Intrusion detection system for LEACH

Software Recommended: NetSim Standard v12.2 32-bit/ 64-bit, Visual Studio 2019

The following steps show how a user can run the IDS in NetSim to detect a malicious node, and then setup a new route to the destination avoiding the malicious node

- Creating Malicious nodes for a particular network scenario is explained in Malicious.c file
- Clustering and cluster head election is explained in LEACH.c file
- To detect the intruder and to send data via a new route, the following files are added in DSR and Zigbee:
  - **Pathrater.c** :

    This file contains code for avoiding the malicious node and finding a new route (once the IDS detects the malicious node) in networks running DSR in Layer 3. Note that this system would work only for UDP and not for TCP, since TCP involves receiving ack's from the destination

    If _NETSIM_PATHRATER_ is defined, the code is used to validate routes. When the Node is a Malicious Node and a Route Reply is processed, the Function verifies the route reply in the route cache and checks for the black listed node i.e.,malicious node. When a malicious node is found, that route entry is deleted from the cache.

  - **Watchdog.c**

    This file contains code for the IDS and is added in Zigbee operating in Layer 3.

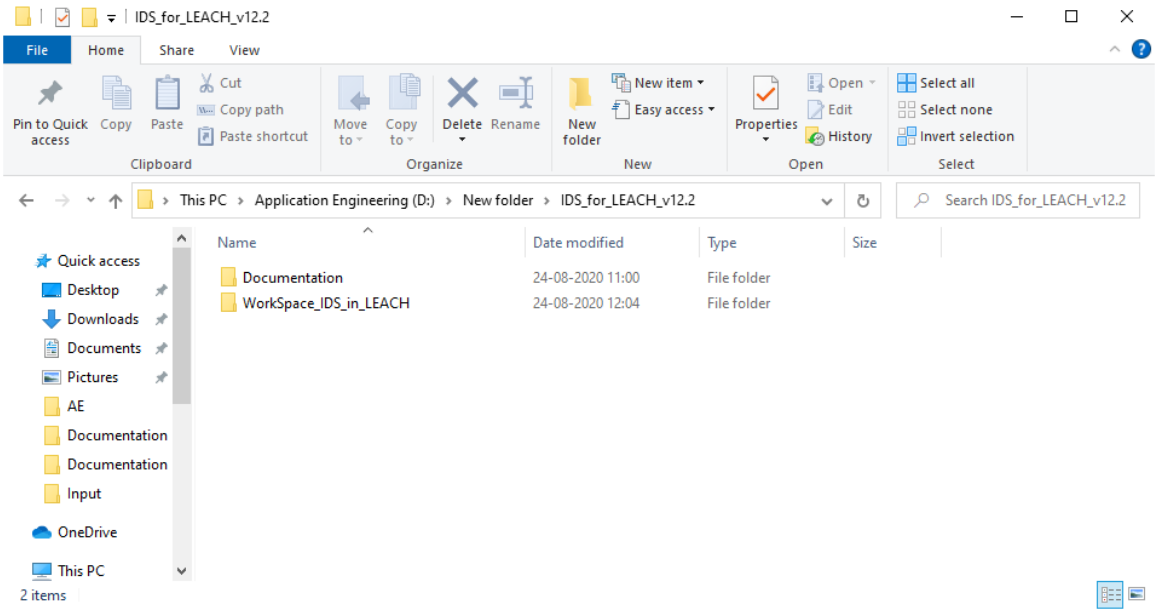
    If _NETSIM_WATCHDOG_ is defined, a watchdog timer starts the moment a packet is sent. Once a packet is forwarded to next hop node, the current node checks for watchdog timer duration if the packet is getting forwarded further on to destination node or not.

    The malicious node doesn't forward packets that it receives. The watchdog timer in the node (which forwarded the packet to the malicious node) expires. A counter is present which measures the number of times the watchdog timer expires (in other words the number of packets sent out but not forwarded by the next hop

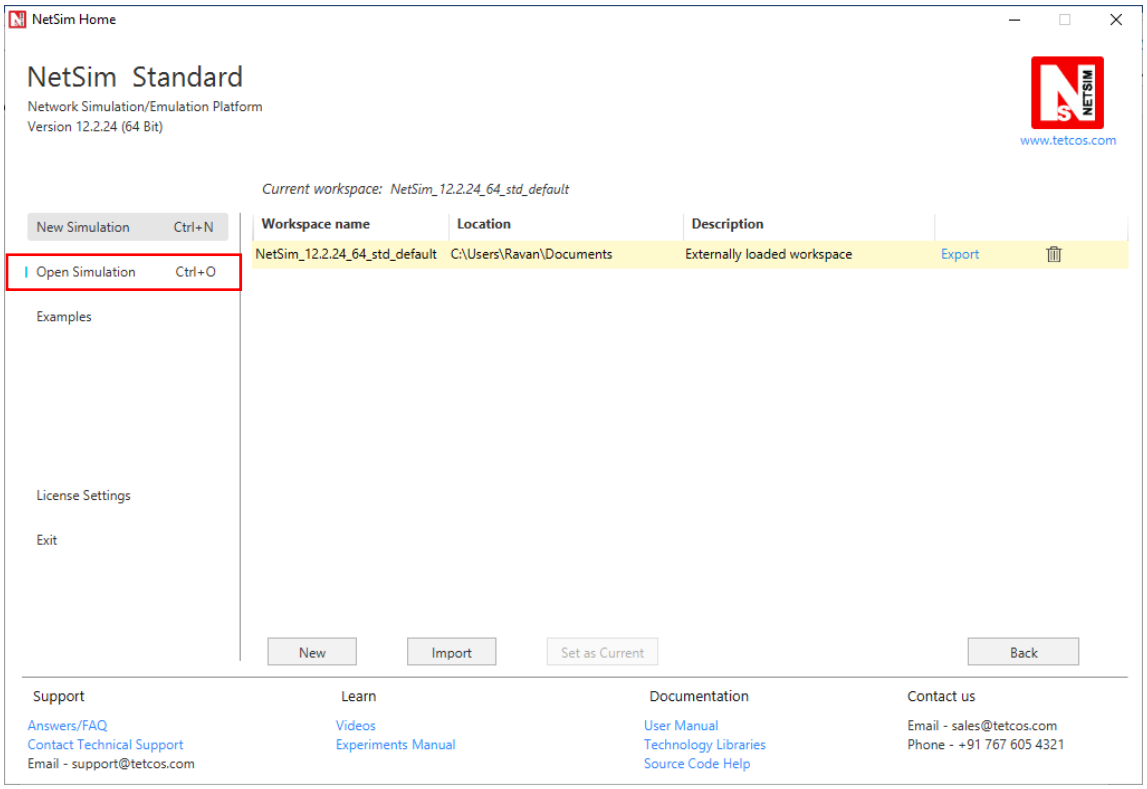
node). Once this counter's value reaches the failure threshold the next hope is marked by the current node as a malicious node.

