InSecTT project summary: SAL contributions

The goal of InSecTT project was on developing solutions for Intelligent, Secure Trustable Things. In this big project with 55 partners, SAL has developed a trustworthiness framework for Wireless Sensor Networks (WSNs) considering lower network layer aspects such as Received Signal Strenght Indicator (RSSI) and wireless channel behaviour.

Trustworthiness is often assessed at higher network layers, involving topics such as cryptography, network orchestration, and application security. However, within the InSecTT project, SAL developed a trustworthiness framework that considers lower network layer aspects of wireless communication. When focusing directly on the communication of nodes within a WSN, trustworthiness becomes increasingly related to reliability: how much can I trust that my connection is stable and coming from a trusted source? To address this issue, SAL has identified **three major topics** related to lower-layer trustworthiness and demonstrated the concepts for each of them.

Passive RSSI sniffing in industrial WSN: Firstly, wireless nodes can be mobile and the physical environment plays a significant role in wireless communication. Changes in the environment can alter the conditions of a wireless link and in some applications, it can be important to localize a wireless node. To ensure trustworthiness, we must verify the location of a wireless node to confirm that it's in the correct position as defined by the application or that it hasn't been replaced by a malicious node. In this topic, SAL has shown that with simple passive RSSI sniffing in different parts of an industrial WSN, it is possible to perform zone-based localization of wireless nodes.

Wireless link interference estimation: Secondly, the behavior of the wireless environment needs to be considered to avoid bad link conditions. Since the wireless channel is usually a shared medium, other devices may attempt to communicate on the same channel, resulting in interference with our network. To ensure trustworthiness, a WSN has to observe the wireless environment and take countermeasures if issues arise. SAL has demonstrated the possibility to estimate the transmission pattern of external devices with periodic transmission patterns and external Bluetooth Low Energy (BLE) devices.

Wireless link supervision and prediction: Thirdly, the condition of the wireless link between two nodes has to be supervised to ensure communication integrity and to predict potential upcoming problems. For this, trustworthiness parameters are defined and continuously monitored. The normal behavior of the wireless network is learned and outliers to this behavior are identified. This allows the early detection of sensor node problems, the hijacking of a wireless communication, or an attack on the WSN. SAL has demonstrated wireless link supervision by applying our trustworthiness framework to detect the hijacking of a WiFi access point.

Only if trustworthiness in all the three introduced lower-layer topics can be guaranteed, reliable communication in for example industrial environment is possible.