Building trust among Virtual Interconnecting Smart Objects in the Future Internet

Theodore Zahariadiς, Helen C. Leligou, Panagiotis Trakadas
Synelixis/TEI of Chalkida,
Chalkida, Greece
{zahariad, leligou, ptrak}@{synelixis.com, teihal.gr}

Mischa Dohler
CTTC
Barcelona, Spain
mischa.dohler@cttc.es

Abstract—**The Future Internet is expected to connect large volumes of diverse devices (called Virtual Interconnected Smart Objects, VISO) for flexibly gathering and reacting upon abundant real-world, real-time information so as to optimize performance and enhance the user experience. The importance of security in said networks has understandably gained increasing interest as of late, with various standardization bodies gearing up efforts in defining suitable security mechanisms. Whilst cryptographic measures to ensure confidentiality, integrity and authentication are well understood in the context of low complexity embedded nodes, trust mechanisms to complement and greatly strengthen this more traditional security approach are in their infancy. Given this window of opportunity, a modular trust management system for VISO is presented. This model can be adapted to the application needs and node capabilities to enhance the trustworthiness of the overall infrastructure and is shown to yield significant gains.**

I. INTRODUCTION

The main goal of the Future Internet is to enhance the user experience which mandates the collection of real world knowledge to improve the performance of currently available user devices. Integrating the proliferating wireless sensor networks that gather real world information as well as actuators that react on this and other information is expected to provide the desired push. However, before using the information, the trustworthiness of the nodes generating the information has to be assured. Although mature security solutions for the infrastructure-based Internet world exist, the security problem has not yet been solved for Virtual Interconnected Smart Objects (VISO). We define as "VISO" small, diverse devices with limited networking, connectivity and processing resources such as wireless sensors, actuators, smart electricity meters or even virtual devices. The reason is that the processing, buffering and power of these node resources are severely limited, prohibiting the implementation of mature IP-world security solutions, while their large number and density on one hand and their mobile, unreliable and opportunistic networking characteristics further lowers their networking reliability.

In most networks of VISO, where self-organization, infrastructure-less operation is a requirement, the nodes cooperate to route/forward data to the sink node, to aggregate data and/or to build the network topology (e.g. elect the cluster head). This cooperation renders them vulnerable to a wide set of attacks from simple denial of cooperation/forwarding to more sophisticated attacks. Several trust management schemes [1]-[6] have been proposed in the literature for this environment albeit little attention has been paid to the implementation feasibility of each approach and even less in standardizing the necessary tools to support their realization. To build trust knowledge, VISOs monitor the behavior of their one-hop neighbors in order to evaluate their trust-worthiness. The classification of the wealth of proposed trust models with regards to different criteria has been attempted in [7] and [8]. Main differentiation attributes include the number and type of monitored behaviors, the method/equation used to evaluate the trust value and its range, the exchange or not of indirect trust information (reputation) among the neighboring nodes, the implementation of the same trust management functionality in all network nodes or the assignment of extra tasks to certain nodes.

The diversity in the network objectives and characteristics and in the device capabilities prevents the design of a "one-fits-all" solution. For example, different sensors may be equipped with different hardware and thus the implementation of a sophisticated trust management scheme may be affordable for one sensor type while this may not be the case for a temperature sensor. Moreover, while the exchange of indirect trust information is valuable when the sensor nodes move around, it becomes of low added value when these are placed in fixed locations. Thus, the benefits of indirect trust exchange depend on the targeted application. However, the necessary communication mechanisms and message types have to be supported by the standardized solutions.

To fit the Future Internet cooperating objects needs, we propose a modular trust management framework. This framework may be considered as orthogonal to any routing algorithm as long as overhearing at networking and access layers are facilitated. In this proposal, we are using an Ambient Trust Sensor Routing (ATSR) algorithm (which is a geographical based algorithm) [9]. However, different approaches (e.g. the RPL routing algorithm adopted by the IETF ROLL WG) could be used. In any case, we assume that each component monitors the behavior of one-hop neighboring nodes in order to identify potential attacks, direct trust is progressively created, while reputation exchange (indirect trust) supports rapidly changing mobile environments.

