

Intrusion detection system in NetSim

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
- To detect the intruder and to send data via a new route, the following files are added in DSR and IEEE802_11:

➤ **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**

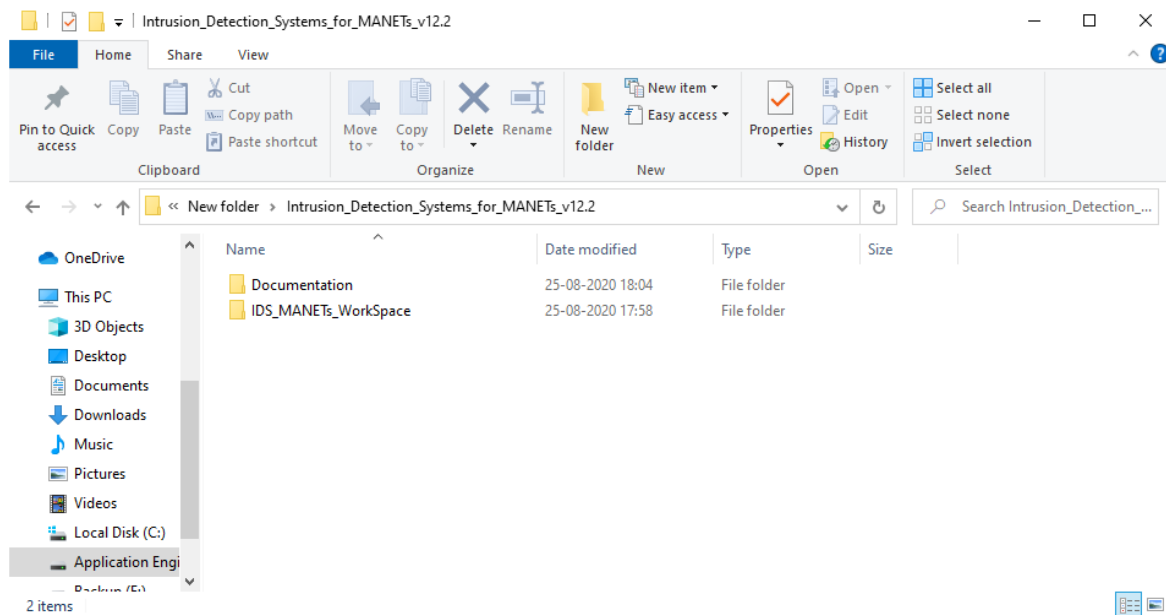
This file contains code for the IDS and is added in IEEE802_11 operating in Layer 2.

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.

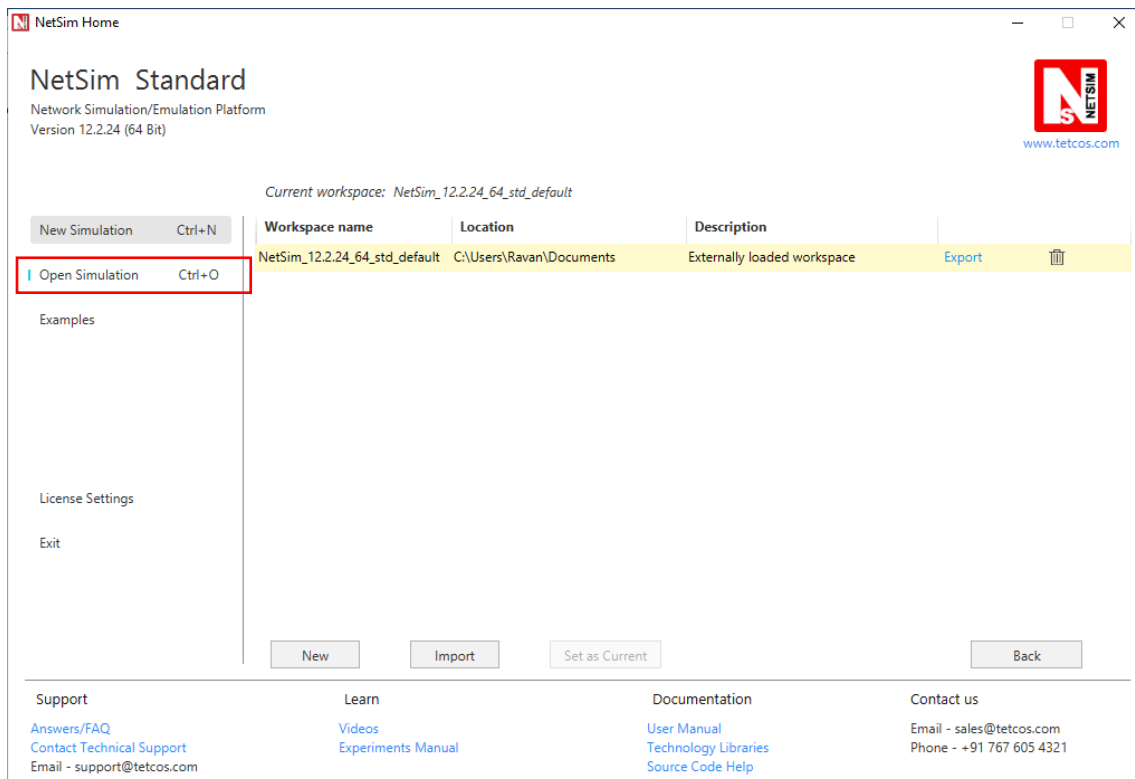
The malicious node doesn't forward packets that it receives. The watchdog timer in the node (which forwarded the packet to the malicious node) expires. A counter is present which measures the number of times the watchdog timer expires (in other words the number of packets sent out but not forwarded by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

