Contemporary Engineering Sciences, Vol. 7, 2014, no. 15, 737 - 742
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2014.4683

A Security Architecture for

Wireless Sensor Networks Environmental

Bijoy Kumar Mandal

Computer Science and Engineering Department,
NSHM Knowledge Campus – Durgapur, Durgapur-713212, India

Debnath Bhattacharyya

Computer Science and Engineering Department,
Vignan University, Vadlamudi-522213, Guntur, AP, India

Kil-hwan Shin

Department of business IT,
Kookmin University, Seoul, Korea
(Corresponding author)

Abstract

The Wireless Sensors Network (WSN) is an emergent technology resulting from progress of various fields. Many applications of networks WSN are developed. In the last years, wireless sensor networks (WSNs) have gained increasing attention from both the research community and actual users. As sensor nodes are generally battery-powered devices, the critical aspects to face concern how to reduce the energy consumption of nodes, so that the network lifetime can be extended to reasonable times. As sensor networks are deployed in adversarial environments and used for critical applications. In this paper, we consider routing security in wireless sensor networks. Many sensor network routing protocols have been proposed, but very less of them have been designed

with security as a goal. We propose security goals for routing in sensor networks. We describe crippling attacks against all of them and suggest countermeasures and design considerations.

Keywords: WSN, IGF, RFID, CTS, ORT

1 Introduction

A wireless sensor network consists of sensor nodes deployed over a geographical area for monitoring physical phenomena like temperature, humidity, vibrations, seismic events, and so on [1]. Our focus is on routing security in wireless sensor networks. Current proposals for routing protocols in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security.

We present crippling attacks against all the major routing protocols for sensor networks. Because these protocols have not been designed with security as a goal, it is unsurprising they are all insecure. We make five main contributions.

- We propose threat models and security goals for secure routing in wireless sensor networks.
- We introduce two novel classes of previously undocumented attacks against sensor networks– sinkhole attacks and HELLO floods.
- We show, for the first time, how attacks against ad-hoc wireless networks and peer-to-peer networks [2] can be adapted into powerful attacks against sensor networks.
- We present the first detailed security analysis of all the major routing protocols and energy conserving topology maintenance algorithms for sensor networks. We describe practical attacks against all of them that would defeat any reasonable security goals.
- We discuss countermeasures and design considerations for secure routing protocols in sensor networks.

2 Background

In some previous work on sensor network routing protocols, base stations have also been referred to as sinks. Base stations are typically many orders of magnitude more powerful than sensor nodes. They might have workstation or laptop class processors, memory, and storage, AC power, and high bandwidth links for communication amongst themselves. However, sensors are constrained to use lower-power, lower bandwidth, shorter range radios. We refer to such a stream as a data flow and to the nodes sending the data as sources.

With only 4 KB of RAM, memory is a resource that must be husbanded carefully, so our security protocols cannot maintain much state. Also, communication bandwidth is extremely dear: each bit transmitted consumes about as much power as executing 800– 1000 instructions [3], and as a consequence, any message expansion caused by security mechanisms comes at significant cost.

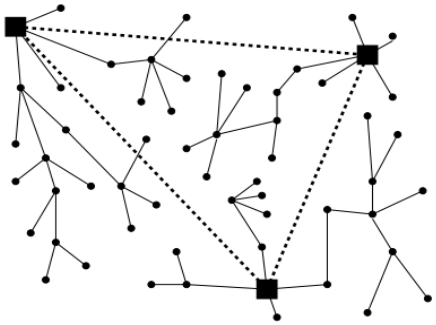

Figure 1. Sensor network architecture to communicate nearest base station

3 Assumptions and attacks

3.1 System assumptions

We assume that radio links are insecure, i.e., attackers may eavesdrop on radio transmissions, inject messages, and record and later replay messages. If an attacker is able to interact with the routing protocol, it can also drop messages for which it is responsible. Attackers possess hardware capabilities similar to that of legitimate nodes, and wireless transmissions use the same power levels. Network nodes move only infrequently or slowly once deployed, and know their own locations. They may additionally know that of their neighbors. This may be fulfilled by many different key distribution schemes in the literature [4]. Nodes trust their own clocks, measurements, and storage.

3.2 Routing attacks

Karlof and Wagner [5] have systematically studied attacks on routing protocols. We summarize these attacks below, noting whether they are applicable. Then we discuss those attacks which are not obviously thwarted in greater detail. In an insider attack, a compromised node uses any means available to legitimate nodes to disrupt the protocol or perform a specific attack listed above.

