2017 3rd International Conference on Electrical Information and Communication Technology (EICT), 7-9 December 2017, Khulna, Bangladesh

Performance Analysis of Cognitive Radio: Netsim Viewpoint

Khaled Mohammed Saifuddin[1], Abu Shakil Ahmed[2], Kazi Fahid Reza[3], Sk Shariful Alam[4], Sharmina Rahman[5]
Khulna University of Engineering & Technology, Khulna-9203, Bangladesh
hamim026@gmail.com[1], shakil.ahmed.bd71@gmail.com[2], fahidreza2708@gmail.com[3], ssa1996@gmail.com[4], sharminalima@gmail.com[5]

Abstract—**Electromagnetic spectrum is very precious as it is limited and performance of a communication system degrades if it is used inefficiently. Cognitive Radio (CR) ensures proper utilization of the available licensed spectrum of Primary User (PU) by allocating the temporary unused portion of it to a Secondary User (SU). In this paper, we have analyzed the impact of PU activities on the SU throughput and assessed the spectral efficiency. Moreover, the performance of CR has been evaluated for different cooperative approaches and compared considering the corresponding fading effects. Furthermore, security threat in Cognitive Radio Network (CRN) due to PU emulation attack from malicious users has been addressed as well as the corrective measure has been proposed to mitigate the risk.**

Keywords—CRN, IFQP cycle length, Congestion control, PUE attack, Throughput, Spectral efficiency, Cooperative spectrum sensing, Channel allocation.

I. INTRODUCTION

Progressively we are getting more accustomed to wireless communication to keep abreast with the dynamic life. The efficiency of the communication system is subject to optimum consumption of electromagnetic spectrum. CR, one of the most trending concepts in wireless communication, ensures the proper utilization of licensed spectrum of PU when it is not in use. The unused spectrum is shared with SU until the PU starts using it once again. Throughput and spectral efficiency of SU are two decisive factors for the performance of CR as they assess the quality of communication over a limited frequency spectrum. Throughput is a measure of successful transmission of data packets, and spectral efficiency refers to the data transmission rate over a given bandwidth. Different parameters have an impact on throughput and spectral efficiency such as the operation of PU, frequency allocation, and congestion control. Moreover, security is one of the primary concern for CRN as illegitimate users may temper the air interface of CR to imitate PU signal characteristics which SUs erroneously identify as legitimate. CRN is venerable for PU Emulation (PUE) attack since it is highly reconfigurable due to its software-based air interface.

A brief overview of some significant approaches towards the improvement of spectrum sensing, better throughput, and enhancement of system performance has been mentioned in TABLE I referring to the respective author/s along with the methodology they have proposed, and the contributions they have offered.

TABLE I. LITERATURE REVIEW ON CRN AND ITS DIFFERENT ASPECTS

Author/s	*Methodology*	*Contribution*
Dhanalakshmi P. et al. [1]	In this paper, normalized throughput has been calculated for both single and multiple SUs under multiple PU using optimal *K*-of-*N* rule.	It has been observed that among cooperative and non-cooperative spectrum sensing techniques, the cooperative one is more efficient.
V. Tumuluru et al. [2]	Spectrum handoff prioritization technique has been used for various Dynamic System Access (DSA) under different CRN topology.	Outcomes of this paper suggest that the handoff buffer has managed to improve the call completion rate of SU.
A. El-Toukhey et al. [3]	The impact of the variation in both arrival rate and service rate of the priority based SUs has been evaluated using three-dimensional Markov model.	The priority of SUs has been capable of enhancing the system performance of CR, and the model has prioritized highest SUs to have channel access for a longer period.
R. Bouraoui et al. [4]	Cooperative spectrum sensing based on censored energy detection has been employed in this paper to enhance the decision accuracy.	The reliability of sensing has been improved using decision fusion rules based on sensor energy detection method.
S. Alam et al. [5]	Energy detection method over different fading channels has been incorporated as well as the dependency of the throughput on the fading channel has been analyzed.	The throughput has been improved by applying this model as it has been observed that throughput in the conventional model decreases rapidly with the increase in time.
S. Alam et al. [6]	In this paper, cooperative detection technique has been utilized for the radio nodes to improve the detection performance.	Cooperative detection technique improves system performance as better throughput has been obtained.
I. Akyildiz et al. [7]	An improved detection scheme using cooperative sensing technique has been proposed that applies hypothesis testing, data fusion, control channel and reporting, and user selection.	Result suggests that the evaluation has been able to improve the detection performance by means of analyzing spatial diversity at the expense of cooperation overhead.
W. Stevens et al. [8]	Four different algorithms have been implemented in this paper such as slow start, congestion avoidance, fast retransmit, and fast recovery.	The implementation of the algorithms have been elaborated, and the pros and cons have been discussed.

