**Sink Hole Attack using RPL in IOT**

**Software:** NetSim Standard v13.2, Visual Studio 2022

**Project Download Link:**

**Project link needs to be updated along with the how to download the project link**

**Introduction**

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

Sinkhole attacks affect the performance of IoT networks protocols such as RPL protocol.

|  |  |
| --- | --- |
| Figure : network configuration of how the traffic flow is configured | Figure Network configuration of actual traffic flow along with the working of malicious node |

**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, rank and sends a DAO message with route information.
* Malicious node upon receiving the DIO message it does not update the rank instead it always advertises a fake rank.
* The other node on listening to the malicious node DIO message the update their rank according to the fake rank.
* After the formation of DODAG, if the node that is transmitting the packet has malicious node as the preferred parent, transmits the packet to it but the malicious node instead of transmitting the packet to its parent, it simply drops the packet resulting in zero throughput.

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 into 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 sink hole 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 id’s of malicious nodes can be set inside the **fn\_NetSim\_RPL\_MaliciousNode()** function.

**Example**

1. The **WorkSpace\_SinkHole\_Attack\_RPL** comes with a sample network configuration that are 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
   1. **5** Wireless Sensors
   2. **1** 6\_LOWPAN Gateway
   3. **1** Router
   4. **1** Wired Node

Chart, line chart

Description automatically generated

Figure 4: IoT Network Topology

1. Channel Characteristics: **Pathloss Only,** Pathloss Model: **Log Distance,** Pathloss Exponent: **2**
2. Run the simulation for 100 Seconds.

**Results and discussion**

Open **rpllog.txt** file from the results dashboard window, then you will find the information about DODAG formation. For every DODAG, 6LoWPAN Gateway is the root of the DODAG.

Graphical user interface, application

Description automatically generated

Figure 5: Result Dashboard Window

* Root is 1 with rank = 1 (Since the Node Id\_1 is always 6LoWPAN Gateway)
* Wireless\_Sensor\_Node\_7 (Malicious Node)
* Packet is ‘transmitted’ by **node 8(Sensor\_8)** is ‘received’ by **node 7(Sensor\_7)** since the node 7 is **malicious node** it drops the packet. So, the Throughput in this scenario is 0.
* Open packet trace file from 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 the node 7 is malicious node, it drops the packet without forwarding it further.

Table

Description automatically generated

Figure 6: NetSim Packet Trace

**Introducing multiple malicious nodes:**

To introduce the multiple malicious nodes in the network, consider a larger network consisting of more of 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 analyzed.

1. Add one more sensor i.e., Sensor\_9 for the similar scenario and create traffic as shown below.

Chart, line chart

Description automatically generated

Figure 7: IoT Network Topology for multiple malicious nodes

1. Make sure that the Routing protocol in the added sensor is same as the network configured.
2. Consider sensor 6 and 7 as malicious nodes with fake rank by defining it in the Malicious.c file as shown below.

Graphical user interface, text, application

Description automatically generated

Figure 8: Defining malicious nodes in Malicious.c file

1. In **fn\_NetSim\_RPL\_MaliciousNode()** function, the if condition for checking malicious nodes needs to be updated.

Graphical user interface, text, application, email

Description automatically generated

Figure 9:If condition for checking multiple malicious nodes

1. Now right click on Solution explorer and select Rebuild.

Graphical user interface

Description automatically generated

Figure 10: solution Explorer rebuild

**Results and discussion**

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

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

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

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 in the bottom left in the plot window.

A picture containing ball, indoor, hitting, yellow

Description automatically generated

Figure 11: 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;