The Impact of Indirect Trust Information Exchange on Network Performance and Energy Consumption in Wireless Sensor Networks


Technological Educational Institute of Chalkis, Electrical Engineering dept., Psahan Evias, 34400, Greece
{leligou, karpa, zahariad, tveli, svoliotis}@teihal.gr

Abstract – As the applications of Wireless Sensor Networks proliferate, security issues raised in this uncontrolled, self-organised systems comprising a large number of nodes with very low processing, buffering and communication capabilities become mandatory as they need to cooperate with each other, even for routing data messages to the desired destination. A solution that has been widely pursued to detect and avoid nodes that perform denial of service (refuse their forwarding services) is trust management, i.e. each node monitors the forwarding behavior of its neighbours in order to detect any node that behaves selfishly and does not forward the packets it receives. To accelerate trust knowledge gathering, nodes exchange their opinions about their common neighbours. This exchange is beneficial mainly in the case of node mobility. The more often this information is exchanged, the faster the trust information is built. However, as the transmission of this information consumes energy (which is a scarce resource in these settings), there is an interplay between the trust building speed and the energy consumption. This interplay is at the focus of the current paper, which investigates the performance of WSNs using computer simulations.

Keywords – Wireless Sensor Networks; Security; Routing; Trust Management; Energy Consumption

I. INTRODUCTION

Wireless Sensor Networks (WSN) support a wide set of solutions in a great variety of application domains such as military fields, urban surveillance, healthcare, homeland security, industry control, intelligent green aircrafts, smart roads and others. As the number of installed devices proliferates, and mobile mix up with static nodes to form more complex sensing systems, their secure integration with other communication systems and applications is currently pursued. Although numerous research articles propose countermeasures to the identified security threats, very limited work towards their implementation has been reported. A challenge faced during the realization of security measures is the limited memory, processing, power and communication bandwidth resources.

An important intricacy of WSNs is that nodes rely on the cooperation among each other to accomplish several tasks including routing. As the nodes are not necessarily within the range of the sink node which collects the sensed data, and they operate in an infrastructure-less manner, each source node forwards data messages to its neighbour for further forwarding towards the sink. This cooperation renders this procedure vulnerable to a wide set of attacks which address the routing procedure [1]. For example, in the blackhole attack, a node exhibits selfish behaviour and refuses to forward its neighbours’ traffic. 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. In other words, a trust management system is implemented. To evaluate the trustworthiness of its neighbours, a node monitors their behaviour (direct observations). The detection of an unexpected behaviour based only on direct measurements and in a reliable way takes some time since an important number of evidence is required. This procedure can be accelerated taking advantage of the neighbours’ experience. In other words, each node (say n1) may calculate its neighbour’s (for example, n3) trust value either based on its own observations (direct evidence) (as in [2]) or combine it with information obtained from other nodes (for example n2 and n5). The information provided by nodes n2 and n5 is called reputation or indirect evidence [3].

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. Indirect measurements play a significant role, because, first, they increase the overhead and energy consumption and, second, this trust information exchange can be exploited by adversaries to ruin the routing functionality of the network [4]. For example, a malicious node (say n5) can spread bad rumours for certain nodes (say n2 and n3) so that their common neighbours do not use them for routing, forcing thus the traffic generated in node n1 pass through n5.

While researchers have paid attention to these attacks designing countermeasures, the network and energy resources spent on the exchange of indirect trust information have attracted very little attention. Given that reputation exchange schemes mainly benefit mobile nodes which frequently change neighbourhood, the frequency of reputation exchange information has to be fine tuned so that the trust information is disseminated prior to data
transmission by mobile nodes in new neighbourhoods, which significantly affects the performance as well as the energy and bandwidth consumption.

In this paper, we assess the performance benefits in terms of packet loss stemming from indirect trust information update and we quantify its main drawback (energy consumption) with respect to the frequency of indirect trust exchange. The rest of the paper describes the trust model used for our investigation and provides insight on the impact of any indirect trust information exchange scheme in section II. Section III presents the simulation results which enable the quantification of benefits and drawbacks while conclusions are drawn in section IV.

II. EXCHANGING INDIRECT TRUST INFORMATION

The indirect trust (IT) value is important mainly for newly initialized nodes or mobile nodes that have recently arrived in a new neighbourhood. If a node is found in different neighbourhoods each time it needs to send a new message, then direct interaction provides no trust info. In this case, if trust information is exchanged between nodes and especially if this exchange happens more frequently than the data message transmission, the source node has gathered (indirectly) trust information before it sends out a new data message. Thus, the exchange of indirect trust is useful mainly when node mobility has to be supported.

Assuming that the trust management developer has opted for indirect trust information exchange, an important design option has to be considered: the frequency of this exchange. The exchange frequency directly affects the speed of trust information dissemination and thus trust knowledge building as well as the energy consumed for this exchange. Numerous approaches have been pursued in the literature, starting from simple broadcasting of reputation request, expecting that all nodes will reply with information regarding their neighbours.

