

Hermitan matrices based malicious cognitive radio detection and bayesian method for detecting primary user emulation attack

Devasahayam Joseph Jeyakumar¹, Boominathan Shanmathi¹, Parappurathu Bahulayan Smitha¹, Sekar Vinurajkumar², Mohanan Murali¹, Muthuraj Mariselvam¹

¹Department of Electronics and Communication Engineering, J.N.N Institute of Engineering, Chennai, India

²Department of Biomedical Engineering, Veltech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India

Article Info

Article history:

Received Jun 2, 2022

Revised Dec 14, 2022

Accepted Dec 20, 2022

Keywords:

Bayesian method

Hermitan matrices method

Malicious cognitive radio detection

Primary user emulation attack

Trust analyzer

ABSTRACT

Cognitive radio (CR) is a facilitating technology to efficiently deal with the spectrum scarceness, and it will significantly enhance the spectrum deployment of upcoming wireless transmission method. Security is a significant concern, although not well tackle in cognitive radio networks (CRN). In CR networks, this approach regard as a security issue happen from primary user emulation attack (PUEA). A PUEA attacker forwards an emulated primary signal and defraud the CR users to avoid them from accessing spectrum holes. Here, we introduce a Hermitan matrices based malicious cognitive radio (CMCR) detection and Bayesian method for detecting PUEA attack in the CRN. In this approach, the Bayesian method is used for detecting the PUEA attack. The trust analyzer evaluates the CR trust. Here, the node trust value is computed by node activeness and inactiveness, degree of data transmission, and hermitan matrices verification. In addition, the Hermitan Matrices method is used to detect the malicious CR user in the CRN. The simulation outcomes propose that the CMCR leads to improve the performance in terms of better detection ratio, minimized the possibility of miss detection ratio. Furthermore, it minimized the possibility of false alarm in the CRN.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Devasahayam Joseph Jeyakumar

Department of Electronics and Communication Engineering, J.N.N Institute of Engineering
Chennai, India

Email: jayakumarjoseph33@gmail.com

1. INTRODUCTION

The rapid propagation of smart devices and the management of the spectral band in the radio communication method have result in an insufficiency of frequencies. To overcome this problem, the design of dynamic spectrum entrée during cognitive radio has become quite attractive. In cognitive radio networks (CRN), two class of spectrum users for example primary users (PUs) and the cognitive radio (CR) user [1]. In CRN, a malicious communicates signals with features which imitate PU to avoid CR users from transmitting. This type of attack is known as a primary user emulation attack (PUEA) attack. Malicious users can develop vulnerabilities in CRNs and origin heavy function degradation through denial of service attacks [2]. Throughout function, CRs expend a significant amount of time to recognize idle channels for communication. Additionally, CRs also necessitate additional security methods to avoid malicious attacks [3].

The CR technology offers the capability for wireless devices to develop the PU, CR user should empty the channel while a PU is identified. Therefore, spectrum sensing is one of the most technological challenges

in CRN to discover the spectrum holes [4]. Cooperative spectrum sensing (CSS) has been introduced to defeat the destructive effect of shadowing, multipath fading, and hidden terminal issues. In CSS, several CR users forward local sensing information for example, evaluated energy or one bit conclusion to the neighbors otherwise to the fusion center (FC). Established on the nature of the obtained information, FC selects hard combination otherwise soft combination system to decide the status of channel [5]. The cryptographic approaches may raise the transmission, storage and computation cost through frankly raising the communication delay [6].

Presently, the authenticity of the devices otherwise applications can be calculated by the trust value. The network trust is discrete as a computing parameter which computes the validity of a detailed node by its earlier or accessible communications lacking raising the cryptographic procedures. Thus, an efficient method to make sure a secure message method is a trust based procedure [7]. It improves the security lacking further raising the network delay as well as overhead. Unfortunately, trusted security methods have not been systematically recognized and are still in their untimely stages in a CRN [8]. A secure and trusted routing is used to distinguish the malicious nodes in the CRN. A trust analyser (TA) is proposed between the CR nodes. The TA handles the table of entire transmitting nodes while computing the trust value through the social impact theory optimizer [9].

This article is structured as follows: section 2 describes the related research work regarding CRN with PUEA detection. Section 3 explains the Hermitan Matrices based malicious cognitive radio detection and Bayesian method for detecting PUEA attack in the CRN. Section 4 contains simulation results of SPUEA and CMCR schemes. Finally, section 5 exist the conclusion.

