International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
Volume 2 Issue 1 –OCTOBER 2013.

Security Functionality in Wireless Sensor Networks Using a Trust-Aware Routing Framework

M. Praveen Kumar[#1]

[#]*Assistant Processor, Department of Computer Science & Engineering,*
King College of Technology, Namakkal, India.

***Abstract*- The multihop routing in wireless sensor networks (WSNs) offers little protection against identity deception through replaying routing information. An adversary can exploit this defect to launch various harmful or even devastating attacks against the routing protocols, including sinkhole attacks, wormhole attacks, and Sybil attacks. The situation is further aggravated by mobile and harsh network conditions. In this paper, we present a trust-aware, location-based routing protocol which protects the WSN against routing attacks, and also supports large-scale WSNs deployments. The proposed solution has been shown to efficiently detect and avoid malicious nodes and has been implemented in state-of-the-art sensor nodes for a real-life test-bed. As it will be discussed, the limited memory, computational power, energy resources and radio bandwidth of sensor nodes deeply impact the implementation strategy, while additionally, the realities of radio propagation, such as loss and asymmetric links, require careful evaluation of the routing selection metrics.**

Index Terms*- *wireless sensor network, trust management, security, implementation cost.

I. INTRODUCTION

Wireless Sensor Networks (WSN) offer efficient, low-cost solutions for a great variety of application domains including military fields, healthcare, homeland security, industry control, intelligent green aircrafts and traffic control in smart roads [1]. Although networking and security technologies are in a mature stage, the limited sensor node resources in terms of memory space, processing power and energy availability, constrain the complexity of the security mechanisms that can be implemented, dictating the need for new protocol approaches design. Due to their distributed nature, WSNs are vulnerable to various attacks [2], including attacks targeting on the disruption of the routing procedure [3]-[5] which is accomplished in a cooperative, multi-hop fashion. While the traditional (or the so called "hard") security measures (e.g. encryption, authentication) are quite efficient in mitigating some types of attacks, there are some specific types of attacks that can be better handled by using a reputation and trust-based management scheme (as an example, we mention the selfish behaviour of a node). In other words, security and trust are tightly coupled and cannot be separated from one another. As mentioned in [6]: "Cryptography is a means to implement security, but it is highly dependent on trusted key exchange.

Trust level: For a node *N*, the trust level of a neighbour is a decimal number in [1], representing *N*'s opinion of that neighbour's level of trustworthiness. Specifically, the trust level of the neighbour is *N*'s estimation of the probability that this neighbour correctly delivers data received to the base station. That trust level is denoted as *T* in this paper.

Energy cost: For a node *N*, the energy cost of a neighbour is the average energy cost to successfully deliver a unit-sized data packet with this neighbor as its next-hop node, from *N* to the base station. That energy cost is denoted as *E* in this paper.

II. RELATED WORKS

Trust-based enhancements on the routing protocols for WSN have been widely addressed in the literature. The most important research results in this direction include:*Trusted AODV:* The well-known AODV routing protocol has been extended by Xiaoqi Li et. al to perform routing by taking into account trust metrics. A trust recommendation mechanism is first introduced and then the routing decision rules of AODV are modified to take into account trust. Of particular interest is that a set of policies is derived for a node to update its opinions towards others since, it is necessary to design a trust information exchange mechanism when applying the trust models into network applications. More specifically, three procedures (Trust Recommendation, Trust Judgment, Trust Update) are defined as well as the accompanying Route Table Extension, Routing Messages Extensions, Trusted Routing Discovery

SPINS: A suite of security protocols optimized for sensor networks (SPINS) has been designed [7] to provide data confidentiality, two-party data authentication, and evidence of data freshness. It involves two secure building blocks: SNEP and μTESLA. SNEP introduces a small overhead of 8 bytes, it maintains a counter but no counter values are exchanged (protecting the network from eavesdropping) and achieves semantic security. μTesla provides authentication for data

broadcast. Emphasis has been placed on the limited processing and memory resources available in sensor networks environment. SPINS claim to provide trusted routing ensuring data authentication and confidentiality. However, it does not deal with Denial of Service Attacks or compromised nodes. It only ensures that a compromised node does not reveal all the keys of the network.

III. PROPOSED WORK

We start by stating the design considerations of TARF in Section 2. Then, we elaborate the design of TARF in Section 3, including the routing procedure as well as the Energy-Watcher and Trust Manager components. In Section 4, we present the simulation results of TARF against various attacks through replaying routing information in static, mobile and RF-shielding conditions. Section 5 further presents the implementation of TARF, empirical evaluation at a large sensor network and a resilient proof-of-concept mobile target detection application based on TARF. To further evaluate the efficacy of TARF in terms of energy efficiency and *throughput*, we have developed a reconfigurable emulator of wireless sensor networks on a two-dimensional plane with Matlab [8]. To effectively simulate a WSN, this emulator uses the object-oriented technique to construct two classes of objects: WSNMANAGER and NODE, to represent the whole network and a sensor node. The interaction between nodes is emulated through event passing. The routing function for a node can be rewritten to adopt different routing protocols; different maps can also be ported into this simulator. To simulate the unreliable wireless transmission, the outcome of one-hop packet transmission is decided by the following model: suppose a node A is wirelessly transmitting a packet to node B, the probability for B to successfully receive such a packet is assumed to be

IV. CONCLUSION

We presented a trust-aware routing protocol that can efficiently detect and avoid nodes issuing routing attacks based on a distributed trust management system. The proposed routing solution was successfully implemented and validated in real-life sensor nodes proving its implementation feasibility. The realisation of a trust-aware routing protocol brings clear performance benefits as both the simulation and real –life test-bed results have shown. The involved implementation cost mainly depends on the adoption of a reputation exchange protocol and on the number of behaviour aspects used for the evaluation of each node's trustworthiness.

V. REFERENCES

[1] [1] I.F. Akyildiz, T. Melodia, and K.R. Chowdury, "Wireless Multimedia Sensor Networks: A Survey", *IEEE Wireless Communications*, December 2007, pp. 32- 39.

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

[3] [3] C. Karlof, and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *Ad Hoc Networks*, Elsevier, ed. Vol. 1, 2003, pp. 293–315.

[4] [4] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", *IEEE Wireless Communications*, October 2007, pp. 85-91.

[5] [5] Y.L. Sun, Z. Han, and 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] [6] A. A. Pirzada, C. McDonald, and A. Datta, "Performance Comparison of Trust-Based Reactive Routing Protocols", *IEEE Transactions on Mobile Computing*, Vol. 5, No. 6, June 2006.

[7] [7] T. Zahariadis, H. Leligou, S. Voliotis, S. Maniatis, P. Trakadas, and P. Karkazis, "An Energy and Trust-aware Routing Protocol for Large Wireless Sensor Networks," *WSEAS Transactions on Communications*, Issue 9, Volume 8, September 2009, pp. 981-991.

[8] [8] P. Trakadas, S. Maniatis, P. Karkazis, T. Zahariadis, H.C. Leligou, and S. Voliotis, "A novel flexible trust management system for heterogeneous wireless sensor networks", *9th International Symposium on Autonomous Decentralized Systems* (ISADS 2009), Athens, Greece, March 23-25, 2009.