



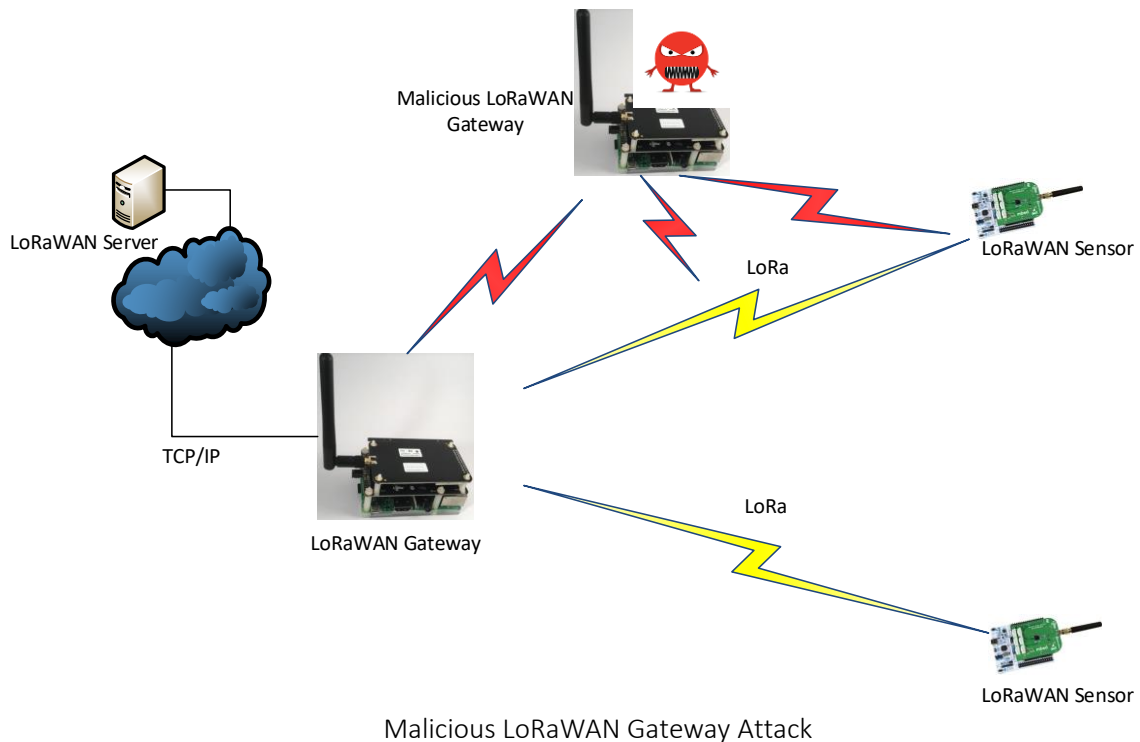
IoT Cyber Attacks Self Detection

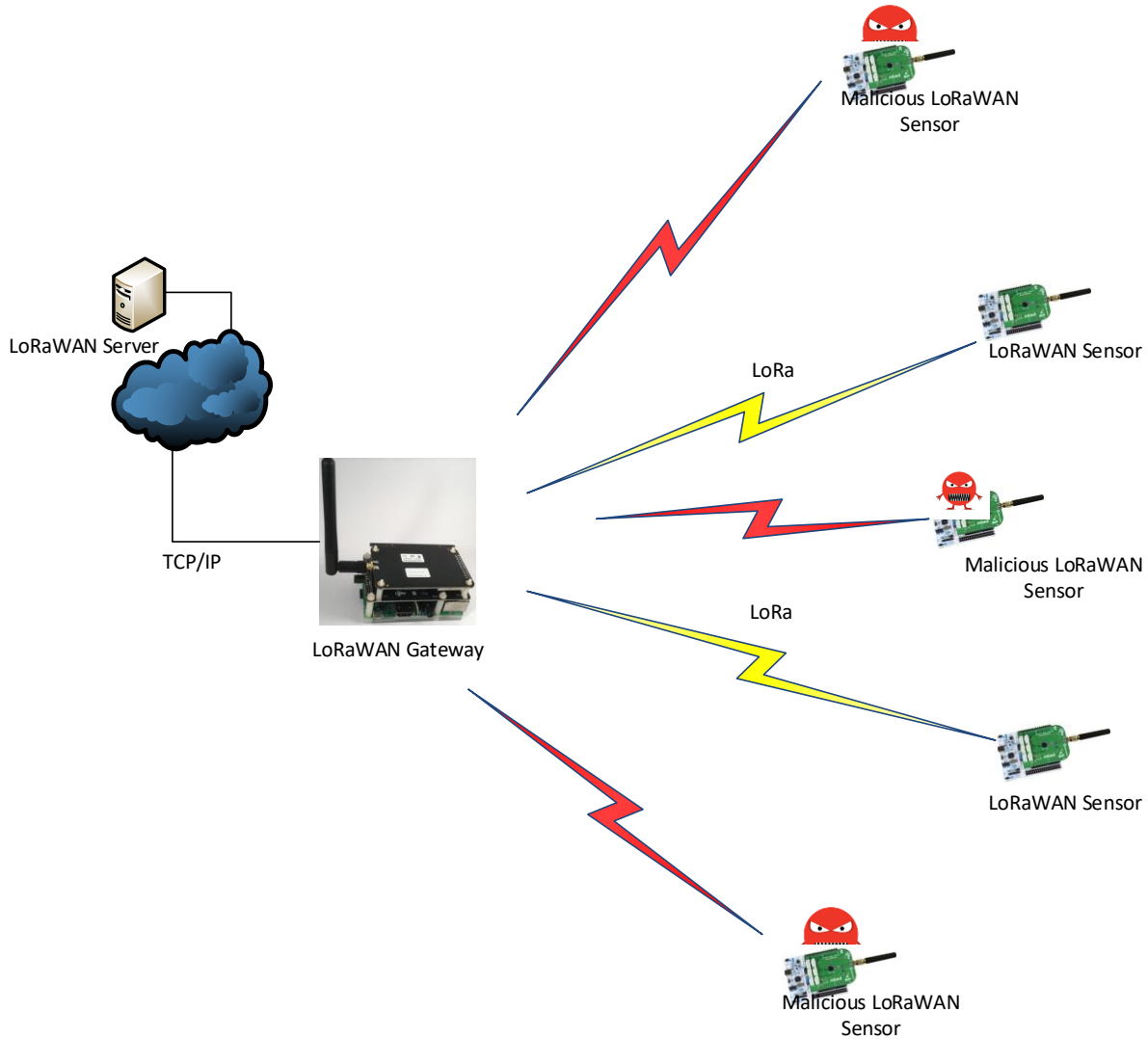
Abstract:

Low-power WAN (LPWAN) is a wireless wide area network specification for Internet-of-Things (IoT) deployments that interconnects low-bandwidth, battery-powered sensors with low bit rates over long ranges.

To meet the challenges of long range, low power consumption and secure data transmission, the sensors are based on LoRa Technology and on LoRaWAN media access control (MAC) layer protocol that manages communication between LPWAN sensors and the Gateway.

LPWAN based LoRaWAN is vulnerable to 2 cyber attack types: Malicious Gateway and sensor flooding attack. Malicious LoRaWAN Gateway can track the sensors-gateway downlink-uplink traffic pattern and then disrupt the traffic. Sensor flooding attack can be generated by multiple coordinated malicious LoRaWAN sensors that can generate traffic simultaneously and so cause the LoRaWAN server to malfunction. LoRaWAN gateways should be able to self-detect such attacks and avoid LPWAN collapse.





Flooding Attack

Goals:

1. Learn about LoRa and LoRaWAN.

Refer to:

<https://www.lora-alliance.org/>

<https://www.link-labs.com/blog/what-is-lorawan>