A game theoretical framework is used to detect the PUEA. A game of imperfect information among the secondary users (Sus), it does not interchange game information among them against the opponents creating the PUEA. The SUs plays as a grand association which attains synchronization every SUs create the same decisions lacking collaboration [10]. Signal activity pattern (SAP) system does not essential any a priori knowledge of PU. It obtains the activity pattern of a signal via spectrum sensing. It rebuilds the monitored signal activity pattern via a reconstruction model. primary user emulation (PUE) detection system that obtains the SAP of PU signal transmitters. However, this approach can't detect the PUEA [11]. The channel-tap power is applied as a radio-frequency fingerprint to entirely recognise PUEAs. The cross-layer intelligent learning ability of a SU is demoralized to launch detection databases through seamlessly joining the quick detection [12]. Belief propagation defence strategy that avoids the distribution of additional network. In this strategy, every SU computes the local function and the compatibility operation calculates the messages, interactions messages and calculates the beliefs until conjunction. The PUE attacker is identified by the belief threshold. If the beliefs is below a threshold, the uncertain can be identified as a PUE attacker [13]. Malicious users can cause heavy performance degradation by denial of service (DoS) attacks. Proactive model predictive control based medium access control protocols for CRs can accelerate the idle channel identity through forecasting channels future states [14].

A smart primary user emulation attacker (SPUEA) that does not create the channel busy all the times through taking into account the attacker as well as PU activity parameters also traffics. In preparation, an attacker may not misbehave every time, since if the attackers inhabit spectrum or else report false results, the attackers will be jammed simply through applying the SPUEA method. The function for the detection of spectrum sensing of false alarm probabilities and gets the SU throughput [15]. A cooperative multiband spectrum sensing approach is operating in the presence of malicious users. Cooperative spectrum sensing is enhancing the recognition operation and enhance the aggregate the attainable throughput [16]. A nonparametric Bayesian method for identifying the PUE attacks. The infinite Gaussian mixture model is accepted and an adjusted collapsed Gibbs sampling method is introduced to categorise the extracted fingerprints [17].

Database assisted frequency domain action recognition approach for detecting PUEA by application of action recognition techniques. Wireless communication functioning across a CRN and it utilize a relational database. This approach detect the PUEA by an energy detection in a particular frequency band. This strategy applies a relational database to record the motion-related feature vectors of PU on this frequency band. While an interrupted communication does not have a competition record in the database, this communication is considered from the PUEA [18]. Cooperative spectrum sensing approach is used to detect the existence of PUEA. In this approach, the joining weights are optimized with the aim of enhancing the available channel detection probability. It examine the influence of the channel estimation errors on the detection probability [19]. An emotion recognition system applying a deep learning method to receive a mel-spectrogram. In this approach, the support vector machine is used to classified the emotions [20]. Harmony search optimization algorithm is used for optimal route selection in the network [21].

Single input fuzzy logic controller (SIFLC) with gradient descent algorithm (GDA) and particle swarm optimization (PSO) for improving the routing efficiency [22]. Multi-feature-based deep convolutional neural networks which recognizes the facial expression. The input are preprocessed and improved through three filtering methods such as Gaussian, Wiener, and adaptive mean filtering. It further functional local binary

pattern that extracts the facial points of every facial expression. The deep features assists to remove the local data lacking acquiring a higher computational effort [23].

A tracking method which merge regression tree and Kalman smoother filtering. Regression tree is recommended by received signal strength indicator. This method to resolve the mapping relation between capacity and the target location. The predicted location measured as the identified information by the Kalman smoother algorithm [24]. Energy-efficiency in a shared based target tracking method can be reached by two methods such as sensing-related and communication-related. In this approach, a prediction algorithm to optimize communication and sensing functions. This method can minimized the energy utilization in the wireless sensor network (WSN) [25]. A swarm intellect optimization technique is used to detect the mischievous nodes and enhance the authentication. Here, the cluster heads (CHs) are chosen by the node weight. Observing behavior, observing energy utilization and fake route ads parameters are determined by the Mischievous nodes [26]. The predictive parser method is applied to verify the sensor authentication. Furthermore, an Elliptical curve cryptography algorithm to reject the eaves dropping attack [27].

2. HERMITAN MATRICES BASED MALICIOUS COGNITIVE RADIO DETECTION AND BAYESIAN METHOD FOR DETECTING PUEA ATTACK IN THE CRN

This approach contains number of CR user, malicious CR, PU and PUEA with a FC. The CR can identify the channel regularly and execute local determinations on the existence of the PU along with its hold clarification. Figure 1 shows the architecture of proposed system. This Figure 1 contains, FC, PU, PUEA, CR and malicious CR.

