Sink Hole Attack using RPL in IOT

Software Recommended: NetSim Standard v11.0, Visual Studio 2015/2017
Project Download Link:
https://github.com/NetSim-TETCOS/SINK_HOLE_RPL_v11.0/archive/master.zip

In sinkhole Attack, a compromised node or malicious node advertises fake rank information to form the fake routes. After receiving the message packet it drop the packet information. Sinkhole attacks affect the performance of IoT networks protocols such as RPL protocol.

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

1. `fn_NetSim_RPL_MaliciousNode( )`
   This function is used to identify whether a current device is malicious or not in-order to establish malicious behaviour.
2. `fn_NetSim_RPL_MaliciousRank( )`
   This function is used to give a fake rank to the malicious node.
3. `rpl_drop_msg( )`
   This function is used to drop the packet by the malicious node if it enters into its network layer.

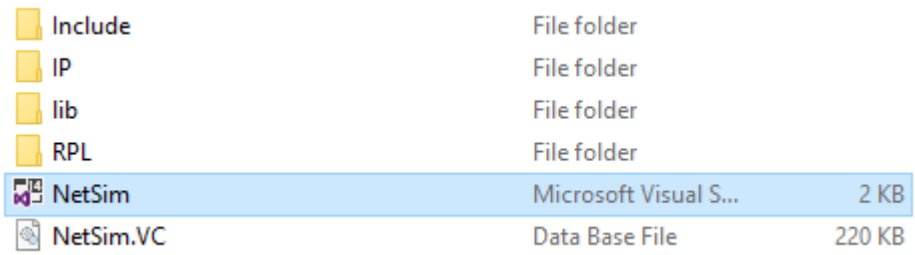
Sink Hole attack – The malicious node advertises the fake rank.
`fn_NetSim_RPL_MaliciousRank( )` is the sink hole attack function.

Black Hole attack – The malicious node drops the packet.
`rpl_drp_msg()` is the black hole attack function

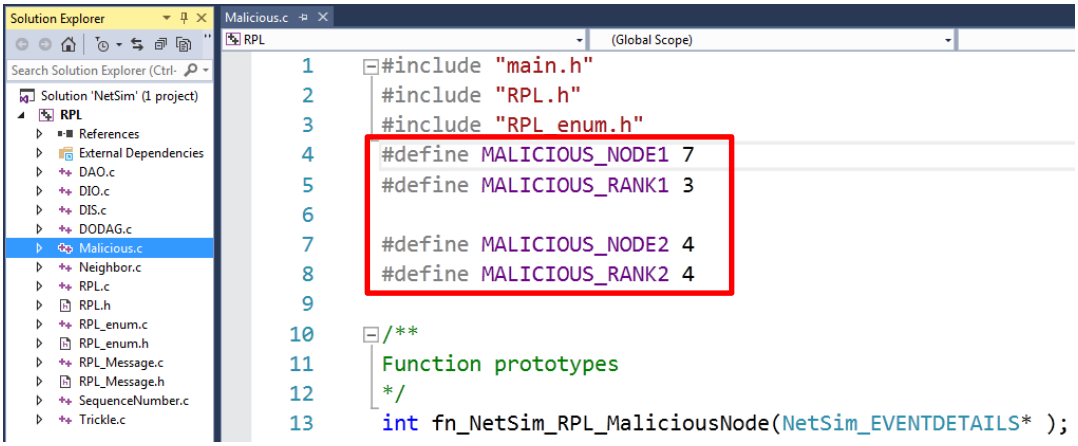
You can set any device as malicious and you can have more than one malicious node in a scenario.
Device id's of malicious nodes can be set inside the fn_NetSim_RPL_MaliciousNode() function.

