Secure Routing to Prevent Sybil Attack in Sensor Networks

Mohammed Abrar[1], P. Subhadra[2]

[1]M. Tech Scholar, Computer Science and Engineering
Vardhaman College of Engineering, Hyderabad, India
abraryc49@gmail.com

[2]Associate Professor, Department of CSE
Vardhaman College of Engineering, Hyderabad, India
subhadra.perumalla@gmail.com

Abstract: ***Evaluation of Wireless Sensor Networks (WSN) for performance evaluation is a popular research area and a wealth of literature exists in this area. Denial-of-Service (DoS) attacks are recognized as one of the most serious threats due to the resources constrained property in WSN. The Zigbee model provided in OPNET 16 is suitable for modelling WSNs. This paper presents an evaluation of the impact of DoS attacks on the performances of Wireless Sensor Networks by using the OPNET modeller. Numerical results, discussions and comparisons are provided for various simulation scenarios. The results can be of great help for optimisation studies in WSN environments under DoS attacks as well as understanding the severity and critical nodes within the WSN. The effects of DoS attacks on the performance of WSNs are considered to critically analyse these issues.***

Keywords: Wireless Sensor Network, Denial of Service attack, Zigbee model, OPNET, DoS attack

1. Introduction

Smart environments represent next evolutionary development step in building, utilities, industrial, home, shipboard, and transportation systems automation. Like any sentient organism, the smart environment relies first and foremost on sensory data from the real world. Sensory data comes from multiple sensors of different modalities in distributed locations. The smart environment needs to the information about its surroundings as well as about its internal workings; this is way to captured in biological systems by the distinction between exteroceptors and proprioceptors. The challenges in the hierarchy detecting the relevant to the quantities, monitoring and collecting the data, assessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions are enormous, network traffic.

Those routing packets, including their original headers are replayed without any modification. Even if this malicious node cannot directly overhear the valid node's wireless transmission, it can collude with other malicious nodes to receive those routing packets and replay them somewhere far away from the original valid node, which is known as a wormhole attack. Since a node in a WSN usually relies solely on the packets received to know about the sender's identity, replaying routing packets allows the malicious node to forge the identity of this valid node.

After "stealing" that valid identity, this malicious node is able to misdirect the network traffic. For instance, it may drop packets received, forward packets to another node not supposed to be in the routing path, or even form a transmission loop through which packets are passed among a few malicious nodes infinitely. It is often difficult to know whether a node forwards received packets correctly even with overhearing techniques. Sinkhole attacks are another kind of attacks that can be launched after stealing a valid identity. In a sinkhole attack, a malicious node may claim itself to be a base station through replaying all the packets from a real base station. Such a fake base station could lure more than half the traffic, creating a "black hole". This same technique can be employed to conduct another strong form of attack - Sybil attack: through replaying the routing information of multiple legitimate nodes titles to the network. A valid node, if compromised, can also launch all these attacks. The harm of such malicious attacks based on the technique of replaying routing information is further aggravated by the introduction of mobility into WSNs and the hostile network condition. Though, mobility is introduced into WSNs for efficient data collection. The detection of routing loops and the corresponding reaction are excluded from the implementation of TrustManager since many existing protocols, such as Collection Tree Protocol on the other and the link connectivity-based the protocol, already provide that feature. As we have worked on the first and efficient fully-functional protocol.

Unlike other security measures, TARF requires neither tight time synchronization nor known geographic information. Most importantly, TARF proves resilient under various attacks exploiting the replay of routing information, which is not achieved by previous security protocols. Even under strong attacks such as sinkhole attacks, wormhole attacks as well as Sybil attacks and hostile mobile network condition, TARF demonstrates steady improvement in network performance. The effectiveness of TARF is verified through extensive evaluation with simulation and empirical experiments on large-scale WSNs. Finally, we have implemented a ready-to-use TARF module with low overhead, which as demonstrated can be integrated into existing routing protocols with ease; the demonstration of a proof-of-concept mobile target detection program indicates the potential of TARF in WSN applications. We start by stating the design considerations of TARF in Section 1. Then we elaborate the design of TARF in Section 2 including the routing procedure as well as the Energy

Watcher and TrustManager components. In Section 3 we present the simulation results of TARF against various attacks through replaying routing in- formation in static, mobile and RF-shielding conditions. Section 4 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.

2. Design Considerations

Before elaborating the detailed design of TARF, we would like to clarify a few design considerations first, including certain assumptions in Section 2.1 and the goals consideration.

2.1 Assumptions

We target secure routing for data collection tasks, which are one of the most fundamental functions of WSNs. In a data collection task, a sensor node sends its sampled data to a remote base station with the aid of other intermediate nodes. Though there could be more than one base station, our routing approach is not affected by the number of base stations; to simplify our discussion, we assume that there is only one base station. An adversary may forge the identity of any legal node through replaying that node's outgoing routing packets and spoofing the acknowledgement packets, even remotely through a wormhole. Additionally, to merely simplify the introduction of TARF, we assume no data aggregation is involved.

