Secure Dynamic Routing Framework Techniques for Wireless Sensor Networks

[1]Dingari Kalpana, [2]M. Ramesh Kumar

[1]Dept. of Computer Science, Vignana Bharathi Institute of Technology, Ghatkesar, Telangana
[2]Dept. of Information Technology, Andhara Pradesh Electronics Corporation, Hyderabad, Telangana, India

Abstract : Wireless sensor networks are ideal candidates for applications to report detected events of interest such as military surveillance and forest fire monitoring. A WSN comprises battery powered sensor nodes with extremely limited processing capabilities. A sensor node wirelessly sends the message to the base station via multi hop path. However the multi hop routing frame work of WSNs often becomes the target of malicious attacks. The multi-hop routing in wireless sensor networks (WSNs) offer little protection against identity deception through replaying routing information. 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, we have designed and implemented a robust secure routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, it provides trustworthy and energy-efficient route.

I. INTRODUCTION

Wireless sensor networks are ideal candidates for applications such as military surveillance. A wireless sensor network is a new technology consists of spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound, pressure and cooperatively pass their data through the network to the base station. Multi-hop routing of the wireless sensor networks often becomes the target of malicious attacks. The attacker may tamper nodes physically, create traffic collisions with seemingly valid transmission, drop or misdirect messages in routes. Basically sensor networks are application dependent. Sensor networks are primarily designed for real time collection and analysis of low level data in hostile environment.

This paper focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception. The harmful attacks focused are selective forwarding, wormhole attacks, sinkhole attacks, and Sybil attacks.

The attacks we identify are

a. Denial of service

b. Modify the packet header

c. Flooding attacks

d. Replaying and recoding data packets.

Denial of service attacks include deliberately dropping packets instead of forwarding them as well as actively interfere in the communication of neighboring nodes.Replaying packets in wireless network differs from replay attacks in conventional wired networks, in terms of both time and space. Malicious nodes can move to different areas of the network to replay data packets. Sequence numbers are primarily used by TCP to maintain the order of packets sent via aconnection.

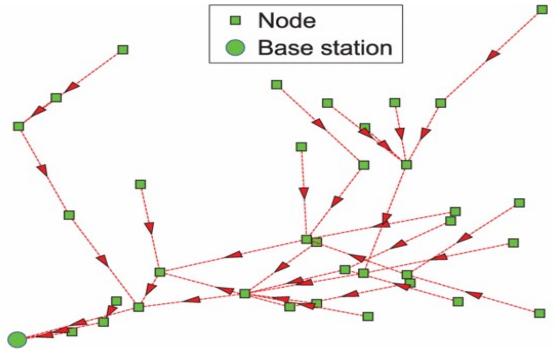

Fig 1: Multi-hop Routing

II. MALICIOUS ATTACKS ON WIRELESS SENSOR NETWORKS

Attacks arising from malicious behavior can be divided into those where packets are originated by the malicious node and those where a malicious node is an intermediate node and receives control packets for forwarding.When a malicious node is originating packets, it can send control packets using its own source address, an address which belongs to an existing node in the ad hoc network, or an arbitrary address which does not belong to anynode. Malicious intermediate nodes can either modify or replay received packets. Current sensor routing protocols are not designed for security and be insecure, mostly optimized for limited capability of the nodes.

This paper focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information. Based on identity deception the adversary is capable of launching harmful and hard to detect attacks against routing such as selective forwarding worm hole attacks, sinkhole attacks.

2.1 Wormhole attacks

A network that tunnel information to another network, that is it gets the data from one network replicate it into another network through tunnel that particular network may confused due to this action. At that time hacker may easily enter and do misuse inside the network.An extraneous A - B link can be artificially created by an intruder node X by worm holing control messages between A and B in the Fig2. A longer wormhole can also be created by two colluding intruders X and X’ in the Fig 3.

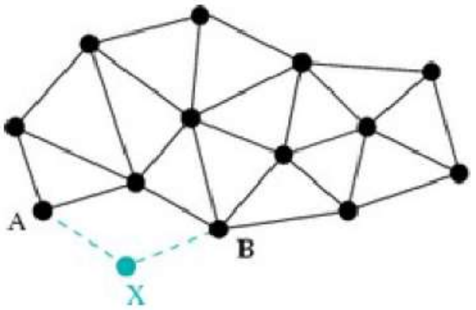

Fig 2:A wormhole created by node X

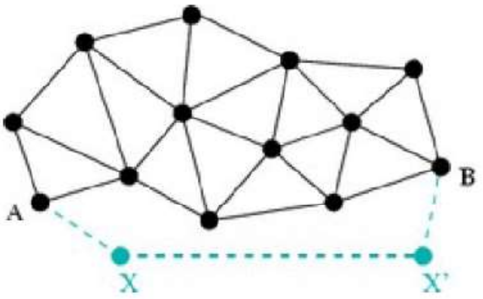

Fig 3: longer wormhole created by 2 colluding nodes X &X’

2.2 Sinkhole Attacks

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 the traffic, creating a black hole.In a sinkhole attack, the adversary’s aim is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center.

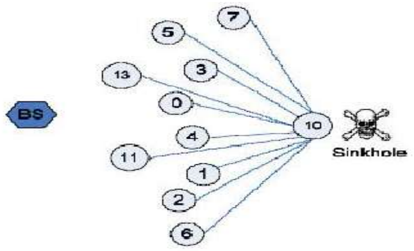

Fig 4: Sinkhole Attack

III. DESIGN OF SDRF

We target secure routing for data collection tasks which is one of the most fundamental functions of WSNs. In a data collection a sensor node sends its sampled data for remote base station with the addition of other intermediate nodes.The SDRF secures the multi-hop routing in WSNs against intruders misdirecting the multi-hop routing by evaluating the trustworthiness of neighboring nodes. SDRF is also energy efficiency, highly scalable andis adaptable.

