Some Security Considerations over Contiki-based Sensor Network

Yan Yan

December 8, 2015

Contents

Chapter 1

Introduction

This paper discusses two security measurements, namely Link Layer Security (LLSEC) and Datagram TLS (DTLS), within Contiki OS.

1.1 Related Work

[1] discusses some security concerns in 802.15.4. LLSEC[2] is the implementation of 802.15.4 security in Contiki.

tinydtls[3] is the implementation of DTLS we used in DTLS related experiments.

1.2 Experiment Setup

All experiments are done within the Cooja simulator.

The setup is as described in Figure 1.1.

- **Adversary** is the malicious party that tries to recover information from the encrypted traffic.
- **Border Router**, or BR, is a device that connects the adversary to the sensor network. However, **BR is not allowed when LLSEC is enabled** as the adversary does not have the key and hence cannot connect into the network.
- **Sniffer** is a device that passively captures all traffics in the sensor network.
- **Target** and **Nodes** are sensors deployed in the sensor network. They communicates to each other through encrypted channels.
- **Sensor Network** discussed in this paper is a 6LowPAN network.

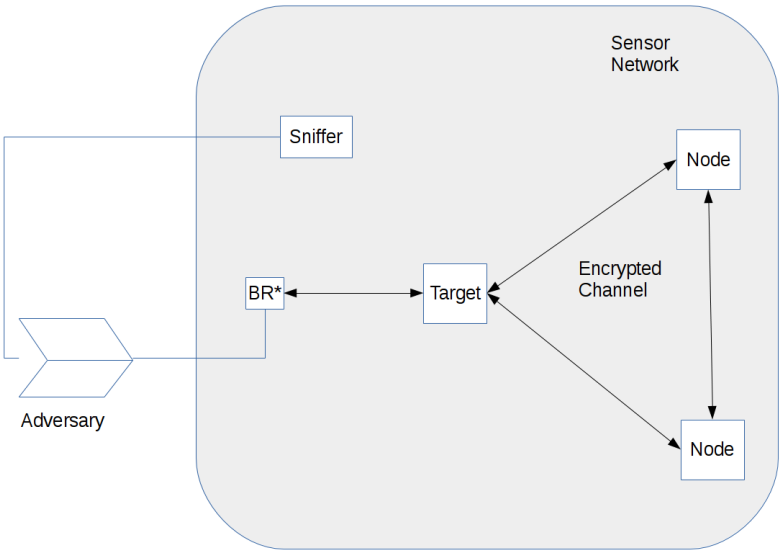

Figure 1.1: Experiment setup

1.3 Adversary Power

The powers assumed in the experiments are considered to be practical in real life.

When LLSEC is enabled, all traffic, including RPL[1] messages, are encrypted; therefore no external nodes can connect to the network. The only power for the adversary is to passively sniff all the traffic.

In other cases where LLSEC is disabled, the adversary will be enabled to join the sensor network through a BR and hence is also capable to send ICMP messages to the target(s).

[1]Routing Procol for Low-power and Lossy Networks

Chapter 2

Link Layer Security

Link Layer Security, or LLSEC, is a security measure that implements cryptography just above the physical layer.

Introducing cryptography at a lower level has several benefits. Firstly, more data being encrypted reduces the observable packet features to an adversary, such as SRC[1] and DST[2] field in the IP header which are very likely to be exploited by the adversary. Secondly, authentication at lower level also prevents an active adversary from joining the network which therefore weakens his power.

Imposing cryptography at a lower level also brings more challenge to the design of sensor network architecture. The first problem is its overhead. Even for a node that only tries to retransmits the packet to its next hop, it must decrypt the whole packet to extract its routing information, and then re-encrypt it before retransmission. This is particularly problematic in a mesh wireless sensor network as it could potentially lead to performance and energy consumption problems. Key management is also challenging due to the lossy and power optimised nature of wireless sensor network.

It is also noticeable that some packet features are not hidden even with LLSEC enabled, such as packet length, timing information and part of the MAC header.

[1]Source Address

[2]Destination Address

2.1 Non core security

2.2 802.15.4 security

2.3 Reset Problem

2.3.1 Initial Vector

2.4 Distinctive packet length for RPL packets

Chapter 3

DTLS

3.1 Conflicting MTU between DTLS and 6lowPAN

The abandoned CoDTLS.

3.2 Overloading DTLS with LLSEC

Chapter 4

Application Detection

4.1 Packet Length

4.2 Response Time

4.3 Pingload: Ping side-channel for Payload

Bibliography

[1] Naveen Sastry and David Wagner. "Security Considerations for IEEE 802.15.4 Networks". In: *Proceedings of the 3rd ACM Workshop on Wireless Security*. WiSe '04. Philadelphia, PA, USA: ACM, 2004, pp. 32–42. ISBN: 1-58113-925-X. DOI: 10.1145/1023646.1023654. URL: http://doi.acm.org/10.1145/1023646.1023654.

[2] URL: https://github.com/kkrentz/contiki/wiki.

[3] URL: http://sourceforge.net/projects/tinydtls/.