Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Routing Security in Wireless Sensor Network

Ajay Rani
M.Tech. Student
Department of Computer Science and Applications
Kurukshetra University, Kurukshetra, Haryana, India

Abstract—Wireless sensor network is a promising new technology in recent years. There are many routing protocols designed in wireless sensor network, but almost no one is designed strictly with security as a goal. Routing security is especially important for sensor networks. This review paper proposed the security goal for routing in sensor network. This review paper shows that how various attacks can be adapted into powerful attacks against sensor network. We define various attacks and suggest counter measure and design considerations. This is the analysis of secure routing in sensor networks.

Keywords— Wireless Sensor networks; security; secure routing

I. INTRODUCTION

Wireless sensor network consists of thousands of node working as self-organising, low power, low cost sensor nodes. In wireless sensor network Potential applications include inventory control, medical monitoring, emergency response, target tracking in battlefields, disaster relief network and many more applications are dependent on the timeliness and accuracy of data collected by separated nodes in wireless sensor network. Therefore the key obstacle in wireless sensor network for all these application is security. Correctness of route and data is necessary condition, that ensure the normal work of wireless sensor network and routing protocol are responsible for this. Our main focus is on the routing security in wireless sensor network. Routing protocols in wireless sensor network optimised for the limited capability and application specific nature but use a rare consideration of security. Although protocol have not been designed with security as a goal. But it is necessary to analyse the security properties. The measure issues that complicates the design of a secure routing protocols in network aggregation. In conventional network secure routing protocol is required to generate the message availability. Message integrity, authenticity and confidentiality are handled by end-to-end security mechanism such as SSH and SSL. End-to end security is possible in convention network because it is not mandatory for intermediate routers to access the contents of message. Where in wireless sensor network, in-network made end-to-end mechanism hard to deploy because intermediate node needs direct access to content of message. Various attacks are possible, two main classes of attacks – sinkhole attack and HELLO floods attack analyse the security of all major sensor network protocols. There are some crippling attacks. Link layer security mechanism can provide some help but not enough. Therefore routing protocols must be implemented with security in mind.

II. VARIOUS ATTACKS ON SENSOR NETWORK ROUTING:

A large amount of sensor nodes are densely deployed communication mode is many-to-one. In large scale deployment, message has to traverse many hops before reaching their destination. With message collection, redundancy elimination and data compression processing, intermediate node also need to undertake the function of router and therefore sensor network are more vulnerable to attacks.

A. *Spoofed , Altered, or Replayed routing information*

The most direct attack against routing protocol is to target the routing information exchanged between nodes. By spoofing, altering, or replaying routing information adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten short routes, generate false error messages, partition the network, increase end-to-end latency etc.

B. *Selective Forwarding*

In multihop networks often it is assumed that the participating nodes will sincerely forward the received message. In selective forwarding attack, a malicious node may refuse to forward any message and simply drop them, so that they are not propagated any further. The simple form is that malicious nodes behaves like a black hole and refuse to forward every packet it sees. A more subtle form of attack is when adversary interested in modifying packets originating from selected few nodes and reliably forwarding remaining packets to limit suspicion of its wrongdoing. We assumes that an adversary launching a selective forwarding attack by following the path of least resistance and, is most effective when the attacker explicitly included on the actual path of a data flow. In next two sections, we discuss

sinkhole and Sybil attack, two mechanisms by which an adversary can efficiently include herself on the path of targeted data flow.

C. *Sinkhole Attacks*

In sinkhole attack adversary's goal is to attract nearby traffic in the particular area by announcing the shortest path to destination. It actually announces a high quality route by transmitting with enough power to reach to destination through single hops or by wormhole attack. Adversary creates a large "sphere of influence" attracting all traffic destined for a station from several hops away. Sinkhole attack can enable many other attacks (selectively forwarding, wormhole attack, spoofed, altered etc.). One of the main goal for establishing a sinkhole attack is that it makes selective forwarding trivial. The main reason those sensor networks are more susceptible to sinkhole attacks are due to their specialized communication pattern.

D. *Sybil Attacks*

In Sybil attack [1] multiple identities are announced by the node in the network. Sybil attack can reduce the effectiveness of fault tolerant schemes for examples: - distributed storage [2], dispersity [5] and multipath [6] routing, topology maintenance [7] and [8] replicas, storage partitions etc. Sybil attacks can also pose a threat to geographical routing protocols. By using Sybil attacks an adversary can be in more than one place at once.

