International Journal of Information and Computation Technology (IJICT)
ISSN 0974-2239 Volume 3, Number 10 (2013)

TRUST EVALUATION BASED SECURITY IN WIRELESS SENSOR NETWORK

[1]Janani.C
[1]M.E. Student, ,
[1]SSM College Of Engineering,
[1]Komarapalayam,
[1]Namakkal District.

[2]Mrs. P.CHITRA B.E., M.S., PH.D.,
[2]Head Of The Department,CSE
[2]SSM College Of Engineering
[2]Komarapalayam,
[2]Namakkal District.

ABSTRACT

The multi-hop 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. Traditional cryptographic techniques or efforts at developing trust-aware routing protocols do not effectively address this severe problem. To secure the WSNs against adversaries misdirecting the multi-hop routing, that has been designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception; the resilience of TARF is verified through extensive evaluation with both implementation and empirical experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions.

Index Terms: Wireless Sensor Networks, Wireless Sensor Network, Trusted Aware Routing Framework (TARF), TinyOS.

I INTRODUCTION

Wireless sensor networks (WSNs) are ideal candidates for applications to report detected events of interest, such as military surveillance and forest fire monitoring. A WSN comprises battery-powered senor nodes with extremely limited processing capabilities. With a narrow radio communication range, a sensor node wirelessly sends messages to a base station via a multi-hop path. However, the multi-hop routing of WSNs often becomes the target of malicious attacks. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes, or jam the communication channel by creating radio interference.

A. PROBLEM STATEMENT

As a harmful and easy-to-implement type of attack, a malicious node simply replays all the outgoing routing packets from a valid node to forge the latter node's identity; the malicious node then uses this forged identity to participate in the network routing, thus disrupting the network traffic. 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, which is known as a wormhole attack.

A node in a WSN 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. It may drop packets received, forward packets to another node not supposed to be in the routing path, or form a transmission loop through which packets are passed among a few malicious nodes infinitely.

Sinkhole attacks can be launched after stealing a valid identity, in which 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, an attacker may present multiple identities to the network. A valid node, if compromised, can also launch all these attacks.

II DESIGN CONSIDERATIONS

ASSUMPTIONS

The target is 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, as shown in Figure 1. 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, 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*.

Finally, a data packet has at least the following fields: the sender id, the sender sequence number, the next-hop node id (the receiver in this onehop transmission), the source id (the node that initiates the data), and the source's sequence number. It insists that the source node's information should be included for the following reasons because that allows the base station to track whether a data packet is delivered. It would cause too much overhead to transmit all the one hop information to the base station. Also, it assumes the routing packet is sequenced.

Goals

High Throughput at a moment is computed over the period from the beginning time (0) until that particular moment. Note that single-hop re-transmission may happen, and that duplicate packets are considered as one packet as far as *throughput* is concerned. *Through put* reflects how efficiently the network is collecting and delivering data. ***Energy Efficiency*** It evaluates energy efficiency by the average energy cost to successfully deliver a unit-sized data packet from a source node to the base station. Note that link-level re-transmission should be given enough attention when considering energy cost since each re-transmission causes a noticeable increase in energy consumption.

Scalability & Adaptability It will evaluate the scalability and adaptability of TARF through experiments with large-scale WSNs and under mobile and hash network conditions. Here it does not include other aspects such as latency, load balance, or fairness. Low latency, balanced network load, and good fairness requirements can be enforced in specific routing protocols incorporating TARF.

III MODULES DESCRIPTION

A. Routing the Network

For a TARF-enabled node N to route a data packet to the base station, N only needs to decide to which neighboring node it should forward the data packet considering both the trustworthiness and the energy efficiency. Once the data packet is forwarded to that next-hop node, the remaining task to deliver the data to the base station is fully delegated to it, and N is totally unaware of what routing decision its next-hop node makes. N maintains a neighborhood table with trust level values and energy cost values for certain known neighbors.

B. Transfer File

In this module, Analysis the Shortest Path algorithm independently routes each logical link on a physical path with the minimum number of hops in trusted network basis. Hence, under the algorithm Shortest Path, each light- path greedily takes the most reliable route and transfers the file.