II. DIRECT TRUST MANAGEMENT

Trust management schemes have been proven to efficiently detect routing attacks, acting as a first line of defense against adversary nodes. To defend against each attack type, different node behavior aspects need to be monitored, affecting the implementation cost of the overall trust management system. For example, to detect adversaries that deny forwarding, each node overhears the wireless medium to check whether its neighbors sincerely cooperate forwarding the packets they receive. More sophisticated attacks, attempting to mislead the routing protocol's state machine (like stale or

wrong routing information advertisement attack and acknowledgement spoofing) can be detected only by more powerful nodes equipped with intrusion detection system functionality. The proposed framework implements a set of trust metrics that have been proven [9] to fit in state-of-the-art sensor nodes (e.g. IRIS) and includes:

- Packet forwarding: To detect nodes that deny to or selectively forward packets, acting in a selfish (malicious or not) manner, each time a source node sends a packet to a neighbor for further forwarding, it enters the promiscuous mode and overhears the wireless medium to check whether the packet was actually forwarded by the selected neighbor.
- Packet precision: Apart from checking forwarding, the overheard message is processed to check the packet's integrity, i.e. that no unexpected modification has occurred.
- Network layer acknowledgements (ACK): To detect the successful end-to-end forwarding of the messages (and detect colluding adversaries), each source node waits for a network-layer ACK per transmitted packet to check whether the packet has successfully reached the sink node.
- Node-related attribute, e.g authentication scheme: The trust management module receives information from higher layer blocks related to the trustworthiness of the neighbors in terms of supported security tools. For example, in case a node may choose among neighbors supporting different authentication mechanisms, the one with better security features should be preferred. Another possible situation is to have different nodes supporting different sets of trust metrics. In this case, nodes monitoring more behavior aspects should be preferred for routing and/or for providing trust information on third nodes.
- Reputation Response and reputation validation are two trust metrics that target the detection of attacks related to the indirect trust model [5] (further details are provided in [9]).

On each sensor node, a trust repository is used to store trust-related information per neighbor (e.g. successful and total attempted interactions). Although in the proposed framework each trust metric is quantified dividing the number of successful interactions to the total number of attempted interactions, multiple alternatives exist (see [8]). The values calculated for each metric are then summed up in a weighted manner to form the direct trust value per neighbor with the weights summing up to 1.

III. REPUTATION EXCHANGE

Another important design choice adopted is the ***reputation exchange*** which is used to accelerate the trust information build-up procedure and is particularly usefully in rapidly changing mobile environments. Each node requests reputation information from its neighbors (regarding third nodes) expecting them to provide their trust knowledge. This may take place either periodically or on an event-basis (possibly reactive) and dictates the need to design a particular protocol. As an example, each node may periodically request trust information from four randomly selected neighbors (one per quadrant) to limit the trust exchange overhead; this is an implementation specific issue which affects the network performance.

The received reputation information is combined with the direct trust value to reach the total trust value (trustworthiness) for each neighbor balancing the weight between direct and indirect trust information based on the number of accomplished direct interactions. The total trust information is then taken into account for routing or higher layer purposes. As this process is also vulnerable to specific attacks [5], including wrong trust information spreading, special measures against them (reputation validation/comparison with other nodes indirect trust information) may be realized.

IV. IMPLEMENTATION CONSIDERATIONS

As the Future Internet is expected to include heterogeneous VISO of dissimilar capabilities, a flexible implementation of trust management schemes should be adopted. Assuming there is an agreement on the trust values range and meaning, neighboring nodes may evaluate trust based on a different subset of trust metrics, while the decision of the exact subset of trust metrics that each nodes supports can be left to the node owner/manufacturer since the implementation of each trust metric requires different volumes of processing and memory capabilities (indicative figures are provided in Section V). Thus, the realized trust metric subset becomes a node-attribute that should be announced to its interested neighbors in order to be taken into account during trust evaluation and routing. A similar approach is followed by the RPL, which includes node-related attributes in the routing metrics taken into account.

For the Future Internet to consist a trusted infrastructure, the necessary tools in terms of message types to support the indirect trust exchange information have to be standardized. As this consumes high node (power and hardware) and network resources (due to the introduced overhead), its realization and activation can be kept as optional. Especially regarding its operation, the possibility to turn off the exchange of indirect trust information can save energy and throughput in case of static nodes.

The possibility of allocating different roles to devices with diverse capabilities under the control and reconfiguration of a central (trusted) unit can introduce significant energy savings especially for more sensitive (low capabilities) nodes. The wireless sensor nodes can be reconfigured according to the specific application needs and/or whenever needed. For example, a subset of the operating nodes can be reconfigured to monitor or not neighboring nodes (since this consumes energy due to the required overhearing). Reconfiguration of sensor nodes over the air is nowadays feasible using appropriate operating systems and middleware applications (see [12]).

V. PERFORMANCE AND COST EVALUATION

To provide a feeling of the benefits and the cost of realizing a trust management scheme, the performance in terms of packet loss and the cost in terms of occupied RAM bytes are provided. To investigate the performance of the proposed scheme, we modeled it using the JSIM open simulation platform [11] which allows for simulating the operation of large sensor networks. The performance results in terms of packet loss are included in Figure 1. As expected, ATSR outperforms the non trust-aware GPSR [10] protocol in the presence of malicious nodes, since ATSR is capable of detecting and avoiding attacks by finding alternative paths to the destination. The proposed ATSR achieves a packet loss ratio of 15% when half of the network nodes are acting as grey-hole.

