ARTIFICIAL INTELLIGENCE FOR CYBER SECURITY

Abstract

In recent digital age, Cyber Security has boomed to priority tip. Security concerns viz. Data Breaches, ID theft, Captcha Hacking, and other similar situations have emerged as harmful data threat to the society. Challenge in designing appropriate rules and process and applying the same on critical data threat scenarios to perfectly combat cyberattacks and crimes are limitless. Recent developments in Artificial Intelligence have resulted in a dramatic escalation of the ever-increasing threat posed by cybercriminals and attacks. It has been used in practically all branches of engineering and research. AI has ushered forth a revolution in everything from robots to healthcare. Cybercriminals were unable to avoid this ball of fire, and as a result, "ordinary" cyberattacks have evolved into "intelligent" ones. In the subject of cybersecurity, artificial intelligence (AI) can serve as a foundational tool because of its ability to adapt quickly to new scenarios. AI-based techniques can be used to identify malware assaults, network intrusions, phishing and spam emails, and data breaches, among other things, and to warn security incidents when they occur.

Keywords: Artificial Intelligence, Cyber Security, Use Cases,

Authors

Galiveeti Poornima
Assistant Professor
Department of Computer Science & Engineering
Presidency University, Bangalore
galiveetipoornima@presidencyuniversity.in

Dr. Pallavi R
Associate Professor
Department of Computer Science Engineering
School of CSE & IS at
Presidency University
Bangalore, India
Pallavi.r@presidencyuniversity.in

I. INTRODUCTION

Modern society's reliance on wireless devices has skyrocketed as wireless technology has improved. The Internet of Things (IoT) is predicted to grow significantly in the near future, with widespread adoption. The ever-increasing number of wireless devices necessitates an enormous amount of spectrum. However, the amount of spectrum available is limited.

The impending problem of a lack of available spectrum has prompted the development of a new idea called cognitive radio. Cognitive Radio, Clancy, T. C, 2008, users are unlicensed users who identify unused licenced spectrum dynamically for their own use without creating any interference to licenced users. Cognitive Radio users are able to utilise this spectrum without generating any problems for licenced users. Cognitive radio extends the ideas of a hardware radio and a software defined radio to a radio that observes and reacts to its operational environment. The most important thing about cognitive radio is that it can recognise its communication environment and change the parameters of its communication scheme on its own to give the secondary users the best service possible, Burbank, J. L. (2008).

II. TYPES OF COGNITIVE RADIO NETWORKS

The two main types of Cognitive Radios are heterogeneous and spectrum-sharing.

1. **Heterogeneous CR:** When primary and cognitive networks interact, heterogeneous networks like the one seen in figure1 are formed. This heterogeneous wireless environment utilises a variety of connectivity options derived from diverse wireless access technologies to service requests from major end-users. The most significant change made to this plan was to incorporate CN's provision of leased services to PN. These services make it possible for licenced users to exchange data with one another in a seamless manner by making use of unlicensed frequency bands.

2. **Spectrum-sharing CR:** As a cognitive radio system becomes more prevalent, the use of spectrum sharing is becoming more commonplace. Non-licensed users can use licenced users' spectrum without affecting the performance of either party, according to the concept of "cognitive sharing." This concurrent sharing of restricted spectrum resources by licenced and unlicensed users increases spectrum use efficiency.

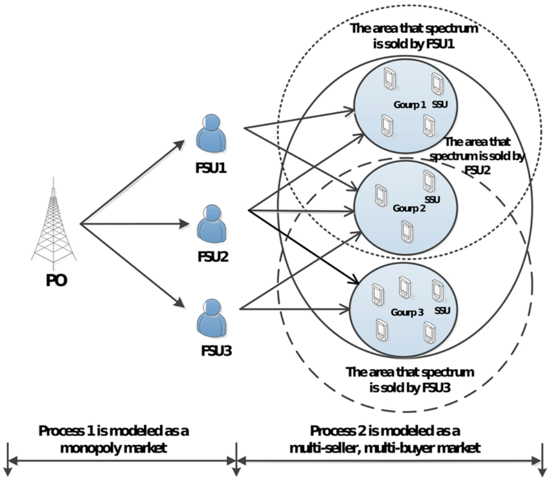
The area that spectrum is sold by FSU1
Gourp 1
SSU
The area that spectrum is sold by FSU2
Gourp 2
SSU
Gourp 3
SSU
The area that spectrum is sold by FSU3
FSU1
FSU2
FSU3
PO
Process 1 is modeled as a monopoly market
Process 2 is modeled as a multi-seller, multi-buyer market

