International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

A Learning Method for Secondary Users to minimize the effect of Jamming in Cognitive Radio Wireless Sensor-Networks State of the art in CR-WSN security

Mr. Shashank D[1], Yuvaraju B N[2]
[1]*Assistant Professor, Department of IS & E, National Institute of Engineering Mysuru*
[2]*Professor, Department of CS & E, National Institute of Engineering, Mysuru*

Abstract: ***Cognition in radio networks has led to architectural changes of wireless sensor networks. Software layer along with digital radio has made cognitive radio a reality. Primary Users working in licensed band face interference by opportunistic Secondary Users in CR-WSNs. The cognitive engine of a cognitive radio (CR) is assigned with some objective function, be it to maximize data rate, minimize interference, or some other optimization goal. The CR has a set of inputs: coding rate, channel access protocol, transmission power, center frequency, encryption algorithm, type of modulation, frame size etc. By changing these inputs, the cognitive engine tries to achieve some output of its objective function. The spectrum is a resource that all nodes in the cognitive radio network fight over. Malicious nodes make use of this to jam users that are trying to share the spectrum. This paper focuses on learning methods that help secondary users minimize the effect of jamming.***
Keywords: Cognitive Radio; Dynamic Spectrum Access; Security Issues in CR-WSN;

I. INTRODUCTION

Wireless networks have grown as a natural extension of phenomenon that computer networks are growing at an exponential rate. And as the number of devices connected to each other and the Internet have grown exponentially [1], spectrum has been divided and sub divided to satisfy needs. These divisions did not transcend geographical spaces because it was sufficient that transmissions did not interfere with each other. During the time of the conception of the idea of spectrum division, this was the most important goal. Recent communication systems such as Long-Term Evolution (LTE), LTE-Advanced (LTE-A), and WiMAX have been designed to support high data rates and many users. Devices located at the edge of a cell are still prone to experience degraded service levels because of limited possibilities of reconfiguring terminals and networks depending on spectrum availability, inefficient spectrum usage, and non-optimal use of radio resources as well as insufficient flexible deployment of base stations (BSs). These limitations of femtocell technology have caused mobile operators to promote the use of Wi-Fi networks to offload traffic from their networks. KDDI Japan has offloaded 50% of its wireless traffic public hotspots and AT&T has moved in the same direction with hotspot connections [2].

A cognitive radio (CR) is an intelligent radio that can be programmed and configured dynamically. Its
transceiver is designed to use the best wireless channels in its vicinity. Such a radio automatically detects available channels in wireless spectrum, then accordingly changes its transmission or reception parameters to allow more concurrent wireless communications in each spectrum band at one location.

This process is a form of dynamic spectrum management. In response to the operator's commands, the cognitive engine can configure radio-system parameters. These parameters include waveform, protocol, operating frequency, and networking. This functions as an autonomous unit in the communications environment, exchanging information about the environment with the networks it accesses and other cognitive radios (CRs). A CR monitors its own performance continuously, in addition to reading the radio's outputs; it then uses this information to determine the RF environment, channel conditions, link performance, etc., and adjusts the radio's settings to deliver the required quality of service subject toan appropriate combination of user requirements, operational limitations, and regulatory constraints.

Some smart radio proposals combine wireless mesh network—dynamically changing the path messages take between two given nodes using cooperative diversity; cognitive radio—dynamically changing the frequency band used by messages between two

consecutive nodes on the path; and software-defined radio—dynamically changing the protocol used by message between two consecutive nodes. Depending on transmission and reception parameters, there are two main types of cognitive radio[3]:
Full Cognitive Radio also called as Mitola radio, where every possible parameter observable by a wireless node (or network) is considered.

A. Spectrum-Sensing Cognitive Radio, in which only the radio-frequency spectrum is considered.
B. Other types are dependent on parts of the spectrum available for cognitive radio:
C. Licensed-Band Cognitive Radio[4], capable of using bands assigned to licensed users (except for unlicensed bands, such as the U-NII band or the ISM band. The IEEE 802.22working group is developing a standard for wireless regional area network (WRAN), which will operate on unused television channels.
D. Unlicensed-Band Cognitive Radio [4], which can only utilize unlicensed parts of the radio frequency (RF) spectrum One such system is described in the IEEE 802.15Task Group 2 specifications, which focus on the coexistence of IEEE 802.11 and Bluetooth. Spectrum mobility: Process by which a cognitive-radio user changes its frequency of operation. Cognitive-radio networks aim to use the spectrum in a dynamic manner by allowing radio terminals to operate in the best available frequency band, maintaining seamless communication requirements during transitions to better spectrum.
E. Spectrum sharing [5]: Spectrum sharing cognitive radio networks allow cognitive radio users to share the spectrum bands of the licensed-band users. However, the cognitive radio users must restrict them transmit power so that the interference caused to the licensed-band users is kept below a certain threshold.
F. Sensing-based Spectrum sharing [6]: In sensing-based spectrum sharing cognitive radio networks, cognitive radio users first listen to the spectrum allocated to the licensed users to detect the state of the licensed users. Based on the detection results, cognitive radio users decide their transmission strategies. If the licensed users are not using the bands, cognitive radio users will transmit over those bands. If the licensed users are using the bands, cognitive radio users share the spectrum bands with the licensed users by restricting the transmission power.