Steps:

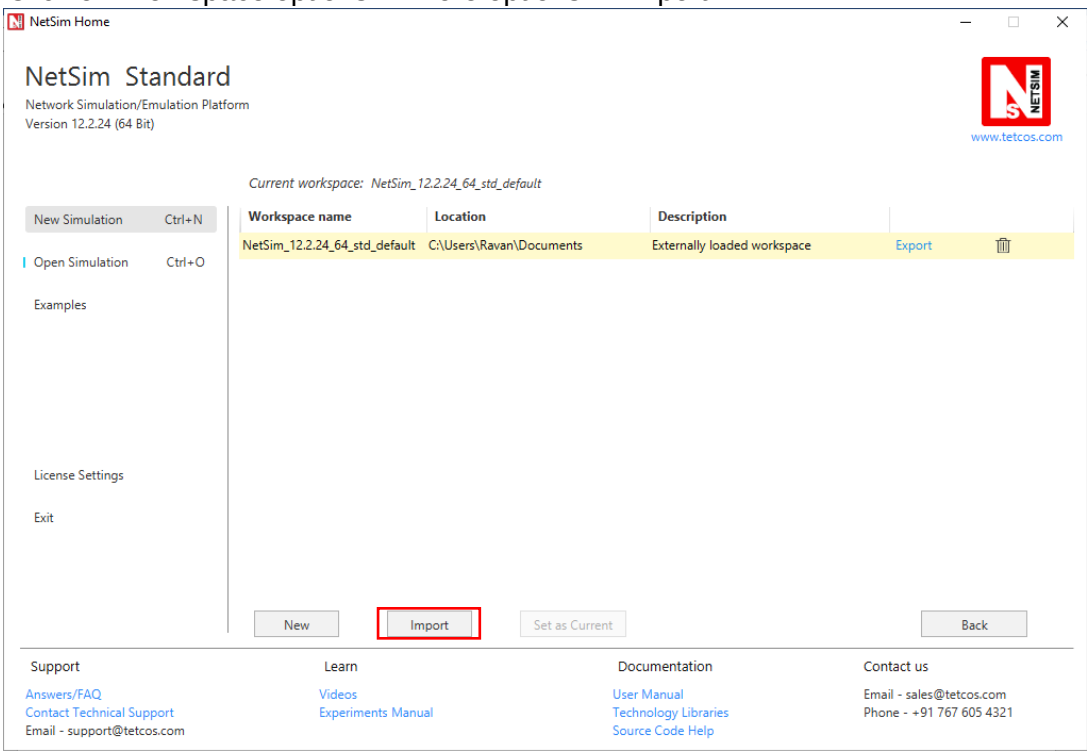
1. The downloaded project folder contains the folders Documentation, and Workspace_IDS_in_LEACH directory as shown below:



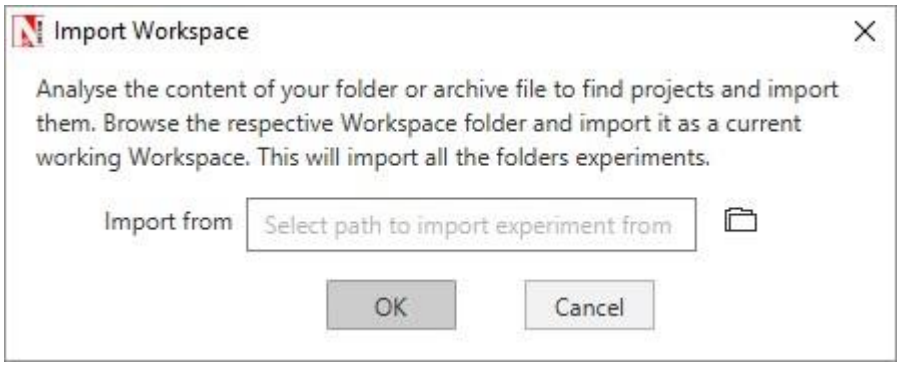
2. After you unzip the downloaded project folder, Open NetSim Home Page click on **Open Simulation** option,



