IJASRM

International Journal of Advanced Scientific Research and Management, Volume 3 Issue 10, Oct 2018

www.ijasrm.com

ISSN 2455-6378

Security framework against denial of service attack on cognitive radio networks

Meenakshi Malhotra[1], Dr. Inderdeep Kaur Aulakh[2]

[1]Research Scholar, Department of I.T, U.I.E.T, Panjab University,
Chandigarh, 160014, India

[2]Associate Prof (Supervisor), Department of I.T, U.I.E.T, Panjab University,
Chandigarh, 160014, India

Abstract

The cognitive radio technique is used to overcome the underutilization problem in the wireless network. The cognitive radio systems are not equipped with the security mechanism to protect them against the denial of service or packet flooding attacks. For the cognitive radio security against the denial of service attacks using packet flooding mechanism can be controlled by allocating the resources to the legitimate users only. To ensure the legitimacy of the primary user (who forwards the data) and secondary users (who perform the spectrum sensing task), we have proposed the key management scheme between both of the users. The idea is to protect the frequency allocation process, where the secondary user is the spectrum sensing agent and the primary user is the data manager. The secondary user will manage the legitimacy assurance of the primary user by sharing the keys before allocating the spectrum. After performing the spectrum sensing, the secondary user asks for the security key from the primary user, if the primary user provides the correct security key, the secondary user leaves the frequency. In case the key exchange verification fails, the secondary user does not share the spectrum information with the imposter primary user to protect against the non-legitimate users, who can further launch denial of service attacks over the cognitive radio channel. The performance results have been obtained in the form of probability of detection, probability of false alarm, data delivery volume, etc. The proposed model has performed significantly well in the case of attack in the experiments performed, which shows the effectiveness of the proposed model to protect the cognitive radio links against the denial of service attacks.

Index Terms—Cognitive Radio Networks, Primary User, Secondary User, Primary User Emulation Attack (PUEA), Denial of Service (DoS) attack, Advance Encryption Standard (AES), Key.

1. Introduction

In the wireless networks, one can use the network resources depending upon the available spectrum. The wireless network deals with the primary user and the secondary user. The primary users are those users which are independent to use the spectrum anytime. The FCC from past decades states that the spectrum of the primary user is not used all the time. That underutilization problem arises in the network overcomes with the help of the technique named Cognitive Radio Technique. The cognitive radio networks allow the secondary user to use the primary user spectrum by keeping in mind the availability of the primary user. If the primary user is using the spectrum then in no case the secondary user can use the spectrum band.

The cognitive radio networks consider four steps i.e Spectrum sensing, spectrum management, spectrum sharing and the spectrum mobility. The Spectrum sensing sense the available spectrum band. Spectrum Management does it work by choosing the best spectrum band. Spectrum Mobility deals with avoiding the interference between the primary user and the secondary user. The spectrum sharing is used to provide the scheduling methods among the users in the network. These four steps are also known as the acyclic process of the cognitive radio networks.

In 2014 [Aulakh I. K. et al.], the negative acknowledge has been considered for determining the effect of feedback response coming from the Unlicensed User and for better decision making, the secondary user's transmitter uses this feedback.

In 2014[Aulakh I. K et al.] to maximize the SU utility, Optimization of probability of false alarm with respect to collision cost is done in a threshold based sensing-transmission structure. The simulation results have obtained in the form of thresholds for probabilities of false alarm as well as in terms of collision costs.

The cognitive radio networks gives a remarkable solution to the problem arises at the time of communication and the underutilization problem. But the attacks can be arrived at any stage of the network. The different types of attack on CR networks include-

- Denial of Service (DoS) attacks,
- System penetration,
- Repudiation,
- Spoofing,
- Authorization,
- Violation,
- Malware infection,
- Data modification.

Like the different types of attack, there are different types of attacker too exist-

- Selfish & Malicious Attackers,
- Power-Fixed & Power-Adaptive Attackers,
- Static & Mobile Attackers

This paper uses two schemes names as Advance Encryption Standard and One-time key generation. For successful process, firstly key generation is done with the help of one time key generation scheme and that random keys are maintained on both the sides like on primary user as well as on the secondary user side. AES scheme encrypt and decrypt the signal with the help of key maintained on both the sides. When any user requests for the signal then the receiver side send the query key and with the help of that query key, sender side gives the response. If the sender side do not respond or give wrong key then after matching process the receiver block the sender and start receiving the request from others. If the sender replies with the right key then the cognitive process starts there. For the simulation results, Matlab has been considered.

The rest of the paper is divided into various sections: Section II discusses the work from which the proposed model is inspired; Section III presents the experimental design to obtain the results against the attack; section IV shows the results obtained in term of GUI in MATLAB, comparison table of the graph values and the data volumes of the signals receives at the sender and the receiver side. Finally, section V gives the conclusion followed by future work.

2. Motivation

In 2013 [Gregori M et al.] for decentralized and cooperative analysis of PUE attack, authors introduced a novel based multiple criteria scheme INCA in Cognitive Radio Ad Hoc Networks. INCA is composed of two phases. In the first phase to gain flexibility, the Normalized Weighted Additive Utility Function has been considered. In the second phase to detect the presence of attacks by a node to another node, the Bayes theorem is considered. After applying both the above mentioned phase, the simulation results showed that INCA can recover the analysis in the presence of PUEA.

[Dang M et. al.] in 2013 authors introduced the concept of compressive sensing (CS) into primary user emulation attack (PUEA) detection. To distinguish between the primary user signal and the PUEAs, the location of the transmitter was considered. In the study, the Received Signal Strength (RSS) was taken. As the RSS contains redundancy in the domain, so to save the sensor measurement the CS theory was taken into study. The researchers introduced an adaptive orthogonal matching pursuit algorithm (AOMP) to adjust the changes belongs of PUEA. Simulation results give the better accuracy with the AOMP algorithm. With the result, the improvement in channel utilization was seen.

[Bagheri A et. al.] In 2013, authors in their work, path loss/shadowing as well as path loss/fading scenarios considered as an important point. Simulation results showed that with the good secondary user at a good distance successful PUEA possibly be obtained with the increment in the number of malicious users.

In 2014 [Chen Y et. al.], authors consider two points, one is cooperative spectrum sensing system as a model and soft fusion as fusion method. With the help of maximal ratio combining method and energy detection, the impact of PUEA on system performance was tested. For the simulation, the proper weight coefficient was taken into consideration which gives the better system performance as a result.

In 2014, [Saber M et. al.] authors in the presence of smart PUEAs introduced a cooperative spectrum sensing scheme. The information from various smart PUEAs is joined at the malicious user fusion center. So finally the information collected from the fusion center is used to maximize the signal to interference-plus noise ratio (CSINR). And from the comparative study it is seemed that it gives better accuracy results in terms of detection.

In 2013, [Abdelhakim M et al.] authors suggested an AES-assisted DTV (Digital TV) scheme. In the suggested scheme, an AES-encrypted reference signal is generalized at the TV transmitter. For the DTV data frames, the generalized signal is used as sync bits. The reference signal can be generated again with the help of shared secret amongst the transceiver. This process is also used to achieve the results of the authentic user. With the help of the proposed scheme, the difference between the licensed user and the malicious user can be achieved. The proposed scheme considers at the time of PUEA in terms of greater accuracy.

[Anand S et. Al.] In 2009, authors focused on primary user emulation attacks (PUEA) in the networks, having no location information. To detect the PUEA, Fenton's approximation and Wald's sequential probability ratio test (WSPRT) were used. Simulation results not only gives the probability of low PUEA but also low probability of missing the primary information.

[Hao D et. Al.] In 2012, authors focused on PUEA keeping an eye on the channel usability. The interaction among the PUE attacker and the Cognitive user is considered which sometimes called as PUEA game. In the cognitive radio networks the objective of secondary user is to discover the best sensing strategy so as to increase the channel usability whereas on the other hand the objective of attacker is to reduce the cognitive users' channel usability. Rather than going for Nash equilibrium solution to the PUEA game, a best anti-PUEA technique was considered. Numerical results showed the optimal sensing strategies, and also showed the channel usability with the differential game solution.

[Wang W et. al.] In 2014, authors determined the collision's initial point. This point is determined by taking the distance between the sender and receiver at the time of two signal interfere. That interference result is then used to determine the location of the authentic primary user. This location information of the authentic user is then compared with the known location of the primary user. Then the comparison result is used to detect the PUE Attack.