II. MODUS OPERANDI OF THE COGNITIVE RADIO

Cognitive Radio is used is many wireless networks apart from just the wireless sensor network. For example, in MANET many CR is used to overcome the drawback of routing protocols. Cognitive Radio works with the digital radio controlled by the software, also called as Software Defined Radio. CR along with SDR has brought in a new dimension in wireless communication. The flexibility offered by the CR-SDR is opening new avenues in wireless transmission. A separate set of protocols are designed to dynamically manage the new network, which along with it brings some serious security drawbacks. Few of the security issues which needs to be mitigated are discussed in this paper.
The CR works in a closed-cycle having only four functions shown in the figure 2.1

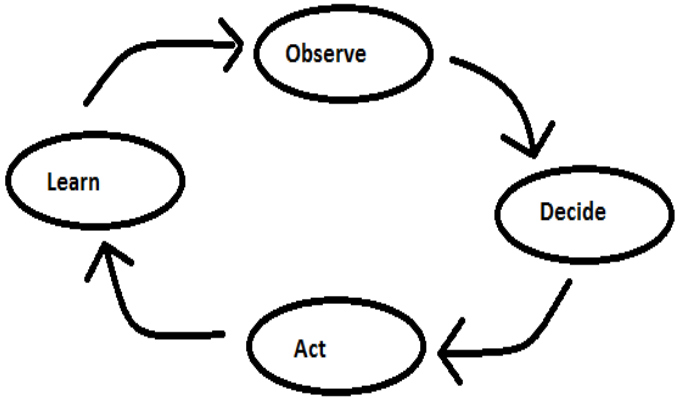

Figure 2.1 Cognitive Radio Closed Cycle

SDR were developed to support varying bandwidth for larger spectrum making use of white spaces or unused bandwidth in the precious natural resource the radio spectrum. In licensed band, often the users will not be used the frequency all the time, giving an opportunity for secondary users to use it temporarily. SDR with cognitive capabilities can change the operating variables both in

hardware level and software level. This changing in environment variables for a radio requires a processing capability called as the engine of cognition – Cognitive Engine.

The self-learning part of this cognitive engine is what makes the CR the most promising communication device for the future responsible for dynamically changing radio environment.

III. SECURITY ISSUES IN CRN

A. *Primary User Emulation Attack*

In a cognitive network, the secondary users are required to vacate the band every time that they detect a primary user (owner of the frequency) attempting to transmit. Malicious users use this basic property to disrupt secondary user communication in an attack known as primary user emulation attack.

The only way a secondary user can overcome this form of attack is if it can differentiate an emulation of the primary user from the actual primary user transmission [7]. Generally, in networking, authentication problems such as these are solved by requiring the transmitter of data to cryptographically sign all data. But this becomes tricky in case of cognitive networks, because the condition upon which unlicensed users can use licensed spectrum (as per the FCC) is that there be ―no modification to the incumbent system (i.e., primary user). Alternatively, location oriented and communication oriented methods of authentications can also be employed to overcome this PUE attacks in cognitive networks.

B. *Spectrum Sensing Data Falsification*

Also known as Byzantine attack where the intruder tries to modify the sensing data in the network [8]. This type of attack is difficult to identify and this ruin the integrity of data in the CRN. The fundamentals of cooperative spectrum sharing are under threat in byzantine attacks. Signal detections techniques employed are too expensive for the CRN and takes up a lot of energy cycles. Rather than communications of the network, the motes will be busy in managing the network which defeats the purpose of the cognitive radios.

C. *Sniffing / Eavesdropping*

A simple network layer attack is capturing the packets and reading the sensitive data [9]. In cognitive radio networks, the attributes and other antenna values are being transmitted and exchanged between the CRs at a high frequency. Capturing control channel is the endgame of the radios involved. A 25% success in sniffing will lead to entire network being taken over by the compromised node.

This passive attack must be mitigated using the means of encryption, which again is a costly affair for wireless nodes running on a limited battery. Considering the ever-changing attributes of CRN encryption and decryptions needs to be changed very often.

