**Sink Hole Attack in AODV**

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

**Project Download Link:**

Sinkhole attack is one of the severe attacks in wireless Ad hoc network. In sinkhole Attack, a compromised node or malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. After receiving 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 networks protocols such as DSR, AODV protocol.

|  |  |
| --- | --- |
| Graphical user interface, diagram, application  Description automatically generated  Figure : network configuration of how the traffic flow is configured | Diagram  Description automatically generated  Figure : Network configuration of actual traffic flow along with the working of malicious node |

**Implementation in AODV**

* In AODV the source broadcasts RREQ packet during Route Discovery.
* The destination on receiving the RREQ packet replies with a RREP packet containing the route to reach the destination.
* But Intermediate nodes can also send RREP packet to the source if they have a route to the destination in their route cache.
* Using this as an advantage the malicious node adds a fake route entry into its route cache with destination node as its next hop.
* On receiving the RREQ packet from the source the malicious node sends a fake RREP packet with the fake route.
* The source node on receiving this packet observes this as a better route to the destination.
* All the Network Traffic is attracted towards the Sinkhole (Malicious Node) and it can either modify the packet Information or simply drop the packet.

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

* **fn\_NetSim\_AODV\_MaliciousNode();** //This function is used to identify whether a 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 malicious, and you can have more than one malicious node in a scenario.

Device ids of malicious nodes can be set inside the **fn\_NetSim\_AODV\_MaliciousNode()** function.

**Steps to simulate**

1. Open the Source codes in Visual Studio by going to Your work -> Source Code and clicking on Open code button in NetSim Home Screen window
2. Expand AODV project and open Malicious.c file and set malicious node id.

Graphical user interface, text, application

Description automatically generated

Figure 3: Set Malicious Node in malicious.c file

1. Now right click on AODV project and rebuild it.

Graphical user interface

Description automatically generated

Figure 4:Screenshot of NetSim project source code in Visual Studio

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

**Example**

1. The **Sink\_Hole\_Attack\_AODV** 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 **SinkHole\_Attack\_AODV\_Example** from the list of experiments.
2. The network consists of 6 wireless nodes with the properties configured as shown below:

Chart

Description automatically generated

Figure 5: Network topology

1. Application Properties

|  |  |
| --- | --- |
| Application Properties | |
| Source ID | **1** |
| Destination ID | **6** |
| Sinkhole(Malicious Node) | **4** |

Table : Application properties

1. Channel Characteristics **pathloss only**, Path Loss Model: **Log Distance**, Path Loss Exponent: **3**
2. Run the Simulation for 100 seconds

**Results and discussions**

1. View the packet animation, You will find the malicious node (Device id 4) gives Route Reply on receiving Route Request and attracts packets towards it. You will also find that the malicious node does not forward the packets that it receives.

Chart, bubble chart

Description automatically generated

Figure : Animation window

1. 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.

Graphical user interface, application, table, Excel

Description automatically generated

Figure 6: Result Dashboard