International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

A Novel Authentication Mechanism for Cognitive Radio Network

B.Sarala, S.Rukmani Devi, M.Suganthy, S.Jhansi Ida

Abstract—By employing an efficient authentication protocol the security of the Cognitive radio Network can be upgraded. This paper portrays a strategy for recognizing the Primary client Emulation Attacks in a CRN using cross layer approach. A few kinds of attacks have been discussed in this paper and an authentication scheme to detect PUEA has been presented. It is identified that the physical layer authentication method can serve as a faster authentication method but with low accuracy in detection.And a cryptography based authentication protocol can serve as a slower authentication method but with high accuracy in detection. In this paper a cross layer confirmation plot that joins both the physical and higher layer authentication is defined. The proposed method can provide good accuracy in detection without sacrificing the speed of the detection.A detecting procedure to detect PUEA in a CRN for a single user has been defined in this paper.

Index Terms—Cognitive Radio Network, authentication, Cross layer authentication

I. INTRODUCTION

COGNITIVE radio is a promising radio technology that is capable of learning from its environment and change its transmission parameters to increase spectrum efficiency. Cognitive radio accommodates more number of users in a given spectrum without sacrificing the speed of communication. Since CR is adaptive to their environment, the secure means of communication is essential. There comes the point of authentication. CR allows primarywhat's more, optional clients to utilize the range successfully. The essential clients are licensed users and they have given the higher priority always than the secondary users. This structure of cognitive radio gives rise to Primary User Emulation Attack. A PUEA is described as follows: A selfish secondary user may emulate its radio parameters like a primary user so as to use the spectrum illegally. PUEA attack reduces the efficiency and effectiveness of the network.

Several researches have been going on in reducing the security threats in a CRN.Most of them are intended towards adding securityin the physical layer [2] or at any higher layer[1] using cryptographic techniques. But due to the tradeoff between the speed and accuracy in detecting PUEA those security methods finds difficulty in serving the purpose.

Hence a cross layer mechanism will be a suitable one to be used in Cognitive radio network.

This paper is composed as pursues. Area II features a couple of sorts of assaults in intellectual radio condition. Section III discusses physical layer authentication method. Section IV deals with higher layer authentication methods.

Segment V portrays the proposed recognizing plan. At long last, Section VI shows the ends.

II. LITERATURE SURVEY

In [15],due of the adaptability of psychological radio networks, they are defenseless for various dangers and security issues that will influence the execution of the system. Little consideration was given to security angles in subjective radio systems that incorporate range sensing(sensing essential client), assaults that debilitate the system at different layers and foe consequences for execution because of the security dangers. In this overview, it talk about the intellectual radio networks, problem associated with detecting and management, attacks on psychological radio networks, attacks on different system layer, dangers on subjective radio systems and the present security and protection arrangements.

In [16], a far reaching rundown of major known security dangers inside a psychological radio network (CRN) system have been presented. Attack strategies have been grouped dependent on the sort of assailants, in particular exogenous (external) aggressors, meddling malignant hubs and ravenous intellectual radios(CRs). This paper additionally talk about dangers identified with foundation – based CRNs and in addition framework less systems, Besides the transient impacts of assaults over CRN execution likewise examined about the disregarded longer term conduct changes that are implemented by such assaults by means of the learning capacity of CRN.

In [17], the channel – tap control is used as a radio – recurrence fingerprint (RF) to totally recognize essential client copying attacks(PUEAs) over the multipath Rayleigh blurring channels. To precisely know personalities of essential users(PUs) and PUEAs, the cross – layer astute learning capacity of a versatile auxiliary client (SU) is abused to build up location database via flawlessly consolidating the snappy recognition of physical (PHY) layer with the exactness of higher layer confirmation.

Manuscript published on November 30, 2019.
* Correspondence Author
B.Sarala*, Assistant Professor, Dept. of ECE R.M.K. Engineering College, Kavaraipettai.
S.Rukumani Devi, Professor, Dept. of ECE R.M.D. Engineering College, Kavaraipettai.
M.Suganthy, Associate Professor, Dept. of ECE Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi
S.Jhansi Ida, Assistant Professor, Dept. of IT, R.M.K. Engineering College, Kavaraipettai.

