Australian Journal of Basic and Applied Sciences, 9(35) November 2015, Pages: 10-16

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Jamming Resistant Partial Random Channel Selection in Cognitive Wi-Fi Networks

[1]K.Karunambiga and [2]M. Sundarambal

[1]*Department of CSE, College of Engineering Guindy, Anna University, Chennai – 600025, India.*
[2]*Department of EEE, Coimbatore Institute of Technology, Affiliated to Anna University, Coimbatore – 641014, India.*

ARTICLE INFO

Article history:
Received 10 October 2015
Accepted 30 November 2015
Available online 24 December 2015

Keywords:
Cognitive Wi-Fi network, jamming attack, frequency hopping, Partial Random Channel Selection

ABSTRACT

Wi-Fi networks support many day to day activities especially in the urban area, which in turn results in spectrum scarcity. The spectrum availability of the Wi-Fi network is increased with the support of cognitive radio (CR). The availability of spectrum is targeted by jamming attack. It is addressed with the help of frequency hopping technique. The key design issue of the frequency hopping is the spectrum selection for next hop. Partial Random Channel Selection (PRCS) is proposed to address the aforementioned problem. This strategy does not depend completely on the statistic of the network traffic as in the existing technique. The performance of PRCS is compared with related approach through extensive Glomosim simulations. The results of simulation confirm that PRCS approach is efficient in selecting the best channel for communication in terms of channel switching delay and throughput.

To Cite This Article: K. Karunambiga and Dr. M. Sundarambal., Jamming Resistant Partial Random Channel Selection in Cognitive Wi-Fi Networks. ***Aust. J. Basic & Appl. Sci.,*** *9(35): 10-16, 2015*

INTRODUCTION

Internet access through wireless devices were raised rapidly, the fixed spectrum was not sufficient to handle the requirement for communication. To cope up with the spectrum requirement Dynamic Spectrum Access (DSA) (Yuhua Xu, *et al*., 2013) was invented. This DSA was achieved with the help of cognitive radio (CR). The cognitive radio is a wireless device which can change its parameter based on the perception of the environment. Secondary user (SU) is a wireless device with the features of cognitive radio, which opportunistically utilize the spectrum when it is not utilized by the primary user (PU), which is known as Dynamic Spectrum Access. The Primary User (PU) is the wireless device which owns the licensed band. In the proposed system the access point (AP) and client station (STA) with cognitive radio together forms the Cognitive Wi-Fi network. The DSA and shared medium property of cognitive Wi-Fi gives an opportunity to adversaries to easily launch the denial of service (DoS) attack by jamming the communication between the transmitter and receiver. In Rohit *et al* (2005) the analysis of the intelligent jamming attack is performed and demonstrated that the throughput of the network was affected extremely. The cooperative nature of the cognitive network and knowledge about the MAC layer has aroused interest of the adversary to launch the link-layer jamming attack. This intelligent DoS attack requires knowledge about the MAC and instantaneous channel state information. It leads to the tradeoff between information gathering and effective jamming. Weyuvan Xu (2006) proposes four generic jammer models - reactive jammer, random jammer and deceptive jamming.

- The constant jamming model the jammer transmits a constant random signal.
- Random jammer oscillates between the sleep slot and jam slot with random time slot.
- In the reactive jamming attack mode, when jammer identifies the activity on the channel, immediately sends out a random signal.
- The deceptive jammer fabricates the signals or replays it on the channel continuously.

All the four techniques reduce the packet delivery ratio, but these techniques are energy-inefficient. In this paper, best of the intelligent jammer and generic jammer is combined as link-layer periodic deceptive jammer. This link-layer periodic deceptive jammer send the valid link-layer frames periodically without interfering the Primary User (PU) on the channel which degrades the performance of the cognitive Wi-Fi network.

