IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 01-03
www.iosrjournals.org

A Secure Routing Framework for Wireless Sensor Network

[1.]J. Ranjani, [2.]S.Vimalathithan,
Asst.Professor, Dept. of IT Indra Ganesan College of Engineering, Trichy.
Associate Professor, Dept. of CSE, Indra Ganesan College of Engineering, Trichy.

Abstract: *The multi-hop routing in wireless sensor network (WSNs) offers little protection against identity deception through replaying routing information. An adversary can exploit this defect to launch various harmful attacks like wormhole attack, sinkhole and Sybil attack. Traditional cryptographic techniques used in trust aware routing framework (TARF) but it do not effectively address this severe problem. To secure the WSNs against adversaries misdirecting the multi-hop routing, we have designed and implemented TARF .Without tight time synchronization or known geographic information. TARF provides trustworthy and energy efficient route. TARF proves effective against those harmful attacks developed out of identity deception.*

I. INTRODUCTION

Wireless sensor networks are highly distributed network in which contain hundreds or thousands of nodes. It is used to monitoring the real time environment. Wireless sensor networks are ideal candidates for applications to report detected events of interest, such as military surveillance and forest fire monitoring. This paper focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception. Based on identity deception, the adversary is capable of launching harmful and hard-to-detect attacks against routing, such as selective forwarding, wormhole attack, sinkhole attack and Sybil attack.

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 relay them somewhere far away from the original valid node which is known as a wormhole attack. 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, it is also known as" black hole".

This same technique can be employed to conduct another strong form of attack is Sybil attack. An attacker may present multiple identities to the network.

TARF mainly guards a WSN against the attacks misdirecting the multi-hop routing, especially those based on identity theft. Finally, we assume 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 one-hop transmission), the source id (the node that initiates the data), and the source's sequence number. We insist 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.

II. RELATED WORKS

The multi-hop routing in wireless sensor networks (WSNs) [1] offers little protection against identity deception through replaying routing information [3].An adversary can exploit this defect to launch various harmful or even devastating attacks like sinkhole attacks [2], wormhole attacks and Sybil attacks. The network routing information is not trusted on always. some kind of unknown may direct or give fake identity and involved as real node.

Traditional cryptographic techniques or efforts at developing trust-aware routing protocols do not effectively address this severe problem. At that time the file could be affected by hackers. So, the network will be damaged. 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.

Many routing, power management, and dissemination protocols have been specially designed for WSNs where energy awareness is an essential design issue. The routing protocols [7] are depending on the application and network architecture. Protocols are classified mainly as fat, hierarchical and location-based routing. For simulation we have taken heretical type for implementation of this paper.

IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 01-03
www.iosrjournals.org

III. SYSTEM DESIGN

TARF aims to achieve the following desirable properties such as high throughput, energy efficiency, scalability and adaptability. TARF secures the multi-hop routing in WSNs against intruders misdirecting the mutli-hop routing by evaluating the trustworthiness of neighboring nodes. It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput.

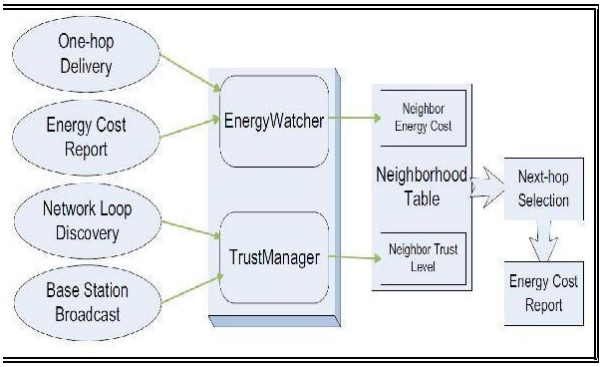

Figure.1 System Architecture

For each node N in a WSN, to maintain such a neighborhood table with trust level values and energy cost values for certain known neighbor. The two main components in TARF is Energy Watcher and Trust Manager .It is used to calculate energy cost and trust values. Based on signature, energy level and trust values, we have to identify the trustworthy neighbor node. The signature is an identity of sensor nodes. Nowadays, TARF is mainly used in forest fire monitoring and military surveillance. It is used to avoid those attacks.

