

Create and detect a Primary User Emulation (PUE) Attack in Cognitive Radio Networks

Software Recommended: NetSim Standard v12.1 (32/64-bit), Visual Studio 2017/2019

Cognitive Radio (CR) is a promising technology that can alleviate the spectrum shortage problem by enabling unlicensed users equipped with CRs to coexist with incumbent users in licensed spectrum bands while causing no interference to incumbent communications. Spectrum sensing is one of the essential mechanisms of CRs and its operational aspects are being investigated actively.

In a hostile environment, an attacker may modify the air interface of a CR to mimic a primary user signal's characteristic, thereby causing legitimate secondary users to erroneously identify the attacker as a primary user. We coin the term *primary user emulation (PUE) attack* to refer to this attack. There is a realistic possibility of PUE attacks since CRs are highly reconfigurable due to their software-based air interface.

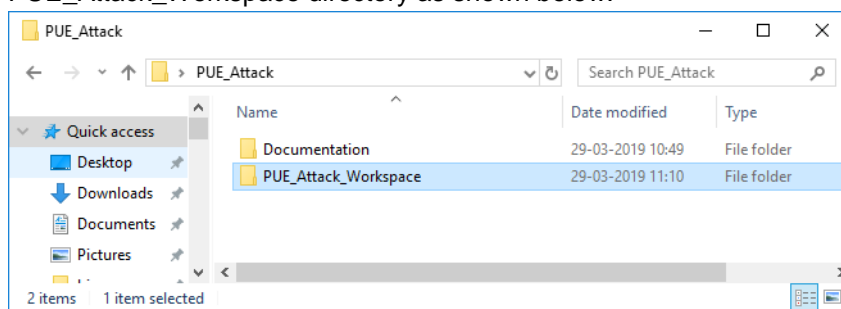
We create a PUE attack by adding two incumbents in the scenario in NetSim. One of the incumbents represents a “real” primary user while the second represents a “Malicious” primary user.

Our next goal is to detect the PUEA by the secondary users. For example purposes we have set the detection time as proportional to the distance of the secondary users from the malicious primary user.

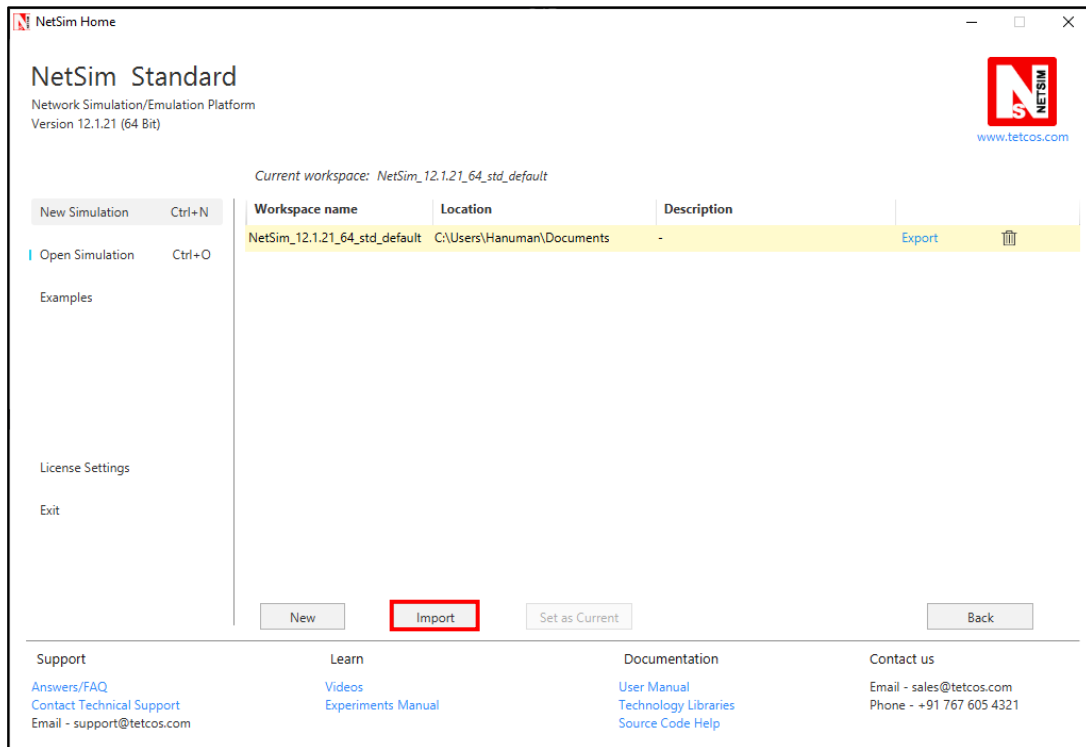
The code given below is for an example implementation of PUE Attack.

