International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Review on Machine Learning Based Security Models for Wireless Networks

Neha Koge[1], Prof. Virendra Verma[2]

Abstract: Machine Learning and Data Driven models are being extensively used for physical layer security securing wireless networks. Typically cognitive software defined cognitive networks rely on channel state information (CSI) to be estimated iteratively to monitor the system against potential cyber attacks. Cognitive networks find their applications in military and defence as well with the advent of internet of things and its allied applications in military warfare. Cognitive Radio Networks often share common resources such as bandwidth or spectrum among several users or stations. Due to continued sharing of resources, cognitive networks often come under security attacks, most common of which are jamming and eavesdropping attacks. In this paper, the basics of machine learning assisted software defined networks have been presented with the focus of security awareness through estimates of channel state information. Previous work in the allied domain has been discussed along with their salient features.

Keywords: Physical Layer Security, Machine Learning, Security Aware Spectrum Assignment, cyber-attacks, false alarm, throughput.

I. INRRODUCTION

Internet of things or IoT is the connection of multiple devices termed as things over internet. A cognitive radio network is a form of network of cognitive radio nodes that are interlinked with each other [1]. It results in a broad cognitive radio network that is powerful and very efficient for radio communication. The performance of the communication is drastically enhanced of that area where the network is created. In such a scenario an individual cognitive radio unit can communicate with many other cognitive radio stations and there will exchange of information in a broad range of area. And in some other instances, many cognitive radio units form a single radio unit and operate as a big network. This gives a wider range of region to operate upon and also enhances the performance and flexibility of the network and also the communication [2]. The flexibility and intelligent working of the cognitive radio makes it very beneficial for the spectrum sensing process. The Cognitive Radio is a new form of radio technology that is gaining momentum in radio technology space. Much technological advancement has been taking place in this domain and following next to the software defined Radio, we have the cognitive radio technology [3]. The CR is the major impetus towards an efficient and robust radio network framework that can benefit in radio communication. For using the radio spectrum band in a more effective and beneficial manner, the concept of cognitive radio has become prominent [4]. This is a form of technology that sues many layers and levels of processing and the cognition of the radio is able to look upon and detect the available frequency bands and search for the best available communication efficacy. Similarly CR is capable of selecting the band of frequency and also the modulation type and the power metrics that are required and are the best fit for the specific conditions of an area and its regulatory policies. A cognitive radio is based on the cognition concept. It is a type of radio that is cognizant or aware of the surrounding environment and its internal and external state. It is capable of evaluating the situation by the help of its knowledge of various communication elements. It can take decisions based on its knowledge and capability. Basically it can look at the parameters of channel, can select the frequency, can detect spectrum availability and type of modulation etc. for effective communication [5].

The basic functioning of the cognitive radio framework can be understood using the following figure. In many cases, it can be modified manually to work and operate in a certain way or manner. It may look after the regulatory policies and the presence of the licensed users and the access of the channel and channel state as well. It works in sync to ensure improved radio communication and proper use of the channel bandwidth available. It is also inter-related closely to software defined radio [6].

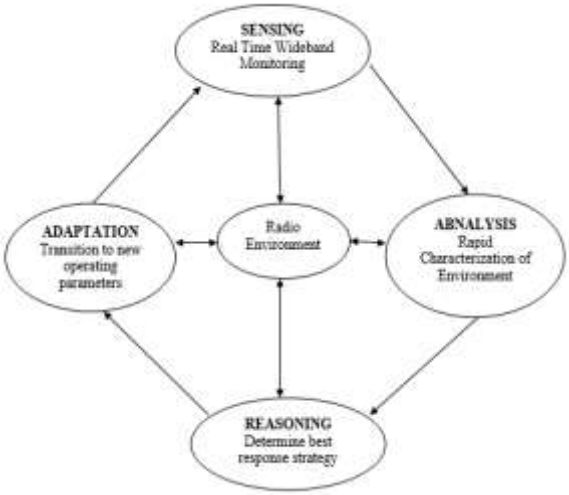

Fig.1 Iterative Channel Sensing

II. SECURITY AWARE CHANNEL ASSIGNMENT IN THE PRESENCE OF CYBER ATTACKS

The cognitive radio framework tries in leveraging the channel state information for the utilization of resources such as bandwidth and energy. The major challenge with cognitive systems comprising of cognitive networks is the fact that finding the channel state information with high accuracy is often extremely complex in nature. The random nature of the medium or channel makes is extremely difficult to assess the true nature of the channel which is often time variant in nature. Security aware channel assignment means the assignment of frequencies to users which have lesser chances of security attacks. The major challenges in security aware channel assignment are [7]:

The major problem that security aware cognitive channels face is the low throughput performance due to lost or corrupt data packets. This primarily happens due to:

1) Wireless nature of network
2) Frequent sharing of spectrum by users
3) Addition of noise in channel degradation
4) Achieving high throughput and security at the same time

However, the need for spectrum sensing for security aware system s lie in the fact that:

1) Cognitive radio networks are prone to attacks because of wireless nature of the channel
2) Jamming attacks are the most common form of attacks in cognitive networks, since it is not easy to break high complexity encryption in time-critical situations.
3) Security aware networks can detect possible jamming attacks which can help in decoding data at receiving end with higher accuracy and high throughput [8].

The spectrum is the most vital resource for increasingly large networks. As already a huge portion of the primary spectrum has been already reserved and assigned, it becomes an uphill task to find spectrum frequency bands for new services. Also there are regulations on the use of spectrum and its access by licensed users and unlicensed users cannot access them. For using the radio spectrum band in a more effective and beneficial manner, the concept of cognitive radio has become prominent. This is a form of technology that sues many layers and levels of processing and the cognition of the radio is able to look upon and detect the available frequency bands and search for the best available communication efficacy.

Thus sensing the spectrum is critically important for the CRN. The graphical illustration of the same if given below [9].

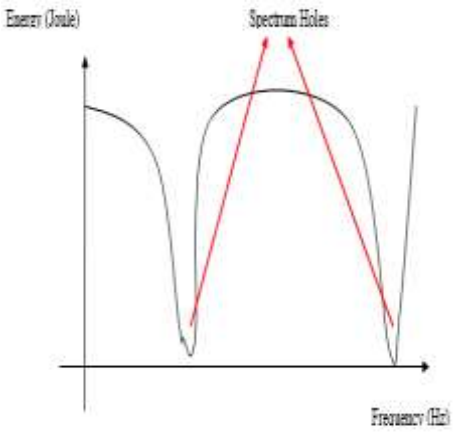

Fig.2 Energy Detection

. The sensing mechanism can be mathematically described as:

$$E_{sensed} = x(f) \quad (1)$$

Here,

E_{sensed} is the sensed energy

x(f) is the frequency dependent energy variation of the signal

However, the situation becomes challenging if there is addition of noise in the channel resulting in higher

energy in the spectrum holes thereby leading to false detection of holes or even non-detection of holes. This is termed as false alarm. The false alarm is computed in terms of a probability. The dependent variable is a function of energy threshold chosen for detection of false alarm. The false alarm probability is given by

$$: Prob(FA) = Prob\left(\frac{H}{N.H.}\right) + Prob(\frac{N.H.}{H}) \quad (2)$$

Here,
Prob denotes probability
FA denotes false alarm
H denotes spectrum hole
N.H. denotes spectrum non-hole

The probability of false alarm is critically affected by noise effects. The threshold detected for noise can be instrumental in the false alarm rate. The challenge associated with avoiding false alarm rate can be somewhat circumvented using other spectrum hole detection techniques such as cyclostationarity detection in which the channel is sensed with respect to repeated or reflected data. Alternative detection techniques can prove to sense the channel more accurately in case energy detection fail. The noise added false alarm is given by [10]:

$$Prob(FA/N) = Prob\left(\frac{H/N}{N.H.}\right) + Prob(\frac{N.H./N}{H}) \quad (3)$$

Here,
Prob denotes probability
N denotes noise
FA/N denotes false alarm when noise addition occurs
H/N denotes spectrum hole when noise addition occurs
N.H./N denotes spectrum non-hole when noise addition occurs

III PREVIOUS WORK

This section presents the previous approaches adopted in the domain.

