Cryptographic key management architecture for dynamic 6LowPan networks

Ruben Smeets[a], Kris Aerts[a], Nele Mentens[a], Dave Singelee[a], An Braeken[b], Laurent Segers[b], Abdellah Touhafi[b], Kris Steenhaut[b], Niccolo De Caro[b]

[a]KU Leuven@KHLim
Firstname.Lastname@Kuleuven.be

[b]Vrije Universiteit Brussel(VUB)
FirstnameLastname@vub.ac.be

Abstract

Wireless sensors are an important facilitator for the Internet of Things. These embedded devices can harvest different types of information such as temperature, pressure and humidity, which offer important data for making decisions regarding various applications such as healthcare, logistics and smart homes. Different sensors working together act as a local sensor network. With the advent of the new 6LowPan standard the sensor nodes can even participate in Internet communications, opening up even more possibilities.

The counter-side is that these networks are more prone to intrusion by unwanted parties. Furthermore implementing security is not straightforward due to the constraint nature of the sensor nodes, although different solutions have been proposed. One of the remaining and most challenging issues is the key management problem. Symmetric key management is generally considered the best suited for wireless sensor networks, but none of the proposed solutions so far cover every scenario.

In this paper, we propose a symmetric key management scheme for wireless sensor networks that uses tamper-proof hardware for key generation and distribution. The scheme requires no deployment knowledge before enrolling and makes use of a trusted central entity for key negotiation to provide end-to-end security. Our implementation and evaluation were performed on the tiny Zolertia Z1 hardware platform, running Contiki. The performance and security evaluation show that our scheme requires a limited amount of storage and provides a good network resilience against node capture.

Keywords: 6LowPan, Wireless Sensor Network Security, Symmetric Key Management, Link-Layer Security, End-to-End Security

MSC: 68-00, 68-01, 94-02, 94A60, 94A62