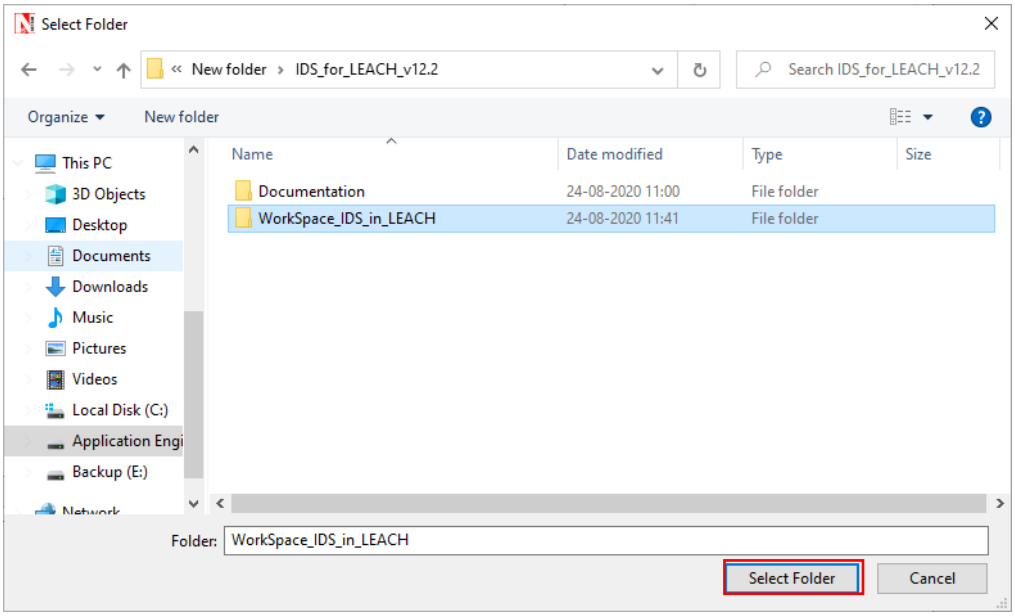
3. Click on Workspace options -> More options -> Import