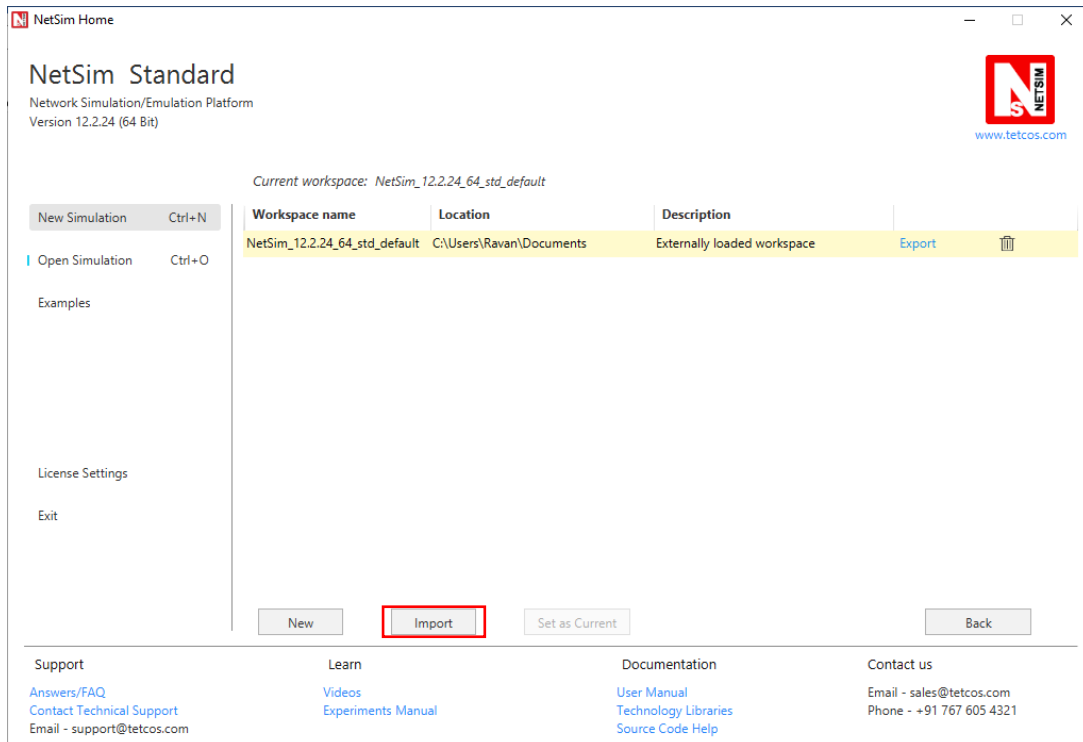
1. The downloaded project folder contains the folders Documentation, and IDS_MANETs_Workspace directory as shown below:



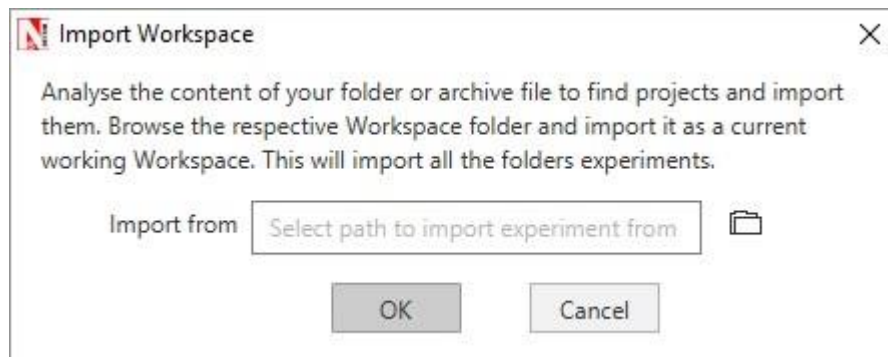
2. After you unzip the downloaded project folder, Open NetSim Home Page click on **Open Simulation** option,



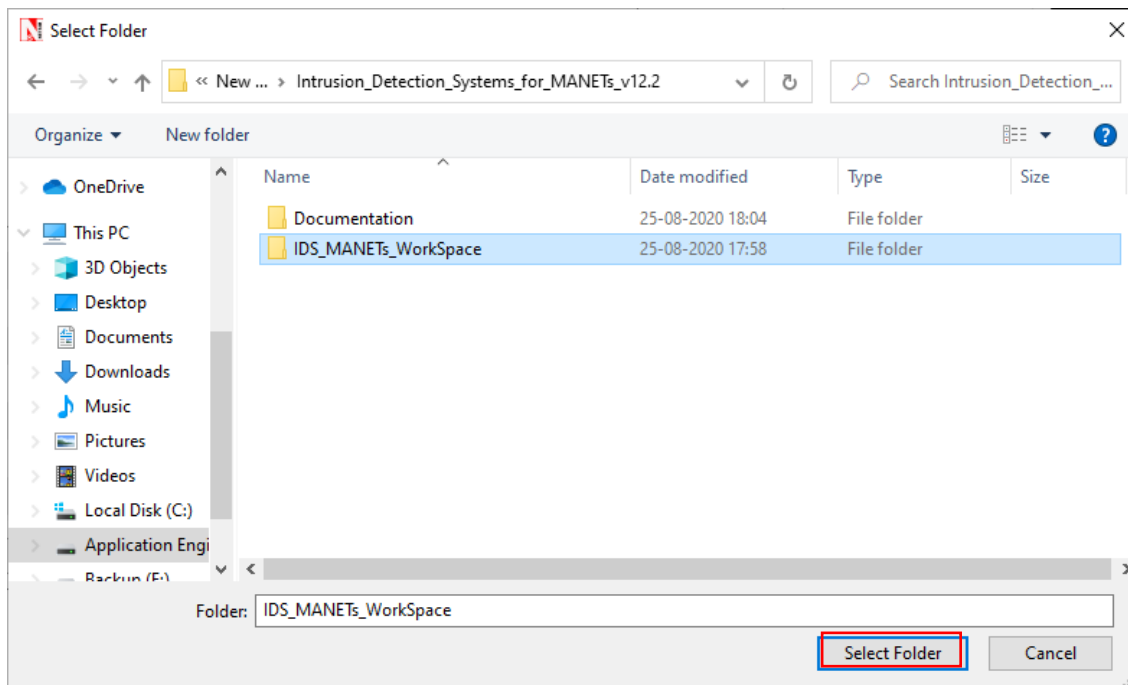
3. Click on Workspace options -> More options -> Import



