Reinforcement based Cognitive Algorithms to Detect Malicious Node in Wireless Networks

G Sunilkumar, Thriveni J, K R Venugopal
Department of CSE, University Visvesvaraya College of Engineering (UVCE), Bangalore, India

Manjunatha C
Department of CSE, Alpha College of Engineering, Bangalore, India

L M Patnaik
Honorary Professor, Department of Computer Science, Indian Institute of Science (IISc), Bangalore, India

ABSTRACT
The growth of wireless communication technologies and its applications leads to many security issues. Malicious node detection is one among the major security issues. Adoption of cognition can detect and Prevent malicious activities in the wireless networks. To achieve cognition into wireless networks, we are using reinforcement learning techniques. By using the existing reinforcement techniques, we have proposed GreedyQ cognitive (GQC) and SoftSARSA cognitive (SSC) algorithms for malicious node detection and the performances among these algorithms are evaluated and the result shows SSC algorithm is best algorithm. The proposed algorithms perform better in malicious node detection as compared to the existing algorithms.

Keywords
Malicious node detection, Reinforcement learning algorithm, Cognition, Wireless networks.

1. INTRODUCTION
In Recent days, lots of developments are happening in wireless networks. Since wireless environments reduces the infrastructure and easy to adopt for all the applications, popularity is increasing rapidly. But it is more vulnerable for the security threats. Malicious node detection is one of the major security issues. To detect the malicious activities in the network, we are adopting cognition to the wireless networks. So that the wireless networks becomes intelligent. To impart the cognition to the wireless networks; machine learning algorithms are used.

There are different types of machine learning algorithms namely, unsupervised learning, supervised learning and reinforcement learning. Here, reinforcement learning algorithms are used for learning. In reinforcement learning, there are different learning techniques are existing [1]. Namely, Softmax, SARSA, Greedy and Q-learning techniques. Among these techniques; combination of Softmax and SARSA technique performs better than the combination of Greedy and Q learning techniques with respect to malicious node detection in wireless networks. Again this performance can be further increased with the concept of cognition. Cognition mainly works on the concept of Observe, Orient, Decide and Act (OODA) loop. If the cognition is achieved for the existing wireless networks then, that network will become smart network.

In reinforcement learning; depending on the interactions carried out in the environment, computational approach is used for learning. Reinforcement learning algorithm enables all their participants to undergo learning process to improve their performance by evaluating the reactions on their past actions.

1.1 What is Cognitive Network?
Cognitive Networks can be defined as an intelligent network encompassing the cognitive process which can perform a goal of achieving current network circumstances, planning, taking certain decision, acting on those perceived conditions, extracting or learning from the consequences of its previous or current actions, all while following end-to-end goals.

The conception of cognitive networks has been vigorous around the cooperative consciousness of the wireless and networking researching societies for a while. In order to achieve the seamless adaptation of radio link parameters, opportunistic use of underutilized spectrum, to get the higher flexibility in modulation and waveform Selection, the scientific or research society has seen an extraordinary progress in system or network development by implementing cognitive techniques. Cognitive networks are the best solution to attain the above mentioned requirements.

The important component of cognitive networks is its Cognition Loop that senses the circumstances, plans the actions to be taken and even according to input from sensors and network policies. It decides which solution or decision might be most effective for achieving end-to-end purpose. These characteristics facilitates the network systems to learn from the past about the situations, plans, decisions, actions and then using experiences for improving the decision in future. A number of researchers have presented their optimistic view about cognitive networks in near future. Mitola [2] summarizes how his cognitive radios could communicate in the circumstance of system-level scope of a Cognitive Network. Saracco [3] indicates towards as the future of information technology. It postulates that the convergence of network intelligence from scheming resources to perceptive user requirements would assist "flatten" the network by moving network intelligence further out towards the edges of the network. Some other discusses cognitive network in optimistic way and with respect to future mobile Internet Protocol networks, arguing that the context sensitivity of these networks could have as interesting an application to networks as cognitive radios had to software defined radios.

1.2 Cognition Cycle – OODA Loop
OODA Loop (Observe, Orient, Decide, and Act) is a model that was developed by US Air Force. The implementation of the assessment making process may be viewed as involving the cycling through four individual but mutually reliant stages: Observation, Orientation, Decision and Action, these stages have come together to be known as OODA loop.

