Summary of "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures" *C. Karlof and D. Wagner [1]*

Maarit.Hietalahti@hut.fi

April 27, 2005

T-79.194 Seminar on Theoretical Computer Science. 27.4.2005

1 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, which means that ensor network security is a difficult challenge.

2 Background and Related work

Computational power in sensor networks is small, public key cryptography is too expensive. Memory is limited, nodes cannot maintain much state. Radio transmission is costly which means that message expansion is costly too. Moore's law is not likely to help: nodes are preferred to get cheaper instead of adding performance. Most solutions in related work require capabilities beyond those of a sensor network, except SPEN and μTESLA [2]

3 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"

What an attacker can do? Wireless radio links are insecure. Attackers can eavesdrop, inject bits and replay packets. Attackers can use many colluding nodes and nodes can be more powerful than normal sensor nodes. Ordinary nodes are not tamper resistant. Base stations are assumed trustworthy but ordinary nodes and aggregation points are not. Attackers were divided to two categories: Laptop attackers vs. mote class attackers. With insider attacks only a graceful degradation can be expected, i.e. the damage caused is proportional to the number of nodes compromised.

Secure routing does not include confidentiality and protection against replay attacks, as they can be better prevented on application layer.

4 Attacks on sensor networks routing

Spoofed, altered, or replayed routing information An unprotected ad hoc 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, such as the sinkhole attack or acknowledgement spoofing. 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.

Sybil attack The Sybil attack [3] 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. This attack is not relevant as a routing attack only, it can be used against any cryptoschemes that divide the trust between multiple parties. For example, to break a threshold crypto scheme one needs several shares of the shared secret.

Wormhole attack The wormhole attack [4] 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. These can be used, for example, to create sinkholes and to exploit race conditions.

HELLO flood attack In a HELLO flood attack a malicious 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 and can confuse the network routing badly.

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.

5 Attacks on specific sensor protocols

In 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: 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 also create routing loops.

6 Directed Diffusion [5]

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 The attacker strongly reinforces downstream nodes and sends spoofed high rate low latency events upstream. This results that legitimate events will be drawn through attacker. Alternate event flows will be negatively reinforced, but the attacker will bepositively reinforced. Attacker also gains full control of the flow and can lauch a selective forwarding attack and modify packets.

Other examples also presented including a laptop attacker that can create a wormhole and manipulate the data flows to it. A multipath version of directed diffusion is suggested as a partial solution for dealing with the Sybil attack. Other attacks were presented: manipulating the clustering in LEACH [6], manipulating agents in Rumor routing [7], in SPAN [8], preventing the nodes from becoming coordinators.

7 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 an increasing counter, as usual. However, an attacker can still forward packets without altering them. Encryption can make selective forwarding difficult but does nothing to a black hole attack.

Insider cannot be prevented to participate in the operations of the network and she can masquarade as any node: This means that identities should be verified, but public keys cannot be used as was seen before. A solution: nodes share own unique symmetric keys with the base station. Another one presented was limiting the number of neighbors per node: attacker can not form symmetric keys with too many nodes in the network. The HELLO flood attack prevention can be done by verifying the bidirectionality of the link. With wormhole attacks, geographic routing helps but brings another problem: should you trust the advertised location information? Wormhole attacks may not be prevented but the routing protocols should be made so that the wormholes are not harmful anymore. Additional solution for the wormhole attack is restricting the structure of the topology.

8 Conclusion

Two new attacks presented (sinkhole and HELLO flood) and a security analysis of 10 routing protocols and 4 energy conserving topology maintenance algorithms revealed attacks against all of them. Countermeasures were presented for almost all attacks. It was seen that cryptography is not enough, link layer encryption and authentication are only a “first approximation” of a solution. As an open problem remains a sensor network protocol that achieves all goals.

References

[1] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier’s AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 1(2–3):293–315, September 2003.

[2] 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.

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

[4] Y.-C. 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.

[5] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva. Directed diffusion for wireless sensor networking. *IEEE/ACM Trans. Netw*, 11(1):2–16, 2003.

[6] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, volume 2, page 10, January 2000.

[7] D. Braginsky and D. Estrin. Rumor routing algorithm for sensor networks. In *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications WSNA’02*, pages 22–31, Atlanta, Georgia, USA, 2002. ACM Press.

[8] Hari Balakrishnan Robert Morris Benjie Chen, Kyle Jamieson. Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. *Wireless Networks*, 8:481 – 494, Sep 2002.