Computers and Electrical Engineering 41 (2015) 115–125

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

An experimental study of attacks on the availability of Glossy ☆

Kasun Hewage [a], Shahid Raza [b,*], Thiemo Voigt [a,b]

[a] Department of Information Technology, Uppsala University, Sweden
[b] SICS Swedish ICT, Isafjordsgatan 22, Stockholm, Sweden

ARTICLE INFO

Article history:
Received 21 November 2013
Received in revised form 3 October 2014
Accepted 7 October 2014
Available online 15 November 2014

Keywords:
Glossy
Security attacks
Sensor networks
Network security
Distributed communication

ABSTRACT

Glossy is a reliable and low latency flooding mechanism designed primarily for distributed communication in wireless sensor networks (WSN). Glossy achieves its superior performance over tree-based wireless sensor networks by exploiting identical concurrent transmissions. WSNs are subject to wireless attacks aimed to disrupt the legitimate network operations. Real-world deployments require security and the current Glossy implementation has no built-in security mechanisms. In this paper, we explore the effectiveness of several attacks that attempt to break constructive interference in Glossy. Our results show that Glossy is quite robust to approaches where attackers do not respect the timing constraints necessary to create constructive interference. Changing the packet content, however, has a severe effect on the packet reception rate that is even more detrimental than other physical layer denial-of-service attacks such as jamming. We also discuss potential countermeasures to address these security threats and vulnerabilities.

1. Introduction

The emergence of the Internet of Things (IoT) has increased the demand on distributed, embedded low power applications as it requires more complex communication patterns than the tree-based many-to-sink communication paradigm that is predominant in conventional wireless sensor networks (WSNs). A recent protocol targeting this domain is Glossy [1], a highly reliable, low latency network flooding mechanism that offers in-built network-wide time synchronization within a microsecond accuracy. The Low-power Wireless Bus (LWB) [2], built on top of Glossy, provides a shared communication bus like infrastructure with a flat network hierarchy. Together, these protocols provide a performance that has not been achieved by tree-based protocols. Furthermore, the LWB supports the diverse IoT communication patterns under a simple single layer communication solution. Network-wide flooding enables the support of one-to-many, many-to-one, and many-to-many communication patterns.

Real-world deployment of WSNs, and hence Glossy, require security as WSNs are often deployed in unattended environments and wireless packets are easy to intercept. Furthermore, WSNs are connected through lossy wireless links and require multi-hop communication. This makes WSNs vulnerable to network eavesdropping and message modification as well as attacks seeking to disrupt network operations.

Glossy has not been designed as a secure protocol. It is therefore worth investigating the potential threats and vulnerabilities of Glossy. The core features of Glossy are the generation of constructive interference [1] and the capture effect [3].

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Felix Gomez.

* Corresponding author.
E-mail addresses: kasun.hewage@it.uu.se (K. Hewage), shahid@sics.se (S. Raza), thiemo@sics.se (T. Voigt).

http://dx.doi.org/10.1016/j.compeleceng.2014.10.004
0045-7906/

Constructive interference occurs when a receiver is able to detect and successfully decode a packet even when packets are generated by multiple transmitters at the same time. A pre-condition is that the transmitters send identical packets. The capture effect is a phenomenon that enables the reception of a packet with relatively high signal strength despite other packets being transmitted almost simultaneously [3]. However, its efficiency decreases when the number of concurrent transmissions increases [4].

As Glossy is one of the first protocols to rely on constructive interference, we propose novel attacks on constructive interference and investigate their effectiveness. Towards this end, we present three novel attacks. The attacks try to break constructive interference by (i) delaying the transmission of packets, (ii) sending packets earlier and (iii) modifying packets so the receiver does no longer receive identical packets which is a precondition for constructive interference.

To evaluate the effectiveness of the attacks, we perform experiments in FlockLab [5], a 30-node testbed that was also used for the original Glossy evaluation. Our results show that the first two attacks are not very effective. The capture effect and low variation of the clock skew under these attacks cause nodes to stay sufficiently synchronized to Glossy phases and enable them to turn on their radios when at least one packet transmission is in progress. Hence, nodes are able to receive packets even though an attack is ongoing. Modifying the packet is more effective, in particular when the attacker tampers the *relay counter* used for time synchronization.

After evaluating the effectiveness of the attacks, we discuss ways of securing Glossy against these and other attacks as Glossy has no built-in security mechanisms. It is important to protect Glossy packets against unauthorized modifications by employing message security services, in addition to intrusion detection systems that guard against security attacks aimed to disrupt networks.

The main contributions of this paper are:

- We present novel attacks that aim to break constructive interference, the underlying mechanism of the Glossy protocol.
- We evaluate the effectiveness of the attacks in a testbed. Our results show that tampering the relay counter to break time synchronization is the most effective attack while Glossy internals make it surprisingly robust against the other attacks. We also demonstrate that tampering the relay counter is more effective than physical layer denial-of-service attacks such as jamming.
- We discuss potential security solutions to protect Glossy-based networks.

The rest of the paper is organized as follows. First, we provide background information about IEEE 802.15.4, capture effect, constructive interference, and Glossy in Section 2. In Section 3, we describe three methods for attacking Glossy. The experiments and their results are presented in Section 4. In Section 5, we discuss security services for Glossy-based networks. Finally, we review related work in Section 6 and conclude in Section 7.

2. Background

2.1. IEEE 802.15.4 physical layer for 2.4 GHz band

IEEE 802.15.4 radios operating in the 2.4 GHz band make use of the Direct-Sequence Spread Spectrum (DSSS) modulation technique with Offset-Quadrature Phase-Shift Keying. Each byte of the data is split into 4-bit segments and mapped to one of 16 symbols in which each symbol is composed of a sequence of 32 chips. The chips are transmitted at 2 MChips/s corresponding to a maximum data rate of 250 kb/s.

The format of a physical layer (PHY) frame of IEEE 802.15.4 is shown in Fig. 1. The preamble is defined to be 4 bytes of 0×00 and the Start of Frame Delimiter (SFD) is one byte set to $0 \times A7$. The frame length is a 7-bit field limiting the length of the maximum PHY payload to 127 bytes.

2.2. Capture effect & constructive interference

The *capture effect* [3] is the phenomenon associated with packet reception in which the radio is able to receive a packet from one sender despite simultaneous transmissions from other transmitters. Suppose, two packets A and B from two transmitters in which the strength of packet A is higher than that of packet B at the receiver. Assume that packet A arrives at the receiver earlier than packet B as shown in Fig. 2(a). The reception of packet A is interfered due to the overlap of packet B. As the radio is busy with the reception of packet A, packet B could be considered as noise. If the signal to noise ratio (SNR) of

Fig. 1. IEEE 802.15.4 physical layer frame structure.