

Sink Hole Attack using RPL in IOT

Software: NetSim Standard v14.2, Visual Studio 2022

Project Download Link:

<https://github.com/NetSim-TETCOS/Sinkhole-Attack-in-IoT-RPL-v14-2/archive/refs/heads/main.zip>

Introduction:

In a sinkhole Attack, a compromised node or malicious node advertises fake rank information to form the fake routes, and after receiving the message packet, it drops the packet information.

Implementation in RPL (for 1 sink):

- In RPL the transmitter broadcasts the DIO during DODAG formation.
- The receiver on receiving the DIO from the transmitter updates its parent list, sibling list, and rank and sends a DAO message with route information.
- Malicious node upon receiving the DIO message does not update the rank instead it always advertises a fake rank.
- The other node on listening to the malicious node DIO message updates its rank according to the fake rank.
- After the formation of DODAG, if the node that is transmitting the packet has a malicious node as the preferred parent, transmits the packet to it but the malicious node instead of transmitting the packet to its parent, simply drops the packet resulting in zero throughputs.

A file **Malicious.c** is added to the RPL project. The file contains the following functions.

- **fn_NetSim_RPL_MaliciousNode();** //This function is used to identify whether a current device is malicious or not in order to establish malicious behavior.
- **fn_NetSim_RPL_MaliciousRank();** //This function is used to give a fake rank to the malicious node.
- **rpl_drop_msg();** //This function is used to drop the packet by the malicious node if it enters its network layer.

- **Fn_NetSim_RPL_FreePacket();** // This function is used inside **rpl_drop_msg()** for dropping the packets.
- **Sink Hole Attack** -The malicious node advertises the fake rank **fn_NetSim_RPL_MaliciousRank();** is the sinkhole attack function.
- **Black Hole Attack:** The malicious node drops the packet, **rpl_drp_msg()** is the black hole attack function

You can set any device as malicious, and you can have more than one malicious node in a scenario. Device IDs of malicious nodes can be set inside the **fn_NetSim_RPL_MaliciousNode()** function.

Example

1. The Workspace **Sinkhole-Attack-in-IoT-RPL** comes with a sample network configuration that is already saved. To open this example, go to Your work in the home screen of NetSim and click on the **SinkHole_Attack_in_RPL_Example** from the list of experiments.
2. The saved network scenario consists of
 - a. **5** Wireless Sensors
 - b. **1** LOWPAN Gateway
 - c. **1** Router
 - d. **1** Wired Node

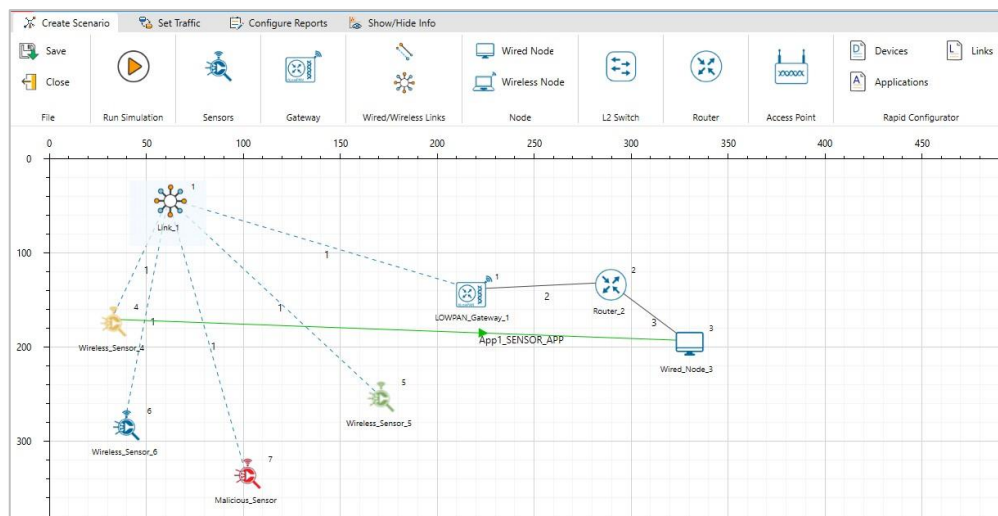


Figure 2: Network Setup of Sinkhole Attack in IOT RPL

3. In Ad-hoc link set the Channel Characteristics: **Pathloss Only**, Pathloss Model: **Log Distance**, Pathloss Exponent: **2**
4. Enable the packet trace on the top ribbon and enable the Wireshark on all the devices
5. Run the simulation for 100 Seconds.