Energy Watcher is responsible for recording the energy cost for each known neighbor, based on N's observation of one-hop transmission to reach its neighbors and the energy cost report from those neighbors. Trust Manager is responsible for tracking trust level values of neighbors based on energy watcher and trust manager algorithm.

IV. CONCLUSION

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. TARF mainly focuses on trustworthiness and energy efficiency to select a reliable route for transmission.

V. IMPLEMENTATION AND RESULT

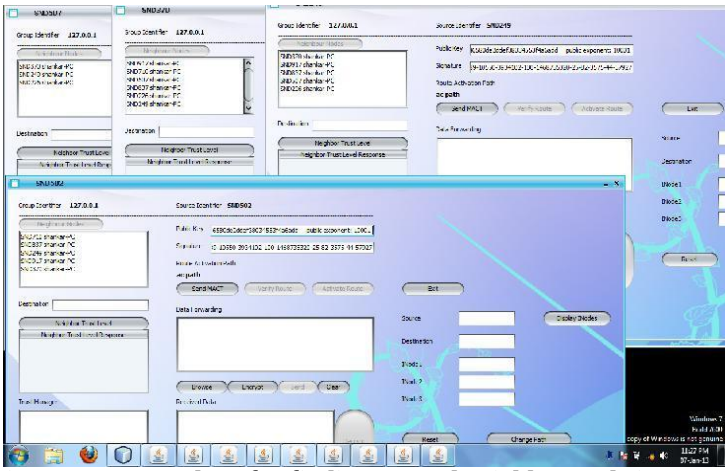

Figure.2: Screen shots for finding trusted neighbor node in TARF

REFERENCES

[1]. G.Zhan, W.Shi, and J.Deng, "Tarf: A trust aware routing framework for wireless sensor network," in proceeding of the 7th European conference on Wireless sensor networks (EWSN'10), 2010.
[2]. C.Karlof and D.Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in proceedings of th 1st IEEE International Workshop on Sensor Network Protocols and Applications, 2003.
[3]. A.Perrig, R.Szewczyk, W.Wen, D.Culler and J.Tygar, "SPINS: Security protocols for sensor networks," Wireless Networks Journal (WINET), vol.8, no.5, pp.521-534, sep. 2002
[4]. Z.Cao, J.Hu, Z.Chen, M.Xus, and X.Zhou, "Fbsr: feedback-based secure routing protocol for wireless sensor networks," International journal of Pervasive Computing and Communictions, 2008.I.FAkyildiz, W.Su, Y.Sankarasubramaniam, and E.Cayirci, "A Surveyon sensor networks," IEEE Communications Magazine, vol.40, no.8, pp.102-114, Aug.2002.
[5]. S.Chang, S.Shieh, W.Lin, and C.Hsieh, "An efficient broadcast authentication scheme in wireless sensor networks, " in proceedings of the 2006 ACM Symposium on Information, computer and communications security (ASIACCS'06). New York, NY, USA: ACM, 2006, PP.311-320.
[6]. J.Al-Karaki and A.Kamal, "Routing techniques in wireless sensor networks: a survey," wireless Communication, vol.11,no. 6, pp.6-28, Dec.2004.
[7]. J.Newsome, E.Shi, D.Song, and A.Perrig, "The sybil attack in sensor networks: Analysis and defenses," in Proc of the 3rd International Conference on Information Processing in Sensor Networks (IPSN'04), Apr. 2004.
[8]. R.Watro, D.Kong, S.Cuti, C.Gardiner, C.Lynn, and P.Kruus, "Tinypk: securing sensor networks with public key technology," in proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN'04). New York, NY, USA: ACM, 2004, PP.59-64.
[9]. T.Ghosh, N.Pissinou, and K.Makki, "Collaborative trust-based secure routing against colluding malicious nodes in multi-hop ad hoc networks," in Local Computer Networks, 2004.29th Annual IEEE International Conference on, Nov.2004, pp.224-231.