**Secure AODV in MANET**

**Software:** NetSim Standard v14.0, Microsoft Visual Studio 2022

**Project Download Link:**

Follow the instructions specified in the following link to download and set up the Project in NetSim:

[https://support.tetcos.com/en/support/solutions/articles/14000128666-downloading-and-setting-up-netsim-file-exchange-projects](about:blank)

**Introduction:**

SAODV is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism by providing security features like integrity and authentication. The reason only route discovery is secured by AODV is that data messages can be protected using a point-to-point security protocol like IPSec. SAODV uses a key management system, and each node maintains public keys, encryption keys, and decryption keys.

To implement SAODV, we have added **Secure AODV.c, RSA.c, and Malicious.c** files in the AODV project. RSA.c file is used to generate keys, encrypt, and decrypt the data. Users can implement their own encryption algorithms by changing the RSA.c file. malicious.c file is used to identify malicious nodes present in the network.

**Real-World Context:**

In the context of military communication, the secure AODV protocol ensures the secure transmission of data from higher-level commands to lower-level commands. This protocol utilizes encryption and decryption keys to ensure that all devices can securely access and read the data. If a malicious device is present in the middle level, the data will not be accessible or readable to the malicious device.

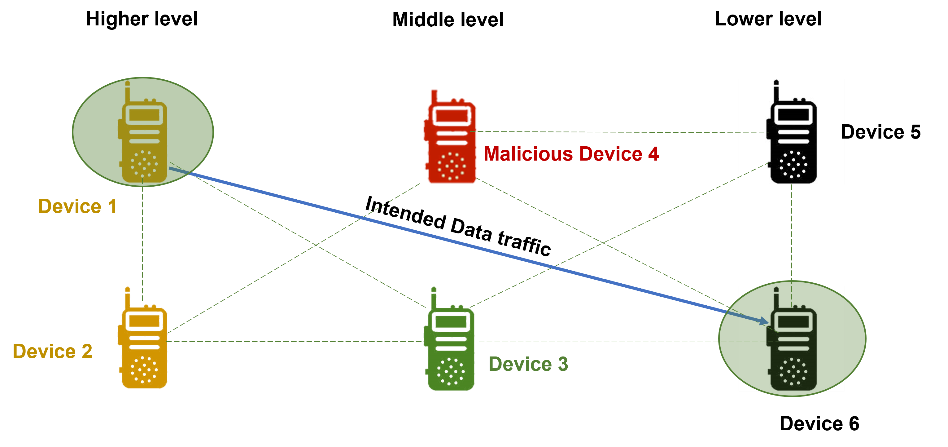


Figure 1:Secure AODV in Military communication using Manet

**Secure AODV Overview:**

1. To discover a route to Device 6, Device 1 sends an RREQ encrypted with Device 6's public key.
2. When Device 6 receives the RREQ, it decrypts it with its private key.
3. Device 6 then sends an RREP back to Device 1, encrypted with Device-1's public key.
4. Device 1 decrypts the RREP with its private key.

If a malicious device tries to intercept the RREQ or RREP, it will not be able to decrypt it because it does not have the private keys of Device 1 or Device 6. Additionally, if a malicious device tries to modify the RREQ or RREP, the other nodes in the network will be able to detect the modification and discard the packet.

**Case 1:**

**Secure AODV implementation:**

1. The **Secure-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 **Secure-AODV-Example** from the list of experiments.
2. After running the simulation, a **Secure\_AODV.log** file gets created in the Result Dashboard Window.