Results and discussion:

Open the **rplog.txt** file from the results dashboard window, then you will find the information about DODAG formation. For every DODAG, LoWPAN Gateway is the root of the DODAG.

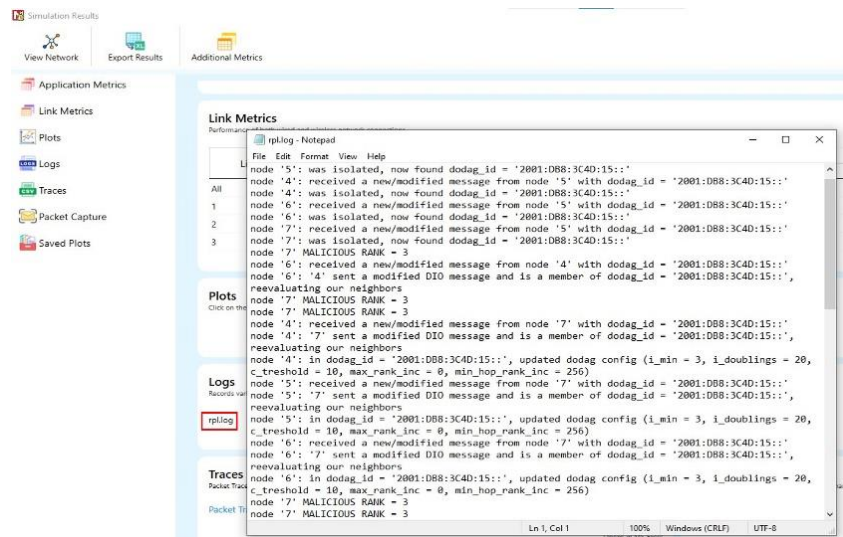


Figure 3: Result Dashboard Window

- Root is 1 with rank = 1 (Since the Node Id_1 is always LoWPAN Gateway)
- Wireless_Sensor_Node_7 (Malicious Node)
- Packet is 'transmitted' by **node 8(Sensor_8)** and is 'received' by **node 7(Sensor_7)** since node 7 is a **malicious node** it drops the packet. So, the Throughput in this scenario is 0.
- Open the packet trace file from the simulation results window and filter the **control packet Type/App Name** to **App1_Sensor_App**.
- Check the data packets flow, the Transmitter_ID, and receiver_ID column. Since node 7 is a malicious node, it drops the packet without forwarding it further.

PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID	APP_LAYER_ARRIVAL_TIME(μs)
177	5	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	4000
185	6	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	5000
194	7	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	6000
206	8	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	7000
221	9	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	8000
234	10	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	9000
252	11	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	10000
263	12	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	11000
272	13	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	12000
282	14	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	13000
301	15	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	14000
309	16	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	15000
322	17	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	16000
332	18	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	17000
340	19	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	18000
348	20	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	19000
359	21	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	20000
368	22	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	21000
377	23	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	22000
385	24	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	23000
394	25	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	24000
403	26	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	25000
416	27	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	26000
426	28	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	27000
437	29	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	28000
446	30	0 Sensing	App1_SENSOR_APP	SENSOR-4	NODE-3	SENSOR-4	SENSOR-7	29000

Figure 4: NetSim Packet Trace Window

Introducing multiple malicious nodes:

To introduce the multiple malicious nodes in the network, consider a larger network consisting of more sensors and with multiple sensor devices generating traffic. Malicious nodes can be distributed in different locations of the network and their impact on the network can be analysed.

