Intrusion detection system in MANET

Software: NetSim Standard v13.3, Visual Studio 2022

Project Download Link:

https://github.com/NetSim-TETCOS/Intrusion-Detection-System-in-MANET-v13.3/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

Introduction

An Intrusion Detection System is a security tool that keeps an eye on the network to detect any strange activity and sends a warning message when it finds something suspicious.

We make a node malicious in the network by which the working of the network is altered, this then will be detected by IDS, it will block the packet transmission to the Malicious Node and the transmission of the packets happens normally.

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.

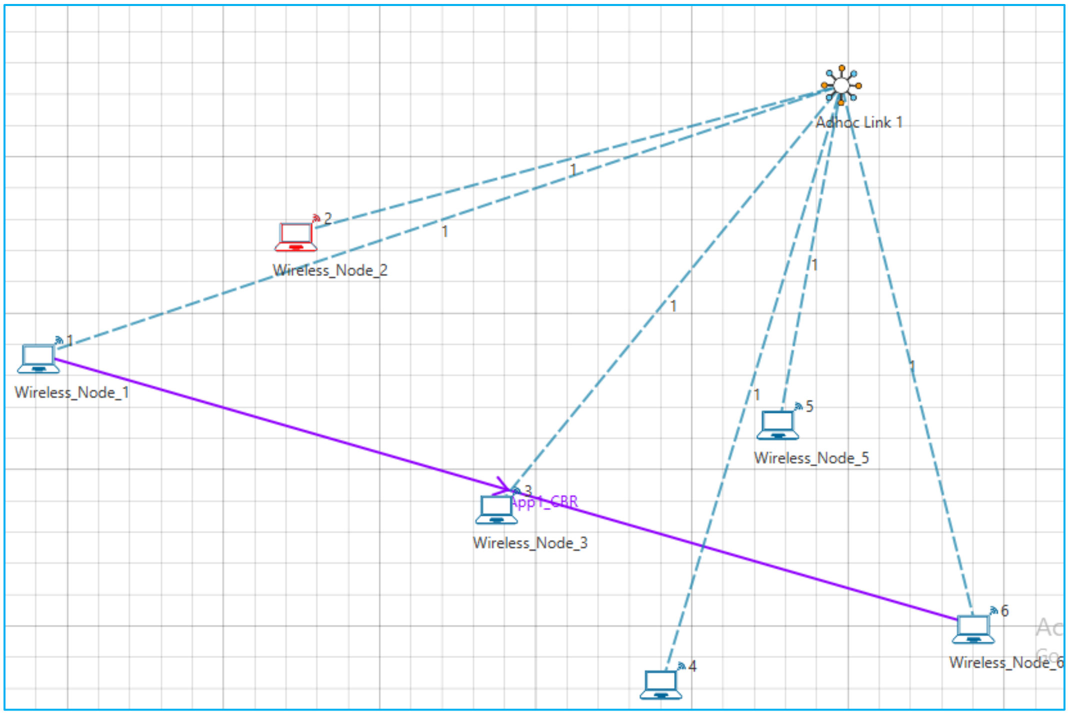


Figure 1: Created network topology with 5 Wireless nodes

2. Wireless Link Properties
   - Channel Characteristics - Pathloss only
   - Path loss model - LOG_DISTANCE
   - Path loss exponent – 2.5
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.