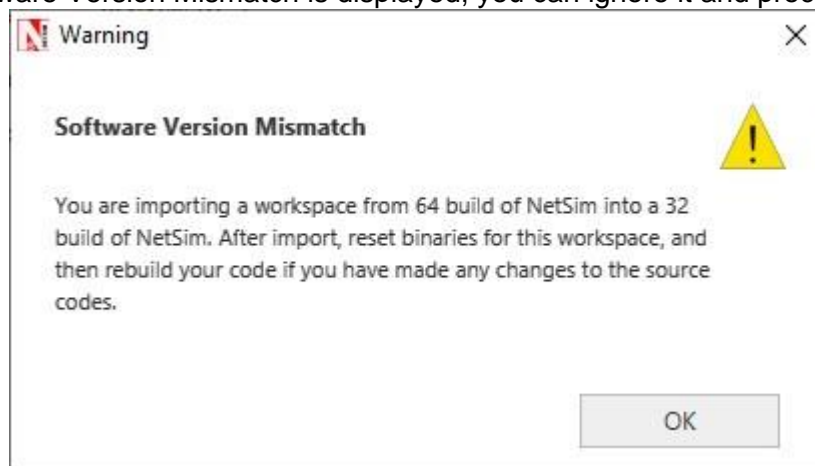
- It displays a window where users need to give the path of the workspace folder and click on OK as shown below:



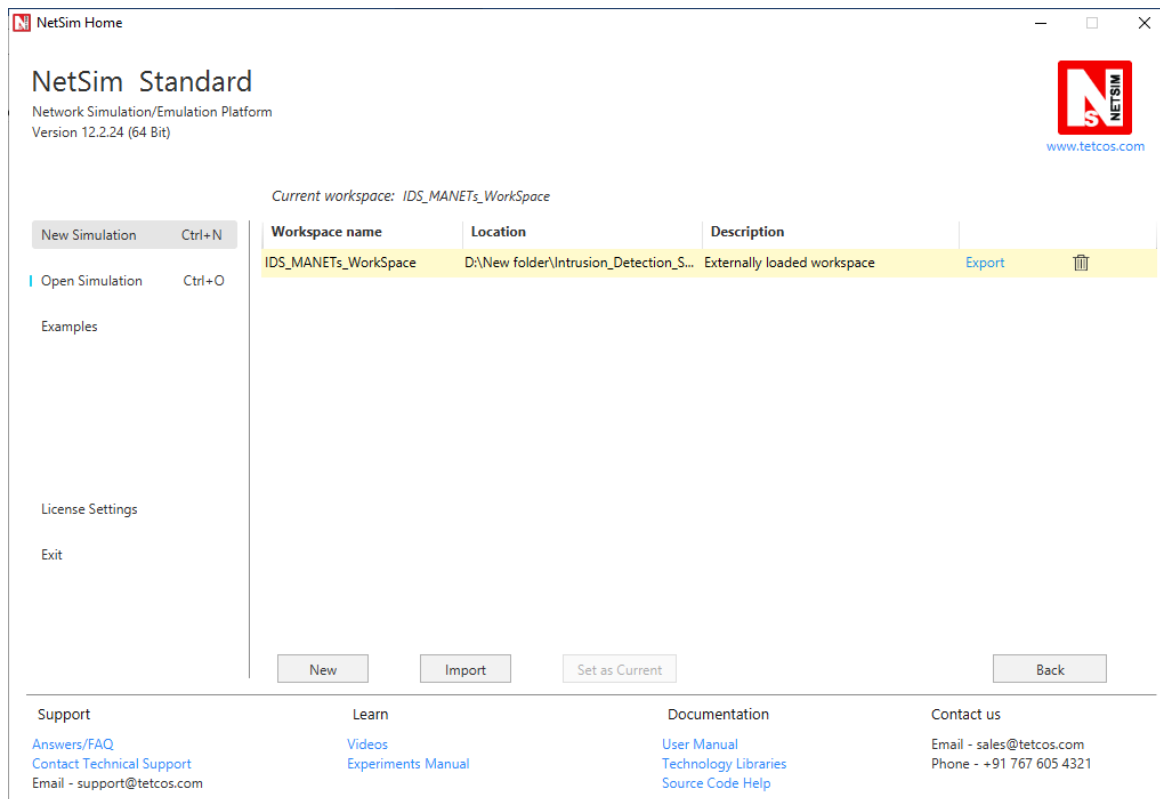
- Browse to the IDS_MANETs_Workspace folder and click on select folder as shown below:



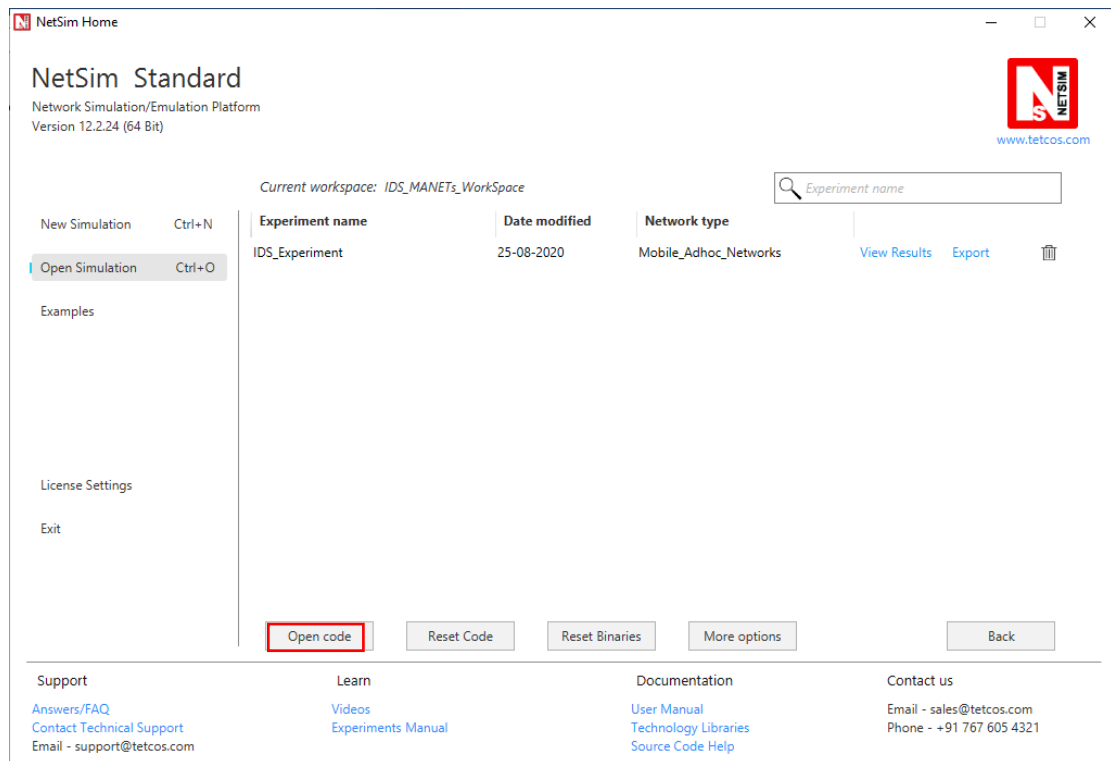
6. After this click on OK button in the Import Workspace window.
7. While importing the workspace, if the following warning message indicating Software Version Mismatch is displayed, you can ignore it and proceed.



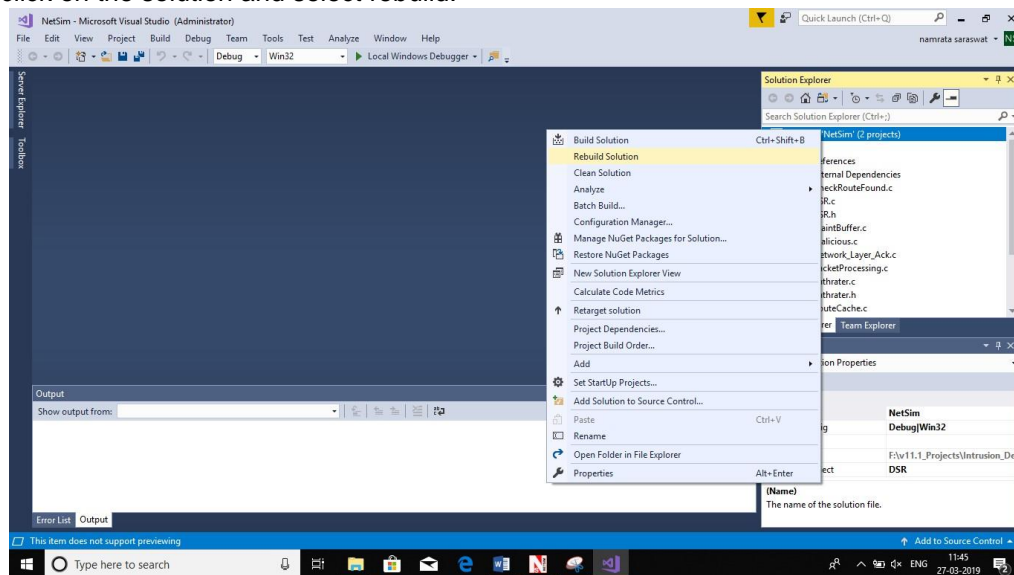
8. The Imported workspace will be set as the current workspace automatically. To see the imported workspace, click on Open Simulation->Workspace Options->More Options as shown below:



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



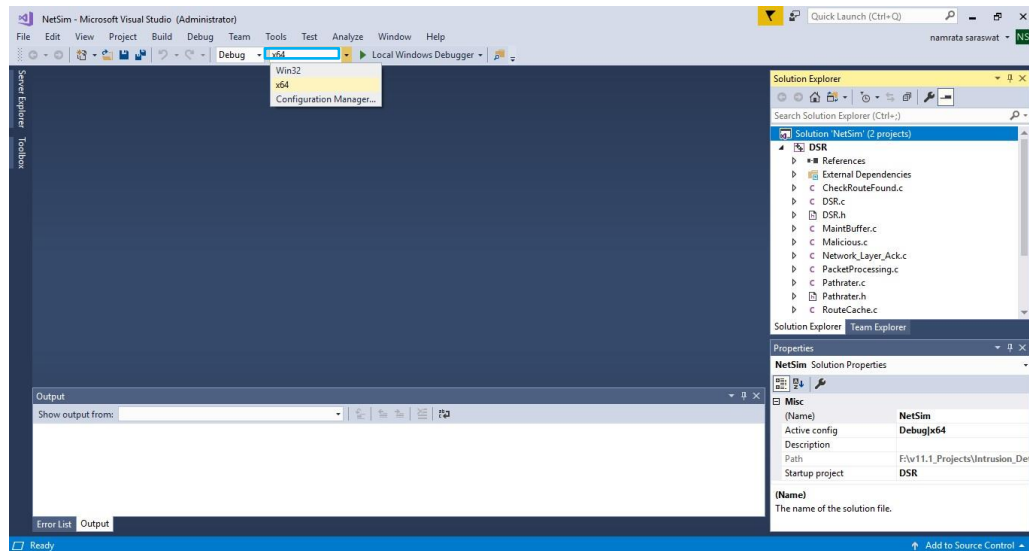
- Right click on the solution and select rebuild.



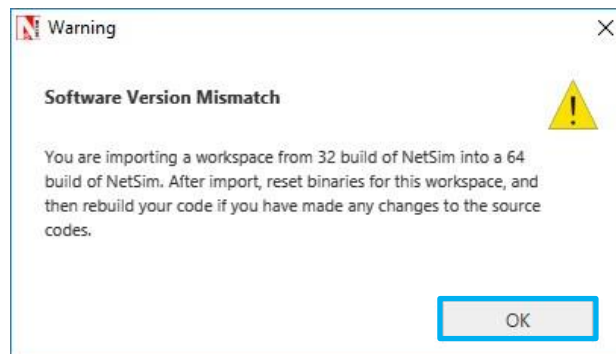
- Upon rebuilding, **libIEEE802_11.dll** and **libDSR.dll** will automatically get updated in the respective bin folder of the current workspace.

Note:

1. While 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:



2. While importing the project in NetSim 64bit version, it will display popup as “**Software version mismatch**”, ignore the warning message and click in **ok**.




Next, to run the IDS code, follow these steps:

Step 1: Go to NetSim home page, click on **Open Simulation**, Click on **IDS_Experiment**.

