# Routing Protocol Overview

# Background Knowledge

- In this document we introduce routing protocol concepts that are important for understanding IoT security attacks, as follows
  - Fundamental sensor network types
    - WSN (Wireless Sensor Network)
    - LLN (Low Power and Lossy Network)
    - 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network)
  - The routing protocol used in IoTrain-Sim security training exercises, RPL (Routing Protocol for Low power and Lossy Networks)
    - RPL security concerns and attack taxonomy

# WSN (Wireless Sensor Network)

- A wireless sensor network is a network formed by a large number of sensor nodes, where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc.
- WSNs are an information gathering method, and the collected data is used to improve the operation of the systems to which it refers to, for instance in industry, agriculture, etc.
- WSNs enables real-time detection, tracking, and even remote control of the nodes in the monitored area
- WSN is a key technology of IoT, and the protocols employed in WSNs are usually different than the protocols in regular wireless networks, such as WLAN

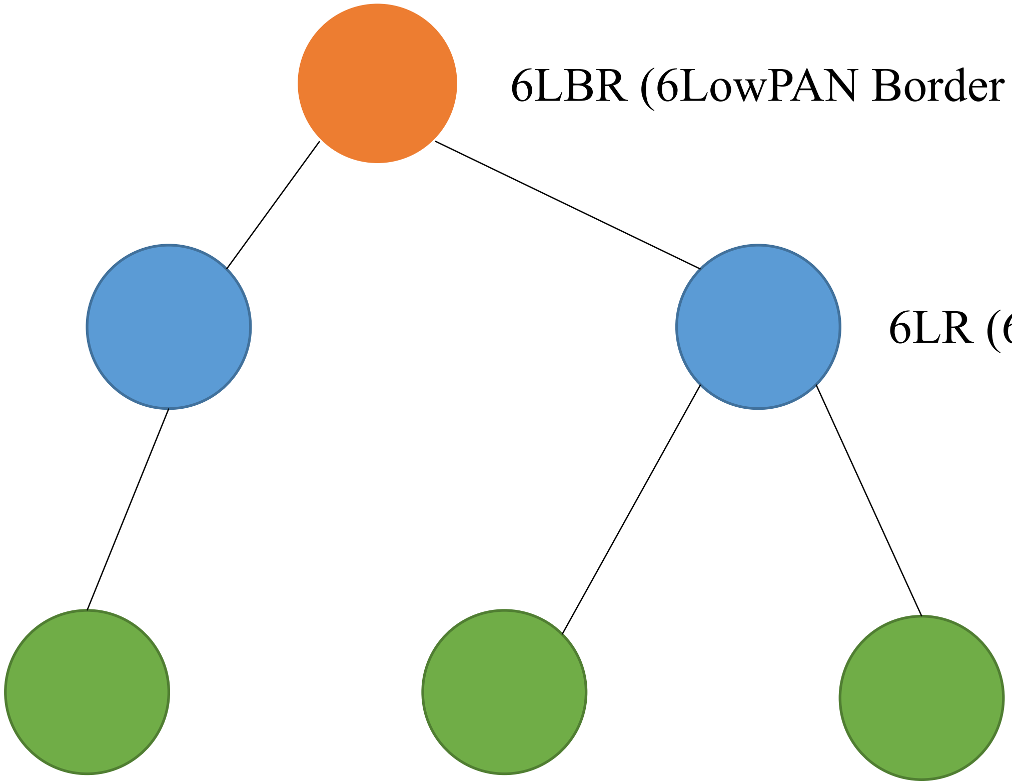
# LLN (Low-Power and Lossy Network)

- LLN is a network composed of many embedded devices with limited power, memory, and processing resources interconnected by a variety of links, such as IEEE 802.15.4 or low-power Wi-Fi
- LLNs are a typical example of WSN and have a wide scope of applications
  - Example application areas include monitoring, building automation, connected home, health care, environmental monitoring, urban sensor networks, energy management, assets tracking