Steps:

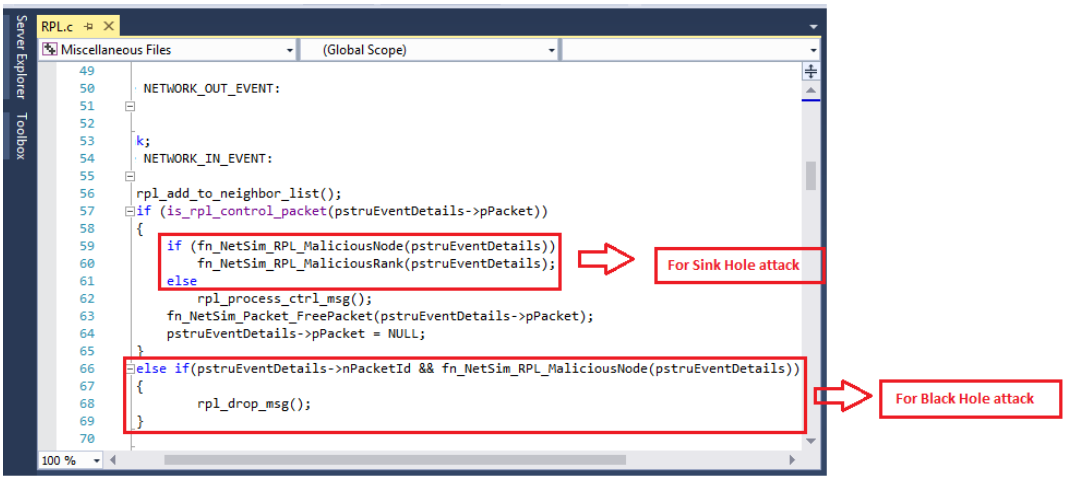
1. Open the Code folder and double click on the NetSim.sln fie to open the project in Visual Studio 2015**.**



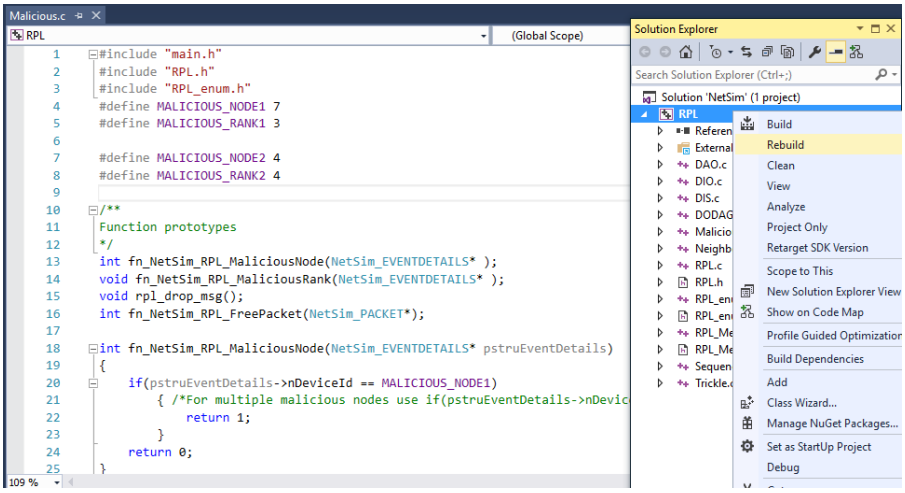
2. Set malicious node id and the fake rank.