4. It displays a window where users need to give the path of the workspace folder and click on OK as shown below:

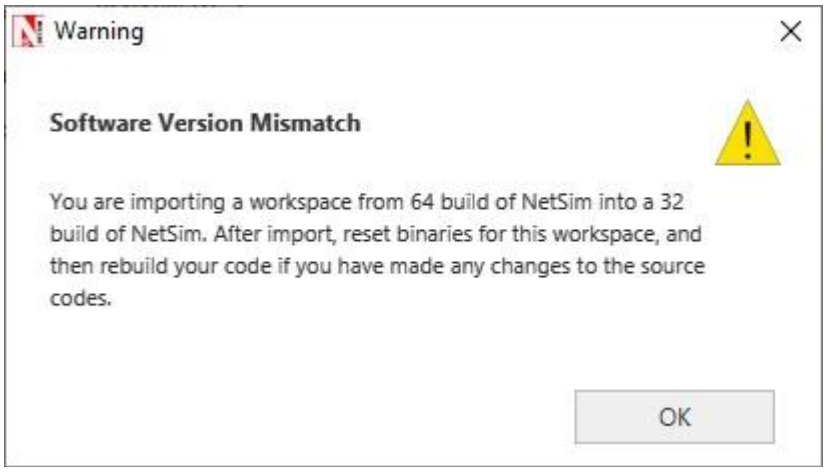


5. Browse to the Workspace_IDS_in_LEACH folder and click on select folder as shown below:

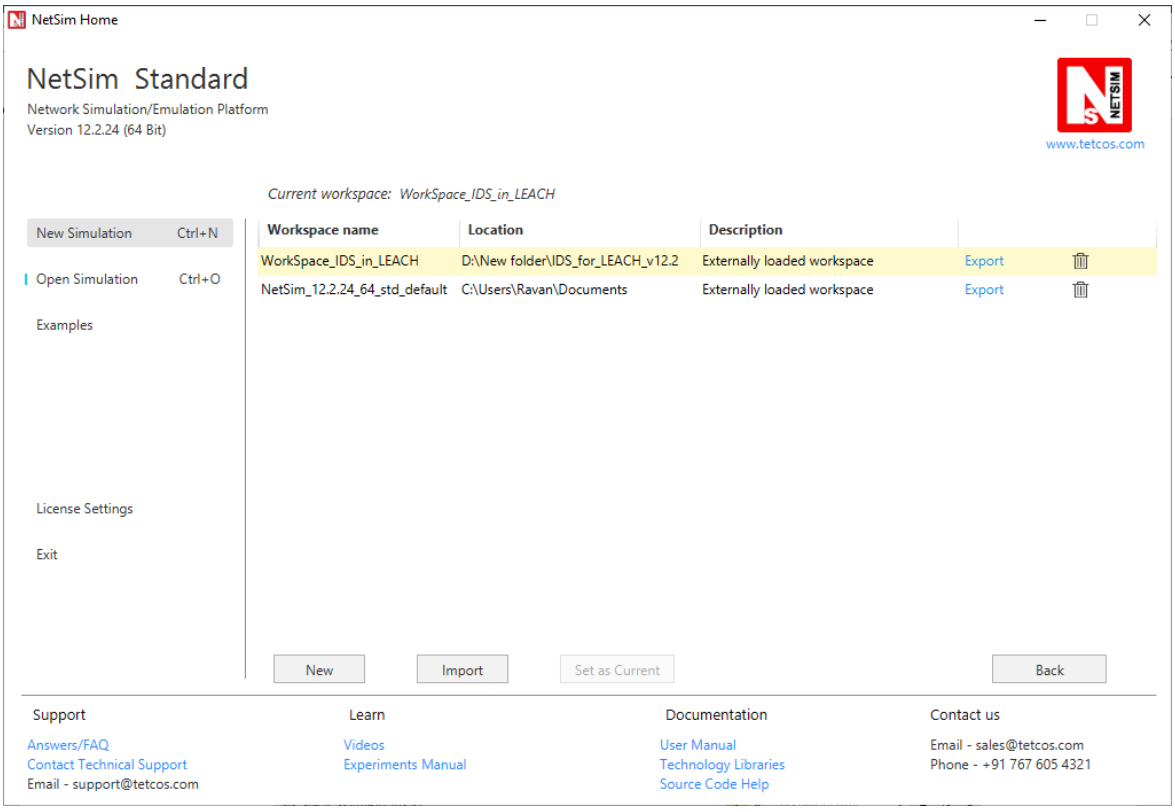


6. After this click on OK button in the Import Workspace window.

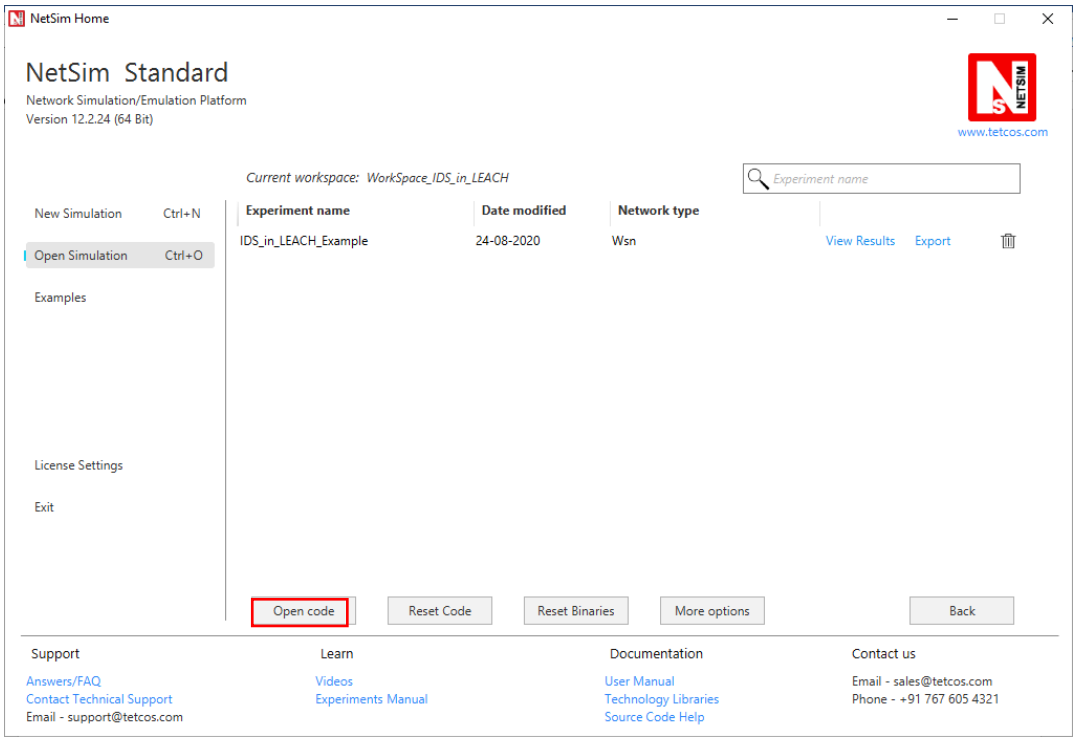
7. While importing the workspace, if the following warning message indicating Software Version Mismatch is displayed, you can ignore it and proceed.



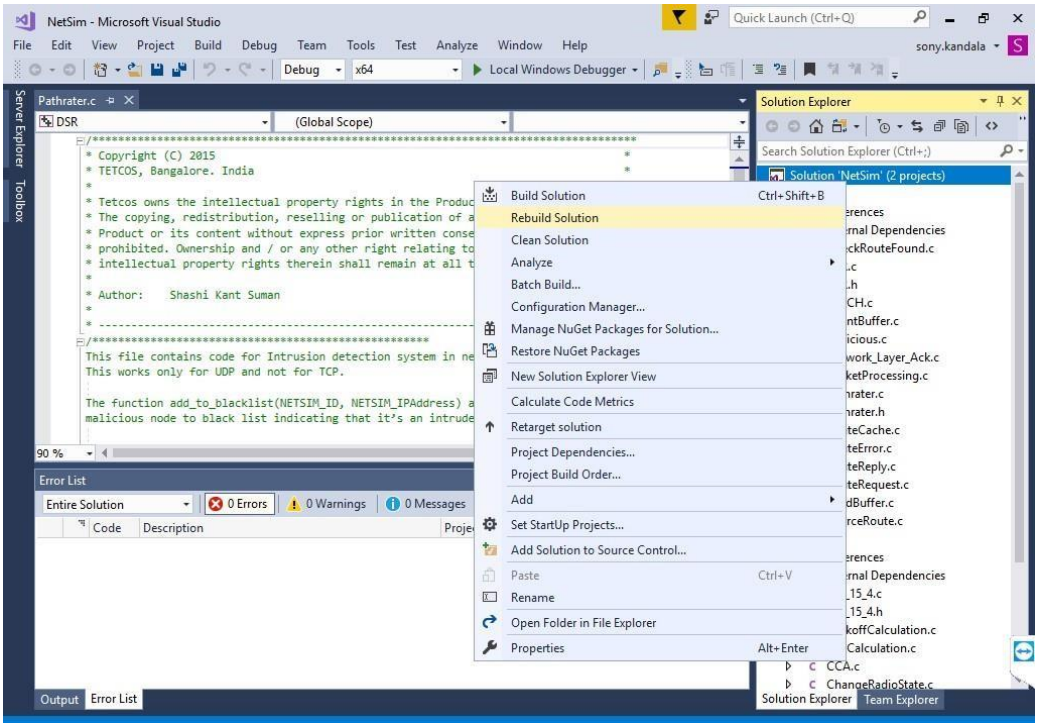
8. The Imported workspace will be set as the current workspace automatically. To see the imported workspace, click on Open Simulation->Workspace Options->More Options as shown below:



9. Open the Source codes in Visual Studio by going to Open Simulation-> Workspace Options and Clicking on Open code button as shown below:



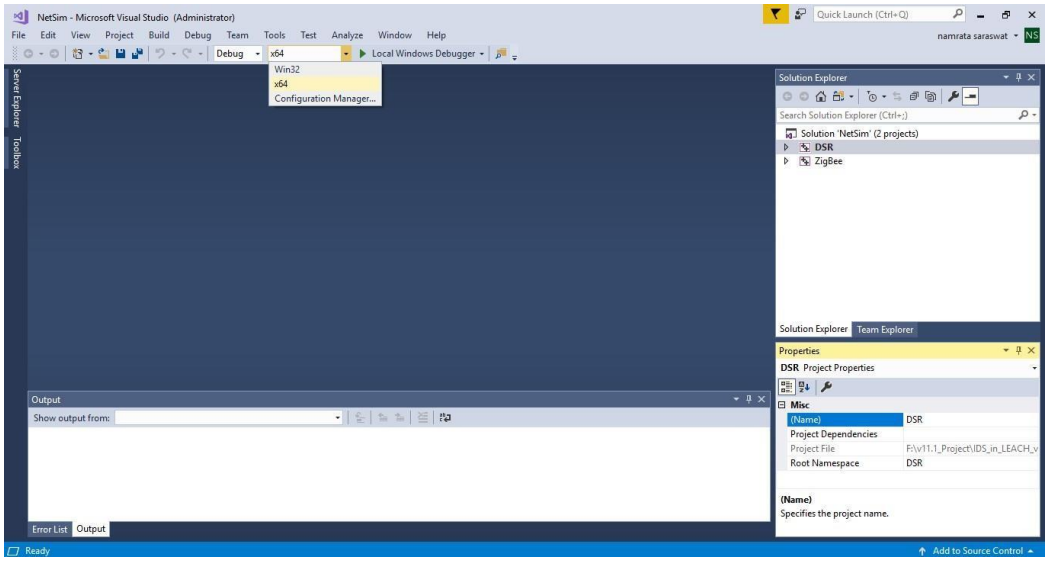
10. Right click on the solution and select rebuild.



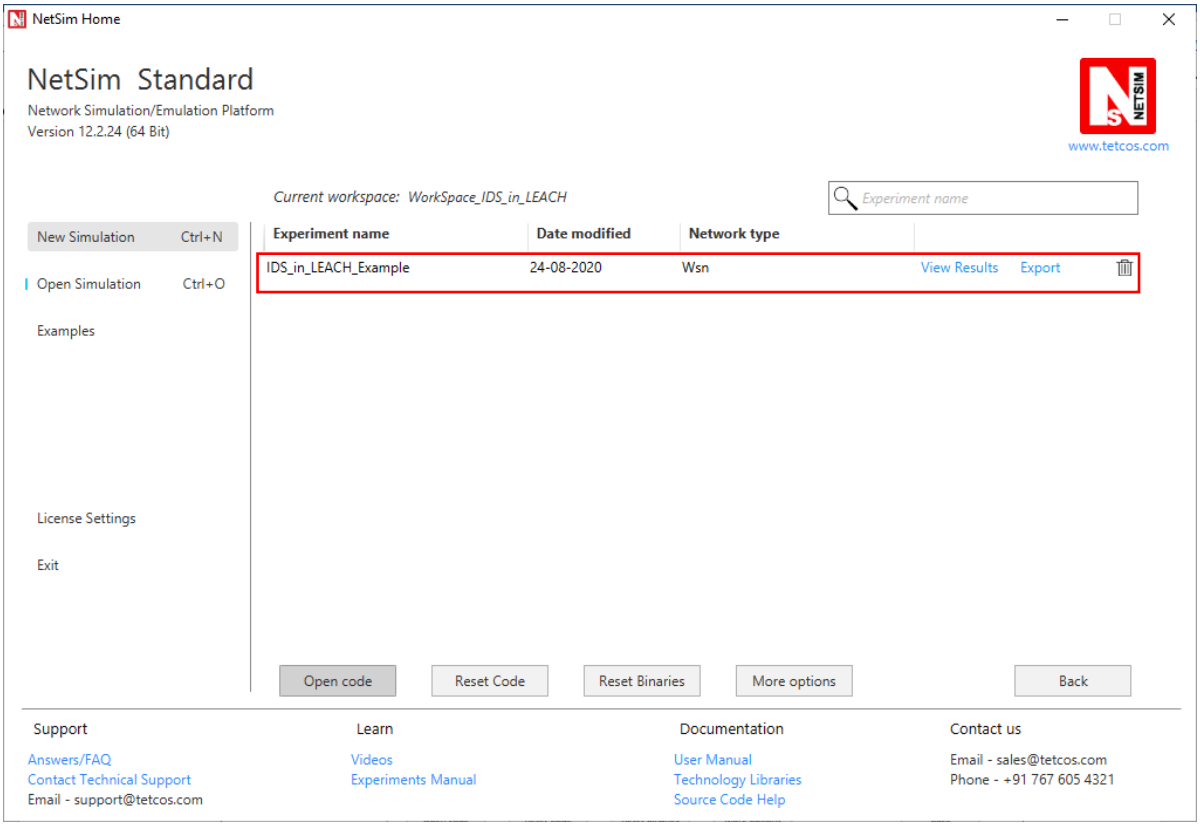
11. Upon rebuilding, **libZigbee.dll** and **libDSR.dll** will automatically get updated in the respective binary folder of the current workspace.