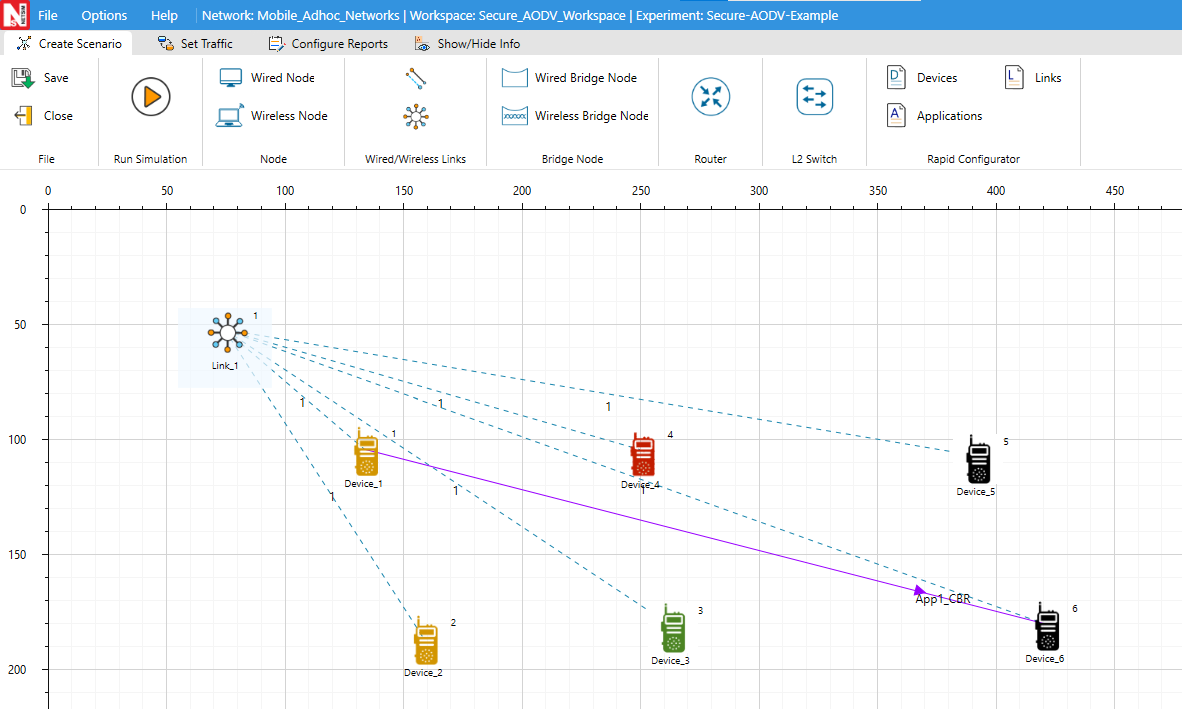


Figure 2: Network setup for Secure AODV in Manet

* Open the Source code in Visual Studio by going to Your work -> Source Code and Open code in the NetSim Home Screen window.
* Expand the AODV project.

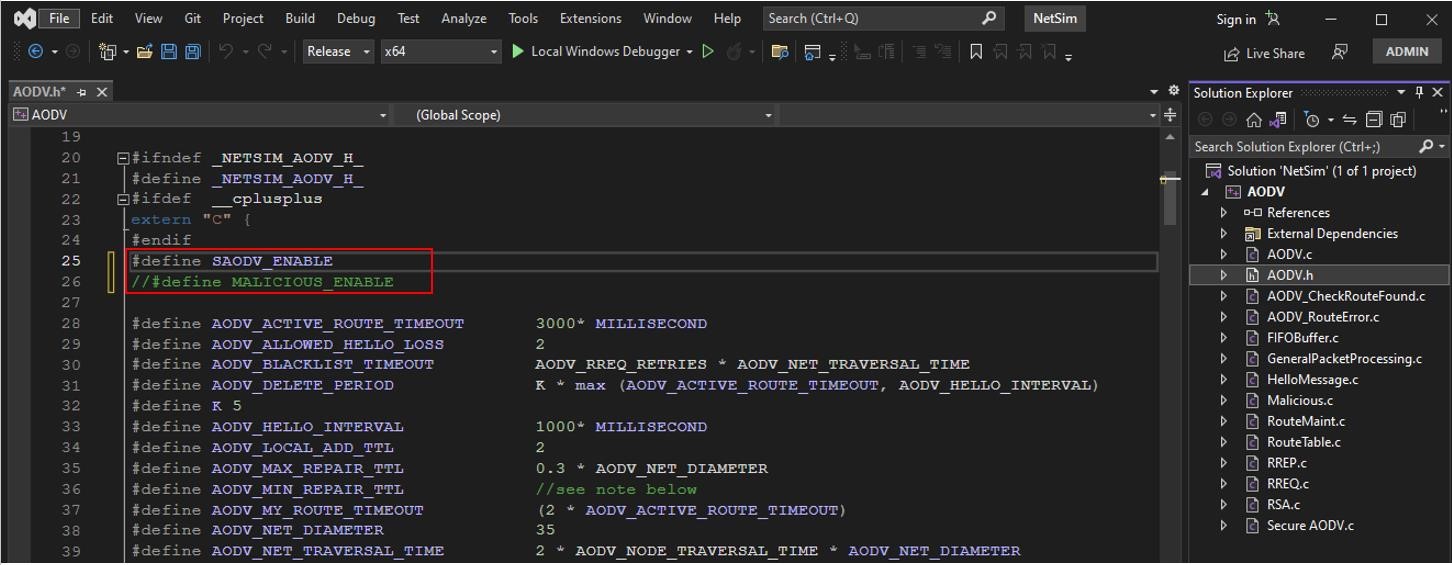


Figure 3: Screenshot of Solution Explorer of AODV project

* Here users can enable Secure AODV (Open **AODV.h** file).

