

Sinkhole Attack in AODV

Software: NetSim Standard v14.1, Visual Studio 2022

Project Download Link:

<https://github.com/NetSim-TETCOS/Sinkhole-Attack-in-AODV-v14.1/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>

Introduction

Sinkhole attack is one of the most severe attack in wireless ad hoc networks. In a sinkhole attack, a compromised or malicious node advertises false routing information to pretend itself as a specific node and receives whole network traffic. After receiving the whole network traffic, it can either modify the packet information or drop them to make the network complicated. Sinkhole attacks affect the performance of ad hoc network protocols such as the AODV protocol.

Real-World Context

In a real-world scenario, a small ad-hoc network consists of a few laptops and mobile devices wirelessly connected to each other. When one node in this network is malicious, the impact can be significant.

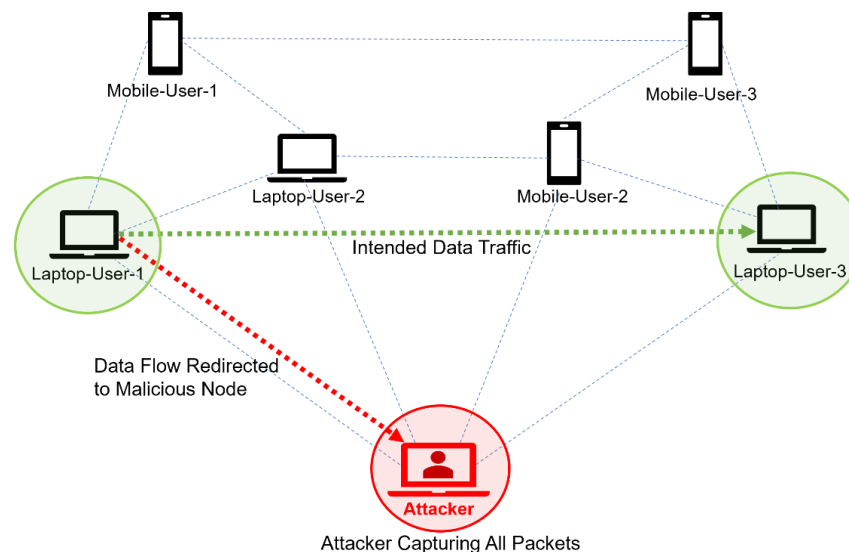


Figure 1: Real world scenario for sinkhole attack in MANET using AODV

Sinkhole attack overview

- The malicious node (attacker) enters the network and starts intercepting and diverting network traffic.
- When Laptop-User-1 attempts to communicate with Laptop-User-3, the malicious node (attacker) intercepts the communication by responding to route requests and diverting data packets.
- As a result, the data that Laptop-User-1 intended for Laptop-User-3 gets redirected to the malicious node (attacker). This could include sensitive information, files, or any data being exchanged.
- The malicious node (attacker) intentionally discards all incoming data packets, effectively preventing the data from reaching its intended destination.

NetSim's Role

We use NetSim to simulate and analyze sinkhole attacks, aiding in the understanding of security vulnerabilities. NetSim offers us the means to replicate real-world scenarios within a controlled, virtual environment.

This document will provide a comprehensive overview of our project's objectives for studying the sinkhole attacks.

Implementation in AODV

- In AODV, the source broadcasts the RREQ packet during route discovery.
- The destination, upon receiving the RREQ packet, replies with an RREP packet containing the route to reach the destination.
- Intermediate nodes can also send RREP packets to the source if they have a route to the destination in their route cache.
- Taking advantage of this, a malicious node adds a fake route entry into its route cache, with the destination node as its next hop.
- Upon receiving the RREQ packet from the source, the malicious node sends a fake RREP packet with the fake route.
- The source node, upon receiving this fake RREP packet, perceives it as a better route to the destination.

- All network traffic is then attracted toward the sinkhole (malicious node), which can either modify the packet information or simply drop the packets.

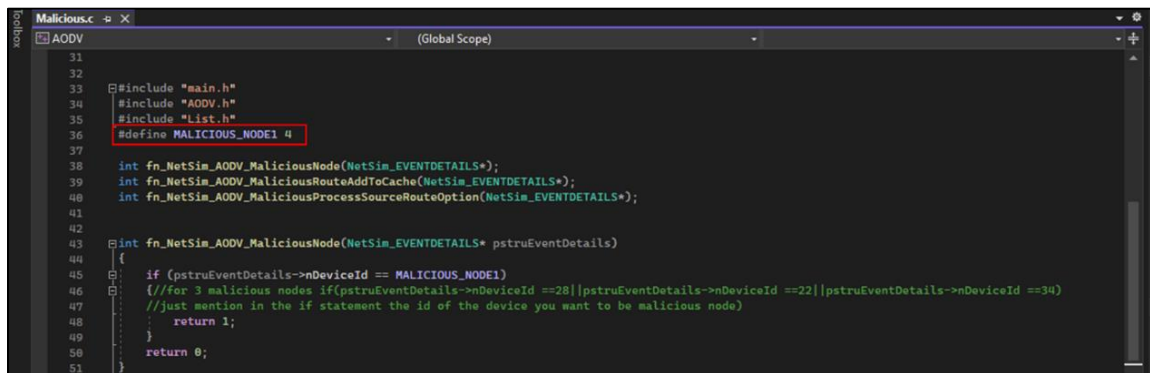
A file named `malicious.c` is added to the AODV project, which contains the following functions:

- **`fn_NetSim_AODV_MaliciousNode()`**; // This function is used to identify whether the current device is malicious or not in order to establish malicious behavior.
- **`fn_NetSim_AODV_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_AODV_MaliciousProcessSourceRouteOption()`**; // This function is used to drop the received packets if the device is malicious, instead of forwarding the packet to the next hop.

You can set any device as a malicious node, and you can have more than one malicious node in a scenario. The device IDs of the malicious nodes can be set inside the **`fn_NetSim_AODV_MaliciousNode()`** function.

Steps to simulate:

1. Open the source code in Visual studio by navigating to “Your work” on the home screen of NetSim. Then, select “Source code” and click on “Open Code”.
2. Expand the AODV project, open the `malicious.c` file, and set the malicious node id.



```

31
32
33 #include "main.h"
34 #include "AODV.h"
35 #include "List.h"
36 #define MALICIOUS_NODE1 4
37
38 int fn_NetSim_AODV_MaliciousNode(NetSim_EVENTDETAILS*);
39 int fn_NetSim_AODV_MaliciousRouteAddToCache(NetSim_EVENTDETAILS*);
40 int fn_NetSim_AODV_MaliciousProcessSourceRouteOption(NetSim_EVENTDETAILS*);
41
42
43 int fn_NetSim_AODV_MaliciousNode(NetSim_EVENTDETAILS* pstruEventDetails)
44 {
45     if (pstruEventDetails->nDeviceId == MALICIOUS_NODE1)
46         { //for 3 malicious nodes if(pstruEventDetails->nDeviceId ==28||pstruEventDetails->nDeviceId ==22||pstruEventDetails->nDeviceId ==34)
47             //just mention in the if statement the id of the device you want to be malicious node)
48             return 1;
49         }
50     return 0;
51 }

```

Figure 2: Set malicious node in the malicious .c file

3. Now right-click on the AODV project and rebuild it.

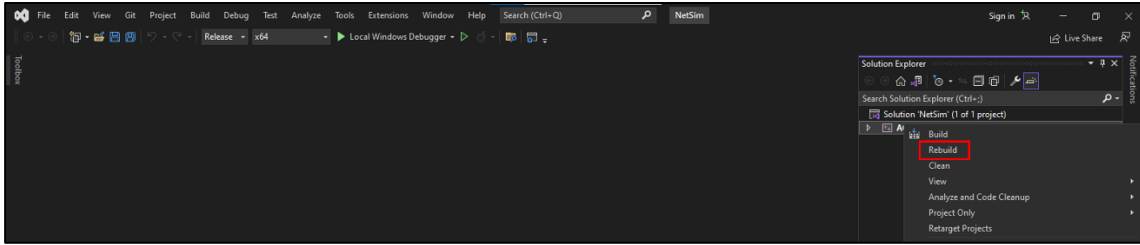


Figure 3: NetSim AODV project source code in Visual studio

4. Upon rebuilding, libAODV.dll will automatically get updated in the respective bin folder of the current workspace.

Example

1. The **Sinkhole-Attack-in-AODV-Workspace** comes with a sample network configuration that is already saved. To open this example, go to “Your work” in the home screen of NetSim and click on the **Sinkhole-Attack-in-AODV-Example** from the list of experiments.
2. The network consists of 7 wireless nodes with the properties configured as shown below:

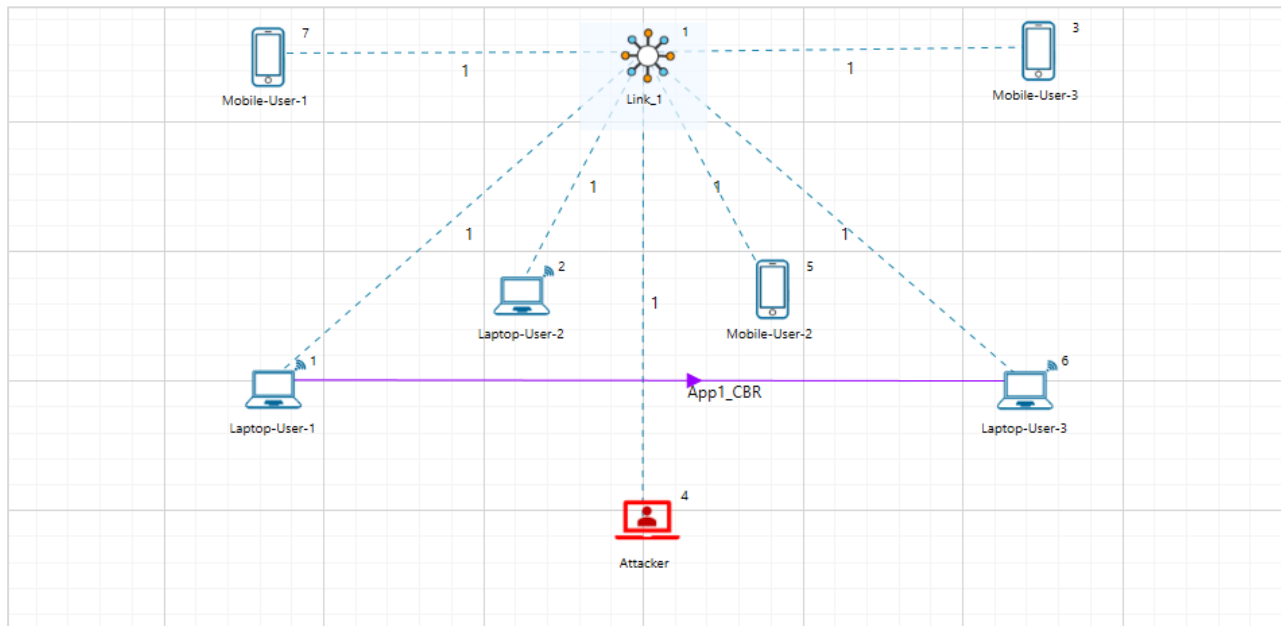


Figure 4: Network Topology

3. Set the Application properties.

Application Properties	
Source ID	1
Destination ID	6

Table 1: Application Properties

4. In the Link set the Channel characteristics: **Pathloss only**, Pathloss model: **Log Distance**, Pathloss exponent: **3**

- Run the simulation for 100 seconds.

Results and discussion

In the packet trace, we illustrate the impact of a malicious node within the MANET, showcasing how it disrupts the normal data transfer process.

PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID
2	0 N/A	Control_Packet	AODV_RREQ	NODE-1	Broadcast-0	NODE-1	NODE-2
3	0 N/A	Control_Packet	AODV_RREQ	NODE-1	Broadcast-0	NODE-2	NODE-1
4	0 N/A	Control_Packet	AODV_RREQ	NODE-1	Broadcast-0	NODE-2	NODE-4
5	0 N/A	Control_Packet	AODV_RREQ	NODE-1	Broadcast-0	NODE-2	NODE-5
6	0 N/A	Control_Packet	AODV_RREP	NODE-4	NODE-1	NODE-4	NODE-2
8	0 N/A	Control_Packet	AODV_RREP	NODE-4	NODE-1	NODE-2	NODE-1
10	1	0 CBR	App1_CBR	NODE-1	NODE-6	NODE-1	NODE-2
12	1	0 CBR	App1_CBR	NODE-1	NODE-6	NODE-2	NODE-4

Figure 5: Analysis of results using packet trace

- From the above screenshot, you will see that the malicious node, node-4, sends an **AODV_RREP** (Route Reply) upon receiving an **AODV_RREQ** (Route Request), attracting packets toward it.
- While node-4 (the malicious node) tries to send a Route Reply (**AODV_RREP**), the legitimate destination, Node-6, also attempts to reply with **AODV_RREP** packets.
- However, node-4's **AODV_RREP** reply is favored because it pretends to be the next node to the destination, even though node-6 is the actual destination.
- The malicious node-4 tries to mislead the network by pretending to be closer to the destination compared to the route reply sent by the actual destination.
- You will also find that the data packets generated by node-1 are not forwarded by the malicious node-4.

This will have a direct impact on the application throughput, which can be observed in the application metrics table in the NetSim simulation results window. The throughput for application 1 registers as zero due to the presence of a malicious node (device Id 4) in the network. This node intentionally drops all data packets instead of transmitting them to their intended destination.

Application Metrics					
End-to-end performance of applications running across the network.					
Application ID	Application Name	Throughput (Mbps)	Delay (μ s)	Packets Generated	Packets Received
1	App1_CBR	0.000000	0.000000	4750	0

Figure 6: Result Dashboard

References

- [1] F. A. K. Humaira Ehsan, "Malicious AODV Implementation and Analysis of Routing Attacks in MANETs," *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*.