

# Dos Attack in 5G NR

**Software Used:** NetSim Standard v12.2 (32/64 bit), Visual Studio 2019

A Denial of Service (DoS) attack is an attempt to make a system unavailable to the intended user(s), such as preventing access to a website. A successful DoS attack consumes all available network or system resources, usually resulting in a slowdown or server crash. Whenever multiple sources are coordinating in the DoS attack, it becomes known as a DDoS (Distributed Denial of Service) attack.

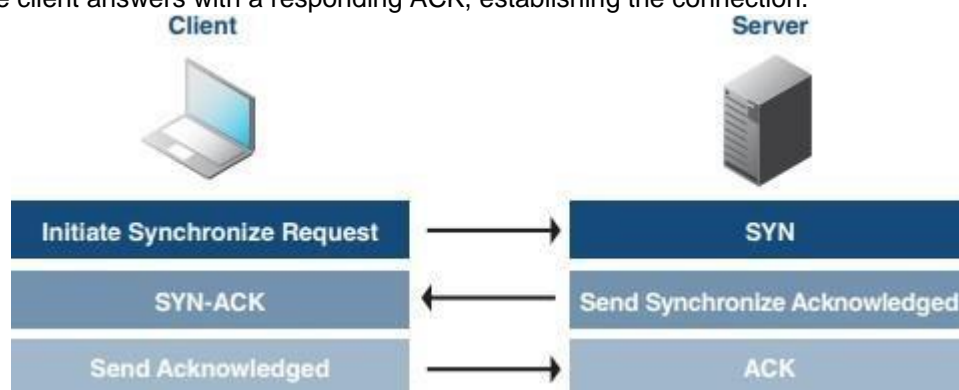
## Standard DDoS Attack types:

1. SYN Flood
2. UDP Flood
3. SMBLoris
4. ICMP Flood
5. HTTP GET Flood

## SYN Flood:

TCP SYN floods are DoS attacks that attempt to flood the DNS server with new TCP connection requests. Normally, a client initiates a TCP connection through a three-way handshake of messages:

- The client requests a connection by sending a SYN (synchronize) message to the server.
- The server acknowledges the request by sending SYN-ACK back to the client.
- The client answers with a responding ACK, establishing the connection.



This triple exchange is the foundation for every connection established using the Transmission Control Protocol (TCP). A SYN Flood is one of the most common forms of DDoS attacks. It occurs when an attacker sends a succession of TCP Synchronize (SYN) requests to the target in an attempt to consume enough resources to make the server unavailable for legitimate users. This works because a SYN request opens network communication between a prospective client and the target server. When the server receives a SYN request, it responds acknowledging the request and holds the communication open while it waits for the client to acknowledge the open connection. However, in a successful SYN Flood, the client acknowledgment never arrives, thus consuming the server's resources until the connection times out. A large number of incoming SYN requests to the target server exhausts all

available server resources and results in a successful DoS attack. Before implementing this project in NetSim, users have to understand the steps given below:

### 1. TCP Log file

- User need to understand the TCP log file which will get created in the temp path of NetSim <Windows Temp Folder>/NetSim>
- The TCP Log file is usually a very large file and hence is disabled by default in NetSim.
- To enable logging, go to TCP.c inside the TCP project and change the function bool isTCPlog() to return true instead of false.

### 2. At malicious node:

Create a new timer event called SYN\_FLOOD in TCP for sending TCP\_SYN packets that should be triggered for every 1000 microseconds. This will create and send the TCP\_SYN packet for every 1000 microseconds. SYN request opens network communication between a client and the target

#### At Target node:

When the target receives a SYN request, it responds acknowledging the request and holds the communication open while it waits for the client to acknowledge the open connection. If a SYN packet arrives at Receiver, it should reply with a SYN\_ACK packet. For this SYN\_ACK packet, add a processing time of 2000 micro seconds in Ethernet Physical Out. This delays the arrival of SYN\_ACK at source node. During this delay, another SYN packet will get created at the malicious node. A large number of incoming SYN requests to the target exhausts all available server resources and results in a successful DoS attack **SYN\_FLOOD in NetSim:**

To implement this project in NetSim, we have created SYN\_FLOOD.c file inside TCP project. The file contains the following functions:

- `int is_malicious_node();`

This function is used to check the node is malicious node or not

- `int socket_creation();`

This function is used to create a new socket and update the socket parameters

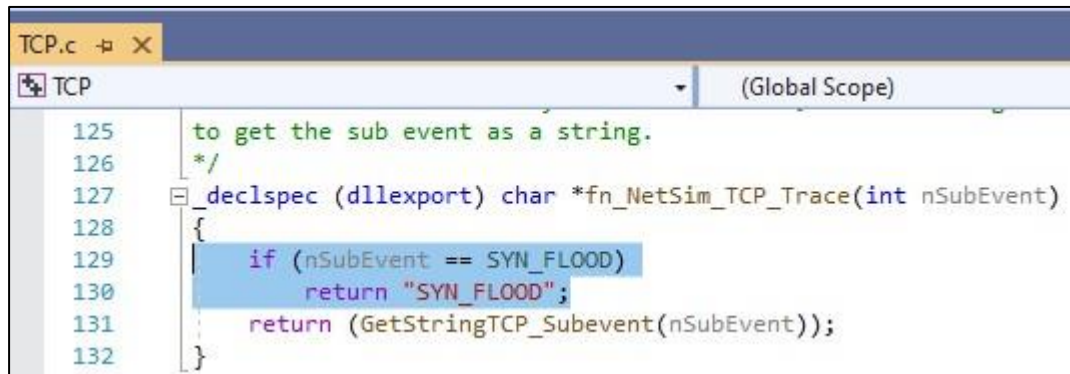
- `static void send_syn_packet(PNETSIM_SOCKET s);`

This function is used to create and send SYN packet to the network layer

- `void syn_flood();`

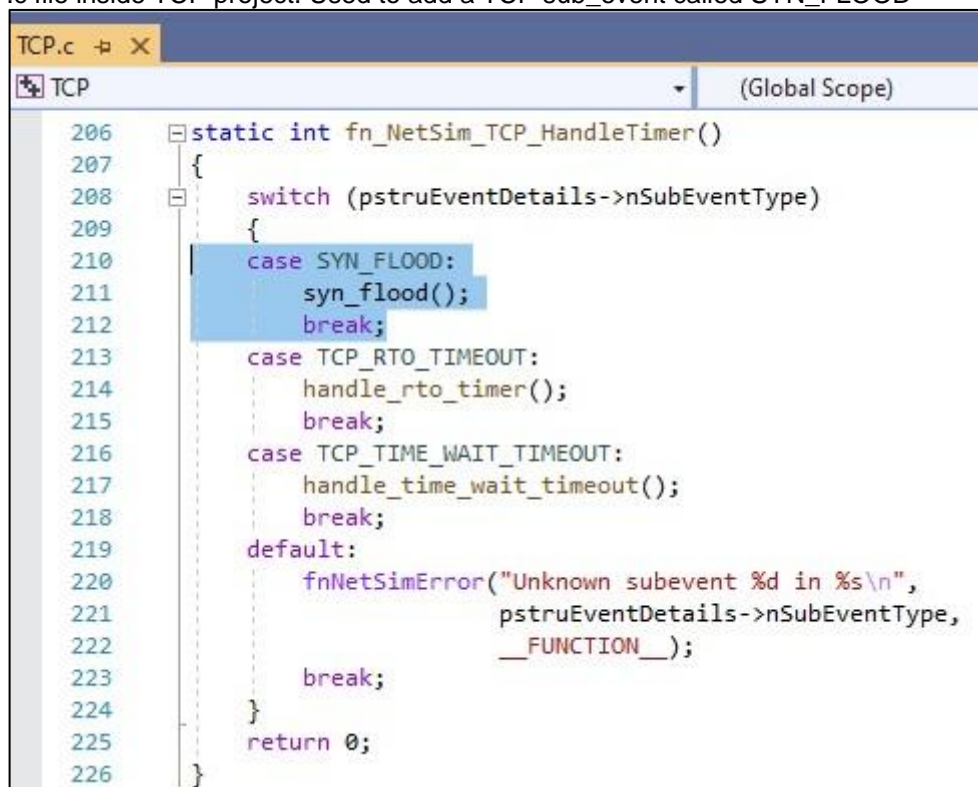
This function is used to check whether the socket is present or not and also adds a timer event called SYN\_FLOOD (triggers for every 1000µs) **Code modifications done in NetSim:**

1. We have added the following lines of code in `fn_NetSim_TCP_Trace()` function present in `TCP.c` file inside TCP project. This is used to add the SYN\_FLOOD sub-events in Event Trace file



```
TCP.c [X]
TCP (Global Scope)
125 to get the sub event as a string.
126 */
127 _declspec(dllexport) char *fn_NetSim_TCP_Trace(int nSubEvent)
128 {
129     if (nSubEvent == SYN_FLOOD)
130         return "SYN_FLOOD";
131     return (GetStringTCP_Subevent(nSubEvent));
132 }
```

2. We have added the following lines of code in `fn_NetSim_TCP_HandleTimer()` function present in `TCP.c` file inside TCP project. Used to add a TCP sub\_event called SYN\_FLOOD



```
TCP.c [X]
TCP (Global Scope)
206 static int fn_NetSim_TCP_HandleTimer()
207 {
208     switch (pstruEventDetails->nSubEventType)
209     {
210     case SYN_FLOOD:
211         syn_flood();
212         break;
213     case TCP_RTO_TIMEOUT:
214         handle_rto_timer();
215         break;
216     case TCP_TIME_WAIT_TIMEOUT:
217         handle_time_wait_timeout();
218         break;
219     default:
220         fnNetSimError("Unknown subevent %d in %s\n",
221                     pstruEventDetails->nSubEventType,
222                     __FUNCTION__);
223         break;
224     }
225     return 0;
226 }
```

3. And modified the following lines of code in `fn_NetSim_TCP_Init()` function present in `TCP.c` inside TCP project

```

TCP.c
TCP
(Global Scope)
fn_NetSim_TCP_Init(stru_NetSim_Network * NETWORK_Formal,
79
80 /*
81 declspec (dllexport) int fn_NetSim_TCP_Init(stru_NetSim_Network* NETWORK_Formal,
82 NetSim_EVENTDETAILS* pstruEventDetails_Formal,
83 char* pszAppPath_Formal,
84 char* pszWritePath_Formal,
85 int nVersion_Type,
86 void** fnPointer)
87 {
88     fn_NetSim_TCP_Init_F(NETWORK_Formal,
89 pstruEventDetails_Formal,
90 pszAppPath_Formal,
91 pszWritePath_Formal,
92 nVersion_Type,
93 fnPointer);
94 NetSim_EVENTDETAILS pevent;
95 memcpy(&pevent, pstruEventDetails, sizeof pevent);
96 for (int i = 0; i < NETWORK->nDeviceCount; i++)
97 {
98     if (is_malicious_node(i + 1))
99     {
100         pevent.nDeviceId = i + 1;
101         pevent.dEventTime += 1000;
102         pevent.nEventType = TIMER_EVENT;
103         pevent.nSubEventType = SYN_FLOOD;
104         pevent.nProtocolId = TX_PROTOCOL_TCP;
105         fnpAddEvent(&pevent);
106     }
107 }
108 return 0;
109 }
110
111
112 /**
113 This function is called by NetworkStack.dll, once simulation end to free the
114 allocated memory for the network.
115 */
98 % No issues found
Output