Now a day OODA (Observe-Orient-Decide-Act) loop is a main model of command and control. In a challenge to clarify why American fighter pilots were more successful than their

adversaries in the Korean War [4] the OODA loop was first developed and its work was to provide military leaders with a method for making decisions and estimating their impact. OODA Loop is represented in Figure 1.

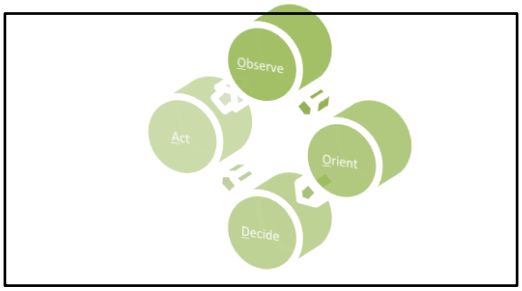

Figure 1: The Cognition Cycle / OODA Loop

Observe: When a venture is engaged in disagreement like they have differences in determining how to lead, or respond to a competitive change then the first action is to observe the situation i.e. to take the unprocessed data concerning its own status, its marketplace, operational environment, its competitors and its customers. Sometimes a venture keenly seeks that information ("pulls" information), sometimes that information is forced ("pushed") upon it. Experience plays a great role in what we observe and our conclusions regarding our environment.

Orient: After observing the situation, the venture now orients itself i.e. performs certain investigation and makes certain estimation, hypothesis and verdict about the situation in order to generate a solid model or image of the total environment. In simple terms we can say that the venture makes an effort to determine what the changing situation means to it and how it will be impacted. The orientation stage of any decision cycle is the key player in decision making as it involves collecting, mixing, and processing all the information available and data to determine truth.

Decide: The venture next decides what to do; which is based on the orientation. Despite that decision is autonomous or involves others, which include customers, partners, regulators, suppliers or even competitors and whether that decision takes the shape of an instant action or involves the formation of a planned plan and response which is delayed. The decision part of the loop is where the leadership is proved up, not by keeping all the answers but by leading the organization.

Act: Finally, the decision is put into action. This includes spread the decision, to manage its execution, and observing the results of the action through the feedback. Action is more than doing something it is about doing something with keeping the result in mind. It is about monitoring the result and making an evaluation about whether you accomplished the proposed result or not, if not then what are the things that go wrong and how to conquer them.

This completes one OODA cycle, and makes the venture again to returns to the observation phase.

1.3 Design challenges of Cognitive Networks

Network Complexity: When the wireless link is introduced in the network it just increases the complexity of the network as the total no of nodes as well the alternate routes and the number of protocols, the communication mediums. Radio signals frequently get fade with signal interference but the wireless links above the radio channels and the nodes joins the network in ad hoc manner so that mesh type architecture can be developed. Mobility in the wireless networks allows them to change their point of contact, location, affecting the path location and make it difficult to attain stability in a limited timeframe. Therefore, the network optimization must be added as functionality for healing itself in cognitive network.

Sensing the Environment: The cognitive controller must be able to get the sensorial information of the surrounding environment and nodes under communication. This information is likely to be existing in the form of measurement which includes different types such as noise measurement, traffic information and the time and location coordinates.

Understanding the Network Status*:* It is the duty of network controller to detect the status of the network and what is the effect of different types of configuration settings on the performance of the network. It is possible to provide the controller with this knowledge by simply hard coding the actions to be taken with respect to the different network condition. Though a cognitive controller must have the ability to learn such dependencies and relieving the effort to provide the knowledge needed to the controller.

Prediction: Knowledge about the past and current status of the network can be provided by the environmental measurement; though, the network configuration must be selected so that it is best in comparison to the status of the network in future. To determine the future status of the network is not an easy task, since there are many outside factors like variation in the network load generated by the user, outside interference, etc. also play key role in the determination of future status of the network. Due to this there must be some prediction strategies which must be adopted.

Decision Making: As soon as the controller gets a better functional understanding of inter-dependencies between the status of the network and the performance with respect to various network settings and configurations and thus it is facilitated with certain robust and proper way for predicting the evolution of network or communication environment, then while it needs to execute its decisions. Here it has been intended to express that in spite of various facilitations the cognitive networks needs to choose the most beneficial network configurations. Based on the network configuration and its complexity and even depending on the characteristics of the provided solution space of the enhancement or optimization problem suffered by the network controller, some effective and robust strategy must be adopted for facilitating a practical decision making process.