Corresponding Author: Mrs.K.Karunmabiga, Department of CSE, College of Engineering Guindy, Anna University, Chennai -600025,Tamil nadu, India.
Phone +(91)8122667016; E-mail: karunambiga.cse12@gmail.com

Table 1: Comparison of Related Works

Related Work	Selection Strategy	Jamming - Resistant	New Channel Holding time (PU activity and Interference level high)	New Channel Holding time (PU activity and Interference level low)	Channel selection overhead
SURF [7]	Statistics based selection	No	High	High	High
Alex *et al* [8]	Statistics based selection	No	High	High	High
Ejaz *et al* [9]	Statistics based selection	No	High	High	High
Qurratul-Ain *et al* [11]	Game theory	No	High	High	High
Yongle *et al* [12]	Knowledge based Selection	Yes	High	High	High
Hai *et al*[13]	Random Selection	Yes	Low	High	Low
Wenjing *et al* [14]	Random Selection	Yes	Low	High	Low

The existing channel selection algorithms choose next channel based on statistics (Mubashir Husain Rehmani *et al*., 2013; Alex Chia-Chun Hsu *et al*., 2007; Ejaz Ahmed, Muhammad Shiraz, Abdullah Gani, 2013) or complete random (Hai Su, *et al*., 2011; Wenjing Wang, *et al*., 2013) strategy. Statistics based Channel Selection (SCS) method allows the jammer to identify the data channel of the user with the same strategy. On the other side complete Random based Channel Selection (RCS) do not leave any clue to the jammer, but the user may land up in the new channel with high PU activity or high interference level. The analysis of the related work based on the jamming-resistant, holding time and channel overhead is given in the table.1. To overcome the aforementioned drawbacks, the PRCS is proposed. The remaining sections are organized as proposed system, results and discussion.

Proposed System:

System Model:

The cognitive Wi-Fi network (CWN) is a combination of Access Points (AP) and Stations (STA). It is assumed that all APs were connected to the wired backbone infrastructure. The stations are associated with each access points when it needs to access the internet and number of stations connected with AP varies dynamically. Wireless channel is model with fading and noise apart from actually data transmission signal. This channel or spectrum is used for communication between the APs and STAs of CWN network. The set of channels utilized for communication are C={C1,C2,…,Cn}, where n is the number of available channels. It is assumed that the bandwidths of all the spectrum are same. The small region with dense wireless communication scenario was considered. The transmission range of each STA's and AP's of varies Cognitive Wi-Fi network falls under the same transmission range. Since all the STA and AP are in the same transmission range, the Channel State at any instance of time is same for all APs and STAs and the number of jammer required to jam all the APs and STAs operating in the same channel is equal to one. For the same reason, single PU was assigned per licensed band. The PU activity is implemented as a power on/off model. The periodic deceptive jammer method was used to achieve the jamming attack, which alternates between silence and jamming mode respectively. Since it is an energy saving method, this jamming can be launched using power constraint devices. The architecture of the Partial Random Channel Selection is shown in the figure.1.

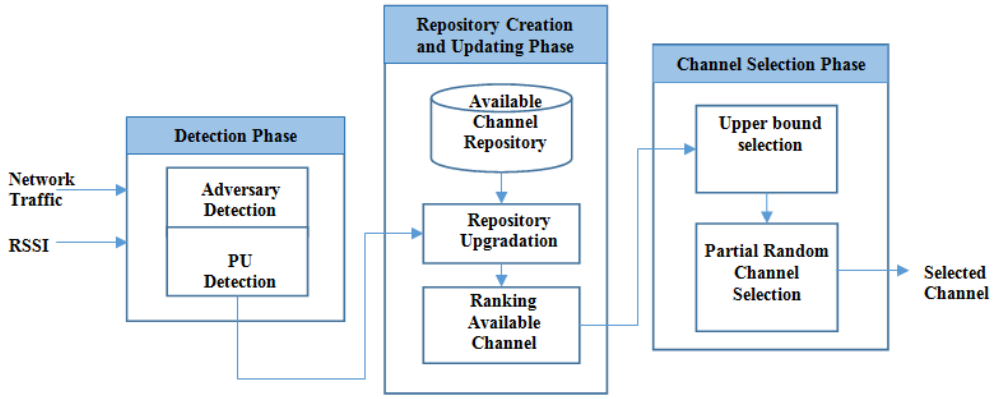

Fig. 1: Architecture of Partial Random Channel Selection

Detection Phase:

The detection of primary user activity is done using energy filtering method (Yu, F.R. and *et al*., 2009). Since the primary user's transmission power level is very high when compared with other wireless device, PU is detected by AP or STA when received energy level of the sensing channel is above the threshold value (Yu, F.R. and *et al*., 2009). If the presence of PU activity is detected by STA, that station sends the report to the corresponding AP. Once the PU activity is detected by AP in the current data channel or AP receives message from STA about the PU, the AP immediately initiates its spectrum selection phase. Similarly the attacker is detected using the threshold method. The detected of intruder in current data channel is identified using Packet Send Ratio (PSR) and Packet Received Ratio (PRR).The mean and the standard deviation of PSR collected over m number of samples are μs and σs. The mean and the standard deviation of PRR collected over s number of samples are μr and σr. The Tr and Ts is the threshold values for the PRR mean and PSR mean respectively. These PSR, PRR are collected and its means and standard deviation are calculated by all the nodes periodically in the network to detect the presence of jammer in the current data channel 'i' is J_i.

Adversary Detection Algorithm:

Input : Packet send ratio and packet received ratio

Output : Ji

Procedure

Calculate the μs & σs for m number of PRR sample over time interval of t

Calculate the μr & σr for m number of PRR sample over time interval of t

if ($\mu r \leq Tr$ && $\mu s \leq Ts$ && $\sigma s \leq 1$ && $\sigma r \leq 1$) then

Ji = absent

else

Ji = present

End Procedure

When the STA detects the presence of jammer in the channel, it simply sends the information to AP. If the AP receives the message form the STA about the presence of jammer or it detects by itself, immediately AP initiates its spectrum selection phase. The adversary and PU detection module checks the data transmission channel periodically for the presence of the PU activity or jammer.

Available Channel Repository Creation:

Initially the proposed system assigns the channel identity for each RF spectrum and makes an entry for each channel in the available channel repository.

Table 2: Initial Available Channel Repository of 'AP1'

Rank	Channel Identity	Number of times Spectrum Accessed
1	1	0
1	2	0
1	3	0
1	4	0
1	5	0

A record for each channel contains rank, channel identity ci and number of times spectrum accessed ai, where i range from 1 to n. The initial available channel list of the 'AP1' with five channels is shown in the table.1. The rank of every channel was assigned '1', because the data transmission is not yet started while creating the repository.

Repository Upgradation and Ranking Available Channels:

After the identification of adversary and primary user by the detection phase, channel selection phase is triggered. When the channel selection phase was initiated, number of times spectrum accessed for a channel is updated. Each time the detection of attacker or PU in the spectrum 'i' by a SU, makes that SU to increment the field 'ai' by 1. Once the number of times spectrum accessed was updated, the rank of all the channels was changed based on the field 'a'.

Table 3: Available Channel Repository of 'AP1' for first scenario

Rank	Channel Identity	Number of times Spectrum Accessed
1	2	0
1	3	0
1	4	0
1	5	0
2	1	1

Table 4: Available Channel Repository of 'AP1' for second scenario

Rank	Channel Identity	Number of times Spectrum Accessed
1	3	9
1	4	9
1	5	9
2	1	14
2	2	14
3	6	23
3	7	23

The ranks are assigned based on the number of times spectrum accessed. The channels which have same 'a' value is assigned to a same rank. Consider the first scenario, where channel c1 is currently utilized by 'AP1'. In this scenario the jammer J1 starts disturbing the communication in the channel c1, which is identified by the detection module of the node 'AP1'. The result of the available channel list after detection of jammer 'J1' is shown in the table.3. Except channel C1, all other channel's 'a' value are similar. So the ranks assigned for C2, C3, C4 and C5 is '1'. Since the number of times spectrum accessed for channel C1 is higher than all other available channels with the rank of '1', C1 is assigned with next rank '2'. The available channel repository of 'AP1' after assigning rank is shown in the table.3. In another scenario 'AP1' detects attacker or PU nine times in the channel C3, C4, C5, fourteen times in the channel C1, C2 and twenty three times in channel C6 and C7. Since the number of times spectrum accessed for channel C3,C4,C5 are same and less compared with other channels, these channels are assigned with the rank '1'. Channel C1, C2 have 'a' value greater than rank '1' channels, but lesser than rest of the channel. So the rank '2' is assigned to C1, C2. The channel C6, C7 achieves the next high 'a' value, so those channels are assigned with the rank '3'. The available channel repository for 'AP1' after updating the 'a' value and assigning rank is illustrated in the table.4.

