Q Learning MDP Approach to Mitigate Jamming Attack Using Stochastic Game Theory Modelling With WQLA in Cognitive Radio Networks

[1]*S.Vimal, [2]Y. Harold Robinson,[3]M.Kaliappan,[4]Subbulakshmi Pasupathi and [5]A.Suresh

Abstract

Cognitive Radio network (CR) is a promising paradigm that helps the unlicensed user (Secondary User) to analyse the spectrum and coordinate the spectrum access to support the creation of common control channel (CCC). The cooperation of secondary users and broadcasting between them is done through transmitting messages in CCC. In case, if the control channels may get jammed and it may directly degrade the network's performance and under such scenario jammers will devastate the control channels. Hopping sequences may be one of the predominant approaches and it may be used to fight against this problem to confront jammer. The jamming attack can be alleviated using one of the game modelling approach and in this proposed scheme stochastic games has been analysed with more single users to provide the flexible control channels against intrusive attacks by mentioning the states of each player, strategies ,actions and players reward. The proposed work uses a modern player action and better strategic view on game theoretic modelling is stochastic game theory has been taken in to consideration and applied to prevent the jamming attack in CR network. The selection of decision is based on Q learning approach to mitigate the jamming nodes using the optimal MDP decision process

Keywords:*Cognitive Radio Networks, Stochastic Game, Wolf Q Learning Algorithm, Common Control Channels, Jammer*

[1*Corresponding Author] *Associate professor, Department of Computer Science and Engineering, Ramco Institute of Technology, Rajapalayam, Tamil Nadu, India (svimalphd@gmail.com)*

[2]*Post Doctoral Fellow, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India (yhrobinphd@gmail.com)*

[3] *Professor, Department of Computer Science and Engineering, Ramco Institute of Technology, Rajapalayam, Tamilnadu, India (kalsrajan@yahoo.co.in)*

[4] Assistant Professor(Senior Grade), *School of Computing, Scope, VIT University, Chennai Campus, Tamilnadu, India (subbu.psk@gmail.com)*

[5]*Associate Professor, Department of CSE, SRM University, Chennai , Tamilnadu, India (prisu6esh@yahoo.com)*

Received: Feb. 10, 2021, Revised: Mar. 08, 2021, Accepted: Mar. 25, 2021

I. INTRODUCTION

The preliminary focus of CR network makes the agents acting as primary users to monitor assignment of unutilised spectrum and dynamic access from licensed band in wireless networks. The CR network technology being a widespread technology enhances the network usage and makes the inefficient access of the spectrum to be properly utilised in the network. Moreover, in addition to various vulnerabilities, the CR network is susceptible towards various network breach activity performed by threats. Spectrum efficiency is a major factor to consider the utilisation in dynamic acces. Spectrum management is comprised to be of four functions such as Sensing, Decision, Mobility and Sharing. Secondary users communicate heterogeneously towards with one another Thestochastic game theory approach controls the jamming attack in the common control channel and share the control messages [20]. These control messages has the ability to provide responsible, access and sharing of channel, identifying neighbours and spectrum management. To analyse and fulfill these errands a distributed common control channel is needed to start the action for every SU. The most comprehensive attack happening in the physical layer is jamming attack which predominantly happens at physical layer and it should be counteracted immediately. Game theory approach is a mathematical modelling that helps us to analyse the interaction among logical players, and creates the ability to apply the strategy to a single player or user and between multiple users in a multilevel hierarchy to predict the activity or event undergoing in networks.

The stochastic game is proposed to be modelled between unlicensed SU and intruders. For reliable and efficient broadcasting and data communication in cognitive radio networks spectrum allocation is done using multiple channels based on the usage monitoring and to transmit control messages from various instances of time according to jammer strategy. Secondary users can predict the jamming attack by hopping among the multi-access channels and grouping of networks [1][2].

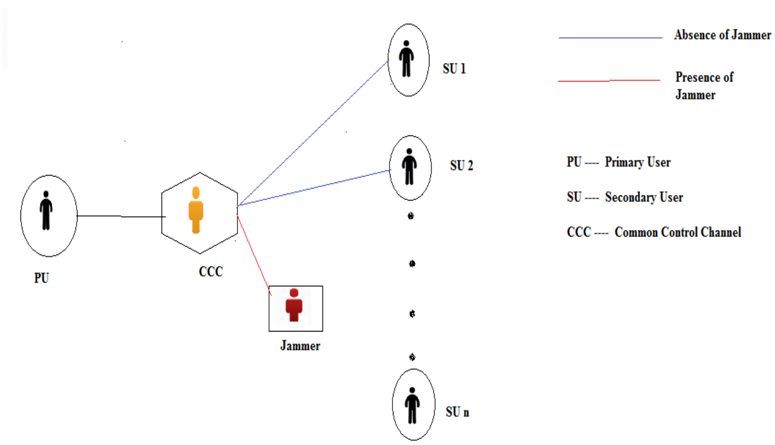

Fig1:Proposed Model

Fig 1 represents the transmission of data in presence of jammer and absence of jammer. Primary user can send the data to common control channel and by using this data get transferred to secondary user. Suppose if any attackers happen to attack the data between the common control channel and secondary user at this time using WQLA and stochastic game theory the attack is prevented. [3]

II. SYSTEM MODELS

The proposed system model includes a cluster of PUs, CRN, SUs, jammer and the timing limitations is considered to be slot and variant in nature.