Uncomment the line **#define SAODV\_ENABLE**,

Comment the line **//#define MALICIOUS\_ENABLE** present in **AODV.h** file.

Rebuild the AODV Project by right-clicking and Run the simulation for 100 sec in the Netsim GUI.

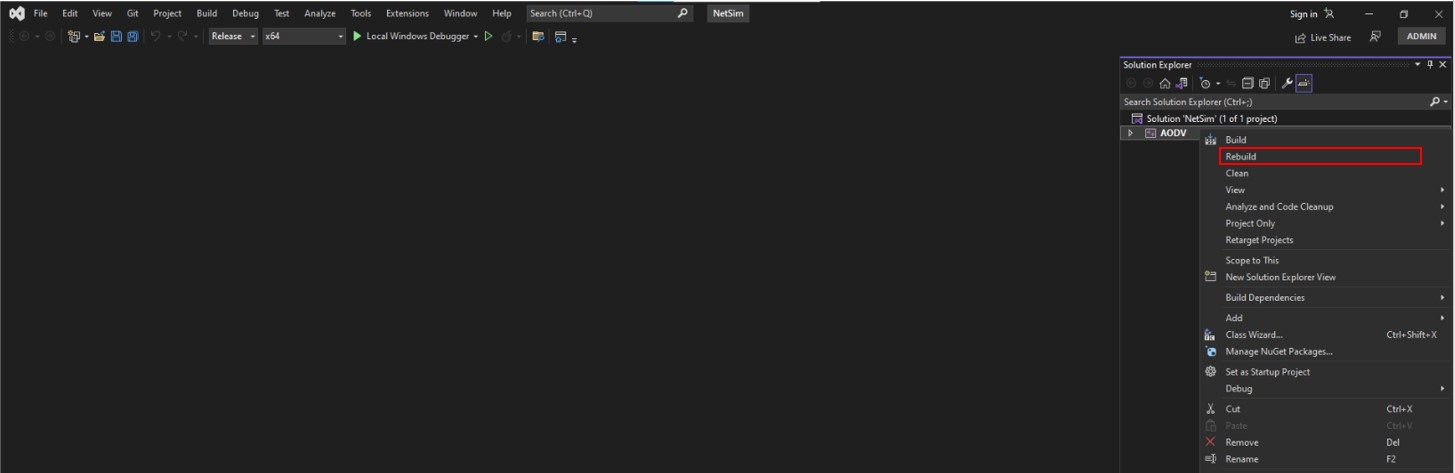


Figure 4: Screenshot of NetSim project Source Code in Visual Studio

A **Secure\_AODV.c** file is added to the AODV project which contains the following important functions:

* **saodv\_encrypt\_packet();** //This function is used to encrypt the control packet data
* **saodv\_decrypt\_packet();** //This function is used to decrypt the control packet data
* **get\_rrep\_str\_data();** //This function is used to get the route reply data from AODV\_RREP control packet
* **get\_rreq\_str\_data();** //This function is used to get the route request data from AODV\_RREQ control packet
* **get\_saodv\_ctrl\_packet\_type();** //This function is used to change the control packet type from AODV (AODV\_RREQ, AODV\_RREP) to SAODV (SAODV\_RREQ, SAODV\_RREP)
* **get\_saodv\_ctrl\_packet();** //This function is called whenever a new control packet is generated
* **get\_aodv\_ctrl\_packet();** //This function is called while processing the control packets

**Results and discussion:**

After Running the simulation of the given Configuration file, open the packet trace in the Result Dashboard Window. In the packet trace, filter the control packets to **SAODV\_RREQ** and **SAODV\_RREP)**

