WSN — A Wireless Sensor Network (WSN) is a network composed of a high number (often heterogeneous) of small, energy- and resource constrained nodes called motes.

The reference standard for WSN communication is the IEEE 802.15.4.

Security — Providing security features in a WSN is challenging:
- Small storage available (50-100 KB of ROM, 8-12 KB of RAM)
- Small and slow micro-controller unit (MCU) (e.g. Atmel, MSP430)
- Vulnerable communication channels (2.4 GHz ISM bands)

IDS — An Intrusion Detection System (IDS) is a component whose purpose is to detect any malicious attempt to compromise the security of the network.

IDS for WSN — WSNs have additional security issues when attacker intrusions are considered (e.g. malicious mote injection, mote-stealing, mote-tampering etc.). In order to detect and defend against classical and specific attacks, an IDS for WSN should be carefully designed while respecting the resource constraints of the WSN motes.

Solution — Adopt WSN-specific lightweight solutions

WIDS

Our approach, the Wireless Sensor Networks Intrusion Detection System (WIDS) [1], is an ad-hoc IDS solution for WSN. It exploits the Weak-Process Models (WPM) [1] to model WSN attacks, using only a small amount of computational resource and storage.

A WPM can be represented as a graph in which nodes represent the state of the mote and the edges represent the possible transitions.

Leaf nodes of the WPM represent a successfully detected attack.

Each transition has a score value and a list of observables events.

WIDS tracks observables, process transitions and update the list of possible states (state trace) in which the WSN could be. At each update interval, WIDS tries to prune all the states from the trace in which the WSN mote is unlikely to be. The remaining states are considered and, if any of them is a state marked as dangerous, a notification of a successful detection is sent to the application.

WIDS: Concept

The WPM represent an example attack model with seven states (including the starting state Reset and the Detected state). Here, the Observable creation for each step is shown along the resulting state traces and the time diagram that results in WIDS selecting the state trace ending with state 5 as dangerous.

Reference

References


Contact Information

Authors email addresses:
- walter.tiberti@graduate.univaq.it
- luigi.pomante.univaq.it