```

- And modified the following lines of code in add\_timeout\_event() present in RTO.c file inside TCP project which avoids RTO timer for malicious nodes

```

RTO.c
TCP
(Global Scope)
52 *rto = min(max((*rto*2), G), (60 * SECOND));
53 print_tcp_log("New RTO = %0.21f", *rto);
54 }
55
56 void add_timeout_event(PNETSIM_SOCKET s,
57 NetSim_PACKET* packet)
58 {
59     NetSim_PACKET* p = fn_NetSim_Packet_CopyPacket(packet);
60     add_packet_to_queue(&s->tc->retransmissionQueue, p, pstruEventDetails->dEventTime);
61     NetSim_EVENTDETAILS pevent;
62     memcpy(&pevent, pstruEventDetails, sizeof pevent);
63     pevent.dEventTime += TCP_RTO(s->tc);
64     pevent.dPacketSize = packet->pstruTransportData->dPacketSize;
65     pevent.nEventType = TIMER_EVENT;
66     pevent.nPacketId = packet->nPacketId;
67     if (packet->pstruAppData)
68     {
69         pevent.nApplicationId = packet->pstruAppData->nApplicationId;
70         pevent.nSegmentId = packet->pstruAppData->nSegmentId;
71     }
72     else
73     {
74         pevent.nSegmentId = 0;
75         if (!is_malicious_node(pevent.nDeviceId))
76         {
77             pevent.nProtocolId = TX_PROTOCOL_TCP;
78             pevent.pPacket = fn_NetSim_Packet_CopyPacket(p);
79             pevent.szOtherDetails = NULL;
80             pevent.nSubEventType = TCP_RTO_TIMEOUT;
81             fnpAddEvent(&pevent);
82             print_tcp_log("Adding RTO Timer at %0.11f", pevent.dEventTime);
83         }
84     }
85 }
86
87 static void handle_rto_timer_for_ctrl(PNETSIM_SOCKET s)
88 {
89     if (isSynbitSet(pstruEventDetails->pPacket))
90         record_syn(s);
91 }
98 % No issues found
Output

```

- Users can give their own number of malicious node in **TCP.h** file inside TCP project

```

TCP.h  TCP
(Global Scope)
49 //USEFUL MACRO
50 #define isTCPConfigured(d) (DEVICE_TRXLayer(d) && DEVICE_TRXLayer(d)->isTCP)
51 #define isTCPControl(p) (p->nControlDataType/100 == TX_PROTOCOL_TCP)
52
53 //Constant
54 #define TCP_DupThresh 3
55 #define NUMBEROFMALICIOUSNODE 2
56 int is_malicious_node(NETSIM_ID devid);
57 //Typedef
58 typedef struct stru_TCP_Socket NETSIM_SOCKET, *PNETSIM_SOCKET;
59
60 typedef enum enum_tcpstate
61 {
62     TCPCONNECTION_CLOSED,
63     TCPCONNECTION_LISTEN,
64     TCPCONNECTION_SYN_SENT,
65     TCPCONNECTION_SYN_RECEIVED,
66     TCPCONNECTION_ESTABLISHED,
67     TCPCONNECTION_FIN_WAIT_1,
68     TCPCONNECTION_FIN_WAIT_2,
69     TCPCONNECTION_CLOSE_WAIT,
70     TCPCONNECTION_CLOSING,
71     TCPCONNECTION_LAST_ACK,
72     TCPCONNECTION_TIME_WAIT,
73 }TCP_CONNECTION_STATE;
74
75 typedef enum enum_tcp_variant
76 {
77     TCPVariant_OLDTAHOE, //Slow Start and Congestion Avoidance
78     TCPVariant_TAHOE, //Fast Retransmit/Fast Recovery
79     TCPVariant_RENO,
80     TCPVariant_NEWRENO,
81     TCPVariant_BIC,
82     TCPVariant_CUBIC,
83 }TCPVARIANT;

```

6. Users can give their own target ID and malicious ID in **SYN\_FLOOD.c** file inside TCP project

```

SYN_flood.c  TCP
(Global Scope)
13 /* ----- */
14
15 #include "main.h"
16 #include "TCP.h"
17 #include "List.h"
18 #include "TCP_Header.h"
19 #include "TCP_Enum.h"
20
21 int malicious_node[NUMBEROFMALICIOUSNODE] = { 2, 6 };
22 static void send_syn_packet(PNETSIM_SOCKET s);
23 //static PNETSIM_SOCKET socket_creation();
24 int target_node = 4;
25 PNETSIM_SOCKET get_Remotesocket(NETSIM_ID d, PPOCKETADDRESS addr);
26 static PPOCKETADDRESS sockAddr = NULL;
27
28 int is_malicious_node(NETSIM_ID devid)
29 {
30     for (int i = 0; i < NUMBEROFMALICIOUSNODE; i++)
31         if (devid == malicious_node[i]) return 1;
32     return 0;
33 }
34
35 void syn_flood()
36 {
37     /*
38     if (!sockAddr)
39     {
40         sockAddr = calloc(1, sizeof * sockAddr);
41         sockAddr->ip = DEVICE_IPADDRESS(target_node, 1);
42     }
43
44     PNETSIM_SOCKET s = get_Remotesocket(malicious_node, sockAddr);
45     */
46 }
47

```

7. Added the following line in TCP\_Enum.h file inside TCP project to add a new TCP\_subevent called SYN\_FLOOD



```

TCP_Enum.h  TCP.h  RTO.c  SYN_flood.c  TCP_Connection.c  TCP.c
TCP (Global Scope)
#include "EnumString.h"

BEGIN_ENUM(TCP_Subevent)
{
    DECL_ENUM_ELEMENT_WITH_VAL(TCP_RTO_TIMEOUT, TX_PROTOCOL_TCP * 100),
    DECL_ENUM_ELEMENT(TCP_TIME_WAIT_TIMEOUT),
    DECL_ENUM_ELEMENT(SYN_FLOOD),
}
#pragma warning(disable:4028)
END_ENUM(TCP_Subevent);
#pragma warning(default:4028)

```

8. SYN\_FLOOD.c file contains the following functions

```

SYN_flood.c  TCP (Global Scope)
16 #include "TCP.h"
17 #include "List.h"
18 #include "TCP_Header.h"
19 #include "TCP_Enum.h"
20
21 int malicious_node[NUMBEROFMALICIOUSNODE] = { 2, 6 };
22 static void send_syn_packet(PNETSIM_SOCKET s);
23 //static PNETSIM_SOCKET socket_creation();
24 int target_node = 4;
25 PNETSIM_SOCKET get_Remotesocket(NETSIM_ID d, PPOCKETADDRESS addr);
26 static PPOCKETADDRESS sockAddr = NULL;
27
28 int is_malicious_node(NETSIM_ID devid)
29 {
30     for (int i = 0; i < NUMBEROFMALICIOUSNODE; i++)
31         if (devid == malicious_node[i]) return 1;
32
33     return 0;
34 }

```

```

SYN_flood.c  TCP (Global Scope)  syn_flood()
34 }
35
36 void syn_flood()
37 {
38     extern PPOCKETADDRESS anySocketAddr;
39     anySocketAddr->ip = DEVICE_WADDRESS(target_node, 1);
40     PNETSIM_SOCKET s = get_Remotesocket(pstruEventDetails->nDeviceId, anySocketAddr);
41     pstruEventDetails->sId = (pstruEventDetails->nDeviceId);
42     NetSim_EVENTDETAILS pevent;
43     if (is)
44     {
45         s = socket_creation();
46         tcp_connect(s, s->localAddr, s->remoteAddr);
47     }
48     else
49     {
50         s->localDeviceId = pstruEventDetails->nDeviceId;
51         s->remoteDeviceId = target_node;
52         s->sId = sId;
53         send_syn_packet(s);
54         memcpy(&pevent, pstruEventDetails, sizeof pevent);
55         pevent.dEventTime = pstruEventDetails->dEventTime + 1000;
56         pevent.nDeviceId = pstruEventDetails->nDeviceId;
57         pevent.nPacketId = 0;
58         pevent.nEventType = TIMER_EVENT;
59         pevent.nProtocolId = TX_PROTOCOL_TCP;
60         pevent.nSubEventType = SYN_FLOOD;
61         rnpAddEvent(&pevent);
62     }
63 }
64
65
66
67
68

```

```

SYN_flood.c  TCP (Global Scope)  send_syn_packet(PNETSIM_SOCKET s)
67 }
68
69 static void send_syn_packet(PNETSIM_SOCKET s)
70 {
71     NetSim_PACKET* syn = create_syn(s, pstruEventDetails->dEventTime);
72
73     s->tc->SND.UNA = s->tc->ISS;
74     s->tc->SND.NXT = s->tc->ISS + 1;
75     tcp_change_state(s, TCPCONNECTION_SYN_SENT);
76
77     s->tc->synRetries++;
78
79     s->tcpMetrics->synSent++;
80
81     send_to_network(syn, s);
82     add_timeout_event(s, syn);
83 }
84

```

```

85 int socket_creation()
86 {
87     static int s_id = 100;
88     ptrSOCKETINTERFACE sId = (ptrSOCKETINTERFACE)pstruEventDetails->szOtherDetails;
89     PNETSIM_SOCKET newSocket = tcp_create_socket();
90
91     add_to_socket_list(pstruEventDetails->nDeviceId, newSocket);
92
93     PSOCKETADDRESS localsocketAddr = (PSOCKETADDRESS)calloc(1, sizeof * localsocketAddr);
94     localsocketAddr->ip = DEVICE_IPADDRESS(pstruEventDetails->nDeviceId, 1);
95     localsocketAddr->port = 0;
96
97     PSOCKETADDRESS remotesocketAddr = (PSOCKETADDRESS)calloc(1, sizeof * remotesocketAddr);
98     remotesocketAddr->ip = DEVICE_IPADDRESS(target_node, 1);
99     remotesocketAddr->port = 0;
100
101     newSocket->SocketId = s_id;
102     s_id++;
103
104     newSocket->localAddr = localsocketAddr;
105     newSocket->remoteAddr = remotesocketAddr;
106
107     newSocket->localDeviceId = pstruEventDetails->nDeviceId;
108     newSocket->remoteDeviceId = target_node;
109
110     newSocket->sId = sId;
111     return newSocket;
112 }
113
114