Figure 1: Heterogeneous CRN

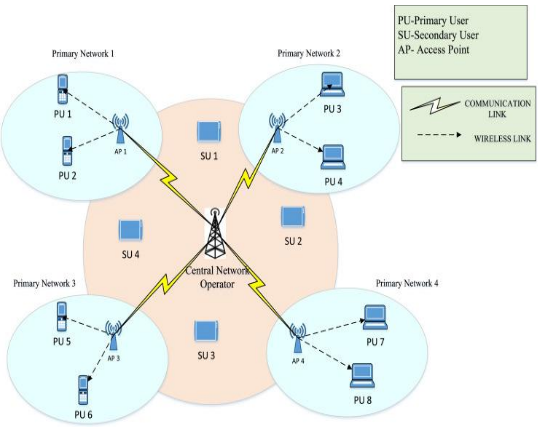

Figure 2: Spectrum Sharing CRN

III. SPECTRUM SHARING TECNIQUES

Interweave, underlay, and overlay are three of the spectrum sharing approaches, Akyildiz, I. F et al, 2008. **Interweave Dynamic Spectrum Sharing** is an adistributive and opportunistic form of spectrum access that enables wireless users to access the spectrum at any moment in a manner that is dynamic. Minimizing BER, reducing power consumption, and increasing throughput are just a few of the many goals that have been set, Kaur, A, 2020. In the case of the **underlay spectrum sharing**, a primary transmitter (PT) and a secondary transmitter (ST) are able to provide simultaneous transmissions to a primary receiver (PR) and a secondary reception (SR), respectively. In order to meet the requirements of the primary system, ST's transmit power is limited. The strong interference from PT and the weak signal from ST make it hard for the secondary system to talk, especially when the two systems are close**.** **Overlay spectrum sharing** technique, instead of sensing and using the primary user channel, this overlay spectrum sharing technique simultaneously utilises the available resource of the primary user by relaying technique and makes use of special NRZ coding for secondary user communication separately with SNR level maintained. Overlay spectrum sharing technique is a form of spectrum reuse.

IV. SPECTRUM SESNING TECHNIQUES

Integration of CR technology in wireless sensor nodes has recently received a lot of attention since it allows sensors to broadcast data packets over both licenced spectrum bands and free ISM bands. The sense of the spectrum is an essential component of CR. The presence of PUs and the emergence of spectrum gaps can be detected by CR through spectrum sensing, which is a vital tool for CR. Signal processing techniques and cooperative sensing techniques are the two main categories of sensing methods. The many methods of spectrum sensing are broken down and categorised in figure 3.

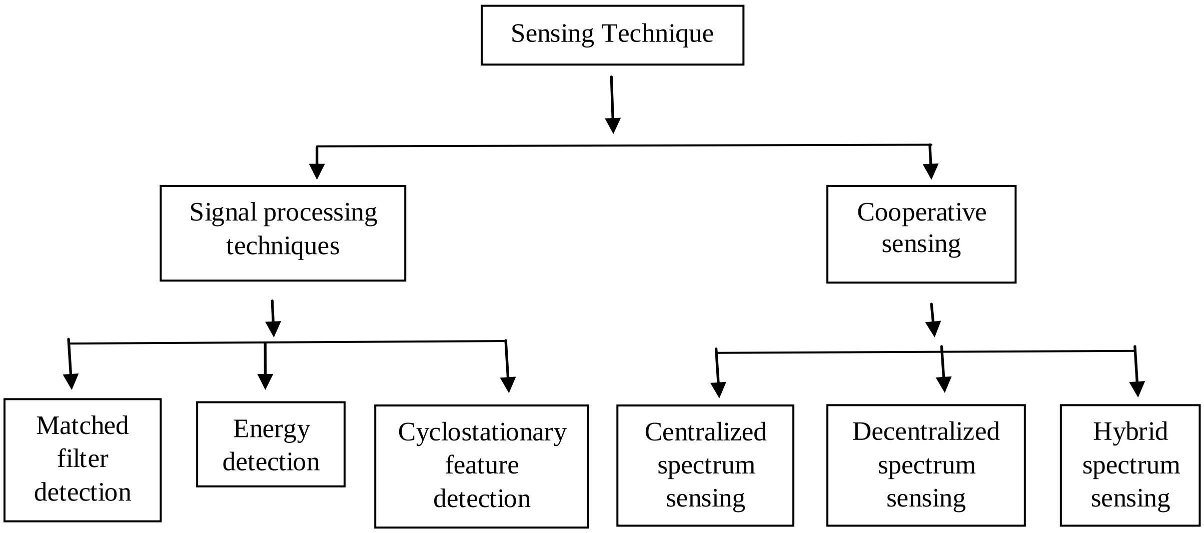
Sensing Technique
Signal processing techniques
Cooperative sensing
Matched filter detection
Energy detection
Cyclostationary feature detection
Centralized spectrum sensing
Decentralized spectrum sensing
Hybrid spectrum sensing