Network Heterogeneity: The applications like internet employs various combinations of transmission technologies, their applications and transmission protocols and the internet protocols doesn't accounts for layer in transmission protocols for having network heterogeneity. In order to improve the performance of the network, the connectivity is divided into certain segments and each segment is optimized for a specific domain. The optimization in performance needs an effective awareness of underlined technologies for transmission between transmitter and receiver nodes over the entire communication path. Across multiple domains, the enhancement technologies or optimization techniques must be distributed in nature and it must have achieved the goal that has been defined at the connecting nodes.

Quality of service (QoS): In order to facilitate QoS requirements made by a number of applications as well as

users, it is required to have a provisioning of limited delay bonds and meanwhile the bandwidth unavailability needs the implementation of reservation control mechanism (RCM).

1.4 Motivation

Wireless networks are more vulnerable to security issues hence lot of research is required to provide better security. Malicious node detection is one of the major security issues. To detect the malicious activities, the proposed concept utilizes reinforcement learning techniques to train the wireless networks and to achieve the cognition. There are different reinforcement learning techniques are existing and these techniques are evaluating with respect to malicious node detection; with and without cognition. We are proposing new GreedyQ Cognitive (GQC) algorithm and SoftSARSA cognitive (SSC) algorithm to detect malicious node and to evaluate among these algorithms to show the better performance than the existing algorithms.

1.5 Organization

The next section of this paper explains the Literature survey, and System model is explained in section III and section IV gives the Implementation, result analysis is explained in section V, conclusions are given in the next section.

2. LITERATURE SURVEY

In [2] a cross-layer altruistic differentiated service protocol (ADSP) for dynamic cognitive radio networks was employed, similar to [3] for quality of service provisioning in CRNs with selfish node coexistence. It could not address the issues of diverse communication environment like in Ad hoc network but it was successfully delivered by COOPON. Authors utilized the advantages of Ad hoc network like its autonomous and cooperative characteristics for better detection reliabilities. Their work exhibited tremendous enhancement in the detection accuracy of selfish attack detection and it was found to be more than 97 percent.

Yongkun Li et al., [6] proposed an optimized strewn detection framework that could be executed by incorporating legitimate network nodes in highly interactive network for identifying the malicious neighboring nodes and attacks like pollution attacks. The authors have employed the developed system for the applications like P2P streaming networks, WMNs and OSNs, and performed well for detecting malicious nodes. This approach was of course an indispensable tool for maintaining the viability of interactive networks but it could not deliver the secure DTN routing towards efficient trust establishment. To overcome these limitations, authors [7] have introduced an approach iTrust, that encompasses the Trusted Authority (TA) for judging the behaviour of nodes on the basis of collected routing evidences as well as probabilistically checking. They used the game theoretical analysis for ensuring the security of DTN routing at a reduced cost. Similarly, in [8] authors have used parallel fusion sensing architecture. By considering these architectures and analyzing them, results shows optimized and reduced transmission overhead incurred by misbehavior detection and detects the malicious nodes effectively.

Nicola Baldo et al., [9] came up with a highly robust and distributed cognitive network access approach having goal for facilitating the best QoS factor with both radio link as well as core network performances. In their work, they have developed a framework, a modular design was demonstrated with generic a technology independent system approach based on fuzzy logic. The system shows significantly better results for cognitive access approach as compared to state of arts techniques [10] [11] [12] and [13] that do emphasizes and considers the 802.11 specific matrices, in terms of both overall performance and fairness. Still these approaches could not deliver the ultimate solution for CRN optimization with other communication factors and circumstances of communication in radio network.

Ryan W Thomas et al., [14] identified three dominant factors which are required to be considered for forming a cognitive network. These factors are the characteristics of the decision-making elements, the details of computational state accessible to those entities, and the extent of control they posses for estimating the consequences of its design tradeoffs, the author have developed a metric known as "price of a feature." This network metric quantifies the influence of those characteristics on the CNs having the objectives of optimizing the lifetime of a multicast flow in a wireless environment. The results obtained presented that despite of the count of receivers, the expected price of partial control increased as the total of cognitive control is reduced. According to it the cognitive control and cognitive process could not enhance the multicast trees unless the network is having higher than 20% cognitive control.