[Li. H et. al.] In 2012, authors discussed quickest detection problem name given to the DoS attack. To reduce the detection delay, a non-parametric version of cumulative sum (CUSUM) algorithm was used to ease the attacks. Using a Spectrum-Aware Split Multipath Routing with the dynamic channel, the simulation results states the effectiveness of the mentioned approach.

[Weifang W] In 2012, author focusing on the security issues arising on the cognitive radio networks discussed the DoS attack at various layers. DoS attack is vulnerable, as the attacker continuously send the frequency or the signal to the authentic user which results in blocking or disabling the authentic user. The discussed paper examined the architecture of cognitive radio networks as well as the DoS attacks in cognitive radio networks in various protocol layers.

[Attar A et.al.] In 2010, authors proposed a Channel Eviction Triggering defense scheme. This paper discussed a special kind of DoS attack which is basically invoked by the Channel Eviction Triggering (CET). In this kind of attack, the rival nodes suspiciously invoke mechanisms to protect the licensed users and thus interrupt secondary access which leads to the manifestation of CET attacks. This type of attack is a kind of cheating to the cognitive radios. The simulation results validate the effectiveness of the introduced CET defense scheme.

In the presence of PUE Attack, [Chen C et. al.] in 2011 authors considered the cooperative spectrum sensing. In the proposed scheme, all the sensing information coming from the secondary users are joint at the fusion center. The optimization of combined weights is done to increase the probability of detection.

[Sengupta S et. al.] Authors in 2011 consider two cases named one-stage and multi-stage case to mitigate the DoS attack in the cognitive radio networks. One-stage case, formulation of the cooperative game between the malicious nodes are done and develop the effective decision strategy. In the case of multi-stage, to determine the behavior of the malicious user and secondary user, the Markov chain model was proposed. Simulation results state that in the one-stage case, the coordinated attack attains was on 10-15% improvement and, in the multistage case, the existence of malicious nodes was notified, which was maximizing the net payoff.

[Chatterjee PS et. al.] Authors in 2015 focused on a different kind of attack in Cognitive Wireless Sensor Networks that is SSDF (Spectrum Sensing Data Falsification) attack. And the SSDF is the kind of DoS attack. In the SSDF attack, a modification is done on the sensing report. With the help of this false information, the secondary user takes the wrong decision about the spectrum usage. To minimize the effect of this attack, the similarity based clustering is used to sense the data or the information.

[Nene MJ et. al.] In 2012 authors deal with SSDF attack. The previous results showed that the various techniques failed when the number of secondary user increases as compare to the authentic secondary user. So the proposed technique is not dependent upon the malicious SUs. And the proposed techniques does it work with the help of primary user's Received Signal Strength (RSS) at an SU, to determine the position and match this value with the calculated once at data fusion center.

To determine the attacks in the network, the authors [Bhunia S et. al.] in 2014 considered the honeypot theory. A defense mechanism was suggested named honeynet. The honeynet determines the strategy of the attacker with the help of the available past information of the attack

[Anand S et. al.] In 2012, authors simulated the result to show the reduced number of call dropped in the network at the time of communication. The secondary networks contain the real time and non-real time traffic. PUEA basically in the radio environment increases the call drop rate and delay in the secondary network. With the help of simulated results, it can be stated that with the increment in the malicious traffic load, a performance improvement on the delay by up to 54% was noticed.

3. Experimental design

The proposed work methodology uses two schemes named as Advance Encryption Standard and One-time key generation. Firstly the emulated user will launch the Denial of Service attack and transmit the packet to the target node in the environment. After receiving the packet send by the emulated user, the target node send the query key to verify the authenticity of the user. The key is maintained by the key table generated on both the authentic ends. If the node reply with the right key then the target node starts sharing the information with the other end otherwise it blocks the user for the future purpose.

a. One-Time key generation policy:

The one-time key generation scheme is used to generate the unique key on both the end. The generated key will be used only for one transaction at a time. The key if used then it became outdated which increase the probability of emulated user not to guess the key. The unique key is on time based and event-based. The key generated is text-based. The key can be in text based or in graph-based.

When the key is generated with the help of random number then a huge variety of generated keys are concatenated to build up the one-time key generation. That number is then converted to the complex number.

The one-time key generation generates a matrix with millions of values which is then picked up randomly. The random pick up of values, from the matrix of million values is done with the help of spherical random function.

Key generation policy under the proposed model is using the mathematical algorithmic flow to generate the key table. With the help of that key table, the key will be exchanged between the sensor nodes in the working cluster.

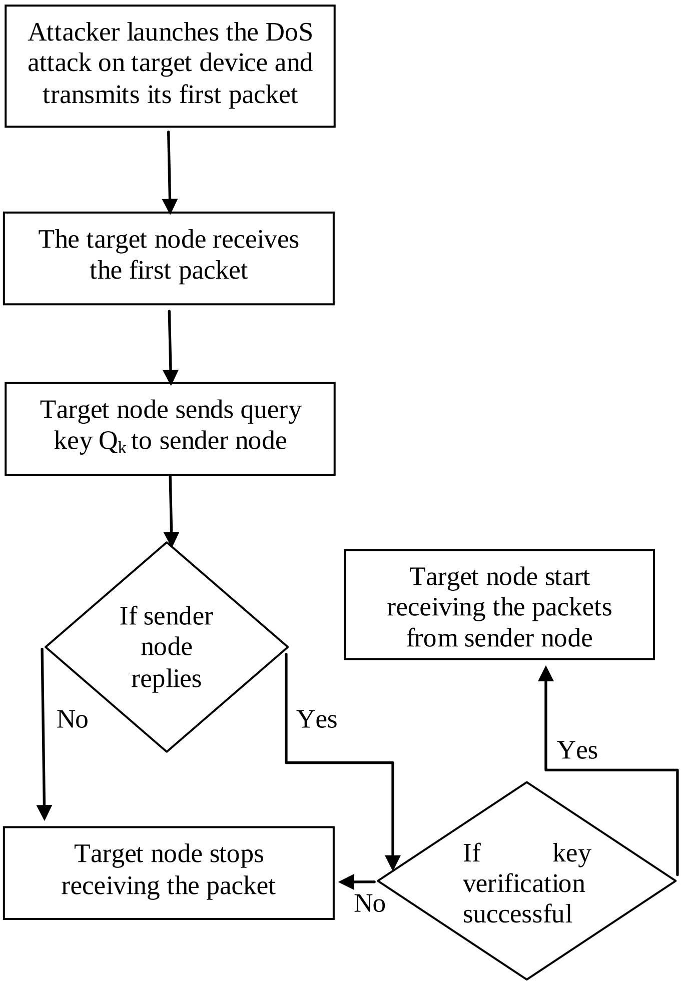

Attacker launches the DoS attack on target device and transmits its first packet
The target node receives the first packet
Target node sends query key Q_k to sender node
If sender node replies
No
Yes
Target node start receiving the packets from sender node
Yes
Target node stops receiving the packet
No
If key verification successful

Fig 1: Flow chart of Proposed Work

ALGORITHM STEPS: RANDOM FUNCTION TO GENERATE RANDOM NUMBER

1. First, initialization of random number generator to make the results repeatable.
2. Generate a radii value for each point in the sphere. These values are in the open interval (0,3) which on the positive side are not uniformly distributed. With the help of mathematic equation, the values have been generated:

$$f(x) = 3 * \int_{1}^{1000000} random * \frac{1}{3}$$

3. Select values randomly and concatenate them to create the OTKP.
4. Return OTKP

b. *AES encryption algorithm:*

The earlier proposed work algorithm has been designed with three major phases of development. The first phase of development associates with including the implementation of improved AES for changed window size or block size. The objective of second phase has been achieved by the improvement in the key-matrix for key-expansion. The third phase has been completed by improving the s-box size and shape for the effective and fit AES scheme. The last phase of the development is associated with the development of data validation and segmentation algorithm to make the encryption application fit for a wider number of situations.

Phase 1: Programming Optimization:

In the proposed method, an improved kind of AES encryption has been used. This improved AES algorithm is used to attain the goal of fast implementation. In the first step, all the input digits are enlarged to 128 bits, which will improve the speed of the system. In one time sequence, data will be enter into the encryption or decryption system. This process will reduce the data entering and passing time.

Phase 2: Static S-BOX:

After the programming optimization static S-BOX process comes. In this design, after achieving the key matrix, in a continuous way every part of the Key-Expansion is done. The Key-Expansion deals with two parts. First part deals with calculating the part before the S-BOX and the second one deals with calculating the part after the data passes through the S-BOX. But the problem remains the same. The problems like multi-input problem and chaos inputs come at many points, which enlarges the requirement of the design space. Applying the new S-box designed, the performance of Anti-Square attacking will be improved.