Figure 3: Spectrum Sensing Techniques

V. ATTACKS ON CRNs

A model for wireless technology, it makes intelligent decisions about transmission and reception settings based on the nearby networks' signals without interfering with anybody else's use. It is possible to categorise the cognitive radio network architecture into two main groups, primary and secondary. The second option is cognitive radio networks, which are sometimes referred to as unlicensed users. Figure 4 depicts the architecture of the cognitive radio, where the lowest layer is the physical layer. Then there are the layers of links, networks, and transport. The functions of each layer are outlined in depth.

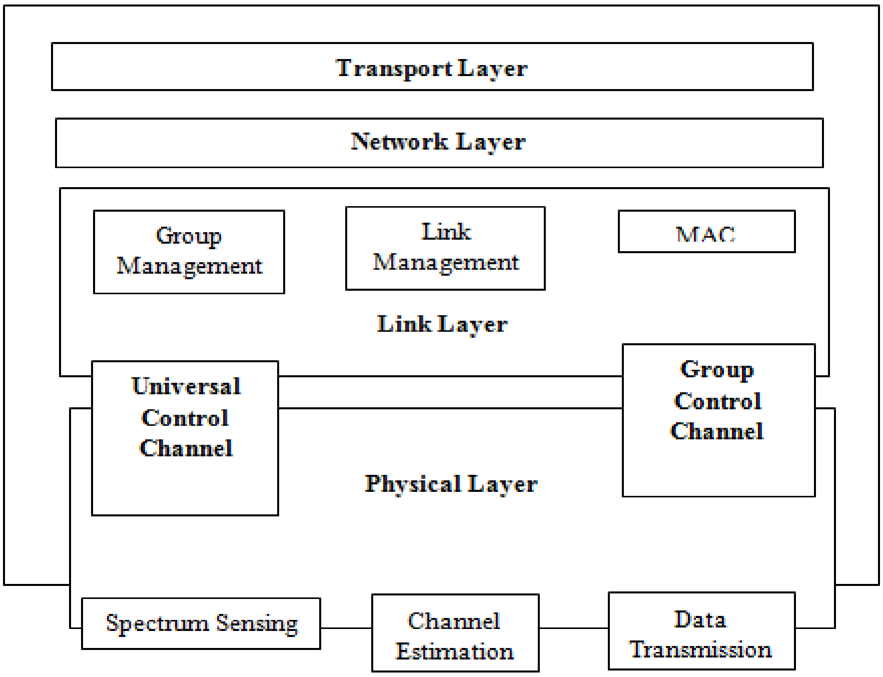

Figure 4: Architecture of Cognitive Radio Network

As per, Sudha & Sarasvathi, 2020, the CRN attacks can be classified into two main categories: 1) Infrastructure based CRN attacks like Jamming, Incumbent emulation, Spectrum sensing data falsification and 2) Infrastructure less CRN attacks such as Selfishness, Intrusion, and Exogenous adversary. Also, as mentioned in [18] the significant issues of the study is that the majority of threats/attacks identified in CRN's related to the cognitive-communication is to secure the spectrum sensing by both primary users and secondary users, Incumbent emulation attacks or sensor jamming.

