Sink Hole Attack using RPL in IOT

Software Recommended: NetSim Standard v12.1 (32-bit/ 64-bit), Visual Studio 2017/2019

Follow the instructions specified in the following link to clone/download the project folder from GitHub using Visual Studio:

https://tetcos.freshdesk.com/support/solutions/articles/14000099351-how-to-clone-netsim-file-exchange-project-repositories-from-github-

Other tools such as GitHub Desktop, SVN Client, Sourcetree, Git from the command line, or any client you like to clone the Git repository.

Note: It is recommended not to download the project as an archive (compressed zip) to avoid incompatibility while importing workspaces into NetSim.

Secure URL for the GitHub repository:

https://github.com/NetSim-TETCOS/SINKHOLE_ATTACK_IN_RPL_v12.1.git

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. After you unzip the downloaded project folder, Open NetSim Home Page click on **Open Simulation** option,

| 🚺 NetSim Home | | | - 🗆 X |
|---|--|---|--|
| NetSim Standard Network Simulation/Emulation Platfor Version 12.1.21 (64 Bit) | m | | www.tetcos.com |
| | Current workspace: WorkSpace_SinkHole_Attack_RPL | | |
| New Simulation Ctrl+N | Choose a Network | | |
| Open Simulation Ctrl+O | Internetworks | LTE/LTE-A Networks | |
| openomulation | Pure Aloha | LTE FemtoCell | |
| Examples | Slotted Aloha | LTE D2D | |
| | GSM | LTE VANET | |
| | CDMA | VANET | |
| | Mobile Adhoc Networks | 5G NR mmWave | |
| | Wireless Sensor Networks | Satellite Comm. Networks | |
| License Settings | Internet of Things | | |
| | Cognitive Radio Networks | | |
| EXIT | | | |
| | | | |
| | | | |
| | | | |
| Support | Learn | Documentation | Contact us |
| Answers/FAQ Contact Technical Support Email - support@tetcos.com | Videos Experiments Manual | User Manual Technology Libraries Source Code Help | Email - sales@tetcos.com Phone - +91 767 605 4321 |

2. Click on Workspace options

| 🚺 NetSim Home | | | | | - 🗆 X |
|--|------------------------------------|-------------------|--|------------------------------|-----------------------------|
| NetSim Standard Network Simulation/Emulation Plat Version 12.1.21 (64 Bit) | d tform | | | | www.tetcos.com |
| | Current workspace: WorkSpace_Sink+ | | C Experiment name | | |
| New Simulation Ctrl+N | Experiment name | Date modified | Network type | | |
| Open Simulation Ctrl+O | | | | | |
| Examples | | | | | |
| | | | | | |
| | | | | | |
| | | No experiments cu | irrently saved in the wo | orkspace | |
| License Settings | | | | | |
| Exit | | | | | |
| | | | | | |
| | | | | | |
| | Workspace options | | | In | nport Experiment |
| Support | Learn | [| Documentation | Contact us | |
| Answers/FAQ Contact Technical Support Email - support@tetcos.com | Videos Experiments Manual | U Ti Si | ser Manual echnology Libraries ource Code Help | Email - sales Phone - +91 | @tetcos.com 767 605 4321 |

3. Click on More Options,

| NetSim Home | | | | | - 🗆 X | | |
|--|-------------------------------------|---|---|----------------------------|----------------------------------|--|--|
| NetSim Standard Network Simulation/Emulation Platfo Version 12.1.21 (64 Bit) | orm | | | | www.tetcos.com | | |
| | Current workspace: WorkSpace_SinkHo | le_Attack_RPL | | C Experiment name | | | |
| New Simulation Ctrl+N | Experiment name | Date modified | Network type | | | | |
| Open Simulation Ctrl+O | | | | | | | |
| Examples | | | | | | | |
| | | No experiments currently saved in the workspace | | | | | |
| License Settings | | | | | | | |
| Exit | | | | | | | |
| | | | | | | | |
| | Open code Reset Code | Reset Binarie | s More optic | ons | Back | | |
| Support | Learn | | Documentation | Contact u | 5 | | |
| Answers/FAQ Contact Technical Support Email - support@tetcos.com | Videos Experiments Manual | L T S | lser Manual echnology Libraries ource Code Help | Email - sale Phone - +9 | :s@tetcos.com)1 767 605 4321 | | |