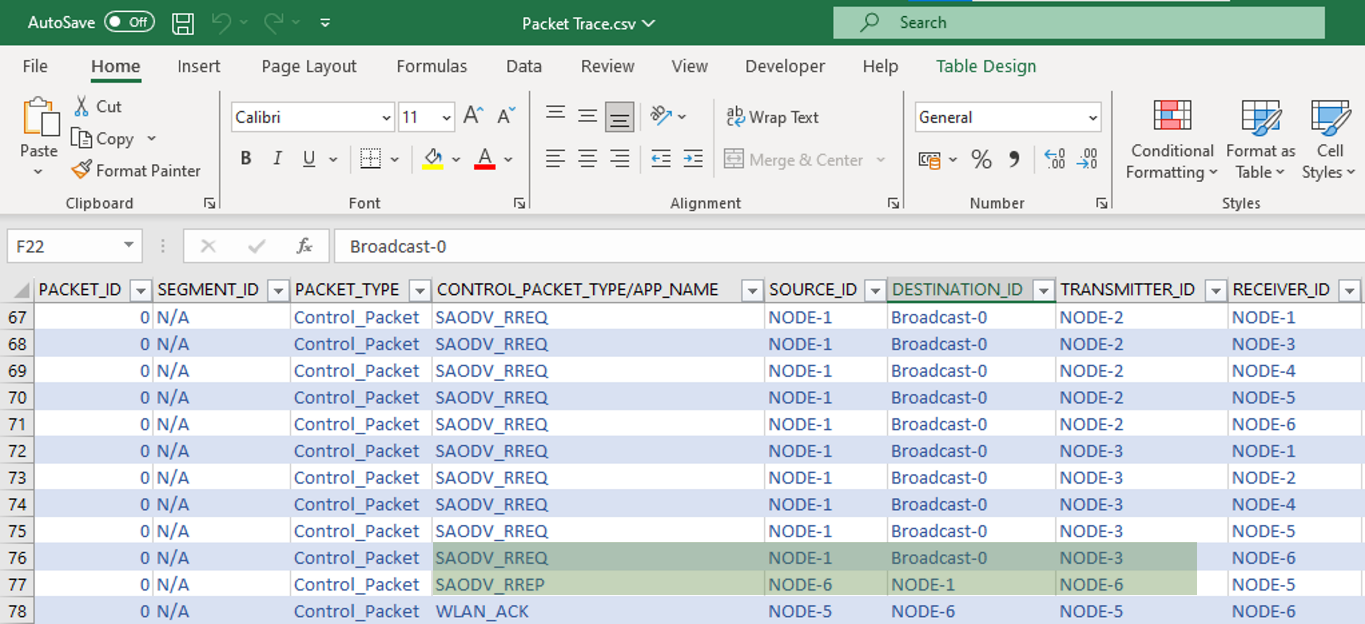


Figure 5: Network Packet trace results for Secure AODV implementation

The SAODV logs certain details in **Secure\_AODV.log**. The Log File can be observed in the Result Dashboard Window.

A screenshot of a computer

Description automatically generated

Figure 6: Secure AODV log file

The format of the log file is such that each control packet is logged. The first line represents the packet type and the numbering used in a NetSim internal numbering system where **30701 is RREQ and 30702 is RREP**. The second line is the message which is encrypted. The third line contains the encrypted message after running the RSA encryption algorithm. The fourth line is after decryption and if everything is OK, the 2nd and 4th lines must match.

**.........................................**

**Packet Type = 30701**

**Org Data = 1,0,1,192.168.0.7,0,192.168.0.2,1**

**Encrypted Data = š ššJÒÜšÀÐÜ Ü× šJÒÜšÀÐÜ ÜÒš**

**Decrypted Data = 1,0,1,192.168.0.7,0,192.168.0.2,1**

**..................................................................................**

**Case 2 :**

**Malicious node implementation:**

Here users can enable the code to implement malicious node

Uncomment #define MALICIOUS\_ENABLE and

comment //#define SAODV\_ENABLE that are present inside AODV.h file and Rebuild the Project.

