

Sink Hole Attack in MANET using DSR

Software Recommended: NetSim Standard v11.0, Visual Studio 2015/2017

Project Download Link:

https://github.com/NetSim-TETCOS/SINK_HOLE_DSR_v11.0/archive/master.zip

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 protocol.

Implementation in DSR:

- In DSR 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_DSR_MaliciousNode()`

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

- `fn_NetSim_DSR_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.

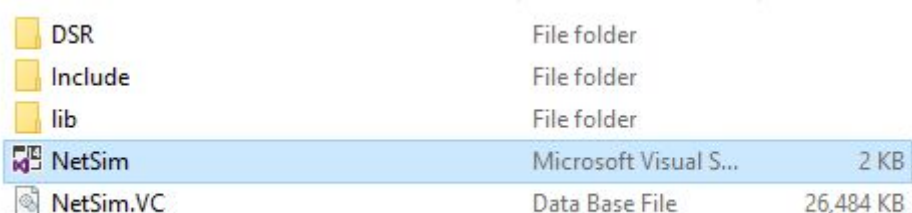
- `fn_NetSim_DSR_MaliciousProcessSourceRouteOption()`

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_DSR_MaliciousNode()` function.

Steps:

1. Open the Sinkhole Attack folder and double click on the **NetSim.sln** file to open the project in Visual Studio.



DSR	File folder	
Include	File folder	
lib	File folder	
NetSim	Microsoft Visual S...	2 KB
NetSim.VC	Data Base File	26,484 KB

2. Set malicious node id.

```

31
32      /* Malicious Node */
33
34
35      #include "main.h"
36      #include "DSR.h"
37      #include "List.h"
38      #define MALICIOUS_NODE1 4
39
40      int fn_NetSim_DSR_MaliciousNode(NetSim_EVENTDETAILS* );
41      int fn_NetSim_DSR_MaliciousRouteAddToCache(NetSim_EVENTDETAILS*);
42      int fn_NetSim_DSR_MaliciousProcessSourceRouteOption(NetSim_EVENTDETAILS*);
43
44
45      int fn_NetSim_DSR_MaliciousNode(NetSim_EVENTDETAILS* pstruEventDetails){{ ... }}
46
47
48      int fn_NetSim_DSR_MaliciousRouteAddToCache(NetSim_EVENTDETAILS* pstruEventDetails){{ ... }}
49

```

3. Now right click on DSR project in the solution explorer and select Rebuild.

```

31
32      /* Malicious Node */
33

```

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



Source – Device id 1

Destination – Device id 6

Sinkhole (malicious node) – Device id 4

Link Properties (Adhoc link1)

Channel characteristics – Path Loss only

Path Loss model – LOG DISTANCE

Path Loss Exponent: 3

8. Run the Simulation for 100 seconds.
9. View the packet animation. You will find that 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.
10. 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.