4. Click on **Import**, browse the extracted folder path and go into the WorkSpace_SinkHole_Attack_RPL directory. Click on Select folder button and then on **OK**.

| N Select Folder | | | | | | | × |
|----------------------|---|----------------------|-------------|----------|-------------------|-----------|---|
| ← → × ↑ 📙 > Thi | s PC > Desktop > File exchange projects_v12.1 | > SINKHOLE_ATTACK_IN | _RPL_v12.1 | <u>ت</u> | Search SINKHOLE_A | ATTACK_IN | ρ |
| Organize 👻 New folde | r | | | | | | ? |
| Documentation ^ | Name | Date modified | Туре | Size | | | |
| MGIT, Hyderaba | | 11-03-2020 15:43 | File folder | | | | |
| OneDrive | WorkSpace_SinkHole_Attack_RPL | 11-03-2020 15:44 | File folder | | | | |
| 💻 This PC | | | | | | | |
| 3D Objects | | | | | | | |
| E Desktop | | | | | | | |
| 🔮 Documents | | | | | | | |
| 🕹 Downloads | | | | | | | |
| 👌 Music | | | | | | | |
| Pictures | | | | | | | |
| 📑 Videos | | | | | | | |
| 🏪 Local Disk (C:) | | | | | | | |
| 🕳 Local Disk (E:) | | | | | | | |
| 🚛 New Volume (F:) 🗸 | | | | | | | |
| Folder | SINKHOLE_ATTACK_IN_RPL_v12.1 | | | | | | |
| | | | | | Select Folder | Cancel | |

5. Go to home page, Click on **Open Simulation > Workspace options** and click on the**Open code** button.

| 🚺 NetSim Home | | | - 🗆 X |
|--|---|---|--|
| NetSim Standard Network Simulation/Emulation Platfo Version 12.1.21 (64 Bit) | rm | | www.tetcos.com |
| | NetSim Home NetSim Standard Vetwork Simulation/Emulation Platform /ersion 12.1.21 (64 Bit) Current workspace: WorkSpace_SinkHole_At New Simulation Ctrl+N Open Simulation Ctrl+O Examples License Settings Exit Open code Reset Code Support Learn Answers/FAQ Contact Technical Support Email - support@tetcos.com | e_Attack_RPL | C Experiment name |
| New Simulation Ctrl+N | Experiment name | Date modified Network type | |
| Open Simulation Ctrl+O | | | |
| Examples | | | |
| | | No experiments currently saved in the w | orkspace |
| License Settings | | | |
| Exit | | | |
| | Open code Reset Code | Reset Binaries More optic | Back |
| Support | Learn | Documentation | Contact us |
| Answers/FAQ Contact Technical Support Email - support@tetcos.com | Videos Experiments Manual | User Manual Technology Libraries Source Code Help | Email - sales@tetcos.com Phone - +91 767 605 4321 |