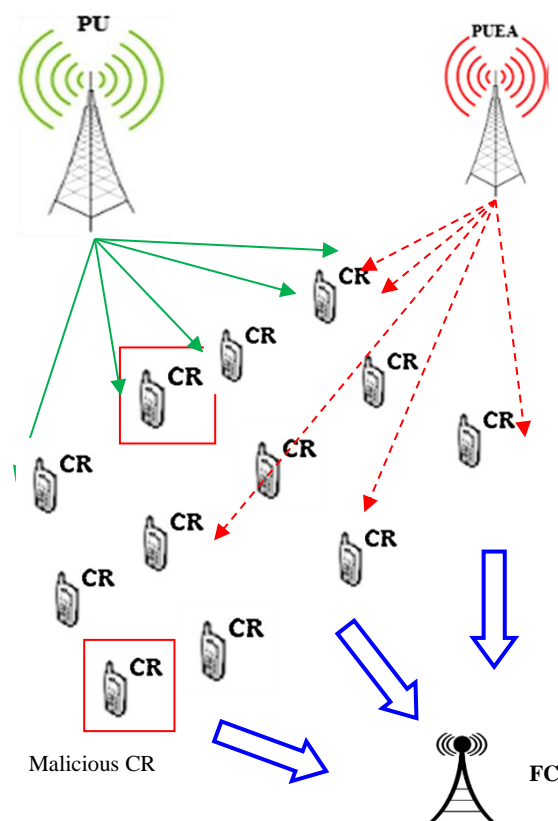


Figure 1. Architecture of proposed system

In this approach, the local spectrum is observed through the received signal strength indicator (RSSI) method. Recognized on the receiver R obtained signal, the distance distinctive R from a transmitter T is work out related the RSSI method. The CR users are inspired as receivers, and any PU; or else, PUEAs are considered as feasible transmitters. Usually, to avoid any forthcoming collision between PU and CRs signals, the PU dictates the entire CR nodes to make the channel clearly; as a result, it will be able to transferring hold data.

The PUEA try to win for the PU signal characteristics to attain at the channel resources. Here, we compute the RSSI is shown in (1).

$$RSSI = -10 \log_{10}(dist) + AP \tag{1}$$

Here k indicates the path-loss exponent of broadcasting, $dist$ indicates the distance between T and R , in addition, AP is the acquired power. A PUEA is present in the CRN that effort to evade the CR users from obtaining the spectrum holes. The local result of the entire sensing nodes will be broadcast a one-bit result to FC. Initially, the PU forward the signal to CR. Then, the CR received the signal and forward PU signals to FC. The FC before gets the PU signal, it checks the CR is real or not by the hermitan matrices with trust value. Figure 2 explains a Hermitan matrices based CR Verification. Thus, a Hermitan matrix is definite as:

$$A = A^T \tag{2}$$

that is the diagonal elements of a Hermitian matrix is real numbers, while other components maybe complex. If A is Hermitian, then as $A = A^T$:

$$A = \begin{bmatrix} d & k + ai \\ k - ai & e \end{bmatrix} \tag{3}$$

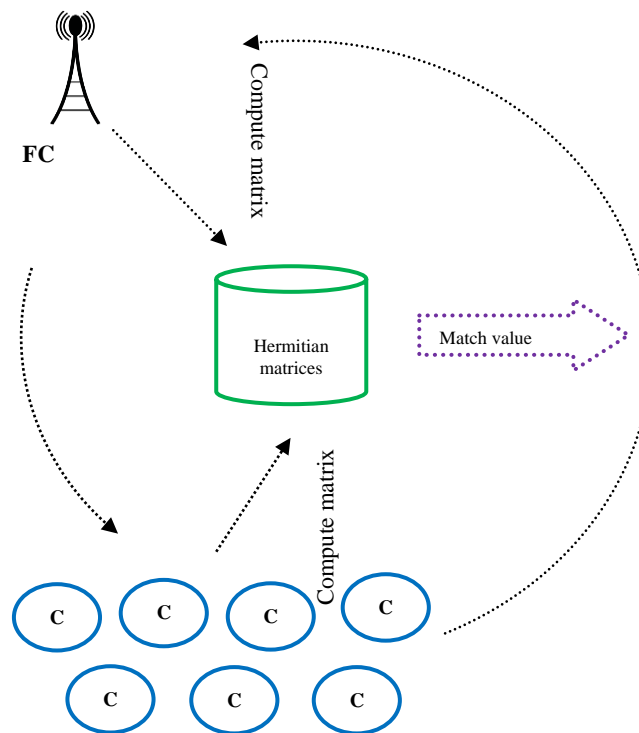


Figure 2. Hermitian matrices based CR verification

here,
 d =CR identity.
 k =secret key.
 e =PU identity.
 i =imaginary unit.