G Sunilkumar et al., [15] presented a research work that not only Monitors activity of user node but also performs an effective function of taking preventive measures if user node transactions are found to be malicious. In this research work the intelligence in cognitive engine has been realized using self-organizing maps (CSOM). In order to realize the CSOMs Gaussian and Mexican Hat neighbor learning functions have been evaluated. The research simulation made in this work, proves the efficiency of Gaussian Learning function is better for cognition engine. The cognition engine being considered in this research work is evaluated for malicious node detection in dynamic networks. In this work the implemented concept results in higher Intrusion detection rate as compared to other similar approaches.

3. SYSTEM MODEL

The proposed System model is shown in Figure 2. In the proposed system model, the wireless sensor network is considered. Initially the wireless sensor network is not trained hence the percentage of intrusion detection is less. Here, in the proposed system two cognitive Reinforcement learning algorithms are used to train the wireless sensor network to get better percentage of intrusion detection. Namely, SoftSARSA Cognitive (SSC) algorithm and GreedyQ Cognitive (GQC) algorithm. During training phase, the network gets trained with the reinforcement learning parameters and pre-defined transactions. Once the wireless sensor network got trained, it becomes intelligent; this intelligent network is called as cognitive wireless sensor network (CWSN). The trained features are stored in the network repository of the CWSN. If the node transactions are done after the training phase, then the new transactions gets monitored by the CWSN and comparison with the predefined transactions and the new transactions will be calculated to detect the percentage of orientation. If the orientation is more than the threshold, then it will be considered as malicious else it is normal transaction. This decision will be taken by the CWSN. Depending on the decision made by the CWSN, the necessary action will be taken by the action methods on malicious node. Here, action methods are implemented using greedy and softmax methods. This updated status for the new transactions is given to the cognitive learning algorithms to train the CWSN again. This process is called as OODA Loop concept and it is repeated continuously to detect the malicious node.

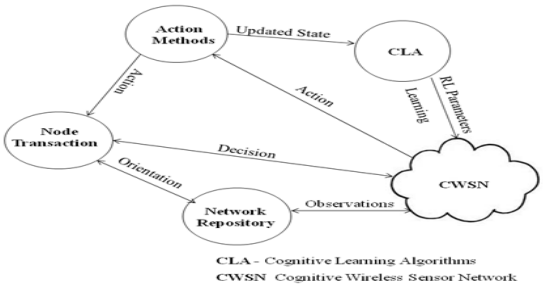

Figure 2: System Model

4. IMPLEMENTATION

4.1 GreedyQ Cognitive (GQC) Algorithm

In GQC Algorithm the inputs are the set of WSN nodes states set ($X = x1, x2, \ldots . xn$) and set of Actions ($Y = y1, y2, \ldots . . yn$). The output will be "an estimated best node cooperation RL approach in Cognitive WSN". First we need to initialize the function M(X, Y) and calculate the greediest probability as explained in the step 3, the obtained states from step 3 will be reinitialized and repeat for each iteration and initialize the new values to X. This iteration will be repeat for choosing Y and assigning the Action to the Y and observe the reward R, and also the new states say X'. Using the previously observed values we need to calculate the updated state and action function M(X, Y) using the step 7 equation. This repeats until it reaches the maximum action.

This is off-policy algorithm for Temporal Difference Learning. The method is still has an effect in that it determines which state-action pairs are visited and updated. However, all that is required for correct convergence is that all pairs continue to be updated. This algorithm is proved that the given sufficient training using the ε-greedy action method, the algorithm concludes with probability 1 to a close approximation of the action-value function for an arbitrary target method. The GQC handles or take care of all the problems of node transactions, rewards without any additional adoption. The GQC Algorithm learns the optimal methods even when the actions were random methods.

GreedyQ Cognitive (GQC) Algorithm:

Input: In the WSN, the set of nodes states 'X' and set of nodes Actions 'Y'

Output: An Estimated Best node Cooperation in Cognitive WSN

Step 1: Begin

Step 2: Initialize the function $M(X, Y)$

Step 3: $Xn + 1 = (kXn + b) mod\ z$

$\epsilon \leftarrow Xn + 1$

Step 4: Re-Initialize set $M(X, Y)$ arbitrarily Where X from Step 3

Step 5: Repeat for each Iteration

Initialize X

Step 6: Repeat for each Iteration

Choose Y from X using the step 5

Take action Y, observe R, and X'

/*---Calculation for new function M(X, Y) ----*/

Step7: $M(X, Y) \leftarrow M(X, Y) + k[R + \delta Max(k), M(X', Y') - M(X, Y)]$

$X \leftarrow X'$;

Repeat until X reaches maximum action

Step 8: end.