1. Add one more sensor i.e., Sensor_9 for a similar scenario and create traffic as shown below.

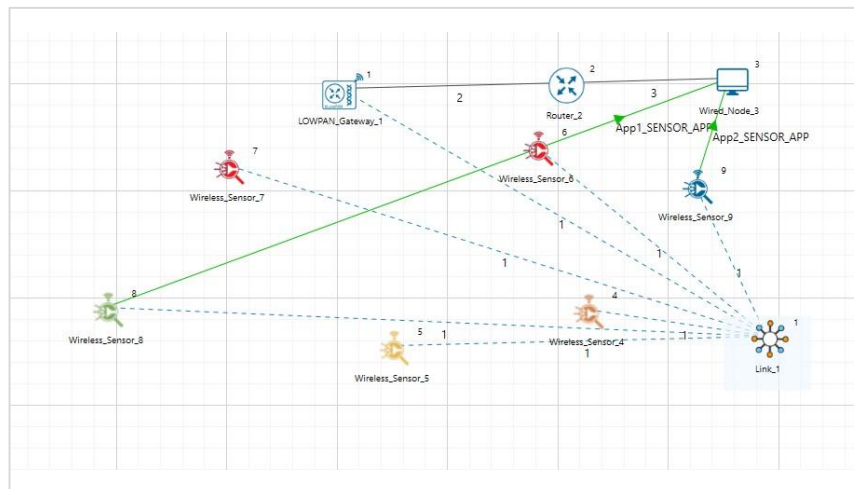
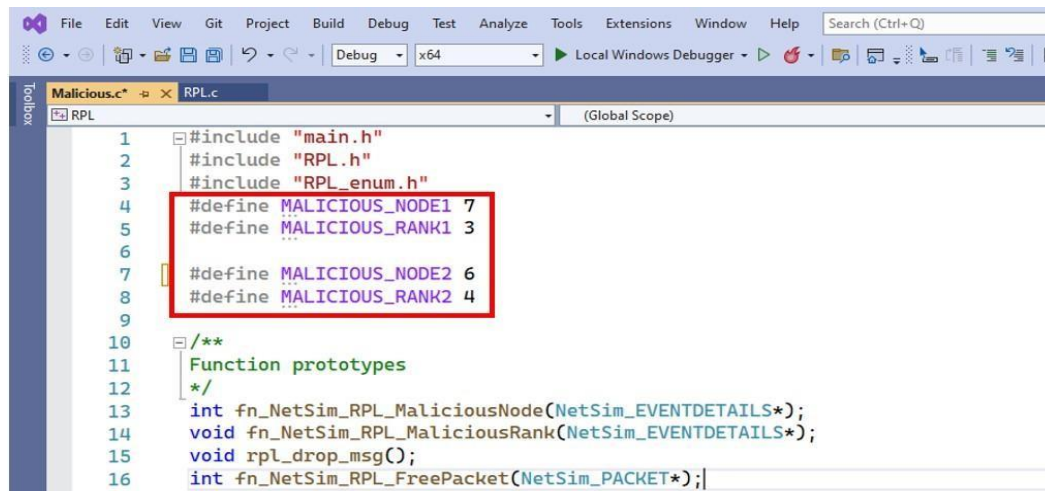


Figure 5: IoT Network Topology for multiple malicious nodes

2. Make sure that the Routing protocol in the added sensor is same as the network configured.
3. Consider sensors 6 and 7 as malicious nodes with fake rank by defining them in the `Malicious.c` at RPL Project file as shown below.