C. Sinkhole and Wormhole Attacks

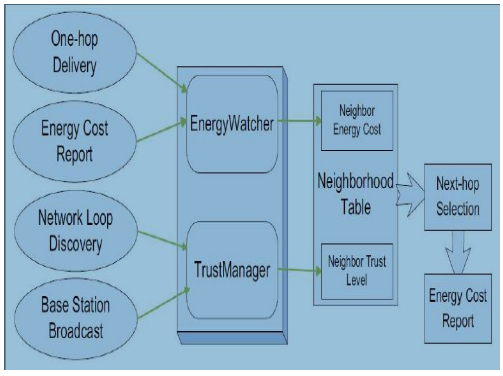
Prevent the base station from obtaining complete and correct sensing data

Particularly severe for wireless sensor networks some secure or geographic based routing protocols resist to the sinkhole attacks in certain level many current routing protocols in sensor networks are susceptible to the sinkhole attack Set of sensor nodes

Continuously monitor their surroundings forward the sensing data to a sink node, or base station Many-to-one Communication vulnerable to the *sinkhole attack*, where an intruder attracts surrounding nodes with unfaithful routing information alters the data passing through it or performs selective forwarding

D. Energy Watcher & Trust Manager

In this module Cluster-based WSNs allows for the great savings of energy and bandwidth through aggregating data from children nodes and performing routing and transmission for children nodes. In a cluster-based WSN, the cluster headers themselves form a sub-network, after certain data reach a cluster header, the aggregated data will be routed to a base station only through such a subnetwork consisting of the cluster headers. A node N's TrustManager decides the trust level of each neighbor based on the following events: discovery of network loops, and broadcast from the base station about data delivery.



.

In this figure, each node selects a next-hop node based on its neighborhood table, and broadcast its energy cost within its neighborhood. To maintain this neighborhood table,

Energy Watcher and *TrustManager* on the node keep track of related events (on the left) to record the energy cost and the trust level values of its neighbors.

IV RELATED WORK

It is generally hard to protect WSNs from *wormhole* attacks, *sinkhole* attacks and *Sybil* attacks based on identity deception. The countermeasures often requires either tight time synchronization or known geographic information. FBSR, as a feedback-based secure routing protocol for WSNs , uses a statistics-based detection on a base station to discover potentially compromised nodes. But the claim that FBSR is resilient against *wormhole* and *Sybil* attacks is never evaluated or examined; the Keyed-OWHC-based authentication used by FBSR also causes considerable overhead. There also exists other work on trust-aware secure routing that is evaluated only through computer simulation, such as.

There are certain existing secure routing solutions for WSNs based on trust and reputation management; however, they rarely address the "identity theft" exploiting the replay of routing information. Two such representative solutions are ATSR and TARP. Neither ATSR nor TARP offers protection against the identity deception through replaying routing information. ATSR is a location-based trust-aware routing solution for largeWSNs. ATSR incorporates a distributed trust model utilizing direct and indirect trust, geographical information as well as authentication to protect the WSNs from packet misforwarding, packet manipulation and acknowledgements spoofing. Another trust-aware routing protocol for WSNs is TARP, which exploits nodes' past routing behavior and link quality to determine efficient paths.

VI CONCLUSIONS AND FUTURE WORK

Designed and implemented TARF, a robust trust aware routing framework for WSNs, to secure multihop 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 neighbors and thus to select a reliable route.

Unlike previous efforts at secure routing for WSNs, TARF effectively protects WSNs from severe attacks through replaying routing information; it requires neither tight time synchronization nor known geographic information. The resilience and scalability of TARF are proved through both extensive simulation and empirical evaluation with large-scale WSNs; the evaluation involves static and mobile settings, hostile network conditions, as well as strong attacks such as wormhole attacks and Sybil attacks.

REFERENCES

[1] Guoxing Zhan, Weisong Shi, "Design and Implementation of TARF: Trust-Aware Routing Framework for WSNs" IEEE Transactions On Dependable And Secure Computing, vol. 9, no. 2, March/April 2012

[2] G. Zhan, W. Shi, and J. Deng, "Tarf: A Trust-Aware Routing Framework for Wireless Sensor Networks," Proc. Seventh European Conf. Wireless Sensor Networks (EWSN '10), 2010.

[4] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[6] M. Jain and H. Kandwal, "A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks," Proc. Int'l Conf. Advances in Computing, Control, and Telecomm. Technologies (ACT '09), pp. 555-558, 2009.
[7] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side," Proc. IEEE Int'l Conf. Wireless and Mobile Computing, Networking and Comm. (WIMOB '08), pp. 526-531, 2008.
[8] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," Proc. Third Int'l Conf. Information Processing in Sensor Networks (IPSN '04), Apr. 2004.