Energy-aware Secure Routing for Large Wireless Sensor Networks

THEODORE ZAHARIADIS, HELEN C. LELIGOU, STAMATIS VOLIOTIS, SOTIRIS MANIATIS, PANAGIOTIS TRAKADAS, PANAGIOTIS KARKAZIS
Electrical Engineering Department,
Technological Educational Institute of Chalkida,
Psahna 34400, Evia
GREECE
{zahariad, leligou, svoliotis, smaniatis, trakadasp, karpa}@teihal.gr

Abstract: - Wireless Sensor Networks (WSN) are vulnerable to a wide set of attacks which threaten the network operation. Although communication and security technologies for computer networks have reached a mature stage, their applicability in WSNs is disputable due to their infrastructure-less operation and the limited node and network resources. Focusing on the routing procedure, this relies in the cooperation among neighboring nodes and a long list of attacks that can cause serious damage have already been identified. The situation is futher aggravated as the next generation wireless sensor network will be larger and larger. To face this problem, we propose a secure routing protocol (Ambient Trust Sensor Routing, ATSR) which adopts the geographical routing principle to cope with the network dimensions and part of the routing attacks, while it relies on a distributed trust model for the detection of another part of the routing attacks. Both direct and indirect trust information is taken into account to evaluate the trustworthiness of each neighbour. An important feature of the proposed routing solution is that it takes into account the remaining energy of each neighbour, thus allowing for better load balancing and network lifetime extension. Based on computer simulation results we evaluate the additional energy consumption caused by the exchange of indirect trust information and the benefits stemming from the adoption of our algorithm.

Key-Words: - Wireless Sensor Networks, routing, security, trust model, energy awareness

1 Introduction

Efficient solutions for a great variety of applications can be built based on a set of low-cost sensors organized in a wireless network. The potential application domains include military fields, healthcare, homeland security, industry control, intelligent green aircrafts and traffic control in smart roads. Although networking and security technologies are in an advanced stage [1], wireless sensor networks present intricacies which dictate the design of new protocols. First, these networks operate in an infrastructure-less ad hoc manner, which implies that the communication relies on the cooperation among nodes for the accomplishment of basic networking tasks such as routing. Each time a sensor needs to send the sensed value to the data sink, it looks for an available neighbor. As these are ad hoc networks designed to operate in a self-organized manner, a malicious node may enter the network. Due to the wireless operation, eavesdropping can be easily performed in this environment which makes the network vulnerable not only to privacy attacks, but also to traffic analysis attacks which threaten the whole network operation. Cryptography and authentication can help but do not suffice due to the constraints described above. To this end, security (although vital for most application cases) is seriously threatened in wireless sensor networks [2] and the routing procedure is at the focus of adversaries due to its importance for the proper network operation and its vulnerability introduced by the required cooperation. The routing attacks as reported in [3] and [4] form a long list and address the sincere execution of the routing procedure. For example, a node exhibiting selfish behaviour may refuse to forward all or part of its neighbours' traffic issuing black-hole (or grey-hole) attack. A malicious node may also modify any packet it forwards (modification/ integrity attack), which affects the communication. More sophisticated attacks (like the replay attacks) try to deceive the routing protocol advertising wrong information.

To combat malicious behaviours, an approach borrowed from human societies has been proposed in the literature: nodes monitor the behaviour of their neighbours in order to establish trust relationships among 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 (see [5]). In other words, a trust management system is implemented [6], [7], [8]. To complete the routing protocol design, once the trustworthiness of each neighbour is evaluated, its exploitation to decide the routing path has to be defined. The selection of the most trusted neighbour [9], although straightforward, may result in the exhaustion of its energy, which contradicts the principle that energy consumption should be considered in all layer protocol design in order to realize the vision of "autonomous, long-lived" sensor networks. Placing emphasis on the energy restrictions, different directions have been pursued: the organization of the sensor networks in clusters has been shown to extend the lifetime of the network ([10], [10], [12]) while routing protocols taking into account the remaining neighbours' energy levels have also been proposed [13], [14], with some of them achieving their goal taking into account the sensing area of each node. In [15] the authors proposed a routing protocol that features improved security and targets the extension of the network lifetime. However, this is achieved at the expense of calculating the sensing area of each neighbour. The combination of energy-awareness with the realization of a trust management system has attracted little attention so far. The implementation of a trust management system increases the energy consumption while to achieve higher security (even when the sensor nodes are moving) and robustness in the trust calculation, in [16], the exchange of trust information is proposed which further increases the node energy consumption due to the transmission and processing of the trust-related messages.