3. Add the code that is highlighted in RPL.c file

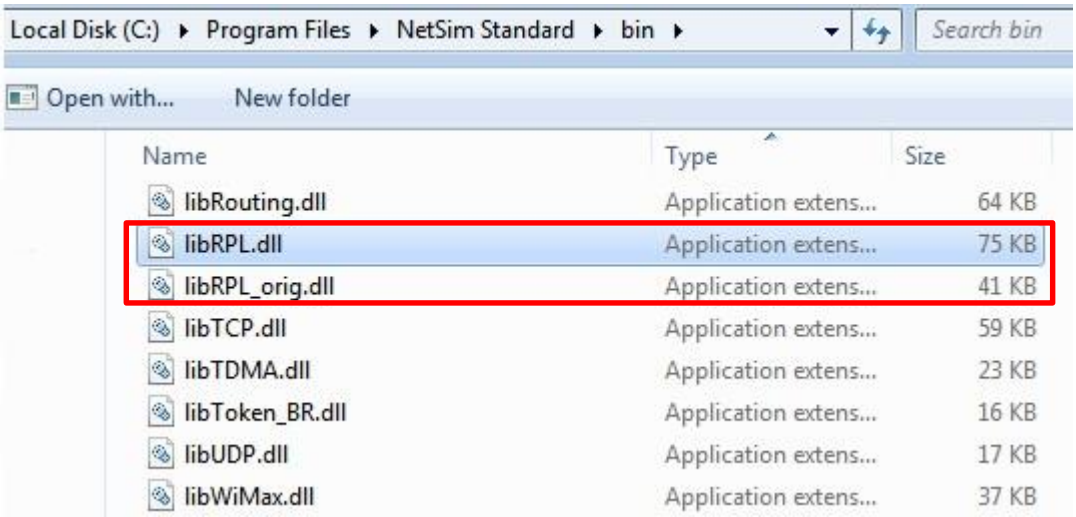


4. Now right click on RPL project in the solution explorer and select Rebuild.



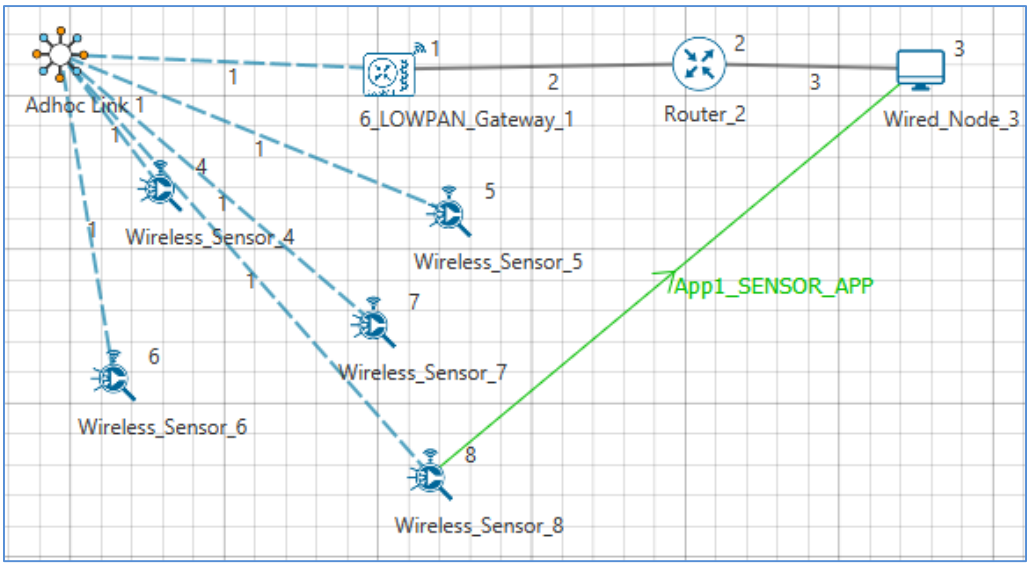
5. Now Copy the newly built libRPL.dll from the DLL folder inside the Simulation – Sinkhole Attack directory.

6. Replace the DLL in NetSim bin folder in the NetSim installation directory, after renaming the original libRPL.dll file.



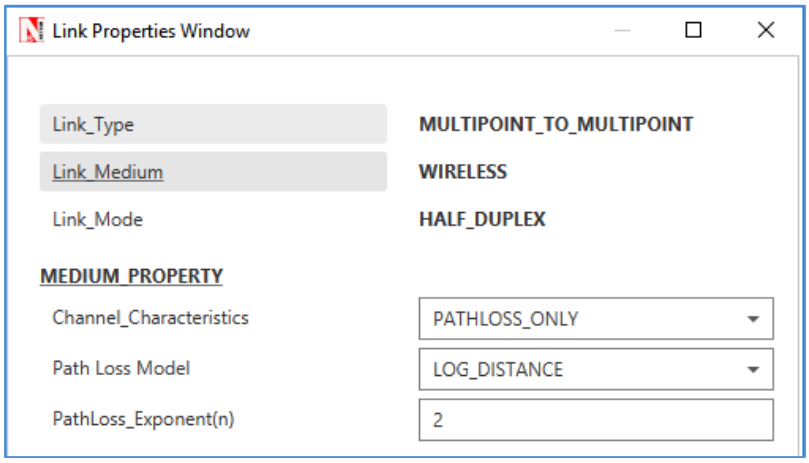
7. Create a network scenario in **IoT (Internet of Things) with UDP running in the Transport Layer and RPL in Network Layer.**

