

Intrusion detection system on LEACH

Software Recommended: NetSim Standard v11.0, Visual Studio 2017

Project Download Link:

https://github.com/NetSim-TETCOS/IDS-in-LEACH_v11.0/archive/master.zip

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.

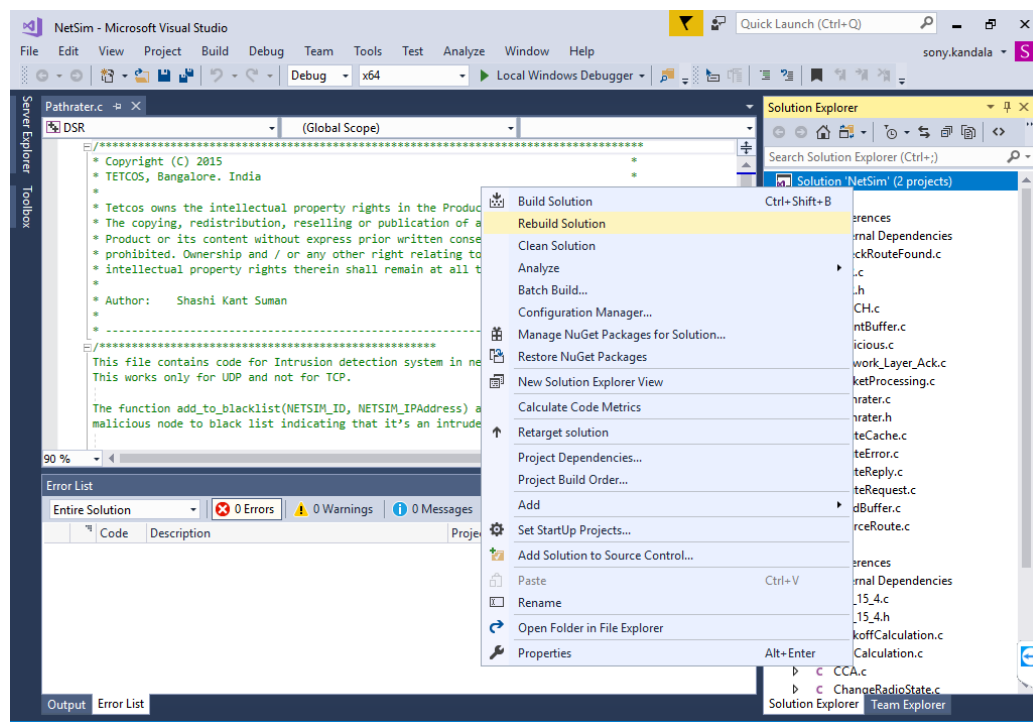
If `_NETSIM_WATCHDOG_` is defined, a watchdog timer starts the moment a packet is sent. Once a packet is forwarded to next hop node, the current node checks for watchdog timer duration if the packet is getting forwarded further on to destination node or not.

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 hop is marked by the current node as a malicious node.

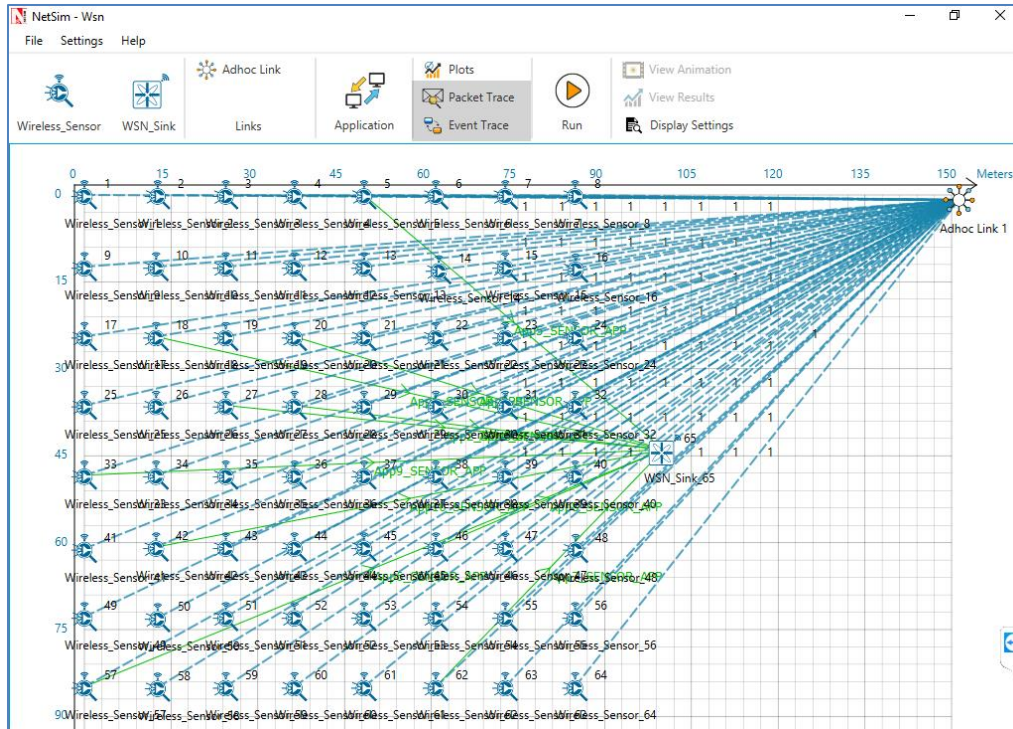
- These updated source files are added in folder DSR and Zigbee projects, which is attached along with.

Steps:

- Open the Code folder and double click on the NetSim.sln file to open the project in visual studio.
- Right click on the solution and select rebuild.



- Now copy the **libDSR.dll**, **libZigbee.dll** from the **DLL** folder.
- Replace the DLLs in NetSim bin folder in the NetSim installation directory (Eg: **C:\Program Files\NetSim Standard\bin**) after renaming the original dll files.
- Open the sample **Configuration.netsim** file provided in the **Config_File** folder along with this project which can be opened in NetSim directly



- 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 above
- Channel Characteristics is set to Pathloss only with LOG_DISTANCE as the path loss model. Path loss exponent is set to a high value 4
- Run the simulation
- 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 55 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 till 55s of simulation time and then it is changed
- 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
- 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		<input type="checkbox"/> Detailed View
DeviceID	Start Time (micro sec)	Detection Time (micro sec)
11	0.000000	56019606.400000

Dedicated Metrics for IDS