2.1. Formation of CRN

In cognitive radio network(CRN), due to the non availability of predetermined and channelized structure, whereas the Secondary User heterogeneously cooperate and collide with each other and shares control messages where each links between the nodes implemented using different communication technology. These messages have played a vital role for gaining channel access, identifying neighbours and spectrum management. In proportion to meet this responsibility [4], Common Control Channels (CCC) should be available and accessible for each secondary user.

The jamming nodes in CCC are best analysed with Qlearning approach, it determines the state transition decisions to bridge the communication more efficiently.The optimal decision is estimated with the state space analysis of each and every individual. It handles the decision of states with stochastic rules and the jamming is analysed based on the reward function based on Markov Decision Process (MDP)[5].

2.2 Spectrum management

Nodes in the CRN can be communicated to pass over the control messages through spectrum functionality which comprises of four stages. A cognitive radio makes decisions on real time sensing on the band to be chosen during transmission phase. In Next stage, the unused frequencies in allocated band have been detected for the primary user at that particular time. After that, the primary user will gain access to the band and secondary have to vacate or lower the power on that band. At last, the idle frequencies can be optimized to minimize the collision among the secondary users.[6]

2.3. Deployment of jammer in network

As the primary and secondary users are in same channel, the performance maximization for both cannot be attained. The jammer or the secondary user tries to degrade the performance of primary so separate channels have been formed for them [7].Primary on one channel will communicate through spectrum to the secondary on another channel. In case of jammer, the interference takes place in its channel and the primary performance will not be decreased[8].

2.4. Attack Avoidance using stochastic model

Secondary users will select the channel from set of channels to transmit the data based on the available frequency or idle frequencies and neighbour information is obtained through the common synchronization parameter which will be used later to broadcast for updating the primary and secondary users[9].

III. STOCHASTIC GAME

A compromising game theoretic approach is multiagentmarkov decision process(MMDP) in which the actions can be determined by the agents. The proposed scheme consists of M stages and N stages. At every stage, the state of the game is specified and the agents predict the actions, strategy chosen by different players, hence the player reward may be calculated on the current state of action. In that proportion the game moves on to next stage and the action repeats[10]. In the stochastic model,the maximum number of distributed players are analysed with their actions and the cost function is performed for the effective analysis[11]. Therefore, the stochastic game is designed as $\left\langle J, S, Ag_{1....|N|}, T, JR_{1....|N|} \right\rangle$ [12] in which the elements are as follows.

i. Jamming Agent's State: In the proposed metrics jammer does not alter player actions and allocation of strategy based on the prevailing conditions. In this stochastic game agents acts as SUs to create CCCs and fight towards the jammer[13].

Jamming Agents are modelled as

$$J = \{S_1, S_2, S_3 ......S_K\} \quad (1)$$

ii. State Space: Jamming Agents has a separate state space (JSS) and comprises of 3 sections:

PU's states: Agents acting as SUs choose the player actions in a mentioned time slot of k th time slot and assumed to be mostly aware of the PU's states and based on the analysis of PU's state it has been defined with

$$JS_P^K = \left\{js_1^k, js_2^k, ..., js_n^k\right\} \quad (2)$$

Where $js_i^k \in \{0,1\}$ shows the ith Primary User availability denoting in the series of k th time slot. Henceforth each Primary User acts independently then Primary User's has a state space player size of 2^n

$$JS_P = JS_1 x JS_2 x.....JS_n \quad (3)$$

b) Slot count for Action: Based on time sensitivity the jammers identifies that common control channel is raising and hence the SU gathers the information that how much slots are succeeded in a set of channels to serve the CCC.[5].This set of channel is denoted by v^t and it varies from 0 to ∞. This prediction enables secondary users to jump to another hop before the another group of channels spots by jammer to attack CCC.Hence the slot count has been fixed to be v^t and it estimates the value till v_{max}. It has specified that$v^t \in V = \{0,1,2,3, \dots, v_{max}\}$. It is noteworthy to be mentioned that $w^t = 0$ denotes the time that jammer spotted secondary user common channel. [14]

c)predicting action of Jamming agent: The stochastic game with its state space is assumed to be of the agent's memory[15]. The Secondary Users uses the previous existing jammer agent memory to predict the action of agent. The agent's previous action from the memory is denoted as a^{t-1}, jamming agent's is defined by

$$J^K = (JS_P^K, a^{t-1}, v^t) \quad (4)$$

iii. Jamming Agents Action and metrics: Each of the Secondary User in each distributed timing parameter slot can choose the best channel allocation from N_s channel and also idle channels in the corresponding network is identified with in the network[16].The action of each of the primary user slot in maximum allocated channels is estimated with the number of SUs actions. The action of state space in the agents

$$Ag_t = \left\{Ag_t(1), Ag_t(2), ..., Ag_t(2^n)\right\} \forall t \in N \quad (5)$$