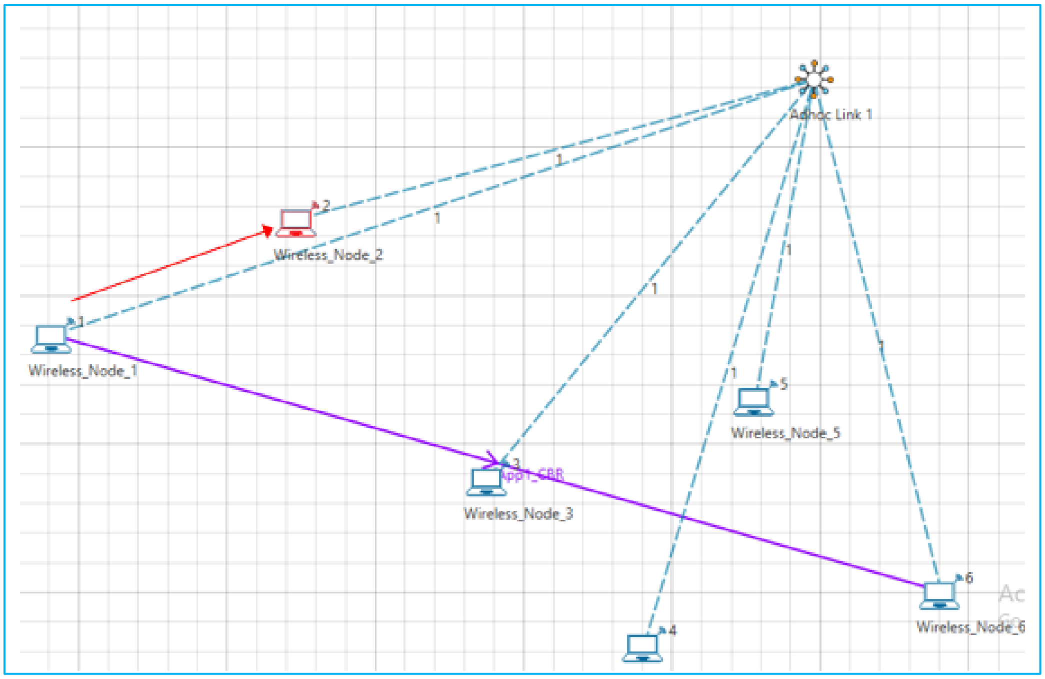


Figure 2: Initial flow of packets till node 2 detected as malicious

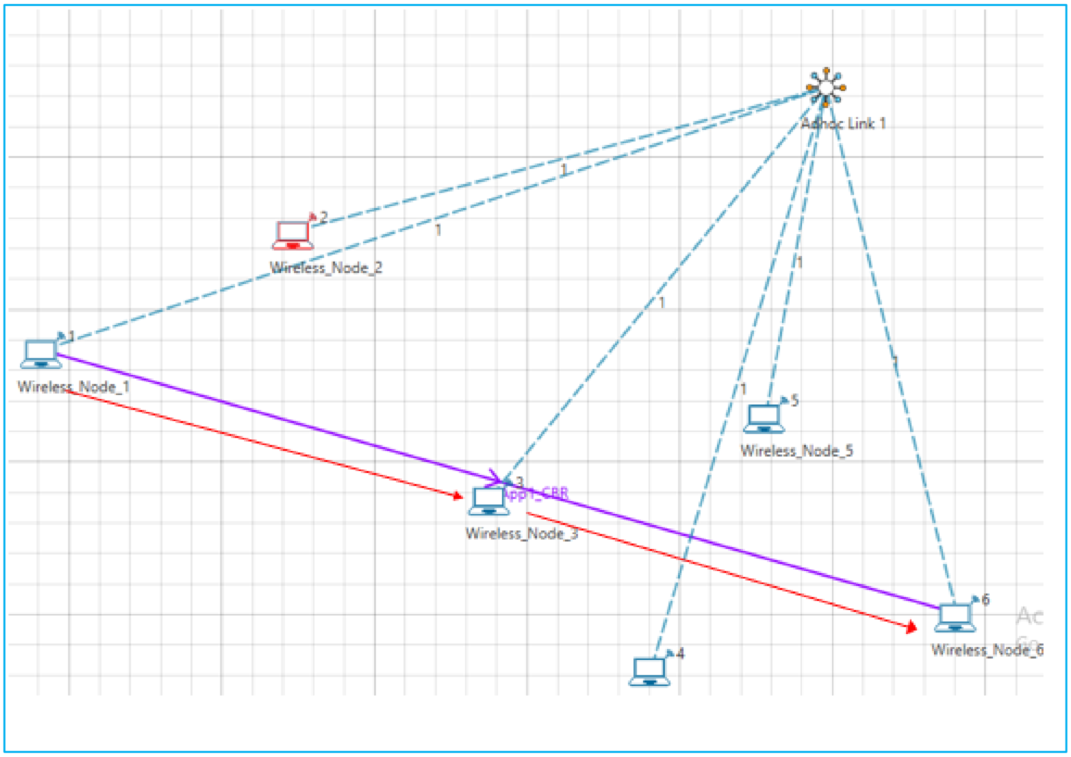
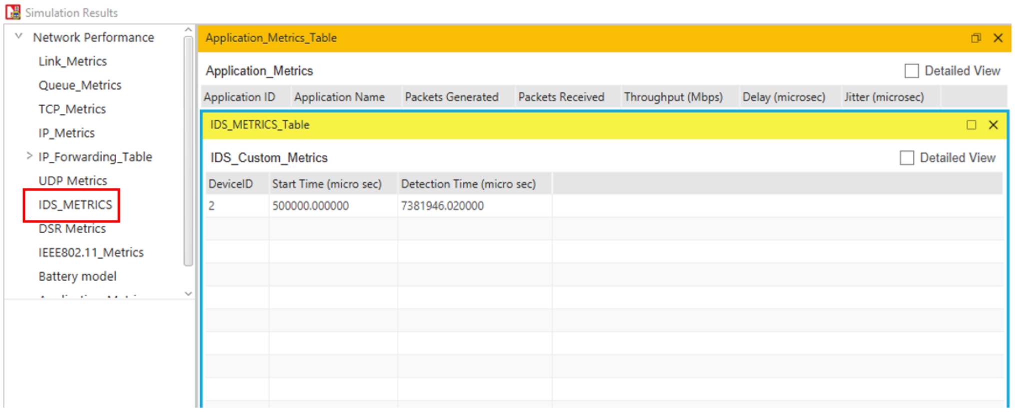


Figure 3: Flow of packets after node 2 is detected as malicious

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).



Application_Metrics

Application ID	Application Name	Packets Generated	Packets Received	Throughput (Mbps)	Delay (microsec)	Jitter (microsec)

IDS_Custom_Metrics

DeviceID	Start Time (micro sec)	Detection Time (micro sec)
2	500000.000000	7381946.020000

Figure 4: 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 (Pathrater.c and Malicious.c)are added in DSR and (Watchdog.c) is added in IEEE802_11:

Malicious.c

This file contains code for turning a node into malicious node

- **fn_NetSim_DSR_MaliciousNode();** //This function is used to identify whether a current device is malicious or not in-order to establish malicious behavior.
- **fn_NetSim_DSR_MaliciousRouteAddToCache();** //This function is used to add a fake route entry into the route cache of the malicious device with its next hop as the destination.
- **fn_NetSim_DSR_MaliciousProcessSourceRouteOption();** //This function is used to drop the received packets if the device is malicious, instead of forwarding the packet to the next hop.

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(Intrusion Detection System) and is added in IEEE802_11 project 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.