To limit the exchanged information, only positive (or negative) information has been proposed to be shared [5]. However, when only positive information is shared, since nodes learn only from their own experience about a malicious node, colluding malicious nodes can extend each other’s survival time through false praise reports. If all N one-hop neighbours are asked triggering the generation of N reputation response messages, the network load would be significantly burdened (increasing collision probability) and the node resource (memory, processing and energy) consumption would also increase significantly. Based on this observation, another way to limit the introduced overhead is to narrow down the set of requested nodes, e.g. asking for indirect trust only highly trusted nodes. Unfortunately this approach allows neighbours to learn which nodes their neighbours trust and then they can try to attack them or perform Sybil attack (steal the ID and pretend they are highly trusted nodes).

To investigate the impact of indirect trust update frequency, we have chosen to consider and model the Ambient Trust Sensor Routing (ATSR) solution, a location based routing approach that incorporates a trust model suitable for large and mobile Wireless Sensor Networks (WSN) (presented in [6]). In this model, every node monitors all one-hop neighbours to check whether they forward the messages they receive towards the sink node. The ratio between the actually forwarded and all the transmitted messages provides an indication, whether the selected neighbour is sincerely cooperating. Values close to 1 indicate a benign node, while values close to 0 indicate malicious nodes. This information is then used to calculate the routing function, based on which the next hop node is selected.

Coming to the indirect trust exchange mechanism, in ATSR, we opted for requesting reputation information from a limited number (four) of neighbours, as a first action towards limiting the introduced overhead. In more detail, the source node randomly selects one node per quadrant so that only four unicast reputation request and four unicast reputation response messages are generated (instead of N+1, in case all neighbours were asked using one broadcast message and N replies). Although the selection of the four nodes could be performed based on direct trust information (i.e. ask the most trusted nodes) or on the remaining energy information, this would reveal to an adversary (performing traffic analysis) certain attributes of the selected (requested) nodes. Moreover, the source node needs to obtain indirect trust information for all of its one-hop neighbours and this can be achieved only by asking uniformly geographically distributed nodes.

Since the reputation exchange is mainly implemented to assist nodes with no or limited (direct) trust knowledge to reach a more reliable conclusion for the trustworthiness of nodes they are interested in, in ATSR a requested node provides its opinion for its neighbours only if it is confident about the direct trust value it has calculated. This is decided based on the number of direct interactions the node has attempted with a neighbour. To avoid the disadvantages of reporting only positive/negative trust information, only confident trust information is reported, limiting this way the amount of communicated data (overhead) and economizing resources.

The reason we have chosen ATSR for our investigation is three-fold: first, it has already taken action towards economizing energy by asking a subset of just four nodes, second, it enhances robustness of indirect trust dissemination by allowing only the exchange of confident trust information and third, it adopts geographical routing which has the minimum routing overhead and inherently supports mobility.

III. SIMULATION RESULTS

The JSim platform [7] has been used to model ATSR for different indirect trust exchange intervals. Although the presented approach can be applied to any routing protocol for trust evaluation purposes, for the simulation needs, the geographical approach is adopted: routing is decided on a hop-by-hop basis and every node selects for forwarding the node that maximizes a routing cost function value, where the distance metric and the total trust value calculated by node A on node B are summed up with weights 0.6 and 0.4 respectively. The distance metric is maximized for one-hop neighbours of node A that are closer to the destination. The
node that corresponds to the maximum value of the routing function is selected for forwarding the packet as it represents a good candidate satisfying both trust and proximity to the destination requirements.

The considered topology includes 100 nodes initially placed on a symmetric 10x10 grid (the inter-node distance is assumed to be 100 distance units). Data messages are transmitted every 4s, beacon messages are transmitted every 2s, while the mobility speed is measured in distance units per second, i.e., mobility speed 2 indicates that a node covers a grid edge distance (100 units) in 50s. All nodes move in continuously and randomly changing direction, the initial trust value for all neighbors has been set equal to 1 (i.e., all nodes are considered to be trusted a priori) and the simulation run time was equal to 4000s for all scenarios. The presented results were obtained after 50 replications. The malicious nodes are issuing black-hole attacks (i.e., they refuse forwarding messages) and they are randomly distributed in the grid in each run. Five data sessions were generating data packets towards the same sink node.

A. The Benefits of Indirect Trust Exchange

To evaluate the benefits of indirect trust exchange on the WSN performance, we performed a scenario set where 30% of network nodes are operating in a malicious mode, refusing to forward the data messages they receive from their neighbors. The main benefit expected from the indirect trust exchange is the improvement in packet loss, since, based on this exchange, a benign node is informed about the malicious behavior of certain nodes before it directly interacts with them. To quantify this benefit, we measured the packet loss for the case where no indirect trust information is exchanged and for the case of different frequencies of indirect trust exchange. The results are presented in Figure 1.