Ara et al. [11] proposed that recently, machine learning has emerged as a promising tool to alleviate the increasing complexity of wireless networks, especially for wireless physical layer security. Hence, this paper introduces intelligent WPLS by concentration on PLA, AS, and relay node selection. First, it presents the background and types of WPLS and ML. Then, revisit the three basic methods of WPLS enhancement, i.e., relay node selection, AS, and authentication, and their integration with ML. Furthermore, several key challenges faced by intelligent WPLS were discussed along with the comprehensive investigation of its different applications in the wireless networks such as the internet of things, device-to-device communication, cognitive radio, non-orthogonal multiple access, and unmanned aerial vehicles. Finally, the appendix includes a detailed survey of ML techniques for WPLS. This article proposes to motivate and help interested readers to easily and rapidly understand the state-of-the-art of WPLS and intelligent WPLS.

Burton et al. [12] proposed data exfiltration methods aim to extract data without authorization from a network or device without detection. In this paper, we present a novel data exfiltration method using Channel State Information (CSI) from ambient WiFi signals. Modulation is performed by modifying the environment by moving a physically actuated machine resulting in a change to the channel response that is measurable by a distant receiver capable of collecting CSI samples. An attacker can use this to exfiltrate data when transmission using conventional methods is impossible, yet the attacker controls a moving mechanism. We discuss the design of the covert channel in detail and produce a proof of concept implementation to evaluate the performance in terms of communication quality. We find that even a simple implementation provides robust communication in an office environment. Additionally, we present several countermeasures against an attack of this type.

Sharifi et al. [13] simulated the cognitive network based on security metrics using network simulator (NS-2) module design, The packet delay, frame transfer rate and the throughput were analyzed. It was shown that additional overhead was indeed needed in case of jamming attacks. This happens due to the missing data packets. The energy spectrum sensing technique was cited as a possible successor to the proposed technique.
R**aza et al. [14]** proposed a time critical approach based network. This network was cognitive in nature thereby sensing the channel and utilizing the channel state information (CSI). The applications of the proposed system could be found in Internet of Things (IoT) based applications. The authors proposed that security aware cognitive networks are those cognitive networks which rely on the channel state information (CSI) for the detection of jamming attacks by possible adversaries.

The channel state information is typically the frequency response of the channel. Based on the channel state information, the jamming activity can be categorized into 3 groups i.e. low jamming activity, moderate jamming activity and high jamming activity.

Prasanna et al. [15] proposed a reliable and secure architecture for routing in cognitive networks. The approach used the channel state information or the frequency response of the channel to detect possibly malicious activity. The routes were dynamically adjusted based on the condition of the network. The main objective of the proposed work was to mitigate the effects of jamming and eavesdropping attacks by possible adversaries. This can be done by sensing the channel which is wireless in nature often termed as radio.

Gai et al. [16] the authors used the cloud platform to implement their approach. The use of big data analytics was also used for a mass storage system that was using the concept of cognitive networks and hence was security aware in nature. The major challenge in this approach was to limit the data usage due to the enormous data size based on cloud and the big data frameworks. The throughput of the system was the governing factor.

Ren et al. [17] proposed techniques based on collaborative resource sharing in cognitive networks. This technique is used for the energy detection mechanism and senses the energy of the channel at any given point of time. The hypothesis that governs this technique is the fact that jamming or attacks would definitely or invariably alter the spectral properties of the cognitive network. This would in turn make the attack or the eavesdropping perceptible.

Sharma et al. [18] presented a survey on the measures of security threats for cognitive networks as cognitive networks are prone to attacks as their functioning was governed by the channel state information. This can be done by sensing the channel which is wireless in nature often termed as radio. The distinction between the channel or radio being affected by attacks or not is to be decided based on the channel state information. This in turn needs the use of some effective detection mechanism.

IV. MACHINE LEARNING FOR SECURITY AWARE CHANNEL ASSIGNMENT

Software Defined Networks are typically hardware constrained. In IoT networks such as WANs, data is shared among different devices (wirelessly) over internet. So the information does not travel through guided media (secure media). The information travels in free space. So it is possible to be attacked by attackers. Particularly in IoTs, if the data shared is critical data, attack on such data can cause serious issues such as [19]:

1) Extraction of Data by Unauthorized users.
2) Data Modification
3) Denial of Service (DOS)
4) Data Corruption

So, securing the data transmission is necessary. However, this is a serious problem in securing the data transfer in IoTs due to the following reasons [20]:

1) The data in conventional IoT networks which connect primarily devices such as mobiles and computers use complex encryption mechanisms such as AEC, TLS etc. for securing the data from attackers.
Ex: In Whatsapp or gmail the data is encrypted using complex encryption algorithms such as AES, SHA, TLS algorithms etc. These algorithms need sufficient memory and processing power (processor) for implementation. Mobile phones or computers generally have sufficient memory and processing power.

