Intrusion detection system in NetSim

Software: NetSim Standard v13.1 64-bit, Visual Studio 2019

Project Download Link:
https://github.com/NetSim-TETCOS/IDS_MANET_v13.1/archive/refs/heads/main.zip

Follow the instructions specified in the following link to download and setup the Project in NetSim:

https://support.tetcos.com/en/support/solutions/articles/14000128666-downloading-and-setting-up-netsim-file-exchange-projects

Steps to simulate

1. Open the Source codes in Visual Studio by going to Your work->Source Code and Clicking on Open code button in NetSim Home Screen window.
2. Right click on the solution in the solution explorer and select Rebuild.

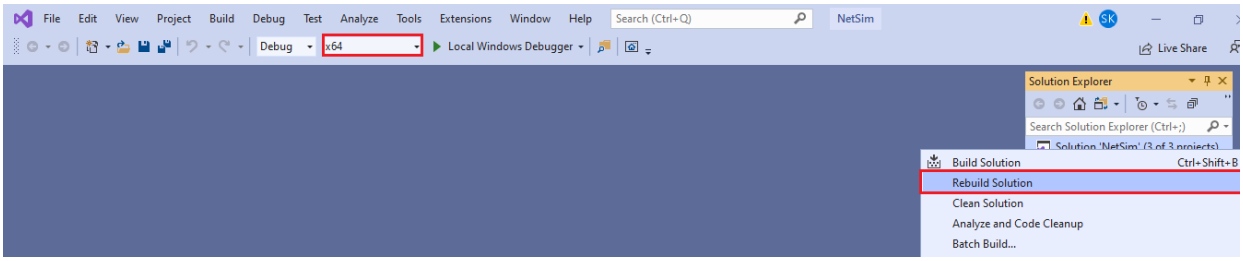

Figure 1: Screen shot of NetSim project source code in Visual Studio

3. Upon successful build modified **libIEEE802_11.dll** and **libDSR.dll** file gets automatically updated in the directory containing NetSim binaries.

Example:

1. The IDS_MANETs_WorkSpace 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 **IDS_Experiment** from the list of experiments.