```

9. Added PROCESSING\_TIME macro in Ethernet.h file inside ETHERNET project

```

22 #pragma comment(lib, "Metrics.lib")
23 #pragma comment(lib, "libTCP")
24 #define isETHConfigured(d,i) (DEVICE_MACLAYER(d,i)->nMacProtocolId == MAC_PROTOCOL_ETHERNET)
25 //Global variable
26 PNETSIM_MACADDRESS multicastSPTMAC;
27
28 #define ETH_IFG 0.960 //Micro sec
29
30 #define Processing_TIME 1000
31
32 typedef enum enum_eth_packet
33 {
34     ETH_CONFIGBPDU = MAC_PROTOCOL_ETHERNET * 100 + 1,
35 }ETH_PACKET;
36
37 /** Enumeration for Switching Technique */
38 typedef enum enum_SwitchingTechnique
39 {
40     SWITCHINGTECHNIQUE_NULL,
41     SWITCHINGTECHNIQUE_STORE_FORWARD,
42     SWITCHINGTECHNIQUE_CUT_THROUGH,
43     SWITCHINGTECHNIQUE_FRAGMENT_FREE,
44 }SWITCHING_TECHNIQUE;
45

```

10. Modified the following lines of code in fn\_NetSim\_Ethernet\_HandlePhyOut() function present in Ethernet\_Phy.c file inside Ethernet project.

```

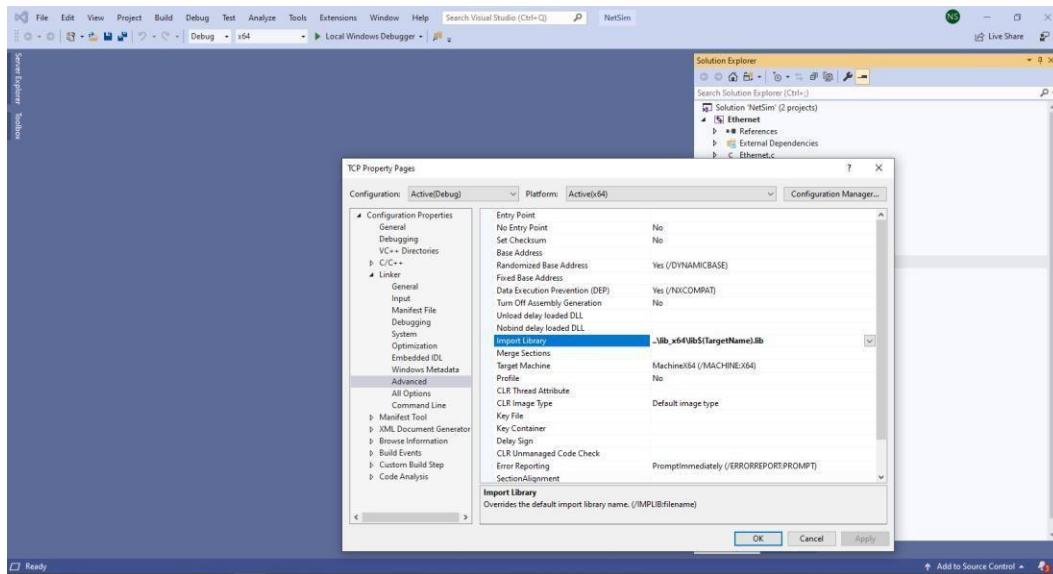
if (!packet)
    return 2; // No packet is there for transmission

double start;

if (pstruEventDetails->nDeviceId == target_node && (packet->nControlDataType == 40102 || packet->nControlDataType == 40105))
{
    if (phy->lastPacketEndTime + phy->IFG <= pstruEventDetails->dEventTime)
        start = pstruEventDetails->dEventTime + Processing_TIME;
    else
        start = phy->lastPacketEndTime + phy->IFG + Processing_TIME;
}
else
{
    if (phy->lastPacketEndTime + phy->IFG <= pstruEventDetails->dEventTime)
        start = pstruEventDetails->dEventTime;
    else
        start = phy->lastPacketEndTime + phy->IFG;
}

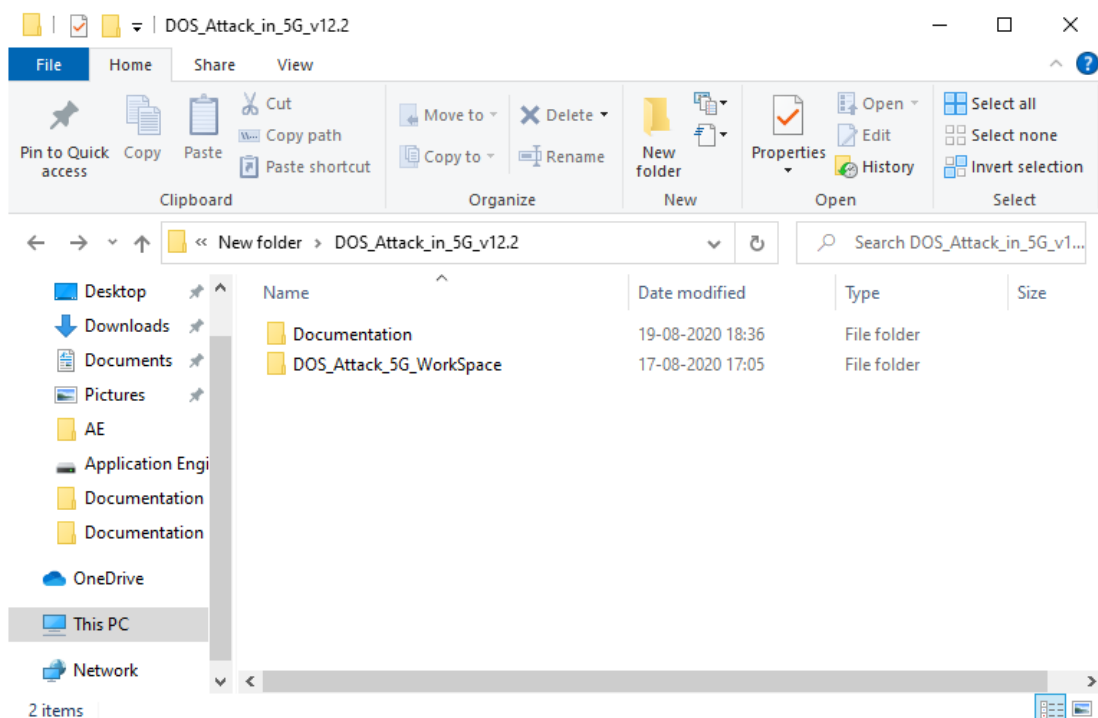
```

11. Right click on TCP project-> Properties->Linker-> Advanced->import library 32-bit and 64-bit  
 ..\lib\lib\$(TargetName).lib or ..\lib\_x64\lib\$(TargetName).lib



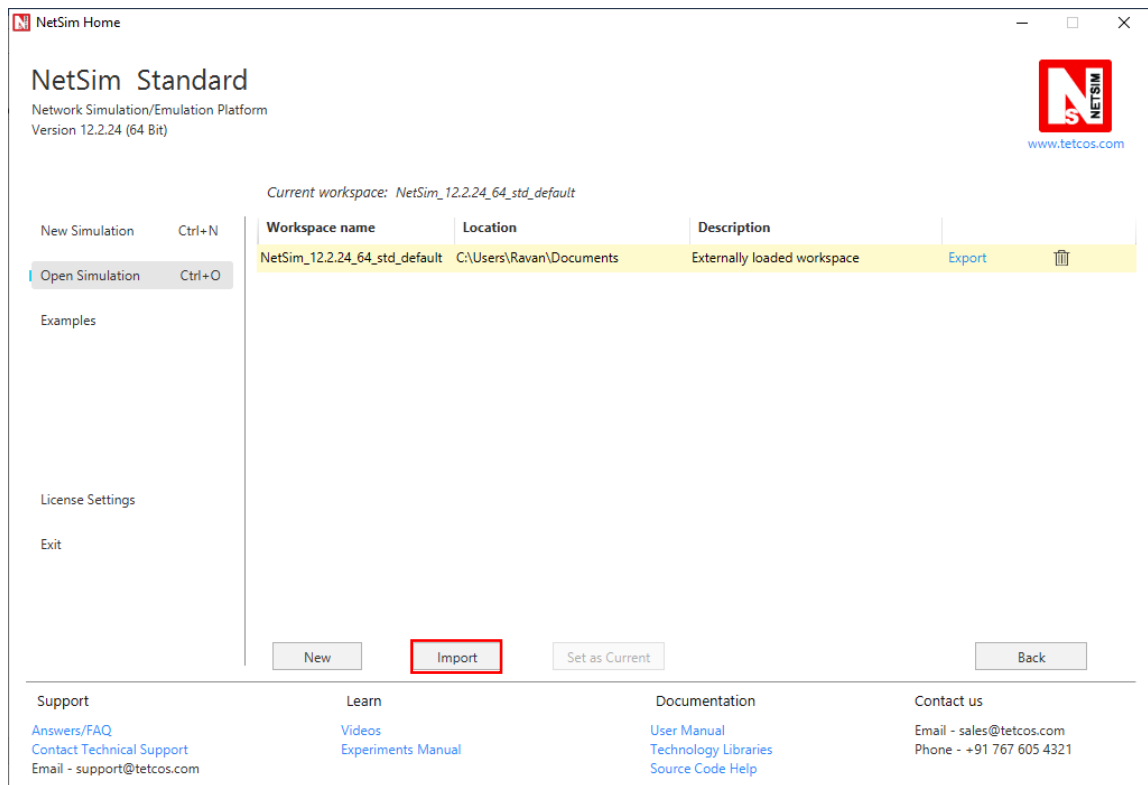
## Steps:

1. The downloaded project folder contains the folders Documentation, and DOS\_Attack\_5G\_Workspace directory as shown below:

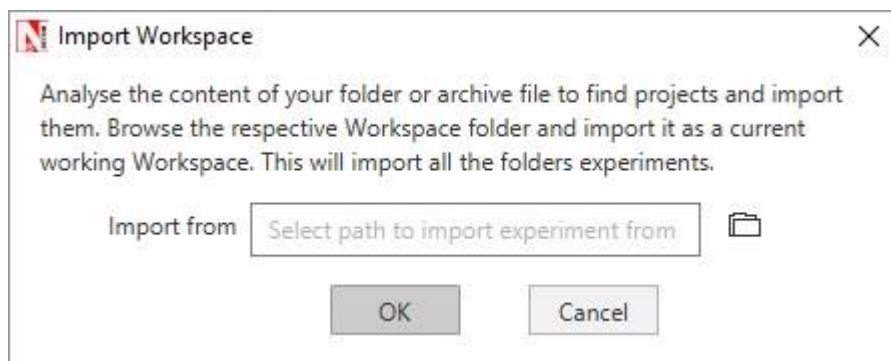


2. Import DOS\_Attack\_5G\_Workspace by going to Open Simulation->Workspace Options->More Options in NetSim Home window. Then select Import as shown below:

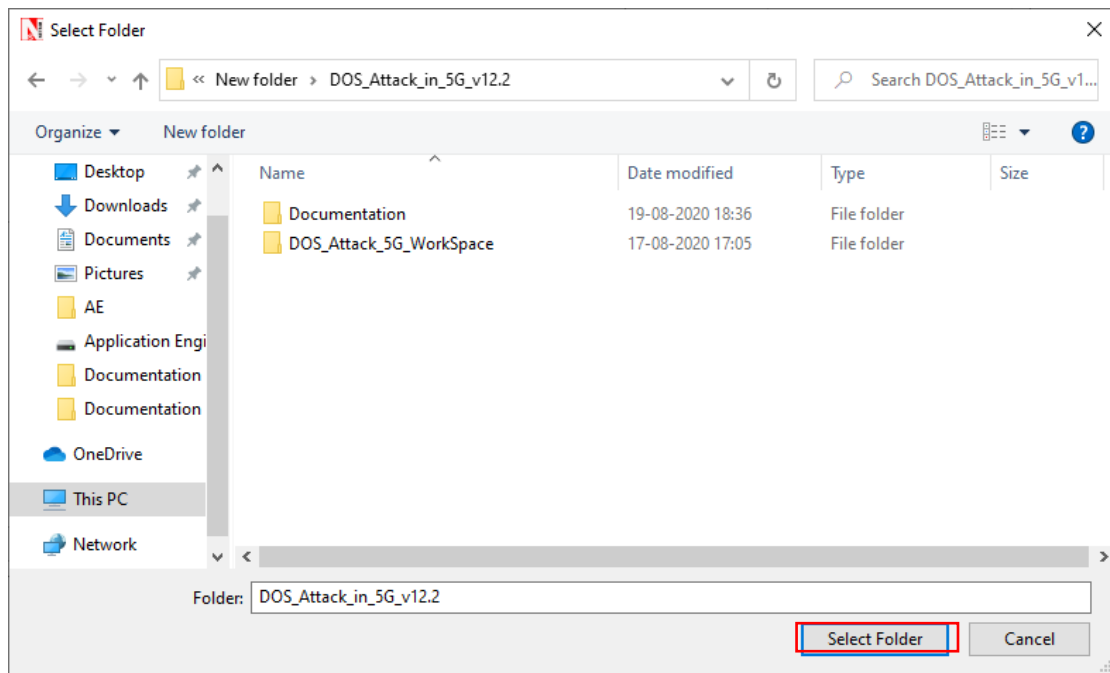




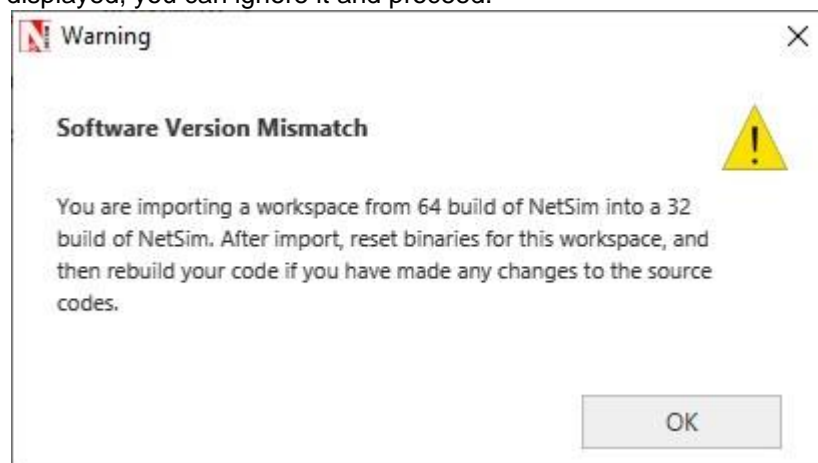
- It displays a window where users need to give the path of the workspace folder and click on OK as shown below:



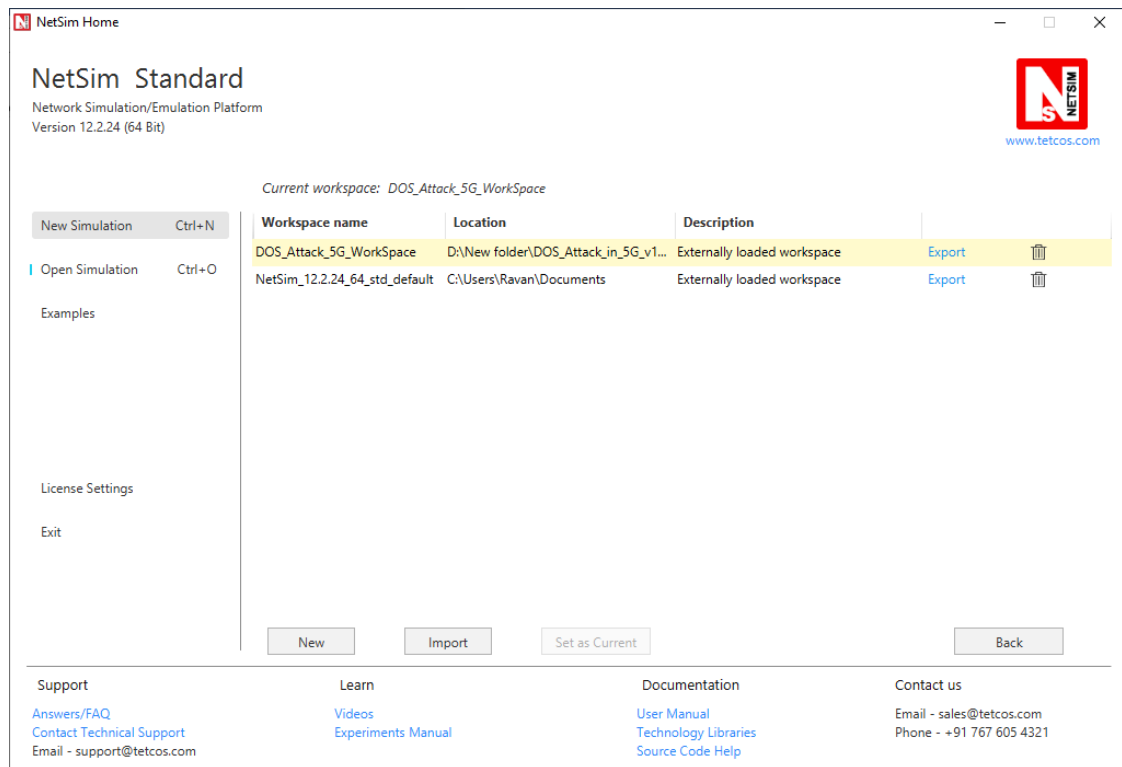
- Browse to the DOS\_Attack\_5G\_Workspace folder and click on select folder as shown below:



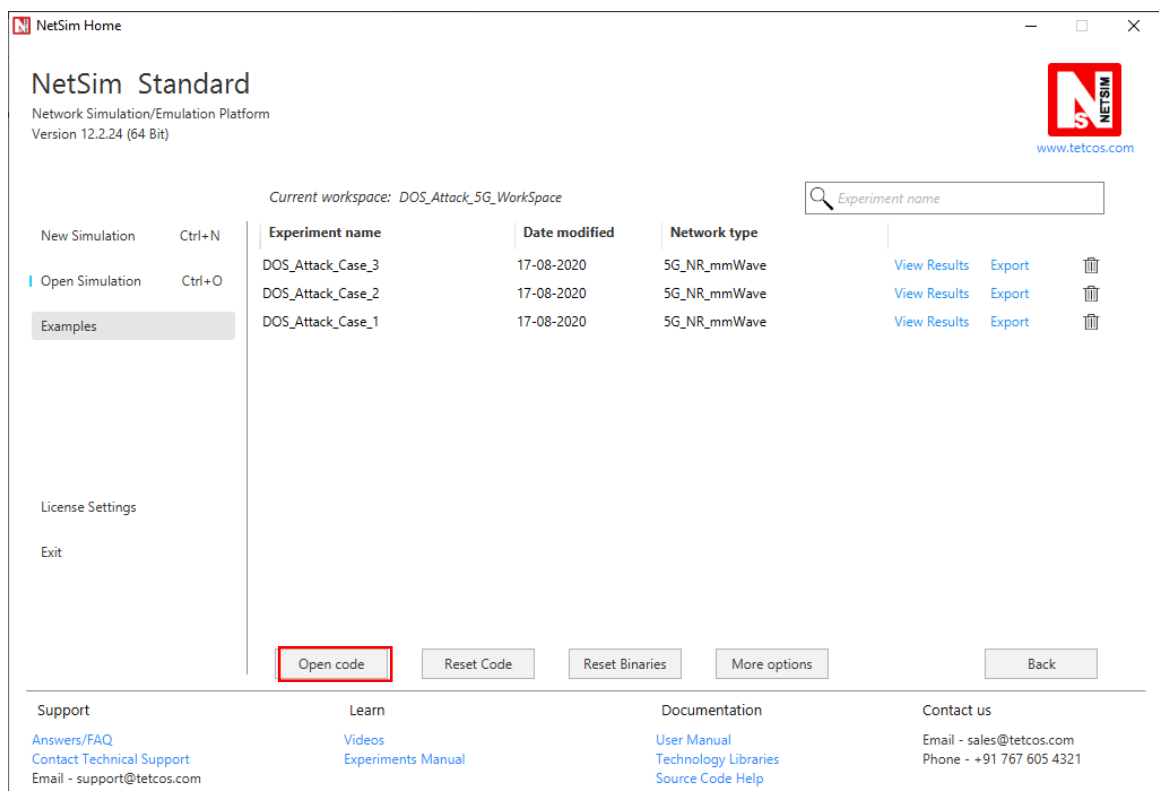
5. After this click on OK button in the Import Workspace window.
6. While importing the workspace, if the following warning message indicating Software Version Mismatch is displayed, you can ignore it and proceed.