2) However, in case of IoTs, the data is typically collected from sensors and connected devices which have very less memory and processing power. So implementing such complex encryption algorithms is not feasible.

Therefore, it is necessary to design mechanisms which would **NOT** include complex encryption techniques [21].

ML algorithms can analyze vast amounts of data to detect anomalies and predict potential security breaches. By integrating ML into channel assignment algorithms, SDNs can dynamically adjust channel allocation based on security risks. ML models can be used for:

Anomaly Detection: ML models can identify abnormal patterns in network traffic indicative of security threats, prompting adaptive channel reassignment.

Reinforcement Learning: Agents learn optimal channel assignment policies through trial and error, considering both performance and security metrics.
Supervised Learning: ML models trained on historical data can predict potential security threats and recommend channel configurations to mitigate risks [22].
ML holds immense potential for enhancing security-aware channel assignment in SDNs. Future research should focus on developing robust ML models capable of addressing evolving security threats while ensuring scalability and efficiency. By integrating ML into SDN frameworks, networks can dynamically adapt to security risks, safeguarding against malicious attacks and ensuring reliable performance [23].

The architecture for channel sensing based on machine learning is depicted in figure 3.

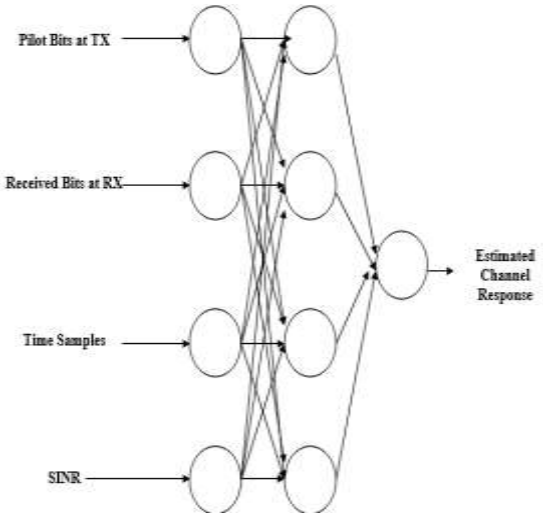

Fig.3 ML model for estimating channel state information

Machine learning offers promising avenues for improving security-aware channel assignment in software-defined networks. By leveraging ML algorithms to analyze network data and detect potential threats, SDNs can dynamically adapt channel assignments to mitigate security risks and ensure network integrity. However, addressing challenges such as data privacy, model robustness, and scalability is crucial for realizing the full potential of ML in enhancing security in SDNs [24].

Conclusion: It can be concluded from the previous discussions that security awareness in spectrum assignment is a critical aspect for cognitive IoT networks catering to defence and military applications or situations which deal with confidential and classified data. Various approaches pertaining to security in cognitive networks have been presented with their salient features. The probability of false alarm has also been investigated for ideal and practical channel conditions. It has been shown that hardware constraints poses a serous challenge in real time critical cognitive IoT networks. The paper presents the conventional and contemporary techniques to mitigate the issue of cyber attacks pertaining to such hardware constrained cognitive IoT Networks.