Steps:

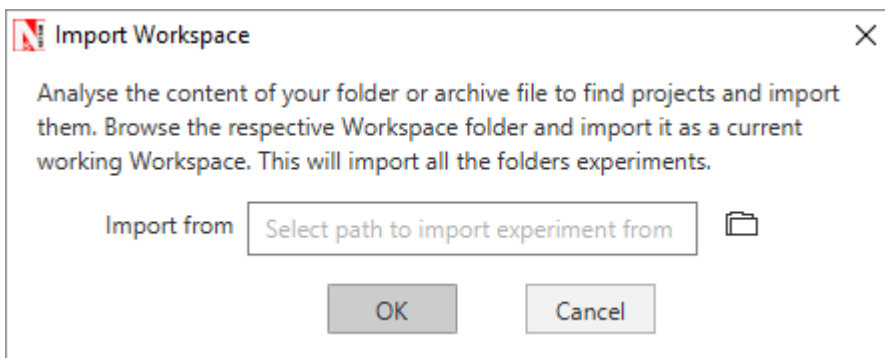
1. The downloaded project folder contains the folders Documentation and PUE_Attack_Workspace directory as shown below:



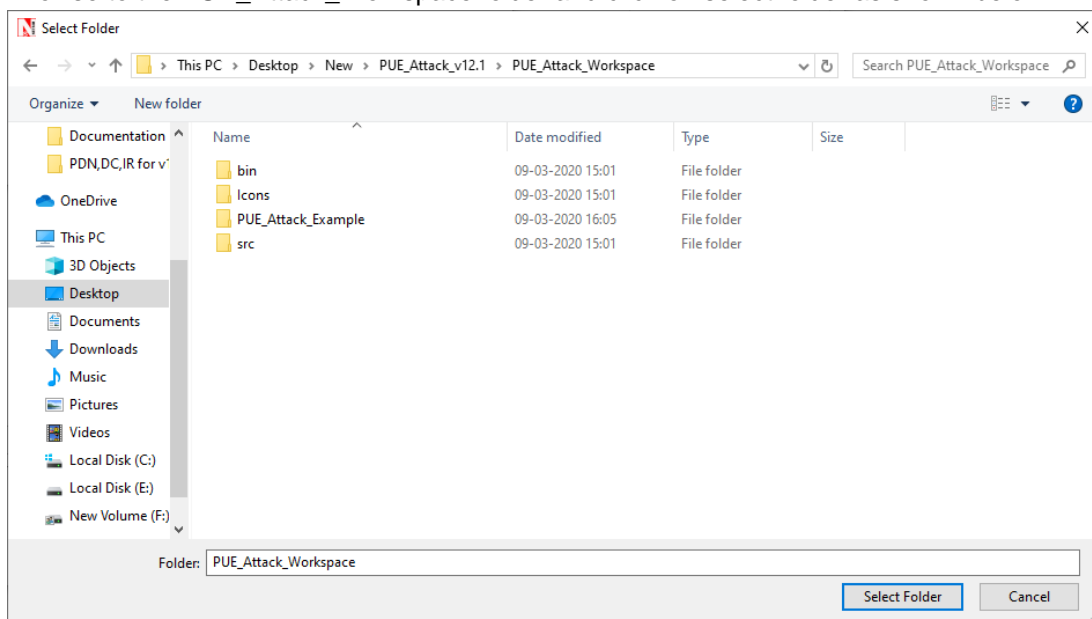
2. Import PUE_Attack_Workspace by going to Open Simulation->Workspace Options->More Options in NetSim Home window. Then select Import as shown below:



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

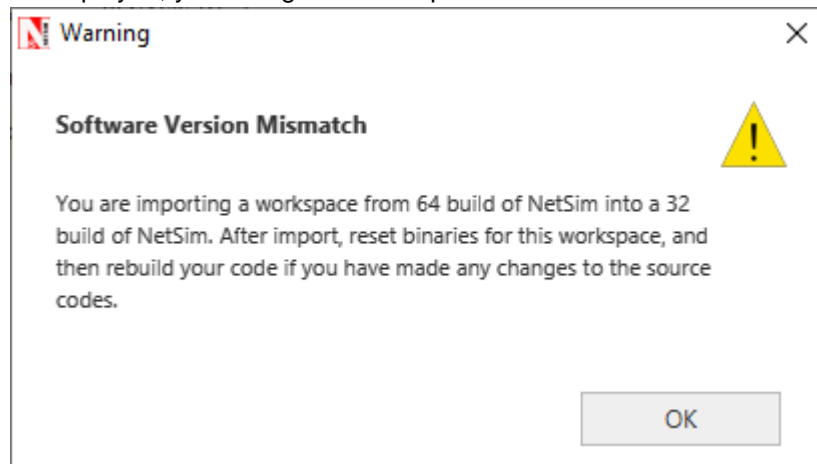


- Browse to the PUE_Attack_Workspace folder and click on select folder as shown below

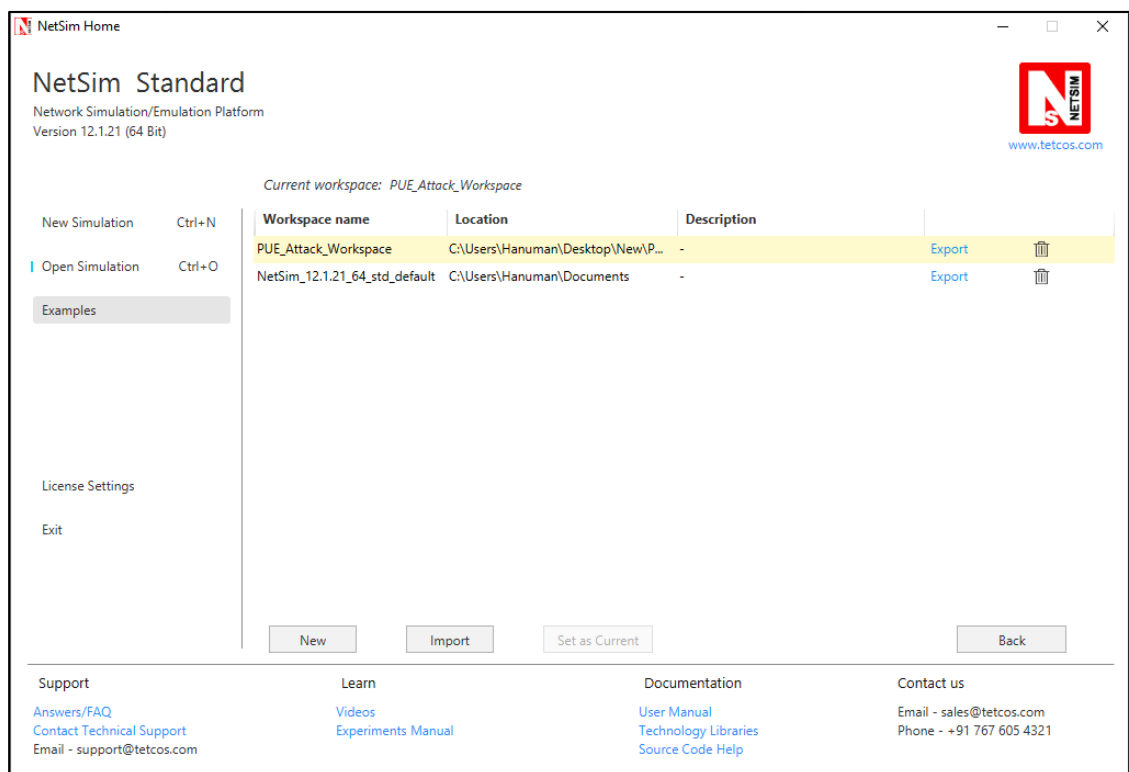


- After this click on OK button in the Import Workspace window.