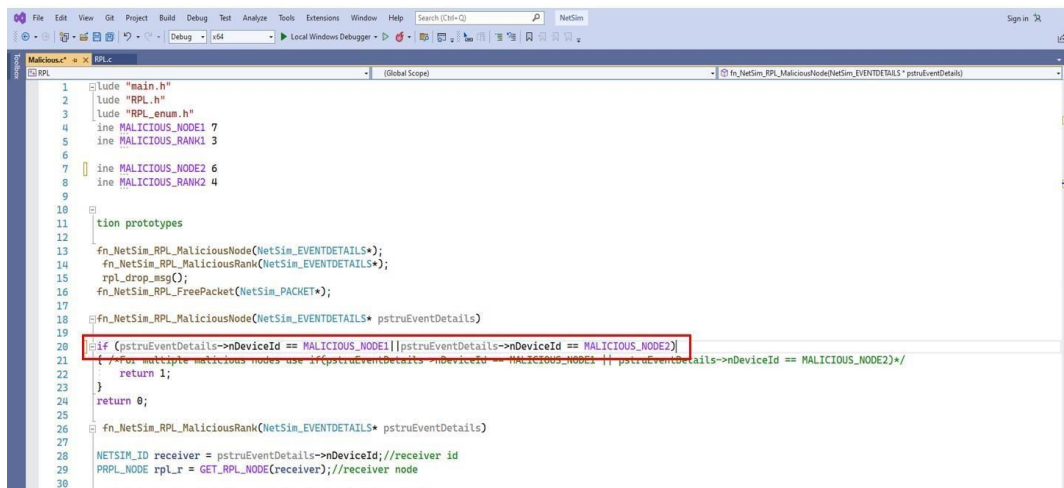
```

1  #include "main.h"
2  #include "RPL.h"
3  #include "RPL_enum.h"
4  #define MALICIOUS_NODE1 7
5  #define MALICIOUS_RANK1 3
6
7  #define MALICIOUS_NODE2 6
8  #define MALICIOUS_RANK2 4
9
10 /**
11  *Function prototypes
12  */
13  int fn_NetSim_RPL_MaliciousNode(NetSim_EVENTDETAILS*);
14  void fn_NetSim_RPL_MaliciousRank(NetSim_EVENTDETAILS*);
15  void rpl_drop_msg();
16  int fn_NetSim_RPL_FreePacket(NetSim_PACKET*);

```

Figure 6: Defining malicious nodes in Malicious.c file

4. In **fn_NetSim_RPL_MaliciousNode()** function, the if condition for checking malicious nodes needs to be updated.



```

1  #include "main.h"
2  #include "RPL.h"
3  #include "RPL_enum.h"
4  #define MALICIOUS_NODE1 7
5  #define MALICIOUS_RANK1 3
6
7  #define MALICIOUS_NODE2 6
8  #define MALICIOUS_RANK2 4
9
10 /**
11  *Function prototypes
12  */
13  int fn_NetSim_RPL_MaliciousNode(NetSim_EVENTDETAILS*);
14  void fn_NetSim_RPL_MaliciousRank(NetSim_EVENTDETAILS*);
15  void rpl_drop_msg();
16  int fn_NetSim_RPL_FreePacket(NetSim_PACKET*);
17
18  int fn_NetSim_RPL_MaliciousNode(NetSim_EVENTDETAILS* pstruEventDetails)
19  {
20  if (pstruEventDetails->nDeviceId == MALICIOUS_NODE1 || pstruEventDetails->nDeviceId == MALICIOUS_NODE2)
21  {
22  // For multiple malicious nodes use if(pstruEventDetails->nDeviceId == MALICIOUS_NODE1 || pstruEventDetails->nDeviceId == MALICIOUS_NODE2)
23  return 1;
24  }
25  return 0;
26  }
27
28  void fn_NetSim_RPL_MaliciousRank(NetSim_EVENTDETAILS* pstruEventDetails)
29  {
30  NETSIM_ID receiver = pstruEventDetails->nDeviceId; //receiver id
31  PRPL_NODE rpl_r = GET_RPL_NODE(receiver); //receiver node
32  }

```

Figure 7: If condition for checking multiple malicious nodes 5.

Now right click on Solution explorer and select Rebuild.