NetSim Home


NetSim Standard

Network Simulation/Emulation Platform
Version 12.2.24 (64 Bit)



www.tetcos.com

Current workspace: IDS_MANETs_WorkSpace

Experiment name	Date modified	Network type	
IDS_Experiment	25-08-2020	Mobile_Adhoc_Networks	View Results Export 

[New Simulation](#) Ctrl+N
[Open Simulation](#) Ctrl+O
[Examples](#)

[License Settings](#)
[Exit](#)

[Open code](#)
[Reset Code](#)
[Reset Binaries](#)
[More options](#)
[Back](#)

Support

[Answers/FAQ](#)
[Contact Technical Support](#)
[Email - support@tetcos.com](mailto:support@tetcos.com)

Learn

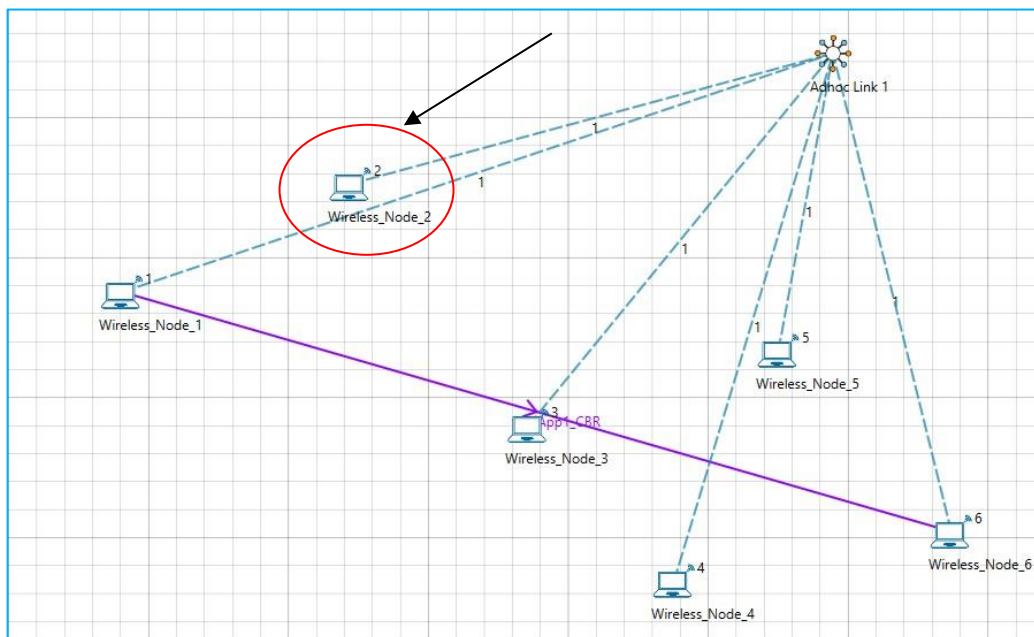
[Videos](#)
[Experiments Manual](#)

Documentation

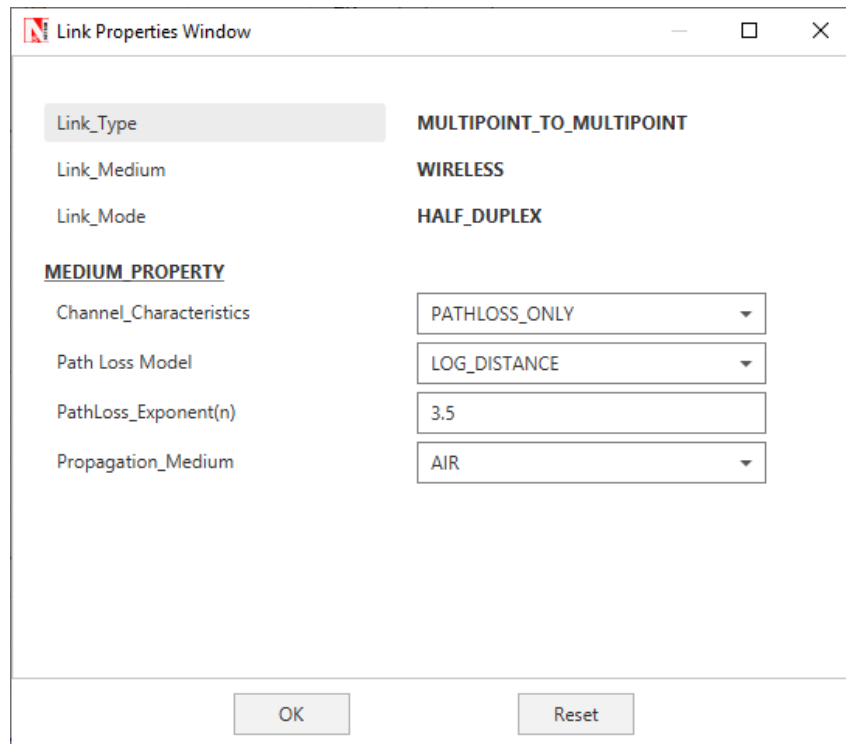
[User Manual](#)
[Technology Libraries](#)
[Source Code Help](#)