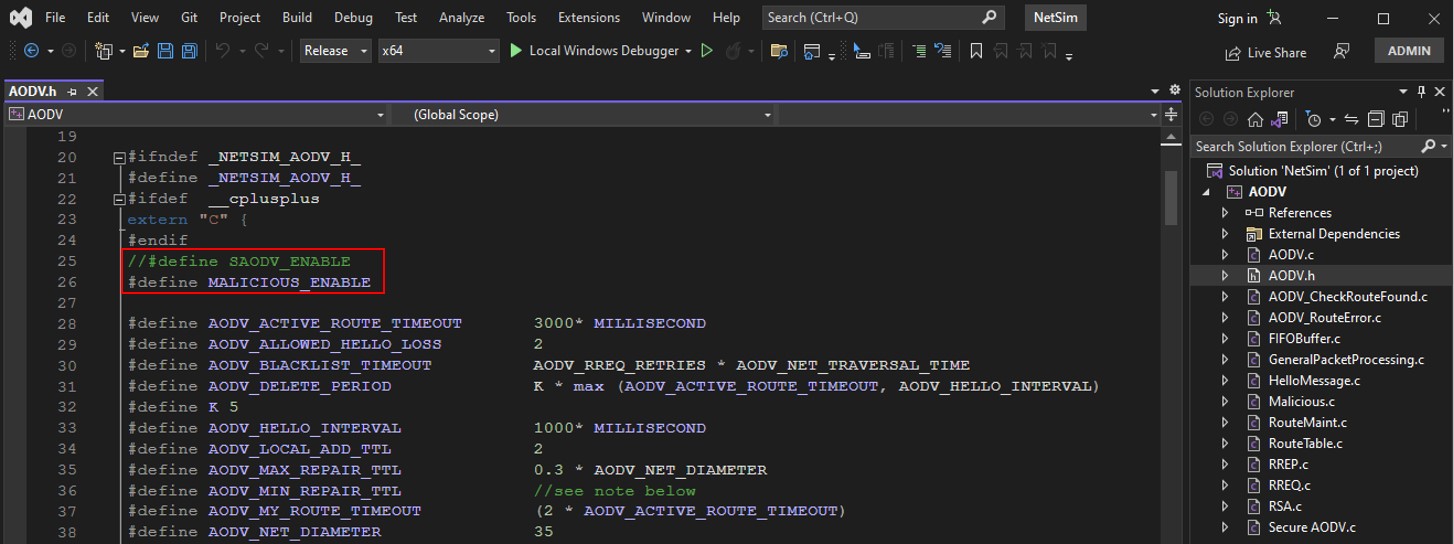


Figure 7: Comment and Uncomment the code of SAODV and Malicious

A malicious node advertises wrong routing information to produce 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.

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

* **IsMaliciousNode();** //This function is used to identify whether a current device is malicious or not in-order to establish malicious behaviour.
* **fn\_NetSim\_AODV\_MaliciousRouteAddToTable();** //This function is used to add a fake route entry into the route table 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

Rebuild the Project and Run the simulation for 100 seconds in Netsim GUI.

**Results and discussion:**

* You can set any device as a malicious node, and you can have more than one malicious node in a scenario.
* Device IDs of malicious nodes can be set using the malicious\_node [ ] array present in malicious.c file. Comment the line #define SAODV\_ENABLE present in AODV.h file.
* Rebuild the project and run the simulation.
* If we run the simulation without SAODV, we will get zero throughputs because the malicious node gets all the packets and drops without forwarding them to the destination. You can notice this in the NetSim packet trace by filtering the PACKET\_TYPE to CBR.

