early. The node's energy can be regarded as a restrictive factor and decreases its routing trust value i.e. the possibility to accomplish the task. For this reason, we have incorporated the energy awareness in the trust value a node calculates for its neighbors. In ATSR, the BEACON message, used in any geographical routing algorithm to allow each node announce its position, is extended to include the "remaining energy" field of the source node. All nodes become aware of the coordinates, but also the remaining energy of their neighbors directly from the modified BEACON message avoiding complex calculations which have been proposed in the literature in order to deduce the remaining energy of each neighbor. At the same time, energy awareness enables load balancing which is important both for the elongation of the network lifetime and the defense against traffic analysis attacks. The remaining energy of each node is expressed as the percentage of the initially available energy.

For the detection of routing attacks, we have designed a fully distributed trust model i.e. the trust management functionality executed in each node in the network is identical. The concept is to create on each sensor a trust repository (Trust Table), which will maintain and handle trust information about each neighboring node. In the Trust Table values regarding a number of events are stored; based on these values, a total trust value is calculated which is then incorporated in the routing function in order to drive the selection of the forwarding node.

One of the most important aspects of the 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 [5]. 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 neighboring 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 neighboring node or the base station. Furthermore, integrity measures and confidentiality measures (e.g. elliptic curve cryptography) can be applied for the communication between neighboring nodes. Consequently, the proper use of these security mechanisms is considered as input for trust value computation.

Monitoring these behavior aspects allows the detection of selfish behavior, selective forwarding and modification attacks, which combined with the attacks inherently addressed by the geographical nature of our routing protocol render the proposed routing protocol immune to a significant set of the routing attacks. The left over attacks include traffic analysis and flooding attacks. To defend against flooding attacks, each sensor should be equipped with a rate shaper, which is a rather costly solution. Instead, if routing packets do not propagate through the network, the impact of this attack will be limited. Additionally, the detection of this attack can be charged to more powerful nodes that can monitor the packet generation rate in their neighborhood. As regards traffic analysis, our protocol tends to distribute the forwarding load, since routing decisions are also based on energy levels. The balancing depends on the

weights assigned to the three routing criteria energy, trust and location information, which make the routing decision more or less sensitive to each of these factors. Another alternative is to assign the detection of more sophisticated attacks to nodes running intrusion detection applications.

As regards the quantification of trust, for each monitored behavior listed above (except confidentiality), node A calculates a trust value $T_i^{A,B}$ regarding node B by dividing the number of successfully completed interactions to the total number of attempted interactions. As regards confidentiality, the relevant trust value is equal to 1 for nodes supporting encryption and 0 for the others. The trust values calculated for the monitored behaviours as well as the remaining energy are combined in a weighted sum to produce the total trust value:

$$DT^{A,B} = (\sum W_i * T_i^{A,B}) \qquad (1)$$

Where W_i stands for the weight of each trust metric including the remaining energy.

In ATSR, the next hop node is selected based on location, trust and energy criteria while the emphasis can flexibly move among them as will be detailed in the simulation results section after the trust model description. To perform routing decisions, we define a weighted routing cost function which incorporates the trust information as well as the location information through the following equation:

$$W_t * DT^{A,B} + W_{di} * D^B \qquad (2)$$

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, and W_t, W_{di} the weight factors of trust and distance components respectively. In other words, the node that is closest to the destination maximizes D^B. The node that maximizes the above sum which represents the routing cost function is selected for forwarding.

It is worth stressing that to avoid hole, the GPSR's strategy for perimeter mode routing is employed.

III. PERFORMANCE RESULTS

To evaluate the efficiency of our approach, we have used the JSIM open simulation platform [7] to model it. The nodes adopt the IEEE 802.15 protocol. We have run simulations for two different network topologies: a network consisting of 100 and another with a network of 1024 nodes.

The first point of investigation is the impact of *Wd*, *Wt*, parameters on the performance. For this investigation we have considered a network of 100 nodes and we have run two scenario sets: one including 20 malicious nodes in the network issuing grey-hole attacks and another with 50 malicious nodes. The results in terms of performed attacks are presented in fig. 1 for different values of W_{di} values. (It is reminded that $W_t+W_{di}=1$).