This algorithm uses the same input, that is the set of WSN nodes states set ($X = x1, x2, \ldots . xn$) and set of Actions ($Y = y1, y2, \ldots . . yn$). The output will be "an estimated best node cooperation RL approach in Cognitive WSN". First we need to initialize the function M(X, Y), calculate the least probability that is $(1 - \epsilon)$, reinitialize the function M(X, Y) for each action assign the ranks or weight to each action as stated in the step 3. Using the ranks we need to initialize the function $M(\zeta, Y)$ arbitrarily, this iteration will be repeat, initialize the X from ranks obtain and choose the action Y from newly chosen states X. Take the new action Y, observe the rewards R and new states X' from new state X' again we need to choose the action Y. Finally compute the resultant function M(X,Y) using the step 7. This process will be repeat until X reaches the maximum actions.

The SSC Algorithm is an on-policy TD Algorithm. The main difference between GQC and this algorithm is the maximum reward points are not necessarily used for updating the RL values. Instead, a new action, and the reward, is selected using the same method that determined the original action. The convergence properties of the SSC algorithm depend on the nature of the method's dependence on GQC, SSC converges with probability 1 to an optimal method and action-value function as long as all state-action pairs are visited an infinite number of times and the method converges in the limit to the greedy method and Proven that this algorithm is much better than the GQC algorithm.

SoftSARSA Cognitive(SSC) Algorithm:

Input: In the WSN, the set of nodes states 'X' and set of nodes Actions 'Y'

Output: An Estimated Best node Cooperation in Cognitive WSN

Step 1: Begin

Step 2: Initialize the function $M(X, Y)$

Step 3: $Xn + 1 \leftarrow (1 - \epsilon)$

Initialize $M(X, Y)$;

For each action Y

$\zeta \leftarrow X$

Step 4: Initialize $M(\zeta, Y)$ arbitrarily Where ζ from Step 3

Step 5: Repeat for each Iteration

Initialize X, $X \leftarrow \zeta$

Choose Y from X

Step 6: Repeat for each Iteration

Take action Y, observe R, and X'

Choose Y from X' from step 5

/*---Calculation for new function M(X, Y) ----*/

Step7: $M(X, Y) \leftarrow M(X, Y) + k[R + \delta M(X', Y') - M(X, Y)]$

$X \leftarrow X'$; $Y \leftarrow Y'$;

Repeat until X reaches maximum actions

Step 8: end.

5. RESULT ANALYSIS

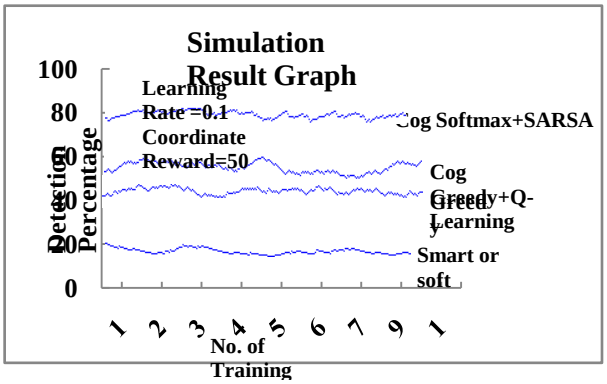

Figure 3: Simulation results generated from simulator

The performance of the Greedy and Softmax algorithms are generated before achieving cognition and the proposed Cognitive GQC and SSC algorithms are shown in Figure 3, which is generated by the simulator. From this graph, the detection percentage for all the mentioned algorithms can be observed.