The secret key (k) computation is specified in (4):

$$\begin{aligned} K &= \log_2 d^R \\ K &= R \frac{\log d}{\log 2} \end{aligned} \tag{4}$$

here, d indicates the CR identity and R indicates the random number.

Here, a CR desires to admittance an unoccupied band, node computes the value of trust (VT) to demanding CRs through authenticating it with the pre-set thresholds. If the CR of VT is higher than the threshold, next the CR is trusted and allowable to admittance the band. A trust analyzer is continued which preserves the evidence of all nodes factors in its routing. Here, the node trust value is computed by node activeness and inactiveness, degree of data transmission, and hermitian matrices verification. Every node trust value exist between 0 and 1. Here, the trust value 0.3 represents that node is a malicious and 0.3 to 0.4 value nodes are chances to exist that node is a compromised nodes in the network. Breadth first search (BFS) tree method is used for dynamically determine the trust threshold between sender and receiver. If confirms the CR is a real then FC obtained the PU signals from CR and verified the PU signal by the Bayesian model. Figure 3 explains a PUEA attack detection in the WSN.

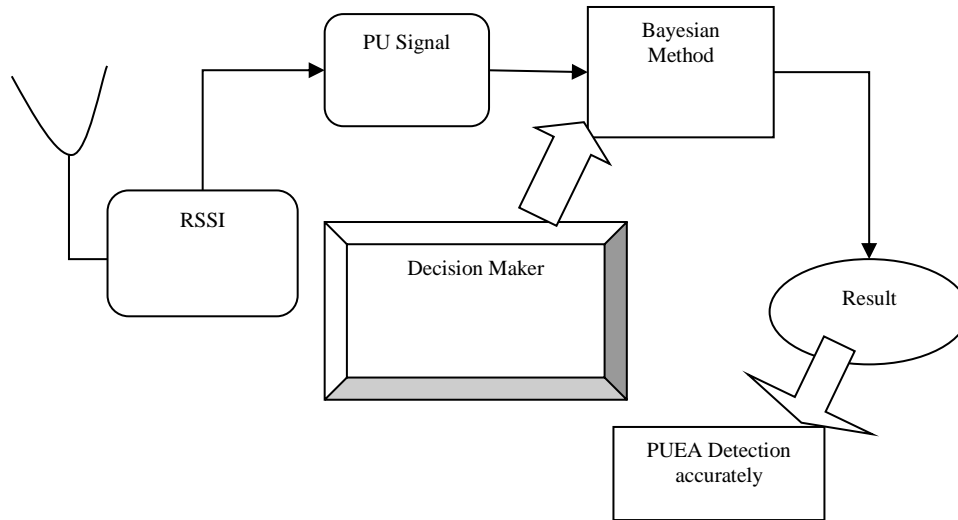


Figure 3. PUEA attack detection

In CSS, compute the RSSI of each CR user is communicated to the FC to assemble a decision concerning the present or non-present the PU signal. The out turn signal (OS) at the FC is specified in (5). Here, β denotes the preset threshold.

$$OS = RSSI \geq \beta \tag{5}$$

3. RESULTS AND DISCUSSION

Here, 100 CR users apply RSSI detection through $M=25$ samples in a detection interval. Moreover, the possibility of a false alarm for the threshold value is 0.1. The network simulator is used for detects the PUEA attacker and malicious CR user in the CRN. Figure 4 describes the error possibility between PU and CR for the CMCR and SPUEA schemes based on signal to noise ratio (SNR). The SPUEA approach SNR value is increased the possibility of the error also increased. Here, the CMCR has the feasibility of lesser error possibility since the hermitian matrices is used to detect the PUEA.

Figure 5 illustrates the false alarm possibility of the centralized multicast contention resolution (CMCR) scheme and SPUEA scheme. Here, the CMCR scheme improves the network function since it results in the smallest amount of false alarms. However, SPUEA scheme increases the false alarm when it increases the SNR.

Figure 6 explains the error possibility of the SPUEA scheme and CMCR scheme based on node density respectively. Here, the CMCR has the feasibility of lesser error possibility since the hermitian matrices is used to detect the PUEA. Figure 7 explains the miss detection possibility of CMCR scheme and SPUEA scheme based on node density respectively. Here, the proposed CMCR has feasibility of lesser miss detection since the CMCR technique hermitian matrices is used to detect the PUEA efficiently. Furthermore, malicious CR is detected by the Trust analysis method. However, SPUEA scheme raises the miss detection when it increases the node density since it can't distinguish the PUEA completely.