978-1-5386-2307-7/17/$31.00 ©2017 IEEE

Author/s	*Methodology*	*Contribution*
X. Xie et al. [9]	In this paper, physical layer network coding technique has been applied to detect the emulators, as well as the starting point of collision, has been determined using the distances between the receiver and the senders.	The difference between the starting points of interference at two receivers is restricted by the positions of the senders. The system has been able to determine the hyperbolas on which the desired sender resides.
J. Unnikrishnan et al. [10]	The paper has proposed a linear-quadratic (LQ) fusion strategy to detect PU based on a deflection criterion for low signal to noise ratio.	The proposed system provides better performance over counting rule and suggests the correlation between the nodes should not be ignored.

In this paper, the impact of PU activity on the SU throughput has been analyzed as well as the spectral efficiency has been assessed. Besides, we have evaluated the performance of CR for different cooperative approaches and made a comparison among them considering the corresponding fading effects. Furthermore, security threat in Cognitive Radio Network (CRN) due to PU emulation attack from malicious users has been addressed as well as the corrective measure has been proposed to mitigate the risk.

We have arranged the paper in an orderly manner. In section II, the performance parameters such as PU operation and IFQP cycle length have been explained with emphasis on their effects on the system performance. In section III, we have proposed a TCP congestion control technique with its different variants like Old Tahoe, Tahoe, Reno, and New Reno as well as the related algorithms to prevent congestion in CRN. In section IV, the PUE attack on CRN and the necessary corrective measure to mitigate the risk have been mentioned. In section V, two different cooperative sensing techniques, i.e., centralized and distributed approaches have been described in brief. We have specified the outcomes in section VI after simulating the effects of PU operation, channel allocation, congestion window as well as the system performance for PU detection, PUE attack detection, and cooperative operation. To conclude the paper the entire work has been summarised in section VII.

II. PERFORMANCE PARAMETERS

A. PU Operation

Throughput and spectral efficiency of SU are two performance parameters of CRN. As PU is the licensed user of spectrum, SU cannot use it when the PU is active. Hence the throughput and spectral efficiency of SU is zero in this condition. SU can use the spectrum only when PU is inactive, and it is an obligation for SU to comply. In case both the PU and SU are allocated to the same frequency band, there is no presence of spectrum hole. As a result, the throughput and spectral efficiency of SU will be negligible.

B. IFQP Cycle Length

The available radio spectrum is divided into several nonoverlapping channels with a view to minimizing adjacent channel interference, especially for traffic channels. CRN aims to provide quality service to as many clients as possible by the efficient allocation of the available bandwidth. Inter Frame Quiet Period (IFQP) indicates the spacing between super-frames for which the intra-frame quiet period specification is valid. For example, if the field is set to 1, the cycle of quiet period repeats for each super-frame. If it is set to 2, the cycle repeats for every two super-frames while for 0, no intra-frame quiet period is scheduled, i.e., the current IFQP is canceled.

III. TCP CONGESTION CONTROL

TCP stands for Transport Layer Protocol and defines the way to establish and maintain connection within a network. It is a connection-oriented and reliable end-to-end protocol that supports a variety of network applications. When too many packets are exchanged, the load of the system goes beyond the capacity and congestion occurs. It leads to performance degradation that TCP takes into consideration. For better throughput and spectral efficiency, congestion must be controlled before or after it occurs. We have used four variants of TCP and a congestion control algorithm to keep the congestion in check. Fig. 1 represents the control algorithm for TCP congestion where cwnd implies congestion window, SMSS stands for Sender Maximum Segment Size, and MSS denotes Maximum Segment Size.

