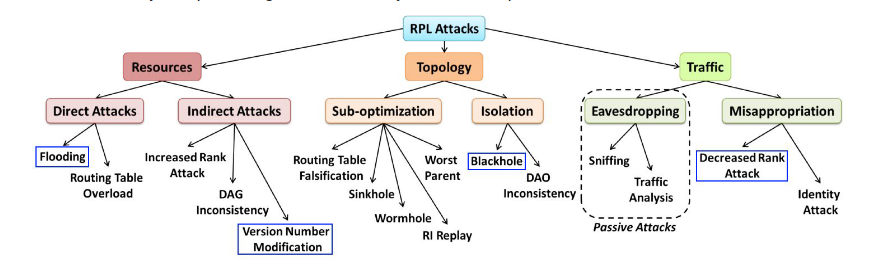
**CONFIGURATION DETAILS OF BLACKHOLE ATTACK USING COOJA SIMULATOR**

Created by - Shevgoor Adithya Kamath

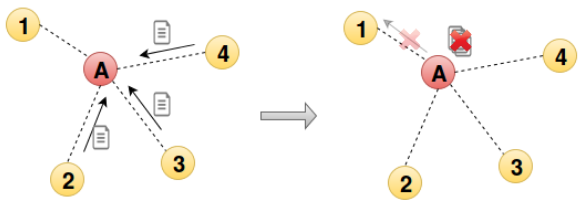
Created on - 01/04/2021

This document aims to provide a simple and convenient way to generate the simulation and deploy malicious (blackhole 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:



Blackhole Modification:



Instead of forwarding the packets, the malicious node drops them. This attack can be seen as a denial-of-service attack. If the position of the node is well chosen, it can isolate several nodes from the network. The selective forwarding attack (greyhole) is a variant of this type of attack. This attack has as consequence to disturb routing paths, it can be used to filter any protocol.

Program to create the malicious motes:

| Location | Replace | With |
| --- | --- | --- |
| rpl-icmp6.c | goto fwd\_dao; | //goto fwd\_dao; |
| rpl-icmp6.c | uip\_icmp6\_send(rpl\_get\_parent\_ipaddr(dag->preferred\_parent),ICMP6\_RPL, RPL\_CODE\_DAO, buffer\_length); | //uip\_icmp6\_send(rpl\_get\_parent\_ipaddr(dag->preferred\_parent),ICMP6\_RPL, RPL\_CODE\_DAO, buffer\_length); |

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 Blackhole attack:

* The increase in the number of DIO messages exchanged indicates the unstable topology with respect to routing of packets.
* DIO packets generated by each node establishes the fact that the nodes have the idea of network instability.
* The reason for the above results -

The DAO are not forwarded to the parent and it causes instability in topology causing nodes to send more DIO messages.

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>