# 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network)

- 6LoWPAN is a low cost and low-power communication network that connects resource-constrained wireless devices, typically wireless sensors or actuators, using a compressed version of the IPv6 protocol
- 6LoWPAN supports multi-hop communication where nodes can forward packets on behalf of other nodes
- To save energy, 6LoWPAN uses duty cycles, so that the radio is turned off most of the time, and is turned on only for a very short time for listening
- As a disadvantage, 6LoWPAN is vulnerable not only to the typical attacks against WSNs, but also to attacks originating from the Internet

# 6LoWPAN Topology Example



6LBR (6LowPAN Border Router)

6LR (6LowPAN Router)

6LN (6LowPAN Node)

6LoWPAN (IPv6 over Low power WPAN) - IPv6 compressed

# RPL Protocol

# RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks)

- RPL is a standardized routing protocol for the IoT, primarily used in 6LoWPAN networks
- RPL operation is based on concepts introduced in the Distance Vector (DV) protocol and the Source Routing Protocol
- Other concepts related to RPL are
  - DAG (Directed Acyclic Graph)
  - DODAG (Destination Oriented DAGs)
  - DODAG Version Number
  - DIO (DODAG Information Objects)
  - DAO (Destination Advertisement Object)
  - DIS (DODAG Information Solicitation)

# Distance Vector (DV) Protocol

- The term distance vector refers to the fact that the said protocol manipulates vectors (arrays) of distances to other nodes in the network
- DV is an intra-domain routing protocol that requires each router to inform its neighbors of topology changes periodically
- DV has a lower computational complexity and message overhead compared to other protocols

# DV Protocol (cont.)

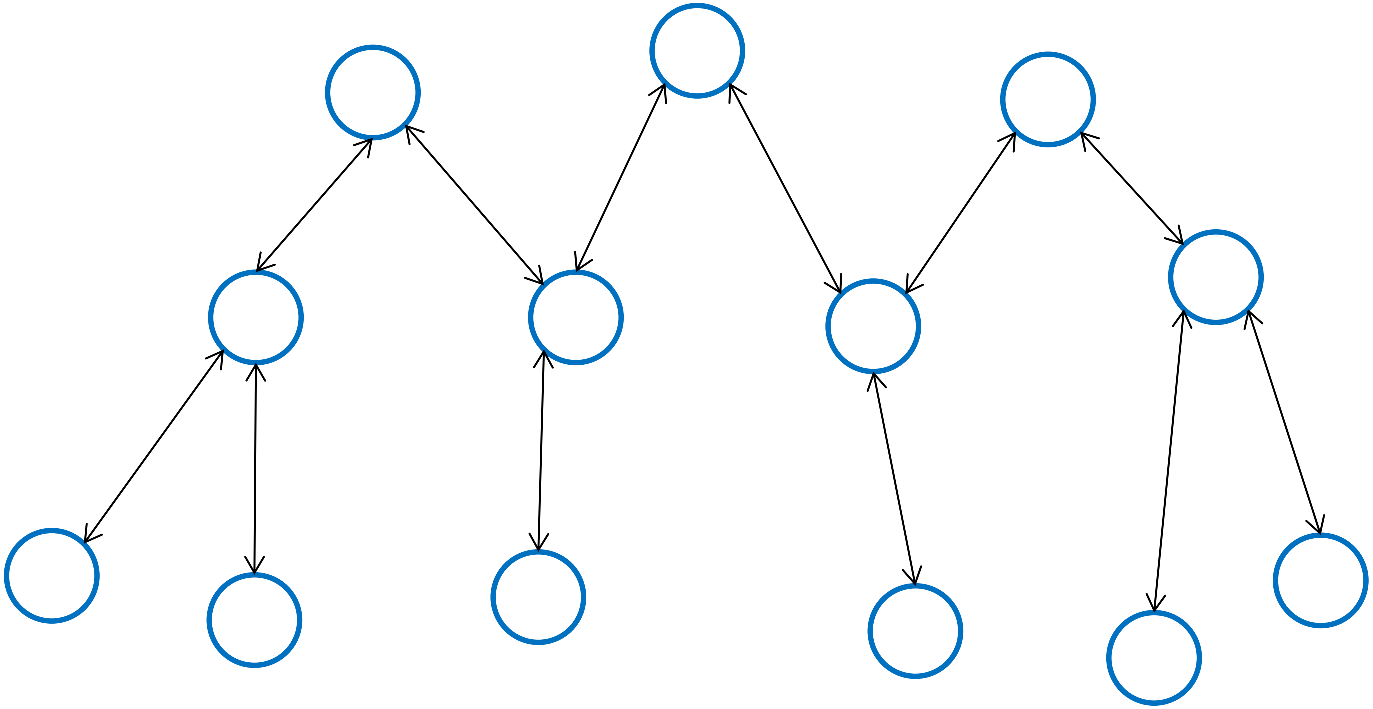
- Distance-vector protocols are based on calculating the Direction and Distance to any link in a network
  - "Direction" usually means the next hop address and the exit interface
  - "Distance" is a measure of the cost to reach a certain node
- The least cost route between any two nodes is the route with minimum distance
- Each node maintains a vector (table) of minimum distance to every node
- The cost of reaching a destination is calculated using various route metrics