<https://books.google.co.il/books?id=iSE6DwAAQBAJ&pg=PT108&lpg=PT108&dq=LoRaWAN+system+s+can+receive+eight+messages+simultaneously&source=bl&ots=4uDTCW0rVm&sig=IlcolgkwCe0EiSRtFfqegns2cy0&hl=iw&sa=X&ved=0ahUKewje2qS777nZAhVP26QKHU4pCbIQ6AEIjAA#v=onepage&q=LoRaWAN%20systems%20can%20receive%20eight%20messages%20simultaneously&f=false>



<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5038744/>

<https://medium.com/home-wireless/testing-lora-radios-with-the-limesdr-mini-part-2-37fa481217ff>

2. Bring-up the LoRaWAN development and working environments (sensor-gateway-server). Refer to instructions in: <https://gitlab.cs.technion.ac.il/lccn/w2019-lorawanrelay>
3. Reconstruct the Malicious Gateway attack and then implement in the gateway using ML:
 - a. Controller Intrusion Detection (CID) through LoRaWAN Server.
 - b. Distributed Intrusion Detection (DID) between the gateways.
4. Simulate flooding attack and then implement in the simulated gateway using ML:
 - a. Controller Intrusion Detection (CID) through simulated LoRaWAN Server.
 - b. Distributed Intrusion Detection (DID) between the simulated gateways.

Requirements:

Introduction to Networking (236334 or 044334)

C Programming

Guided by:

Aviel Glam (Rafael), Itai Dabran (ICST), Itzik Ashkenazi (LCCN)