For the obtained results we can see that for low values of W_{di} lower number of attacks is observed which directly reflects low packet loss values. As also expected, higher number of attacks is experienced in the case of 50 malicious nodes in the network. The results in terms of average packet latency (not included here due to space restrictions) reveal that values lower that 0.3 result in higher latency values. This happens because in this case each node selects highly trusted neighbors for forwarding which are not necessarily placed on the direction towards the destination.

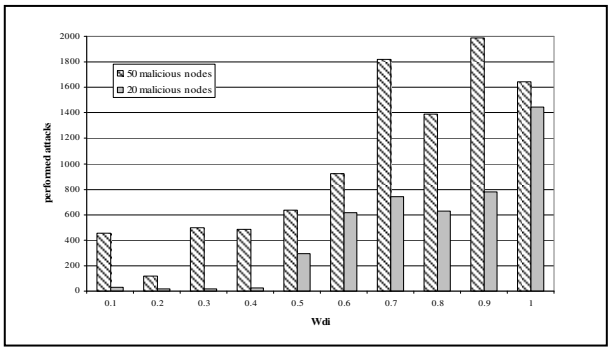

Figure 1. Number of measured attacks as a function of W_{di} for 20 and 50 malicious nodes in the network

The overall conclusion of this investigation is that W_{di} values close to 0.4 or 0.5 result in acceptable performance both in terms of packet loss, latency and number of experienced attacks.

In the second scenario set, a sensor network comprising of 1024 nodes was considered with the nodes organised on a regular grid (32 x 32). Ten data sessions are setup transferring data from ten different nodes towards one destination node that operates like a sink node (or a base station). The overall operation resembles that of a real sensor network. All data sessions transfer packets of 31 bytes each to the destination, with a frequency of one packet every two seconds.

In this scenario set, we varied the number of malicious nodes (0, 100, 200, 300, 400, and 500 nodes), in order to investigate how the protocol can react to an increasing number of malicious nodes existing in the network. The malicious nodes are randomly distributed over the grid. (For results regarding the efficiency detection of black-hole and grey-hole attacks, the reader is referred to [6]). The malicious nodes issue grey-hole, integrity, authentication, and confidentiality attacks.

The routing algorithms employed are the original GPSR, as well as ATSR with weight for trust (W_T) equal to 0.6 and weight for distance (*Wdi*) equal to 0.4. The weight values used for the calculation of direct trust, in the ATSR case, are 0.2, 0.1, 0.2, 0.2, 0.2, 0.1 for forwarding, network acknowledgment, integrity, authentication, confidentiality and remaining energy metrics respectively.

The metrics used for the evaluation include the packet loss, the experienced average packet latency as well as the number of performed attacks. The latter reflects the energy the nodes consume in vanish without succeeding in forwarding the packets, since for each

attack the relevant packet is not successfully reaching the destination.

Packet loss for both algorithms is graphically depicted in Figure 2, where the performance of our protocol is compared to that of the original GPSR algorithm which does not take any measure to avoid malicious nodes. The results show that ATSR outperforms GPSR in all cases, and operates rather satisfactorily even in case of 500 malicious nodes, although there are four different attacks and the weight for each metric does not have a large value, as restricted by the rule that all weights must sum up to 1. The non zero packet loss observed for ATSR in the case of no malicious nodes in the network (0.43% perceived packet loss), is attributed to collisions that occur near the destination node. Another interesting observation is that GPSR achieves a higher packet loss when 400 malicious nodes exist in the network compared to the case when 500 malicious nodes exist. However, this can be easily explained by the fact that gray-hole attacks, resulting in packet loss, are randomly placed in the grid. We shall shortly see that the total number of attacks when 500 malicious nodes exist in the network is the biggest value compared to other cases.

Mean packet latency is graphically depicted in Fig. 3. ATSR results in higher mean packet latency in all cases, especially when the number of malicious nodes increases, since it finds alternative albeit "longer" paths to the destination. It is worth stressing that in the GPSR case, it is the latency of the packets that reached the destination that was taken into account in the calculations while a significant part of the transmitted traffic does not manage to find its way to the sink.