The Cognitive radio network attacks as per, Khan & Barman, 2016, can be further classified into several categories as:

1. Based on the Cognitive Radio (CR) functionality, as show in Table I.

2. Attack based on Protocol Layer

Table 1: Attacks based on CR functions

Cognitive Radio Function	Type of attacks
Spectrum sensing	Overlap, Denial of Service, Lion or Jamming Message, Spectrum Sensing Data Falsification (SSDF).
Spectrum Sharing	Snooping, DoS, and Disguising Your Identity Misbehavior or a selfish attack in disguise, Depletion of essential resources, Scam Based on False Documents
Spectrum Management	Utility with a Bias and Incorrect Feedback

Spectrum Mobility	Interference with information regarding routing

Table 2: CR attacks based on Protocol Layers

Protocol Layer	Type attacks
Physical Layer	PUEA (primary user emulation attack), Jamming, OFA (objective function attack), and CCDA (common code execution and denial of service assault) (common control data attack)
Link Layer	SSDF (Spectrum-Sensing Data Forgery), CS-DoS (Control-Channel-Saturation-Denial-of-Service), and SN (Selfish (SCN)
Network Layer	Wormhole attack, Sink hole attack, Hello flood attack
Transport Layer	Lion attack, Jellyfish attack
Application Layer	Cognitive radio virus attack, Logic Error Attack, Buffer Overflow attack

VI. REINFORCEMENT LEARNING TECHNIQUES

Reinforcement Learning (RL) is a machine learning technique in which an agent learns to complete a task through repeated trail and error interactions with a dynamic environment. In contrast to both supervised and unsupervised learning, RL use an algorithm that is based on feedback. With this learning method, the agent can make a series of decisions that maximize a reward metric for the task without any help from a person or being told to do so. Because of its capacity for learning, it is suitable for usage with neural networks. On school of thought refers to this as "deep reinforcement learning". Using RL, it is feasible to construct a wide variety of problem-solving models. RL is a big part of the models used to make simulators, detect objects in self-driving cars and robots, and do a lot of other things. The general process for training an agent with reinforcement learning includes the following steps:

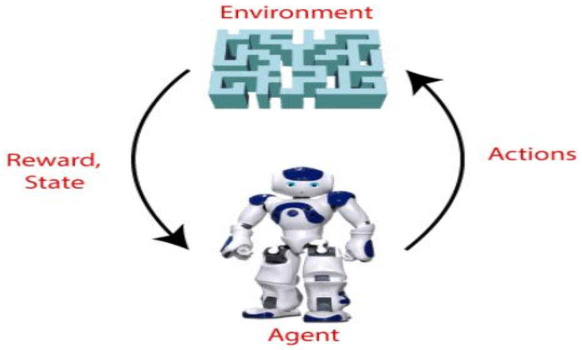

Figure 5: Training an Agent

The jamming assault is one of the primary concerns when it comes to the security of spectrum sharing in cognitive radio, particularly in an IoT network. CR networks' security concerns around proactive jamming and reactive jamming in spectrum sharing have been resolved. Salameh, Almajali, Ayyash, & Elgala, 2018. Assigning channels in the context of active and passive jamming attacks is performed using a probabilistic channel assignment technique. The application of machine learning and deep learning Because it builds mathematical models from observations, or training data, cognitive IoT networks offer a more viable approach. The application of machine learning and deep learning Cognitive IoT networks are a more promising alternative since they create mathematical models from observations (i.e., training data), which may then be used for prediction or decision-making. The instructional methods make it possible to automatically gain knowledge and make improvements based on experience, Nallarasan & Kottursamy, 2021.

Another jamming attack effort for the cognitive radio network with an anti-jamming job using a Markov decision process and deep reinforcement learning method can be used. To learn a policy and to maximise the rate of successful transmission, the mechanism is used. Using a Double Deep Q Network (Double DQN) model, the jammer is detected. When training the Q network, the Transformer encoder is used to estimate an action-value pair from raw spectral data. One of the anti-jamming strategies that are used in cognitive radio is called channel hopping, Nallarasan & Kottursamy, 2021.

There are several types of reinforcement learning algorithms like 1) Q-learning, 2) Deep Q Learning (DQN), 3) Double DQN, and 4) Deep Deterministic Policy Gradient (DDPG) are used to address the jamming attacks, Sudha & Sarasvathi, 2022.

1. **Q-Learning:** Q-Learning is a Reinforcement learning policy that finds the next best action. This activity is chosen at random, and the goal is to achieve the greatest possible prize. Q-learning is a model-free, off-policy reinforcement learning algorithm that will determine the optimum course of action given the agent's present condition. Depending on where the agent is in the environment, it will decide what to do next. The purpose of the model is to identify the most appropriate way to proceed in light of the existing circumstances. To achieve this goal, it might develop its own set of guidelines or deviate from the official policy. Because of this, there is no genuine requirement for a policy; hence, we refer to it as "off-policy." Model-free means that the agent makes predictions based on the predicted response of the environment in order to move forward. Learning is accomplished not via the application of a reward mechanism but rather through the process of trial and error.

