Simulating simple DDoS attacks in an IoT Network in NetSim

Modified on: Fri, 9 Feb, 2024 at 10:37 AM

Applicable versions	**NetSim Academic**	**NetSim Standard**	**Netsim Pro**

Applicable Releases	**v13.3**	**v14.0**

A DOS (Denial of Service) attack in IoT (Internet of Things) involves overwhelming a device or network with traffic in order to disrupt its normal operation and deny service to legitimate users. This can be achieved by flooding the network with a large volume of traffic or sending packets with malformed headers to exploit vulnerabilities in the target system. The impact of a DOS attack on an IoT device or network can be significant, as many IoT devices have limited processing power and memory resources. As a result, they may not be able to handle the large volume of traffic generated by the attack, leading to service disruptions or even device failures. When multiple attackers coordinate a DoS attack, it is known as a DDoS (Distributed Denial of Service) attack.

The article explains different types of DDoS (Distributed Denial of Service) attacks and the workspaces corresponding to these attacks are attached at the end of this article.

For instructions on importing the workspaces, please refer to the article - ***Downloading and Importing the workspace*** **(https://support.tetcos.com/en/support/solutions/articles/14000128666)**

Botnet Attack

A botnet attack in IoT (Internet of Things) is a type of cyber attack where a network of compromised IoT devices, such as smart home appliances, security cameras, and routers, is used to carry out malicious activities. In a botnet attack, a hacker gains control of a large number of IoT devices, often through exploiting vulnerabilities or weak security measures, and uses them to launch coordinated attacks.

Once a hacker has control of a botnet, they can carry out a variety of malicious activities, including:

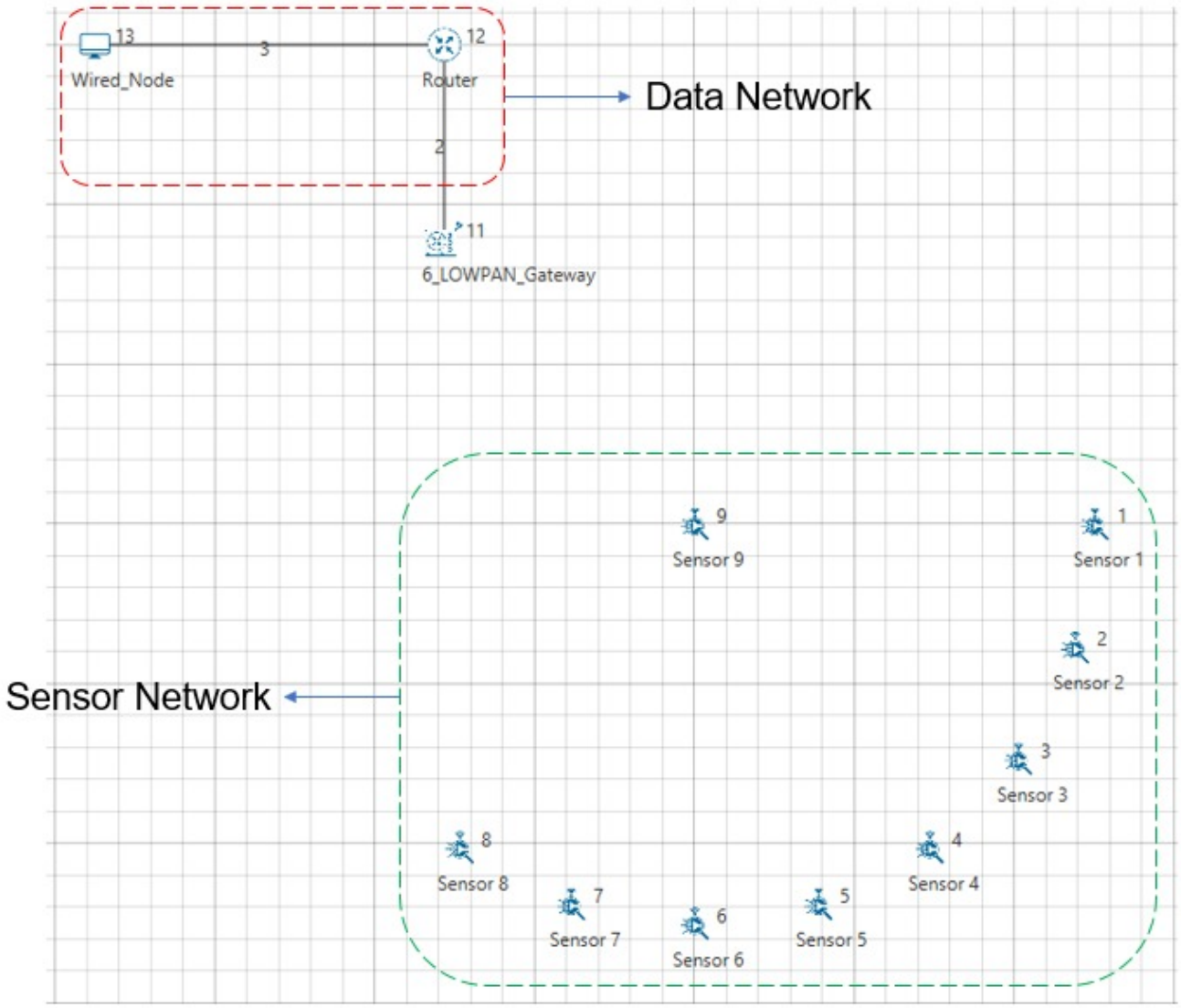
1. DDoS attacks: A distributed denial-of-service (DDoS) attack floods a website or network with traffic, making it unavailable to legitimate users.
2. Data theft: A hacker can use a botnet to steal sensitive data, such as financial information or personal data, from devices on the network.
3. Spamming: A botnet can be used to send large volumes of spam emails or messages.
4. Cryptomining: A hacker can use a botnet to mine cryptocurrency using the processing power of compromised devices.