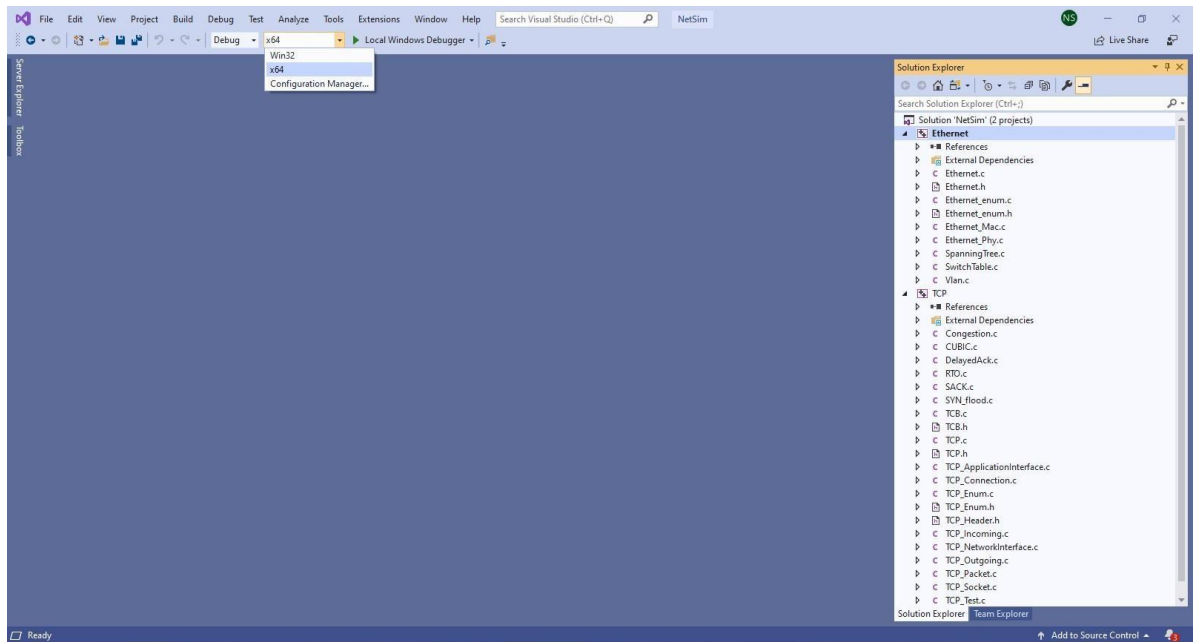
7. The Imported workspace will be set as the current workspace automatically. To see the imported workspace, click on Open Simulation->Workspace Options->More Options as shown below:



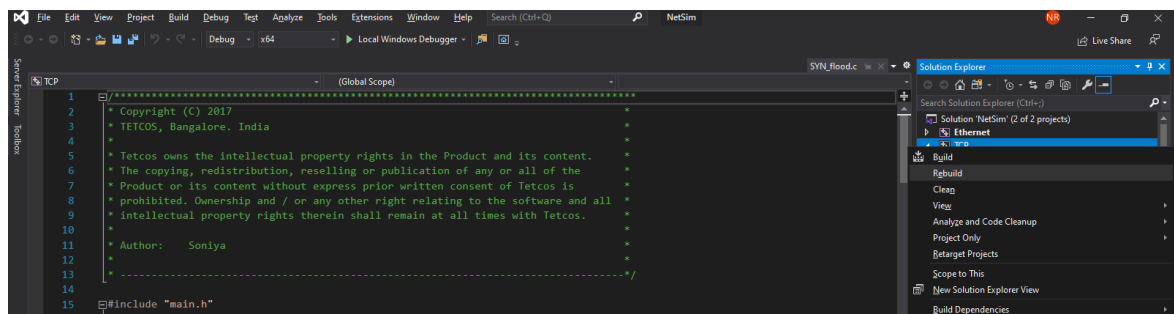
- Open the Source codes in Visual Studio by going to Open Simulation-> Workspace Options and Clicking on Open code button as shown below:



- Under the **TCP** project in the solution explorer you will be able to see that **SYN\_FLOOD.c** file.
- Based on whether you are using NetSim 32 bit or 64 bit setup you can configure Visual studio to build 32 bit or 64 bit Dll files respectively as shown below:



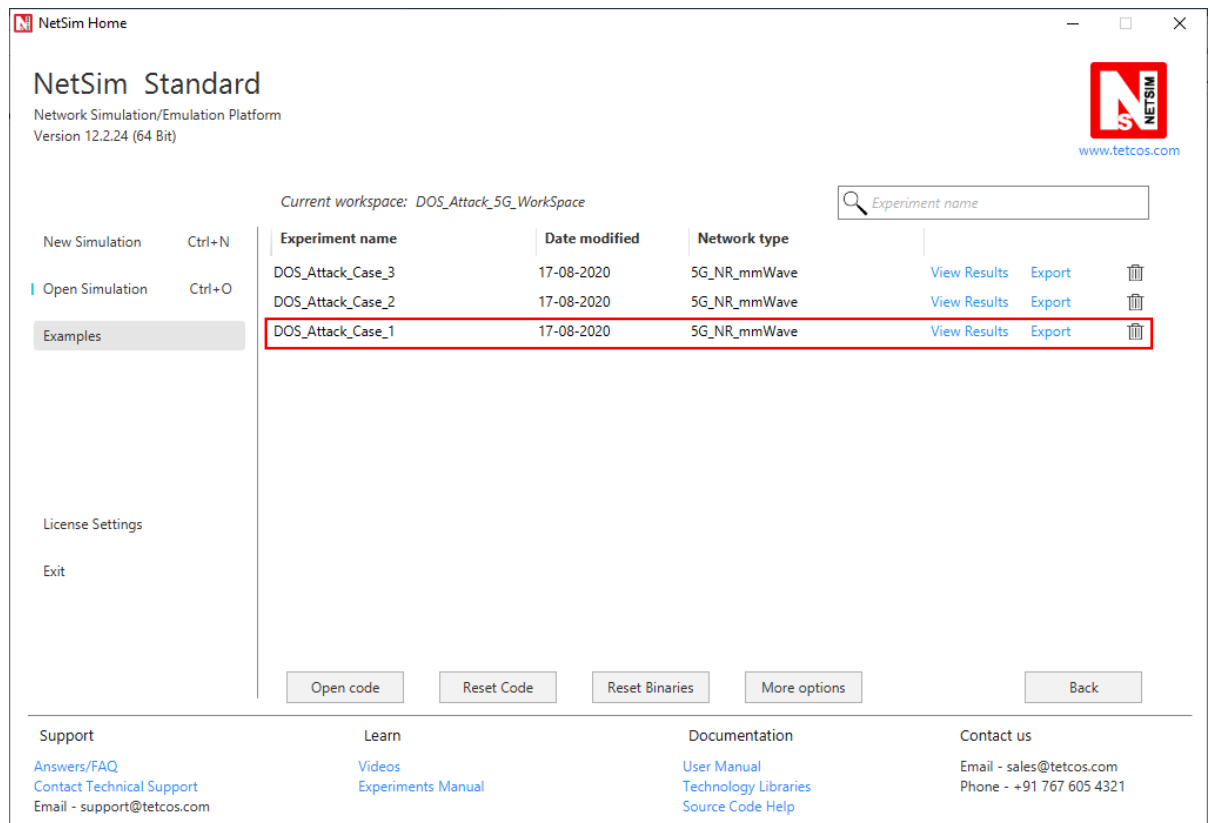
11. Right click on the solution in the solution explorer and select Rebuild. (Note: first rebuild the TCP project and then rebuild the Ethernet project)



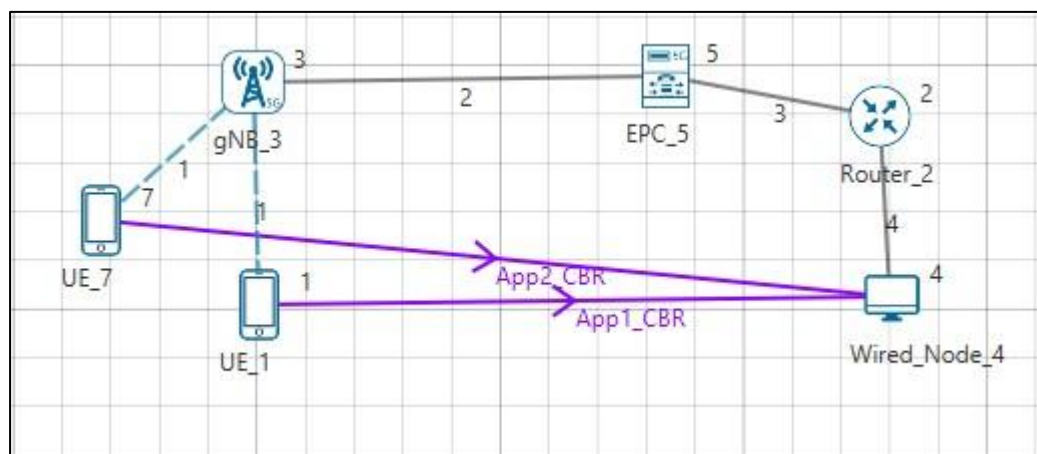
12. Upon successful build modified libTCP.dll and libEthernet.dll file gets automatically updated in the directory containing NetSim binaries.

### Case-1: Without Malicious Node

1. Then DOS\_Attack\_5G\_Workspace comes with a sample configuration that is already saved. To open this example, go to Open Simulation and click on the DOS\_Attack\_Case\_1 that is present under the list of experiments as shown below:

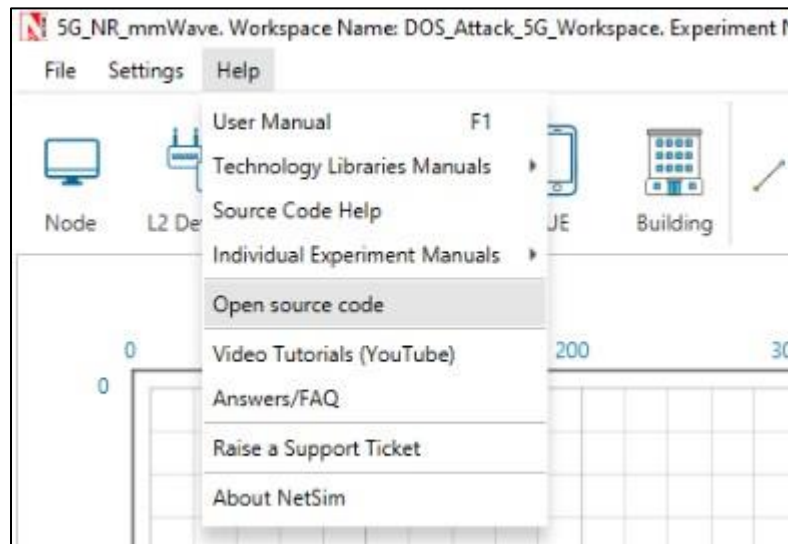


- The saved network scenario consisting of 2 UEs, 1 gNB, 2 router, 1 EPC, 1 Router and 1 wired node in the grid environment forming a 5G NR mmWavw Network. Traffic is configured from Wired node to the Wireless node.