Phase 3: Segmentation and Validation algorithm:

The last phase deals with the merging of AES algorithm with traditional data segmentation as well as with the validation algorithm. This step could validate the data size according to the input data size, resulting in increasing the speed of encryption and decryption. The AES algorithm is used to encrypt and decrypt for lesser data otherwise the segmentation algorithm is applied prior to encrypt and decrypt.
The explained mechanism has added the robustness and flexibility in the AES algorithm. Additionally, AES encryption carries the encryption keys, the segmentation algorithm is used prior the encryption and after that AES decryption is applied while the transmission of the signals. For improvement, the design is divided into nine rounds which include three parts in itself. Every three

rounds will be reputed as one block. The three blocks will be responsible to complete the whole nine rounds. This pipeline method will increase the operating speed of the system. Two connected blocks in the algorithm do not contain the delay and will save time for the data transmission.

ALGORITHM 1: THE PROPOSED AES ALGORITHM ENCRYPTION PROCESS

```
1.  Input Data Matrix (d)
2.  Data Matrix Validation $\rightarrow$ validate(d) $\rightarrow$ $d_M$
3.  Data Matrix Segmentation $\rightarrow$ segment(dM) $\rightarrow$ $d_m^i$
4.  Input Security Key ($S_k$)
5.  KeyExpansion($S_k$)
6.  InitialRound $\rightarrow$ AddRoundKey ($S_k$)
7.  Rounds $\rightarrow$ For Loop
        a.  SubBytes($d_m^i$)
        b.  ShiftRows($d_m^i$)
        c.  MixColumns($d_m^i$)
        d.  AddRoundKey($d_m^i$)
8.  Rounds $\rightarrow$ End For Loop
9.  Final Round $\rightarrow$ MixColumns (False)
        a.  SubBytes($d_m^i$)
        b.  ShiftRows ($d_m^i$)
        c.  AddRoundKey($d_m^i$)
10. Data Matrix Merger $\rightarrow$ merge($d_m^i$) $\rightarrow$ $dE_M$
11. Data Matrix Reverse validation $\rightarrow$ rvalidate
    ($dE_M$) $\rightarrow$ dE
```

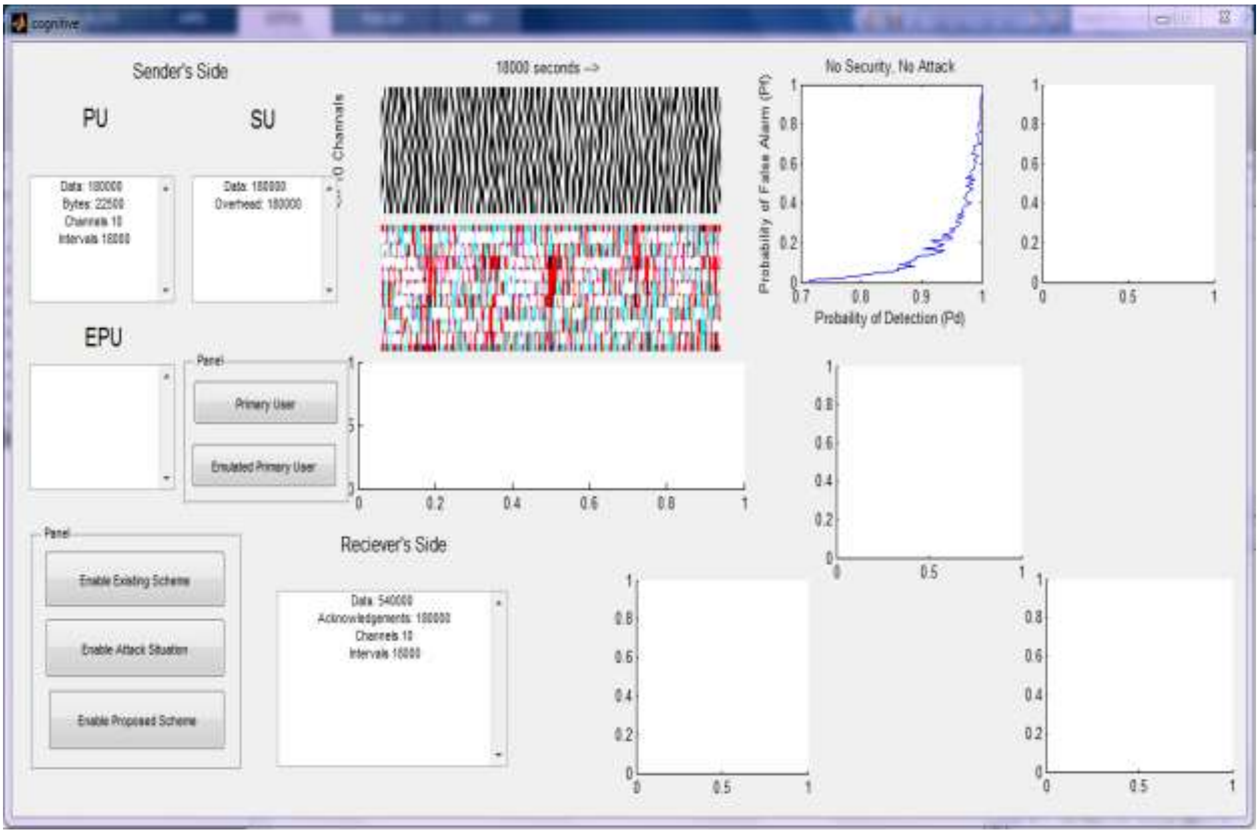
The decryption process is much more complicated as compare to encryption process. Decryption process also consumes much more time. For this problem, two feasible solutions are found: decomposing the columns and constructing some forms.

The proposed algorithm is based on a complex predictive key sharing mechanism. The key sharing mechanism consists of the various complex key scrambling mechanisms. These mechanisms have been used to protect the key theft during the transmissions. Also the key is sent in the form of decimal formats during the transmission, which can easily confuse the hacker. Because the attacker may get the key as the normal mathematical data, being transmitted in the packet data.

ALGORITHM 2: PROPOSED SCHEME KEY EXCHANGE ALGORITHM

```
1.  Get random key
        X = rand*100;
2.  Define n in the range between 1 and n, where n
    is the number of rows in the key table
3.  Select the key A on the secondary user end,
    which will be further sent towards the primary
    user
4.  Encrypt the Key A using the advance encryption
    standard (AES) algorithm on the secondary user
    end
5.  Transmit Key A to primary user end
6.  Primary user decrypt the key A using the reverse
    AES algorithm
7.  Primary user finds the corresponding key in its
    key table information as Key B
8.  Primary user select and encrypt the key B.
9.  Transmit Key B to secondary user
10. Secondary user decrypt the Key B, obtain Key
    AB from its key table information
11. Match the key and return the decision logic
```