In this paper, we present a secure routing protocol called Ambient Trust Sensor Routing (ATSR), which is based on a distributed trust management system combined with a geographical routing. It is capable of detecting malicious nodes in order to avoid them during routing decisions, while energy awareness is embedded in the routing protocol, allowing for better load balancing in the sensor network. We place special emphasis on evaluating the energy consumption with and without indirect trust information exchange and we prove the advantages caused by the energy awareness.

In the rest of the paper, we first present ATSR in section 2. The simulation model is briefly outlined in section 3. The performance results concerning the detection of malicious nodes are presented in section 4 while the focus is on the energy consumption with the relevant results included in section 5. Conclusions are drawn in section 6.

2 Ambient Trust Sensor Routing (ATSR)

The proposed Ambient Trust Sensor Routing (ATSR) routing protocol follows the geographical approach. 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) presented in [17], 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 decrease its routing trust value i.e. the possibility to accomplish the task. For this reason, we have incorporated the energy awareness in the total trust value a node calculates for its neighbors. In our novel routing protocol, the BEACON message is extended to include the "remaining energy" field of the source node. Following this scheme, 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, i.e. the reported in the BEACON message value is:

$$T_E = V_{now}/V_{initial} \quad (1)$$

where V_{now} and $V_{initial}$ stand for the remaining and initial energy level respectively.

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.

2.1 Trust evaluation

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 [18]. Trading-off security and implementation cost, we have selected a set of metrics which includes metrics that reveal the cooperation willingness of the nodes both as regards routing and the reputation information exchange. In more detail, the behaviour aspects to monitor are:

- *Packet forwarding*: To detect nodes that deny to or selectively forward packets.
- *Network layer Acknowledgements (ACK)*: Each node should check whether it receives the network layer ACK from the Base Station.
- *Message Integrity*: The source node overhears the wireless medium to check whether the packet was forwarded without unexpected modifications.
- *Node Authentication*: Distinguish between nodes successfully passing the authentication procedure each time they are challenged.
- *Confidentiality*: Nodes supporting encryption or other confidentiality schemes are earmarked in order to be preferred over those not supporting, if possible.
- *Reputation Response*: Each time a node transmits a reputation request message to a neighbor, the reputation requests number stored in the trust table for this neighbor increases while the reputation response number increases only if the neighbor replies. In this way, nodes that do not cooperate in the execution of the reputation protocol are assigned lower trust values.
- *Reputation Validation*: To protect against bad-mouthing attacks and wrong reputations being spread around, each time a node A receives a reputation response message from node C regarding node B, if node A is confident about the direct trust value it has calculated for node B, it compares the received value (i.e. the reputation provided from node C) with its own direct trust on node B. If the difference exceeds a predefined threshold, then the provided reputation is considered as "wrong reputation"; otherwise it is a "correct reputation". Node A is confident for the trust value it has calculated for node B only if it has performed an adequate Number Of direct Interactions (noi).

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 [15], 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.

As regards the quantification of trust, for each monitored behavior listed above (except confidentiality), node A calculates a trust value regarding node B based on the following equation:

$$T_i^{A,B} = \frac{S_i^{A,B}}{S_i^{A,B} + F_i^{A,B}} \qquad (2)$$

where S_i and F_i stand for the number of successful and failed co-operations respectively. 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 seven monitored behaviours as well as the remaining energy (T_E metric) are combined in a weighted sum to produce the total trust value:

$$DT^{A,B} = \sum_{1}^{8} (W_i * T_i^{A,B}) \quad (3)$$

Where W_i stands for the weight of each trust metric with all weights summing up to 1 so that the total trust value ranges from 0 to 1.

