Secure Wireless Link for Ultra-low Power Wireless Sensor Networks

C. Kassapoglou Faist

CSEM provides solutions for secure communication in wireless sensor networks, addressing data protection (authentication, encryption, freshness, and confidentiality), entity authentication and key management. Implementations can be tailored to the needs of the application, to support various standards (IEEE 805.15.4 and 805.15.6, Bluetooth LE) and to run on a variety of embedded platforms.

As ultra-low power (ULP) smart wireless devices are becoming ubiquitous, the security of wireless communication links becomes vital. However, the wireless medium is open to anyone – or anything, making it easy to overhear and interfere with, thus requiring protective measures. In order to provide our customers with secure solutions, CSEM has been active in acquiring state-of-the-art know-how in wireless communication security for resource constrained devices and developing approaches to design adequate solutions, in particular in terms of key management. The solutions are tailored to the requirements of the application and cover the entire system lifecycle (installation, commissioning, replacement, etc.). The implementations run on various ULP embedded platforms and cover a variety of application domains ranging from environmental monitoring to safety in transportation.

The security services provided are: unilateral or mutual entity authentication for protection against man-in-the-middle (MITM) attacks; data authentication and integrity; confidentiality through end-to-end data encryption for privacy; data freshness, for protection against replay of old valid messages; access control and authorization. Most of these services rely on cryptography. As an example, Figure 1 shows CSEM's WiseMAC communication stack integrating security.

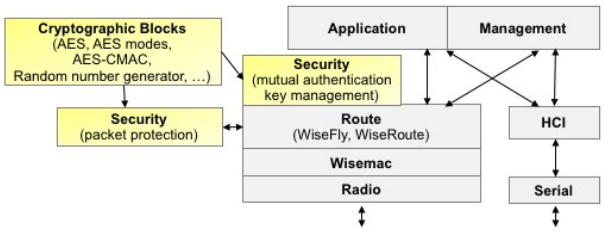

Figure 1: Security in WiseStack.

Due to limited resources (memory, computing power, energy consumption), the implementation of cryptography is based on symmetric cryptographic ciphers, which are less resource demanding. Specifically, we use the AES encryption algorithm (e.g. AES-128), which is a strong algorithm, with integrated hardware implementations available on a few platforms. AES is used for encryption (AES-CTR) and message authentication (AES-CBC) as well as in keyed hash functions involved in entity authentication and key agreement protocols (AES-CMAC), and in the incorporated strong random number generator [1].

The use of symmetric algorithms makes key establishment more complex and requires some form of initial trust. Using a network-wide key for all links in the network is not recommended, because of the lack of robustness in the event that a node is compromised. Instead, each node shares its own secret keys with the sink: a master key that is used exclusively to derive session keys and the current time-limited session key used to protect the data. No other node is able to derive these keys. The session key is established using the master key and random data that the two parties exchange at session establishment, following a mutual authentication protocol. This approach may seem complex, but it is the best way to prevent key compromise: the master key is not exposed to attacks. Moreover, it provides a mechanism for session key refresh.

Distribution and management of the master keys depends on trust assumptions and configuration set-up. The difficulty is to install each master key on both the device and the sink (or base station) without a third party intercepting it. A simple solution is to have it installed on the node at the time of manufacturing and load it onto the sink manually. If the network set-up takes place in a controlled environment, the master key can be sent to the node by the sink over the air during an initialization phase where attacks are considered improbable. However, there are advantages in using a scheme where key distribution involves an operator device enabled with wired or close-range communication (serial, NFC): an out-of-band channel is available to load the key and proximity provides a guarantee on node identity. The operator device can either generate a master key for each node-sink pair (and later discard it) or read it on one device and copy it to the other. In case that the operator device is not trusted, the master key can be computed on each device based on a network-wide pre-programmed key (unknown to the operator) and on secret data loaded by the operator. As an alternative, a key transfer scheme can also be used: the two devices establish a temporary key during an authenticated pairing procedure - where, for example, they use the operator device to uniquely identify each other - and then have the master key transferred from one to the other, encrypted with the temporary key.

In addition to pairwise keys and in order to authenticate its broadcast messages, the sink can generate a group key and send it to each node individually, encrypted with the corresponding session key. Moreover, a mechanism allowing a node to establish pairwise keys with its neighbors in order to authenticate routing messages can also be provided.

CSEM has integrated security in small- and medium-size wireless sensor networks, in star or mesh topology. Platforms include a MSP430-CC1101 (AES hardware implementation), a MSP430-CC1125, as well as the in-house icyCOM SoC. Future work consists of proposing a Diffie-Hellman exchange based on elliptic curve cryptography, enabling the derivation of a secret key (the master key) over an authenticated channel without requiring a prior shared secret (but being more demanding on memory and computation resources).

[1] FIPS PUB 140-2, "Security requirements for cryptographic modules", (2001).