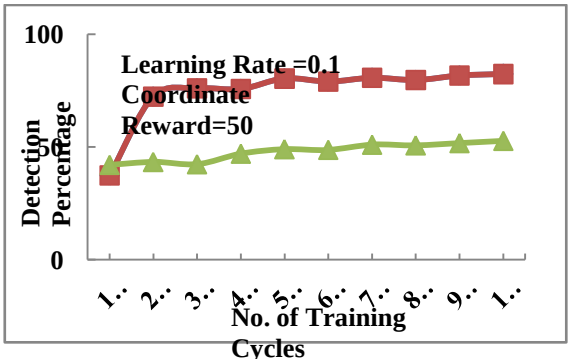

Figure 4: No. of Training Cycles Vs Detection Percentage

The variations in detection rate with respect to training cycles can be observed in Figure 4. As the number of training cycles increases, the malicious node detection rate also increases. Here,learning rate and co-ordinate rewards are kept constant. For GreedyQ Cognitive algorithm, maximum detection percentage is about 52.67 and 82.23 is for SoftSARSA cognitive algorithm.

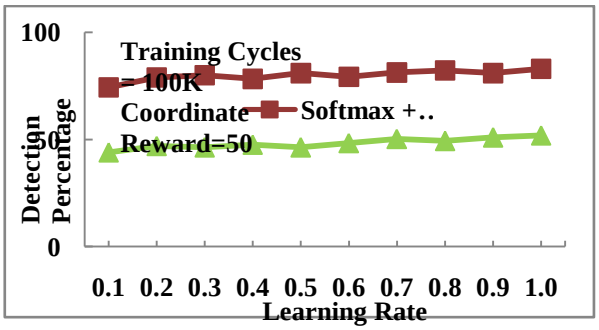

Figure 5: Learning Rate Vs Detection Percentage

From Figure 5, variations in detection rate with respect to learning rate can be observed. As the Learning rate increases, the malicious node detection rate also increases. Here, Training cycles and co-ordinate rewards are kept constant. For GreedyQ Cognitive algorithm, maximum detection percentage is about 52 and 83 is for SoftSARSA cognitive algorithm.

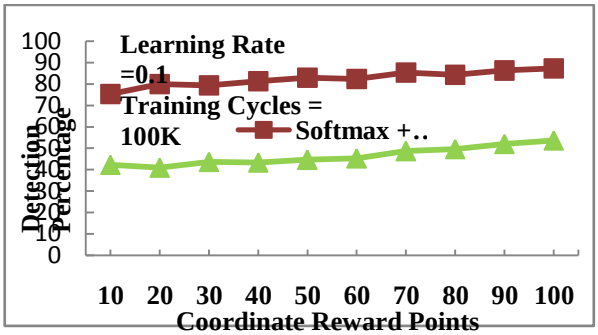

Figure 6: Co-ordinate reward points Vs Detection Percentage

From Figure 6, variations in detection rate with respect to Co-ordinate reward points can be observed. As the Co-ordinate reward points increases, the malicious node detection rate also increases. Here, Training cycles and Learning rates are kept constant. For GreedyQ Cognitive algorithm, maximum detection percentage is about 53.67 and 87.33 is for SoftSARSA cognitive algorithm.

6. CONCLUSIONS

In this paper, different reinforcement learning techniques are evaluated with respect to malicious node detection with and without cognition. The proposed new GreedyQ cognition algorithm and SoftSARSA Cognitive algorithm are also evaluated by changing the parameters like learning rate, co-ordinate reward points and number of training cycles. With cognition, the maximum malicious detection rate for proposed GreedyQ cognitive algorithm is 53.67% whereas SoftSARSA cognitive algorithm is 87.33%. But the same algorithms yields lower results without cognition.

7. REFERENCES

[1] Milos Rovcanin, Eli De Poorter, Ingrid Moerman and Piet Demeester, “An LSPI based reinforcement learning approach to enable network cooperation in cognitive wireless sensor networks”, Proceedings of International conference on Advanced Information Networking and Applications Workshops, pp. 82-89, March 2013.

[2] J Mitola III, ”Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio”, PhD thesis, Royal Institute of Technology, Sweden.

[3] R Saracco, “Forecasting the future of information technology: How to make research investment more cost-effective”, IEEE Communications Magazine, vol. 41, pp. 38–45, December 2003.

[4] John Boyd, ” A discourse on winning and losing: Patterns of conflict”, Conceptual Spiral and the meaning of life, 1986.

[5] K Cheng Howa, M Maa, and Y Qin, “An Altruistic Differentiated Service Protocol in Dynamic Cognitive Radio Networks Against Selfish Behaviors”, IEEE Transactions on Computer Networks, vol. 56, no. 7, pp. 2068–79, 2012.