2.2 Routing Procedure

TARF, as with many other routing protocols, runs as a periodic service. The length of that period determines how frequently routing information is exchanged and updated.

At the beginning of each period, the base station broadcasts a message about data delivery during last period to the whole the network consisting of a few contiguous packets (one packet may not hold all the information). Each such packet has a field to indicate how many packets are remaining to complete the broad- cast of the current message.

The completion of the base station broadcast triggers the exchange of energy report in this new period. Whenever a node receives such a broadcast message from the base station, it knows that the most recent period has ended and a new period has just started. No tight into the time synchronization is required for a node to keep track of the beginning or ending of a period. During each period, the Energy Watcher on a node monitors energy consumption of one-hop transmission to its neighbours and processes energy cost reports from those neighbours to maintain energy cost entries in its neighbourhood table; its Trust Manager also keeps track of network loops and processes broadcast messages from the base station about data delivery to maintain trust level entries in its neighbourhood table. To maintain the stability of its routing path, a node may retain the same next-hop node until the next fresh broadcast message from the base station occurs. Mean-while to reduce traffic, its energy cost report could be configured to not occur again until the next fresh broadcast message from the base station. If a node does not change its next- hop node selection of until the next broadcast message from the base station, that guarantees all paths to be loop-free, as can be deducted from the procedure of next-hop node selection.

However, as noted in our experiments, that would lead to slow improvement in routing paths. Therefore, we allow a node to change its next-hop selection in a period when its current next-hop node performs the task of receiving and delivering data poorly. Next, we introduce the structure and exchange of routing information as well as how nodes make routing decisions in TARF.

3. Implementation on and Empirical Evaluation

In order to evaluate TARF in a real-world setting, we implemented the TrustManager component on TinyOS 2.x, which can be integrated into the existing routing protocols for WSNs with the least effort. Originally, we had implemented TARF as a self- contained routing protocol on TinyOS 1.x before this second implementation. However we decided to redesign the implementation considering the following factors. First, the first implementation only supports TinyOS 1.x, which was replaced by TinyOS 2.x; the porting procedure from TinyOS 1.x to TinyOS 2.x tends to frustrate the developers. Second, rather than developing a self-contained routing protocol, the second implementation only provides a TrustManager component that can be easily incorporated.

Implementation, we noted that the existing protocols provide many nice features, such as the analysis of link quality, the loop detection and the routing decision mainly considering the communication cost. Instead of providing those features, our implementation focuses on the trust evaluation based on the base broadcast of the data delivery, and such trust information can be easily reused by other protocols.

Finally, instead of using TinySec exclusively for encryption and authentication as in the first implementation on TinyOS1.x, this implementation let the developers decide which encryption authentication techniques to employ; the encryption and authentication techniques of TARF may be different than that of the existing protocol.

4. Conclusions

We have designed and implemented TARF, a robust trust-aware routing framework for WSNs, to secure multi-hop routing in dynamic WSNs against harmful attackers exploiting the replay of routing information. TARF focuses on trustworthiness and energy efficiency, which are vital to the survival of a WSN in a hostile environment. With the idea of trust management, TARF enables a node to keep track of the trustworthiness of its neighbours and thus to select a reliable route. Our main contributions are

listed as follows. Unlike the way previous efforts at secure routing for WSNs, TARF effectively protects WSNs from severe the attacks through replaying routing information; it requires neither tight time synchronization nor known geographic information.

References

[1] J. Newsome, E. Shi, and D. Song, "The Sybil Attack in Sensor Network: Analysis & Defences," The Third Intl. Symposium on Information Processing in Sensor Networks (IPSN'04), Berkeley, California, USA: ACN Press, 2004, pp.185-191

[2] D. Murat, and S. Youngwhan, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," World of Wireless, Mobile and Multimedia Networks, WoWMoM 2006. International Symposium, 2006, pp.259-268

[3] J. Wang, G. Yang, Y. Sun, and S.Chen, "Sybil attack detection based on RSSI for wireless sensor network," WiCom '07: International Conference on Wireless Communications, Networking and Mobile Computing, September 2007, pp. 2684-2687, 21-25

[4] L. Shaohe, W. F. Xiaodong, Z. Xin, and Z. Xingming, "Detecting the Sybil Attack Cooperatively in Wireless sensor Networks," in International Conference on Computational Intelligence and Security, CIS '08. Vol.1 2008, pp.442-446

[5] Z. Qinghua, W. Pan, S. Douglas, and P Ning, "Defending against Sybil attacks in sensor networks," Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshop (ICDCSW'05), 2005, pp.185-191

[6] J.R. Douceur. The Sybil attack. In First International Workshop on Peer-to Peer Systems (IPTPS'02), Mar 2002