2.2 The Role of the Indirect Trust

The indirect trust (IT) value is important mainly for newly initialized nodes or recently arrived nodes (in case of mobility). To trigger the indirect trust exchange process, each node periodically issues a reputation request message. A crucial design issue affecting the produced network load and the consumed node resources is to decide which nodes should be queried for indirect trust evidence. Given that the trust model will be incorporated in a location–based routing solution, the candidate nodes are all one-hop neighbors (this may change if another type of routing protocol was selected). We opted for requesting reputation information from a limited number (e.g. four) of neighbors, 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. Although the selection of the four nodes could be performed based on direct trust information or on 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 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, a requested node provides its opinion for its neighbors only if it is confident about the direct trust value it has calculated. This is decided upon the so-called confidence factor of node i considering node j, which increases with the Number Of Interactions between node i and node j. So, following this novel scheme, the requested node scans its trust table and includes in its reputation response message, the direct trust value it has calculated for all neighbors corresponding to confidence factor exceeding a predefined threshold (e.g. above 0.9). To avoid the disadvantages of reporting only positive/negative trust information, we have chosen to report only confident trust information, limiting this way the amount of communicated data (overhead) and economizing resources.

Once node i that transmitted the reputation request message receives the reputation responses from nodes, containing their trust info for each neighboring node j, the received values are summed up adopting the relevant direct trust as weight factors, so that a reputation provided by a highly trusted node counts more. Finally, the Total Trust (TT) value for a neighbor j is produced combining direct and indirect trust values in the following formula:

$$TT^{A,B} = C^{A,B} * DT^{A,B} + (1 - C^{A,B}) * IT^{A,B} \qquad (4)$$

where $C^{A,B}$ is the confidence factor described previously. It is obvious that as the number of interactions (and thus the confidence factor, C) increases, the direct trust value becomes more significant than the reputation information.

2.3 Trust and energy-aware routing cost function

Once the trustworthiness of a node has been evaluated, the next step is to exploit this information during routing decisions. Choosing the most trusted node results in a robust and secure sensor network design. However, it is not the best option since it results in the exhaustion of the trusted node power resources due to poor load balancing. Another option is to set a trust threshold, and route packets through nodes exceeding this threshold (e.g. [15]. The selection of the threshold can be application specific, offering flexibility but is not a straightforward procedure, while it may result in low connectivity in certain cases.

The node that will be selected to forward a packet has to be highly trusted, as close to the destination as possible and at the same time have enough remaining energy to complete its forwarding task.

As regards the distance of the neighbor to the base station, the relevant metric included in the routing function is computed as follows:

$$T_d^{A,B} = 1 - \frac{d_i}{\sum d_i} \qquad (4)$$

Where d_i is the distance of neighbor i to the base station and Σd_i stands for the sum of the distances of all its neighbours to the base station. Following equation (4), the shortest distance maximizes the value.

The distance to the base station and the total trust value (which has already incorporated the remaining energy value) are summed up in a weighted manner and are used to calculate the Routing Function following the equation:

$$RF^{A,B} = W_d * T_d^{A,B} + W_T * T^{A,B} \qquad (5).$$

Where W_d and W_T, represent the significance of distance and trust (which incorporates the energy) criterion. The node that maximizes this routing

function is selected for forwarding the packet as it represents a good candidate satisfying an integrated set of requirements. The weight factors can play an important role as will be shown in the performance section.

3 ATSR Performance evaluation

The performance of the proposed secure routing protocol has been evaluated through computer simulations. The JSim platform [19] has been used to model our approach. The simulated network topology includes 100 sensor nodes placed in a 10x10 grid as shown in Fig. 1.

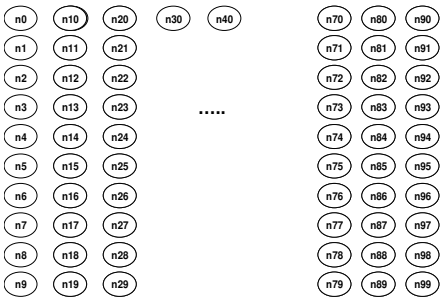

Fig. 1 The WSN topology used in the simulation scenarios.

The initial trust value for all neighbors has been set equal to 1 (i.e. all nodes are considered to be trusted a priori). The modeled trust metrics are combined with the distance to the Base Station with weighting factors varying in the different scenarios. In the following scenarios, malicious nodes perform grey-hole attack, i.e. they randomly drop the packets traversing them unless otherwise stated. We first evaluate the proposed trust and energy-aware routing protocol as regards its efficiency in detecting the malicious nodes and then we focus on the features related to the energy awareness.

