The link key security in wireless sensor networks

Dissertation thesis abstract

Petr Švenda

This dissertation thesis targets the area of wireless sensor networks (WSNs), in particular their security of link key establishment. We focus on how link keys can be established in memory and computation restricted environment of WSNs, how link security behaves under a selected attack, and what methods can be used to strengthen their resilience against compromise. We based our work on the assumption that partial compromise in the WSNs is inevitable and network architecture should be prepared to cope with related security issues. We work with two basic link key establishment concepts based on symmetric cryptography -- memory efficient probabilistic pre-distributions and lightweight key exchange without pre-distributed secrets. Both key distribution concepts behave differently when the network is attacked. We study resulting compromised patterns and propose two separate mechanisms based on support from neighbouring nodes for improving the network resiliency – one for the probabilistic pre-distribution and second for both of them.

The first mechanism uses group support for authenticated key exchange to substantially increase the resilience of an underlying probabilistic key pre-distribution scheme against the threat of node capturing. The resiliency of probabilistic pre-distribution schemes generally increases if more keys can be put into key ring on every single node, but such an increase is limited by the node storage capacity. The proposed protocol creates a large virtual key ring in an efficient and secure way from the key rings of separate nodes. The proposed protocol itself is resilient against partial compromise inside a group of neighbours.

The second proposed mechanism improves the fraction of secure links after compromise of some links due to attacker eavesdropping when key exchange between neighbours is made in plaintext (Key Infection approach). Our proposed mechanism from the family of secrecy amplification protocols exploits the non-uniformity of link compromise patterns in Key Infection and provides a significantly better fraction of secure links than previously published protocols, especially for denser networks. We additionally provide detailed evaluation of existing secrecy amplification protocols with respect to network density, repeated iterations, composition of protocols and different quantities of attacker eavesdropping nodes on our network simulator – previous works dedicated little attention to these aspects.

We later realized that the secrecy amplification protocols can also be used to improve the fraction of secure links and strengthen node capture resilience for probabilistic pre-distribution. It works even better here than for the Key Infection approach for which the secrecy amplification protocols were originally proposed for. A network with half of its links compromised can be made reasonable secure with less than 10\% of compromised links when the secrecy amplification protocols are applied. However, some combinations

of secrecy amplification protocols that worked for Key Infection do not work for probabilistic pre-distribution (do not increase number of secure links) and thus only impose unnecessary communication overhead. Instead of analyzing each separate compromise pattern arising from the combination of a particular key distribution method and attacker strategy, we proposed an automated approach based on the combination of a protocol generator and network simulator.

We utilize evolutionary algorithms to facilitate guided search for well-performing secrecy amplification protocol created as a series of elementary instructions. Every candidate protocol is evaluated on our network simulator for a particular compromise pattern. The protocols with a better fraction of secure links are used as templates (``parents'') for the next generation of candidate protocols. Using this method, we were able to automatically re-invent all human-designed secrecy amplification protocols proposed so far and find a new protocol that outperforms them. With respect to classical human-made protocols, an increase in number of secure links was obtained by the efficient combination of the simpler protocols and an unconventional interleaving of elementary instructions that enable protocol execution even when one of the participants is out of reach of the radio transmission.

The practical disadvantage of secrecy amplification protocols is the number of necessary messages resulting in high communication overhead during the link key establishment. We propose an alternative construction which exhibits only linear (instead of exponential) increase of necessary messages when the number of neighbours in communication range (network density) is growing. As a message transmission is a battery expensive operation, this more efficient protocol can significantly save this resource. Designing secrecy amplification protocol in such scenario is more difficult as more parties are involved and the relative positions of the nodes must be taken into account as well. Again, we used described an automatic protocol search to find a protocol for a message restricted scenario with comparable performance to protocols with original assumptions.

Finally, we explore the dark side and propose a new concept for automatic search for attack strategies with demonstrative applications to link key security for probabilistic pre-distribution and Key Infection approaches. The similar framework as for protocols generation was used and candidate attacker strategy is combined from elementary operations and evaluated on network simulator or in real system. Attacker strategies that increase the number of compromised links with respect to several deterministic algorithms or random case were found. Our framework can be used to improve the success of an attacker with the ability to perform selective actions and even to provide novel and unconventional attacks.