The proposed strategy enable PHY to layer totally recognize the personalities of PU's and PUEAs. For SNR= -2DB and the false caution likelihood of 0.1, the SU can distinguish a PUEA with the identification likelihood of 0.9673 under the portable speed of 70 km/h.

In[18],an endeavor is made to portray a propelled essential imitating assault and a propelled countermeasure against such an assault. In particular, that both the assailants and protector can apply estimation systems and learning techniques to get the key data of nature and consequently configuration better procedures.

In [19],a novel methodology for validating essential clients motion in CRNs, which fits in with FCC prerequisite, has been created. This methodology incorporates cryptographic signature and remote connection signature (got from physical radio channel attributes) to empower essential client identification in nearness of assailants

III. VRIOUS ATTACKS IN COGNITIVE RADIO NETWORK

A.Physical layer attacks

Physical layer attacks involve altering the transmission radio parameters so as to attain higher priority than the secondary users to use the spectrum. One of the important physical layer attacks is the PUEA [7]. A malicious secondary will emulate itself like a primary user so as to achieve sufficient priority to use the network infrastructure[12-13].The other major attack in physical layer is th Essential client copying assault in a CRN can be characterized into following two sub-classifications. (i)Policy radios, (ii) Learning radios. The impact of the assault vanishes when the aggressor leaves the divert in the previous one. Also, the impact goes on for quite a while in the later one.

Objective function attack. To explain the objective function attack let's consider the following objective function of a cognitive radio network.

$$F = W_1R+W_2S. \qquad (1)$$

Where R is the transmission rate, S is the security level and $W_1$and $W_2$are the weight functions. If a user of the CRN selects a high security level, then the malicious user will try to jam that particular user, thereby reducing its objective function. Thus the victim user is compelled to reduce the security level so as to make the objective function normal. Then the malicious user can easily hack the communication from that user. Eavesdropping is the next major attack in physical layer. In this attack the less secured data in a wireless medium is modified by the attacker. So the information received on the other end is not the original content sent by the source. To avoid this attack any higher layer cryptography based security can be incorporated in the communication protocol.In Cognitive radio systems, numerous optional systems may exist in the meantime over a similar locale. The transmissions from malignant elements in a single system can make impedance the essential and optional clients of the other system. Since the malignant clients or aggressors may not be under the immediate supervision of the auxiliary base station of the injured individual system, this sort of assault is extremely hard to forestall.

In a decentralized intellectual system, auxiliary client may settle on wrong choice because of false criticism from one malignant optional client. This thusly will make extreme impedance the authorized client. For a model, a pernicious hub in the system may not tell the other optional clients in the system about the return of the authorized client, who can't detect the data because of blurring or long separation. Such an assault is called as false criticism assault.

In DOS assault, the primary target of malignant hub is to keep great auxiliary hubs from getting to the empty radio recurrence band. An assailant may endeavor to stick a system and consequently diminish a genuine client's data transfer capacity, anticipate access to an administration, or upset support of a particular framework or a client.

A. *Higher layer attacks*

The attacks that can happen other than physical layer are said to be higher layer attacks. Range detecting information misrepresentation is one of the significant assaults in CRN. It happens when an assailant sends a false range detecting report to its neighbors or to the information combination focus. This assault can influence both the Centralized and disseminated CRNs. In a brought together CRN in the event that it is influenced, then a user may be denied from using the service or a user may be permitted to use the spectrum that has been already occupied by any other user. In distributed CRN the problem becomes more complex.Since, there is no way to stop the error propagation

In the hole attack the hub which imagines is known as an hole. There are different kinds of opening assaults, for example, Black gap assault, Gray gap assault, Worm gap assault. Dark opening assault is characterized as assault in which the malevolent hub pulls in/ask for parcels from each other hub and drops every one of the bundles. The dim opening assault is characterized as the assault in which the noxious hub specifically drops the bundles. The worm gap assault is characterized as the assault in which the malignant client utilizes two sets of hubs and there exist a private association between the two sets. The worm opening assault is a considered as hazardous assault among all. It can forestall course disclosure where the source and the goal are in excess of two jumps away. Conventions like Ariadne or secure AODV avoids such kinds of assaults.