4. ATSR evaluation in detecting the malicious nodes

To evaluate the efficiency of our secure routing protocol in the presence of malicious nodes, we first compare it with the case where no trust awareness is adopted, i.e. when plain geographical routing is performed. In the case of geographical routing, even if only one malicious node issuing black-hole attack exists in the path, the connection is blocked while with the proposed algorithm the malicious nodes will be detected and avoided. Since there is little interest in comparing zero connectivity to full connectivity, we have chosen to compare GPSR with the proposed algorithm for the case where grey-hole attacks are performed, which allows for certain connectivity even when GPSR is adopted.

We have run different scenarios for varying number of malicious nodes. In this scenario set, the weights used for the calculation of the total trust were 0.5, 0.2, 0.1, and 0.2 for the forwarding, network ACK, integrity and remaining energy metrics respectively. As regards the weights of the routing function, W_d was set equal to 0.6 and W_T to 0.4 We have also run the same network set up using the GPSR algorithm for comparison reasons. The results are shown in Fig. 2.

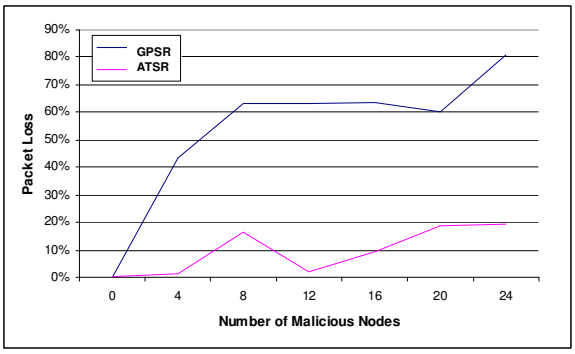

Fig. 2 Packet loss for different number of malicious (grey-hole) nodes in the network

It is obvious that our protocol performs better than GPSR in the presence of malicious nodes since it detects the attacks and succeeds in finding alternative paths to the destination, due to the presented trust model. The loss ratio is kept below 20% as long as the number of malicious nodes remains lower than 24% of the network nodes. In this case, adopting GPSR results in 80% packet loss, which leads to network collapse.

For the same scenario set, we have measured the throughput of the network, expressed as the volume of traffic received at the destination. In Fig. 3, the evolution of throughput in time (expressed in seconds) for 0 and 24 malicious nodes are shown. When no malicious nodes exist in the network, plain GPSR and our trust and energy aware routing protocol, provide similar results, as shown in curve orGPSR-0 and teGPSR-0. Since in this case all nodes are honest and highly trusted, the routing for both algorithms is based on location information. When 24 malicious nodes appear, our teGPSR performs significantly better than plain GPSR (curves orGPSR-24 and teGPSR-24). It is worth stressing that in this case, following our protocol, the nodes need some time to gather direct measurements and build trust information for their

neighbours. This is shown by the increasing throughput in the first 20s of operation (11-31s in the figure).

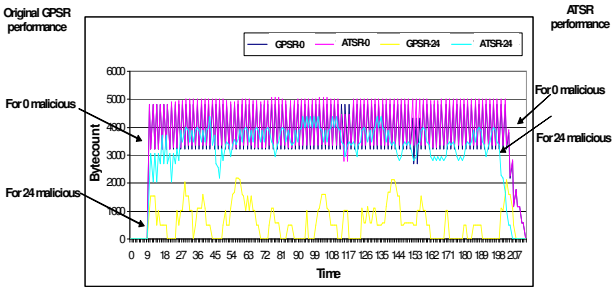

Fig. 3 The evolution of throughput in time for 0 and 24 malicious nodes in the network

From that point on, the throughput is almost stable and similar behaviour with the one observed for 0 malicious nodes is experienced, even though the simulated attack is the grey hole attack where a node randomly drops the packets. Once the malicious nodes are detected, the rest nodes communicate avoiding them, without any performance degradation from the case where no malicious nodes exist.

In ATSR, where geographical information is combined with trust information in a weighted sum producing the routing cost function, we can flexibly move the emphasis from geographical information to trust. To better investigate this aspect, we have run a second scenario set, where we have kept 24 malicious nodes in the network and we vary the weight of geographical information (W_d) in the routing function. (The weight of the trust value (W_T) is always equal to 1- W_d.) The results are shown in Fig. 4. When W_d is equal to 1, our approach becomes equivalent to plain GPSR since routing is based only on location information and packet loss is very high (80%) in this case, where 24 malicious nodes exist.