4 Attacks on sensor network

Many sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to attacks against general ad-hoc routing protocols. The main attacks available to an adversary are to create a black hole, pose as multiple identities (Sybil attack), or disrupt the routing protocol through denial of service attacks.

4.1. Black Hole / Selective Forwarding Attack

In the CTS rushing attack, an attacker exploits the cooperative nature of next-hop selection. When an Open RTS (ORTS) message is received, neighbors set timers proportional to their desirability as forwarding candidates. When attacker A overhears an ORTS message, it sends a CTS message, whether it is in the forwarding area or not. Other nodes overhear the CTS from the attacker and abort the protocol. Unsuspecting ORTS senders in the neighborhood of the attacker always choose to send their messages into the black hole created by A as shown in Figure 2.

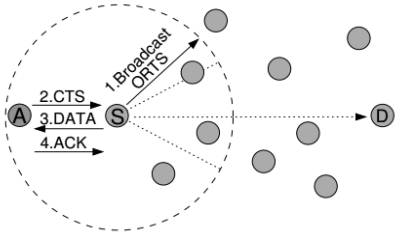

Figure 2. CTS Rushing Attack by A against S

4.2. Sybil Attack

In a Sybil attack, an attacker illegitimately claims to be multiple nodes by sending messages with different identities and locations. Its additional identities are virtual Sybil nodes.

- Identity and Location: A Sybil node can either fabricate a new identity or steal an identity from a legitimate node [6].
- Communication: We assume Sybil nodes can communicate directly with legitimate nodes in the following way.

4.3. Denial of Service Attack

The goal of this type of attack is to deny service to the nearby nodes in a manner that is less intrusive and costly than jamming. The attacker partially executes the IGF protocol to cause nearby nodes to waste energy transmitting messages, waste time waiting on completion of the protocol, or prematurely abort the protocol.

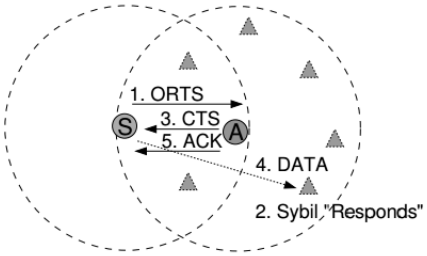

Figure 3. Node A performs a Sybil attack against S

4.4. Secure routing protocol

We propose a novel secure routing protocol family, called Secure Routing Protocol which keeps the advantages of dynamic binding in IGF, yet provides effective defenses against the attacks discussed above. The protocols provide tradeoffs between security and state maintenance, and configurability that can be adapted at runtime as shown in Table 1.

Table 1. Algorithm of next-hop selection for message from current node S to ultimate destination D

```
1  if (include destination)
2    ORTS ← ⟨S, S_location, D, D_location, FwdArea⟩
3  else
4    ORTS ← ⟨S⟩

6  broadcast ORTS message

8  /* Every neighbor N receives ORTS message, and if
        in FwdArea, sets CTS response timer
        proportional to next−hop desirability, sending
        CTS = ⟨N, N_location⟩ upon expiry. */

10 CTS_candidates ← ∅
11 while (collection window open)
12   if (CTS received AND N_location ∈ FwdArea)
13     add N to CTS_candidates

15 choose C ∈ CTS_candidates for next hop
16 send DATA to C
```

5 Conclusion

Secure routing is vital to the acceptance and use of sensor networks for many applications. We have presented a secure routing protocol family for wireless sensor networks that builds atop the inherently attack-containing, dynamic binding. Rather than maintain routing tables, it chooses the next hop dynamically and none deterministically. This contains the effect of compromise to a local neighborhood, increases robustness to node mobility and failure, and spreads energy drain more evenly across neighbors. We leave it as an open problem to design a sensor network routing protocol that satisfies our proposed security goals.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, Wireless Sensor Networks: a Survey, *Computer Networks*, Vol.38, N. 4,(2002).

[2] Y.C. Hu, A. Perrig, and D. B. Johnson, Wormhole detection in wireless ad hoc networks, Department of Computer Science, Rice University, (2002), 1 – 384.

[3] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, System architecture directions for networked sensors, *in Proceedings of ACM ASPLOS IX* (2000).

[4] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A secure routing protocol for ad hoc networks, *In Proceedings of the IEEE International Conference on Network Protocols(ICNP),* (2002).

[5] C. Karlof and D. Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures, *In First IEEE International Workshop on Sensor Network Protocols and Applications*(2003), 1-15.

[6] Y. Xu, J. Heidemann, and D. Estrin, Energy conservation by adaptive clustering for ad-hoc networks, in Poster Session of MobiHoc ,(2002).

Received: May 1, 2014