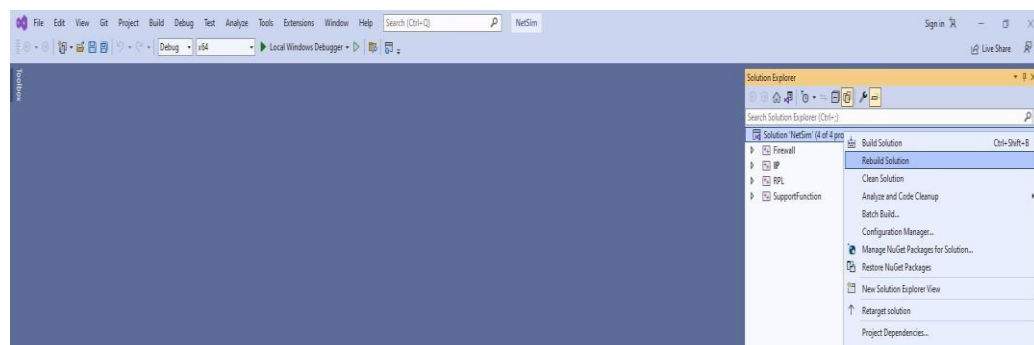
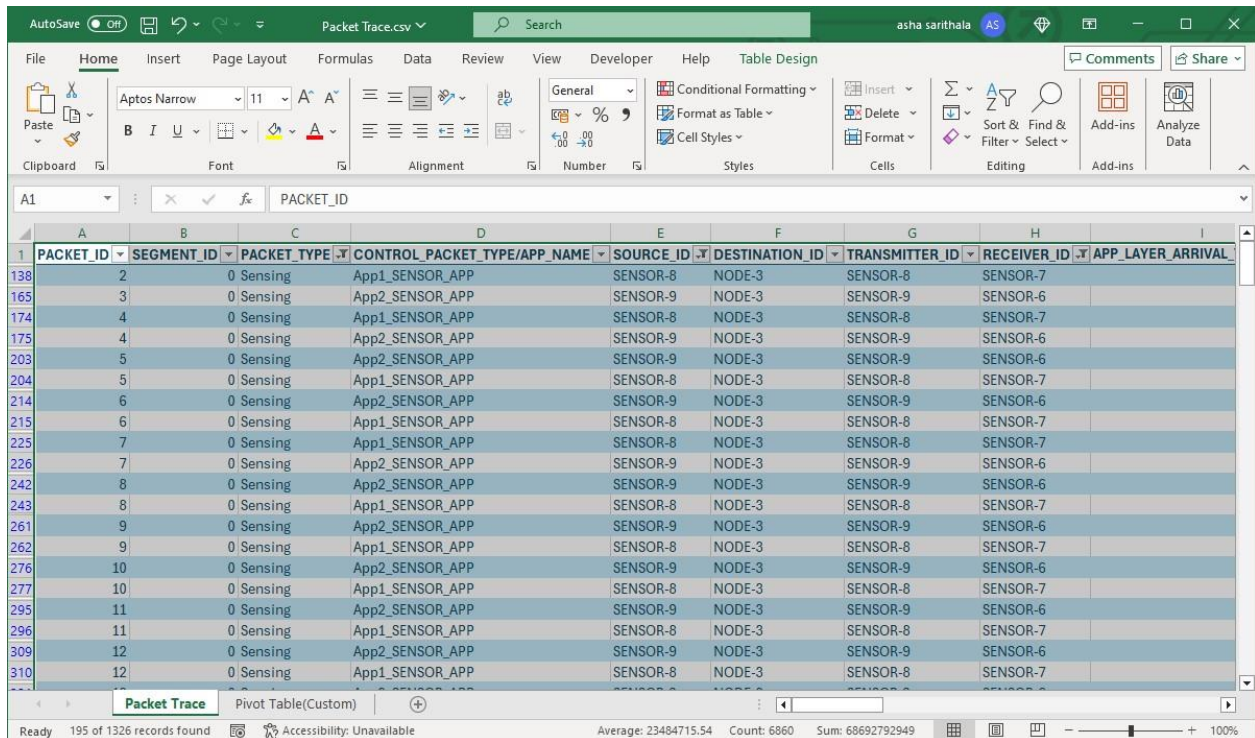


Figure 8: solution Explorer rebuild.