6. Set malicious node id and the fake Rank.

| Solution Explorer 🔹 म 🗙 | Malicious.c 😕 🗙 | |
|---|-----------------|--|
| 000 10-500 | 🕾 RPL | - (Global Scope) - |
| Search Solution Explorer (Ctrl- 🔎 - | 1 | ⊟#include "main.h" |
| Solution 'NetSim' (1 project) | 2 | #include "RPL.h" |
| RPL Beferences | 3 | <pre>#include "RPL enum.h"</pre> |
| External Dependencies | 4 | #define MALICIOUS_NODE1 7 |
| ♦ ++ DAO.c ♦ ++ DIO.c | 5 | #define MALICIOUS_RANK1 3 |
| *+ DIS.c | 6 | |
| A DODAG.c A Malicious.c | 7 | #define MALICIOUS_NODE2 4 |
| ** Neighbor.c | 8 | #define MALICIOUS_RANK2 4 |
| P 🖻 RPL.h | 9 | |
| ▶ ++ RPL_enum.c ▶ ि RPL enum.h | 10 | ∃/** |
| ++ RPL_Message.c | 11 | Function prototypes |
| RPL_Message.h | 12 | */ |
| P *+ SequenceNumber.c ↓ *+ Trickle.c | 13 | <pre>int fn_NetSim_RPL_MaliciousNode(NetSim_EVENTDETAILS*);</pre> |

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

| 🖭 Miscellane | eous Files - (Global Scope) - | • |
|--------------|---|------------------|
| 49 | | + |
| 50 | NETWORK_OUT_EVENT: | A |
| 51 | | |
| 52 | | |
| 53 | k; | |
| 54 | NETWORK_IN_EVENT: | |
| 55 | | |
| 56 | <pre>rpl_add_to_neighbor_list();</pre> | |
| 57 | <pre>if (is_rpl_control_packet(pstruEventDetails->pPacket))</pre> | |
| 58 | { | |
| 59 | if (fn_NetSim_RPL_MaliciousNode(pstruEventDetails)) | |
| 60 | fn_NetSim_RPL_MaliciousRank(pstruEventDetails); For Sir | nk Hole attack |
| 61 | else | |
| 62 | <pre>rpl_process_ctrl_msg();</pre> | |
| 63 | <pre>fn_NetSim_Packet_FreePacket(pstruEventDetails->pPacket);</pre> | |
| 64 | <pre>pstruEventDetails->pPacket = NULL;</pre> | |
| 65 | } | |
| 66 | <pre>else if(pstruEventDetails->nPacketId && fn_NetSim_RPL_MaliciousNode(pstruEv</pre> | entDetails)) |
| 67 | { | For Black Hole : |
| 68 | rp1_drop_msg(); | POT Black Hole a |
| 69 | []} | |

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

| licious.c 🕫 🗙 | | | Solution Explorer | |
|------------------|--|----|-------------------------------------|----------|
| RPL | (Global Scope) · | | 0000.0.5000. | × - |
| 1 🗁#in | clude "mein.h" | ÷ | Search Solution Emplorer (Ctrl+-) | |
| 2 #10 | clude "RPL.n" | A | Solution 'NetSim' (2 of 2 projectr) | |
| 4 #de | Cable Priceson 1 | | Build Solution | Chile Sh |
| 5 #de | fine MALICIOUS RANKI 3 Rectangular Se | | Build Solution | CUI+3 |
| 6 | | | Rebuild Solution | |
| 7 #de | tine MALECOS ROBER A | | Clean Solution | |
| 9 | THE PREVENCE 4 | | Analyze and Code Cleanup | |
| 10 =/** | | | Batch Build | |
| 11 Fun | ction prototypes | | Configuration Manager | |
| 12 */ | | | Manage NuGet Packages for Solution | |
| 13 int | In NetSim RPL MaliclousHode(NetSim EVENTDETAILS*); | | Partore NuGet Backager | |
| 14 VOI | a In_Heclam_Heclam_Heclam_Control (Heclam_Control (Heclam_He | | | |
| 16 int | fn NetSim RPL FreePacket(NetSim PACKET*); | | New Solution Explorer View | |
| 17 | | | Calculate Code Metrics | |
| 18 ⊡int | <pre>fn_NetSim_RPL_MaliciousNode(NetSim_EVENTDETAILS* pstruEventDetails)</pre> | | | |
| 19 1 | (fforterEucetEntells_semand.etd -= NAUTCTONE NODEL) | | T Retarget solution | |
| 21 | <pre>// f // For multiple malicious = neelines_model; // * For multiple malicious = neelines_model == MALICIOUS NODE: pstruEventDetails->nDeviceId == MALICIOUS NODE:</pre> | */ | Project Dependencies | |
| 22 | return 1; | | Project Build Order | |
| 23 | } | | | |
| 24 | return 0; | | Add | |
| 25 [] 26 Evoi | d fa MatSim DDL MaliciaurDack/MatSim EVENTATIS* actor/EventActalic) | | Set StartUp Projects | |
| 27 { | | | 13 Add Solution to Source Control | |
| 28 | NETSIM ID receiver = pstruEventDetails->nDeviceId;//receiver id | | | |
| 29 | PRPL_NODE rpl_r = GET_RPL_NODE(receiver);//receiver node | | D Paste | Ctrl+ |
| 30 | | | E Rename | |
| 31 | switch (pstrucventuetalis->pracket->ncontroluatalype % 100) | 1 | Constanting File Final and | |