4. Simulated results

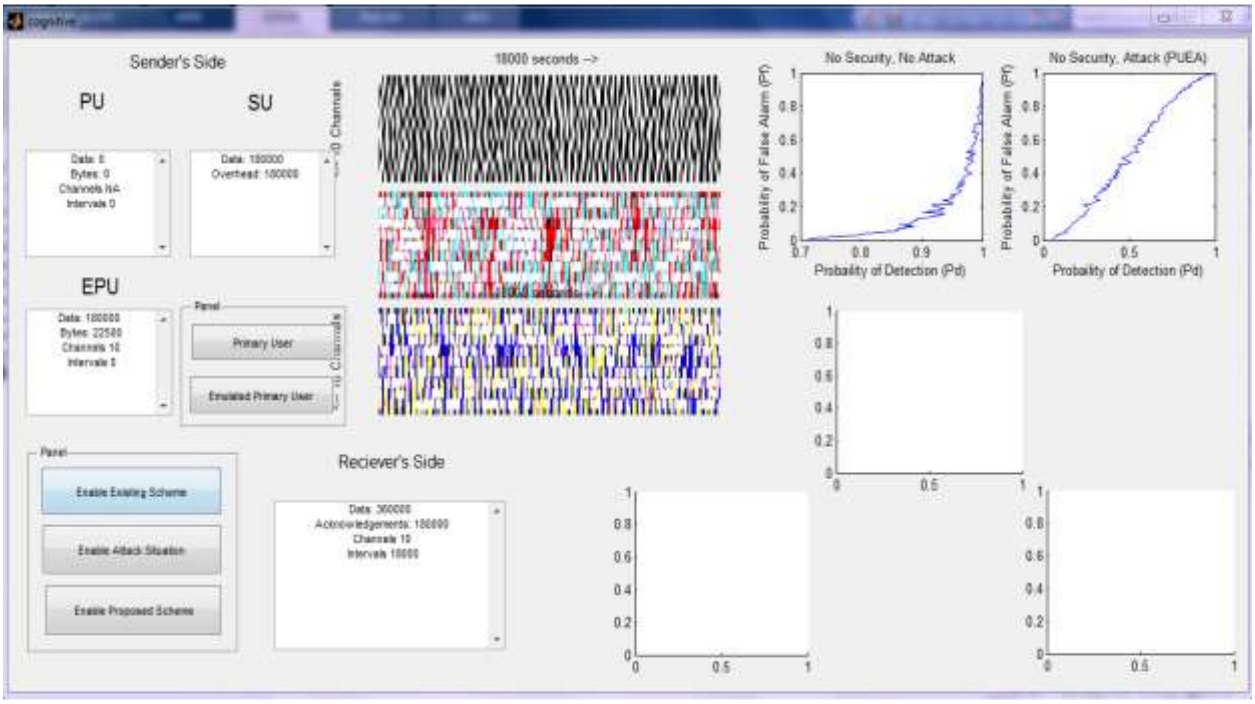


Data: 180000
Bytes: 22500
Channels 10
Intervals 18000

Data: 180000
Overhead: 180000

Data: 540000
Acknowledgements: 180000
Channels 10
Intervals 18000

Fig 2: Primary User Signal transmission



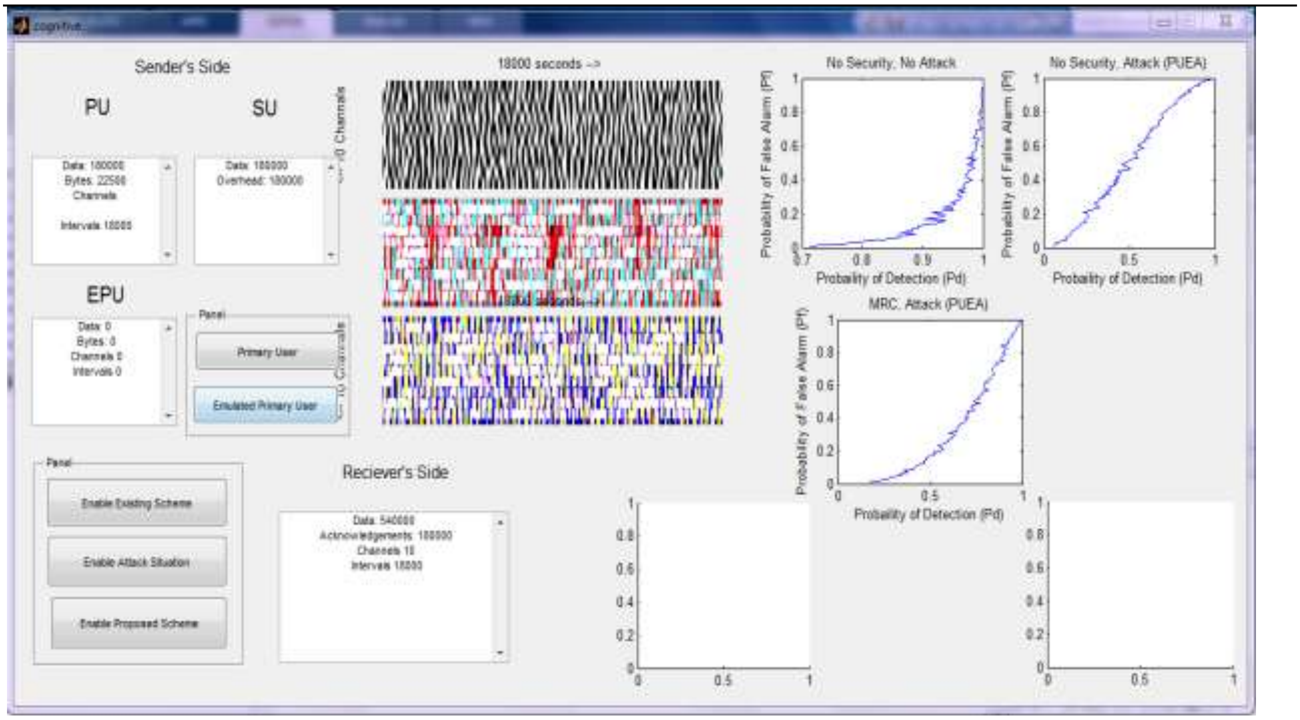
Data: 0
Bytes: 0
Channels NA
Intervals 0

Data: 180000
Overhead: 180000

Data: 180000
Bytes: 22500
Channels 10
Intervals 0

Data: 360000
Acknowledgements: 180000
Channels 10
Intervals 18000

Fig 3: Signal Transmission in case of PUEA attack



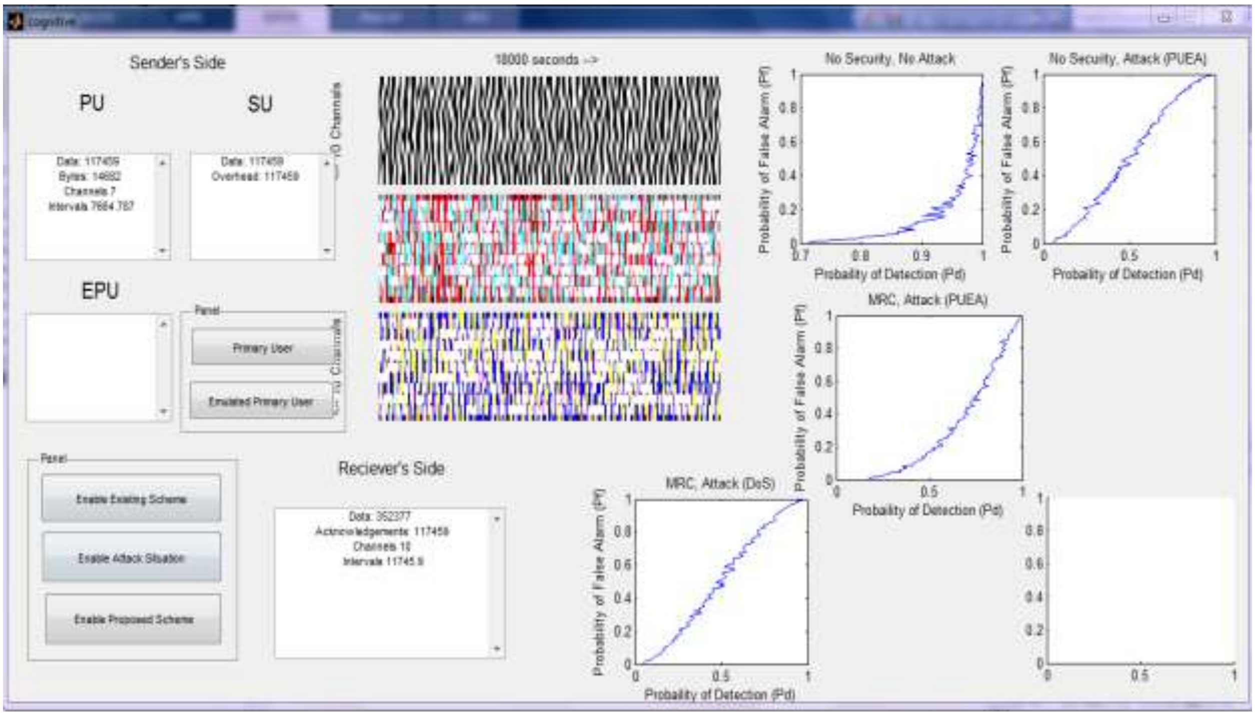
Data: 180000
Bytes: 22500
Channels
Intervals 18000