![Figure 1. Packet loss for 30% malicious nodes in the network.](image)

The packet loss observed for 30% malicious nodes in the network is higher when indirect trust is not exchanged, which proves the benefit of this procedure. Comparing the packet loss obtained for different mobility speeds, as mobility speed increases, packet loss increases as well. Nodes arriving in a new neighborhood need to exchange indirect trust information to perform routing decisions in a trust-aware manner. It is also evident that varying the indirect trust exchange frequency, small performance variation is observed.

B. The Impact of Indirect Trust Exchange Frequency on Packet Loss

It is essential for a system developer and implementer to decide how frequently the indirect trust information will be exchanged. While by intuition, it can be stated that increasing this frequency, the performance in terms of packet loss is expected to improve, this improvement has to be quantified and to be compared with possible drawbacks. To provide insight to the reader, we first investigate the packet loss as a function of mobility speed in a network with no malicious nodes. (It is reminded that mobility speed is expressed in distance units (du) per second, where the distance unit can be selected based on the initial nodes’ distance.) The results are included in Figure 2.

![Figure 2. Packet loss for 0% malicious nodes in the network as a function of the mobility speed.](image)

A first obvious effect is that the packet loss (even in the absence of malicious nodes) increases with the mobility speed. This happens because as nodes move around, they send a message for forwarding to a neighbor, who is no longer in their range, and thus the packet is lost. A second observation is that the performance difference among the different tested cases is rather small compared to the packet loss introduced by the mobility. While the highest packet loss for mobility speed equal to 1.5 distance units per second is 15%, the packet loss decrease brought by different trust approaches cannot exceed 5%, which however is an improvement of almost 30% of the highest packet loss.

Having quantified the packet loss caused by node mobility, it is now possible to evaluate the benefits brought by the trust management scheme, which targets the detection and avoidance of malicious nodes, i.e., the network performance should not be affected by the existence of malicious nodes. To this aim, we have run simulation scenarios assuming that 30% of network nodes are acting maliciously. The observed packet loss is depicted in Figure 3.

![Figure 3. Packet loss for 30% malicious nodes in the network.](image)

It is clear that when indirect trust is exchanged, the degradation in packet loss is less than 5% compared to the case where no malicious nodes exist in the network. This reveals how efficient the indirect trust exchange can be when nodes move around. When no indirect trust is exchanged, the impact of the presence of 30% malicious nodes is about 10%
and the absolute value of the observed packet loss reaches 25% for mobility speed equal to 1.5du/s. The performance improvement brought by the indirect trust exchanged varies depending on the frequency of the exchanged trust information. However, this variation is no more than 3%. While someone would expect that the highest frequency exchange (3s in the tested cases) would lead to the best performance, this is not verified by the simulation results. The reason is that when indirect trust is exchanged every 3s, the messages generated for this reason cause significant congestion and, thus, part of the benefits of indirect trust exchange are canceled by the produced collisions.

![Figure 3. Packet loss for 30% malicious nodes in the network as a function of the mobility speed](image)

**C. Energy Consumption**

Any node in a wireless sensor network consumes energy for transmitting and receiving data and control messages. Data messages are either generated by the node itself (including the data it sensed) or received from other nodes and should be forwarded to the sink node. Control messages carry routing information as well as indirect trust information in our case. The routing information in geographical protocol is the node’s location which is included in periodically issued beacon messages. To evaluate the energy consumption we have averaged the energy consumption of all the nodes in the network since these are changing roles (forwarding or not packets to the sink node) as they move around. The results for different indirect trust exchange intervals (RR) are depicted in Fig. 4 for different values of the mobility speed.

![Figure 4. Energy consumption rate (expressed in percentage of the initial node energy consumed every 1000s) as a function of the mobility speed (in distance units per second)](image)

The main conclusion drawn from this figure is that for any mobility speed, the energy consumption is lower for less often indirect trust information reporting. For more frequent indirect trust exchange, the energy consumption increases by more than 50%. This should guide any system designer to carefully select the indirect trust exchange frequency because this affects the energy consumption, without bringing corresponding benefits in terms of packet loss.

**IV. CONCLUSIONS**

Wireless Sensor Networks are vulnerable to a wide set of routing-related attacks. To defend against these attacks, the nodes monitor the behavior of their neighbors and calculate the trustworthiness which is then used to make trust-aware decisions. To accelerate the trust knowledge building procedure, nodes exchange trust opinions. This exchange enables the faster detection of malicious nodes and thus packet loss is improved. This advantage is even more evident as the mobility speed increases. However, the indirect trust exchange consumes the scarce energy resources and this consumption increases with the exchange frequency. The simulation results show that this increase is very important and is not justified by relevant improvements in packet loss. To this end, the indirect trust exchange improves the network performance (when mobility has to be supported) but the exchange frequency should be very well considered.

**ACKNOWLEDGMENT**

The work presented in this paper was partially supported by the EU-funded FP7-ICT-257245 VITRO project.

**REFERENCES**