2. **Deep Queue Learning (DQN):** Deep Q-Learning is a form of learning that makes use of a deep neural network. In order for Deep Q-Learning to function, the initial state must first be presented to the neural network, after which the network must produce an output that is the Q-value of each and every conceivable action. The following is an illustration of the difference between Q-Learning and Deep Q-Learning:

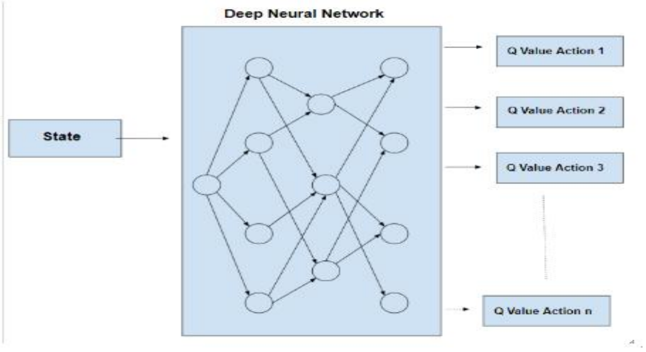

Figure 6: Deep Q learning (DQN)

3. Deep Deterministic Policy Gradient (DDPG) is a strategy for reinforcement learning that combines Q-learning and Policy gradients. DDPG stands for "deep deterministic policy gradient." The Actor and Critic models make up the actor-critic approach known as DDPG. The actor is a policy network that accepts the state as an input and outputs the exact action (continuous), rather than a probability distribution of actions. The Q-value network that feeds in state and activity and spits out criticism. The DDPG approach is considered "off" policy. In the continuous action setting, where DDPG is used, the actor computes the action directly rather than selecting from a probability distribution over actions, hence the "deterministic" in DDPG. In a continuous action context, DDPG is preferable to the more traditional actor-critic setup.

VII. CONCLUSION

Reinforcement learning, or RL, is an approach to artificial intelligence that has been implemented to enable each unlicensed user to observe and carry out optimal behaviours for performance enhancement in a wide range of schemes in CR, such as dynamic channel selection and channel sensing. This has been accomplished by the application of an artificial intelligence technique known as reinforcement learning.

BIBILOGRAPHY

[1] Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. In Countering cyber-attacks and preserving the integrity and availability of critical systems (pp. 170–192). IGI Global.

[2] Calderon, R. (2019). The benefits of artificial intelligence in cybersecurity.

[3] Donepudi, P. K. (2015). Crossing point of artificial intelligence in cybersecurity. American journal of trade and policy, 2(3), 121–128.

[4] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the internet of things (iot) cybersecurity. Discover

[5] Internet of things, 1 (1), 1–14.

[6] Lorenzo, P., Stefano, F., Ferreira, A., & Carolina, P. (2021). Artificial intelligence and cybersecurity: Technology, governance and policy challenges. Centre for European Policy Studies (CEPS).

[7] Mohammed, I. A. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY[IJIERT], 7(9).

[8] Morovat, K., & Panda, B. (2020). A survey of artificial intelligence in cyber-security. In 2020 international conference on computational science and computational intelligence (csci) (pp. 109–115).

[9] Patil, P. (2016). Artificial intelligence in cybersecurity. International journal of research in computer applications and robotics, 4(5), 1–5.

[10] Sadiku, M. N., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial intelligence in cyber security. International Journal of Engineering Research and Advanced Technology, 6 (05), 01–07.

[11] Samtani, S., Kantarcioglu, M., & Chen, H. (2020). Trailblazing the artificial intelligence for cybersecurity discipline: a multi-Disciplinary research roadmap (Vol. 11) (No. 4). ACM New York, NY, USA.

[12] Soni, V. D. (2020). Challenges and solution for artificial intelligence in cyber-security of the usa. Available at SSRN 3624487.

[13] Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence forcybersecurity: a systematic map-ping of literature. IEEE Access, 8, 146598–146612.

[14] Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. Cyber, Intelligence, and Security, 1 (1), 103–119.