Results and discussion:

Sensor 8 will consider sensor 7 as a parent and sensor 9 will consider sensor 6 as a parent instead of sensor 4 since sensor 6 advertises a lower rank compared to sensor 4. Packets that reach sensors 7 and 6 get dropped. Results can be visualized in the rpllog.txt and packet trace.



The screenshot shows the NetSim packet trace window, which is a Microsoft Excel spreadsheet. The spreadsheet contains a table with the following columns: PACKET_ID, SEGMENT_ID, PACKET_TYPE, CONTROL_PACKET_TYPE/APP_NAME, SOURCE_ID, DESTINATION_ID, TRANSMITTER_ID, RECEIVER_ID, and APP_LAYER_ARRIVAL. The data is organized into rows, with the first row (row 1) serving as the header. The subsequent rows (rows 2 through 12) contain data for various packets, including their IDs, segment IDs, types, and the source and destination IDs. The status of each packet is listed in the APP_LAYER_ARRIVAL column.

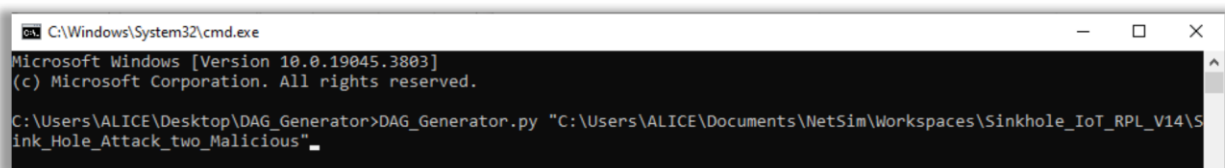
PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID	APP_LAYER_ARRIVAL
138	2	0 Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7	
165	3	0 Sensing	App2_SENSOR_APP	SENSOR-9	NODE-3	SENSOR-9	SENSOR-6	
174	4	0 Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7	
175	4	0 Sensing	App2_SENSOR_APP	SENSOR-9	NODE-3	SENSOR-9	SENSOR-6	
203	5	0 Sensing	App2_SENSOR_APP	SENSOR-9	NODE-3	SENSOR-9	SENSOR-6	
204	5	0 Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7	
214	6	0 Sensing	App2_SENSOR_APP	SENSOR-9	NODE-3	SENSOR-9	SENSOR-6	
215	6	0 Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7	
225	7	0 Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7	
226	7	0 Sensing	App2_SENSOR_APP	SENSOR-9	NODE-3	SENSOR-9	SENSOR-6	
242	8	0 Sensing	App2_SENSOR_APP	SENSOR-9	NODE-3	SENSOR-9	SENSOR-6	
243	8	0 Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7	
261	9	0 Sensing	App2_SENSOR_APP	SENSOR-9	NODE-3	SENSOR-9	SENSOR-6	
262	9	0 Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7	
276	10	0 Sensing	App2_SENSOR_APP	SENSOR-9	NODE-3	SENSOR-9	SENSOR-6	
277	10	0 Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7	
295	11	0 Sensing	App2_SENSOR_APP	SENSOR-9	NODE-3	SENSOR-9	SENSOR-6	
296	11	0 Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7	
309	12	0 Sensing	App2_SENSOR_APP	SENSOR-9	NODE-3	SENSOR-9	SENSOR-6	
310	12	0 Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7	

Figure 9: NetSim packet trace window.

You can also check the distribution of ranks with the help of the DODAG visualizer-

Downloaded workspace contains “DAG_Generator.py” file ,Go to the “DAG_Generator.py” file path, open the command line interface ,Run the “py” file by providing the path of saved RPL experiment with packet trace enabled. (not understandable how to run needed more explanation)

<https://support.tetcos.com/support/solutions/articles/14000134056-how-to-visualize-the-rpl-dodag-in-netsim-iot-simulations->