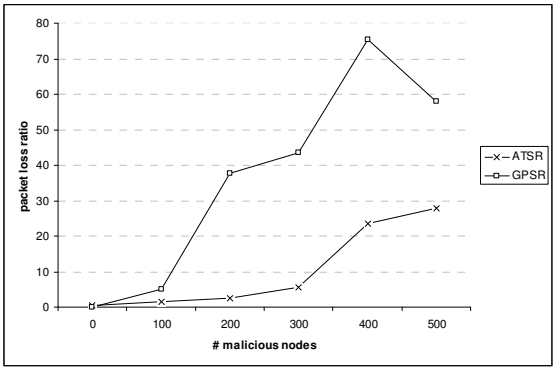

Figure 2. Packet loss ratio for GPSR and ATSR

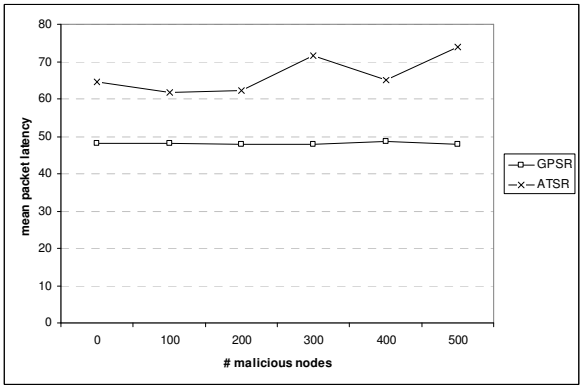

Figure 3. Mean packet latency in msec for GPSR and ATSR

The total number of attacks for GPSR and ATSR is graphically depicted in Fig. 4. It is evident that ATSR outperforms GPSR, and responds gradually and rather satisfactorily to the increasing number of malicious nodes existing in the network. The successful operation of the protocol is partly due to the fact that distance plays a less significant role in large networks, especially for nodes placed far from destination, since distance differences are very small, so trust is the main factor for routing.

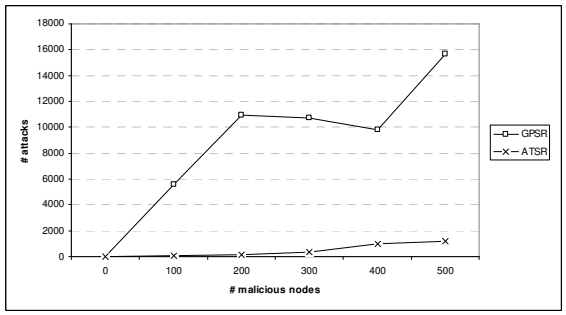

Figure 4. Total number of attacks for GPSR and ATSR

IV. CONCLUSIONS

The expansion of WSN applications mandates the design of scalable protocols while security is considered a key requirement. We have presented a scalable and flexible routing protocol which adopts the geographical approach to efficiently support large network populations and incorporates a scalable fully distributed trust model. The simulation results show that malicious nodes are detected even when the network consists of 1000 nodes and routing is accomplished through alternative paths.

ACKNOWLEDGMENT

The work presented in this paper was partially funded by the ARTEMIS JU under the ARTEMIS-2008-100032 SMART (Secure, Mobile Visual Sensor Networks Architecture) project.

REFERENCES

[1] Ian F. Akyildiz, Tommaso Melodia, Kaushik R. Chowdhury, "A survey on wireless multimedia sensor networks", The International Journal of Computer and Telecommunications Networking, Vol. 51 , Iss. 4, March 2007, pp. 921-960.

[2] V. C. Giruka, M. Singhal, J. Royalty, S. Varanasi, "Security in wireless sensor networks", Wirel. Commun. Mob. Comput. 2008; 8:1–24..

[3] Asad Amir Pirzada, Chris McDonald, and Amitava Datta "Performance Comparison of Trust-Based Reactive Routing Protocols", IEEE Transactions on Mobile Computing, Vol. 5, No. 6, June 2006

[4] Karp, K., Kung, H. T.: GPSR: Greedy Perimeter Stateless Routing for WirelessNetworks. In MobiCom 2000, (2000)

[5] Th. Zahariadis, P. Trakadas, H. Leligou, et.al., "Securing wireless sensor networks towards a trusted Internet of Things", IoS Press, ISBN 978-1-60750-007-0, pp.47 – 56

[6] Theodore Zahariadis, Panagiotis Trakadas , Sotiris Maniatis, Panagiotis Karkazis, Helen C. Leligou, Stamatis Voliotis, "Efficient detection of routing attacks in Wireless Sensor Network", 16th International Workshop on Systems, Signals and Image Processing, June 18-20, 2009, Chalkida, Greece.

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