Sessions in cognitive networks systems last just for a brief timeframe because of much of the time happening retransmissions. In this manner, extensive quantities of sessions are being started. Security conventions at the vehicle layer like SSL and TLS set up cryptographic key sat the start of each transport layer sessio Since quantities of sessions in psychological systems are substantial, vast quantities of keys are built up, in this manner expanding the likelihood of utilizing a similar key twice. Key reiterations can be misused to break the basic figure framework. The WEP and TKIP conventions utilized in IEEE 802.11 are more inclined to key reiteration assaults.

Application layer is the best most layer of the convention stack. It gives application administrations to the end clients. Conventions that keep running at the application layer totally depend on the administrations given by the hidden lower layers. Subsequently, any assault on physical, connection, system or transport layers mayadversy affect the application layer.

Even though different kinds of malicious attacks presents, in this work Primary user emulation attack [10] is taken as a major problem and a cross layer solution to detect PUEA is presented.

IV. PHYSICAL LAYER AUTHENTICATION METHOD

Physical layer validation includes dissecting the physical properties of the flag to separate the essential client imitating assault from the first Primary User. In work [3] the creators built up a propelled essential client copying assaultand proved that such an attack can break the conventional naïve detection method of physical layer authentication. And they suggested using the invariant of the communication channel to estimate channel parameters. This method effectively counteracts the PUEA. Analyzing the physical layer properties can be broadly classified into two categories. (i) Utilizing transmission specific characteristics and (ii) Using channel-specific features.

In work [4], the creators utilized remote connection marks got from the channel properties to recognize the lawful essential clients. In any case, this strategy makes utilization of an aide hub as a crossing over component between the essential client and the optional client.

Other physical layer validation strategy incorporates vitality identification and highlight recognition strategies. In vitality recognition strategy the vitality of the caught flag is figured. And if the energy level is beyond the threshold it is said to be the primary user or else it is the secondary user. This kind of testing is called hypothesis test.

$$D = \begin{cases} PUEA & H < H_t \\ PU & H > H_t \end{cases} \qquad (2)$$

Equation (2) represents the hypothesis test mathematically. Where in (2) D denotes the decision and H stands for measured channel property and H_t stands for threshold voltage for the corresponding channel property.

The effectiveness of the hypothesis test is analyzed based on the false probability and false alarm as follows.

Suppose H0 – Signal from the essential client and H1 – Signal from the PUEA. The likelihood of the false alert (PFA) is the injured individual observes a flag to be a PUEA, yet initially the flag is being transmitted from an essential client.

$$P_{FA} = Pr\,(H_1 \mid H_0) \qquad (3)$$

Furthermore, the likelihood of misdetection is named as the likelihood the victim classifies a signal as a primary user but originally the signal is being transmitted from a PUEA. It is given by the equation (4).

$$P_{MD} = Pr\,(H_0 \mid H_1) \qquad (4)$$

In the above scenario the PUEA will run in the network to increase this probability whereas the aim of the secondary user is to reduce these probabilities. From the above analysis it is clear that the physical layer detection schemes cannot produce accurate results. There are possibilities for miss detection is high in most of the cases. So higher layer authentication schemes are used in wireless networks.

V. HIGHER LAYER AUTHENTICATION METHOD

BeforeThis section presents an overview of the higher layer authentication mechanism used in cognitive radio networksHigher layer authentication schemes use cryptographic techniques which are proven to be a fool proof technique in authentication.Inthe work [5-6], the authors proposed a public key based encryption scheme to distinguish between primary users and malicious PUEA.

A. *Public Key Cryptography*

Public key cryptography relies on encryption using a key and decryption using a different but related key. It is best illustrated using the following relations.

$$X = D_{KU}[E_{KR}[X]] \qquad (5)$$

$$X = D_{KR}[E_{KU}[X]] \qquad (6)$$

In the above equation X represents the message D and E represents the decryption and encryption respectively. Ku is the public key and KR is he private key.Usingthese public key ciphers the transmitted message can be signed by the transmitter using its private key. The beneficiary can confirm the honesty of the substance by utilizing general society key of the planned transmitter. By along these lines the general population key figures are utilized as computerized marks.

B. *Procedure for transmitting a signal*

The essential client creates a couple of open and private keys by a concentrated key age calculation. At that point people in general key is imparted to every one of the clients of the CRN.The transmitted signal is then encrypted by the transmitter using its private key. Since the transmitter is the only one who knows its private key, the data cannot be signed by any malicious users.

