SIMULATION REPORT

Version Number Modification Attack

1. Introduction

Goal: Demonstrate that this attack through power tracking results. With its modified RPL file, the malicious node increases the version number before forwarding received DIO messages, thus triggering unnecessary global repairs.

2. Configuration

Wireless Sensor Network

The simulation lasts 120 seconds and is not repeated.

The WSN contains:

- 1 root node of type *root-dummy* built upon a *Z1*
- 10 sensors of type *sensor-dummy* built upon a *Z1*
- 1 malicious mote of type *malicious-sensor* built upon a *Z1*

The sensors are spread across an area of 200.0 meters side and centered around the root node at a minimum distance of 20.0 meters and a maximum distance of 200.0 meters. They have a maximum transmission range of 50.0 meters and a maximum interference range of 100.0 meters.

The WSN configuration is depicted in Figures 1 and 2:

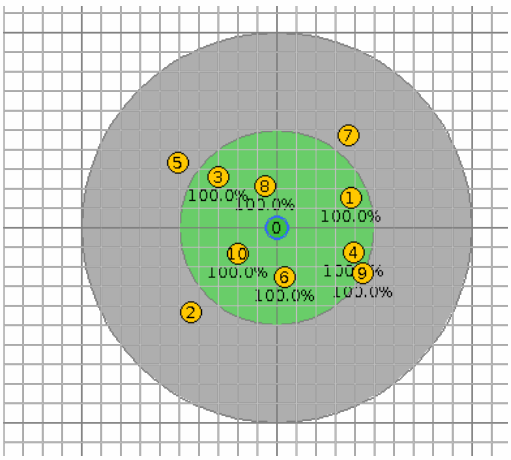

Fig 1 - WSN configuration without the malicious mote before starting the simulation.

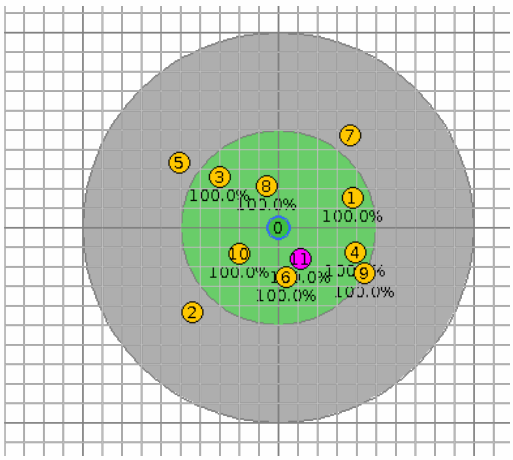

Fig 2 - WSN configuration with the malicious mote before starting the simulation.

Attack

The attack is composed of the following building blocks:

- increased-version

3. Results

In this section, the pictures on the left side corresponds to the results for the simulation without the malicious mote. These on the left are for the simulation with the malicious mote.

Resulting DODAG

The resulting Destination Oriented Directed Acyclic Graph (DODAG) is depicted in the following pictures:

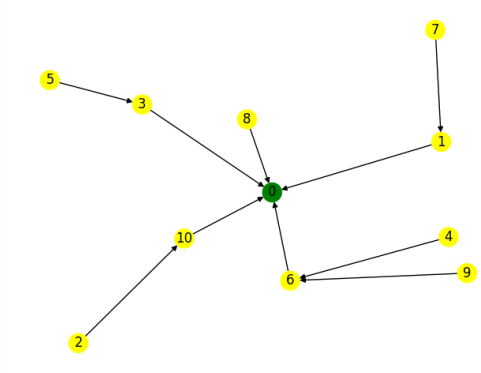

Fig 3 - Final DODAG for the simulation without the malicious mote.

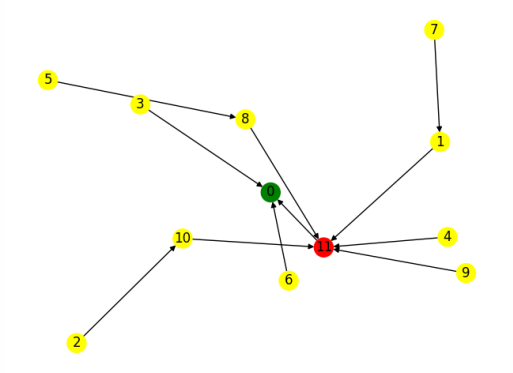

Fig 4 - Final DODAG for the simulation with the malicious mote.

As it can be seen, the DODAG is impacted by the malicious node (in violet) due to the repeated global repairs.

***Important note**: The resulting DODAG's could be not representative if the duration is not long enough. Ensure that it is set appropriately.*

Power Tracking Analysis

The power tracking is depicted in the following pictures:

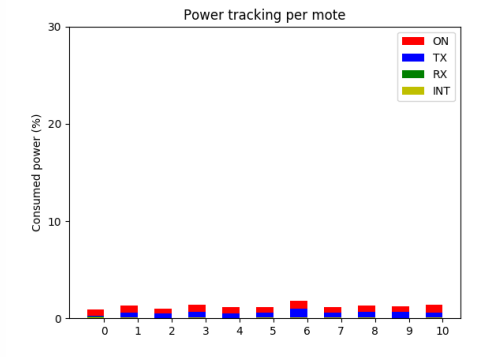

Fig 5 - Power tracking histogram for the simulation without the malicious mote.

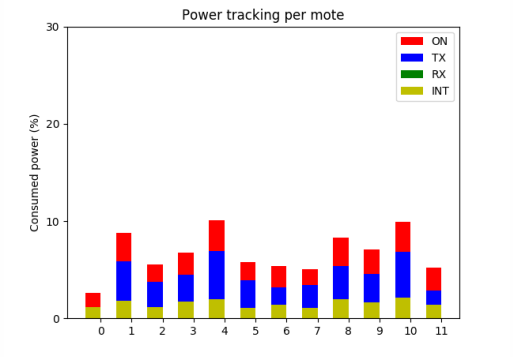

Fig 6 - Power tracking histogram for the simulation with the malicious mote.

By looking at the power consumption, one can ascertain that this attack enjoys a certain efficiency on the whole network as it triggers lots of messages because of the global repair mechanism.