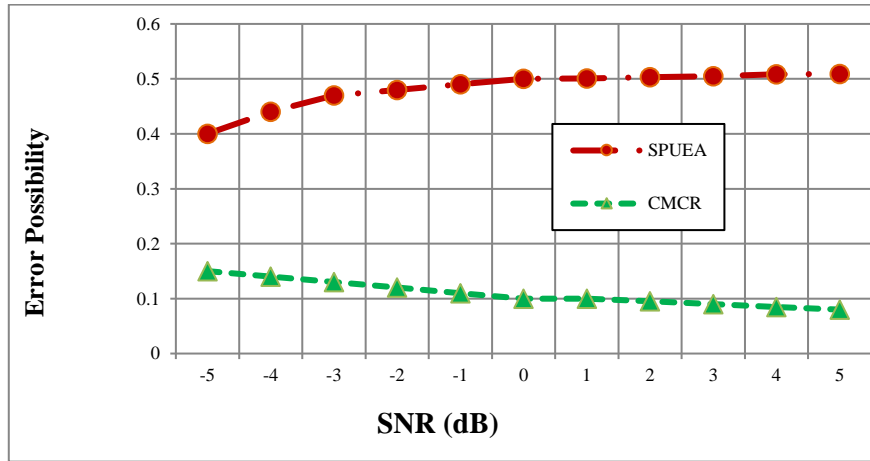


Figure 4. Error possibility of SPUEA and CMCR schemes based on SNR

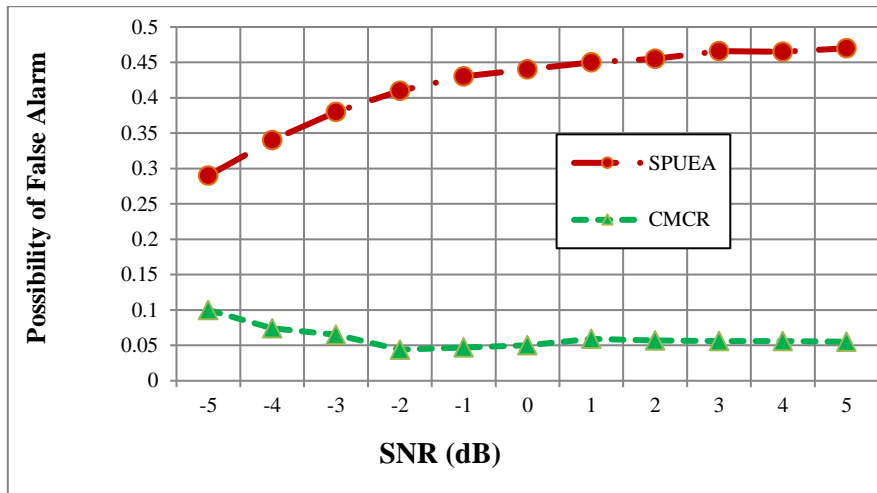


Figure 5. False alarm possibility of SPUEA and CMCR schemes based on SNR

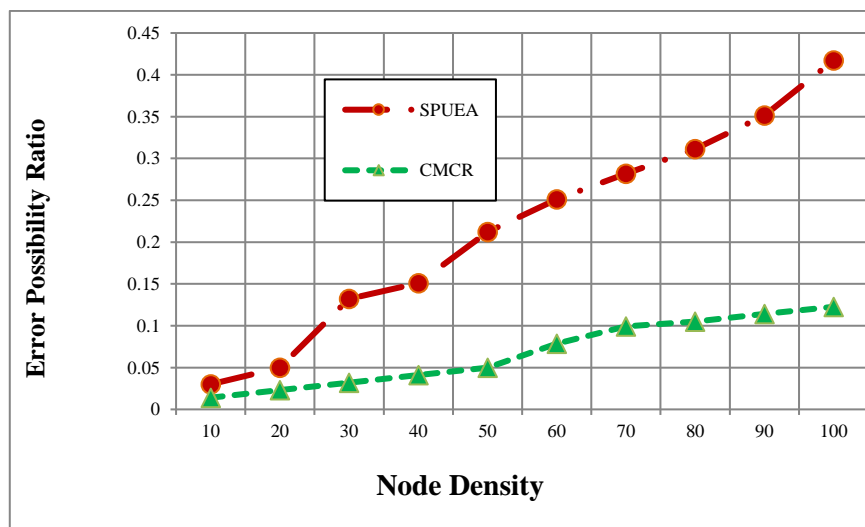


Figure 6. Error possibility of SPUEA and CMCR schemes based on node density

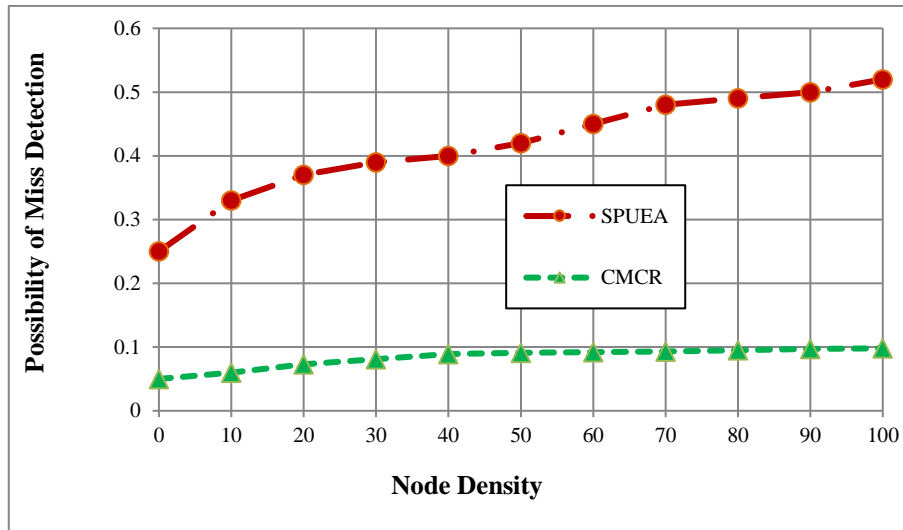


Figure 7. Miss detection possibility of SPUEA and CMCR schemes based on node density

4. CONCLUSION

This paper launched the concept for detecting the malicious CR and PUEA in the CRN. A trust analyzer is efficiently resolved malicious CR user through exploiting the behavioural features of every CR user. This paper presents a Hermitan Matrices based malicious Cognitive radio detection and Bayesian method for detecting PUEA attack in the CRN. In this approach, the Bayesian method is used for detecting the PUEA attack. The trust analyzer evaluates the CR trust. The node trust value is computed by node activeness and inactiveness, degree of data transmission, and hermitan matrices verification. In addition, the Hermitan Matrices method is used to detect the malicious CR user in the CRN. The simulation outcomes explained that the CMCR leads to improve the performance in terms of better detection ratio, minimized the possibility of miss detection ratio. Furthermore, it minimized the possibility of false alarm in the CRN.





REFERENCES

- [1] S. S. Oyewobi and G. P. Hancke, "A survey of cognitive radio handoff schemes, challenges and issues for industrial wireless sensor networks (CR-IWSN)," *Journal of Network and Computer Applications*, vol. 97, pp. 140–156, Nov. 2017, doi: 10.1016/j.jnca.2017.08.016.
- [2] S. P. Nalluri and R. R. Kurra, "Unsupervised feature selection for text clustering using differential inverse document frequency," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 4, pp. 790–797, Aug. 2021, doi: 10.21817/indjcs/2021/v12i4/211204014.
- [3] M. Rana and M. R. Shuvo, "Detection of primary user emulation attack in sensor networks," in *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, Nov. 2018, pp. 1–6, doi: 10.1109/ATNAC.2018.8615239.