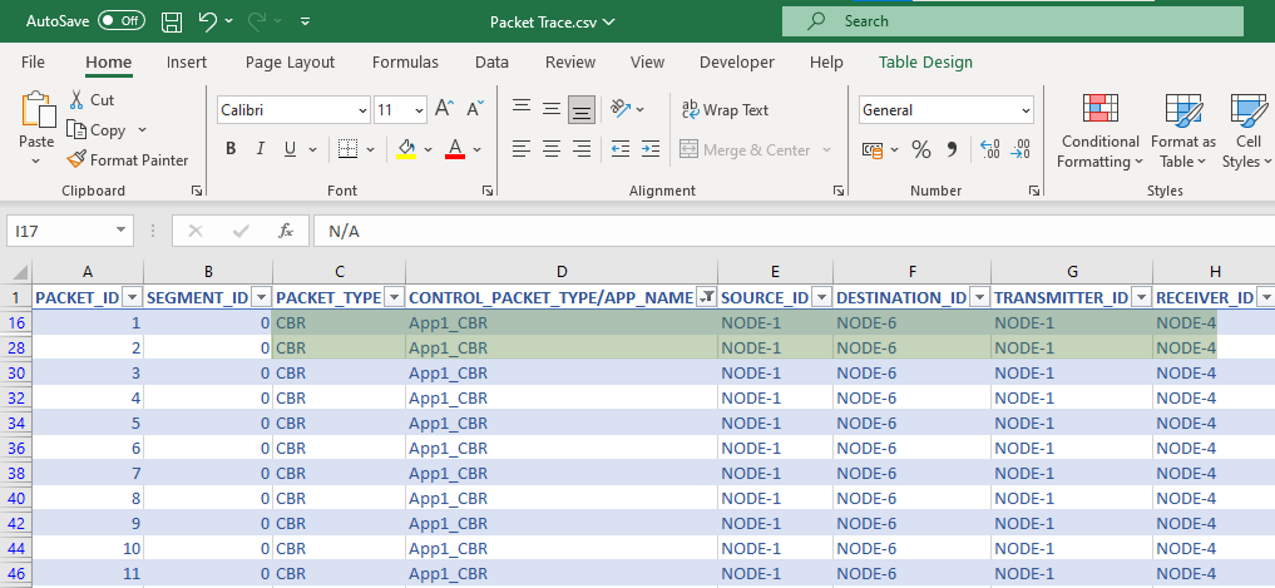


Figure 8: NetSim Packet trace results for Malicious node implementation

**Case 3:**

**Both Secure AODV and Malicious node implementation:**

Enable (Uncomment) the below mentioned lines of code present in AODV.h file.

#define SAODV\_ENABLE

#define MALICIOUS\_ENABLE

Rebuild the Project and run the simulation for 100 sec in Netsim GUI.

**Results and discussion**:

Packets will be transmitted to the destination since SAODV helps in overcoming the Malicious Node problem. Route reply RREP from malicious node 4 will not be accepted by Node 1. It takes the Route reply from node 2 and forms the route. This can be observed in Packet Trace by filtering the CONTROL\_PACKET\_TYPE to SAODV\_RREP. Malicious node 4 is transmitting the Route Reply (RREP) to node 3, but node 3 is not forwarding to any nodes .On the other hand, when it comes to node 6, it is sending the RREP to node 5, then from 5 to 3, from 3 to 2 and finally from 2 to 1.