We explain below how to simulate a simple DDoS attack in an IOT Network in NetSim. Config files for both cases are attached.

Case 1: Without a Malicious Node (No attacker).

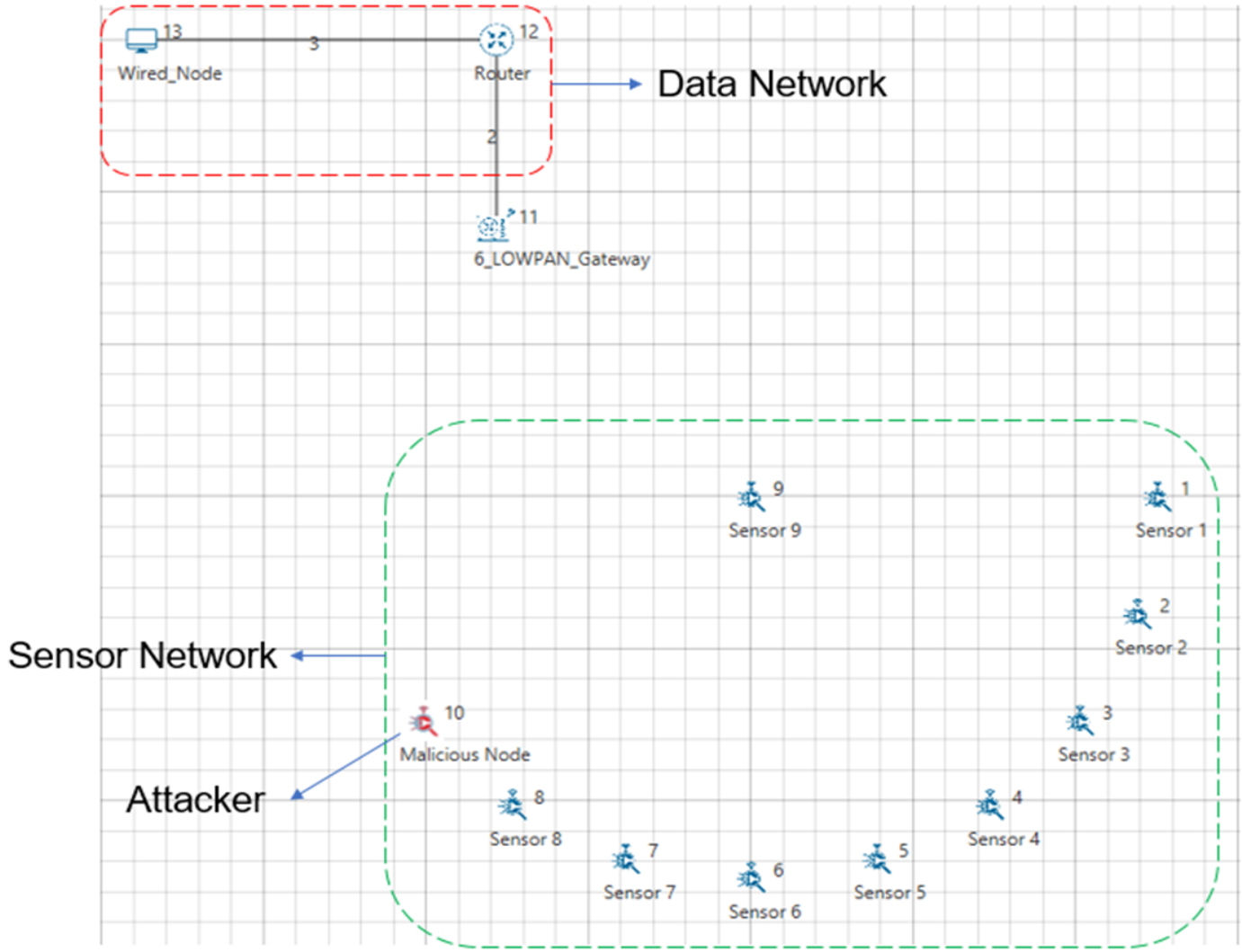
In NetSim, click on New Simulation > Internet of Things

- Drop 9 Sensors, 1 6LOWPAN gateway, 1 router, and 1 wired node as shown in the figure below.
- Set the routing protocol to RPL in the sensors.
- Set wireless link channel characteristics as path loss only.
- Pathloss model = Log Distance with Pathloss exponent = 4.5.
- Configure traffic from all sensors 1 through 8 such that the packets are transmitted to the gateway via sensor 9. The traffic rate is low; it is 20 packets per second.
- This parameter set is considered for this particular example and can be suitably modified by the user based on their scenario.
- Run the simulation for 100 seconds and measure the throughput obtained by sensors 1 through 8.



Case 2: With a Malicious Node (With a DOS attack node)

- Same model as case 1 with the additional malicious node
- Configure traffic from all sensors 1 through 8 such that the packets are transmitted to the gateway via sensor 9. The traffic rate is low; it is 20 packets per second.
- Add a malicious node 10. Configure traffic such that packets are transferred via sensor 9. This has a "high" generation rate to flood the network; it is 1000 packets per second.
- Run the simulation for 100 seconds and measure the throughput obtained by sensors 1 through 8.



Results (v14.0/v13.3)

Application	Case 1 - Normal Operation Throughput (Mbps)	Case 2 - DDoS Attack Throughput (Mbps)
Sensor 1	0.003789	0.000712
Sensor 2	0.001201	0.000192
Sensor 3	0.004383	0.00076
Sensor 4	0.007476	0.001221
Sensor 5	0.005849	0.003633
Sensor 6	0.004195	0.003338
Sensor 7	0.001424	0.001544
Sensor 8	0.006226	0.004386
Malicious Node	N/A	0.014886
Sum Throughput (Mbps) Sensor 1 through 8	**0.034543 (34.54 Kbps)**	**0.015786 (15.78 Kbps)**

We see that the introduction of the malicious node led to a more than 50% drop in throughput, from 34.54 to 15.78 Kbps.

