**Intrusion detection system for LEACH**

**Software:** NetSim Standard v13.2, Visual Studio 2022

**Project Download Link**:

<https://github.com/NetSim-TETCOS/IDS_LEACH_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>

**Example**

1. The **WorkSpace\_IDS\_in\_LEACH** 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\_in\_LEACH\_Example** from the list of experiments.
2. 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 shown below.

Graphical user interface, diagram, application

Description automatically generated

**Figure 1:** 64 sensors uniformly placed, with the SINKNODE

1. Wireless Link Properties

* Channel Characteristics - Pathloss only
* Path loss model - LOG\_DISTANCE
* Path loss exponent – 2.5

1. Run the simulation for 100 seconds.

**Results and discussion**

* 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.

Chart

Description automatically generated

Figure : Packet Animation Window

* You will also note that the cluster heads keep changing dynamically in Clusters 2, 3 and 4.
* In cluster1, initially the cluster members transmit 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. 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.

Graphical user interface, application, table, Excel

Description automatically generated

**Figure 3:** NetSim Packet trace after filtering Sensor 18, 20, 27 and 28 as source ID

* 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.

Graphical user interface, application, table, Excel

Description automatically generated

**Figure 4:** Undo filter in Source\_Id column and transmitter\_Id column by selecting only Sensor-11

* 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.

Table

Description automatically generated

**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.
* 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 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 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 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.