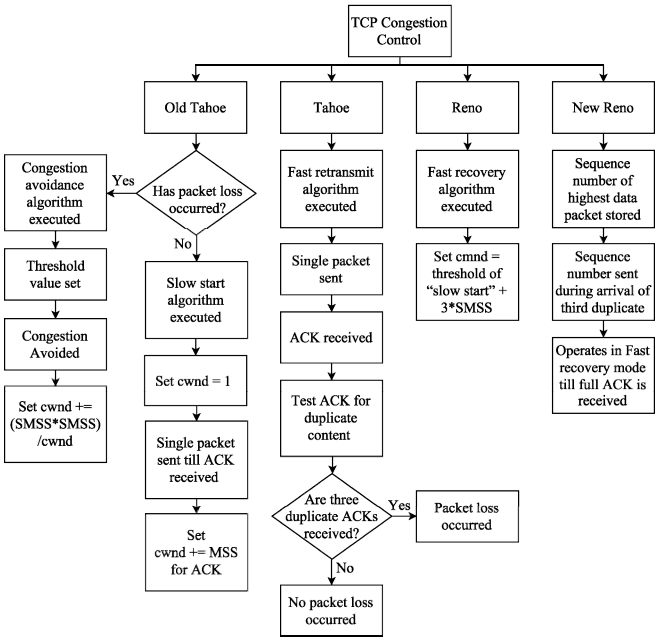

Figure 1. TCP congestion control technique.

A. Old Tahoe

Being one of the earliest variants of TCP, Old Tahoe incorporates slow start and congestion avoidance algorithm in order to update the congestion window (cwnd). When no packet loss occurs, the slow start algorithm is executed. As per the algorithm, cwnd refers to the maximum size of a packet that can be transmitted without any acknowledgment (ACK). In the beginning, TCP can send one packet until it receives an

ACK. When the ACK is received, the size of cwnd increases exponentially. We have used congestion avoidance algorithm when packet loss occurs. At first, a threshold value is set to avoid the congestion. In this case, congestion window size is increased linearly.

B. *Tahoe*

Tahoe, an enhanced edition of Old Tahoe, uses fast retransmit algorithm for quicker response. Fast retransmit detects packet loss by checking the number of duplicate ACKs. If the system receives three duplicate ACKs, it indicates packet loss.

C. *Reno*

Reno preserves the core principles of Tahoe though it is less destructive than the later one to reduce the congestion window. Reno based TCP uses fast recovery algorithm for congestion control. A slow start threshold value is set to half of the congestion window where the cwnd is equal to the summation of slow start threshold and three times of the SMSS [8].

D. *New Reno*

New Reno is preferable to Reno based TCP as it improves throughput in case of multiple packet loss. New Reno based TCP congestion control stores the sequence number of the highest data packet and sends it during the arrival of the third duplicate packet in order to avoid packet loss [8]. TCP keeps executing fast recovery algorithm until it receives a full ACK.

IV. PUE ATTACK

The security of CRN is often in jeopardy for access of illegitimate malicious users as they may temper the air interface of CR to imitate PU signal characteristics which SUs erroneously identify as legitimate. PUE attack on CRN poses a severe threat to its implementation since CR is highly reconfigurable due to its software-based air interface [7]. We have proposed a method to create and detect a PUE attack in CRN. Detection of the position of the transmitter is a prerequisite for identifying an attacker, and then effective countermeasures can be carried out. We have simulated a PUE attack in NetSim by adding two PUs one of which is a real and the other is malicious in the scenario. After carrying out PUE attack, we have evaluated the detection accuracy of SU.

V. COOPERATIVE OPERATION

Multipath fading, shadowing, and uncertainty of receiver affect the detection performance of CRN. Cooperative spectrum sensing is an effective method to mitigate these impacts as it provides a better perception of the spectrum usage over the area where the CRs are located [9]. Cooperative operation refers to sharing individual sensing information about the unused spectrum by the CR nodes with a master node or every other node with a view to improving the detection performance. We have evaluated the detection performance for different types of cooperative approach and compared between the centralized and distributed ones on the basis of fading.

A. *Centralized Approach*

In centralized sensing approach, a master node collects individual sensing data from other nodes and broadcasts information about available spectrum to the nodes after detection. The master or central node further analyzes and determines the usable frequencies those are not in use by PU. Due to security concerns, the central unit collects information only from the reliable nodes and processes it. In a simulation environment, various numbers of nodes can be introduced to find out the optimized performance of centralized cooperation under different parameters.