E. *Wormhole Attacks*

In wormhole attack [3] a tunnel is made by attacker in order to attract packets and transmit packets to another place in network. A very simplest form of this attack is placement of a single node between two distant nodes by offering a shortest route. An adversary situated close to the base station may completely disrupt routing by creating a well-placed wormhole. This can create a sinkhole. It can also be used to exploit routing race conditions and effective even if routing information is authenticated and encrypted. Detection of wormhole is quite difficult if used in conjunction with Sybil attack.

F. *HELLO flood Attacks*

Many protocols require nodes to broadcast HELLO packets to announce themselves as a neighbour, and the node receiving such packet may assume that it is within radio range of the sender. This assumption may be false because an attacker broadcasting routing or other information with large transmission power may convince every other node in network that adversary is its neighbour. Therefore a strong HELLO message will be broadcast by attacker and the network may be left in the state of confusion.

G. *Acknowledgement Spoofing Attacks*

Several sensor routing algorithm rely on link layer acknowledgement. An adversary can spoof link layer acknowledgements. Main goal is to convince the sender that a weak link is strong or a dead link is alive. An adversary can effectively establish a selective forwarding attack by using acknowledgement spoofing by encouraging the target node to transmit packets on poor link.

III. ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS

TABLE 1

PROTOCOL	RELEVANT ATTACKS
TinyOS beaconing	Bogus routing information, selective forwarding, sinkhole, Sybil, wormhole, HELLO floods
Directed diffusion and its multipath variant	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Geographic routing(GPSR,GEAR)	Bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, selective forwarding, sinkholes, wormholes, HELLO floods
Clustering based protocols (LEACH,TEEN, PEGASIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes
Energy conserving topology maintenance (SPAN, GAF, CEC, AFECA)	Bogus routing information, Sybil, HELLO floods

IV. COUNTERMEASURES

A. Outsider attacks and link layer security

A majority of outsider attacks against sensor network routing protocols can be prevented by simple link layer encryption and authentication by using a globally shared key. Major classes like, Wormhole attacks and hello floods attacks are not countered by link layer encryption and authentication mechanisms, because adversary is prevented from joining the networks nothing prevents her from using a wormhole to tunnel the packets.

In the presence of insider attacks or compromised nodes, link layer security mechanisms using a global shared key are completely ineffective.

Insider can attack network by:-

1) Spoofing (injecting bogus routing information),
2) Creating sinkholes
3) Selectively forwarding packets
4) Sybil attack
5) Broadcasting HELLO floods

B. The Sybil Attacks:-

By using a globally shared key an insider cannot be prevented from participating in the network. It allows insider to masquerade as any node. One solution for this is, use of unique symmetric key with a trusted base station for every node. Two nodes can then use a Needham Schroeder protocol to verify the identity of each other node. A pair of node can use resulting key to generate an authenticated and encrypted link between them. The base station can reasonably limit the neighbours a node can have and generate an error message when exceeds. Therefore a node is restricted to use any other node except their verified nodes. But an adversary can create a wormhole to convince them that they are neighbours but will not be able to eavesdrops on or modify any future communications.

C. HELLO Flood Attacks

To prevent a HELLO flood attacks is to verify the bidirectionality of link before sending any useful information. One possible solution to this attack is use of identity verification protocol using a trusted base station for every node to authenticate each of its neighbours. If the compromised node have a sensitive receiver and powerful transmitter then it does not prevent it from authenticating itself to a large number of nodes in network, an observant base station in network may be able to detect a HELLO flood is imminent. in such case adversary need to authenticate itself to every victim, and if adversary claims itself as a neighbour then it will raise an alarm.

D. Wormhole and Sinkhole Attacks

When wormhole attacks [3] and sinkhole attack is used in combination they are difficult to prevent. Because Wormhole use a private, out of band channel invisible to underlying sensor network and sinkhole are difficult to defend against

1) If it is used in protocols which use advertised information, because this information is hard to verify.
2) When route is established based on reception of packets as in TinyOs beaconing.

Best solution is carefully design routing protocol in which wormholes and sinkhole are meaningless.