9. Upon rebuilding, **libRPL.dll**, **libIP.dll**,**SupportFunction.dll** and **Firewall.dll** will automatically get replaced in the respective bin folders of the current workspace

Note:

1. Based on whether you are using NetSim 32 bit or 64 bit setup you can configure Visual studio to build 32 bit or 64 bit Dll files respectively as shown below:

| ST File |) NetSim - Microsoft Visuel Studio (Administrator) • Edit View Project Build Debug Team Tools Test Analyze Window Help ○ - ⓒ [1] - ☆ I Debug - 1, 564 | V Quick Launch (Ctrl- | 0 P - 5 × namrata saraswat ~ NS |
|-------------------------|--|--|---|
| Server Explorer Toolbox | Win32 x64 Cooffguration Manager | Solution Explorer ● ① ① ① ① ① ① ① ○ ○ ○ Search Solution Explorer (Ctr ① Solution Explorer (Ctr □ Solution Explorer (Str ● Sign Freevall ● Sign PPL | • 0 × 0 × 0 × 0 × 0 × 0 × 0 × 0 × 0 × 0 |
| | | Solution Explorer Team Exp | lorer |
| | | Properties | |
| | | IP Project Properties | * |
| | | 11 24 P | |
| | Output • # × | B Misc | |
| | Show output from: | (Name) | IP |
| | | Project Dependencies | |
| | | Project File | F:\v11.1_Project\SinkHole_Attack |
| | | Root Namespace | IP |
| | Error List Output | (Name) Specifies the project name. | |
| | | | ↑ Add to Source Control ▲ |
| - | 🛛 Type here to search 🕼 🛱 💼 🔒 🕿 😧 🥥 🗐 🕅 🥵 | # ^ % | ■ ¢× ENG 12:07 |

2. While importing the workspace, if the following warning message indicating Software Version Mismatch is displayed, you can ignore it and proceed.



10. Go to NetSim home page, click on **Open Simulation**, Click on **SinkHole_Attack_in_RPL_Example**.

| NetSim Home | | | | | | – 🗆 🗙 |
|---|--|--------------------------------|---------------|---|-------------------------|------------------------------------|
| NetSim St Network Simulation/E Version 12.1.21 (64 Bit | andard | orm | | | | www.tetcos.com |
| | Sim Home EtSim Standard vork Simulation Platform ion 12.1.21 (64 Bit) Current workspace: WorkSpace_SinkHole_Attack_RPL w Simulation Ctrl+N en Simulation Ctrl+O amples ense Settings t | | | | C Experiment name | |
| New Simulation | Ctrl+N | Experiment name | Date modified | Network type | | |
| Open Simulation | Ctrl+O | SinkHole_Attack_in_RPL_Example | 09-03-2020 | Internet_of_Things | View Results | Export 🔟 |
| Examples | | | | | | |
| | | | | | | |
| | | | | | | |
| License Cettings | | | | | | |
| License Settings | | | | | | |
| Exit | | | | | | |
| | | | | | | |
| | | Workspace options | | | | Import Experiment |
| Support | | Learn | | Documentation | Contact | us |
| Answers/FAQ Contact Technical Sup Email - support@tetco | oport os.com | Videos Experiments Manual | | User Manual Technology Libraries Source Code Help | Email - sa Phone - · | les@tetcos.com ⊧91 767 605 4321 |