Bit-and-piece attack

A "bit and piece" DDoS attack in an IoT network is a type of Distributed Denial of Service (DDoS) attack that targets Internet of Things (IoT) devices by sending small amounts of traffic to a large number of devices. This type of attack is also known as a low-rate DDoS attack.

In a bit-and-piece attack, the attacker sends a small amount of traffic to multiple IoT devices, such as smart home appliances, security cameras, or routers. The traffic may include a range of packet types, such as TCP, UDP, and ICMP, and the packets may be sent intermittently over a long period of time.

Because the traffic is distributed across many devices, each individual device receives a small amount of traffic that is difficult to distinguish from legitimate traffic. However, when combined, the traffic overwhelms the network and causes a denial of service for legitimate users trying to access the network.

We explain below how to simulate a simple Bit-and-piece DDoS attack in an IOT Network in NetSim. Config files for the below cases are attached.

In NetSim, click on New Simulation > Internet of Things

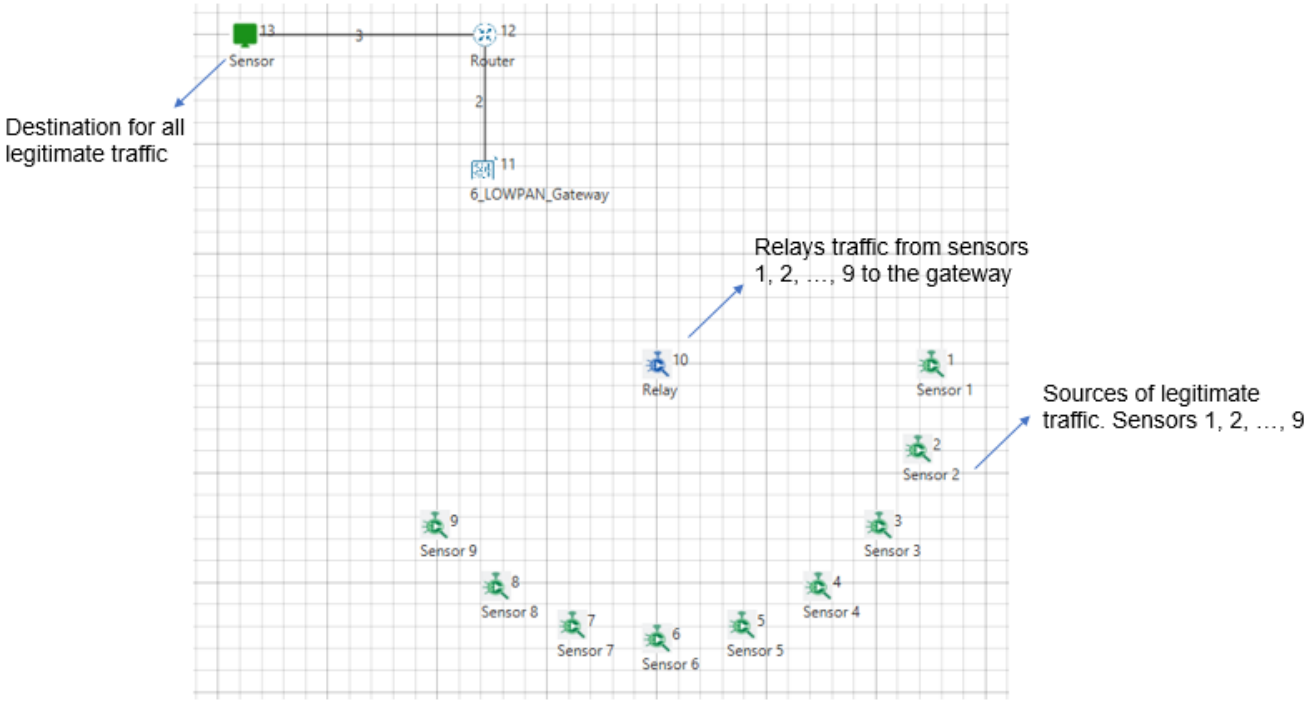
- Drop 10 sensors, 1 6LOWPAN Gateway, Router and 1 Wired node (server)
- Configure 9 applications. Each application is from a sensor (1, 2, …, 9) to the server, such that packets of size 50 Bytes are sent at a rate of 20 packets/ sec.
- The network topology and routing are such that traffic from all sensors flow through sensor 10, and then to the gateway and onwards to the server. We call this as **case #1**.