- Help Open Source code





4. In TCP.h set **NUMBEROFMALICIOUSNODE** as 1.

```

SYN_flood.c*  TCP.h  RTO.c
TCP (Global Scope)
43
44 #pragma comment (lib, "NetworkStack.lib")
45
46 _declspec(dllexport) target_node;
47
48
49 //USEFUL MACRO
50 #define isTCPConfigured(d) (DEVICE_TRXLayer(d) && DEVICE_TRXLayer(d)->isTCP)
51 #define isTCPControl(p) (p->nControlDataType/100 == TX_PROTOCOL_TCP)
52
53 //Constant
54 #define TCP_DupThresh 3
55 #define NUMBEROFMALICIOUSNODE 1
56 int is_malicious_node(NETSIM_ID devid);

```

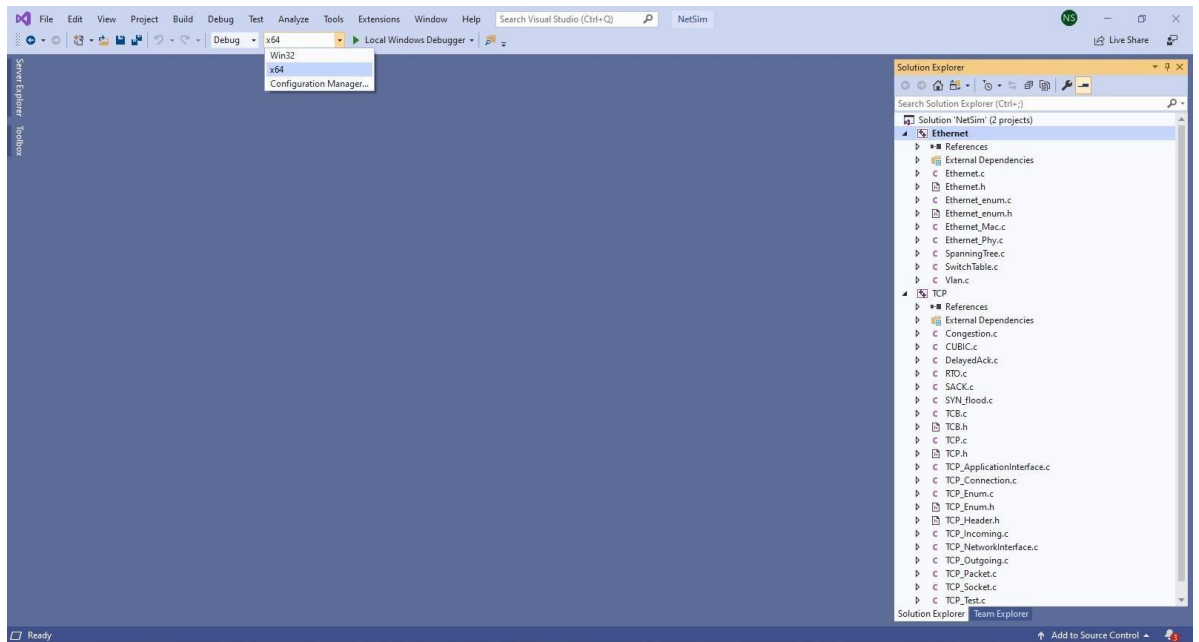
5. In SYN\_FLOOD.c set **malicious node** as 0.

```

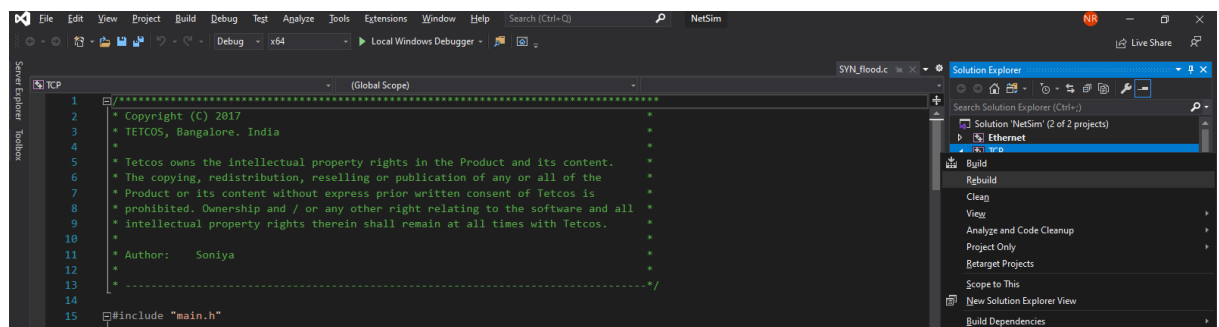
SYN_flood.c*  TCP.h  RTO.c
TCP (Global Scope)
7
8 * Product or its content without express prior written consent of Tetcos is
9 * prohibited. Ownership and / or any other right relating to the software and all
10 * intellectual property rights therein shall remain at all times with Tetcos.
11 * Author: Soniya
12 *
13 * -----*/
14
15 #include "main.h"
16 #include "TCP.h"
17 #include "List.h"
18 #include "TCP_Header.h"
19 #include "TCP_Enum.h"
20
21 int malicious_node[NUMBEROFMALICIOUSNODE] = { 0 };
22 static void send_syn_packet(PNETSIM_SOCKET s);
23 //static PNETSIM_SOCKET socket_creation();

```

6. Based on whether you are using NetSim 32 bit or 64 bit setup you can configure Visual studio to build 32 bit or 64 bit DLL files respectively as shown below:



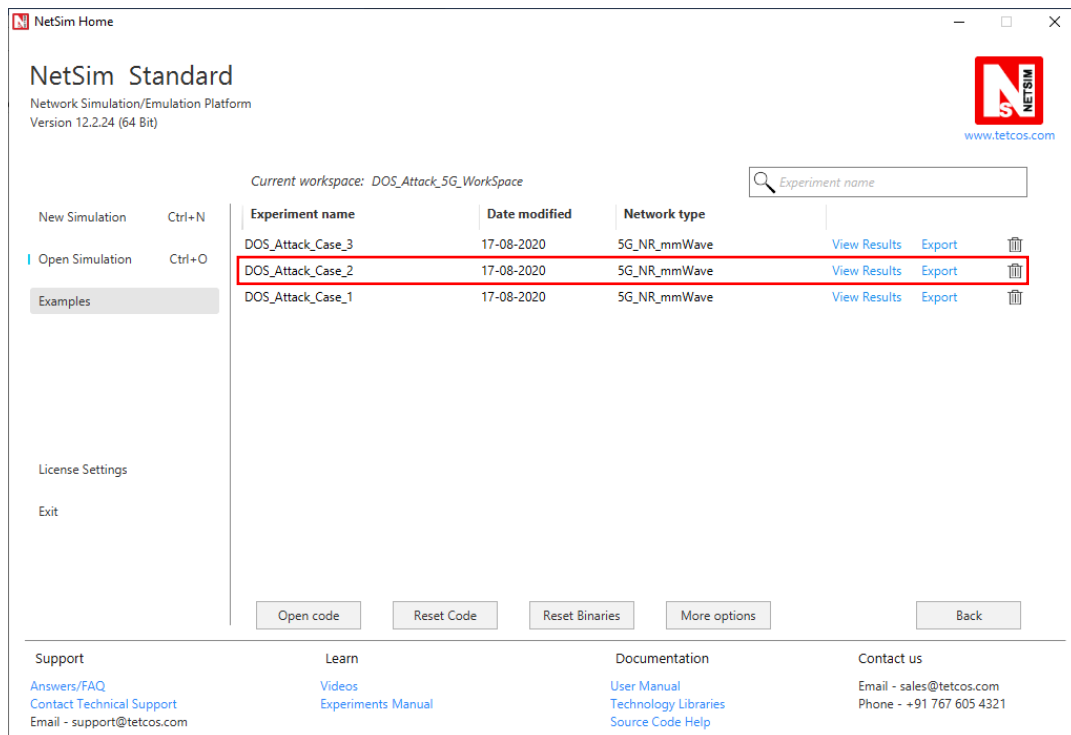
7. Right click on the solution in the solution explorer and select Rebuild. (Note: first rebuild the TCP project and then rebuild the Ethernet project)



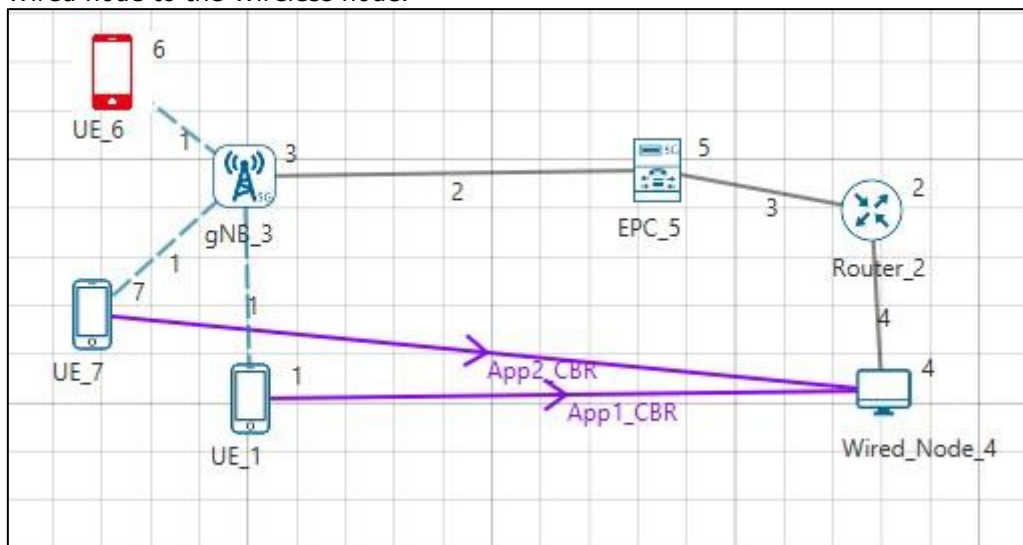
8. Upon successful build modified libTCP.dll and libEthernet.dll file gets automatically updated in the directory containing NetSim binaries.
9. Run the simulation for 5 seconds.

## Case-2: With one Malicious Node

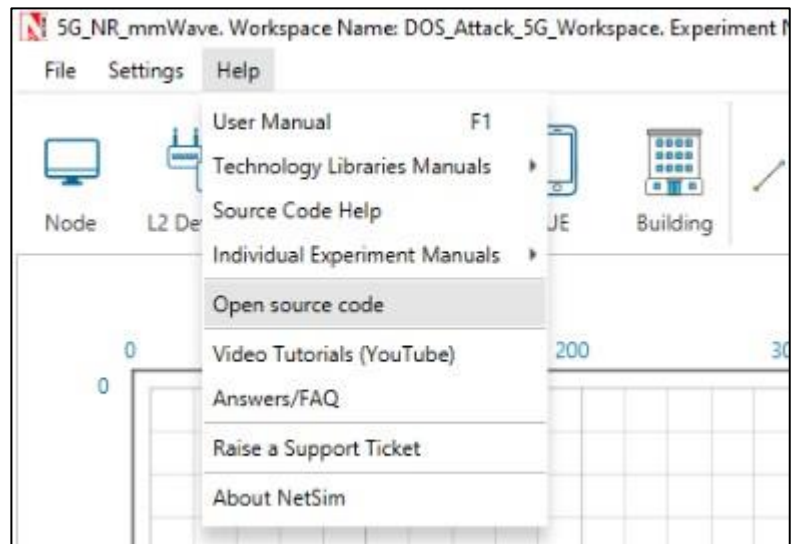
1. Then DOS\_Attack\_5G\_Workspace comes with a sample configuration that is already saved. To open this example, go to Open Simulation and click on the DOS\_Attack\_Case\_2 that is present under the list of experiments as shown below:



- The saved network scenario consisting of 3 UEs, 1 gNB, 2 router, 1 EPC, 1 Router and 1 wired node in the grid environment forming a 5G NR mmWave Network. Traffic is configured from Wired node to the Wireless node.