C. *Procedure for receiving a signal*

A receiver should receive the public keys from the central facility. And using that public key appropriate transmitter's signal can be decrypted and verified. Since the transmitter just realizes its private key it is unthinkable for an aggressor to sign the substance of the essential transmitter.

This is the way of using the higher layer protocols to detect the malicious users. But it takes more time for encryption and decryption usually. And a centralized architecture is required to establish communication between the users to share the public keys.

Thus the accuracy of detecting the malicious users is very high whereas the speed of detection is very low. So employing either method leads to a disadvantage. And so a cross layer approach will be a good solution to solve this problem.

VI. CROSS LAYER AUTHENTICATION METHOD

The Fig. 1 shows the sensing procedure for a CRN node to differentiate the primary user and PUEA.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

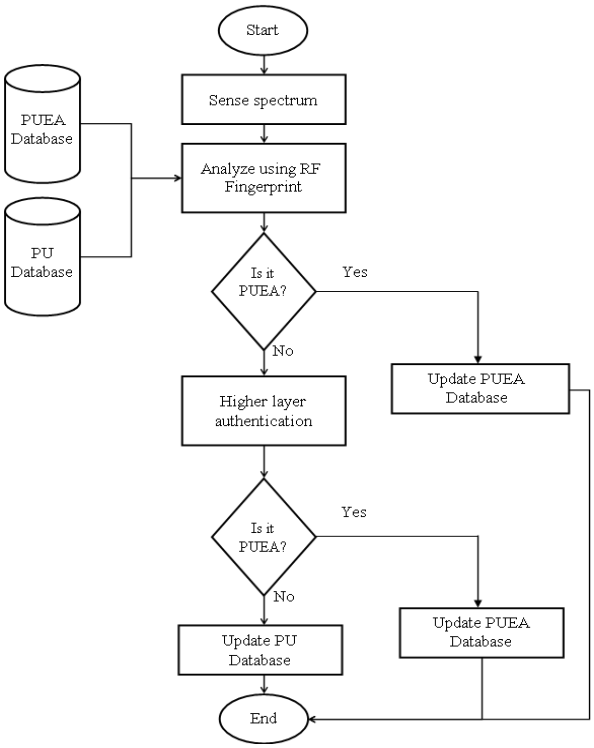

Fig. 1 Proposed Sensing procedure for a CRN

In this method, the secondary user first starts analyzing the radio frequency fingerprints of the transmitter such as channel tap power[11]. Then by conducting a simple hypothesis test the secondary user will be able to identify the transmitter. It is pre-requested that the secondary user is already having the PU and PUEA database to conduct hypothesis test [9]. Even after hypothesis test is done.on the off chance that the optional client can't distinguish the PUEA then it go for higher layer validation. In the higher layer confirmation it is anything but difficult to recognize the essential client and the PUEA. Since the optional client is given the PU and PUEA database, in light of the trustworthiness the transmitter can be characterized into any of the classifications.

Once the detection procedure is finished the PU and PUEA database is updated. So that in future the same RF properties need not be analyzed using the higher layer authentication. Thus the proposed method saves time in a long term usage without sacrificing the accuracy in detection.Once all the PUEA are identified by the secondary user and based on the strength of the created database the time for detecting the PU and PUEA becomes very less making this algorithm suitable for cognitive radio network.

VII. SIMULATION OF PROPOSED METHOD

To achieve the required detection accuracy with reduced detection time, a time optimized encryption algorithm is needed. In [14],the authors proposed an encryption algorithm called Simeck, which is used throughout this paper. The Simeck algorithm is chosen over the other advanced encryption algorithms such as AES and DES.

The encryption cost of Simeck calculation is appeared in Fig. 2. The time required by the calculation to figure the figure content for a given plain content is assigned as encryption cost.