Contact us

[Email - sales@tetcos.com](mailto:sales@tetcos.com)
[Phone - +91 767 605 4321](tel:+917676054321)



Step 2: Channel Characteristics is set to Pathloss only with LOG_DISTANCE as the path loss model. Path loss exponent is set to a high value 3.5 Example:



The screenshot shows a window titled "Link Properties Window" with standard Windows window controls (minimize, maximize, close). The window contains the following configuration:

Link_Type	MULTIPOINT_TO_MULTIPPOINT
Link_Medium	WIRELESS
Link_Mode	HALF_DUPLEX
MEDIUM PROPERTY	
Channel_Characteristics	PATHLOSS_ONLY
Path Loss Model	LOG_DISTANCE
PathLoss_Exponent(n)	3.5
Propagation_Medium	AIR

At the bottom of the window are two buttons: "OK" and "Reset".

Step 3: An application is set between node 1 and node 6

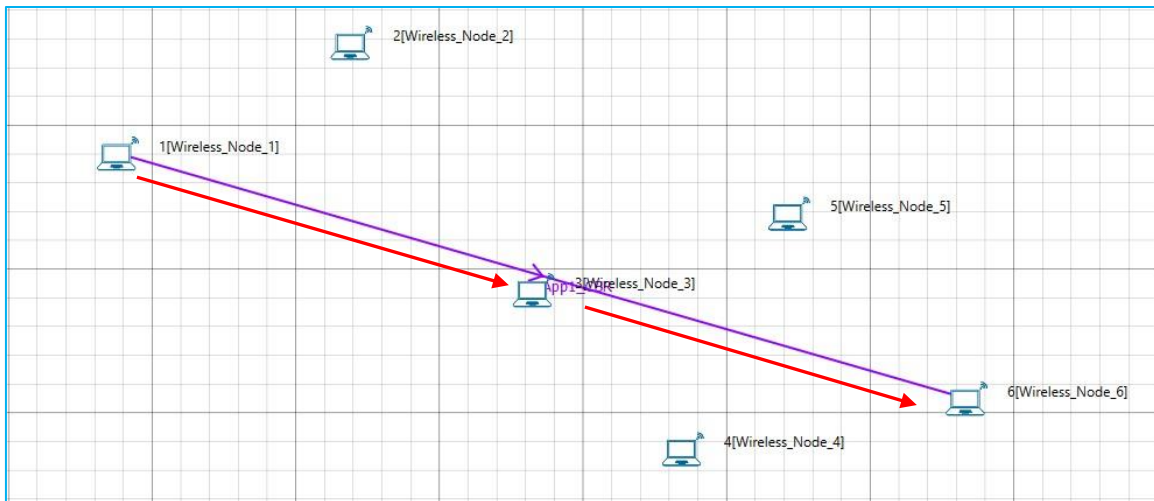
APPLICATION	
Application_Method	UNICAST
Application_Type	CBR
Application_ID	1
Application_Name	App1_CBR
Source_Count	1
Source_ID	1
Destination_Count	1
Destination_ID	6
Start_Time(s)	5
End_Time(s)	100000
Src to Dest	Show line
Encryption	NONE
Random_Startup	FALSE
QoS	BE
Priority	Low
Session_Protocol	NONE

Step 4: Run the simulation

Step 5: View packet animation. Here you would notice initially all traffic would flow to the malicious nodes. 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 7.39 seconds, the malicious node is detected and the route to destination would change in the subsequent route discovery process.



Initial flow of packets till node 2 detected as malicious



Flow of packets after node 2 is detected as malicious

The time at which a malicious node is detected can be obtained from the CUSTOM METRICS (IDS 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.

[illegible]

Dedicated Metrics for IDS