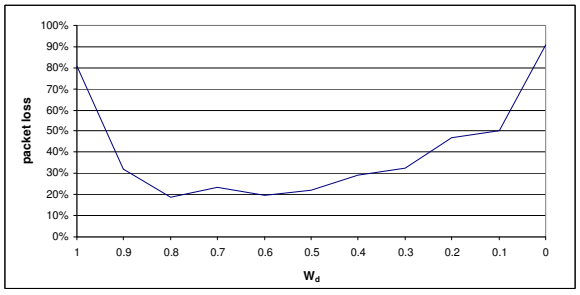

Fig. 4 Packet loss for different balance between geographical and trust information

Similar or even worse results are obtained when the weight of geographical information approaches zero, since routing is performed based only on trust information. In this case, the packets travel long paths through highly trusted nodes by they rarely manage to find their destination. The lowest packet loss ratios are observed when trust and geographical information are balanced or slightly biased towards geographical, i.e. when W_d ranges from 0.5 to 0.8.

5. Evaluating the energy consumption

In an attempt to thoroughly investigate and profile the energy consumption in a WSN, we performed a wide set of simulation scenarios.

Every node in a WSN consumes energy mainly for transmission and reception purposes. It transmits routing and data messages and thus the energy consumption depends on the node location and the data messages it generates or forwards.

To quantify these dependencies, we have run a scenario set with no malicious nodes in the network (i.e. in this scenario the proposed algorithm behaves as location-based protocol without any trust or energy awareness). 100 nodes are placed in a 10x10 grid as shown in Fig. 1. Eight nodes transmit data to the base station (node 99). The simulated application issues one packet of 31 bytes every two seconds while the Beacon interval is 0,5 seconds on average, and the reputation request interval is three seconds (unless otherwise stated).

We have measured the energy consumption of nodes 97, 89, 85, 4 which are forwarding packets generated from 4, 2, 2 and 0 connections respectively. Based on the obtained results, we have calculated and included in Table 1 the energy consumption for the case where both data and routing messages circulate in the network and the energy consumption when only routing messages are exchanged.

Node ID	paths the node participates in	Energy consumption for data and routing message exchange (per 1000s)	Energy consumption when only routing messages are exchanged	Energy consumption due to data message forwarding
97	4	0.12	0.035	0.086
89	2	0.09	0.033	0.057
85	2	0.12	0.06	0.06
4	0	0.05	0.05	0

Table 1: Energy consumption for nodes 4, 85, 89, 97 when no energy awareness is incorporated in the routing protocol

Starting from the case where only routing messages are generated, exactly as expected, the energy consumption depends on the position of the node in the network. Node 85 consumes more energy than node 4 which is at the periphery and node 4 consumes more energy than nodes 89 and 97 which are located at the periphery and near the niche of the grid.

When both data and routing messages are generated, nodes 97, 89 and 85 forward data messages and participate in 4, 2 and 2 data paths respectively. Subtracting the energy consumed due to beacon messages, we have calculated the energy consumed for the forwarding (reception and transmission) of the data messages. From Table 1, it is obvious that the energy consumption depends on the number of supported connections, which is analogous to the number of forwarded data messages (all connections generate data messages with the same frequency). Moreover, the energy required for forwarding the data is slightly greater than the energy required for the exchange of routing messages for the selected locations. It should however be pointed out that this difference depends on the relation between the frequency of routing messages exchange and the frequency of data messages exchange. The frequency of routing messages exchange, when location based routing is adopted, depends on the level of mobility that needs to be supported while the data exchange frequency depends on the application. In our simulation scenario, each node transmits a beacon message every 0.5s. In real life application, the inter-beacon interval depends on the level of mobility that needs to be supported.

To evaluate the benefits of performing energy-aware routing, we have run a simulation scenario where the routing decisions are based 40% on location attributes and 60% on remaining energy. To do so, we have set W_d=0.4, W_T=0.6, and W_e =1 (W_e is the weight for the remaining energy metrics). The same data flows were initiated and the results have shown that the path from node 61 to the base station changes after 544 data packets have been transmitted, from 61-73-85-97-99 to 61-82-94-96-98-99. Node 82 undertakes the responsibility of forwarding part of the packets sent from node 61 to node 99 and this causes an increase in its energy consumption. As long as node 82 acts as forwarding node, its energy drops by 0.08 every 1000s while when it only exchanges routing messages, it drops by 0.06. This way, the exhaustion of node 97 which previously participated in the path for the whole simulation run is avoided.