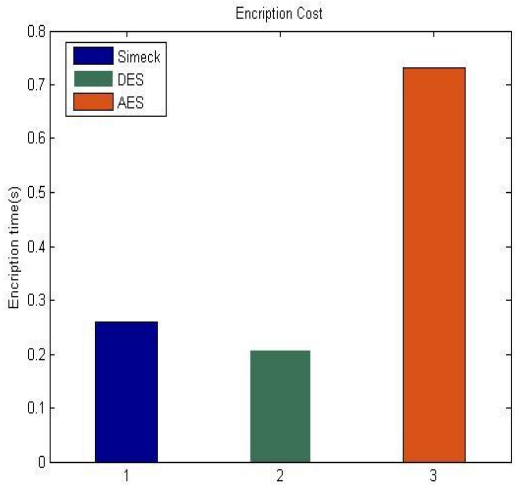

Fig. 2 Encryption Cost

The Simeck algorithm outperforms the other advanced encryption schemes. And also it provides an added advantage that it is easy to implement in the hardware.Even though the DES algorithm has a lesser encryption cost than the Simeck the complexity in implementation of the *Switch boxes* and *Permutation boxes* makes it unsuitable for CR. So Simeck algorithm is used in this work.

A. *Specifications of Simeck Algorithm*

Lightweight square figure family Simeck is signified Simeck2n/mn, where n is the word size and n is required to be 16, 24 or 32; while 2n is the square size and mn is the key size. All the more particularly, Simeck family incorporates Simeck32/64, Simeck48/96, and Simeck64/128. For instance, Simeck32/64 alludes to perform encryptions or decodings on 32-bit message squares utilizing a 64-bit key. These three size decisions of the figures expect to fit distinctive uses of installed frameworks including RFID frameworks, and these sizes are likewise contained in the details of Simon and Speck groups of square figures. Simeck is intended to be amazingly little in equipment impressions and to be reduced in programming executions also. The round capacity and the key calendar calculation pursue the Feistel structure. A plaintext to be scrambled is first isolated into two words l0 and r0, where l0 contains the most noteworthy n bits, and r0 comprises of the slightest critical n bits. At that point these two words are handled by the Simeck round capacity for certain number of rounds, lastly the two yield words li and ri are connected to shape an entire figure content, where I indicates the aggregate number of rounds

The round function of Simeck is given by the equation (7).

$$R_{ki}(l_i; r_i) = (r_i \oplus f(l_i) \oplus k_i;\ l_i) \quad \dots (7)$$

$f(l_i)$is the intermediate function. $R_{ki}(l_i; r_i)$forms the required cipher text. The scrambled figure content is then QPSK balanced. This information is then sent through the channel utilizing OFDM multiplexing system. Method for sending an information is appeared in Fig. 3.

Retrieval Number: D6499118419/2019©BEIESP
DOI:10.35940/ijrte.D6499.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

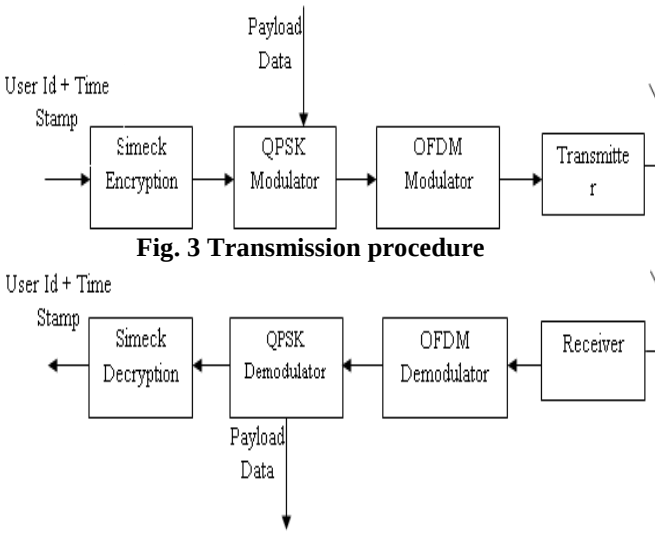

Fig. 3 Transmission procedure

Fig. 4 Receiving a data

The reverse operation is done in the receiver to recover the original data. In these simulation two symbols of data is sent through two transmitters. OFDM with 64 subcarriers are used. The null carriers and Pilot carriers are inserted to avoid Inter symbol interference. Fig. 5 shows the OFDM signal generated for a reference data.

