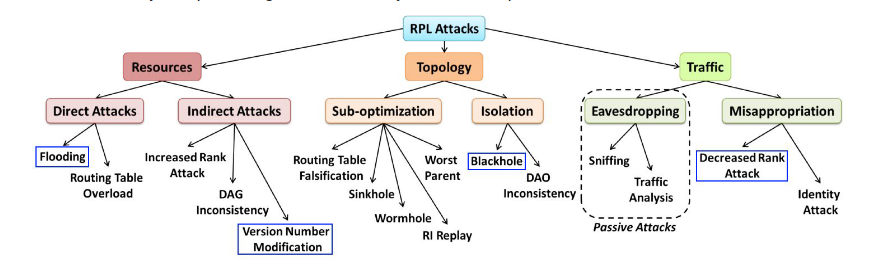
**CONFIGURATION DETAILS OF RPL DECREASE RANK ATTACK USING COOJA SIMULATOR**

Created by - Shevgoor Adithya Kamath

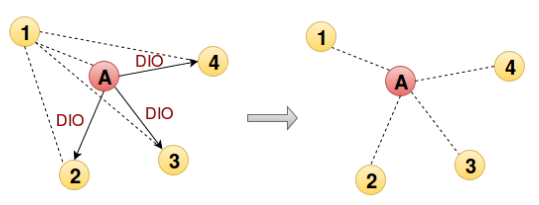
Created on - 29/03/2021

This document aims to provide a simple and convenient way to generate the simulation and deploy malicious (decrease rank attacks) 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:



Decreased Rank:



It is implemented by advertising a lower rank to make the legitimate nodes connect to the DODAG via the attacker.This can be a basis for sinkhole, blackhole or also eavesdropping attacks.

Program to create the malicious motes:

| Location | Replace | With |
| --- | --- | --- |
| udp\_sender.c |  | #define RPL\_CONF\_MIN\_HOPRANKINC 0 |
| rpl-timers.c | rpl\_recalculate\_ranks(); |  |

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 Decrease rank attack:

* The malicious node will advertise a better rank than neighbours, causing the DAG to be modified.
* This attack does not damage a network, however, combining with other building blocks could be very effective because it allows the attacker to suck all the traffic to him.
* DAG is changed, legitimate nodes in the neighbourhood of the malicious node have now set it as their parent.
* Took a lot of time to start data transmission(network stabilization took time).
* High power consumption by the attacker node and its neighbours. Initially only the unaffected nodes send packets.

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>