8. For example, you can create a scenario as shown in the following screenshot:



Environment Properties:

- Right click anywhere on the Environment Grid and select Properties.
- Select the Channel Characteristics and set the parameters accordingly.



Output

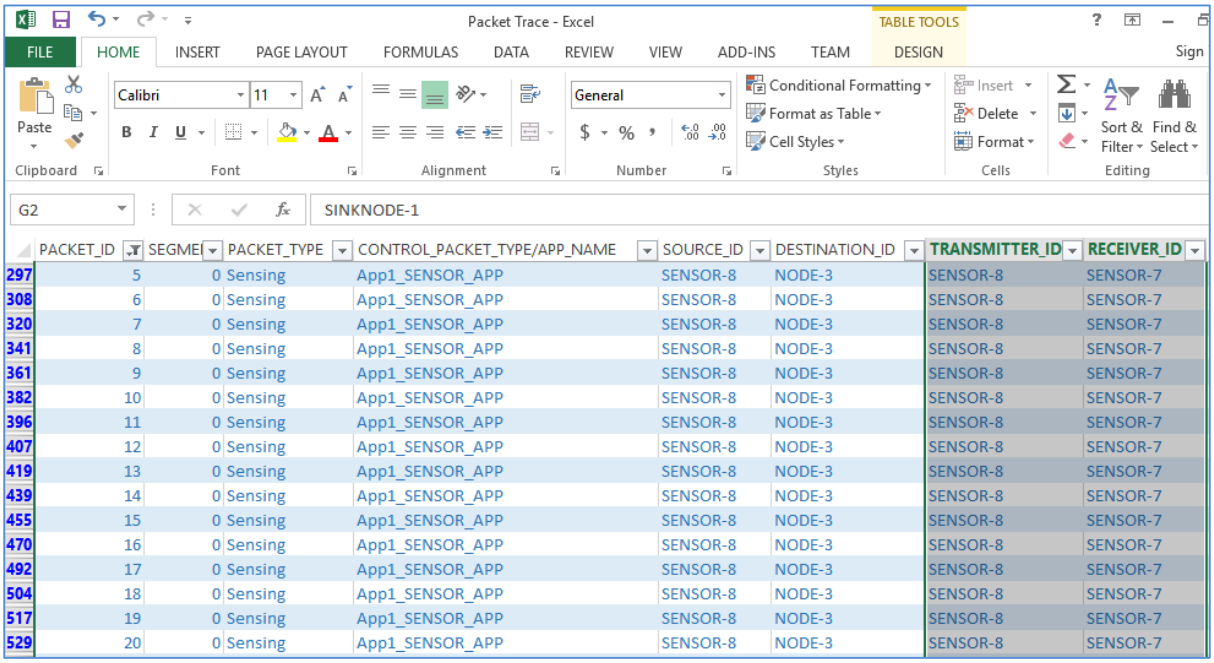
- Press + R and type %temp%, Temp folder will be opened.
- In Temp folder you will find a folder named NetSim.
- In NetSim, you will find a txt file named rpllog.txt

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

- Root is 1 with rank = 1 (Since the Node Id_1 is 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 only the data packets now check the **Transmitter_Id and receiver_Id** column. Since the node 7 is malicious node it drops the packet without forwarding it further.



	PACKET_ID	SEGME	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID
297	5	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
308	6	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
320	7	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
341	8	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
361	9	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
382	10	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
396	11	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
407	12	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
419	13	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
439	14	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
455	15	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
470	16	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
492	17	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
504	18	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
517	19	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
529	20	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7