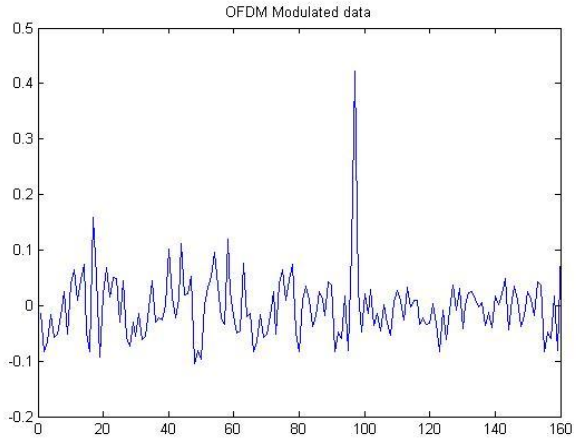

Fig. 5 OFDM signal for a reference data

For the most part the execution of the recognition plans for subjective radio advancements are estimated by beneficiary working attributes bend. i.e. by ascertaining the Probability of Detection versus Likelihood of False caution rate bend [8].

Likelihood of False caution is characterized as pursues:

1.A client is said to be a Primary User when it is really a Primary User Emulation Attack.

2.A client is said to be a Primary User Emulation Attack when it is really a Primary User.

Likelihood of False alert is characterized in the range [0 1]. What's more, concerning that the recognition capacity of the proposed plan is ascertained.

Fig. 6 demonstrates the Probability of identification as a component of Probability of false alert for a channel SNR = -4dB.

As it is normal the PD raises more than 0.9 notwithstanding for PFa= 0.

To contrast the gotten outcomes and that of work [3], both the techniques are reenacted under same conditions. The outcomes are plotted in Fig. 7

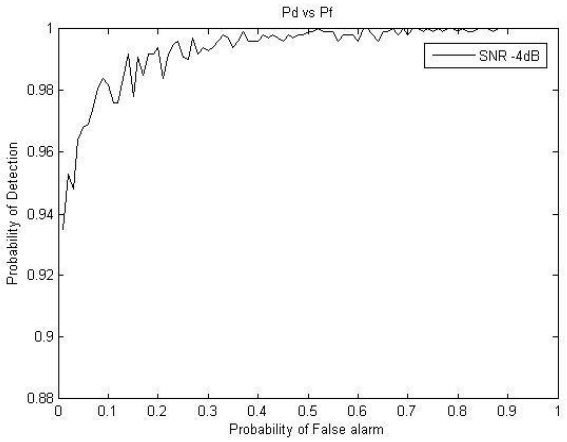

Fig. 6 $P_D$vs P_F

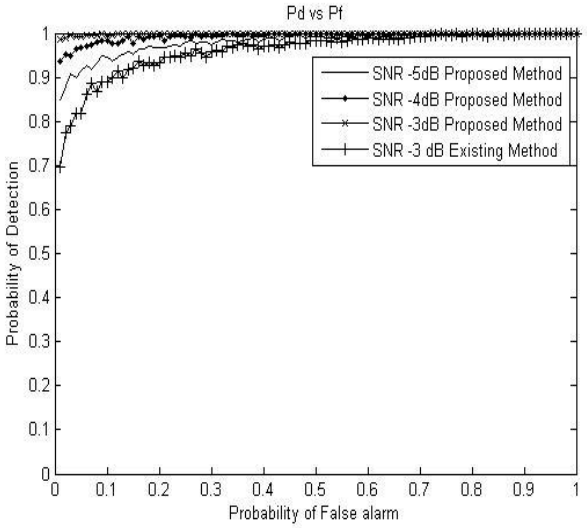

Fig. 7 comparing the proposed and existing method

To additionally demonstrate the strength of the proposed strategy the execution of the framework, the location capacity is registered at different clamor levels. The gotten outcomes are appeared in Fig. 8.

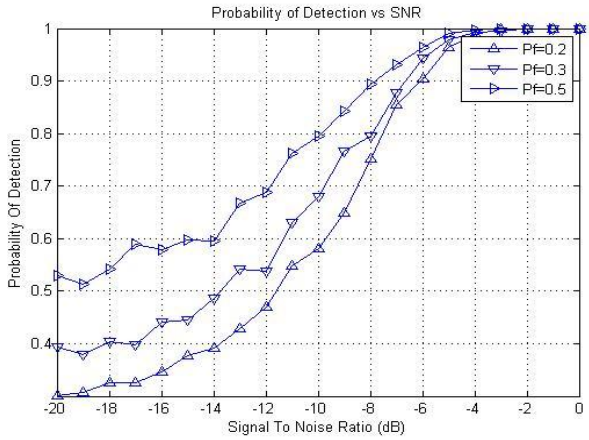

Fig. 8.$P_D$vs SNR

The obtained results prove that the system is stable over various noise levels.

