Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

C. Karlof and D. Wagner

presentation by Maarit Hietalahti

Helsinki University of Technology

Laboratory for Theoretical Computer Science

`Maarit.Hietalahti@hut.fi`

T-79.194 Seminar on Theoretical Computer Science. 27.4.2005

Contents

Introduction

- Sensor networks are usually not designed with security in mind, yet security is difficult to add later on
- If adversaries can distrupt or interfere with routing, sensor network becomes grippled or useless
- Resource limitations are a two or three orders of magnitude worse than in ad hoc networks
- => Sensor network security is a difficult challenge

Background and Related work

- Computational power: public key cryptography is too expensive
- Memory: Nodes cannot maintain much state
- Radio transmission costly => message expansion costly
- Moore's law not likely to help: nodes are preferred to get cheaper instead of adding performance
- Most related work requires capabilities beyond those of a sensor network, except SPEN and μ TESLA [1]

Problem statement

Goal: "Every eligible receiver should receive all messages intended for it and be able to verify the integrity of every message as well as the identity of the sender"

1. Attackers can eavesdrop, inject bits, replay packets
2. Attackers can use many colluding nodes and nodes can be more powerful than normal sensor nodes
3. Ordinary nodes are not tamper resistant
4. Base stations are assumed trustworthy, ordinary nodes and aggregation opints are not
5. Laptop attackers vs. mote class attackers
6. Insider attacks: graceful degradation
7. Secure routing does not include confidentiality and protection against replay attacks.

Attacks on sensor networks routing

Spoofed, altered, or replayed routing information An unprotected sensor routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing information.

Selective forwarding A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node. The attack can be used to make a denial of service attack targeted to a particular node. If all packets are dropped, the attack is called a “black hole”.

Sinkhole attack In a sinkhole attack, a malicious node uses the faults in a routing protocol to attract much traffic from a particular area, thus creating a sinkhole.

Attacks on sensor networks routing, continued

Sybil attack The Sybil attack [2] is targeted to undermine the distributed solutions that rely on multiple nodes' cooperation or multiple routes. In a Sybil attack, the malicious node gathers several identities for posing as a group of many nodes instead of a one.

Wormhole attack The wormhole attack [3] usually needs two malicious nodes. The idea is to distort routing with the use of a low-latency out-of-bound channel to another part of the network where messages are replayed.

HELLO flood attack Amalicious node can send, record or replay HELLO-messages with high transmission power. It creates an illusion of being a neighbor to many nodes in the networks

Acknowledgement spoofing If a protocol uses link-layer acknowledgements, these acknowledgements can be forged, so that other nodes believe a weak link to be strong or disabled nodes alive.

Attacks on specific sensor protocols

- TinyOS beaconing: any node can claim to be a base station
- If routing updates are authenticated a laptop attacker can still do a wormhole/sinkhole attack: See pictures 4-6.
- Laptop attacker can also use a HELLO flood attack to the whole network: all nodes mark it as its parent, but their radio range will not reach it
- Mote-class attackers can create routing loops

Directed Diffusion

Goals:

- Suppression: Denial of service attack by spoofing negative reinforcements
- Cloning: Replaying an interest from a base station with the attacker listed as a base station
- Path influence: Using spoofed positive and negative reinforcements and bogus data events

Example: Strong reinforcement of nodes downstream and sending spoofed high rate low latency events upstream. Results:

- legitimate events will be drawn through attacker
- alternate event flows will be negatively reinforced
- attacker will be positively reinforced
- attacker gains full control of the flow and can lauch a selective forwarding attack and modify packets

Example: Other examples

Directed diffusion: other examples: Laptop attacker can create a wormhole and manipulate the data flows to it. Multipath version of directed diffusion can be dealt with the Sybil attack.

- LEACH: manipulating the clustering
- Rumor routing: manipulating agents
- SPAN: preventing the nodes from becoming coordinators

Countermeasures

- Link layer encryption and authentication with a common symmetric key prevents most outsider attacks: adversary cannot join the topology
- Replay attacks are prevented by using a counter
- Attacker can still forward packets without altering them:
- Encryption can make selective forwarding difficult but does nothing to a black hole attack

Countermeasures, continued

- Insider cannot be prevented to participate in the operations of the network
- Insider can masquarade as any node:
- => identities should be verified, but public keys cannot be used
- Solution: nodes share own unique symmetric keys with the base station.
- Limiting the number of neighbors per node: attacker can not form symmetric keys with every node
- HELLO flood: verify the bidirectionality of the link
- Wormhole attacks: geographic routing helps but brings another problem: trust in the location information
- Wormhole attacks may not be prevented but they are not so useful anymore
- Additional solution: Restricting the structure of the topology

Conclusion

- Two new attacks presented (sinkhole and HELLO flood)
- Security analysis of 10 routing protocols and 4 energy conserving topology maintenance algorithms => attacks against all of them
- Countermeasures for almost all
- Cryptography is not enough
- link layer encryption and authentication are only a “first approximation” of a solution
- Open problem: a sensor network protocol that achieves all goals

References

[1] A. Perrig, R. Szewczyk, Victor Wen, D. Culler, and J. D. Tygar. SPINS: Security protocols for sensor networks. In *Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MobiCom 2001*, July 2001.

[2] J. Douceur. The sybil attack. In *Proceedings of the IPTPS 2002*, Cambridge, MA, USA, March 2002.

[3] Yih-Chun Hu, A. Perrig, and D. B. Johnson. Wormhole detection in wireless ad hoc networks. Technical report, Department of Computer Science, Rice University, December 2001. Technical Report TR01–384.