The conclusion of this simulation run is that following the proposed routing algorithm the data paths change before the forwarding nodes are exhausted, bringing all the benefits of load balancing.

5.1 The impact of the remaining energy weight factor: W_e

Our next objective is to study whether the weight factor of the remaining energy affects the energy consumption. For this reason, we tried two different values for the energy weight factor: in the first scenario We=0.9 while in the second We=0.6.

The results show that the path between 61 and 99 changes

- after 544 data messages when We=1
- after 604 data messages when We=0.9
- after 910 data messages when We=0.6

So, as the weight factor increases, the source node selects a different path earlier to avoid the exhaustion of the best (based on location attributes only) neighbour.

5.2 Energy performance Under Trust-aware Routing

Having investigated the factors that affect the energy consumption in a WSN, in this section we will investigate energy–related effects when the proposed trust model is activated. Since our target is to design a secure routing protocol, it is important to evaluate the interplay of the proposed trust model with the energy consumption. For this reason, we have carried out four simulation scenarios:

1. without energy awareness and without activating the reputation exchange protocol
2. without energy awareness and with the reputation protocol
3. with energy awareness and without the reputation protocol and
4. with energy awareness and with the reputation protocol activated

In this scenario set, nodes 22, 43, 23, 32, 42, 53, 35 and 55 were generating data packets destined to node 66. Based on a graphical tool that we have developed to depict the simulated sireless sensor network, node 55 participates in 7 connections while it also generates data packets towards the base station. Node 53 participates in 2 data paths and node 42 only generates data packets. Nodes 44, 54, 64, 65, 46, 56 were behaving as black-hole nodes (refusing to forward packets).

5.2.1 No energy awareness – no indirect trust

We have run the simulation scenario but without activating the reputation exchange protocol which is useful only when node mobility has to be supported.

For the observation window, 200,000 beacon messages are generated while 40,000 data packets are forwarded in the WSN.
The results show that comparing node's 55 energy consumption with node 53, the difference is now evident: node 53 consumes 50% of its initial energy while node 55 consumes 55% in the same time span. Comparing node 55 with node 42, the first one consumed 70% of its energy while node 42 only 47% in the same time.The data packets that managed to reach their destination although black-hole nodes exist in their path are included in Table 2 which also reports the average latency.

Source node	Data packets successfully forwarded	Latency (ms)
55	1800	1.19
35	1800	2.68
43	1800	2.68
53	1800	2.68
23	1798	4.34
32	1798	4.37
42	1797	4.37
22	1800	4.37

Table 2: successfully forwarded data packets when no energy awareness is taken into account and the reputation protocol is not activated

5.2.2 No energy awareness – indirect trust involved

When the nodes exchange reputation messages (in order to calculate the indirect trust value for their neighbours), the total energy consumption for routing and trust messages becomes larger than that for data message generation and forwarding. To evaluate this effect, we run a scenario with no energy awareness and indirect trust involved. Namely, we set W_d=0.6, W_t=0.4, W_e=0 (W_1=0.4 and W_3=0.6).
Based on the obtained results, we observe that the energy of node 55 is exhausted earlier than node 53 but the difference is rather small. This is due to the fact that during the simulation the numbers of routing and trust-related messages were higher by order of magnitude than the data packets. Namely, 200,000 beacon, 100,000 reputation request and 340,000 reputation response messages were generated, while the data packets that were greedily forwarded accounted for 28,000 only. (Other 10,000 data packets were forwarded following the perimeter mode, which proves that voids were generated in the network.) The problems caused by the absence of energy awareness are two:

- Once node 55 is exhausted, the nodes using it for forwarding packets to the base station seek for alternative paths. The existence or not of such paths depends on the location of malicious nodes. Thus, nodes that are surrounded by malicious neighbours are blocked when the single honest neighbour is exhausted.
- The sensing area covered by node 55 is no longer covered.

As shown in Table 3, other nodes manage to transmit and successfully reach the base station for significantly higher number of data packets while others are blocked earlier. As expected, those not blocked have to route their packet through longer paths, thus the measured latency is higher.