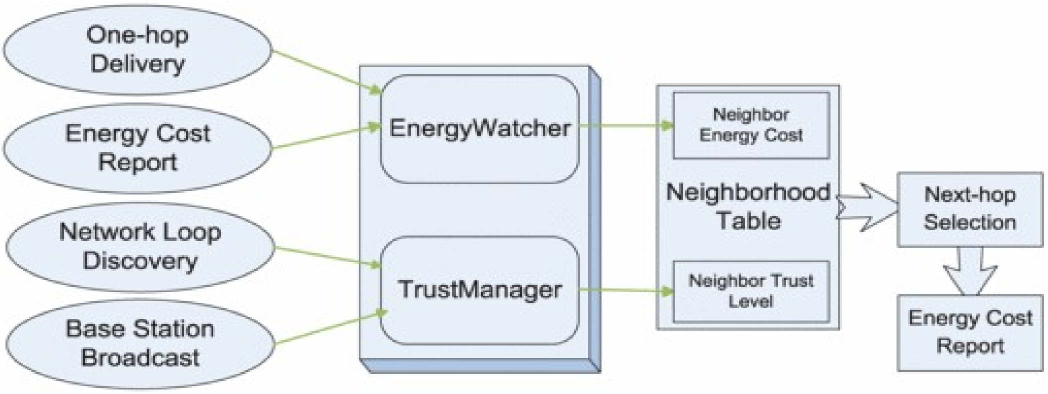

Fig 5 Analysis of Energy Watcher and Trust Manager

Neighbor: For anode N, a neighbor of N is a node theta is reachable from N with one-hop wireless transmission.

Trust Level: The trust level of a neighbor is N’s estimation for a node N is the probability that this neighbor correctly delivers data received to the base station.

Energy cost: For a node N the energy cost of a neighbor is the average energy cost to successfully deliver a unit sized.

3.1 Energy efficiency

Data transmission accounts for a major portion of the energyconsumption. We evaluate 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 retransmission should be given enough attention when considering energy cost since each retransmission causes a noticeable increase in energy consumption. If every node in a WSN consumes approximately the sameenergy to transmit a unit-sized data packet, we can use another metric hop-per-delivery toevaluate energy efficiency. Under that assumption, the energy consumption depends on thenumber of hops, i.e., the number of one-hop transmissions occurring. To evaluate how efficiently energy is used, we can measure the average hops that each delivery of a data packet takes, abbreviated as hop-per-delivery.

3.2Trust Manager Efficiency

TrustManager identifies the low trustworthiness of various attackers misdirecting the multi-hop routing, especially those exploiting the replay of routing information. It isnoteworthy that TrustManager does not distinguish whether an error or an attack occurs to the next-hop node or other succeeding nodes in the route.

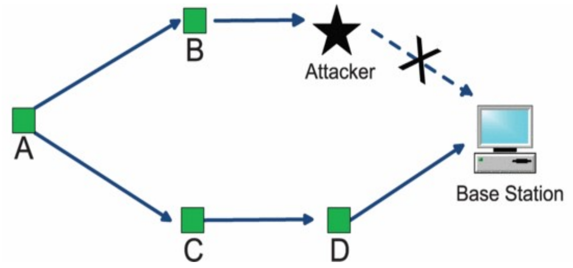

Fig 6:An exampleto illustrate how the TrustManager works

IV. SCALABILITY AND ADAPTABILITY

SDRF should work well with WSNs of large magnitude under highly dynamic contexts. We will evaluate the scalability and adaptability of SDRF through experiments with large-scale WSNs and under mobile and hash network conditions.

Here, we do 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 SDRF.

V. CONCLUSION

SDRF, a robust trust-aware routing framework for WSNs, to secure multi-hop routing indynamic WSNs against harmful attackers exploiting the replay of routing information.SDRF focuses on trustworthiness and energy efficiency, which are vital to the survival of a WSN in a hostile environment.

REFERENCES

[1] Y.B. Lin and I. Chlamtac, Wireless and Mobile Network Architecture, John Wiley & Sons, October 2000

[2] P. Nicopolitidis, M.S. Obaidat, G.I. Papadimitriou, and A.S. Pomportsis, Wireless Networks, John Wiley & Sons, November 2002.

[3] Y. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A secure On-Demand Routing for Ad-Hoc Networks,” Proceedings of ACM MOBICOM 2002, pp 12-23, September

[4] L.Zhou and Z.J. Haas ,”Securing Ad Hoc Networks,” IEEE Network Magazine, Vol. 3, no 6, pp. 24-30, December 1999.

[5] C. Karlof, N. Sastry, and D. Wagner, “Tinysec: A Link Layer Security Architecture for Wireless Sensor Networks,” Proc. ACM Int'l Conf. Embedded Networked Sensor Systems (SenSys '04), Nov. 2004.

[6] G. Zhan, W. Shi, and J. Deng, “Design, Implementation and Evaluation of Tarf: A Trust-Aware Routing Framework for Dynamic WSNs,”

[7] T. Ghosh, N. Pissinou, and K. Makki, “Collaborative Trust-Based Secure Routing against Colluding Malicious Nodes in Multi-Hop Ad Hoc Networks,” Proc. 29th Ann. IEEE Int'l Conf. Local Computer Networks, pp. 224-231, Nov. 2004.

[8] A. Abbasi and M. Younis, “A Survey on Clustering Algorithms for Wireless Sensor Networks,” Computer Comm., vol. 30, pp. 2826-2841, Oct. 2007.

[9] 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.

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

◈◈◈