- Help Open Source code



4. In TCP.h set **NUMBEROFMALICIOUSNODE** as 1.

```

SYN_flood.c*  TCP.h  RTO.c
TCP (Global Scope)
43
44 #pragma comment (lib, "NetworkStack.lib")
45
46 _declspec(dllexport) target_node;
47
48
49 //USEFUL MACRO
50 #define isTCPConfigured(d) (DEVICE_TRXLayer(d) && DEVICE_TRXLayer(d)->isTCP)
51 #define isTCPControl(p) (p->nControlDataType/100 == TX_PROTOCOL_TCP)
52
53 //Constant
54 #define TCP_DupThresh 3
55 #define NUMBEROFMALICIOUSNODE 1
56 int is_malicious_node(NETSIM_ID devid);

```

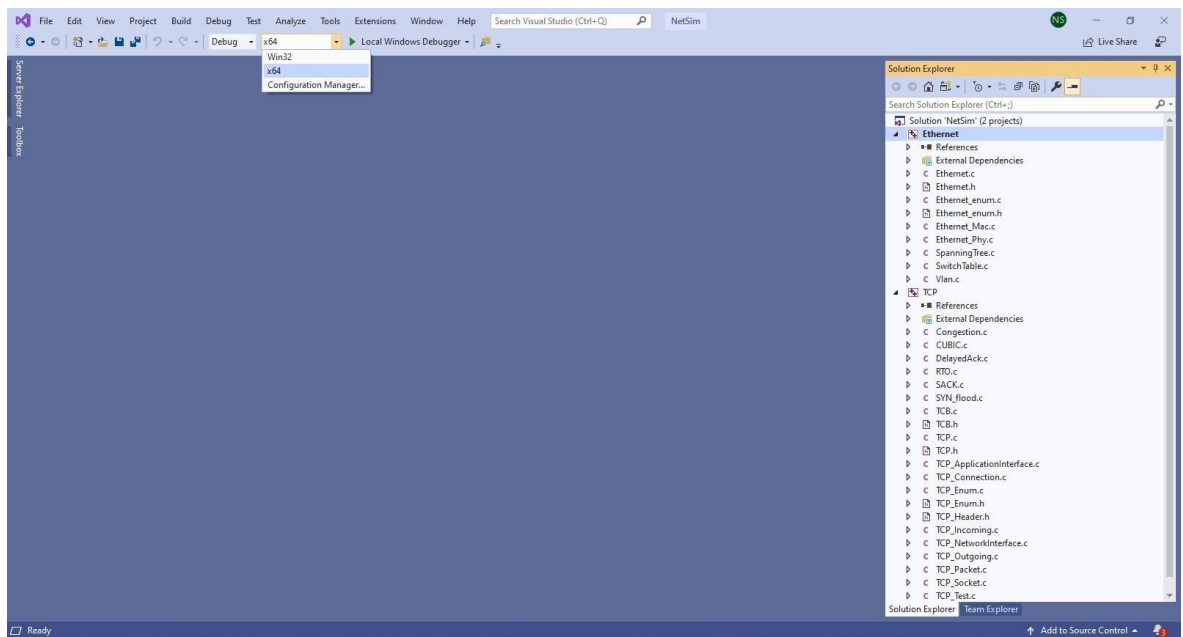
5. In SYN\_FLOOD.c set **malicious node** as 6.

```

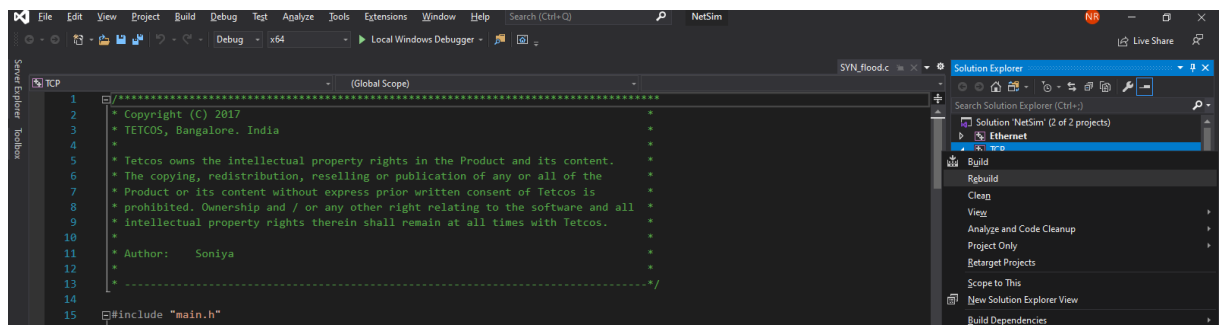
SYN_flood.c  TCP.h
TCP (Global Scope)
12
13 *
14 * -----
15 #include "main.h"
16 #include "TCP.h"
17 #include "List.h"
18 #include "TCP_Header.h"
19 #include "TCP_Enum.h"
20
21 int malicious_node[NUMBEROFMALICIOUSNODE] = {6};
22 static void send_syn_packet(PNETSIM_SOCKET s);
23 //static PNETSIM_SOCKET socket_creation();
24 int target_node = 4;

```

6. Based on whether you are using NetSim 32 bit or 64 bit setup you can configure Visual studio to build 32 bit or 64 bit DLL files respectively as shown below:



7. Right click on the solution in the solution explorer and select Rebuild. (Note: first rebuild the TCP project and then rebuild the Ethernet project)

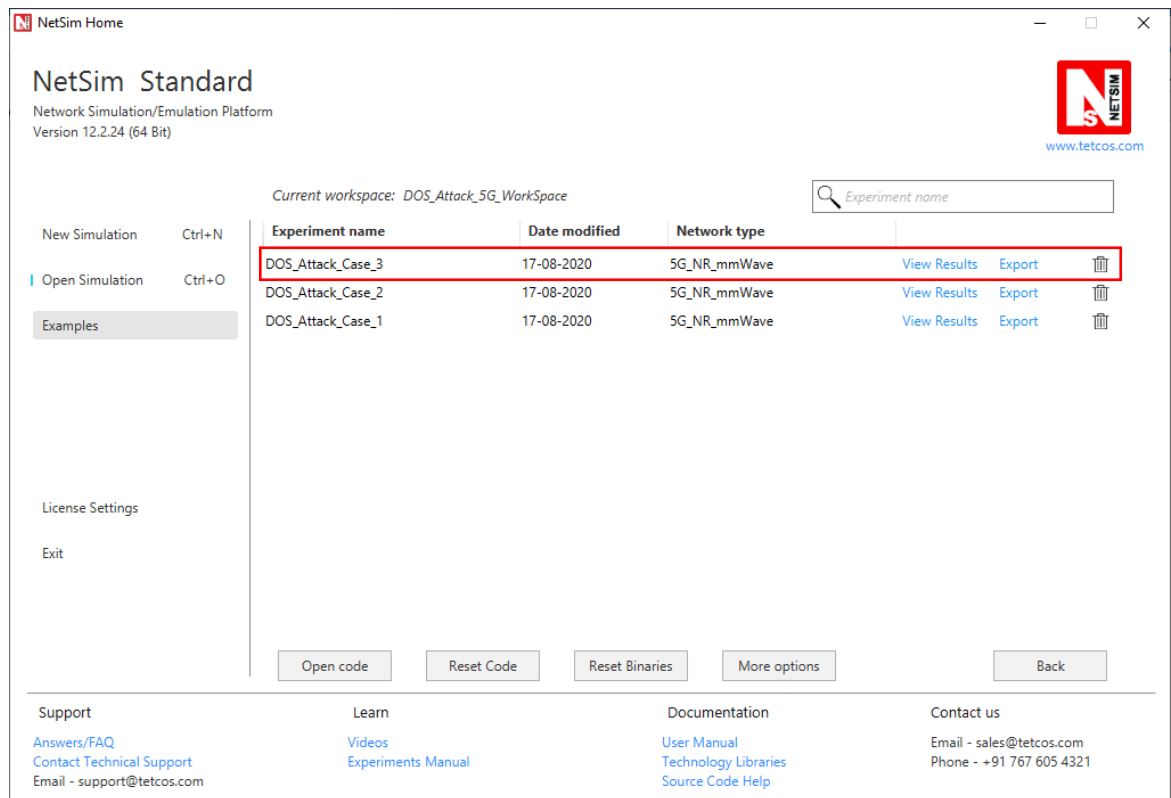


8. Upon successful build modified libTCP.dll and libEthernet.dll file gets automatically updated in the directory containing NetSim binaries.
9. Run the simulation for 5 seconds.

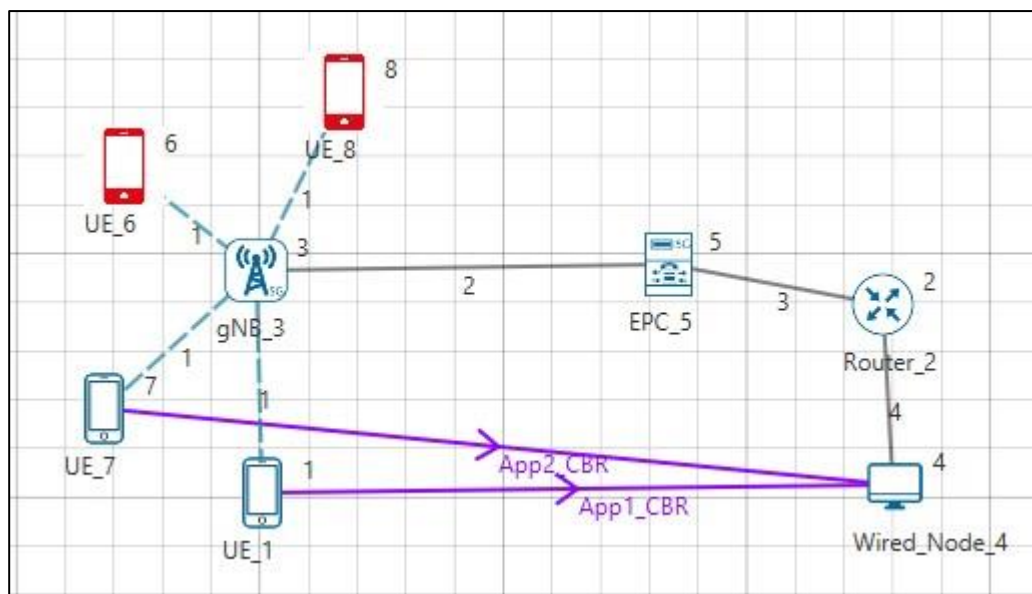
### Case-3: With two Malicious Node

1. Then DOS\_Attack\_5G\_Workspace comes with a sample configuration that is already saved. To open this example, go to Open Simulation and click on the DOS\_Attack\_Case\_3 that is present under the list of experiments as shown below:

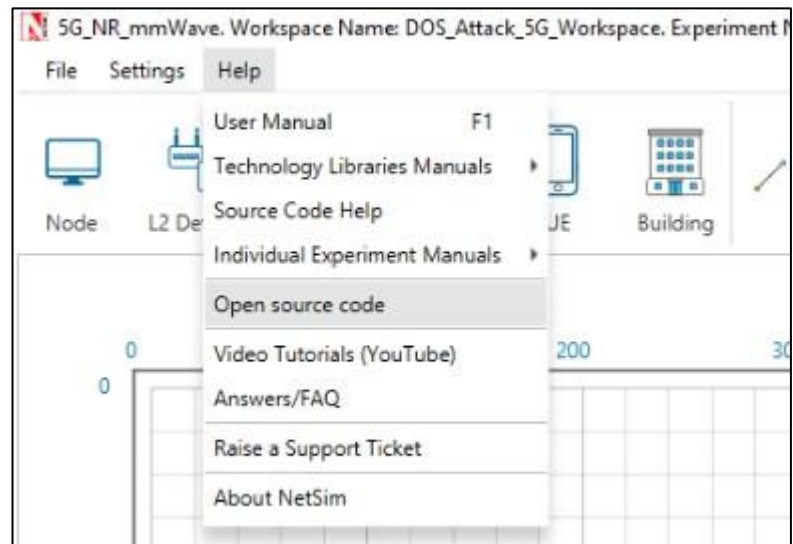




- The saved network scenario consisting of 4 UEs, 1 gNB, 2 router, 1 EPC, 1 Router and 1 wired node in the grid environment forming a 5G NR mmWave Network. Traffic is configured from Wired node to the Wireless node.