In (5), JA_t(i) mentions the determined space state of user in the t th agent with its action playing in the I th role of idle Primary user state space based on the agent metrics and the primary user size can be computed by

$$|Ag(js)| = |Ag(js_p)| = \sum_{i=0}^{L(js_p)} \binom{c(js_p}{i} \quad (6)$$

where$C(js_p)$ specifies the total average of primary channels which is idle in js_pth Primary User current space action state and it has been denoted with W(s)=min(Ns,C(s)) [17].The current scenario in the state space shows that no primary user is subject to be active and no predetermined actions in the state setup space[18].The primary state space is denoted by A_0 and the predicted size is $\sum_{i=0}^{n} \binom{n}{i}$

Subsequently the state space of the proposed game's can be defined as

$$S = JS_p X A_o X v \quad (7)$$

and its space size can be estimated as

$$|s| = |JS_p^t| . |A_o| . |V| = 2^n \left(\sum_{i=0}^{n} \left(\frac{n}{i} \right) . (v_{\max} + 1) \right) \quad (8)$$

It is measured to keep track of v^t and the same player action being used increases agents state action space size and the Secondary Users cooperation is assumed to be of in a coordinal ratio after the state space representation.

iv. Shifting Probability: Based on the individual players action role Primary users activity from actions n variation and it is to be analysed with probability of state transition rule[19].

v. Reward function of Jamming Agents: The reward function for the SU agents will be provoked with the aim of SU to battle against the masquerade and to increase the network performance in sharing the CCC messages between SU and agents[20]. This predominal increase may happen at the neighbourhood limit and it may lead to increase in reward function at CCC.Infavour of Secondary user to have a efficient performance to prelude the jammer and sensing report from CCC, it should develop a possible report of state space to increase the reward function[21]. If jammer finds all of the CCC,Secondary users are assumed to be of increase the cost of the reward function [22].The changes happening in the action may incur a sufficient loss in SU state flow and the cost is also assumed to be of low with the reward function specified to be of

$$JR_K^t = \frac{1}{B_k} \sum_{i=1}^{B_k} \left(\frac{c_{k1}}{L(js_p)} \right)_{n\left(a^t \neq a^{t-1}\right)} \quad H, K = 1,2 \ldots K \quad (9)$$

Where B_k,$C_{k,i}$ and H signifies the total mean average of distributed neighbors of kth user, count of Common Control Channels between kth and ith agent nodes and cost of hopping action respectively[23].

IV. Q learning Algorithm:

The objective of the RL model is to observe behaviour of neighbour nodes by predicting the time series analysis between the trustable nodes besides in the jamming area and Q learning algorithm is identified as an optimal solution for the jamming intervention. This proposed approach impacts the dynamic approach of the jamming nodes characteristics to analyse the jammed nodes.

Q-Learning is a structure free algorithm which helps to find an optimal action-selection policy for any given decision process. It activates the agent to learn the operating environment in an interactive manner. This proposed RL is embedded in SUs which comprises of three paradigms approach such asevent state, parametric action and recognisedreward. Events represent the situations or agents that are affecting the optimal decision. Since jamming node can affect the factors of the operating environment which leads to an agent to make wrong decisions and grovers algorithm may be a wide spread algorithm to analyse this concern too. Reward represents the profit of an agent in each state /action. Action represents the move taken by the agent in order to increase reward for each SU. Here State $ST_{i\in J,\delta}^{j} \epsilon ST$ represents the status value of a neighbour node $i\epsilon I$, in the environment where I refers the set of neighbour nodes of node j, the action $ac_{t\in T,t}^{j} \epsilon ac$ represents which neighbour node (t) to be selected by the source node (j) in each state and reward $rw_{p\in P,\delta}^{j}\left(ac_{t\in T,\delta}^{j}\right) = 1$ shows that in the action ac_t jamming nodes are absent in the operating environment where as negative reward value intimates that jamming nodes are there in the environment. Q-values of State/action pair i.e.$Q_\delta\ (ST_\delta\ , ac_\delta\ )$ will be estimated through Q-learning algorithm. At action ac_δ and time $\delta + 1$ intermediate rewards $Q_{\delta+1}\ (ST_{\delta+1}, ac_{\delta+1}\ )$ are received for any state/action pair. The future/discounted reward can be represented as $¥max_{ac\in AC}\ Q_\delta\ (ST_{\delta+1}, ac)$ for agent at time $\delta + 1, \delta + 2, \dots\dots$ this value will get updated in the Q-table.