We then simulate 3 attack cases

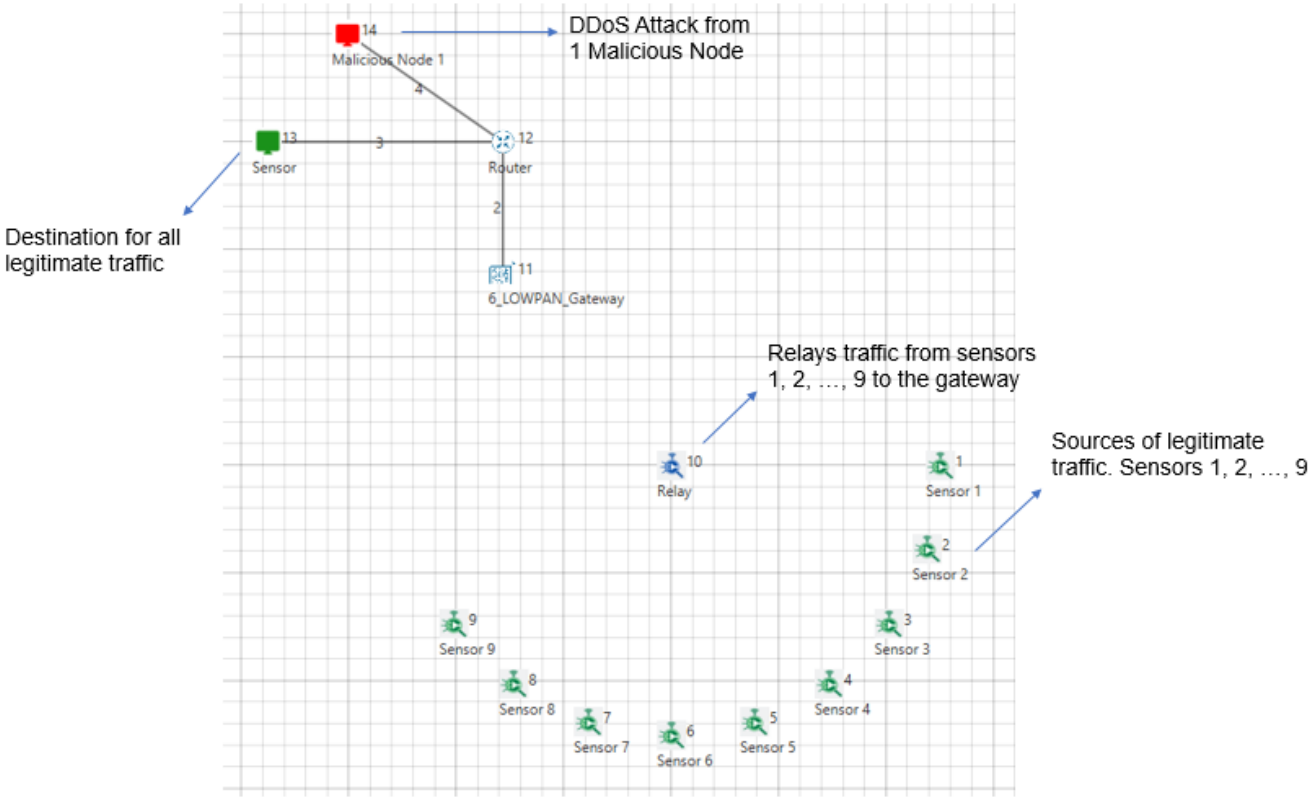
- **Case 2:** Add 1 malicious node (wired). Configure traffic from malicious node to all sensors (1, 2, …, 9). Packets of size 10 Bytes (representing a small amount of attack data) are sent at a rate of 20 packets/sec exponentially.
- **Case 3:** Add 2 malicious nodes (wired). Configure traffic from 2 malicious nodes to all sensors (1, 2, …, 9). Packets of size 10 Bytes (representing a small amount of attack data) are sent at a rate of 20 packets/sec exponentially.
- **Case 4:** Add 3 malicious nodes (wired). Configure traffic from 3 malicious nodes to all sensors (1, 2, …, 9). Packets of size 10 Bytes (representing a small amount of attack data) are sent at a rate of 20 packets/sec exponentially.
- Run the simulation for 100 seconds.