Note:

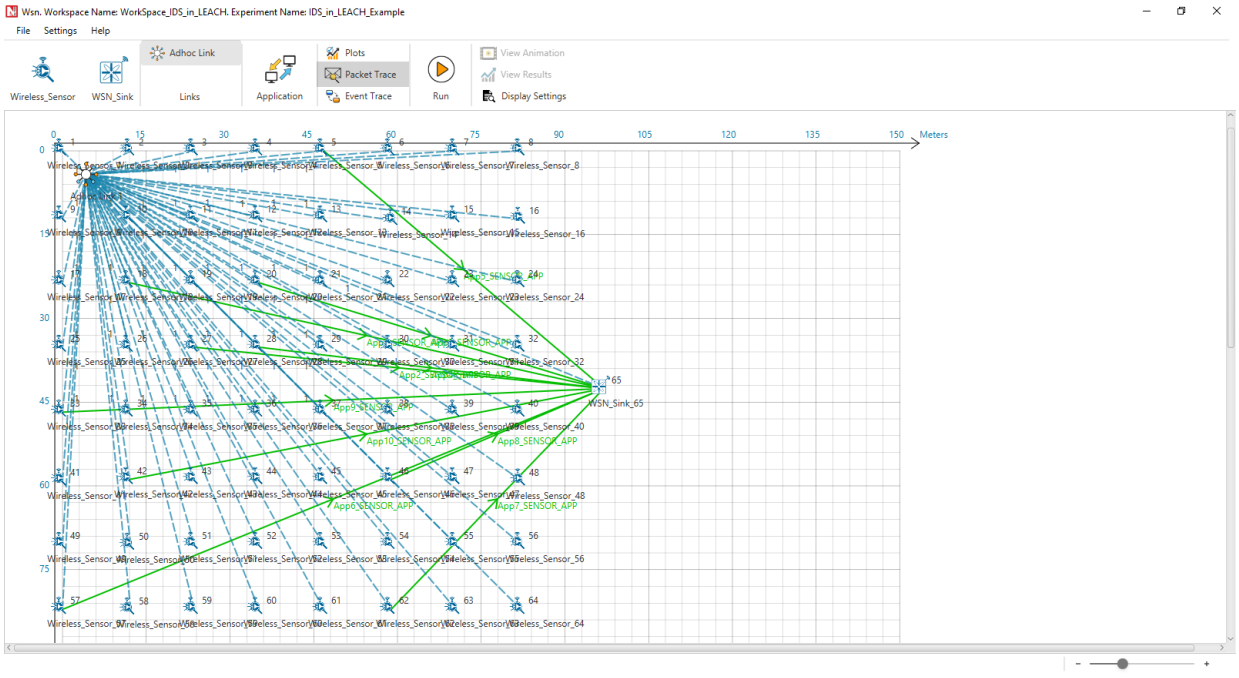
1. Based on whether you are using NetSim 32 bit or 64 bit setup you can configure Visual studio to build 32 bit or 64 bit Dll files respectively as shown below:



12. Go to NetSim home page, click on **Open Simulation**, Click on **IDS_in_LEACH_Example**.



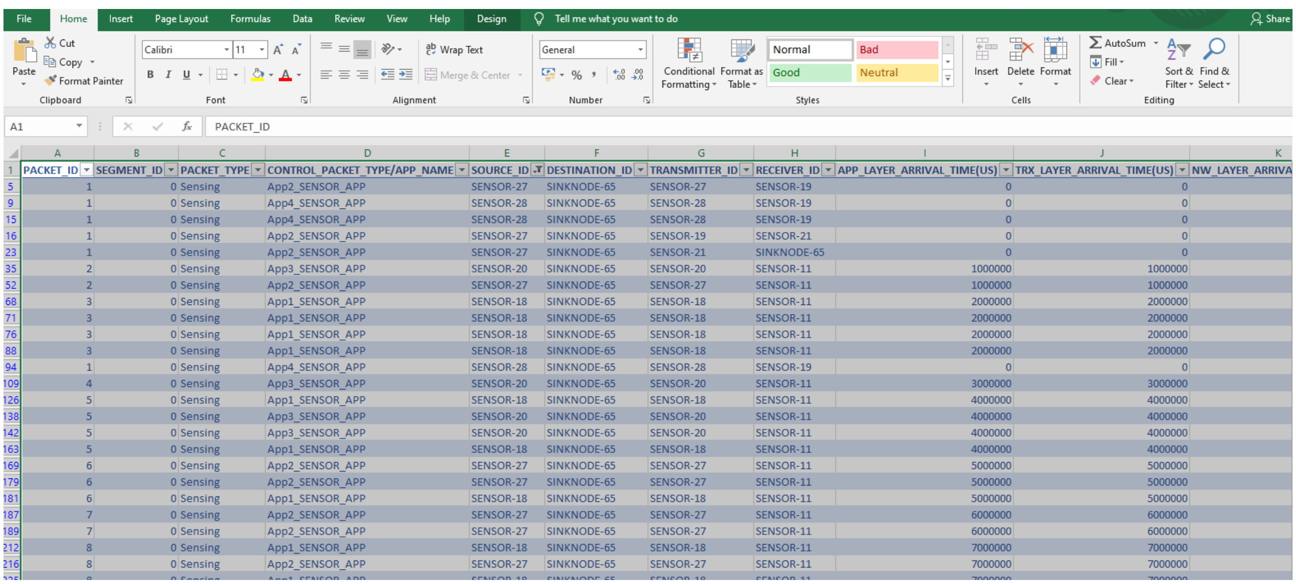
13. This Network is created in WSN Network as per the Number of clusters and size of clusters that are set in the LEACH code. By default the code runs for a scenario with 64 sensors uniformly placed, with the SINKNODE placed as per the screenshot below



14. Channel Characteristics is set to Pathloss only with LOG_DISTANCE as the path loss model. Path loss exponent is set to a high value 3
15. Run the simulation

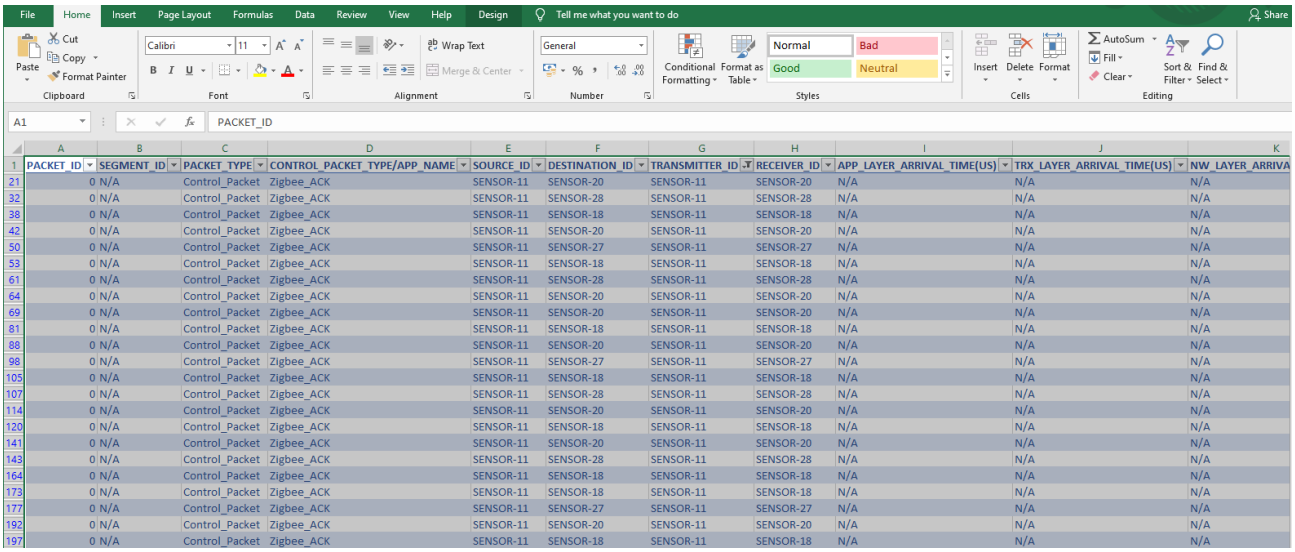
Result

- View the packet animation. You will note that the sensors directly start transmitting packets without route establishment since the routes are statically defined in LEACH.
- You will also note that the cluster heads keep changing dynamically in Clusters 2, 3 and 4.
- In cluster1, initially the cluster members transmits packets to malicious node (device id 11) since it advertises false battery information to become a cluster head. Per the original code setting the Watchdog timer is set to 2 seconds and the failure threshold is set to 20 packets. So you would notice that around 62 seconds, the malicious node is detected and then cluster head is elected dynamically based on the remaining energy of the sensor
- This can be observed in Packet trace by applying filters to Source_ID column by selecting only Sensor-18, 20, 27 and 28. You will be able to see that the receiver id is sensor-11 from 1s till 62s of simulation time and then it is changed when it gets blacklisted.



	PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID	APP_LAYER_ARRIVAL_TIME(US)	TRX_LAYER_ARRIVAL_TIME(US)	NW_LAYER_ARRIVA
5	1	0	Sensing	App2_SENSOR_APP	SENSOR-27	SINKNODE-65	SENSOR-27	SENSOR-19	0	0	
9	1	0	Sensing	App4_SENSOR_APP	SENSOR-28	SINKNODE-65	SENSOR-28	SENSOR-19	0	0	
15	1	0	Sensing	App4_SENSOR_APP	SENSOR-28	SINKNODE-65	SENSOR-28	SENSOR-19	0	0	
16	1	0	Sensing	App2_SENSOR_APP	SENSOR-27	SINKNODE-65	SENSOR-19	SENSOR-21	0	0	
23	1	0	Sensing	App2_SENSOR_APP	SENSOR-27	SINKNODE-65	SENSOR-21	SINKNODE-65	0	0	
35	2	0	Sensing	App3_SENSOR_APP	SENSOR-20	SINKNODE-65	SENSOR-20	SENSOR-11	1000000	1000000	
52	2	0	Sensing	App2_SENSOR_APP	SENSOR-27	SINKNODE-65	SENSOR-27	SENSOR-11	1000000	1000000	
68	3	0	Sensing	App1_SENSOR_APP	SENSOR-18	SINKNODE-65	SENSOR-18	SENSOR-11	2000000	2000000	
71	3	0	Sensing	App1_SENSOR_APP	SENSOR-18	SINKNODE-65	SENSOR-18	SENSOR-11	2000000	2000000	
76	3	0	Sensing	App1_SENSOR_APP	SENSOR-18	SINKNODE-65	SENSOR-18	SENSOR-11	2000000	2000000	
88	3	0	Sensing	App1_SENSOR_APP	SENSOR-18	SINKNODE-65	SENSOR-18	SENSOR-11	2000000	2000000	
94	1	0	Sensing	App4_SENSOR_APP	SENSOR-28	SINKNODE-65	SENSOR-28	SENSOR-19	0	0	
109	4	0	Sensing	App3_SENSOR_APP	SENSOR-20	SINKNODE-65	SENSOR-20	SENSOR-11	3000000	3000000	
126	5	0	Sensing	App1_SENSOR_APP	SENSOR-18	SINKNODE-65	SENSOR-18	SENSOR-11	4000000	4000000	
138	5	0	Sensing	App3_SENSOR_APP	SENSOR-20	SINKNODE-65	SENSOR-20	SENSOR-11	4000000	4000000	
142	5	0	Sensing	App3_SENSOR_APP	SENSOR-20	SINKNODE-65	SENSOR-20	SENSOR-11	4000000	4000000	
163	5	0	Sensing	App1_SENSOR_APP	SENSOR-18	SINKNODE-65	SENSOR-18	SENSOR-11	4000000	4000000	
169	6	0	Sensing	App2_SENSOR_APP	SENSOR-27	SINKNODE-65	SENSOR-27	SENSOR-11	5000000	5000000	
179	6	0	Sensing	App2_SENSOR_APP	SENSOR-27	SINKNODE-65	SENSOR-27	SENSOR-11	5000000	5000000	
181	6	0	Sensing	App1_SENSOR_APP	SENSOR-18	SINKNODE-65	SENSOR-18	SENSOR-11	5000000	5000000	
187	7	0	Sensing	App2_SENSOR_APP	SENSOR-27	SINKNODE-65	SENSOR-27	SENSOR-11	6000000	6000000	
189	7	0	Sensing	App2_SENSOR_APP	SENSOR-27	SINKNODE-65	SENSOR-27	SENSOR-11	6000000	6000000	
212	8	0	Sensing	App1_SENSOR_APP	SENSOR-18	SINKNODE-65	SENSOR-18	SENSOR-11	7000000	7000000	
216	8	0	Sensing	App2_SENSOR_APP	SENSOR-27	SINKNODE-65	SENSOR-27	SENSOR-11	7000000	7000000	

- Now undo filter in Source_Id column and apply filter to transmitter_Id column by selecting only Sensor-11. You will be able to see that no data packets are forwarded by the malicious node



PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID	APP_LAYER_ARRIVAL_TIME(US)	TRX_LAYER_ARRIVAL_TIME(US)	NW_LAYER_ARRIVA
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-20	SENSOR-11	SENSOR-20	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-28	SENSOR-11	SENSOR-28	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-18	SENSOR-11	SENSOR-18	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-20	SENSOR-11	SENSOR-20	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-27	SENSOR-11	SENSOR-27	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-18	SENSOR-11	SENSOR-18	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-28	SENSOR-11	SENSOR-28	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-20	SENSOR-11	SENSOR-20	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-20	SENSOR-11	SENSOR-20	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-18	SENSOR-11	SENSOR-18	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-20	SENSOR-11	SENSOR-20	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-27	SENSOR-11	SENSOR-27	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-18	SENSOR-11	SENSOR-18	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-28	SENSOR-11	SENSOR-28	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-20	SENSOR-11	SENSOR-20	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-18	SENSOR-11	SENSOR-18	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-20	SENSOR-11	SENSOR-20	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-28	SENSOR-11	SENSOR-28	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-18	SENSOR-11	SENSOR-18	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-18	SENSOR-11	SENSOR-18	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-27	SENSOR-11	SENSOR-27	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-20	SENSOR-11	SENSOR-20	N/A	N/A	N/A
0	N/A	Control_Packet	Zigbee_ACK	SENSOR-11	SENSOR-18	SENSOR-11	SENSOR-18	N/A	N/A	N/A

- This will have a direct impact on the Application Throughput which can be observed in the Application Metrics table present in NetSim Simulation Results window. The throughput for applications 1, 2, 3 and 4 are less since the source ids belongs to cluster1 having malicious node (device id 11).
- The time at which a malicious node is detected can be obtained from the CUSTOM METRICS in the results window where the start time - time from which a node becomes malicious, detection time - time at which the node was added to blacklist can be obtained.

CUSTOM_METRICS_Table

Custom_IDS_Metrics Detailed View

DeviceID	Start Time (micro sec)	Detection Time (micro sec)
11	0.000000	62004192.000000

Dedicated Metrics for IDS