# Source Routing (Path Addressing) Protocol

- A source routing protocol allows the sender of a packet to partially or completely specify the route the packet takes through the network
- Such a protocol enables a node to discover all the possible routes to a host and chose the best one
- In the next slides we present several other concepts related to the RPL protocol, such as DAG and DODAG

# DAG (Directed Acyclic Graph)

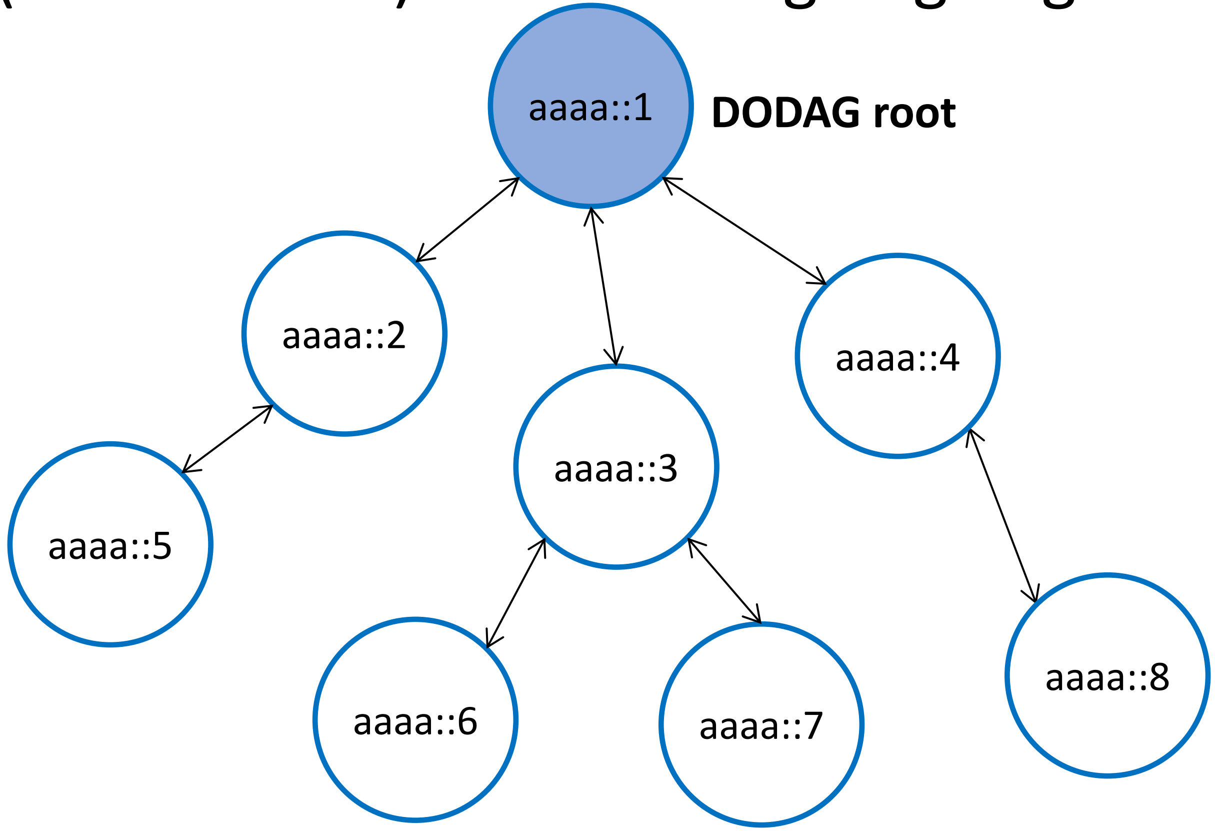
- RPL creates a destination-oriented directed acyclic graph (DODAG) between the nodes in a 6LoWPAN