B. *Distributed Approach*

In distributed sensing approach, CR nodes share their sensing information with one another instead of providing it to the master node and make individual decisions for usage of the unused spectrum. Unlike centralized approach, distributed approach employs individual radios having much higher level of autonomy in place of a backbone infrastructure [10]. Moreover, some overheads are considered for the approach such as sensing delay, throughput, and packet loss. We have examined the overheads of packet loss and throughput for both centralized and distributed approaches and determined their performance limits.

VI. SIMULATION RESULT

We have carried out the simulations in NetSim by creating network scenarios, modeling traffic, and analyzing performance metrics. The CRN topology has been shown in Fig. 2.

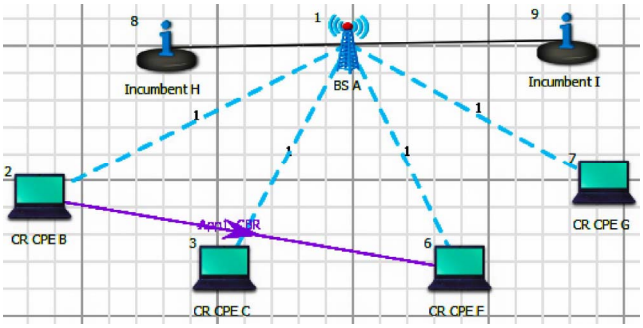

Figure 2. CRN topology.

We have designed the topology incorporating two PUs, four SUs, and one Base Station and considered the default properties for each device, physical layer, and data link layer.

A. *Effect of PU Operation*

We have taken three samples with different operational interval time to observe the effect of PU Operation. The samples have been set as shown in TABLE II and each of them has been simulated for 100s. Besides, we have calculated the throughput and spectral efficiency of SU. A comparative analysis of spectral efficiency and throughput with operational intervals of PU have been shown in Fig. 3. In the first sample, PU constantly uses the entire spectrum as the operational interval is set 0s. Hence the value of throughput and spectral

efficiency is almost zero. With the increment of the operational interval, the values of both throughput and spectral efficiency increase sharply.

TABLE II. SAMPLES AND THE OPERATIONAL INTERVALS

Sample	sample 1	Sample 2	Sample 3
Operational interval	0s	10s	15s

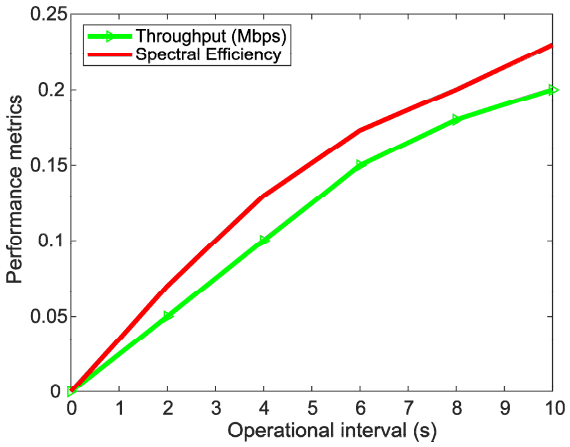

Figure 3. Variation of throughput and spectral efficiency with operational intervals of PU.

B. *Effect of Channel Allocation*

In a CRN system, channels are allocated by varying cycle lengths of IFQP. We have compared the throughput with the IFQP cycle length which has been ranged from 1 to 15 as shown in Fig. 4.

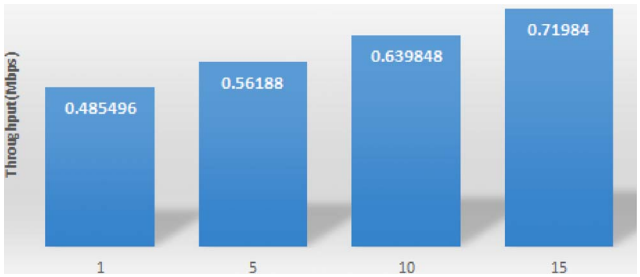

Figure 4. Effect of channel allocation on throughput.

This simulation suggests the throughput increases with the cycle length of IFQP.

C. *Effect of Congestion Window*

By default, NetSim uses Old Tahoe for TCP congestion control that depends on the timer to expire before retransmission of a packet is allowed. Hence, we have used several variations of TCP such as Tahoe, Reno, and New Reno along with Old Tahoe for simulation.

Fig. 5 shows New Reno and Tahoe offer more spectral efficiency than Reno and Old Tahoe respectively. The New Reno offers the best spectral efficiency while Old Tahoe offers the least on the contrary.