Compare network performance

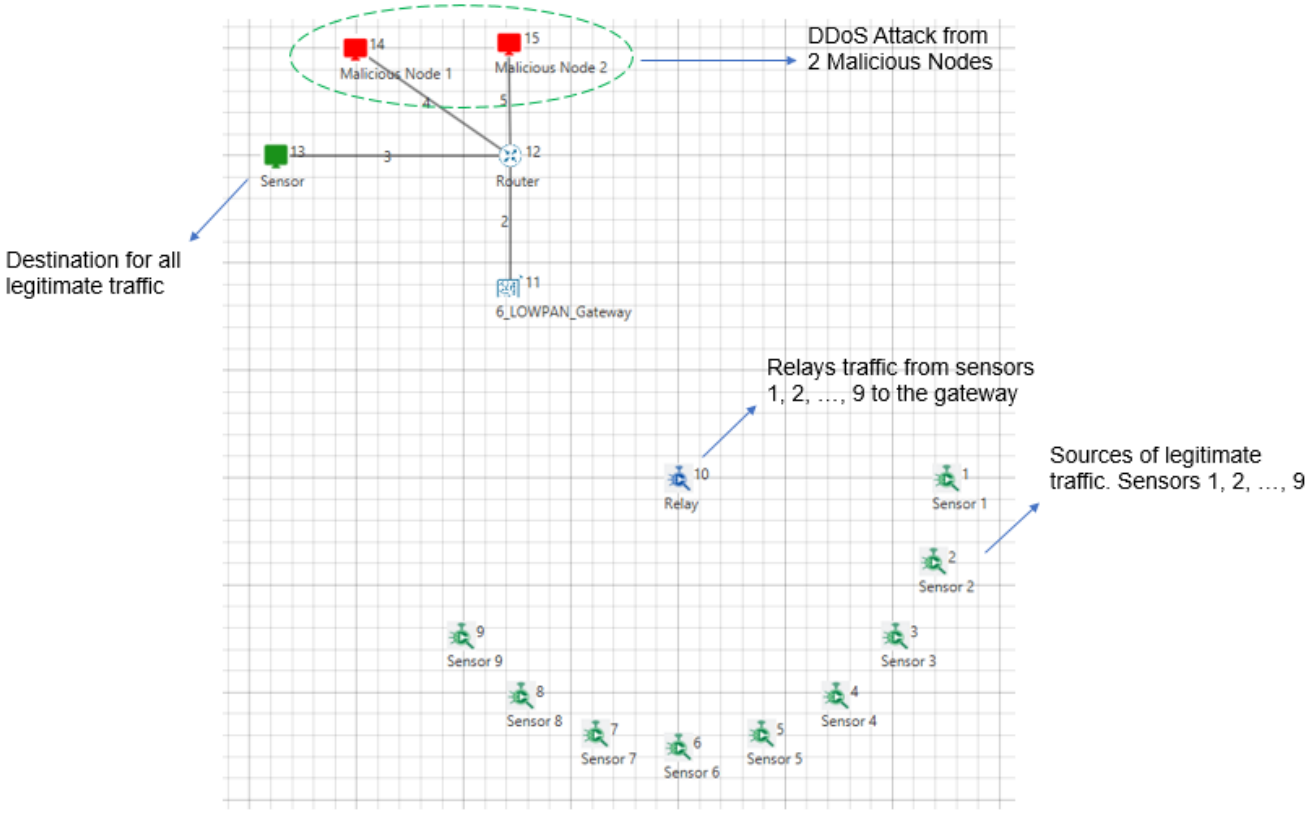
- We take sum throughput of the “Sensor applications” as our measure of performance


