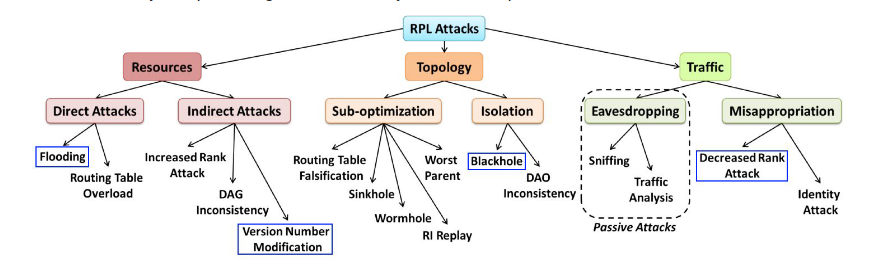
**CONFIGURATION DETAILS OF RPL FLOODING ATTACK USING COOJA SIMULATOR**

Created by - Shevgoor Adithya Kamath

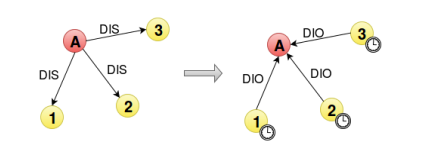
Created on - 22/03/2021

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



Flooding:



This attack consists of generating a large amount of traffic through DIS messages, causing nodes within range to send DIO messages (used to advertise information about DODAG’s to new nodes) and reset their trickle timers (supposed to increase as the network stabilizes).Note That, if secure DIS are used, this attack can still be performed using a compromised node.

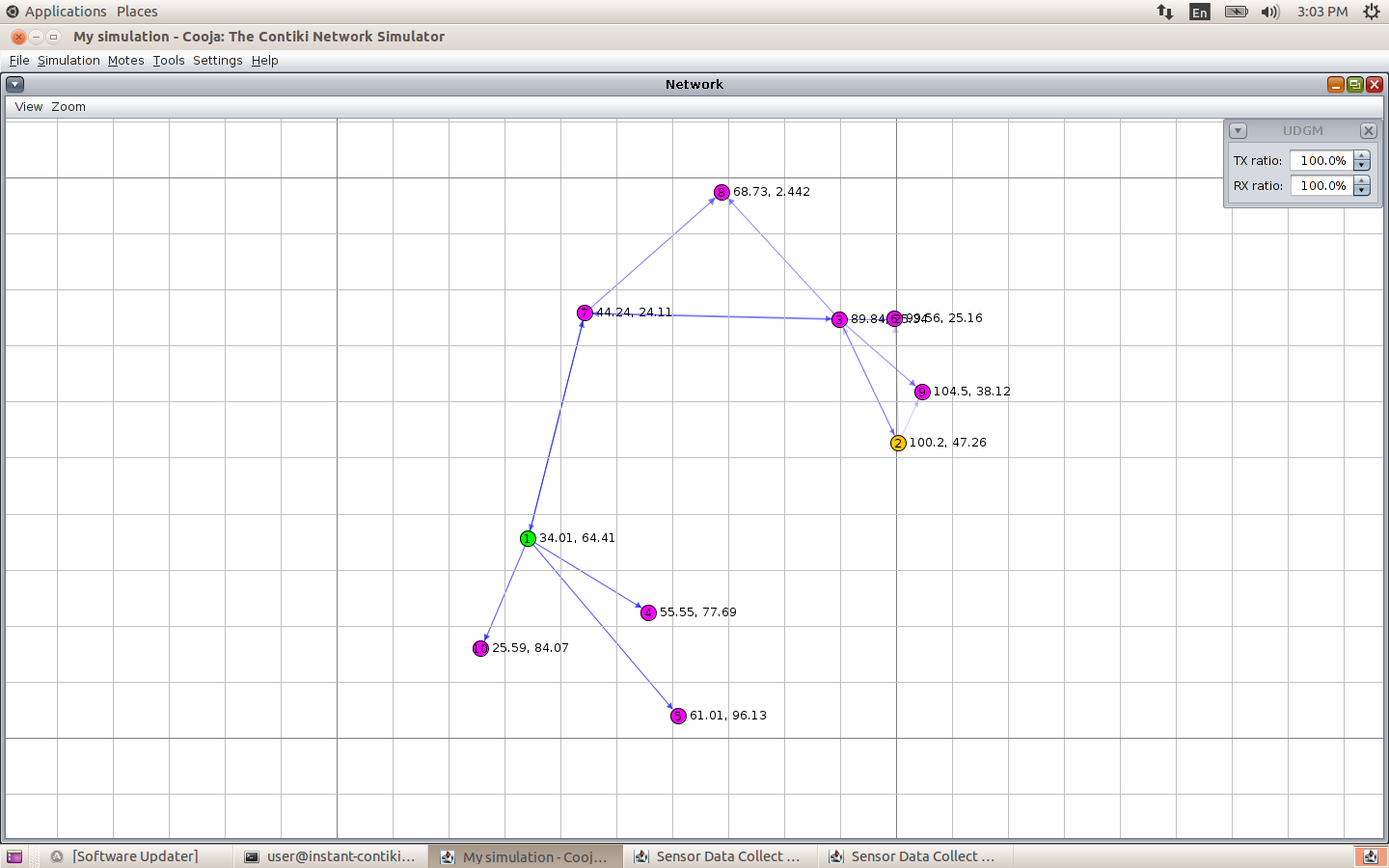
Program to create the malicious motes:

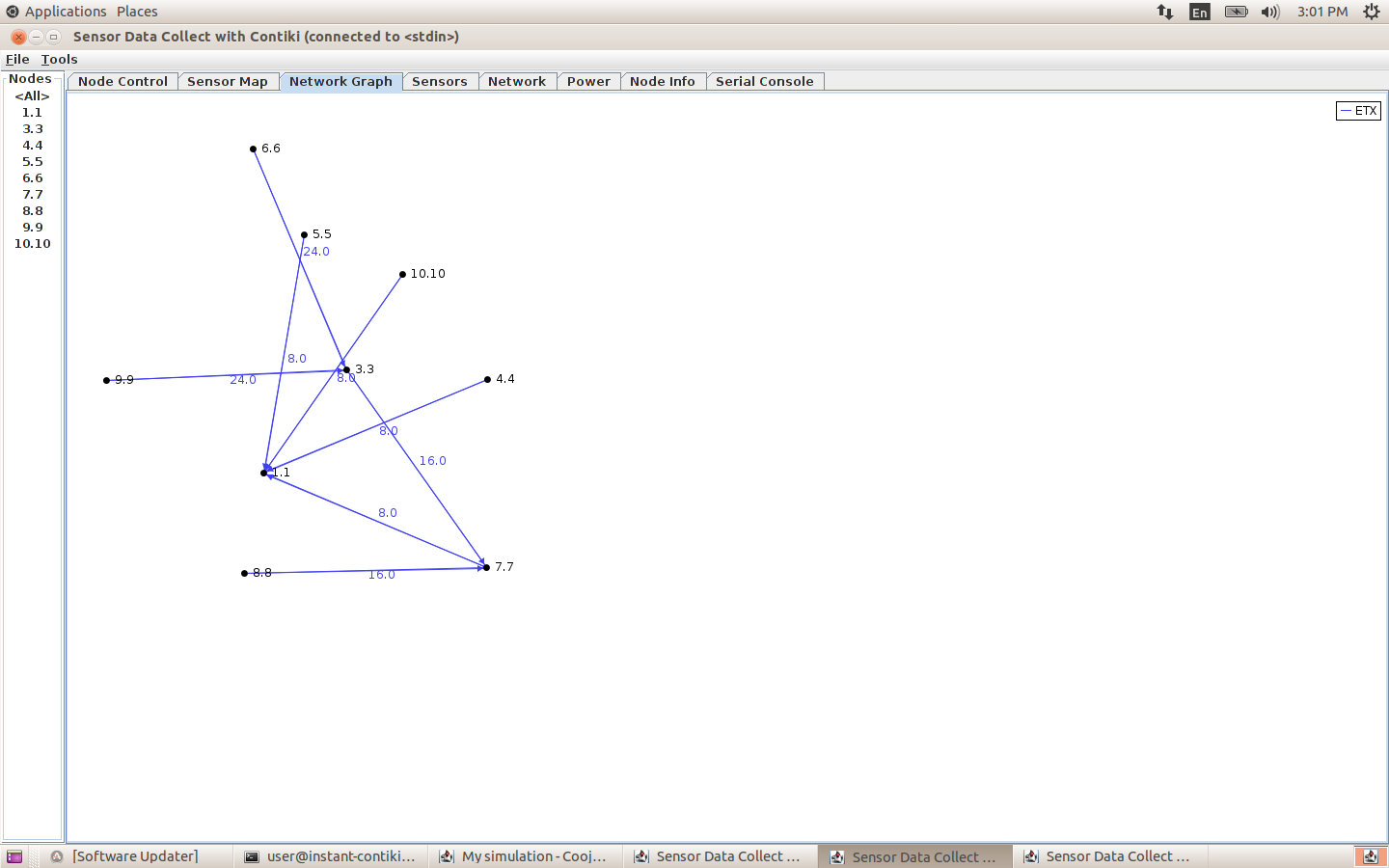
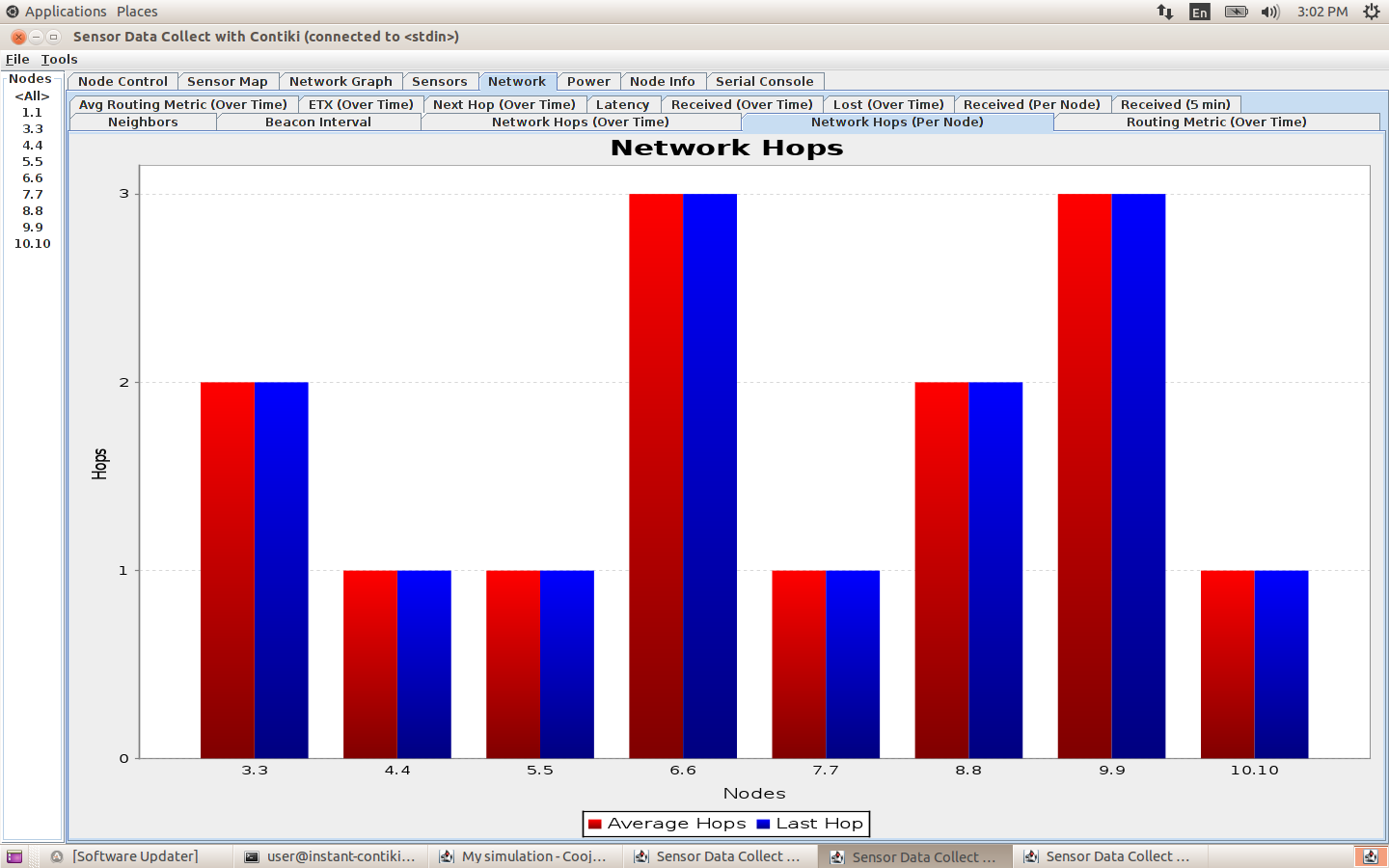
| Location | Replace | With |
| --- | --- | --- |
| udp\_sender.c |  | #define RPL\_DIS\_INTERVAL 0  #define RPL\_DIS\_START\_DELAY 0 |
| rpl-timers.c | next\_dis++; | next\_dis++;  int i=0;  while (i<10)  {  i++;  dis\_output(NULL);  } |

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 Flooding attacks:

* The malicious node immediately starts sending DIS messages to its neighbours, then triggering DIO messages and trickle timers reset.
* No change in DAG.
* Important energy exhaustion is observed.
* Particularly impacted by the attack in terms of ON and RX times due to multicast DIS.
* Around 1% of total packets were DIS messages generated from malicious node 2 to disturb the network and every other node generated 0.1% DIS 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