References

1. H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao and Q. Wu, “Deep Reinforcement Learning Based Intelligent Reflecting Surface for Secure Wireless Communications,” IEEE, Feb. 2020.
2. K. St. Germain and F. Kragh, “Physical-Layer Authentication Using Channel State Information and Machine Learning,” IEEE, Jun. 2020.
3. A. Senigagliesi, L. Baldi and E. Gambi, “Performance of Statistical and Machine Learning Techniques for Physical Layer Authentication,” arXiv, 2020.
4. A. Albehadili et al., “Machine Learning-Based PHY-Authentication for Mobile OFDM Transceivers,” in Proc. IEEE VTC 2020-Fall, 2020.
5. G. Gao, N. Ni, D. Feng, X. Jing and Y. Cao, “Physical Layer Authentication Under Intelligent Spoofing in Wireless Sensor Networks,” Signal Processing, vol. 166, 2020.
6. L. Liao et al., “Multiuser Physical Layer Authentication in Internet of Things with Data Augmentation,” IEEE Internet of Things J., vol. 7, no. 3, pp. 2077–2088, Mar. 2020.
7. H. Fang, X. Wang, Z. Xiao and L. Hanzo, “Autonomous Collaborative Authentication with Privacy Preservation in 6G: From Homogeneity to Heterogeneity,” IEEE Network, vol. 36, no. 6, pp. 28–36, Jul. 2022.
8. R. Xie et al., “A Generalizable Model-and-Data Driven Approach for Open-Set RFF Authentication,” IEEE Trans. Inf. Forensics Security, vol. 16, pp. 4435–4450, Aug. 2021.
9. C. Li, C. She, N. Yang and T. Q. S. Quek, “Secure Transmission Rate of Short Packets with Queueing Delay Requirement,” IEEE Trans. Wireless Commun., vol. 21, no. 1, pp. 203–218, Jan. 2022.

10. X. Zeng, C. Wang and Z. Li, "CVCA: A Complex-Valued Classifiable Autoencoder for mmWave Massive MIMO Physical Layer Authentication," presented at IEEE INFOCOM Workshops, 2023
11. Ara and B. Kelley, "Physical Layer Security for 6G: Toward Achieving Intelligent Native Security at Layer-1," in IEEE Access, 2024, vol. 12, pp. 82800-82824.
12. T Burton, K Rasmussen, "Private data exfiltration from cyber-physical systems using channel state information" ACM SIGSAC Conference on Computer and Communications Security, ACM 2021, PP.223-235.
13. AA Sharifi, M Sharifi, MJM Niya, "Secure cooperative spectrum sensing under primary user emulation attack in cognitive radio networks: Attack-aware threshold selection approach", vol.70, issue.1, Elsevier 2020.
14. Syed Hashim Raza Bukhari ,Sajid Siraj,Mubashir Husain Rehmani," NS-2 based simulation framework for cognitive radio sensor networks", SPRINGER 2019/.
15. K. J. Prasanna Venkatesan ,V. Vijayarangan, "Secure and reliable routing in cognitive radio networks", SPRINGER 2018.
16. K Gai ,Meikang Qiu ,Hui Zhao, "Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data",IEEE 2017.
17. Ju Ren ,Yaoxue Zhang ,Qiang Ye , Kan Yang ; Kuan Zhang ,Xuemin Sherman Shen," Exploiting Secure and Energy-Efficient Collaborative Spectrum Sensing for Cognitive Radio Sensor Networks", IEEE 2016.
18. R.K. Sharma ;,Danda B. Rawat," Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey",IEEE
19. A. Khamaiseh, I. Alsmadi, and A. Al-Alaj, "Deceiving Machine Learning-based Saturation Attack Detection Systems in SDN," in Proc. IEEE NFV-SDN, 2020.
20. M. Assis, L. F. Carvalho, J. Lloret, and M. L. Proença Jr., "A GRU Deep Learning System Against Attacks in Software Defined Networks," J. Network and Computer Applications, vol. 177, p. 102942, 2021.
21. J. Bhayo et al., "A Time-Efficient Approach Toward DDoS Attack Detection in IoT Network Using SDN," IEEE Internet of Things J., vol. 9, no. 5, pp. 3612–3630, Mar. 2022.
22. A. Bahashwan, M. Anbar, S. Manickam, T. Al-Amiedy, M. Aladaileh, and I. H. Hasbullah, "A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking," Sensors, vol. 23, no. 9, p. 4441, May 2023. ijisae.org
23. N. Niknami and J. Wu, "Advanced ML/DL-Based Intrusion Detection Systems for Software-Defined Networks, in Network Security Empowered by Artificial Intelligence, Y. Chen et al., Eds., Adv. in Inf. Security, vol. 107, Springer, Cham, pp. 59-84, Feb.2024.
24. M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," in Proc. IEEE 21st WoWMoM, Aug. 2020