Data: 180000
Overhead: 180000

Data: 0
Bytes: 0
Channels 0
Intervals 0

Data: 540000
Acknowledgements: 180000
Channels 10
Intervals 18000

Fig 4: Existing solution on PUEA

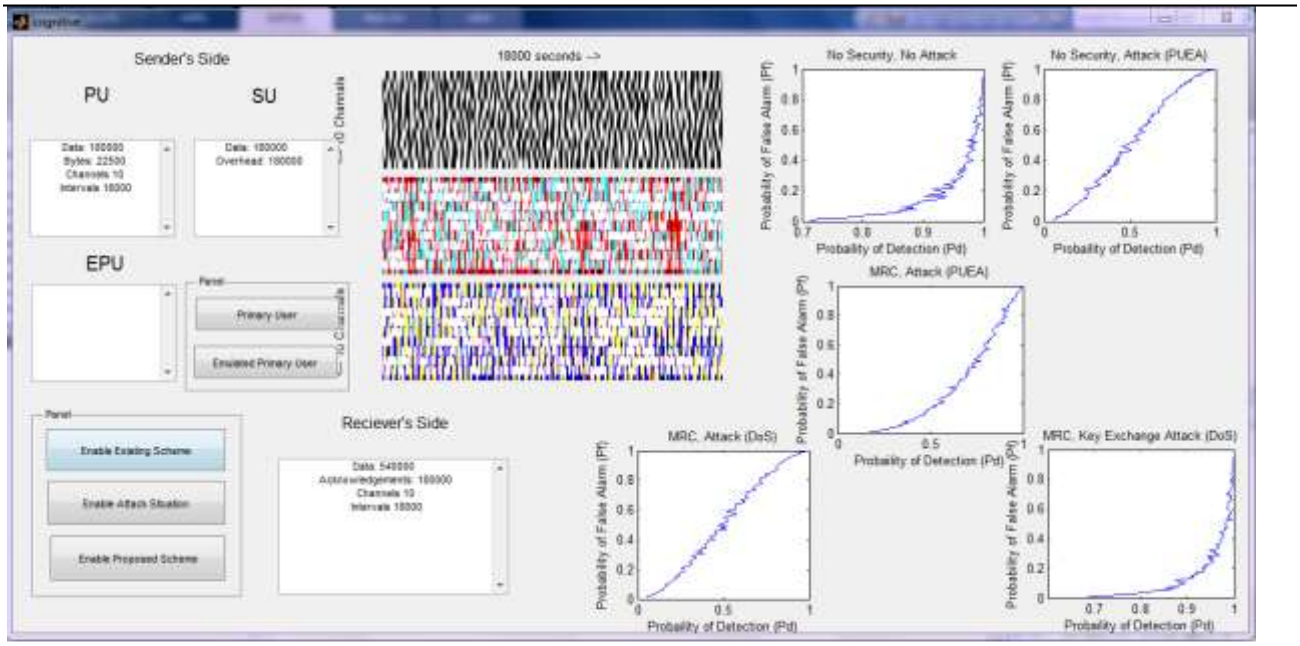


Data: 117459
Bytes: 14682
Channels 7
Intervals 7684.787

Data: 117459
Overhead: 117459

Data: 352377
Acknowledgements: 117459
Channels 10
Intervals 11745.9

Fig 5: Existing Solution Technique on DoS attack



Data: 180000
Bytes: 22500
Channels 10
Intervals 18000

Data: 180000
Overhead: 180000

Data: 540000
Acknowledgements: 180000
Channels 10
Intervals 18000

Fig 6: Proposed Work Technique Results

The above figure 2 shows the data volume values as well as the graph of probability of detection versus probability of false alarm. When the primary user send the signal then the probability of detection as well as the probability of false is on the normal mode. In the figure 2, the normal transmission of the signal is done so no effect on the probability of detection and false alarm is to be seen.

In the case of fig 3, when the emulated user affect the process of cognitive radio then it gains the information of primary user and behaves like the primary user. As the emulated user is receiving the information of primary user then it vanish the information of primary user. Emulated user now send that signal with zero interval and affect the secondary user. When there is an attack situation then the data will be send in zero interval. That process affect the data volume as well as probability of false alarm. In this emulated user case, it can be seen in figure 3 that the probability of false alarm is increased as compare to the normal signal transmission case.

In fig 4, After applying the existing scheme on the Primary User Emulation Attack then it eliminate the effect of emulated user and then Primary user safely does it process in the network. With the previous work done on the Primary User Emulated Attack, it can be noticed that the probability of false alarm has decreased. The previous work vanishes the effect of emulated user. It can be noticed that the probability of false alarm is less but not as much less as compare to the normal signal transmission case.

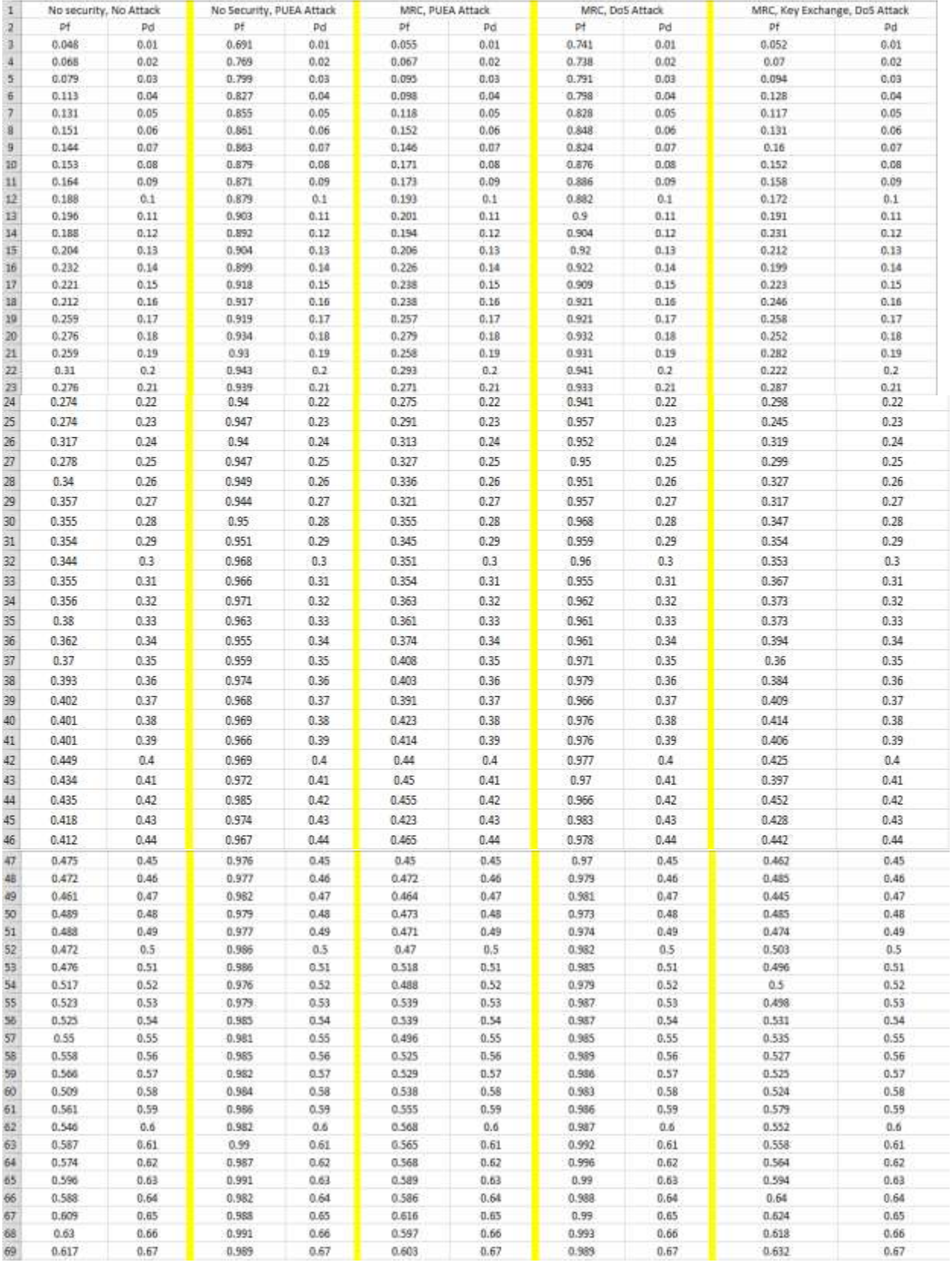
In fig 5, after applyng the previous solution on the Denial of Service attack then it can be noticed that it directly affect the data values of sender side as well as on the receiver side. The channels on the sender side are lesser and the channels sensed on the receiver side is different. The data value of the primary and the secondary user is reduced with this attack. The graph between probability of false alarm and probability of detection shows that the probability of false alarm increases in this case. This happens because it affect the data values and channels which as a result increase the probability of detecting the false user.

In fig 6, when applying the proposed solution on the Denial of Service attack then it can be noticed with the simulation result that the primary user is not affected with the attack. The data values, channels at the sender side is same as the data values, volume on the receiver side. In short the data values are same as the original values. The probabilty of false alarm versus probability of detection graph shows that with the help of this proposed work the probability of false alarm decreases if compare to the previous work and the attack situation.