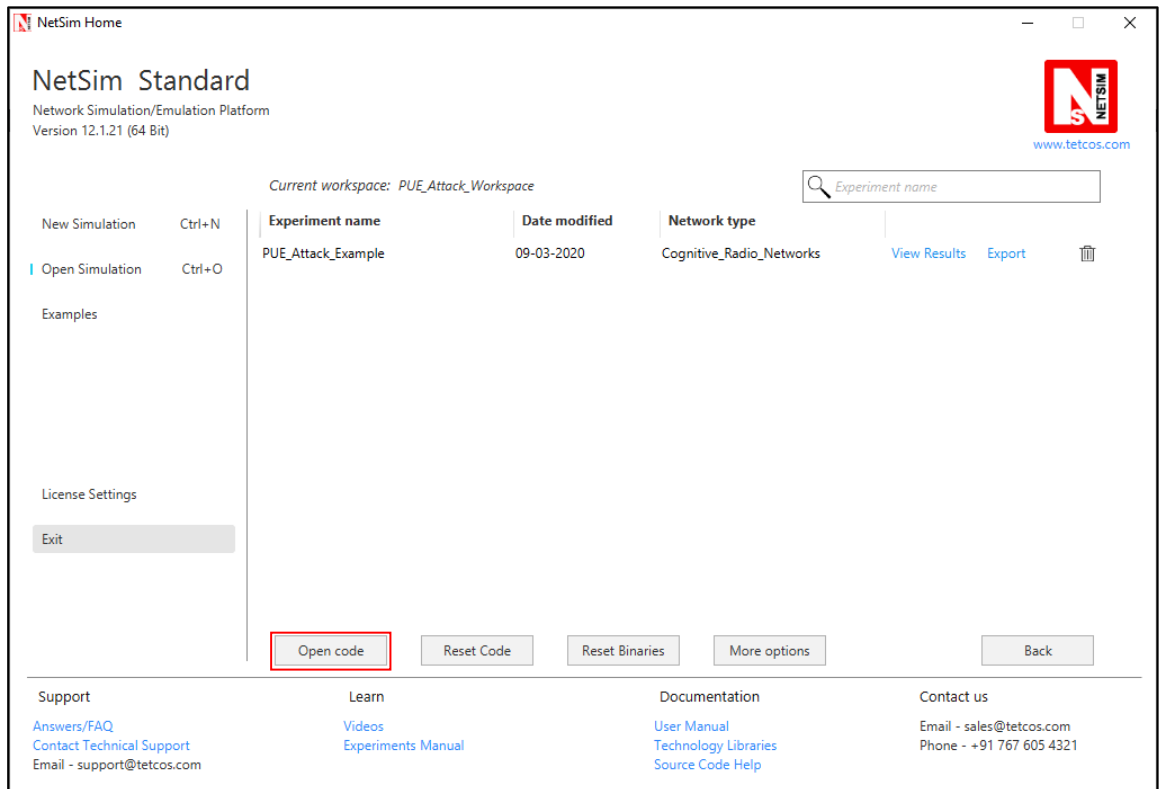
6. While importing the workspace, if the following warning message indicating Software Version Mismatch is displayed, you can ignore it and proceed.



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:



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



9. Go to **CognitiveRadio** project->Open **SpectrumManager.c**. Inside the **SpectrumManager.c** file, the code to be modified is commented as **PUE Attack code**. Do the required modifications.

```

290
291
292 struct stru_802_22_SSFOutput* fn_NetSim_CR_CPE_SSF(struct stru_802_22_SSFInput* input, NETSIM_
293
294 {
295     struct stru_802_22_SSFOutput* output = (struct stru_802_22_SSFOutput*)fnpAllocateMemory(1
296     unsigned int nLoop;
297     double dDistance;
298     int Additional_delay;
299     int Detection_time;
300     int nflag = 0;
301     static FILE *fp_CR=NULL; // Code for PUE Attack
302
303     double p = fn_NetSim_Uilities_GenerateRandomNo(&DEVICE(nDevId)->u1Seed[0],
304     &DEVICE(nDevId)->u1Seed[1])/NETSIM_RAND_MAX;
305     if(p<(double)input->nMaxProbabilityOfFalseAlarm/100.0)
306         nflag = 1;
307
308     // Code for PUE Attack
309     if(!fp_CR)
310         fp_CR=fopen("CR_Detect.txt", "w");
311
312     // End
313
314     for(nLoop=0; nLoop<input->nIncumbentCount; nLoop++)
315     {
316         if(input->pstruIncumbent[nLoop]->nIncumbentStatus == IncumbentStatus_OPERATIOAL)
317         {
318             dDistance = fn_NetSim_Uilities_CalculateDistance(DEVICE_POSITION(nDevId), input->

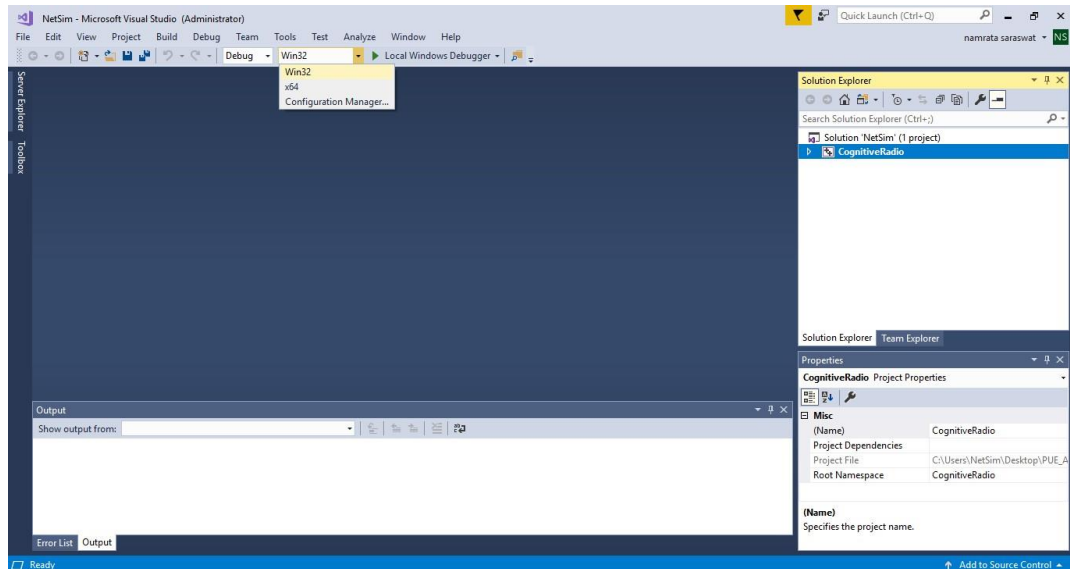
```

```

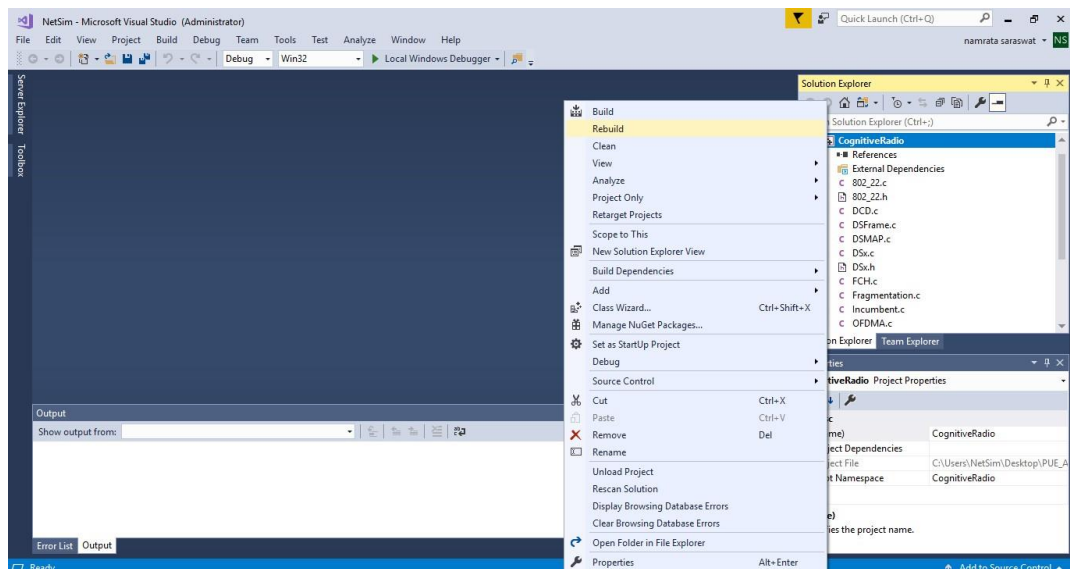
302 double p = fn_NetSim_Uilities_GenerateRandomNo(&DEVICE(nDevId)->u1Seed[0],
303 &DEVICE(nDevId)->u1Seed[1])/NETSIM_RAND_MAX;
304 if(p<(double)input->nMaxProbabilityOfFalseAlarm/100.0)
305     nflag = 1;
306
307 // Code for PUE Attack
308 if(!fp_CR)
309     fp_CR=fopen("CR_Detect.txt", "w");
310
311 // End
312
313 for(nLoop=0; nLoop<input->nIncumbentCount; nLoop++)
314 {
315     if(input->pstruIncumbent[nLoop]->nIncumbentStatus == IncumbentStatus_OPERATIOAL)
316     {
317         dDistance = fn_NetSim_Uilities_CalculateDistance(DEVICE_POSITION(nDevId), input->pstruIncumbent[nLoop]->position);
318         if(dDistance <= input->pstruIncumbent[nLoop]->dKeepOutDistance)
319         {
320             //Incumbent detected
321
322             // ***** PUE Attack project code start
323             // dDistance is the distance between CR CPE and incumbent and is got from above
324             Additional_delay = dDistance / 10;
325             // We have randomly set 10 as the velocity of the signal based on which
326             // the additional delay is got. If you increase this you will see a lower
327             // delay and vice versa
328             Detection_time = pstruEventDetails->dEventTime + Additional_delay;
329             fprintf(fp_CR, "Time to detect incumbent %d by CPE %d is %d microseconds \n", nLoop+1, nDevId, Detection_time);
330             fflush(fp_CR);
331
332             // ***** Project code end
333
334             //check for possible interference
335
336