Settings that were done to create the network scenario for SinkHole Attack:

- 1. Create a network scenario in IoT (Internet of Things) with UDP running in the Transport Layer and RPL in Network Layer.
- 2. For example, you can create a scenario as shown in the following screenshot:



Environment Properties:

- Right click on the Adhoc link icon and select Properties.
- Select the Channel Characteristics and set the parameters accordingly.

| 🚺 Link Properties Window | – 🗆 X |
|--------------------------|--------------------------|
| | |
| Link_Type | MULTIPOINT_TO_MULTIPOINT |
| Link_Medium | WIRELESS |
| Link_Mode | HALF_DUPLEX |
| MEDIUM PROPERTY | |
| Channel_Characteristics | PATHLOSS_ONLY - |
| Path Loss Model | LOG_DISTANCE - |
| PathLoss_Exponent(n) | 2 |

Output

Open **rpllog.txt** file from simulation results window,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)

| Nimulation Results | | | | | | | | |
|----------------------------|-------------|---------------------|---------------|------------------|-----------------|-------------------|-----------------|-------|
| ♥ Simulation Results | Queue_Me | Queue_Metrics_Table | | | | | | |
| Link_Metrics | Queue | Queue Metrics | | | Detailed View | | | |
| Queue_Metrics | Device id | Port id | Queued packs | t Dequeued pack | et Dropped pac | ket | | |
| TCP_Metrics | 1 | 1 | 13 | 13 | 0 | | | |
| IP_Metrics | 1 | 2 | 17 | 17 | 0 | | | |
| IP_Forwarding_Table | 2 | 1 | 16 | 16 | 0 | | | |
| UDP Metrics | 2 | 2 | 0 | 0 | 0 | | | |
| IEEE802.15.4_Metrics | - | | | | | | | |
| Battery model | | | | | | | | |
| Application_Metrics | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| Export Results (.xls/.csv) | | | | | | | | |
| Print Results (.html) | | | | | | | | |
| | | | | | | | | |
| Open Packet Trace | Application | n_Metrics_ | Table | | | | | a × |
| | Applicat | tion_me | trics | Detai | ed View | | | |
| ✓ Log Files | Application | n Id App | lication Name | Packet generated | Packet received | Throughput (Mbps) | Delay(microsec) | Jitte |
| ospf.log | 1 | Арр | 1_SENSOR_APP | 100 | 0 | 0.000000 | 0.000000 | 0.000 |
| ospf Hello.log | | | | | | | | |
| ospf SPE.log | | | | | | | | |
| rollog | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

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.

| 1 | PACKET_ID 💌 | SEGMENT_ID 💌 | PACKET_TYPE | CONTROL_PACKET_TYPE | APP_NAME 🕶 SOURCE_ID 💌 | DESTINATION_ID | TRANSMITTER_ID | RECEIVER_ID |
|-----|-------------|--------------|-------------|---------------------|------------------------|----------------|----------------|-------------|
| 129 | 2 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 153 | 3 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 165 | 4 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 185 | 5 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 196 | 6 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 204 | 7 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 220 | 8 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 239 | 9 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 247 | 10 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 263 | 11 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 276 | 12 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 284 | 13 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 296 | 14 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 304 | 15 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 323 | 16 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| 338 | 17 | 0 | Sensing | App1_SENSOR_APP | SENSOR-8 | NODE-3 | SENSOR-8 | SENSOR-7 |
| - | | | | | | | | |