Sink Hole Attack in NetSim

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.

**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 the 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 DSR project which contains the following functions:

* fn\_NetSim\_AODV\_MaliciousNode ( )

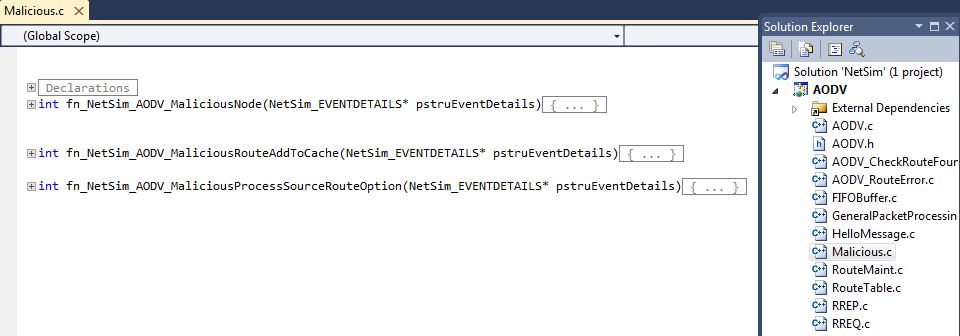
This function is used to identify whether a current device is malicious or not in-order to establish malicious behavior.

* 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 ()

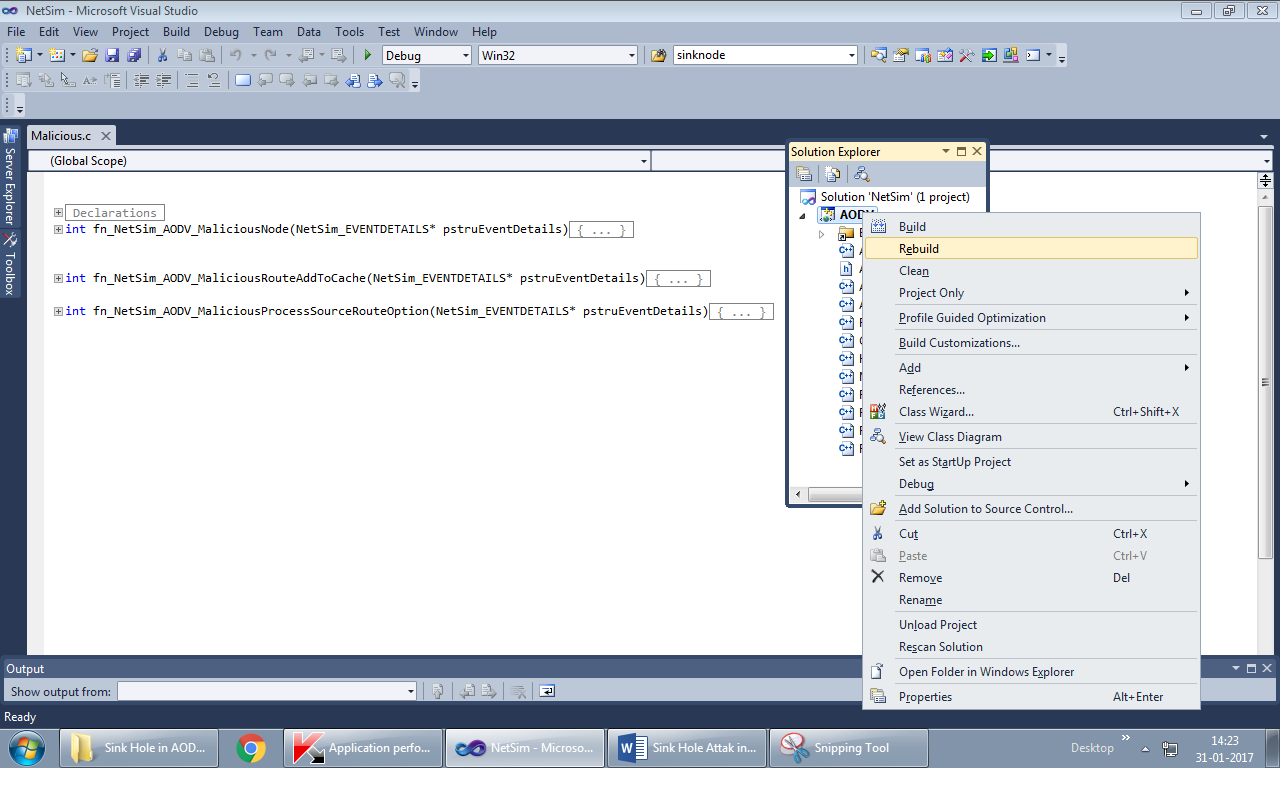
This function is used to drop the received packets if the device is malicious, instead of forwarding the packet to the next hop.



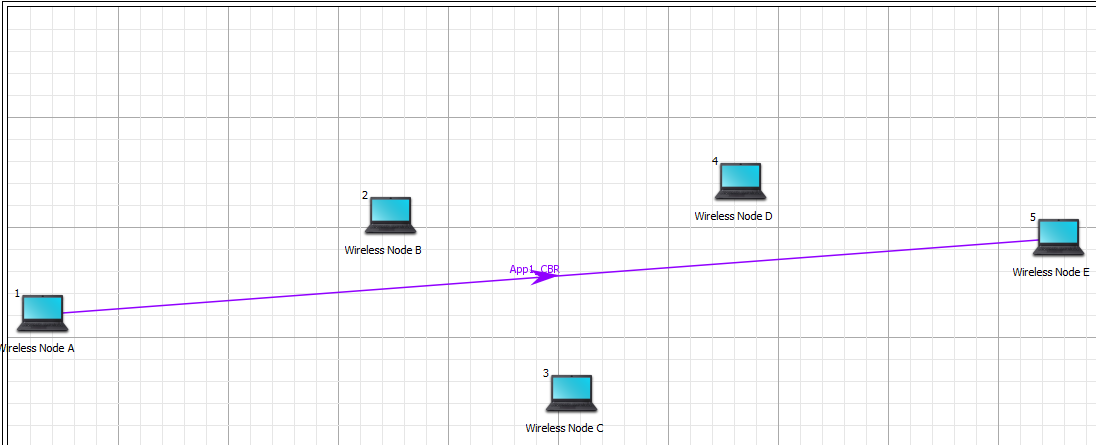
You can set any device as malicious and you can have more than one malicious node in a scenario. Device id’s of malicious nodes can be set inside the fn\_NetSim\_AODV\_MaliciousNode () function.

**Steps to run Sinkhole Attack code in NetSim:**

1. Open the Simulation – Sinkhole Attack folder and double click on the NetSim.sln fie to open the project in Visual Studio.
2. Now right click on AODV project in the solution explorer and select Rebuild.



1. Now Copy the newly built libAODV.dll from the DLL folder inside the Simulation – Sinkhole Attack directory.
2. Replace the DLL in NetSim bin folder in the NetSim installation directory, after renaming the original libAODV.dll file.
3. Create a network scenario in MANET with UDP running in the Transport Layer.
4. For example, you can create a scenario as shown in the following screenshot:



Malicious

Destination

Source

Source – Device id 1

Destination – Device id 5

Sinkhole (malicious node) – Device id 2

1. In environment properties set,

Channel characteristics – Line of sight

Path loss Exponent – 2.7

1. Run the Scenario.
2. View the packet animation. You will find that the malicious node (Device id 2) gives Route Reply on receiving Route Request and attracts packets towards itself. You will also find that the malicious node does not forward the packets that it receives.