The information about situation/event pairs and the future and present rewards are represented in a two dimensional matrix│ST│× │ac│. The agent decides to take an action with the optimal value **δ*** .While taking any action if agents get any positive reward then the Q-value gets increased. So, to maximize the collective reward (C **δ***) of all agents, the Q-value is given below.

$$C^{\boldsymbol{\delta}^*}(ST_\delta\ ) = max_{ac\in AC}\ Q_\delta\ (ST_\delta, ac)$$

Optimal can be given as, $\boldsymbol{\delta}^*(ST_\delta\ ) = argmax_{ac\in AC}\ Q_\delta\ (ST_\delta, ac)$

4.1Algorithm:

a) Examine present running state of agent ST_δ .
b) Verify the type of i whether it is exploitation or exploration.
c) Choose the best action depends on the result of i, calculate the collective reward for the agent.
d) Select action ac_δ .
e) Collect the reward for the state ST in time $\delta + 1$ in action ac_δ , $rw_{\delta+1}(ST_{\delta+1}\ )$.

V. WOLF Q learning Algorithm

Initialise the parameters to executeWoLF Q learning algorithm.At each initial stage Secondary users approach their strategy with N channels in CCC and the action is being utilised with the help of MA protocols[24].SU selects their neighbour in the network and transmit the control packets through broadcasting within the network, it estimates the reward of the network. The strategy may be unique in nature in each of the SU in the network, actions are also being analysed with the efforts of the channel to estimate the control information to be utilised among the practisioned usage parameters[25][26]. The primary user state can be analysed with the secondary users game action and the repository may be included from the cost of reward function[27].In Fig 4 and Fig 5 the value of (v) is estimated and secondary users predict the game state of action and update the Q values. Learning rate from Q values is computed and SUs update their player strategies based on the reward function[28][29].

5.1Algorithm:

1. Initialize the metrics

(a) Assume the initial learning rate as α ,δ_w, δ_I , and discount factor of the learning to be β and ε
(b) Let time slot t = 0
(c) For all s ∈ S, $a^1 \in A^1, a^2 \in A^2, \dots, a^n \in A^n$
Let $Q_o^t(s, a^1, a^2, \dots, a^n) = 0$
$\pi_o^i(s, a^i) = \frac{1}{|A^i|}$, $\overline{\pi}_o^i(s, a^i) = \frac{1}{|A^i|}$,
C^i(s) =0
(d) Initialize s_0
(e)select action $a^1, a^2, \dots, a^n$based on distributed probability[13] π (s,a) with space transition in state s_0

2. Loop

(a) Execute action $a^1, a^2, \dots, a^n$ in state s_t
(b)Examine event reward $(r_t^1, \dots, r_t^n)$ and updated state s_{t+1}

(c) Estimate the values of Q using the WOLF rule having values i=1,2,…,n
$Q_{t+1}^{i}(s,a^{1},\ldots,a^{n})=(1-\alpha)Q_{t}^{i}(s,\vec{a})+\alpha[r_{t}^{i}+\beta.\prod_{i=1}^{n}\pi^{i}*(s_{t+1},a^{i}),Q_{t}^{i}(s_{t+1},\vec{a})]$

(d) Examine mean policy $\overline{\pi}^{i}$ for all values of i=1,2,….,n

$C^{i}(s)=C^{i}(s)+1\forall a' \in A^{i},\overline{\pi}^{i}(s,a')=\overline{\pi}^{i}(s,a')+\frac{\overline{\pi}^{i}(s,a')-\overline{\pi}^{i}(s,a')}{C^{i}(s)}$

(d) Update π^{i}(s,a) and δ

(e) Predict the next action for the subsequent new states s_{t+1} for all π^{i}(s,a)

3. Loop end

4. SIMULATION AND NUMERICAL RESULTS

The simulations has been performed based on the proposed game and WOLF Q learning .The value of H representing the distribute neighbour information is assumed to be of small and hence it has been encouraged to jump over various hopping to new actions and the channels in CCC will be decreased automatically as shown in fig 2[30]. When the value of H increases, secondary users are subject to alter the player action,strategies and jammer absorbs the data in CCC and blocks the contents in CCC[31]. The assignment of value H has been fixed in metrics to analyze and predict the outcomes using WoLF Q learning algorithm and it has been defined with α = Number of active CCC Links / Total number of CCC Links [32][33]. The study metrics focuses on the jammer indication in the CCC and most of the PU are assumed to be non idle throughout the process.[34][35].