13
Sensor
3
12
Router
2
11
6_LOWPAN_Gateway
Destination for all legitimate traffic
Relays traffic from sensors 1, 2, …, 9 to the gateway
10
Relay
1
Sensor 1
Sources of legitimate traffic. Sensors 1, 2, …, 9
2
Sensor 2
9
Sensor 9
3
Sensor 3
8
Sensor 8
4
Sensor 4
7
Sensor 7
6
Sensor 6
5
Sensor 5

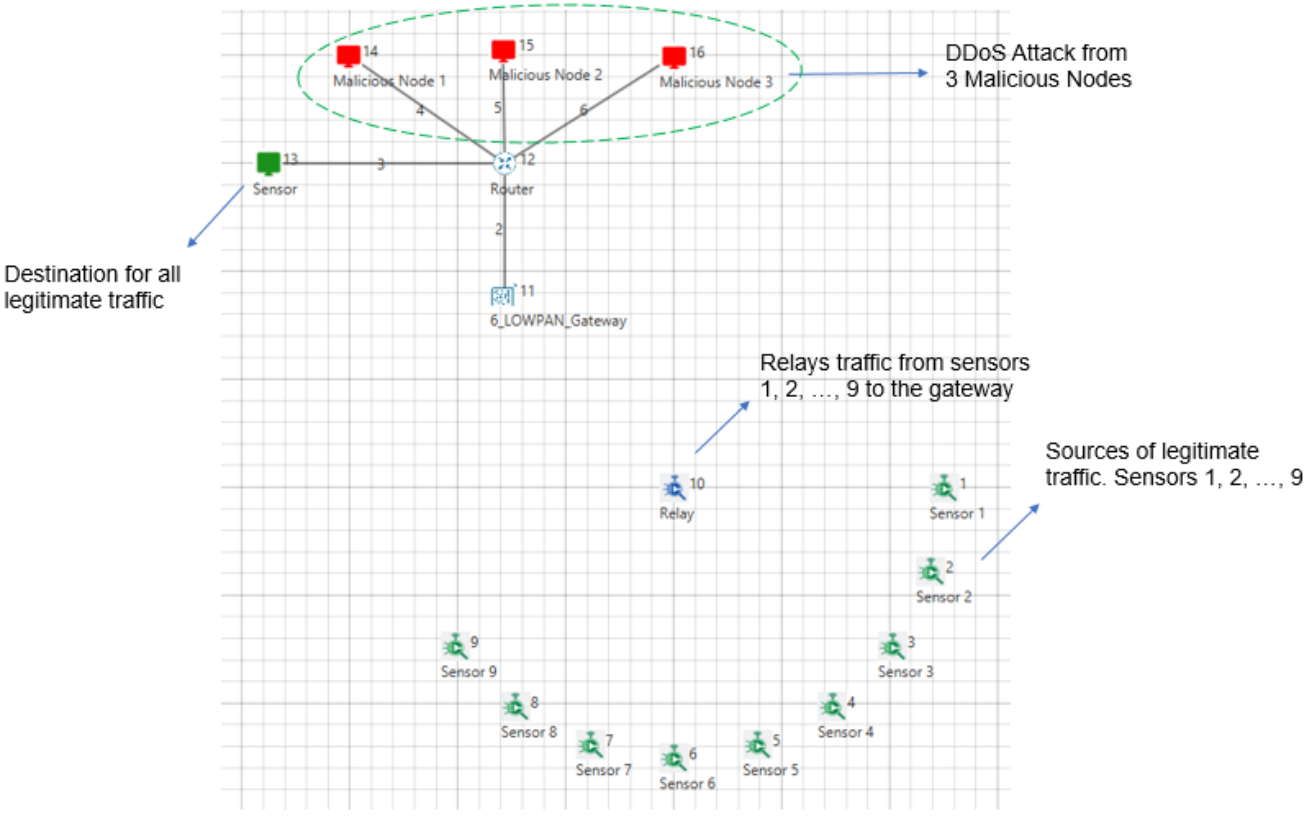
Case 1


14
Malicious Node 1
DDoS Attack from 1 Malicious Node
4
13
Sensor
3
12
Router
2
11
6_LOWPAN_Gateway
Destination for all legitimate traffic
Relays traffic from sensors 1, 2, …, 9 to the gateway
10
Relay
1
Sensor 1
Sources of legitimate traffic. Sensors 1, 2, …, 9
2
Sensor 2
9
Sensor 9
3
Sensor 3
8
Sensor 8
4
Sensor 4
7
Sensor 7
6
Sensor 6
5
Sensor 5

Case 2



Case 3



Case 4

Results (v14.0/13.3)

When the network uses **UDP protocol** the output results are as follows:

Application	Case 1 : Normal Operation Throughput (Mbps)	Case 2 : 1 - attacker node Throughput (Mbps)	Case 3: 2 - attacker nodes Throughput (Mbps)	Case 4: 3 - attacker nodes Throughput (Mbps)

Sensor 1	0.003577	0.002401	0.001968	0.001752
Sensor 2	0.000853	0.000672	0.000596	0.00048
Sensor 3	0.002185	0.001577	0.001445	0.001233
Sensor 4	0.007332	0.004942	0.003966	0.003546
Sensor 5	0.004501	0.003417	0.002724	0.002428
Sensor 6	0.004527	0.00317	0.002582	0.002242
Sensor 7	0.001184	0.000976	0.000788	0.000672
Sensor 8	0.006346	0.004406	0.003609	0.002953
Sensor 9	0.002189	0.001625	0.001329	0.001089
Sum Throughput (Mbps) of Legitimate Traffic	**0.032694 (32.6 Kbps)**	**0.023186 (23.1Kbps)**	**0.019007 (19.1Kbps)**	**0.016395 (16.3Kbps)**

We observe:

- A ≈ 25% drop in throughput of legitimate traffic with 1 bit-and-piece DDoS attack node.