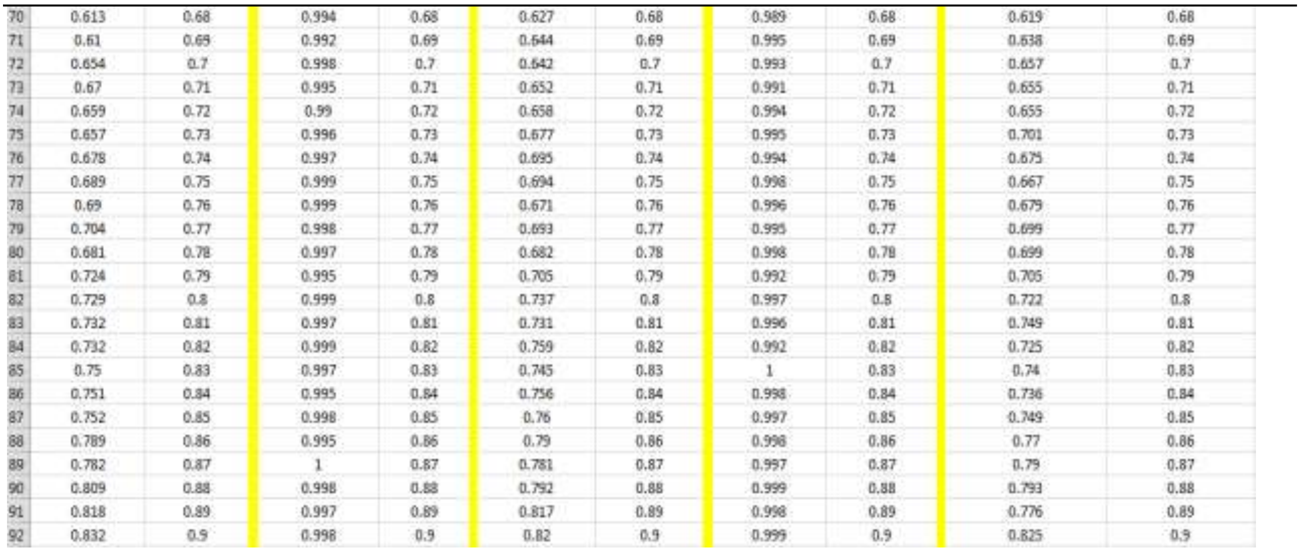
The below table 1 gives the detailed view of each value in the probability of detection and the probability of false alarm graph. With these value, it can be seen that the proposed work gives better result if compare to previous work.

The below table 1, the focused point is the probability of false alarm as the values of probability of detection kept static. It can be concluded that the proposed work gives better result in terms of data volume if compare to previous solution.

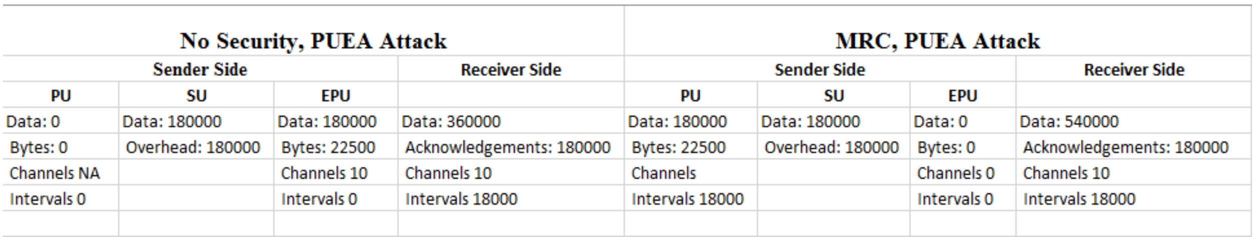
Table 1: Comparison table of Existing Technique and Proposed Technique



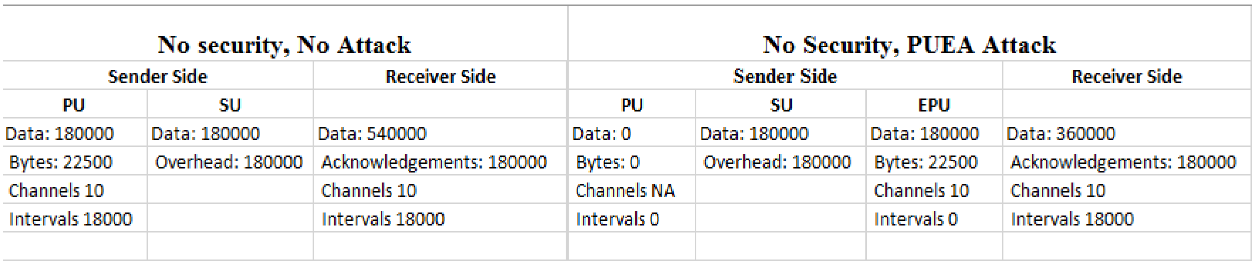
1	No security, No Attack		No Security, PUEA Attack		MRC, PUEA Attack		MRC, DoS Attack		MRC, Key Exchange, DoS Attack	
2	Pf	Pd	Pf	Pd	Pf	Pd	Pf	Pd	Pf	Pd
3	0.048	0.01	0.691	0.01	0.055	0.01	0.741	0.01	0.052	0.01
4	0.068	0.02	0.769	0.02	0.067	0.02	0.738	0.02	0.07	0.02
5	0.079	0.03	0.799	0.03	0.095	0.03	0.791	0.03	0.094	0.03
6	0.113	0.04	0.827	0.04	0.098	0.04	0.798	0.04	0.128	0.04
7	0.131	0.05	0.855	0.05	0.118	0.05	0.828	0.05	0.117	0.05
8	0.151	0.06	0.861	0.06	0.152	0.06	0.848	0.06	0.131	0.06
9	0.144	0.07	0.863	0.07	0.146	0.07	0.824	0.07	0.16	0.07
10	0.153	0.08	0.879	0.08	0.171	0.08	0.876	0.08	0.152	0.08
11	0.164	0.09	0.871	0.09	0.173	0.09	0.886	0.09	0.158	0.09
12	0.188	0.1	0.879	0.1	0.193	0.1	0.882	0.1	0.172	0.1
13	0.196	0.11	0.903	0.11	0.201	0.11	0.9	0.11	0.191	0.11
14	0.188	0.12	0.892	0.12	0.194	0.12	0.904	0.12	0.231	0.12
15	0.204	0.13	0.904	0.13	0.206	0.13	0.92	0.13	0.212	0.13
16	0.232	0.14	0.899	0.14	0.226	0.14	0.922	0.14	0.199	0.14
17	0.221	0.15	0.918	0.15	0.238	0.15	0.909	0.15	0.223	0.15
18	0.212	0.16	0.917	0.16	0.238	0.16	0.921	0.16	0.246	0.16
19	0.259	0.17	0.919	0.17	0.257	0.17	0.921	0.17	0.258	0.17
20	0.276	0.18	0.934	0.18	0.279	0.18	0.932	0.18	0.252	0.18
21	0.259	0.19	0.93	0.19	0.258	0.19	0.931	0.19	0.282	0.19
22	0.31	0.2	0.943	0.2	0.293	0.2	0.941	0.2	0.222	0.2
23	0.276	0.21	0.939	0.21	0.271	0.21	0.933	0.21	0.287	0.21
24	0.274	0.22	0.94	0.22	0.275	0.22	0.941	0.22	0.298	0.22
25	0.274	0.23	0.947	0.23	0.291	0.23	0.957	0.23	0.245	0.23
26	0.317	0.24	0.94	0.24	0.313	0.24	0.952	0.24	0.319	0.24
27	0.278	0.25	0.947	0.25	0.327	0.25	0.95	0.25	0.299	0.25
28	0.34	0.26	0.949	0.26	0.336	0.26	0.951	0.26	0.327	0.26
29	0.357	0.27	0.944	0.27	0.321	0.27	0.957	0.27	0.317	0.27
30	0.355	0.28	0.95	0.28	0.355	0.28	0.968	0.28	0.347	0.28
31	0.354	0.29	0.951	0.29	0.345	0.29	0.959	0.29	0.354	0.29
32	0.344	0.3	0.968	0.3	0.351	0.3	0.96	0.3	0.353	0.3
33	0.355	0.31	0.966	0.31	0.354	0.31	0.955	0.31	0.367	0.31
34	0.356	0.32	0.971	0.32	0.363	0.32	0.962	0.32	0.373	0.32
35	0.38	0.33	0.963	0.33	0.361	0.33	0.961	0.33	0.373	0.33
36	0.362	0.34	0.955	0.34	0.374	0.34	0.961	0.34	0.394	0.34
37	0.37	0.35	0.959	0.35	0.408	0.35	0.971	0.35	0.36	0.35
38	0.393	0.36	0.974	0.36	0.403	0.36	0.979	0.36	0.384	0.36
39	0.402	0.37	0.968	0.37	0.391	0.37	0.966	0.37	0.409	0.37
40	0.401	0.38	0.969	0.38	0.423	0.38	0.976	0.38	0.414	0.38
41	0.401	0.39	0.966	0.39	0.414	0.39	0.976	0.39	0.406	0.39
42	0.449	0.4	0.969	0.4	0.44	0.4	0.977	0.4	0.425	0.4
43	0.434	0.41	0.972	0.41	0.45	0.41	0.97	0.41	0.397	0.41
44	0.435	0.42	0.985	0.42	0.455	0.42	0.966	0.42	0.452	0.42
45	0.418	0.43	0.974	0.43	0.423	0.43	0.983	0.43	0.428	0.43
46	0.412	0.44	0.967	0.44	0.465	0.44	0.978	0.44	0.442	0.44
47	0.475	0.45	0.976	0.45	0.45	0.45	0.97	0.45	0.462	0.45
48	0.472	0.46	0.977	0.46	0.472	0.46	0.979	0.46	0.485	0.46
49	0.461	0.47	0.982	0.47	0.464	0.47	0.981	0.47	0.445	0.47
50	0.489	0.48	0.979	0.48	0.473	0.48	0.973	0.48	0.485	0.48
51	0.488	0.49	0.977	0.49	0.471	0.49	0.974	0.49	0.474	0.49
52	0.472	0.5	0.986	0.5	0.47	0.5	0.982	0.5	0.503	0.5
53	0.476	0.51	0.986	0.51	0.518	0.51	0.985	0.51	0.496	0.51
54	0.517	0.52	0.976	0.52	0.488	0.52	0.979	0.52	0.5	0.52
55	0.523	0.53	0.979	0.53	0.539	0.53	0.987	0.53	0.498	0.53
56	0.525	0.54	0.985	0.54	0.539	0.54	0.987	0.54	0.531	0.54
57	0.55	0.55	0.981	0.55	0.496	0.55	0.985	0.55	0.535	0.55
58	0.558	0.56	0.985	0.56	0.525	0.56	0.989	0.56	0.527	0.56
59	0.566	0.57	0.982	0.57	0.529	0.57	0.986	0.57	0.525	0.57
60	0.509	0.58	0.984	0.58	0.538	0.58	0.983	0.58	0.524	0.58
61	0.561	0.59	0.986	0.59	0.555	0.59	0.986	0.59	0.579	0.59
62	0.546	0.6	0.982	0.6	0.568	0.6	0.987	0.6	0.552	0.6
63	0.587	0.61	0.99	0.61	0.565	0.61	0.992	0.61	0.558	0.61
64	0.574	0.62	0.987	0.62	0.568	0.62	0.996	0.62	0.564	0.62
65	0.596	0.63	0.991	0.63	0.589	0.63	0.99	0.63	0.594	0.63
66	0.588	0.64	0.982	0.64	0.586	0.64	0.988	0.64	0.64	0.64
67	0.609	0.65	0.988	0.65	0.616	0.65	0.99	0.65	0.624	0.65
68	0.63	0.66	0.991	0.66	0.597	0.66	0.993	0.66	0.618	0.66
69	0.617	0.67	0.989	0.67	0.603	0.67	0.989	0.67	0.632	0.67