- Help Open Source code



4. In TCP.h set **NUMBEROFMALICIOUSNODE** as 2.

```

SYN_flood.c* TCP.h* RTO.c
TCP (Global Scope)
43
44 #pragma comment (lib,"NetworkStack.lib")
45
46 _declspec(dllexport) target_node;
47
48
49 //USEFUL MACRO
50 #define isTCPConfigured(d) (DEVICE_TRXLayer(d) && DEVICE_TRXLayer(d)->isTCP)
51 #define isTCPControl(p) (p->nControlDataType/100 == TX_PROTOCOL_TCP)
52
53 //Constant
54 #define TCP_DupThresh 3
55 #define NUMBEROFMALICIOUSNODE 2
56 int is_malicious_node(NETSIM_ID devid);
57 //Typedef
58 typedef struct stru_TCP_Socket NETSIM_SOCKET, *PNETSIM_SOCKET;
59

```

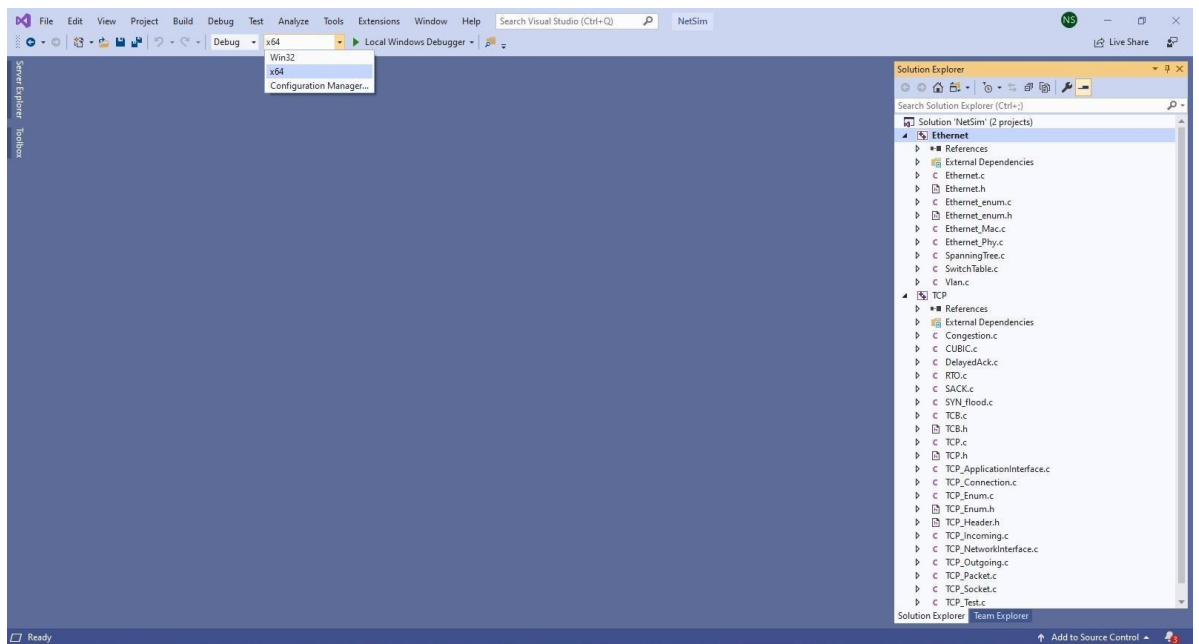
5. In SYN\_FLOOD.c set **malicious node** as 6 , 8.

```

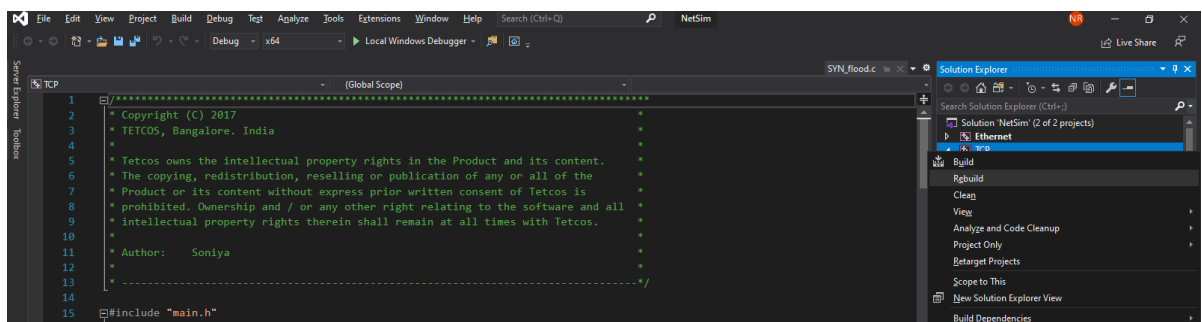
SYN_flood.c TCP.h
TCP (Global Scope)
12 *
13 * -----
14
15 #include "main.h"
16 #include "TCP.h"
17 #include "List.h"
18 #include "TCP_Header.h"
19 #include "TCP_Enum.h"
20
21 int malicious_node[NUMBEROFMALICIOUSNODE] = {6,8};
22 static void send_syn_packet(PNETSIM_SOCKET s);
23 //static PNETSIM_SOCKET socket_creation();
24 int target_node = 4;
25 PNETSIM_SOCKET get_Remotesocket(NETSIM_ID d, P SOCKETADDRESS addr);
26 static P SOCKETADDRESS sockAddr = NULL;

```

6. Based on whether you are using NetSim 32 bit or 64 bit setup you can configure Visual studio to build 32 bit or 64 bit DLL files respectively as shown below:



7. Right click on the solution in the solution explorer and select Rebuild. (Note: first rebuild the TCP project and then rebuild the Ethernet project)



8. Upon successful build modified libTCP.dll and libEthernet.dll file gets automatically updated in the directory containing NetSim binaries.
9. Run the simulation for 5 seconds.

## Result:

After simulation, open metrics window and observe the Application\_Throughput is decreasing for both applications as we increase the malicious node because of the SYN flood sent from the malicious node.

In case 1 there is no malicious node so there will be no SYN\_FLOOD packets.

<b>Simulation Results</b> Network Performance Link_Metrics Queue_Metrics TCP_Metrics IP_Metrics > IP_Forwarding_Table UDP_Metrics Application_Metrics LTENR_SDP	Application_Metrics_Table						
	Application_Metrics <input type="checkbox"/> Detailed View						
	Application Id	Application Name	Packet generated	Packet received	Throughput (Mbps)	Delay(microsec)	Jitter
	1	App1_CBR	10289	4980	11.631350	1203695.221799	982.1
	TCP_Metrics_Table						
	TCP_Metrics <input type="checkbox"/> Detailed View						
	Source	Destination	Segment Sent	Segment Received	Ack Sent	Ack Received	Duplicate ack received
	UE_1	ANY_DEVICE	0	0	0	0	0
	Link_Metrics_Table						
	Link_Metrics <input type="checkbox"/> Detailed View						
	Link_id	Link_throughput_plot	Packet_transmitted	Packet_errored	Packet_collided		
	All	NA	44453	12961	38	0	0
	Queue_Metrics_Table						
	Queue_Metrics <input type="checkbox"/> Detailed View						
	Device_id	Port_id	Queued_packet	Dequeued_packet	Dropped_packet		
	2	1	1	1	0		
Export Results (.xls/.csv) Print Results (.html) Open Packet Trace Open Event Trace > Log Files Restore To Original View							

	Throughput_APP1 (Mbps)	Throughput_APP2 (Mbps)
<b>Case-1: Malicious Node =0</b>	11.63	11.63
<b>Case-2: Malicious Node =1</b>	11.47	11.48
<b>Case-3: Malicious Node =2</b>	11.28	11.31

Go to the result window open Event trace, user can find out the SYN\_FLOOD packets via filtering subevent type as SYN\_FLOOD.

Event Trace.csv												
AutoSave Off												
Search												
sagar khetagouda												
File Home Insert Page Layout Formulas Data Review View Help Table Design												
Clipboard Font Alignment Number Styles Cells												
A1 Event_Id												
	Event_Id	Event_Type	Event_Time(US)	Device_Type	Device_Id	Interface_Id	Application_Id	Packet_Id	Segment_Id	Protocol_Name	Subevent_Type	
78	1	TIMER_EVENT	1000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
109	97	TIMER_EVENT	2000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
132	129	TIMER_EVENT	3000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
173	152	TIMER_EVENT	4000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
275	195	TIMER_EVENT	5000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
316	295	TIMER_EVENT	6000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
418	338	TIMER_EVENT	7000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
463	438	TIMER_EVENT	8000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
607	485	TIMER_EVENT	9000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
652	627	TIMER_EVENT	10000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
771	674	TIMER_EVENT	11000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
816	791	TIMER_EVENT	12000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
960	838	TIMER_EVENT	13000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
1003	980	TIMER_EVENT	14000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
1147	1025	TIMER_EVENT	15000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
1190	1167	TIMER_EVENT	16000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
1315	1212	TIMER_EVENT	17000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
1366	1335	TIMER_EVENT	18000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
1510	1388	TIMER_EVENT	19000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
1555	1530	TIMER_EVENT	20000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
1699	1577	TIMER_EVENT	21000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	
1743	1719	TIMER_EVENT	22000	UE	6	0	0	0	0	0 TCP	SYN_FLOOD	

**Note:** Users can also create their own network scenarios in 5G NR mmWave and run simulation.