RPL DAG example

# DODAG (Directed Acyclic Graph)

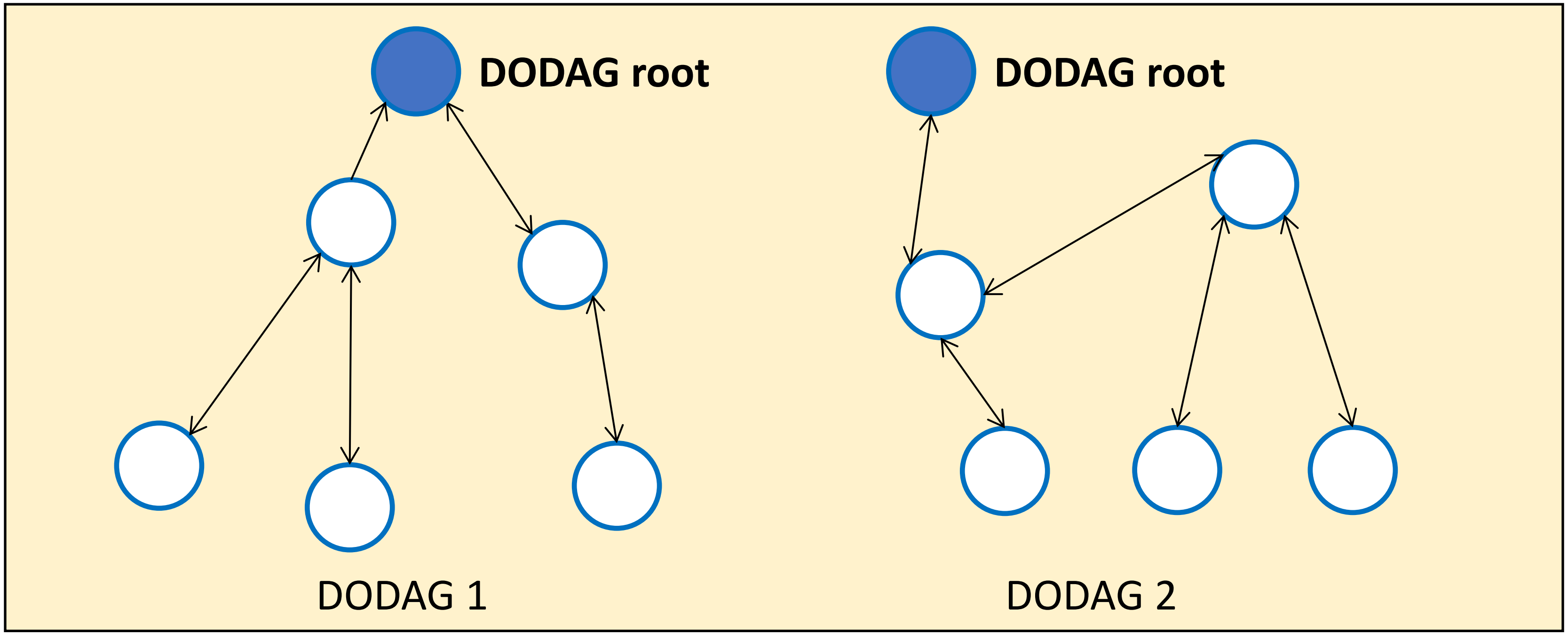
- A DAG rooted at a single destination at a single DAG root (DODAG root) with no outgoing edges