Source node	Data packets successfully forwarded	Latency (ms)
55	850	3.8
35	857	3
43	860	2.7
53	858	2.6
23	1114	9.7
32	1125	14
42	1154	14
22	1131	22

Table 3: successfully forwarded data packets when no energy awareness is taken into account and reputation protocol is activated

5.2.3 Energy awareness –indirect trust not involved

To evaluate the benefits of taking into account the remaining node energy, we have run a simulation scenario where the same source nodes were constantly injecting data packets. The energy weight was set equal to 0.8.
The energy consumption with and without energy awareness is tabulated in Table 4, where an obvious decrease in average energy consumption can be observed. The difference is more evident for node 55 which services 7 connections and thus the number of data packet it forwards is higher than the other nodes.
Studying the exact moment that the source node chooses an alternative path to route the packets, when energy is taken into account, we observe that the path alternates after the transmission of a different number of packets for each path.

Node ID	We=0, no IT	We=0.6, no IT	We=0.8, no IT	We=0.8, IT inv.	We=0, IT inv.
53 (forwarding packets from 2 paths)	16.6	16.5	14.8	55	57
55 (forwarding packets from 7 paths)	18.3	18	15	56	59
45	17.14	17	15	55	58
42 (generates data packets)	12.4	12.2	10	37.5	39.5

Table 4: Energy consumption (%) in 1000s with and without energy awareness with Indirect Trust (IT) involved or not

This happens because the routing decision is changed when the energy difference between two candidate nodes is balanced with the distance difference, i.e. two candidate nodes that are located in equal distance to the destination, the path will change as soon as the remaining energy becomes different. When the node with more energy is not at the same distance from the destination, the source node will select it only if the energy difference is greater than the distance difference. For this reason, the relevant weights play a significant role as is evident comparing the different columns in Table 4.

5.2.4 Energy awareness – indirect trust involved

Finally we run a scenario set with the same source nodes, where the reputation protocol was activated. The energy weight was set equal to 0.8.

Due to the exchange of reputation messages, the energy drops quickly thus the paths alternate more frequently than in the previous scenarios. For example, based on the results from our graphical tool, the data packets generated by node 22, were travelling to node 66 either through 22→34→55→66 or through 22→43→55→66. The paths are equivalent as regards the number of hops and the distance of the selected nodes to the base station. Thus, due to significant energy consumption for the exchange of reputation messages, the path alternates very frequently (every 2-3 data packets) for the first 450 packets. After that, the path changes to 22→24→45→66 while when 1050 packets have been successfully transmitted it further changes to 22→42→63→75→66. The other data flows exhibit similar behavior.

Another interesting observation is that due to congestion, significant part of the data packets is lost, although malicious nodes are avoided due to our trust model. For example, the data packet generated from node 23 travel through a different path now to the destination namely through 23→25→45→66. The trust model realizes that the previously used path is not successful and decides a new path.

To quantify the benefits, based on the simulation results we have calculated the energy consumption for certain nodes of interest as shown in Table 4. It is evident that energy awareness results in lower energy consumption for nodes that are otherwise burdened by the forwarding tasks.

5.2.5. Energy-results assessment

Summarising, we have investigated the parameters that affect the energy consumption in a WSN and we have evaluated the improvements brought by the proposed secure energy-aware routing solution. The obtained simulation results show that:

- The energy consumption depends on the location of a node in the network since the location directly affects the number of routing messages received by the node, as shown in the figure where different nodes consume different energy volumes even when adopting the same routing approach. Thus, energy should be taken into account during routing protocol design.
- Significant energy resources are consumed for the transmission and reception of the routing messages when these are periodically issued. The situation is further aggravated when a reputation exchange protocol comes into play, to enhance security in the presence of mobile nodes. Although the extra energy consumption depends on the frequency of the reputation exchange and in our simulations we have assumed worst case scenarios, reputation exchange protocols should be activated only when the introduced benefits justify the sacrificed energy. In the reported results we have assumed both very frequent beacon and reputation messages exchange which result in 3 times more reputation request messages and 7 times more beacon messages than data packets.
- The proposed protocol takes into account the remaining energy of each neighbour during routing

decisions. It clearly extends the lifetime of the nodes and thus the lifetime of the network. However, as the energy is only taken into account when forwarding data, the benefits (energy savings) depend on the relation between the frequency of data exchange and routing/trust message exchange.

- The benefits brought by the proposed routing solution depend on the weight factor used for energy in the trust calculation equation. As expected, when the weight factor increases, higher energy saving are achieved.

To this end, energy should be taken into account during the design of any protocol for the WSNs since it significantly affects the network lifetime and performance.