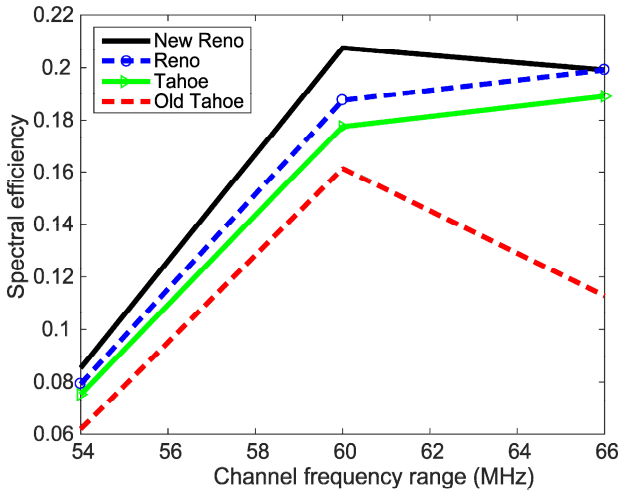

Figure 5. Spectral efficiency vs. Channel Frequency for different congestion control technique

D. *PU Detection*

We have ensured the detection of PU or incumbent before simulating and detecting a PUE attack in order to keep PU activity free from interference. Hence different operational intervals have been set for both the SUs and the PUs so that no interference can occur. Fig. 6 shows the variation of sensing delay with different operational intervals. The runtime of the simulation is 100s. Here SU has higher sensing delay than PU.

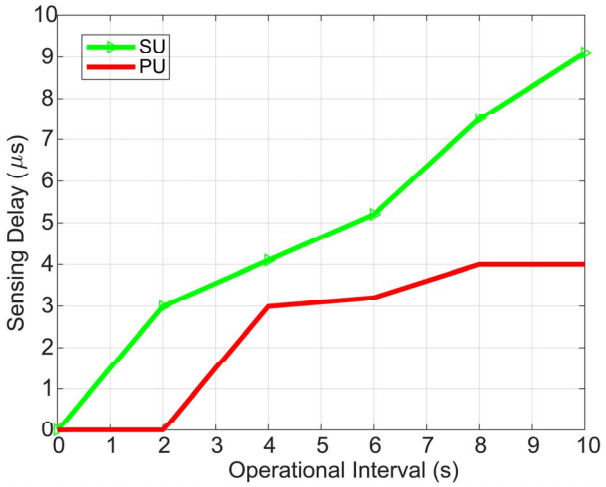

Figure 6. Incumbent detection in a CRN.

E. *PUE Attack Detection*

We have simulated a PUE attack in NetSim with two PUs one of which is real and the other is malicious along with two SUs, and a base station as shown in Fig. 7.

The detection time has been set proportional to the distance of the SUs from the malicious PU and the appropriate operational interval for both PUs has been selected. Here initially additional delay has been considered to be the one tenth of the value of distance and varied for one hundredth and one thousandth to analyze the effect of the time delay.

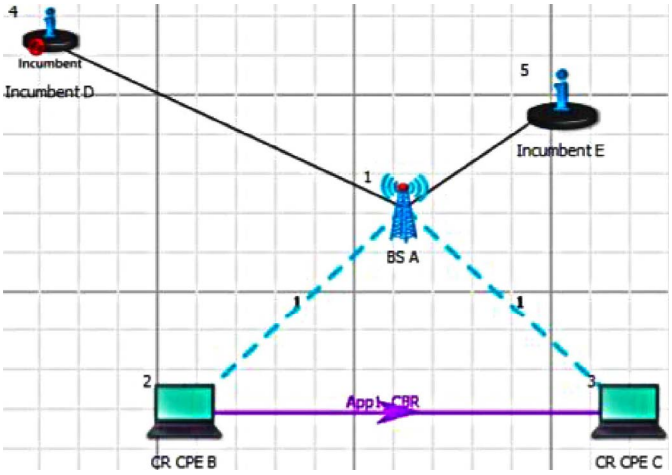

Figure 7. PUE attack topology.

The operational time for real and malicious PU has been set 9s and 4s respectively, and the operational interval has been set 9s and 10s for them in sequence. The active and inactive states for both real and malicious PUs have been shown in TABLE III.