- A ≈ 50% drop in throughput of legitimate traffic with 3 bit-and-piece DDoS attack nodes.

Slow HTTP DoS attack

A slow HTTP Denial of Service (DoS) attack is a type of DDoS attack that exploits the HTTP protocol's weakness by sending a request to a server in a slow and controlled manner. This type of attack overwhelms the web server by keeping the connections open and sending slow requests in a way that the server cannot respond to legitimate requests from other clients. Slow HTTP attacks can target different layers of the HTTP protocol, such as the application layer, transport layer, or network layer.

The SlowHTTP test tool is a software application that simulates a Slow HTTP Denial of Service (DoS) attack on a web server to test its ability to handle such attacks. These tools are designed to send a slow and controlled HTTP request to a server, which can help identify potential vulnerabilities that could be exploited by attackers.

We can perform a SlowHTTP DoS attack using NetSim Emulator. For more information click on the link given below.

https://support.tetcos.com/support/solutions/articles/14000130254-how-to-perform-slowhttptest-dos-attack-through-netsim-emulator- (https://support.tetcos.com/support/solutions/articles/14000130254-how-to-perform-slowhttptest-dos-attack-through-netsim-emulator-)

Useful links

1. NetSim IoT Library Overview: **https://www.tetcos.com/iot-wsn.html** (https://www.tetcos.com/iot-wsn.html)
2. NetSim v14 IoT Documentation: (https://www.tetcos.com/help/v13.3/Technology-Libraries/IOT-WSN.html)**https://tetcos.com/downloads/v14/IOT-WSN.pdf** (https://tetcos.com/downloads/v14/IOT-WSN.pdf)