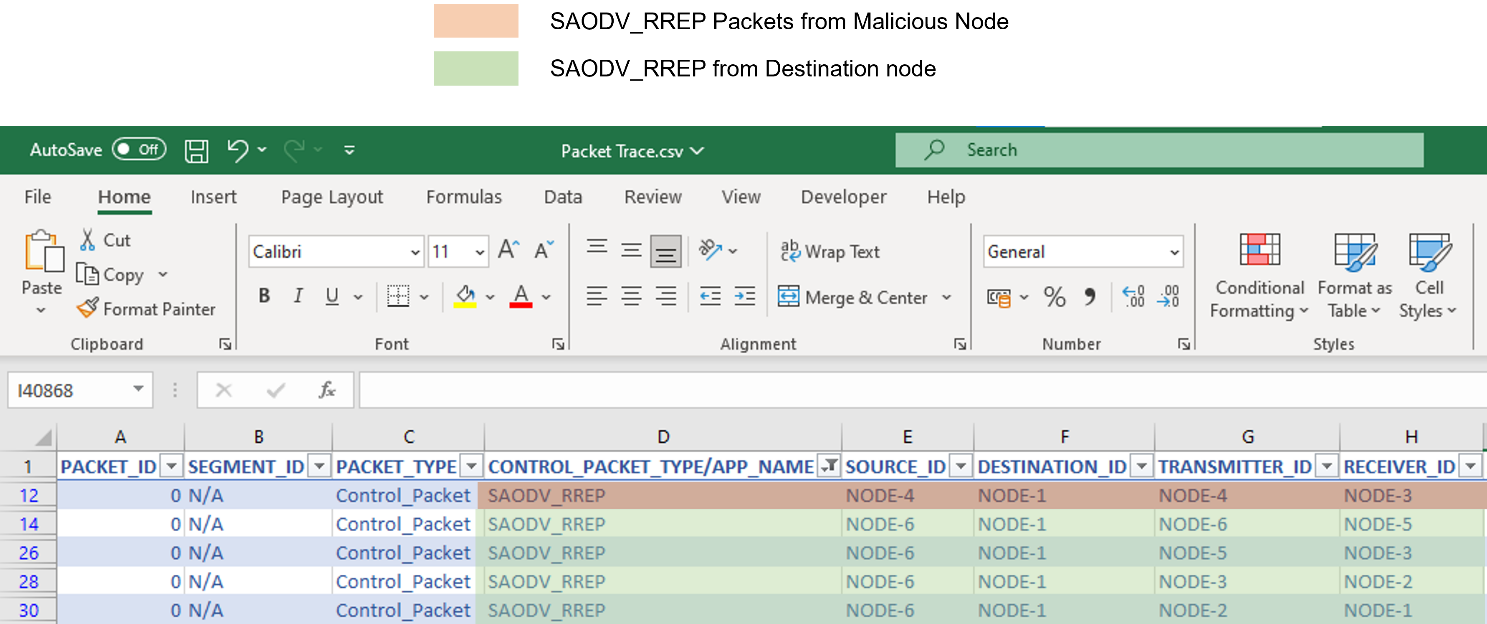


Figure 9: NetSim Packet trace results for Secure AODV and Malicious node implementation

The SAODV logs certain details in **Secure\_AODV.log**. The Log File can be observed in the Result Dashboard Window.

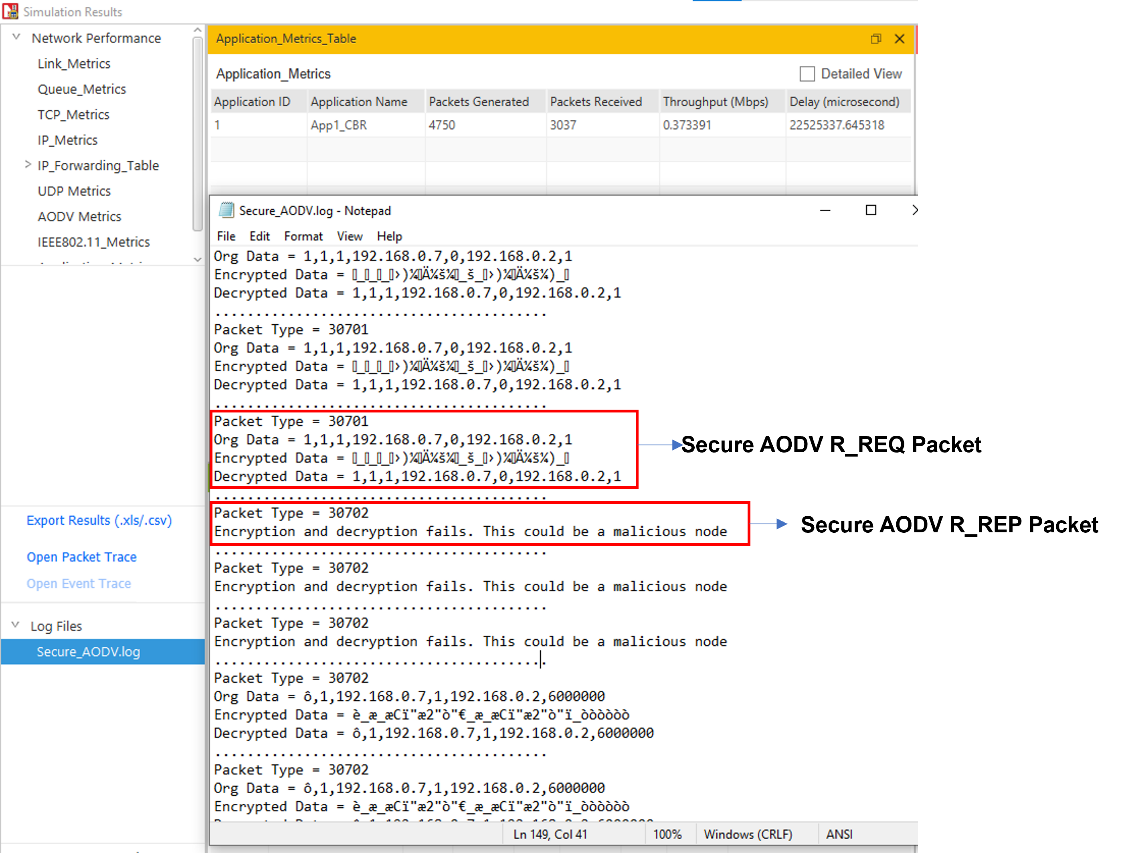


Figure 9: Secure AODV log file

The Packet type 30701 = RREQ is the request packet and the Packet type 30702=RREP is the reply packet, when the malicious node tries to decrypt the message.