E. Leveraging Global Knowledge

Securing large network means security of their inherent self-organising and decentralised nature. If network size is limited, topology is well structured or controlled, global knowledge can be leveraged in security mechanism. Topology change can be accounted; node can periodically update a base station with appropriate information. Drastic and suspicious changes can indicate a node compromise and appropriate action can be taken. In geographic routing information advertised from neighbouring nodes, must be trusted. A compromised can advertise itself in between a target and base station. A probabilistic selection of next hop can help this problem, but not a perfect solution. A node routes around a hole then adversary can help by representing itself only reasonable node to forward packets to. Therefore restricting the structure of topology eliminates requirements for node to advertise their location.

F. Selective Forwarding

A compromised node, located near to source or base station, then it has a high probability to include itself on a data flow to launch a selective forwarding attack. As a solution multipath routing can be used to counter these types of attacks. Message routed over path whose nodes are completely disjoint can offer same probabilistic protection when node is compromised. Use of multipath braided paths [4] may provide probabilistic protection against this. Allowing node to dynamically choose next hop from a set of possible candidates can reduce the chances of adversary gaining control.

G. *Authenticated Broadcast and Flooding*

If trustworthy base station is present then adversary cannot spoof or flooded messages. Authenticated broadcast is useful for local node interaction. Many protocols require broadcasting HELLO messages, these messages should be authenticated and impossible to spoof. These require some conventional setting either use

1) Digital signature
2) Have packets overhead that exceed the length of typical sensor network.
3) TESLA [9] a protocol that uses symmetric key cryptography used for authenticated broadcast flooding.
4) SPIN [10] and Gossiping algorithms [11], [12] techniques used to reduce messaging cost and collision, which use robust dissemination of messages.

V. CONCLUSIONS

Secure routing is vital to acceptance and used in sensor network for many applications. We demonstrated that currently used routing protocols for sensor networks are insecure. This is an open problem to design sensor network routing protocol that satisfies the proposed security goals. Link layer encryption and authentication may be a reasonable approximation for defenses against mote class outsiders, where cryptography alone is not sufficient. The possible presence of laptop-class adversaries and insiders and limited applicability of end to end security mechanisms necessitates the careful protocol design as well.

REFERENCES

[1] J.R.Douceur, the Sybil attack, in: 1st International workshop on Peer-to-Peer Systems (IPTPS' 02), 2002 [SD-008].
[2] J. Hill, R. Szewczyk, A Woo, S. Hollar, D. culler, K.Pister, System architecture directions for networked sensors, in: proceedings of ACM ASPLOS IX, 2000 [SD-008]
[3] Y-C. Hu, A Perrig, D.B. Johnson, Packet leashes: a defense against wormhole attack in wireless networks, in: IEEE Infocom, 2003 [SD-008]
[4] D Ganesan, R Govindan, S Shenker, D Estrin Highly-resilient, energy-efficient multipath routing in wireless sensor networks. Mobile computing and communications review, 4 (5) (2001), pp. 11-25 [SD-008]
[5] A Banerjea, taxonomy of dispersity routing schemes for fault tolerant real-time channels, in: proceedings of ECMAST, vol.26, 1996, pp.129-148 [SD-008]
[6] K.Ishida, Y. Kakuda, and T.Kikuno, A routing protocol for finding two node-disjoint paths in computer networks, in: International conference on Network Protocols, 1992, pp. 340-347 [SD-008]
[7] Y.Xu, J. Heidemann, D.Estrin, Geography-informed energy conservation for ad hoc routing, in; Proceedings of the Seventh Annual ACM/IEEE International conference on mobile computing and networking, 2001[Sd-008]
[8] B Chen, K Jamieson, H Balakrishnan, R Morris
Span: an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks
ACM wireless networks Journal, 8 (5) (2002), pp. 481-494 [Sd-008]
[9] A.perrig, R. Szewczyk, V.Wen, D.Culler, and J.Tygar, "SPINS: security protocols for sensor networks," in proceedings of mobile networking and computing 2001, 2001.
[10] J.Kulik, W.R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," wireless networks, vol. 8, no. 2-3, pp. 169-185, 2002.
[11] M.-J. Lin, K. Marzullo, and S. Masini, "Gossip versus deterministic flooding: low message overhead and high reliability for broadcasting on small networks, Tech. rep. CS 1990-0637, 18, and 1999.
[12] L. Li, J. Halpern, and Z. Haas, "Gossip- based ad hoc routing, "in IEEE Infocom 2002, 2002.