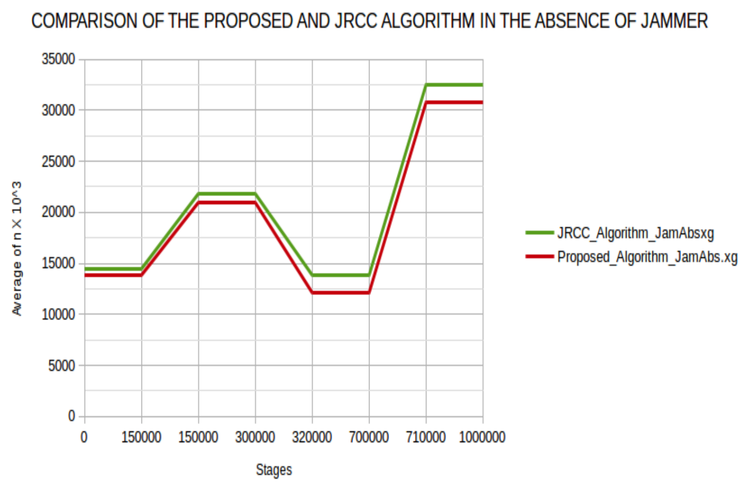

Fig 2: Estimation of Non Jammer network with JRCC and proposed Algorithm

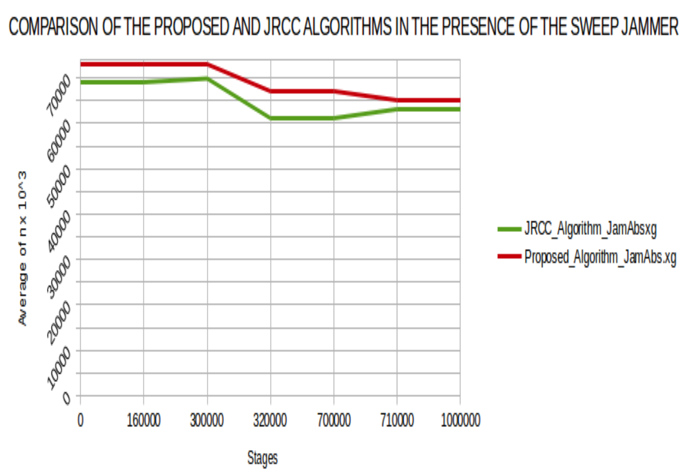

Fig 3:Estimation of Jammer network with JRCC and proposed Algorithm

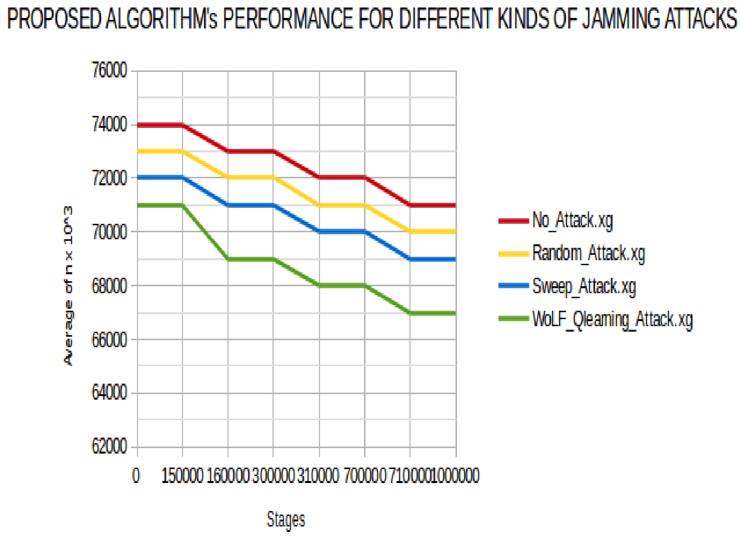

Fig 4: Proposed Algorithm's Performance for various Jamming attack

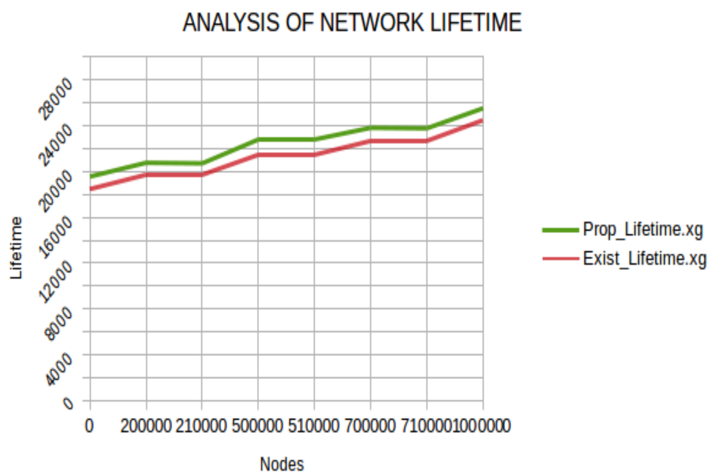

Fig 5:Analysis of Network Lifetime

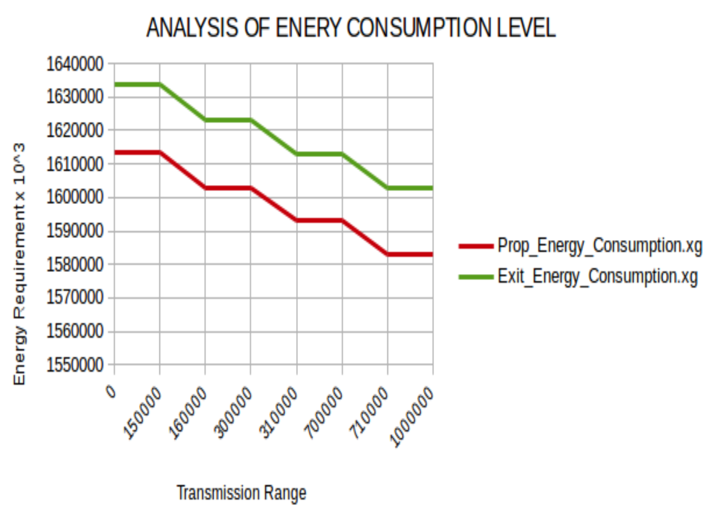

Fig 6: Analysis of Energy Consumption Level

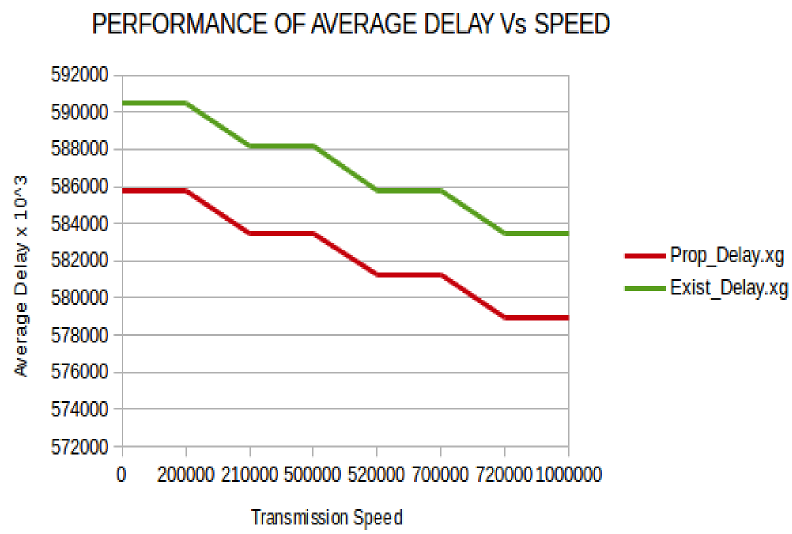

Fig 7: Performance of Average Delay vs Speed

VI. CONCLUSION:

In this proposed approach, the security in CRN to prelude the jamming attack has been rectified using stochastic game approach[36]. The proposed algorithm, the action prediction to the same state space, the time slot and reward function cost effectiveness is predicted using the neighbour SU, it reduces the attacks more efficiently too[37].JRCC and WOLF Q learning algorithm outlines the jammer control to be neutralised and error free transmission in CCC. In Fig 6 and Fig 7, the energy consumption level and delay spread are being measured using the above algorithm [38][39]. The Q learning approach supports the stochastic game modelling to enhance in a way of state prediction for SU to make a optimal decision in the state space prediction[40].

VII. References

[1] SiamakDastangoo, Carl E. Fossa, Youngjune L. Gwon and Hsiang-TsungKung " Competing Cognitive Resilient Networks", IEEE Transactions on Cognitive Communications and Networking ,Volume: 2, Issue: 1, 2016 .

[2] Brandon F. Lo and Ian F. Akyildiz"Multiagent Jamming-Resilient Control Channel Game for Cognitive Radio Ad Hoc Networks",IEEE International Conference on Communication,2012.

[3] AmrutaP.Chaudhary, SharvariS.Tantarpale, Badnera, Amravati India, SeemaH.Rajput, Kondhwa "A Novel Approach to Secure Cognitive Radio Network using Dynamic Quiet Period Scheduling for Detection Of Control Channel Jamming Attack"in International Journal of Innovative and Emerging Research in Engineering Volume 3, Special Issue 1, ICSTSD,2016.

[4] FetenSlimeni, Bart Scheers, ZiedChtourou and Vincent Le Nir "Jamming mitigation in cognitive radio networks using a modified Q-learning algorithm" IEEE Conference Publications,2015.

