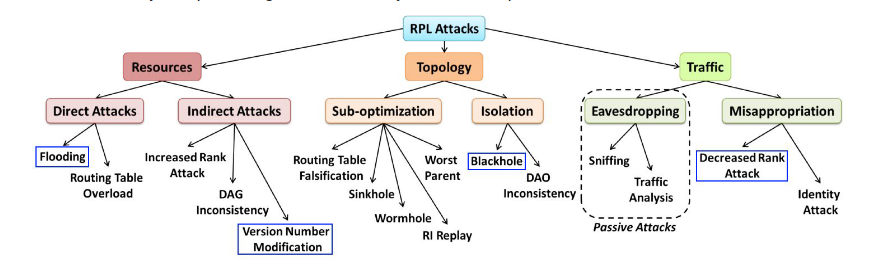
**CONFIGURATION DETAILS OF RPL VERSION NUMBER MODIFICATION ATTACK USING COOJA SIMULATOR**

Created by - Shevgoor Adithya Kamath

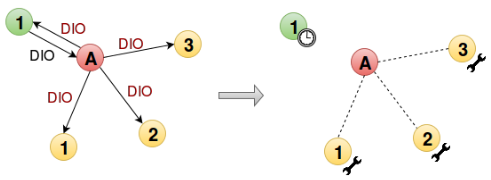
Created on - 29/03/2021

This document aims to provide a simple and convenient way to generate the simulation and deploy malicious (version number modification attack) motes for a Wireless Sensor Network (WSN) that uses Routing Protocol for Low-power and lossy devices (RPL) as its network layer.

Taxonomy of RPL Attacks:



Version Number Modification:



This is an indirect attack causing the exhaustion of resources. When global repair is required DODAG's root increases the version number. So attacking is initiated by Version Number Modification, which causes unnecessary graph rebuildings. Indeed, as the root receives the DIO with an invalid version number, it updates it and resets its trickle timer (as depicted by the timer in the figure below) for resending a new DIO. By contrast, normal nodes initiate a global repair (as depicted by the wrench), that is, they remove their parents and use the received DIO to update their new parent.

Program to create the malicious motes:

| Location | Replace | With |
| --- | --- | --- |
| rpl-icmp6.c | dag->version; | dag->version++; |

Configurations used for the simulation:

| Parameters | Name in Contiki | Location | Default values |
| --- | --- | --- | --- |
| Interference Range | INT Range | Cooja | 100 meters |
| Transmission Range | TX Range | Cooja | 50 meters |
| Transmission Ratio | TX Ratio | Cooja | 100% |
| Reception Ratio | RX Ratio | Cooja | 100% |
| Number of normal udp\_sender motes |  |  | 9 |
| Number of malicious motes |  |  | 1 |
| Number of sink motes |  |  | 1 |

* Initial arrangement of motes -
* DODAG formed after 1 hour of simulation -
* Network Hops output -

Result found when simulating RPL Version Number Modification attack:

* Changes in DAG will occur causing unnecessary graph rebuildings.
* As this is a resource attack, there should be significant increase in power usage and energy exhaustion.

Bibliography:

1. Mobile and Embedded Computing Report

<https://www.google.com/url?sa=i&url=https%3A%2F%2Frpl-attacks.readthedocs.io%2Fen%2Flatest%2Freport.pdf&psig=AOvVaw3HTWE8chSyyHodOTXtIsQo&ust=1616503315184000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCICo-6H2w-8CFQAAAAAdAAAAABAI>

1. <https://rpl-attacks.readthedocs.io/en/latest/>
2. <https://github.com/BavyaBalakrishnan/RPL_ATTACKS_COOJA/blob/master/ANALYSIS%20OF%20THE%20IMPACT%20OF%20VARIOUS%20ATTACKS%20ON%20RPL%20USING%20CONTIKI%20OS%20AND%20COOJA%20SIMULATOR.pdf>