RPL DODAG in which each node has a unique IPv6 address

# RPL Instances

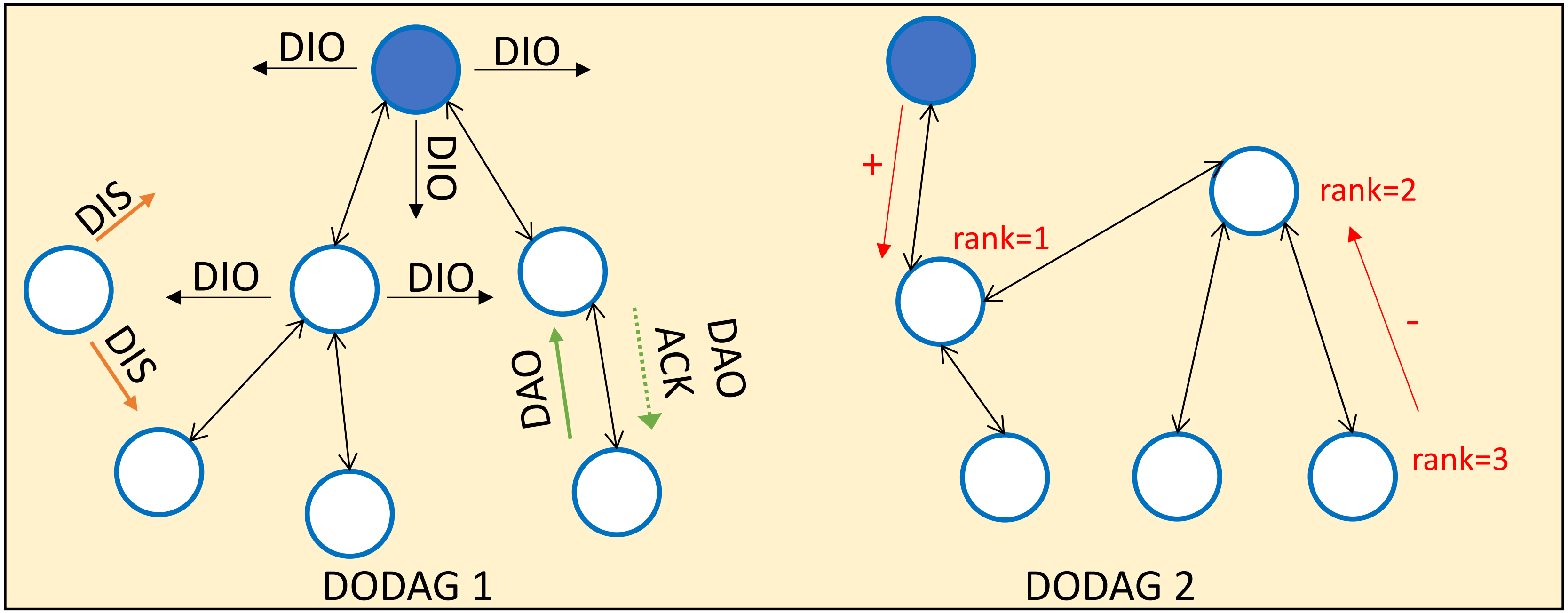
- An RPL instance is a set of DODAGs that share an RPLInstanceID  id, which is a unique identifier in a network
  - DODAGs with the same RPLInstanceID share the same function used to compute the position of node in the DODAG



RPL with id “RPLInstance1”