D. *Intelligent Jamming Attack*

Illegal transmission of RF signals intending to disrupt the communications of PUs is not an easy one to counter in wireless networks [10]. Few of the methods employed are channel hopping and power allocation varying and sometimes a mix of both. The work proposed in this paper revolves around using the concept of zero-sum games from artificial intelligence in evading the intelligent jamming attack. The learning strategy used is Q-Learning [12]; to learn the policy of the jammer.

IV. SYSTEM MODEL

The spectrum environment has been modeled roughly similarly in most game formulations. We consider a model based on them all. We use $p^t = 0$ to denote the channel is not being used by a PU at time t, and $p^t = 1$, to denote that it is. Because a secondary user (SU) needs to be constantly aware of the presence of the license owner on the spectrum, we keep track of two probabilities p^t01, the probability of the channel changing from an idle state to one of being occupied, in terms of primary user access, and p^t10, the probability of changing from an occupied state to an idle one.

The action set A, the set of available actions an SU can take, are decided based on the amount of information that it keeps track of for each state. If users keep track of the state history in terms of if the channel has been jammed in the previous state or not, we have a simpler action set wherein the user either decides to transmit on a previously jammed band, or decides not to. A more complicated action set would be to keep track of histories separately for control and data channels. The SU then has a more complex action set of choosing to retain the channel as a data (or control) channel, or switching to control (or data), or leaving the band idle.

An SU is only aware of jamming attempts on channels that it uses for signal transmission (by for e.g., absence of acknowledgments from the receiver). Channels the SU left idle will not reflect jamming attempts in their state histories.

The reward a user gets depends on the success of transmission. If the transmission is a success, the payoff assigned is positive (the utility of the channel), if it is a failure the payoff negative (the cost of transmission), and if the channel is left idle the payoff zero. The user tries to maximize the expected payoff by choosing an appropriate policy.

The game can now be modeled as a Markov Decision Process (MDP). Most literature considers channel hopping as the primary defense against jammers, but another defense strategy, manipulating power of transmission has been recently explored [11]. The focus is mostly on channel hopping.

A. Formalizing reward and strategy

A more complicated way of quantifying payoff would be to include other measures of QoS such as packet loss, jitter, or data throughput. But as mentioned we only consider the success of signal transmission. Formally,

$$R(s, a) = \sum_l [\, N(s, a)_l^1 \,.\, U + N(s, a)_l^0 \,.\, C \,]$$

Where R (s, a) is the total reward at state 's' on action 'a';

$N_l^1(s, a)$ represents successful transmission on channel l;

$N(s, a)_l^0$ represents jammed transmission; **U** and **C** respectively denote utility transmission and cost of transmission.

Representing the value of being in a state as sum of expected rewards

$$V_{\pi i}(s) = E\,[\, \sum_{t=0}^{(infinity)} R(s^t, a^t) \mid s = s^0, a^0 = \pi(s^0),]$$

Where $V_{\pi i}(s)$ is the value of the i^{th}policy.

Using the bellman equation, the above equation can be split into an expected reward at the current state, andthe value of the successive state, if followed policy π from the following state onwards.

$$V_{\pi i}(s) = E\,[\, R(s, a) \mid s^0, a^0] + \sum_{s'} P(s', a' \mid s, a)\, V_{\pi i}(s')$$

where s' is every subsequent state reached

policy π_i, P(s', a' | s, a) is the probability of transitioning to state s' and choosing action a' (according to the policy) on taking action 'a' from the current state 's'.

The value function of the deterministic optimal policy must satisfy the Bellman optimality equation.

$$V_*(s) = \max_\pi \{\, R(s, a) + \sum P(s', a' \mid s, a) \,.\, V_*(s') \,\}$$

The optimal policy is then the policy followed for the maximum value function. This policy is learned from Q-learning algorithm described in next section. Because the SU's gain is the jammer's loss, the same is modelled as a zero-sum game.

V. LEARNING ALGORITHM USED IN MODELING

A. Policy Iteration

requires complete knowledge of the model. It is also highly computationally intensive because it requires the computation of value functions of all potential immediate next states.

1. choose an arbitrary policy π'
2. loop
3. $\pi \leftarrow \pi'$
4. compute the value function of policy π:
5. solve the linear equation
6. $V_\pi(s) = R(s, \pi(s)) + \gamma \sum_{s' \in S} T(s, \pi(s), s') V_\pi(s')$
7. improve the policy at each state:
8. $\pi'(s) = \arg\max_a \left(R(s, a) + \gamma \sum_{s' \in S} T(s, a, s') V_\pi(s')\right)$
9. until $\pi = \pi'$

ϒ denotes the discount factor, by which more value is assigned to immediate rewards than to rewards far away in the future.
Q-learning is a temporal-difference learning method i.e., the value of a state is only used to back up to the previous state's value.