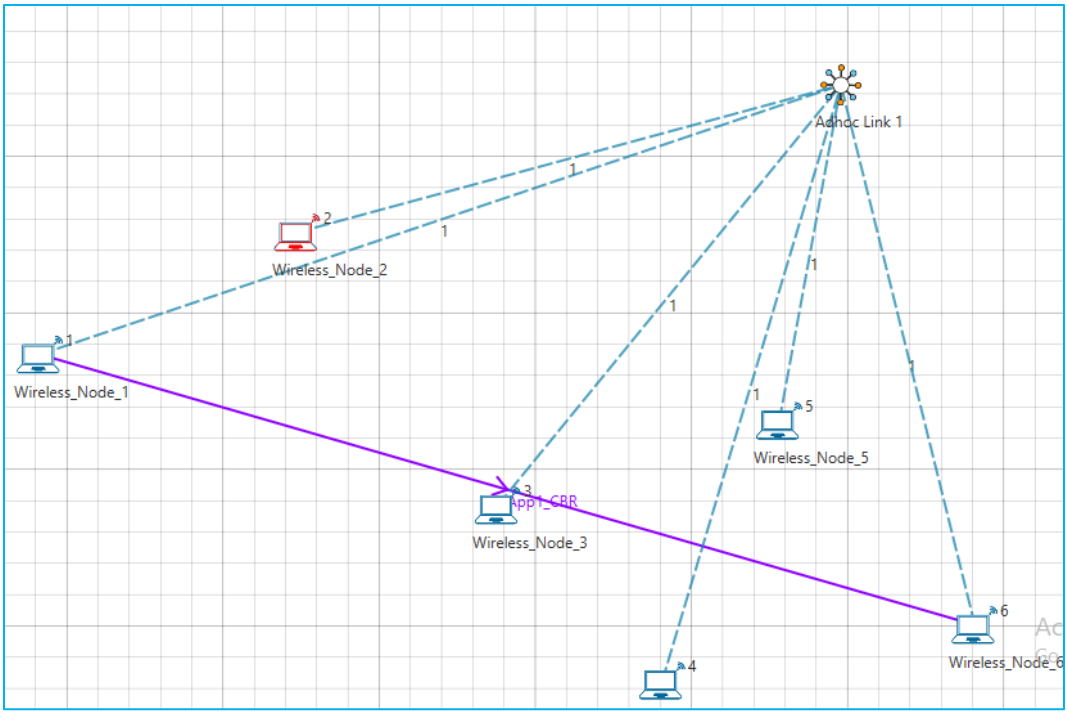

Figure 2: Created network topology with 5 Wireless nodes

2. Wireless Link Properties
   - Channel Characteristics - Pathloss only
   - Path loss model - LOG_DISTANCE
   - Path loss exponent - 3.5
3. An application is Created between Wireless_Node_1 to Wireless_Node_6 and other properties are default.
4. Run the simulation.

Results and discussion

View packet animation. Here you would notice initially all traffic would flow to the malicious nodes. As 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.