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ALICE\Desktop\DAG_Generator>DAG_Generator.py "C:\Users\ALICE\Documents\NetSim\Workspaces\Sinkhole_IoT_RPL_V14\Sink_Hole_Attack_two_Malicious"
```

Note: please ensure that wireshark and packet trace are enabled, and that the pandas, network, and matplotlib packages are installed before running the script.

The DODAG plots appear vertically flipped when compared to the network topology in NetSim since the origin (0,0) is at the top left in NetSim whereas it is at the bottom left in the plot window.

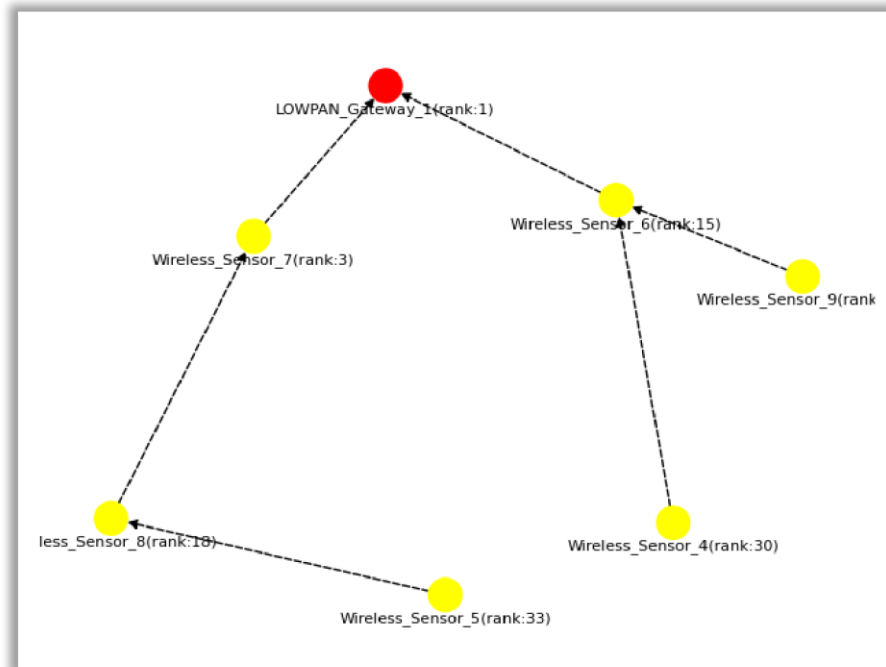


Figure 9: RPL DODAG Visualizer

Note: Conditions for Malicious node to be able to attract other legitimate nodes: •

The malicious node should be within the range of other nodes.

- The malicious nodes' DIO broadcast should be received by other nodes with a rank lower than other DIO messages received.

Appendix: NetSim source code modifications

Set malicious node id and the fake Rank in **Malicious.c** file which is present under **RPL** project

```
#include "main.h"
#include "RPL.h"
#include "RPL_enum.h"
#define MALICIOUS_NODE1 7
#define MALICIOUS_RANK1 3

#define MALICIOUS_NODE2 6
```

```
#define MALICIOUS_RANK2 4
```

Code changes done in **fn_NetSim_RPL_Run()**, in **RPL.c** file, within RPL project

```
_declspec (dllexport) int fn_NetSim_RPL_Run()
{
    switch (pstruEventDetails->nEventType)
    {
        case
NETWORK_OUT_EVENT:
        {
        }
        break;
        case
NETWORK_IN_EVENT:
        {
            rpl_add_to_neighbor_list();
            if
(is_rpl_control_packet(pstruEventDetails->pPacket))
            {
                if (fn_NetSim_RPL_MaliciousNode(pstruEventDetails))
                fn_NetSim_RPL_MaliciousRank(pstruEventDetails);
            }
            else
            {
                rpl_process_ctrl_msg();
                fn_NetSim_Packet_FreePacket(pstruEventDetails->pPacket);
                pstruEventDetails->pPacket = NULL;
            }
            else if (pstruEventDetails->nPacketId &&
fn_NetSim_RPL_MaliciousNode(pstruEventDetails))
            {
                rpl_drop_msg();
            }
        }
        break;
    }
}
```