Some Security Considerations over Contiki-based Sensor Network

Yan Yan

December 7, 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[**tinydtls**] is the implementation of DTLS we used in the experiments.

1.2 Experiment Setup

All experiments are done within the Cooja simulator.

Chapter 2

Link Layer Security

2.1 Non core security

2.2 802.15.4 security

2.3 Reset Problem

2.4 Distinctive packet length for RPL packets

Chapter 3

DTLS

3.1 Conflicting MTU between DTLS and 6lowPAN

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.