```

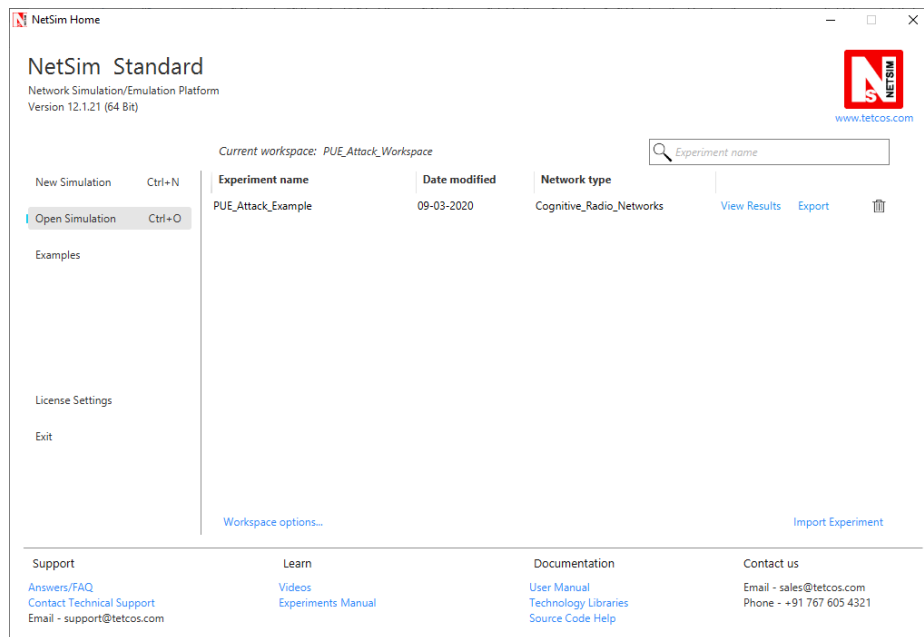
10. Based on whether you are using NetSim 32 bit or 64 bit setup you can configure Visual studio to build 32 bit or 64 bit DLL files respectively as shown below:



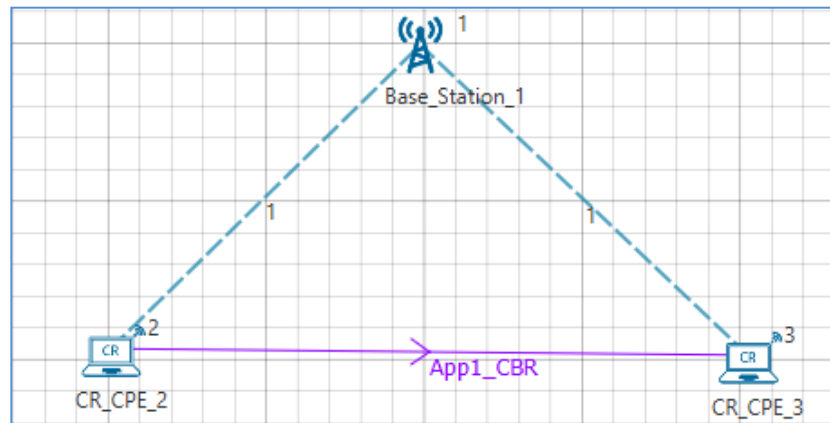
11. Right click on the Solution in the solution explorer and select Rebuild.



12. Upon successful build modified libCognitiveRadio.dll file gets automatically updated in the directory containing NetSim binaries.
13. Then PUE_Attack_Workspace comes with a sample configuration that is already saved. To open this example, go to Open Simulation and click on the PUE_Attack_Example that is present under the list of experiments as shown below:



14. The network scenario loads as shown below:



Following settings were done in the devices for this example.

15. In **CR-Base_Station_1/INTERFACE_1 (COGNITIVE_RADIO) Incumbent** properties, the **Incumbent count** is set as **2**

16. In the Incumbent properties:

In malicious (Incumbent_1), **ON_Duration(s) – 4, OFF_Duration(s) – 10**

In Incumbent (Incumbent_2), **ON_Duration(s) – 9, OFF_Duration(s) – 9**

Keep Distance = 500m in both incumbent and the distance between the CPE and Incumbent is <500. This ensures that the incumbent is detected. If the incumbent is beyond the keep out distance then it is not detected.

The timing diagram is as follows:

Malicious --- 0s to 10s (OFF), 10s to 14s (ON), 14s to 24s (OFF), 24s to 28s (ON) ... and so on

Incumbent --- 0s to 9 s (OFF), 9s to 18s (ON), 18s to 27s (OFF), 27s to 36s (ON) ... and so on

Cr_Bs

Cr_Bs

GENERAL
INTERFACE_1 (COGNITIVE_RADIO)