TABLE III. ACTIVE AND INACTIVE STATES OF PUS

Real PU (OFF)	Real PU (ON)	Malicious PU (OFF)	Malicious PU (ON)
0s to 9s	9s to 18s	0s to 10s	10s to 14s
18s to 27s	27s to 36s	14s to 24s	24s to 28s
36s to 45s	45s to 54s	28s to 38s	38s to 42s
54s to 63s	63s to 72s	42s to 52s	52s to 56s
72s to 81s	81s to 90s	56s to 66s	66s to 70s
90s to 99s	99s to 108s	70s to 80s	80s to 84s
-	-	84s to 94s	94s to 98s
-	-	98s to 108s	-

TABLE IV. TIME VARIATIONS FOR PUE ATTACK DETECTION

Detected By	Detected	Delay time (micro second)
CPE2	Incumbent 1	9129743
CPE3	Incumbent 1	9129741
CPE2	Incumbent 2	24049746
CPE3	Incumbent 2	24049746
CPE2	Incumbent 2	38129746
CPE3	Incumbent 2	38129746
CPE2	Incumbent 1	4500974
CPE3	Incumbent 1	45009741
CPE2	Incumbent 1	63049743
CPE3	Incumbent 1	63049743
CPE2	Incumbent 2	63049743
CPE3	Incumbent 2	80049746
CPE2	Incumbent 2	94049746
CPE3	Incumbent 2	94049746

NetSim generates a text file after the simulation that contains the required time to detect the PUE attack. Point to be noted that the throughput of the PU may be affected by the mobility of the SU. The time variation for detection of PUE attack has been presented in TABLE IV.

F. Cooperative Operation

We have compared between the performances of centralized and distributed cooperative sensing by using the topology shown in Fig. 8. The aim of using centralized sensing is to mitigate the fading effects of the channel and increase the detection performance. According to Fig. 9, centralized cooperative sensing concedes less packet loss and hence provides better performance than the decentralized one for the same number of nodes. Moreover, the occurrence of packet loss decreases in centralized cooperative sensing with increasing number of nodes while quite the opposite nature has been observed for the decentralized or distributed approach.

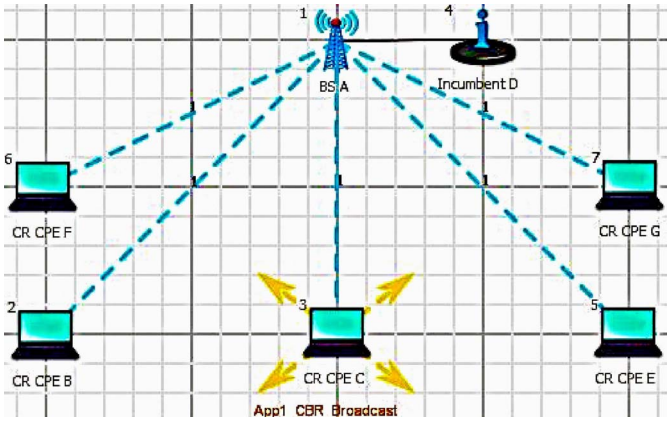

Figure 8. Topology for cooperative CRN.

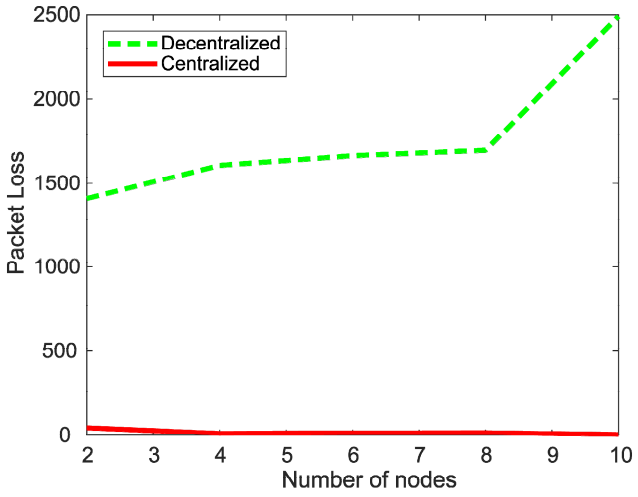

Figure 9. Comparison between fading effects in different cooperation.

In case of throughput, centralized sensing approach yields better performance than the decentralized one as per Fig. 10 suggests.