[5] Changlong Chen and Min Song, University of Toledo ChunSheng Xin "A Game-Theoretical Anti-Jamming Scheme for Cognitive Radio Networks"IEEE Networks, Volume: 27, Issue: 3, 2013.

[6] [Karin Sallhammar, Bjarne E. Helvik, Svein J. Knapskog Centre for Quantifiable Quality of Service " On Stochastic Modeling for Integrated Security and Dependability Evaluation" in IEEE Conference Publications,2006

[7] C Manogna.KNaik, "Detection of Jamming attack in Cognitive Radio Networks",International Journal of Recent Advances in Engineering & Technology (IJRAET),2014.

[8] Balogun ,A. Krings "On The Impact of Jamming Attacks on Cooperative Spectrum Sensing in

Cognitive Radio Networks” ACM,2013.

[9] Ian F. Akyildiz , Brandon F. Lo , Ravikumar Balakrishnan, Cooperative spectrum sensing in cognitive radio networks: A survey, Physical Communication, v.4 n.1,March, 2011, p.40-62,

[10] Asterjadhi, M. Zorzi, JENNA: A Jamming Evasive Network coding Neighbor discovery Algorithm for Cognitive Radio Networks, In IEEE ICC Workshop on Cooperative and Cognitive Mobile Networks (CoCoNet3), Cape Town, South Africa, May, 2010

[11] KresimirDabcevic,AlejandroBetancourt,LucioMarcenaro and Carlo S Regazzoni“Intelligent cognitive radio jamming-a game – theoretical approach”,Springer,2014.

[12] FetenSlimenia, Bart Scheersb, ZiedChtouroua, Vincent Le Nirb, RabahAttia “Cognitive Radio Jamming Mitigation using Markov Decision Process and Reinforcement Learning”,The International Conference on Advanced Wireless, Information, and Communication Technologies,2015.

[13] B. F. Lo“A survey of common control channel design in cognitive radio networks”,IEEE Physical Communication,2011.

[14] I. F. Akyildiz, W.-Y. Lee, and K. R. Chowdhury “Crahns: Cognitive radio ad hoc networks,”AD hoc networks,2009.

[15] A. Masri, C.-F. Chiasserini, and A. Perotti “Control information exchange through uwb in cognitive radio networks,” in International Symposium on Wireless Pervasive Computing (ISWPC),2010.

[16] D. L. Wasden, H. Moradi, and B. Farhang-Boroujeny “Design and implementation of an underlay control channel for cognitive radios”inIEEE Journal on Selected Areas in Communications,2012.

[17] J. Hu M. P. Wellman "Nash q-learning for general-sum stochastic games" ,Journal of Machine Learning Research,vol. 4 no. 6, 2003, pp. 1039-1069.

[18] M. Bowling M. Veloso "M (2002) multiagent learning using a variable learning rate" ,Artificial Intelligence,vol. 136, no. 2, 2002, pp. 215-250.

[19] S. Abdallah V. Lesser "A multiagent reinforcement learning algorithm with non-linear dynamics" ,Journal of Artificial Intelligence Research,vol. 33 no. 3, 2014, pp. 521-549.

[20] Albert H. R. Ko R. Sabourin F. Gagnon "Performance of distributed multi-agent multi-state reinforcement spectrum management using different exploration schemes" ,Expert Systems with Applications An International Journal,vol. 40 no. 10, 2013, pp. 4115-4126..

[21] K. Bian, J.-M. Park, and R. Chen “A quorum-based framework for establishing control channels in dynamic spectrum access networks,”Proceedings of the 15th annual international conference on Mobile computing and networking, ACM,2006

[22] J. Zhao, H. Zheng, and G.-H. Yang “Distributed coordination in dynamic spectrum allocation networks,” First IEEE InternationalSymposium on New Frontiers in Dynamic Spectrum Access Networks, IEEE,2007

[23] R.S. Sutton A.G. Barto,” Introduction to Reinforcement Learning”, MIT Press, 1998.

[24] P.Vidhyarani ,S. Vimal,”Defense against Routing towards Primary User attack in Cognitive Radio Networks”, TCIFES 2015- International Conference on Technological Convergence For Information, Food, Health and Energy Security- 1 & 2 May 2015.

[25] S.Vimal,L.Kalaivani,”Secure Authentication mechanisms to mitigate PUE attacks for mobile Cognitive Radio networks” IEEE,IEEE CSI,IEEE-ITS & BRNS sponsored International Conference on Computing Technologies and Intelligent Data Engineering, 7-9 Jan 2016.

[26] M Kaliappan, B Paramasivan,”Enhancing secure routing in mobile ad hoc networks using a dynamic bayesiansignalling game model”,Computers& Electrical Engineering 41, 301-313,2015.