DATA LINK LAYER

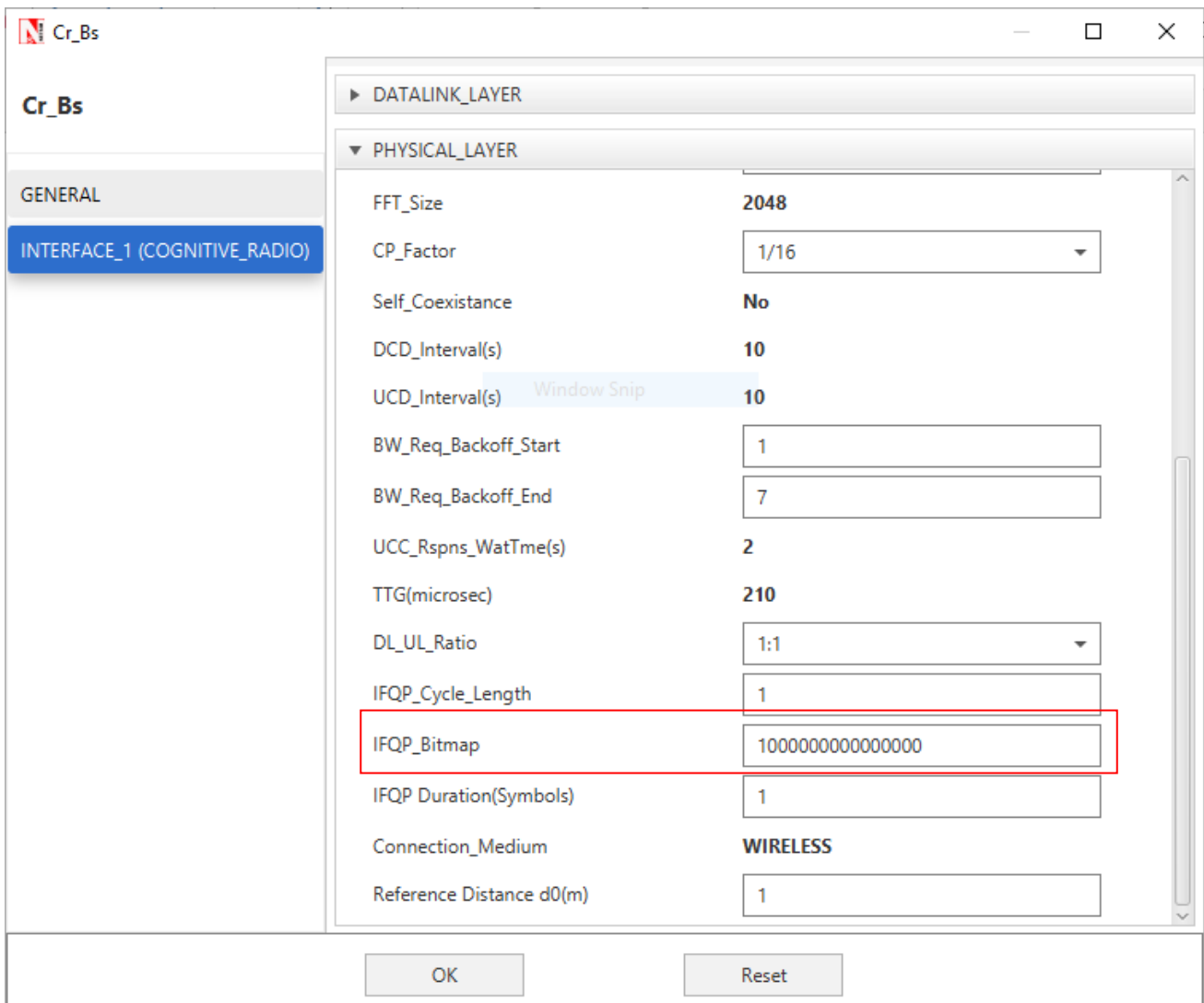
ON_Duration(s)4
OFF_Duration(s)10
Keepout_Distance(m)500
Oper_DistributionConstant

INCUMBENT2
NameIncumbent 2
ID2
X_Co_Ordinate50
Y_Co_Ordinate100
Z_Co_Ordinate0
Oper_Freq_Start(MHz)54
Oper_Freq_End(MHz)60
ON_Duration(s)9
OFF_Duration(s)9
Keepout_Distance(m)500

PHYSICAL LAYER

OKReset

17. In physical layer, the **IFQP_Bitmap** is set to 1000000000000000



18. Now run the simulation 50 Sec.

19. You can see the delay in the **CR_Detect.txt** file inside bin folder. This additional delay has been set by the following code,

Additional_delay = dDistance / 10;

(You can also change the values as 10/100/1000 and analyse different variation in delay.)

A file "**CR_Detect.txt**" will be created in the bin folder (NetSim installation directory) with the following contents:

```

CR_Detect.txt - Notepad
File Edit Format View Help
Time to detect incumbent 2 by CPE2 is 9129741 microseconds
Time to detect incumbent 2 by CPE3 is 9129761 microseconds
Time to detect incumbent 1 by CPE2 is 24049741 microseconds
Time to detect incumbent 1 by CPE3 is 24049761 microseconds
Time to detect incumbent 1 by CPE2 is 38129741 microseconds
Time to detect incumbent 1 by CPE3 is 38129761 microseconds
Time to detect incumbent 2 by CPE2 is 45009741 microseconds
Time to detect incumbent 2 by CPE3 is 45009761 microseconds

```

This is a simple implementation of creating and detecting a PUE Attack by making modifications to primary user detection in CR.