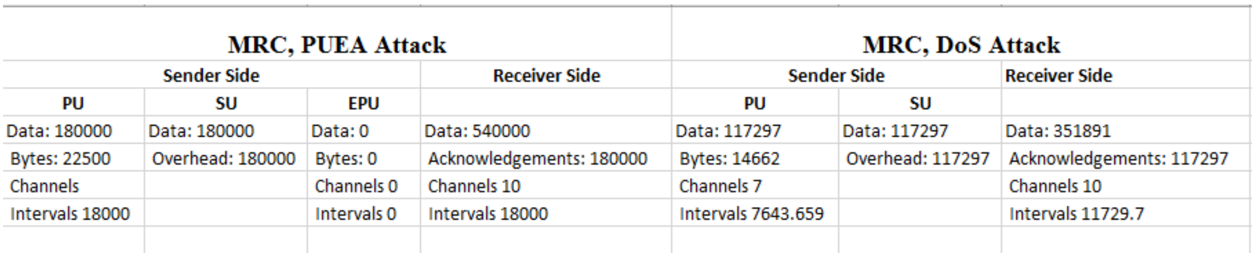
70	0.613	0.68	0.994	0.68	0.627	0.68	0.989	0.68	0.619	0.68
71	0.61	0.69	0.992	0.69	0.644	0.69	0.995	0.69	0.638	0.69
72	0.654	0.7	0.998	0.7	0.642	0.7	0.993	0.7	0.657	0.7
73	0.67	0.71	0.995	0.71	0.652	0.71	0.991	0.71	0.655	0.71
74	0.659	0.72	0.99	0.72	0.658	0.72	0.994	0.72	0.655	0.72
75	0.657	0.73	0.996	0.73	0.677	0.73	0.995	0.73	0.701	0.73
76	0.678	0.74	0.997	0.74	0.695	0.74	0.994	0.74	0.675	0.74
77	0.689	0.75	0.999	0.75	0.694	0.75	0.998	0.75	0.667	0.75
78	0.69	0.76	0.999	0.76	0.671	0.76	0.996	0.76	0.679	0.76
79	0.704	0.77	0.998	0.77	0.693	0.77	0.995	0.77	0.699	0.77
80	0.681	0.78	0.997	0.78	0.682	0.78	0.998	0.78	0.699	0.78
81	0.724	0.79	0.995	0.79	0.705	0.79	0.992	0.79	0.705	0.79
82	0.729	0.8	0.999	0.8	0.737	0.8	0.997	0.8	0.722	0.8
83	0.732	0.81	0.997	0.81	0.731	0.81	0.996	0.81	0.749	0.81
84	0.732	0.82	0.999	0.82	0.759	0.82	0.992	0.82	0.725	0.82
85	0.75	0.83	0.997	0.83	0.745	0.83	1	0.83	0.74	0.83
86	0.751	0.84	0.995	0.84	0.756	0.84	0.998	0.84	0.736	0.84
87	0.752	0.85	0.998	0.85	0.76	0.85	0.997	0.85	0.749	0.85
88	0.789	0.86	0.995	0.86	0.79	0.86	0.998	0.86	0.77	0.86
89	0.782	0.87	1	0.87	0.781	0.87	0.997	0.87	0.79	0.87
90	0.809	0.88	0.998	0.88	0.792	0.88	0.999	0.88	0.793	0.88
91	0.818	0.89	0.997	0.89	0.817	0.89	0.998	0.89	0.776	0.89
92	0.832	0.9	0.998	0.9	0.82	0.9	0.999	0.9	0.825	0.9



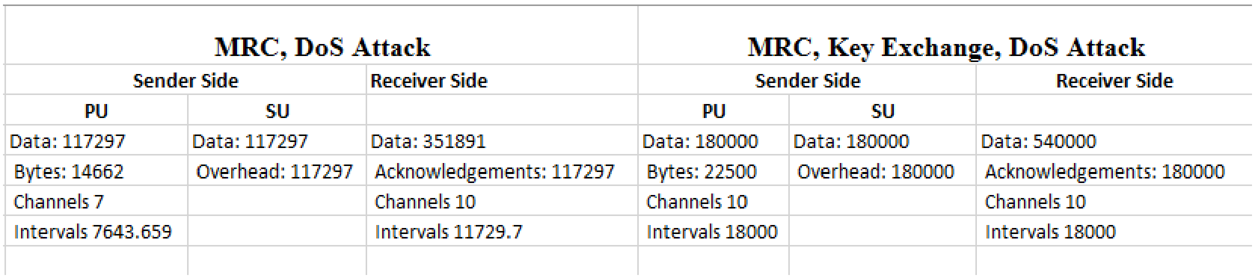
No Security, PUEA Attack				MRC, PUEA Attack			
Sender Side			Receiver Side	Sender Side			Receiver Side
PU	SU	EPU		PU	SU	EPU	
Data: 0	Data: 180000	Data: 180000	Data: 360000	Data: 180000	Data: 180000	Data: 0	Data: 540000
Bytes: 0	Overhead: 180000	Bytes: 22500	Acknowledgements: 180000	Bytes: 22500	Overhead: 180000	Bytes: 0	Acknowledgements: 180000
Channels NA		Channels 10	Channels 10	Channels		Channels 0	Channels 10
Intervals 0		Intervals 0	Intervals 18000	Intervals 18000		Intervals 0	Intervals 18000