- [4] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 5, pp. 3718–3731, May 2016, doi: 10.1109/TWC.2016.2526601.
- [5] N. Muchandi and R. Khanai, "Cognitive radio spectrum sensing: A survey," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Mar. 2016, pp. 3233–3237, doi: 10.1109/ICEEOT.2016.7755301.
- [6] K. M. Thilina, K. W. Choi, N. Saquib, and E. Hossain, "Machine learning techniques for cooperative spectrum sensing in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 11, pp. 2209–2221, 2013, doi: 10.1109/JSAC.2013.131120.
- [7] H. Kaur and G. Singh, "Measuring performance of variants of TCP congestion control protocols," *Indian Journal of Computer Science and Engineering*, vol. 8, no. 3, pp. 285–296, 2017.
- [8] C. S. B. Yadav and R. Sheshadri, "Wireless intrusion detection and prevention system for IEEE 802.11 based wireless sensor network," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 20, no. 1, pp. 30–36, 2018.
- [9] G. Rathee, F. Ahmad, C. A. Kerrache, and M. A. Azad, "A trust framework to detect malicious nodes in cognitive radio networks," *Electronics*, vol. 8, no. 11, p. 1299, Nov. 2019, doi: 10.3390/electronics8111299.
- [10] I. Kakalou and K. E. Psannis, "Coordination without collaboration in imperfect games: the primary user emulation attack example," *IEEE Access*, vol. 6, pp. 5402–5414, 2018, doi: 10.1109/ACCESS.2018.2791519.
- [11] C. Xin and M. Song, "Detection of PUE attacks in cognitive radio networks based on signal activity pattern," *IEEE Transactions on Mobile Computing*, vol. 13, no. 5, pp. 1022–1034, May 2014, doi: 10.1109/TMC.2013.121.
- [12] T. N. Le, W.-L. Chin, and W.-C. Kao, "Cross-layer design for primary user emulation attacks detection in mobile cognitive radio networks," *IEEE Communications Letters*, vol. 19, no. 5, pp. 799–802, May 2015, doi: 10.1109/LCOMM.2015.2399920.
- [13] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1850–1860, Nov. 2012, doi: 10.1109/JSAC.2012.121102.