To evaluate the implementation cost of the proposed trust scheme, we developed the relevant code which was successfully compiled for IRIS motes. Focusing on the trust model, the memory requirements per trust metric are included in Figure 2 while the implementation of all the proposed trust metrics consumes 1795bytes of RAM. The reputation exchange management (mentioned as reputation protocol in the figure) consumes significant resources which drives designers to believe that this should not be implemented in static sensor networks.

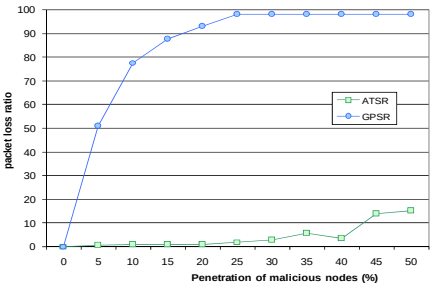

Figure 1. Packet loss ration (in %) versus the penetration of malicious grey-hole nodes in the network

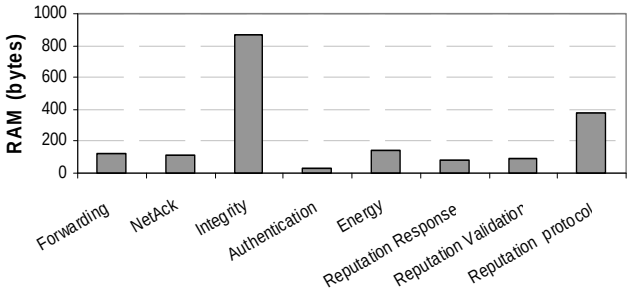

Figure 2. Implementation cost per trust metric measured in terms of RAM bytes

VI. CONCLUSIONS

To enable trusted cooperation of devices in the Future Internet, trust management has to be supported in a flexible, yet efficient way. Given that the trust models that have been proposed in the literature differ in the number and type of supported trust metrics, in the way they quantify trust and in indirect trust exchange protocol realization, we believe that a) the number and type of supported trust metrics should be decided by the node implementer to fit its hardware resources but should be announced to the neighbors at run time, b) the role of the nodes in evaluating trust can be differentiated and reconfigured by a central trust unit (assuming it exists) and c) the exchange of indirect trust necessitates the provision of specific messages and also dictates the capability of activating-deactivating it to economize resources, depending on the application requirements.

ACKNOWLEDGMENT

This publication is based on work performed in Project FP7 ICT-257245 VITRO, which is partially funded by the European Commission.

REFERENCES

[1] A. Rezgui and M. Eltoweissy “TARP: A Trust-Aware Routing Protocol for Sensor-Actuator Networks” IEEE International Conference on Mobile Adhoc and Sensor Systems, (MASS 2007), Pisa, Italy, October 8 – 11, 2007

[2] Garth V. Crosby and Niki Pissinou, “Cluster-based Reputation and Trust for Wireless Sensor Networks” Consumer Communications and Networking Conference, 2007. CCNC 2007Las Vegas, NV, USA, Jan. 2007

[3] Wei Zhang, Sajal K. Das, and Yonghe Liu, “A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks” 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, IEEE SECON, Reston, VA, USA, Sept. 25-28, 2006

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

[5] Yan (Lindsay) Sun, Zhu Han, K. J. Ray Liu, “Defense of Trust Management Vulnerabilities in Distributed Networks”, IEEE Communications Magazine, Vol. 25, No.2, February 2008, pp. 112-119.

[6] Haiguang Chen, “Task-based Trust Management for Wireless Sensor Networks”, International Journal of Security and Its Applications, Vol. 3, No. 2, April, 2009, pp:21-26.

[7] G. Theodorakopoulos and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad-Hoc Networks," IEEE Journal on Selected Areas in Communications (JSAC), Vol. 24, No. 2, Feb. 2006 pp. 318-328.

[8] Th. Zahariadis, H. Leligou, P. Trakadas, S. Voliotis, “Trust management in Wireless sensor Networks” European Transaction on Telecommunications, Vol. 21, Issue 4, June 2010, pp: 386-395 (DOI 10.1002/ett.1413).

[9] Th. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou, Charalambos Vangelatos, Lionel Besson, “Design and implementation of a trust-aware routing protocol for large WSNs”, Int. Journal of Network Security & Its Applications, July 2010, Vol. 2, No 3, pp. 52-68.

[10] Karp B, Kung HT. “GPSR: Greedy Perimeter Stateless Routing for WirelessNetworks”, MobiCom 2000.

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

[12] E. Ladis, T. Zahariadis, H. C. Leligou, et.al. “SMART: Secure, Mobile visual sensor networks ArchiTecture”, SECON2009