Detecting Routing Attacks in Industrial IoT

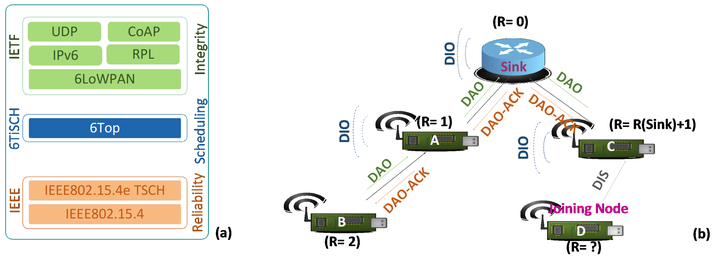
Areej Althubaity, Computer Science and Engineering, University of Connecticut Advisor: Song Han

Abstract

We focus on securing the routing protocol in the IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH) network architecture from internal attacks. We have designed lightweight Intrusion Detection Systems (IDSs) that have high detection accuracy and incurring a moderate overhead on the devices storage, computation, and energy resources.

Motivation

6TiSCH has brought the deterministic and time-critical industrial networks to the Internet. 6TiSCH devices, however, are not temper-resistance sensors and the Routing Protocol for Low-Power and Lossy Networks (RPL) that has been adapted in the architecture is vulnerable to a number of internal attacks. Protecting the 6TiSCH network and securing the low-capability devices from any attack is a goal that must be fulfilled.



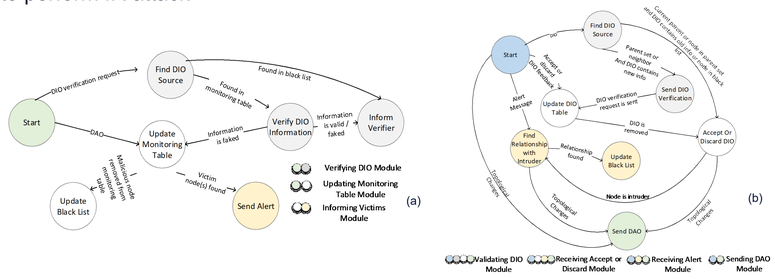
(a) Overview of the 6TiSCH architecture; (b) an example of an RPL DODAG graph. The black arrows indicate a parent-child relationship and the numbers in parenthesis are node's Rank value. DIO, DIS, DAO, and DAO-ACK are the four different ICMPv6 control messages used in the RPL protocol

RPL Internal Attacks

Some features in the RPL protocol are left without any proper protection mechanisms; for example device's location in the routing topology (Rank) and loops' avoidance and detection rules. These attacks are:

- ***Decreased Rank (DR)***: where the compromised device lures its neighbors that its very closed to the root of the routing topology;
- ***Rank Attack based on the Objective Function (RAOF)***: where the compromised device lures its neighbors by advertising better routing metrics;
- ***Increased Rank (IR)***: the compromised device creates loop in the routing topology;
- ***Worst Parent Selection Attack (WPS)***: where the compromised device selects the worse path toward the root of the routing topology.

Different scenarios of Rank-related attacks: (a) Healthy RPL topology; (b) Malicious node F establishes DR attack by multicasting DIO with fake Rank; (c) Malicious node E initiates RAOF attack by advertising better path cost; (d) Malicious node F performs WPS attack by selecting the worst parent in its parent set that is node E; (e) Malicious node E selects one of its direct children node G to perform IR attack



ARM's finite state machine on: (a) the root of the routing topology and (b) the rest of the RPL devices

Intrusion Detection Systems

We have introduced a centralized IDS named ARM (**A**uthenticated **R**ank and routing **M**etric) to detect DR and RAOF and later we have proposed a fully distributed IDS named FORCE (**FO**rged Rank and routing metri**C** d**E**tector) to detect all the aforementioned attacks. In ARM:

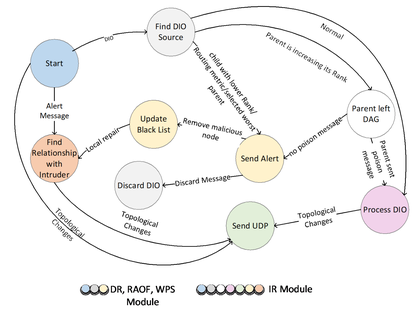
- the root is responsible for making the detection decisions;
- the devices periodically share with the root their routing information.

While in FORCE:

- each device should monitor its neighborhood and analyze each received routing control messages.

However, both IDSs:

- have been simulated using Contiki network simulator (COOJA);
- Comparing to the state-of-the-art IDSs, they have high detection accuracy and low false positive rate and incur a moderate overhead on the resources.



FORCE's finite state machine on each device