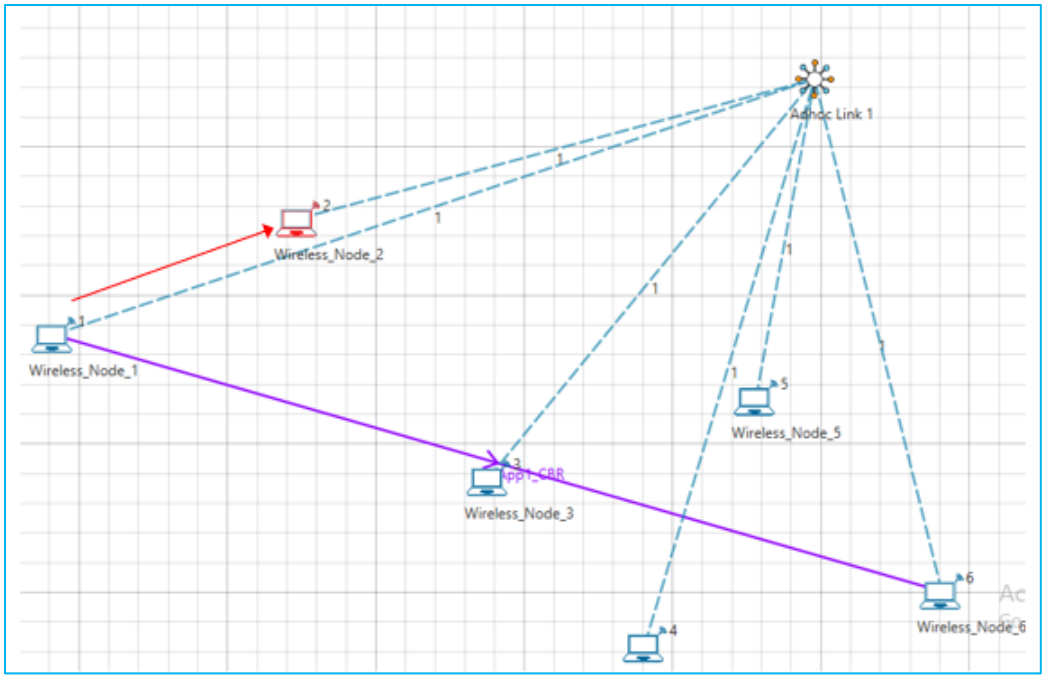

Figure 3: Initial flow of packets till node 2 detected as malicious

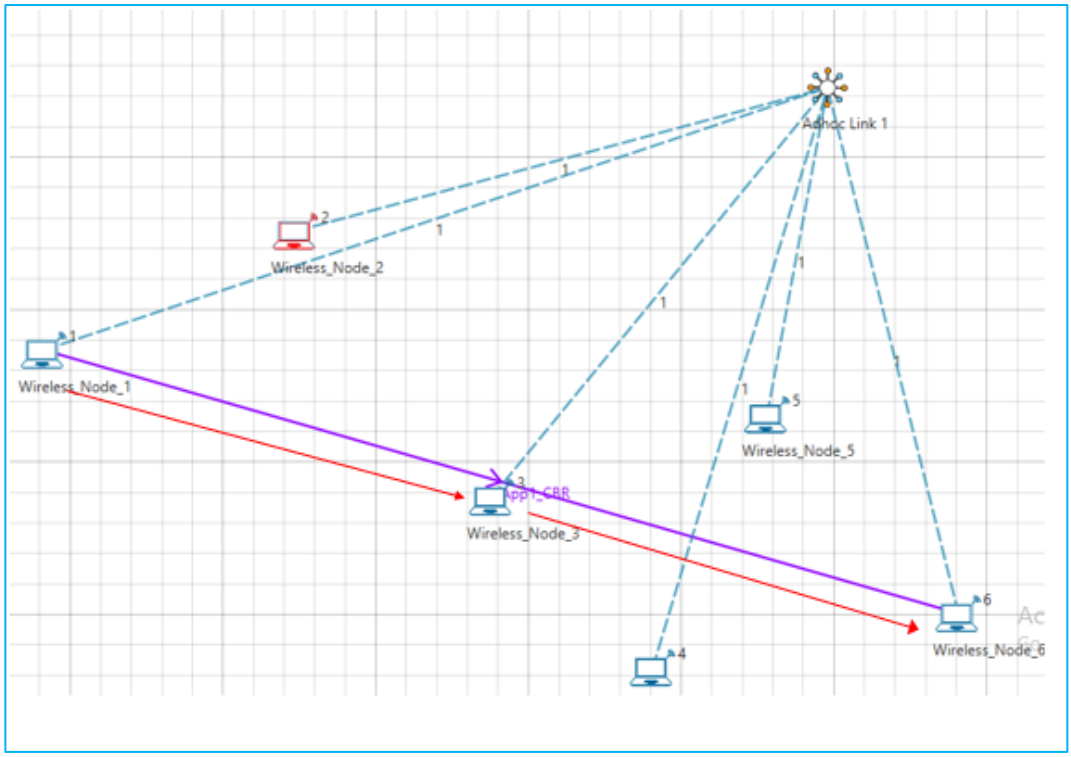

Figure 4: Flow of packets after node 2 is detected as malicious

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.

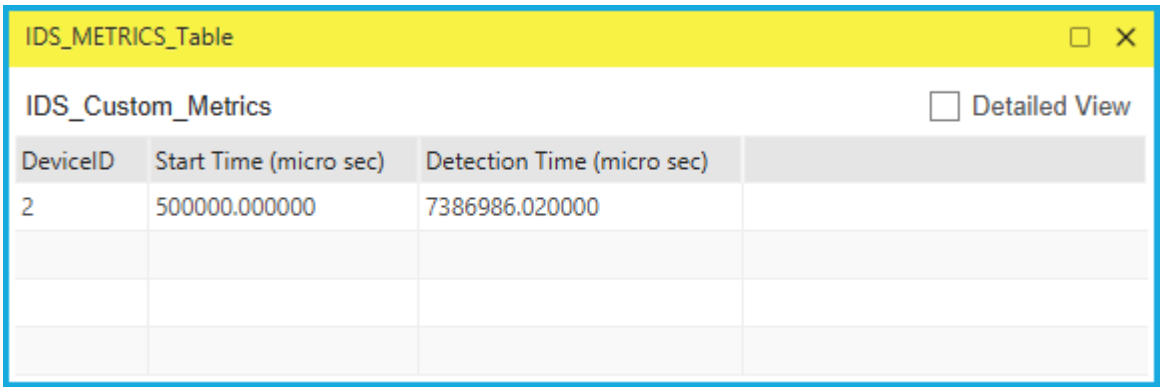

Figure 5: Dedicated Metrics for IDS

Files Used in this project

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 blacklisted 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 does not 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.