VIII. CONCLUSION

In this work the different kinds of attacks in a CRN are discussed and the PUEA is taken as a challenge and a new cross layer authentication approach is proposed to seamlessly increase the security of the cognitive radio networks.From the research work it is identified that the detection time can be reduced by reducing the encryption time. So a simple as well as complex to break encryption algorithm is used in the work. More over detection time is further reduced by encrypting only the User ID and current timestamp. This reduces the detection time up to 90%. The proposed method accumulates the advantages of both the physical layer authentication and the higher layer authentication methods. And at the same time the disadvantages of both the methods are alleviated.

REFERENCES

1. C. N. Mathur and K. P. Subbalakshmi,(2007) "Digital signatures for centralized DSA networks," in Proc. 1st IEEEWorkshopCogn. Radio Netw. pp. 1037–1041.
2. H. Shokri-Ghadikolaei and R. Fallahi,(2012) "Intelligent sensing matrix setting in cognitive radio networks," IEEE Commun. Lett., vol. 16, no. 11, pp. 1824–1827.
3. TrongNghia Le, Wen-Long Chin, Wei-Che Kao, (2015), "Cross-Layer Design for Primary User Emulation Attacks Detection in Mobile Cognitive Radio Networks", IEEE Communications letters, VOL. 19, NO. 5
4. W. L. Chin et al.,(2014) "Cooperative detection of primary user emulation attacks based on channel-tap power in mobile cognitive radio networks," Int.J.Ad Hoc Ubiquitous Comput., vol. 15, no. 4, pp. 263–274.
5. Yenumula B. Reddy (2013), "Security Issues and Threats in Cognitive Radio Networks", IARIA.
6. Y. Liu, P. Ning, and H. Dai, (2010) "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in Proc. IEEE Symp. Security Privacy,pp. 286–301.
7. Z. Chen and C. Chen,(2009) "Modeling primary user emulation attacks and defenses in cognitive radio networks," in Proc. IEEE 28th Int. Perform. Comput. Commun. Conf., pp. 208–215.
8. A. Goldsmith, Wireless Communications. Cambridge, U.K.: CambridgeUniv. Press, 2005.
9. V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in 14th Annual International Conference on Mobile Computing and Networking (MobiCom'08), Sept. 2008, pp. 116-127.
10. R. Chen, J. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE Journal on Selected Areas in Communications, Special Issue on Cognitive Radio Theory and Applications, vol. 26, no. 1, Jan. 2008.
11. T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 2, April-June 2005, pp. 93-108.
12. Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in Proc. of the Fifth ACM Wireless Security Workshop (WiSe'06), Los Angeles, CA, Sept. 2006, pp. 33-42.
13. E. Peh and Y. Liang, "Optimization for cooperative sensing in cognitive radio networks," in Wireless Communications and Networking Conference, Hong Kong, Mar. 2007, pp. 27-32.
14. Gangqiang Yang, Bo Zhu, ValentinSuder, Mark D. Aagaard, and Guang Gong, "The Simeck Family of Lightweight Block Ciphers", IACR 2015.
15. YenumulaBG.Reddy," Security Issues and Threats in Cognitive Radio Networks", IARIA 2013.
16. Alireza Attar, Helen Tang, Athanasios V., Vasilakos, F. Richard Yu, Victor C.M .Leung," A Survey of Security Challenges in Cognitive Radio Networks: Solution anmd Future Research Directions", Proceedings of IEE,2012,Vol. 100, No 12.
17. TrongNghia Le, Wen-Long Chin, Wei-Che Kao, "Cross –layer design for primary user Emulation Attacks Detection in Mobile Cognitive Radio networks", IEEE communications letter,2015 Vol.19,NO.5.
18. Zesheng Chen, TodorCookley, Chao Chen and Carlos Pomalaza-Raez,"Modeling Primary User Emulation Attack and defenses in Cognitive Radio Networks,2009,PCCC.2009.5403815.
19. Yao Liu,PengNing,Huaiytu Dai," Authenticating Primary Users in Cognitive Radio Networks via integrated Cryptographic and wireless link Signature", 2010, IEEE Symposium on security and Privacy