6 Conclusion

Ambient Trust Sensor Routing (ATSR) algorithm has been shown to detect fast malicious nodes and reacts in their detection, finding alternative paths. As soon as the malicious nodes are detected, the network performance becomes identical to the one observed for no malicious nodes in the network. Additionally, its energy awareness allows for better load balancing which improves the network lifetime and is considered a measure against traffic analysis attacks. The weights introduced in the calculation of the total trust value as well as those introduced in the routing function allow for flexible configuration, trade-offs and fine tuning of the algorithm as has been shown through computer simulations. ATSR bases its decisions on local information which renders it suitable for large wireless sensor networks while at the same time, node and network resources are economized. The simulation results show that significant energy is consumed for routing and trust purposes and thus the frequency of exchange of this information should be very well considered. ATSR guides the sensor nodes select for forwarding the neighbour that is not only closer to the destination but also has enough remaining energy, leading to better load balancing and energy savings.

Acknowledgement

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

References:

[1] Th. Zahariadis, S. Voliotis, "Adaptive Middleware Platform for Next Generation Mobile Networks," *WSEAS Transactions on Communications*, Vol. 3, Iss. 1, January 2004, pp. 155-160

[2] V. C. Giruka, M. Singhal, J. Royalty, S. Varanasi, "Security in wireless sensor networks", *Wireless Communications & mobile Computing* Vol. 8, 2008, pp.1–24.

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", *IEEE Wireless Communications*, Vol. 14, No. 5, October 2007, pp. 85-91.

[4] C. Karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113-127, May 2003.

[5] H. Li, M. Singhal, "A Secure Routing Protocol for Wireless ad hoc Networks", *Int. Conference on system Sciences*, Hawaii, January 4-7, 2006.

[6] A. Rezgui and M. Eltoweissy "TARP: A Trust-Aware Routing Protocol for Sensor-Actuator Networks" *IEEE International Conference on Mobile Ad hoc and Sensor Systems*, MASS 2007, Pisa, Italy, October 2007.

[7] Junbeom Hur; Younho Lee; Hyunsoo Yoon; Daeseon Choi; Seunghun Jin "Trust evaluation model for wireless sensor networks" *Advanced Communication Technology Conference*, 2005, ICACT 2005, Page(s):491 – 496

[8] 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

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

[10] Taewook Kang, Jangkyu Yun, Hoseung Lee, Icksoo Lee, Hyunsook Kim, Byunghwa Lee, Byeongjik Lee Kijun Han, "A clustering method for energy efficient routing in wireless sensor networks Source" *6th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications*, Corfu Island, Greece, 2007 pp 133-138

[11] Ching-Mu Chen, Tung-Jung Chan, Tair-Rong Chen, "A Non_Ack routing protocol in ad-hoc wireless sensor networks", *WSEAS Transaction On Communications* Vol. 7, Iss. 8, August 2008, pp 847-856

[12] Yoon-Su Jeong, Yoon-Cheol Hwang, Sang-Ho Lee, "Efficient Cluster-based Routing Protocol for Wireless Sensor Network" *WSEAS Transaction On Communications* Iss. 5, Vol. 5, May 2006

[13] Jeng-Wei Lee; Yi-Tsung Chen; Yau-Hwang Kuo, "Energy-Efficient Geographic Relay for Ad-Hoc Wireless Networks", 3rd International Conference on *Intelligent Information Hiding and Multimedia Signal Processing*, 26-28 Nov. 2007, (IIHMSP 2007).

[14] Razia Haider, Muhammad Younas Javed, Naveed S. Khattak, "EAGR: Energy Aware Greedy Routing in Sensor Networks", Conf. on *Future generation communication and networking*, Dec. 2007.

[15] N. B-Ghazaleh, K. D. Kang, and K. Liu, "Towards Resilient Geographic Routing in Wireless Sensor Networks", 1st ACM Workshop on *QoS and Security for Wireless and Mobile Networks*, Montreal, Canada, Oct., 2005.

[16] G. F. Marias, V. Tsetsos, O. Sekkas, P. Georgiadis "Performance evaluation of a self-evolving trust building framework ",Workshop of the 1st International Conference on *Security and Privacy for Emerging Areas in Communication Networks*, Sept 2005

[17] B. Karp, H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for WirelessNetworks", *MobiCom 2000*

[18] 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

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