1. Initialize Q(s, a) arbitrarily
2. loop for each episode
3. initialize s
4. loop for each step of the episode
5. choose a from S using policy derived from Q (e.g., ϵ-greedy, softmax)
6. take action a; observe r and s'
7. $Q(s, a) \leftarrow Q(s, a) + \alpha [r + \Upsilon \max_a Q(s', a') - Q(s, a)]$
8. $s \leftarrow s'$
9. until s is terminal

Here, α is the learning rate, set between 0 and 1.
Value iteration requires a complete knowledge of analysis model, and thus it is computationally expensive. Also, this policy iteration is not used frequently in anti-jamming policy learning. For the same reason, the value iterations is not considered in the hypothesis presented in the following paper.

VI. CONCLUSION

In scenario of a single secondary user and a jammer learning method using Q-learning function, ϵ-greedy approach can be used. ϵ here, denotes the tradeoff between exploration and exploitation. With a small probability ϵ, the agent seeks to randomly choose one of the possible actions. With probability (1 - ϵ) the agent chooses to exploit already learned optimal behavior.
The three agents used in the model are the environment, the secondary user and the jammer. Both secondary user and the jammer keeps track of the states that have been jammed. They both choose from the pool of previously jammed or non-jammed channel, depending on their learning methods.
The environment agent is introduced with the sole purpose of consolidating the stats among all the three, which keeps the record of successful jams.
Using these preconditions and running the model, we get the following graph for 10 channels and 2 preoccupied by primary users.

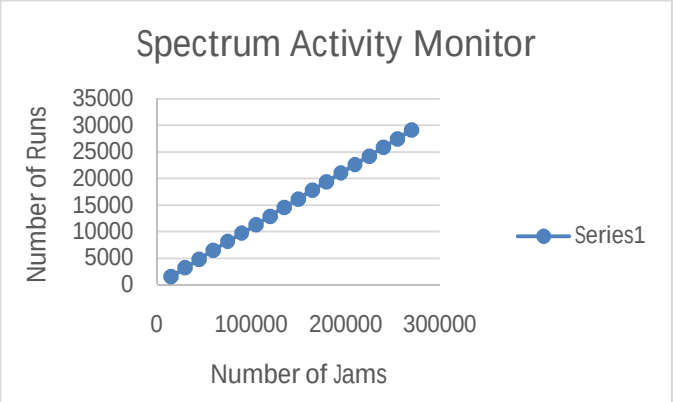

Fig 6.1 Spectrum Activity Monitor graphs as speculated by the environment agent using artificial intelligence analysis.

With just 20% of the channels being occupied by the primary user 1/3rd of the time, with an initial rate of being jammed 40% of the time, the rate should fall to around 12.1% by its 1000th run. Beyond the 6000th run of the game, the agents would have learnt how to best avoid each other's policies and stagnate to around 10.5% jamming rate.

Whereas when as much as half the available channels are occupied by a primary user simultaneously, 1/3rd of the time, the jamming rate must fall from around 35%, and stagnates to around 12.3% in 600,000 runs of the game.

REFERENCES

[1] Cisco USA.Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021, March 2017.
[2] Fei Hu, Sunil Kumar. Multimedia over Cognitive Radio Networks: Algorithms, Protocols, and Experiments. CRC Press 2014
[3] Lingyang Song, RistoWichman, Yonghui Li, Zhu Han Cambridge University Press, Full-Duplex Communications and Networks 02-Mar-2017
[4] Akyildiz, Ian F., et al. "A survey on spectrum management in cognitive radio networks." IEEE Communications magazine 46.4 (2008).
[5] Akyildiz, Ian F., et al. "A survey on spectrum management in cognitive radio networks." IEEE Communications magazine46.4 (2008).
[6] Kang, Xin, et al. "Sensing-based spectrum sharing in cognitive radio networks." IEEE Transactions on Vehicular Technology58.8 (2009): 4649-4654.
[7] Chen, Ruiliang, Jung-Min Park, and Jeffrey H. Reed. "Defense against primary user emulation attacks in cognitive radio networks." IEEE Journal on selected areas in communications26.1 (2008).
[8] Yu, F. Richard, et al. "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios." Military Communications Conference, 2009. MILCOM 2009. IEEE. IEEE, 2009.
[9] Sharma, Rajesh K., and Danda B. Rawat. "Advances on security threats and countermeasures for cognitive radio networks: A survey." IEEE Communications Surveys & Tutorials 17.2 (2015): 1023-1043.
[10] Chen, Changlong, et al. "A game-theoretical anti-jamming scheme for cognitive radio networks." IEEE Network 27.3 (2013): 22-27
[11] “Intelligent cognitive radio jamming - a game-theoretical approach”, K. Dabcevic, A. Betancourt, L. Marcenaro, C. S. Regazzoni, 201
[12] Watkins, Christopher JCH, and Peter Dayan. "Q-learning." Machine learning 8.3-4 (1992): 279-292.