**.........................................**

**Packet Type = 30702**

**Encryption and decryption fail. This could be a malicious node.**

**.........................................**

**Appendix: NetSim source code modifications**

**We have added Secure\_AODV.c, RSA.c and Malicious.c files, we have added the following macros code in AODV.h file within AODV project.**

#define SAODV\_ENABLE

#define MALICIOUS\_ENABLE

**Then we have added the following lines of code in enum\_AODV\_Ctrl\_Packet in AODV.h file**

//#ifdef SAODV\_ENABLE

SAODV\_RREQ,

SAODV\_RREP,

SAODV\_RERR,

//#endif

**We have added the following function prototypes in AODV.h file, within AODV project.**

#ifdef SAODV\_ENABLE void get\_saodv\_ctrl\_packet(NetSim\_PACKET\* packet); void get\_aodv\_ctrl\_packet(NetSim\_PACKET\* packet); void saodv\_copy\_packet(NetSim\_PACKET\* dest, NetSim\_PACKET\* src); void saodv\_free\_packet(NetSim\_PACKET\* packet); void remove\_from\_mapper(void\* ptr, bool isfree);

#endif // SAODV\_ENABLE bool IsMaliciousNode(NETSIM\_ID devId);

**We have added the following function prototypes in AODV.c file** int fn\_NetSim\_AODV\_MaliciousRouteAddToTable(NetSim\_EVENTDETAILS\*); int fn\_NetSim\_AODV\_MaliciousProcessSourceRouteOption(NetSim\_EVENTDETAILS\* );

**Changes to NETWORK\_IN event in fn\_NetSim\_AODV\_Run() function in AODV.c file, within AODV project**

#ifdef SAODV\_ENABLE switch (pstruEventDetails->pPacket->nControlDataType)

{

case SAODV\_RREQ:

case SAODV\_RREP: case SAODV\_RERR:

get\_aodv\_ctrl\_packet(pstruEventDetails->pPacket);

break;

}

if (pstruEventDetails->pPacket == NULL)

{

return -1; //Decryption fail.

}

#endif // SAODV\_ENABLE

We have added the following lines of code in AODVctrlPacket\_RREQ and default cases in NETWORK\_IN event to check the current node is malicious or not.

if (IsMaliciousNode(pstruEventDetails->nDeviceId)) fn\_NetSim\_AODV\_MaliciousRouteAddToTable(pstruEventDetails);

**Changes code in fn\_NetSim\_AODV\_CopyPacket () function, in AODV.c file, within AODV project**

#ifdef SAODV\_ENABLE switch(srcPacket->nControlDataType)

{

case SAODV\_RERR: case SAODV\_RREQ: case SAODV\_RREP:

saodv\_copy\_packet(destPacket,srcPacket); return 0; break;

default:

#endif

return fn\_NetSim\_AODV\_CopyPacket\_F(destPacket,srcPacket);

#ifdef SAODV\_ENABLE

break;

}

#endif

**Changes code in int fn\_NetSim\_AODV\_FreePacket () present in the AODV.c file, within AODV project**

#ifdef SAODV\_ENABLE switch (packet->nControlDataType)

{

case SAODV\_RERR: case SAODV\_RREQ: case SAODV\_RREP:

saodv\_free\_packet(packet); return 0; break; default:

remove\_from\_mapper(packet->pstruNetworkData->Packet\_RoutingProtocol, true);

return 0; break;

}

#endif // SAODV\_ENABLE

**Changes code in fn\_NetSim\_AODV\_GenerateRREQ (), fn\_NetSim\_AODV\_RetryRREQ () and fn\_NetSim\_AODV\_ForwardRREQ () functions present in RREQ.c file, within AODV project**

#ifdef SAODV\_ENABLE

get\_saodv\_ctrl\_packet(packet);

#endif

**Changes code in fn\_NetSim\_AODV\_GenerateRREP(), fn\_NetSim\_AODV\_ForwardRREP () and fn\_NetSim\_AODV\_GenerateRREPByIntermediate () functions present in RREP.c file, within AODV project**

#ifdef SAODV\_ENABLE

get\_saodv\_ctrl\_packet(packet);

#endif