[27] Q. Mahmoud, Cognitive Networks: Towards Self-Aware Networks. John Wiley and Sons, 2007. . Alhakami, A. Mansour, and G. A. Safdar, “Spectrum Sharing Security and Attacks in CRNs: a Review,” International Journal of Advanced Computer Science and Applications(IJACSA), vol. 5, no. 1, 2014, pp. 76–87.

[28] Vimal, S., Kalaivani, L. &Kaliappan, Collaborative approach on mitigating spectrum sensing data hijack attack and dynamic spectrum allocation based on CASG modeling in wireless cognitive radio networks, M. Cluster Computing (2017),https://doi.org/10.1007/s10586-017-1092-0

[29] A.C. Talay D.T. Altilar "Self Adaptive Routing for Dynamic Spectrum Access in Cognitive Radio Networks" ,J. Network Computer Applications,vol. 36 no. 4,2013, pp. 1140-51.

[30] J.Y. Yu P.H.J. Chong "A Survey of Clustering Schemes for Mobile Ad Hoc Networks" ,IEEE Commun. Surveys &Tutorials,vol. 7, no. 1, 2005, pp. 32-48.

[31] K.-L.A. Yau et al. "Clustering Algorithms for Cognitive Radio Networks: A Survey" ,J. Network Computer Applications,vol. 45, 2014, pp. 79-95.
[32] M. Youssef et al. "Routing Metrics of Cognitive Radio Networks: A Survey" ,IEEECommun. Surveys &Tutorials,vol. 16, no. 1, 2014, pp. 92-109 ,.
[33] X. Chen B. Fu Y. He M. Wu "Timesharing-tracking framework for decentralized reinforcement learning in fully cooperative multi-agent system" ,AutomaticaSinica IEEE/CAA Journal of,vol. 1 no. 2 April 2014, pp. 127-133.
[34] M. Bowling M. Veloso "M (2002) multiagent learning using a variable learning rate",ArtificialIntelligence,vol. 136 no. 2 2002, pp. 215-250.
[35] Q. Zhao L. Tong A. Swami Y. Chen "Decentralized cognitive mac for opportunistic spectrum access in ad hoc networks: A pomdp frame-work" ,Selected Areas in Communications IEEE Journal on,vol. 25 no. 3, ,April2007, pp.589-600.
[36] Dr.E.Mariappan,et.al.," Energy Efficient Routing protocol using Grover's Searching algorithm using MANET" Asian Journal of Information Technology,Vol:15,issue:24,2016.
[37] P.Subbulakshmi,et.al.,,"Secure data packet transmission in manet using enhanced identity-based cryptography (eibc)".International Journal of New Technologies in Science and Engineering Vol. 3, Issue 12, Pg:35-42,Dec 2016.
[38] Subbulakshmi,p.,et.al., "Honest Auction Based Spectrum Assignment and Exploiting Spectrum Sensing Data Falsification Attack Using Stochastic Game Theory in Wireless Cognitive Radio Network", Wireless Personal Communication (2017). https://doi.org/10.1007/s11277-017-5105-3.
[39] Vimal, S., Kalaivani, L.,Kaliappan,M.,Suresh,A., Xiao-Zhi Gao, Varatharajan ,R., Development of secured data transmission using machine learning based discrete time partial observed markov model and energy optimization in Cognitive radio networks, Neural Comput&Applic (2018), DOI: 10.1007/s00521-018-3788-3.
[40] Madhumitha Ramamurthy, Y. Harold Robinson, S. Vimal, A. Suresh,"Auto encoder based dimensionality reduction and classification using convolutional neural networks for hyperspectral images,Microprocessors and Microsystems, Volume 79,2020,103280,ISSN 0141-9331,https://doi.org/10.1016/j.micpro.2020.103280.

저자 소개

S.Vimal

2021 : Associate professor in Dept. Of Computer Engineering, Ramco Institute of Technology,Rajapalayam,Tamilnadu,India

Research Interests : AI, Wireless Communication and Big Data Analytics

Y. Harold Robinson

2020 : Post Doctoral Fellow, School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India

Research Interests : AI, Wireless Communication and Big Data Analytics

M.Kaliappan

2018 : Professor, Department of Computer Science and Engineering, Ramco Institute of Technology, Rajapalayam, Tamilnadu, India

Research Interests : AI, Wireless Communication and Big Data Analytics

P.Subbulakshmi

2020 : Assistant professor(Senior Grade), School of Computing, Scope, VIT University, Chennai Campus, Tamilnadu, India

Research Interests : AI, Wireless Communication and Big Data Analytics

A.Suresh

2021 : Associate professor, Department of CSE, SRM University, Chennai , Tamilnadu, India

Research Interests : AI, Wireless Communication and Big Data Analytics