[6] Minho Jo, Longzhe Han, Dohoon Kim, Hoh Peter, “Selfish Attacks and Detection in Cognitive Radio Ad-Hoc Networks”, IEEE Transactions on Network, June 2013.

[7] Yongkun Li, John C S Lui, “On Detecting Malicious Behaviors in Interactive Networks: Algorithms and Analysis”, IEEE, 2012.

[8] Haojin Zhu, Suguo Du, Zhaoyu Gao, Mianxiong Dong, Zhenfu Cao, "A Probabilistic Misbehavior Detection Scheme towards Efficient Trust Establishment in Delay-tolerant Networks", IEEE Transactions on Parallel and Distributed Systems, 2013.

[9] Praveen Kaligineedi, Majid Khabbazian, Vijay K Bhargava, "Malicious User Detection in a Cognitive Radio Cooperative Sensing System", IEEE Transactions on Wireless Communications, vol. 9, no. 8, August 2010.

[10] Nicola Baldo, Michele Zorzi, "Cognitive Network Access using Fuzzy Decision Making", IEEE Transactions on Wireless Communications, Vol. 8, no. 7, July 2009.

[11] K Sundaresan and K Papagiannaki, "The need for cross-layer information in access point selection", Proceedings of International Conference on Internet Measurement, Brazil, Oct. 2006.

[12] A Nicholson, Y Chawathe, M Chen, B Noble and D Wetherall, "Improved access point selection", Proceedings of International Conference on Mobile Systems, Applications and Services, Sweden, June 2006.

[13] D Deng and H Yen, "Quality-of-service provisioning system for multimedia transmission in IEEE 802.11 wireless LANs", IEEE Journals on Communication, vol. 23, no. 6, pp. 1240–1252, 2005.

[14] M Matsumoto and T Itoh, "QoS-guarantee method for public wireless LAN access environments", Proceedings of International Conference on Wireless Networks, Communications and Mobile Computing, USA, June 2005.

[15] Ryan W Thomas, Luiz A DaSilva, Madhav V Marathe, Kerry N Wood, "Critical Design Decisions for Cognitive Networks", IEEE, 2007.

[16] G Sunilkumar, Thriveni J, K R Venugopal, L M Patnaik, "Cognitive Approach Based User Node Activity Monitoring for Intrusion Detection in Wireless Networks", International Journal of Computer Science Issues, vol. 9, Issue 2, no. 3, March 2012.

8. AUTHOR'S PROFILE

Sunilkumar G has completed Bachelor of Engineering in Electronics and Communications from Visvesavaraya Technological University,Belgaum, Master of Engineering in Information Technology from University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He is a research scholar in Bangalore University. He has 8 years of teaching experience. Currently he is an Assistant Professor in the Dept. of CSE, Alpha College of Engineering, Bangalore. His area of interest includes Cognitive Networks, Cloud Computing, and Network Security.

Manjunatha C has completed Bachelor of Engineering in CSE an M .Tech in Computer Network Engineering from Visvesavaraya Technological University,Belgaum, He has 3 years of Industrial experience. His area of interest includes Cognitive Networks and Network Security.

Thriveni J has completed Bachelor of Engineering, Masters of Engineering and Doctoral Degree in Computer Science and Engineering. She has 4 years of industrial experience and 18 years of teaching experience. Currently she is an Associate Professor in the Dept. of CSE, University Visvesvaraya College of Engineering, Bangalore. She has over 40 research papers to her credit. Currently she is guiding 7 Ph.D Students. Her research interests include Networks, Data Mining and Biometrics.

Venugopal K R is currently Special Officer, DVG Bangalore University and Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 51 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems etc.. During his three decades of service at UVCE he has over 400 research papers to his credit. He was a Post Doctoral Research Scholar at University of Southern California, USA. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining.

L M Patnaik is a Ex-Vice Chancellor, Defense Institute of Advanced Technology, Pune, India. He was a Professor since 1986 with the Department of Computer Science and Automation, Indian Institute of Science, Bangalore. During the past 35 years of his service at the Institute he has over 700 research publications in refereed International Journals and refereed International Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India; Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to High Performance Computing and Soft Computing. Currently he is Honarary Professor, Indian Institute of Science Bangalore, India. His areas of research interest have been Parallel and Distributed Computing, Mobile Computing, CAD for VLSI circuits, Soft Computing and Computational Neuroscience.