No security, No Attack			No Security, PUEA Attack			
Sender Side		Receiver Side	Sender Side			Receiver Side
PU	SU		PU	SU	EPU	
Data: 180000	Data: 180000	Data: 540000	Data: 0	Data: 180000	Data: 180000	Data: 360000
Bytes: 22500	Overhead: 180000	Acknowledgements: 180000	Bytes: 0	Overhead: 180000	Bytes: 22500	Acknowledgements: 180000
Channels 10		Channels 10	Channels NA		Channels 10	Channels 10
Intervals 18000		Intervals 18000	Intervals 0		Intervals 0	Intervals 18000



MRC, PUEA Attack				MRC, DoS Attack		
Sender Side			Receiver Side	Sender Side		Receiver Side
PU	SU	EPU		PU	SU	
Data: 180000	Data: 180000	Data: 0	Data: 540000	Data: 117297	Data: 117297	Data: 351891
Bytes: 22500	Overhead: 180000	Bytes: 0	Acknowledgements: 180000	Bytes: 14662	Overhead: 117297	Acknowledgements: 117297
Channels		Channels 0	Channels 10	Channels 7		Channels 10
Intervals 18000		Intervals 0	Intervals 18000	Intervals 7643.659		Intervals 11729.7



MRC, DoS Attack			MRC, Key Exchange, DoS Attack		
Sender Side		Receiver Side	Sender Side		Receiver Side
PU	SU		PU	SU	
Data: 117297	Data: 117297	Data: 351891	Data: 180000	Data: 180000	Data: 540000
Bytes: 14662	Overhead: 117297	Acknowledgements: 117297	Bytes: 22500	Overhead: 180000	Acknowledgements: 180000
Channels 7		Channels 10	Channels 10		Channels 10
Intervals 7643.659		Intervals 11729.7	Intervals 18000		Intervals 18000

5. Conclusion and future scope

The cognitive radio carriers are intelligent end-to-end radio connections, which deliver data efficiently in comparison with the ordinary wireless connections. The cognitive radio channels can overcome the channel noise, but does not protect the data against denial of service attacks. The denial of service attacks are launched on the cognitive radio by flooding the packets on the available frequency in order to make the channel resources unavailable to the other data connections. Such attacks can be prevented by controlling the data communication between the sender and receiver. The proposed system is proposing the key exchange policy between the secondary user and primary users. The scenario is based upon the secondary user role as the spectrum sensing agent whereas the primary user is intended to send the data to the other end. The communication between the secondary and primary user has been protected using the novel lightweight key exchange scheme in order to protect against the denial of service attacks. For the attack prevention, the proposed model ensures the connection with the legitimate users only and does not permit to receive the data from the unauthorized users, which directly affects the cognitive radio security and does not allow any flooding attack over the secure channel. The proposed model performance has been measured using the Probability of detection and Probability of false alarm. The proposed model has been performed during the denial of service attack, which shows the effectiveness of the proposed model.

In the future, the proposed model can be enhanced to secure the end-to-end channel between the cognitive radio ends. Also, the proposed model can be enhanced with robust data encryption along with the key exchange scheme for the hardened security of the cognitive radio channel.

Acknowledgment

I would like to thank my co-author Dr. Inderdeep Kaur Aulakh for providing me with her valuable guidance in this field. Her continuous and valuable support has been of great help in completing the research work.

References

[1] Aulakh I. K., & Vig R. (2014, March). Optimization of secondary user access in cognitive radio networks. In Engineering and Computational Sciences (RAECS), 2014 Recent Advances in (pp. 1-6). IEEE.

[2] Aulakh I. K., & Vig R. (2014, March). Optimization of SU's probability of false alarm for dynamic spectrum access in cognitive radio. In Computing for Sustainable Global Development (INDIACom), 2014 International Conference on (pp. 710-715). IEEE.

[3] Gregori M, Nogueira M, Queiroz S & Soto J (2013, June). A flexible multi-criteria scheme to detect primary user emulation attacks in CRAHNs. In World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a (pp. 1-6). IEEE.

[4] Dang M., Zhao Z, & Zhang H. (2013, October). Detection of primary user emulation attacks based on compressive sensing in cognitive radio networks. In Wireless Communications & Signal Processing (WCSP), 2013 International Conference on (pp. 1-5). IEEE.

[5] Bagheri A, Shahini A, Shahzadi, A, & Tabatabaee S. (2013, December). An analytical model for primary user emulation attacks in IEEE 802.22 networks. In Connected Vehicles and Expo (ICCVE), 2013 International Conference on (pp. 693-698). IEEE.

[6] Chen Y, Dong X, Peng T, Shi W & Yang J. (2014, July). Cooperative spectrum sensing against attacks in cognitive radio networks. In Information and Automation (ICIA), 2014 IEEE International Conference on (pp. 71-75). IEEE.

[7] Saber M. J, & Sadough S. M. S. (2014, May). Robust cooperative spectrum sensing in cognitive radio networks under multiple smart primary user emulation attacks. In Electrical Engineering (ICEE), 2014 22nd Iranian Conference on (pp. 1745-1748). IEEE.

[8] Abdelhakim M, Alahmadi A, Li T & Ren J. Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard. InGlobal Communications Conference (GLOBECOM), 2013 IEEE 2013 Dec 9 (pp. 3229-3234). IEEE.

[9] Anand S, Jin Z & Subbalakshmi KP. Detecting primary user emulation attacks in dynamic spectrum access networks. InCommunications, 2009. ICC'09. IEEE International Conference on 2009 Jun 14 (pp. 1-5). IEEE.

[10] Hao D & Sakurai K. A differential game approach to mitigating primary user emulation attacks in cognitive radio networks. InAdvanced Information Networking and Applications (AINA), 2012 IEEE 26th International Conference on 2012 Mar 26 (pp. 495-502). IEEE.

[11] Wang W & Xie X. Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding. Procedia Computer Science. 2013 Jan 1;21:430-5.

[12] Li H, Qian L & Sorrells C. Quickest detection of denial-of-service attacks in cognitive wireless networks. InHomeland Security (HST), 2012 IEEE Conference on Technologies for 2012 Nov 13 (pp. 580-584). IEEE.

[13] Weifang W. Denial of service attacks in cognitive radio networks. In Environmental Science and Information Application Technology (ESIAT), 2010 International Conference on 2010 Jul 17 (Vol. 2, pp. 530-533). IEEE.

[14] Attar A, Bilén SG, Leung VC & Sodagari S. Denial of service attacks in cognitive radio networks through channel eviction triggering. InGlobal

Telecommunications Conference (GLOBECOM 2010), 2010 IEEE 2010 Dec 6 (pp. 1-5). IEEE.

[15] Chen C, Cheng H & Yao YD. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack. IEEE Transactions on Wireless Communications. 2011 Jul;10(7):2135-41.

[16] Sengupta S, Subbalakshmi KP & Tan Y. Analysis of coordinated denial-of-service attacks in IEEE 802.22 networks. IEEE Journal on Selected Areas in Communications. 2011 Apr 1;29(4):890-902.

[17] Chatterjee PS & Chatterjee S. A comparison based clustering algorithm to counter SSDF attack in CWSN. InComputational Intelligence and Networks (CINE), 2015 International Conference on 2015 Jan 12 (pp. 194-195). IEEE.

[18] Nene MJ & Yadav S. RSS based detection and expulsion of malicious users from cooperative sensing in cognitive radios. InAdvance Computing Conference (IACC), 2013 IEEE 3rd International 2013 Feb 22 (pp. 181-184). IEEE.

[19] Bhunia S, Sengupta S & Vázquez-Abad F. Cr-honeynet: A learning & decoy based sustenance mechanism against jamming attack in crn. InMilitary Communications Conference (MILCOM), 2014 IEEE 2014 Oct 6 (pp. 1173-1180). IEEE.

[20] Anand S, Jin Z & Subbalakshmi KP. Impact of primary user emulation attacks on dynamic spectrum access networks. IEEE Transactions on Communications. 2012 Sep;60(9):2635-43.