- [14] M. Patnaik, V. Kamakoti, V. Matyas, and V. Rehak, "PROLEMus: A proactive learning-based MAC protocol against PUEA and SSDF attacks in energy constrained cognitive radio networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 2, pp. 400–412, Jun. 2019, doi: 10.1109/TCCN.2019.2913397.
- [15] A. Karimi, A. Taherpour, and D. Cabric, "Smart traffic-aware primary user emulation attack and its impact on secondary user throughput under rayleigh flat fading channel," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 1, pp. 66–80, 2020, doi: 10.1109/TIFS.2019.2911168.
- [16] M. J. Saber and S. M. S. Sadough, "Multiband cooperative spectrum sensing for cognitive radio in the presence of malicious users," *IEEE Communications Letters*, vol. 20, no. 2, pp. 404–407, Feb. 2016, doi: 10.1109/LCOMM.2015.2505299.
- [17] N. T. Nguyen, R. Zheng, and Z. Han, "On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification," *IEEE Transactions on Signal Processing*, vol. 60, no. 3, pp. 1432–1445, 2012, doi: 10.1109/TSP.2011.2178407.
- [18] D. Pu and A. M. Wyglinski, "Primary-user emulation detection using database-assisted frequency-domain action recognition," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4372–4382, Nov. 2014, doi: 10.1109/TVT.2014.2316831.
- [19] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2135–2141, Jul. 2011, doi: 10.1109/TWC.2011.041311.100626.
- [20] S. R. Kothuri and D. N. R. Rajalakshmi, "A hybrid feature selection model for emotion recognition using shuffled frog leaping algorithm (SFLA)-incremental wrapper- based subset feature selection (IWSS)," *Indian Journal of Computer Science and Engineering*, vol. 13, no. 2, pp. 354–364, Apr. 2022, doi: 10.21817/indjcs/2022/v13i2/221302040.
- [21] R. C. Muniyandi, M. K. Hasan, M. R. Hammoodi, and A. Maroosi, "An improved harmony search algorithm for proactive routing protocol in VANET," *Journal of Advanced Transportation*, vol. 2021, pp. 1–17, Feb. 2021, doi: 10.1155/2021/6641857.
- [22] F. N. Zohedi, M. S. M. Aras, H. A. Kasdirin, and N. B. Nordin, "New lambda tuning approach of single input fuzzy logic using gradient descent algorithm and particle swarm optimization," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 25, no. 3, p. 1344, Mar. 2022, doi: 10.11591/ijeecs.v25.i3.pp1344-1355.
- [23] A. Chen, H. Xing, and F. Wang, "A facial expression recognition method using deep convolutional neural networks based on edge computing," *IEEE Access*, vol. 8, pp. 49741–49751, 2020, doi: 10.1109/ACCESS.2020.2980060.
- [24] O. Demigha, W. K. Hidouci, and T. Ahmed, "On Energy efficiency in collaborative target tracking in wireless sensor network: A review," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 1210–1222, 2013, doi: 10.1109/SURV.2012.042512.00030.
- [25] M. El Midaoui, E. M. B. Laoula, M. Qbadou, and K. Mansouri, "Logistics tracking system based on decentralized IoT and blockchain platform," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, no. 1, pp. 421–430, Jul. 2021, doi: 10.11591/ijeecs.v23.i1.pp421-430.
- [26] D. J. Jeyakumar and A. R. Basha, "Swarm intellect optimization technique (SIOT) based mischievous detection and improve Authentication in Mobile Wireless Sensor Network," *Turkish Online Journal of Qualitative Inquiry*, vol. 12, no. 7, 2021.
- [27] D. J. Jeyakumar and S. Lingeshwari, "Fake sensor detection and secure data transmission based on predictive parser in WSNs," *Wireless Personal Communications*, vol. 110, no. 1, pp. 531–544, Jan. 2020, doi: 10.1007/s11277-019-06740-0.