# DODAG Version Number and Rank

- To identify and maintain a network topology, RPL uses the DODAG Version Number and Rank mechanism
  - DODAG Version is a specific DODAG iteration with a given id, and the Version Number is a sequential counter incremented by the DODAG root
  - DODAG Rank defines the node's individual position relative to other nodes with respect to a DODAG root



RPL with id "RPLInstance1"

# DIO, DAO and DIS

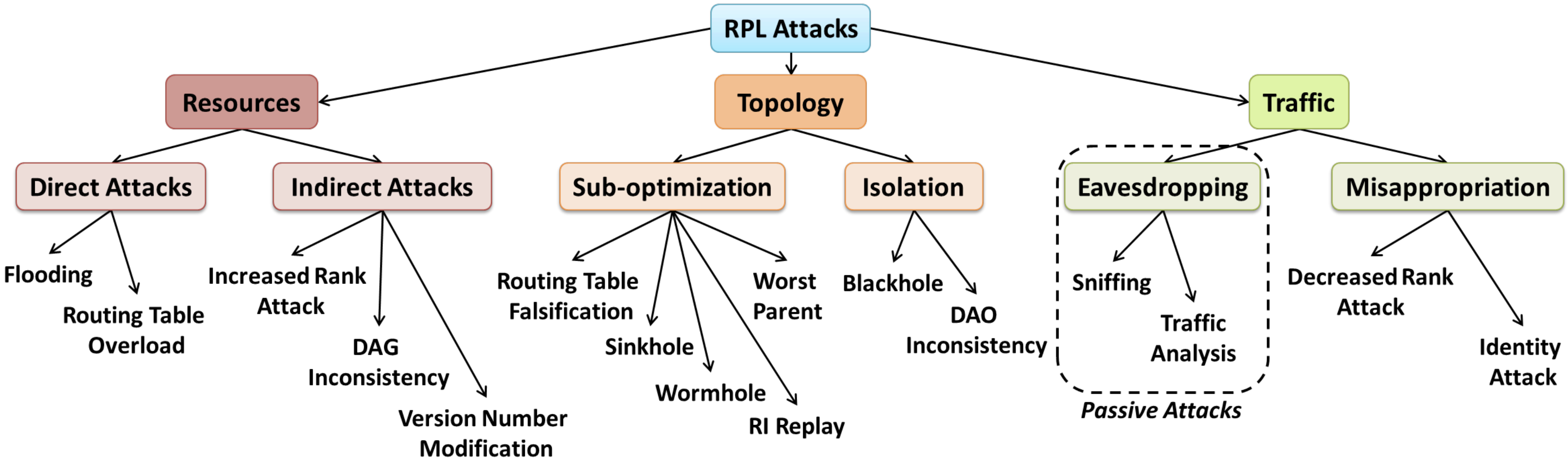
- DODAG Information Objects (DIO) are used to advertise information used to build the RPL DODAG
- Destination Advertisement Object (DAO) messages are used to advertise information required to support downward traffic towards leaf nodes
  - Each child node sends a DAO message to its parents upon joining the network
  - Parent nodes can explicitly poll the sub-DODAG for DAO messages using DIO messages
- DODAG Information Solicitation (DIS) messages are used by nodes to request graph related information from the neighboring nodes

# RPL Security Concerns

- The RPL protocol is susceptible to a large variety of security attacks
- The characteristics of LLN networks such as resource constraints, lack of infrastructure, limited physical security, dynamic topology and unreliable links make them particularly vulnerable and difficult to protect against security attacks
- Some of the above issues are not specific to the RPL protocol, and can be applied to other wireless sensor networks or even to wired networks

# Security Attacks on RPL

- Taxonomy of attacks on RPL-based networks that is the basis for our security training content



- For details, see: A. Mayzaud, R. Badonnel, I. Chrisment, “A Taxonomy of Attacks in RPL-based Internet of Things”, *International Journal of Network Security*, Vol.18, No.3, pp.459-473, May 2016. https://hal.inria.fr/hal-01207859/document