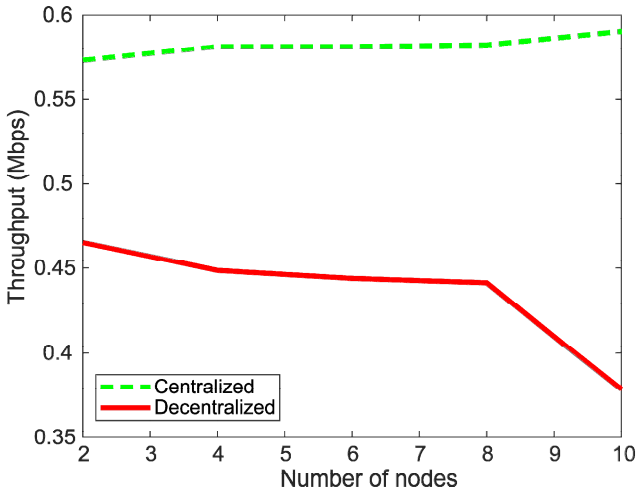

Figure 10. Obtained throughput in different cooperation technique.

VII. CONCLUSION

CR is a wireless communication technique that ensures proper utilization of the available licensed spectrum of PU by allocating the temporary unused portion of it to SUs. However, SUs can use the spectrum only when PU is inactive, and it is an obligation for SUs to comply. In this paper, we have conducted comparative analysis among several performance parameters of CRN through simulation, and different topologies have been designed with performance appraisal. The channels have been allocated by varying the cycle length of IFQP with which the throughput varies proportionally. Moreover, four variants of TCP control algorithm such as Old Tahoe, Tahoe, Reno, and New Reno have been employed to reduce the congestion in CRN. We have observed that both the throughput and the spectral efficiency increase notably with the rise in the operational interval of PU. The SUs are more sensitive to operational interval than PU in case of sensing delay. Different operational intervals have been set for both the SUs and the PUs in order to prevent interference to PU activity. As security assessment, a PUE attack has been modeled in NetSim and the time variation for detection of the attack has been presented. In case of spectrum sensing method, the centralized cooperative sensing technique is preferable to decentralized one as it concedes less packet loss and provides better throughputs for the same number of nodes. Furthermore, the occurrence of packet loss decreases in centralized cooperative sensing with increasing number of nodes while quite the opposite behavior has been perceived as the decentralized approach. In CRN, centralized cooperative sensing technique, greater cycle length, wider operational interval, and New Reno congestion control protocol offers better performance for proper utilization of electromagnetic spectrum.

REFERENCES

[1] Dhanalakshmi P., Divya S., Kamila S.A., Muthumeenakshi K. and Radha S., "Modeling and analysis of Cognitive Radio with multiple primary/Secondary users and imperfect sensing", *2014 International Conference on Recent Trends in Information Technology*, 2014.

[2] V. Tumuluru, P. Wang, D. Niyato and W. Song, "Performance analysis of cognitive radio spectrum access with prioritized traffic", *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1895-1906, 2012.

[3] A. El-Toukhey, A. Ammar, M. Tantawy and I. Tarrad, "Performance analysis of different opportunistic access based on secondary users priority using licensed channels in cognitive radio networks", *2017 34th National Radio Science Conference (NRSC)*, 2017.

[4] R. Bouraoui and H. Besbes, "Cooperative spectrum sensing for cognitive radio networks: fusion rules performance analysis", *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2016.

[5] S. Alam, J. Chowdhury, M. Rashed, S. Anjuman and R. Zaman, "Throughput analysis of narrowband cognitive radio networks for fading channel", *2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, 2016.

[6] S. Alam, M. Lucio and C. Regazzoni, "opportunistic spectrum access of sparse wideband in stand-alone and cooperative cognitive radio networks", *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, 2015.

[7] I. Akyildiz, B. Lo and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: a survey", *Physical Communication*, vol. 4, no. 1, pp. 40-62, 2011.

[8] W. Stevens, "TCP slow start, congestion avoidance, fast retransmit, and fast recovery algorithms," *RFC 2001*, Jan. 1997.

[9] X. Xie and W. Wang, "Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding", *Procedia Computer Science*, vol. 21, pp. 430-435, 2013.

[10] J. Unnikrishnan and V. Veeravalli, "Cooperative sensing for primary detection in cognitive radio", *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 18-27, 2008.