BIOGRAPHIES OF AUTHORS






Dr. Devasahayam Joseph Jeyakumar     is a Professor in the Electronics and Communication department at J.N.N Institute of Engineering. He has completed a Bachelor of Engineering degree in Electronics and Communication from National Engineering College, Kovilpatti. He has completed a Master of Engineering in Applied Electronics. He received his Ph.D. degree from Anna University, Chennai. He has a total experience of 26 years, including teaching and industrial. His current research interests are signal processing, vlsi, networks, wireless sensor networks and cognitive radio networks. He has attended a number of seminars, short-term courses, workshops and conferences. He has published 20 papers in international conference proceedings. He has published 15 articles in International and Reputed Journals. He can be contacted at email: jayakumarjoseph33@gmail.com.






Boominathan Shanmathi     is an Assistant Professor in the Department of Electronics and Communication Engineering, J.N.N Institute of Engineering, Kannigaipair, thiruvallur-601102, Tamilnadu, India. She completed Bachelor of Engineering degree in Electronics and Communication from J.N.N Institute of Engineering, Kannigaipair affiliated to Anna University in 2016. She completed Master of Engineering in Applied Electronics from Sri Venkateswara College of Engineering, Sriperambathur affiliated to Anna University, Chennai in 2018. Currently she is pursuing Ph.D. at Anna University, Chennai. Area of her research is application of Image processing, deep learning. Her current interests are communication system, signal and image processing, digital logic circuits. She can be contacted at email: mathiboominathan0510@gmail.com.






Parappurathu Bahulayan Smitha    is an Associate Professor in the Department of Electronics and Communication Engineering., J.N.N Institute of Engineering, Kannigaipair, Thiruvalur-601102, Tamilnadu, India. She completed Bachelor of Engineering degree in Electronics and Communication from Periyar Maniammai College of Technology for Women, Vallam, Thanjavur, Tamil Nadu affiliated to Bharathidasan University. She completed Master of Engineering in Electronics and Control from Sathyabama Institute of Science and Technology, Sathyabama Deemed University, Chennai in 2005. Currently she is pursuing Ph.D. at Sathyabama Institute of Science and Technology, Chennai. Research area: cyber physical systems and distributed control systems and area of interest: cyber physical systems, microprocessors and microcontrollers, antennas and wave propagation, microwave engineering, communication systems, image processing, control systems. She can be contacted at email: smithapb@jnn.edu.in.






Sekar Vinurajkumar    is an Assistant Professor in the Department of Biomedical Engg., Veltech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai 600 062, Tamilnadu, India. He completed Bachelor of Engineering degree in Electronics and Communication from Jerusalem College of Engineering, Chennai affiliated to Anna University in 2008. He completed Master of Engineering in Medical Electronics from CEG Campus, Anna University, and Chennai in 2011. Currently he is pursuing Ph.D. at Anna University, Chennai. Area of his research is application of Image processing in medical images. He can be contacted at email: rajkumar.vinu@gmail.com.



Mohanan Murali    obtained his B.Tech. Degree in Electronics and Communication Engineering from Dr.M.G.R. university Chennai and M.E. Degree in Medical Electronics from College of Engineering, Guindy campus, Anna University, Chennai-600 025. He is working as Assistant Professor in the Department of Biomedical Engineering of J.N.N. Institute of Engineering, Kannigaipair, Thiruvallur District-601 102. His field of Interest includes signal processing, image processing, medical electronics, wireless sensor network, wireless network and integrated electronics. He has attended number of seminars, short-term course, summer schools and conferences. He published 13 papers in national conference proceedings. He is published 20 papers in International & UGC Journals proceedings. He is the Life time member of ISTE (India). He is working as Academic Coordinator in J.N.N. Institute of Engineering, Kannigaipair, and Thiruvallur District-601102. He is guided 35 U.G. projects and 3 P.G projects. He can be contacted at email: muralimohanan@gmail.com.



Muthuraj Mariselvam    is an Assistant Professor in the Department of Electronics and communication at J.N.N Institute of Engineering, Kannigaipair, thiruvalur-601102, Tamilnadu, India. He completed Bachelor of Engineering degree in Electronics and Communication from Sree Sowdambika College of Engineering, Aruppukottai affiliated to Anna University in 2009. He completed Master of Engineering in VLSI Design from Sri Venkateswara College of Engineering and Technology, Tirupachur affiliated to Anna University, and Chennai in 2013. Area of interest: digital circuits, vlsi design, image and signal processing, low power VLSI. He can be contacted at email: mariselvam.ms@gmail.com.