Channel Selection phase:

When the attacker or PU is detected in the current data channel, the spectrum selection phase is invoked. The Channel selection phase detects next channel for communication using two modules: upper bound selection and partial random channel selection.

Upper Bound Selection:

The upper bound selection module gets the available channel from the repository upgradation and ranking available channel module. The upper limit U for the selection of channel was set using the upper bound selection (UBS) algorithm.

UBS Algorithm:

Input : Available channel repository

Output : Upper limit U

Procedure

L=Number of entries in the available channel repository

```
Temp = 1
U = 0
for i = 1 to L then
{
if (Rank (Repository[i]) == Temp)
{
U = U + 1
}
else
{
Ratio = i / L
if ( Ratio <  T )
{
Temp = Rank (Repository[i])
}
else
exit
}
}
End Procedure
```

The number of channels with the same rank and less value in the number of times the channel access were included in the upper limit. If the ratio calculated between the number of channels in the first rank and total number of available channel L was below the threshold T, the channels in second rank were considered for the upper limit. Still the count of the channels in the first and second rank was not sufficient to reach the threshold, considered the next rank. This process was continued until the ratio calculated on the number of channels in the selected rank with the previous count was more than the threshold. Once the calculated ratio crosses the threshold, the upper limit was fixed and passed for partial random channel selection phase.

Partial Random Channel Selection:

The partial random channel selection (PRCS) algorithm selects the next data communication channel. The upper limit U was set by the upper bound selection module. Random selection was limited up to the limit U. The limit was selected based on the number of times the channel accessed statistics. This algorithm is given below with the limit U and the ranked available channel repository as input.

PRCS Algorithm:

Input : Upper limit U and available channel repository

Output: Channel selected S

Initialize: Interval I=V1, Start_random R=V2, Pseudo noise P =R

Procedure:

If P >(R+I) then

P=R;

else

P=P+1;

RS = rand(security_key+P);

S = RS % U;

End Procedure

The upper limit U was the index position of the repository within that range random selection S was done. The RS was the random seed which was mapped between the range 1 and U. The random seed was selected using the random function with the seed of security key and pseudo noise P. Each AP was assigned with a unique security key, within an AP each random selection was varied using the pseudo noise P. The pseudo noise starts with the base value V2 and incremented by after each selection until the value V1, where V1 and V2 are constant values. Finally the new channel selected information was communicated to all the stations associated with the AP, which initiated the channel selection phase.

RESULTS AND DISCUSSION

Cognitive Wi-Fi network performance is analyzed under the periodic deceptive jamming attack. The Cognitive Wi-Fi network is designed with three radios in AP and one radio in STA. The APs and STAs of the different cognitive Wi-Fi network cluster are placed in the spatial area of 10m x 10m to achieve the overlapping of transmission range of all the clusters on one another. Each AP is associated with two STAs.

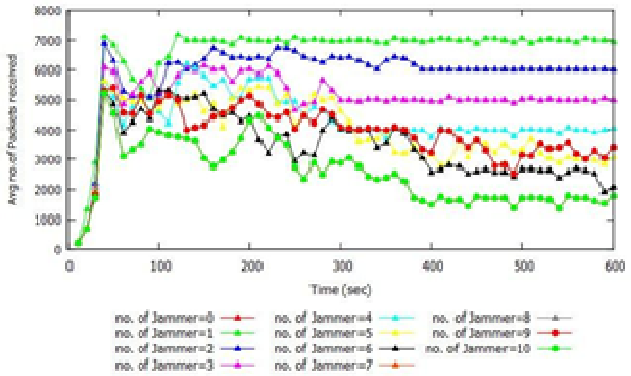

Fig. 2: RCS - Throughput

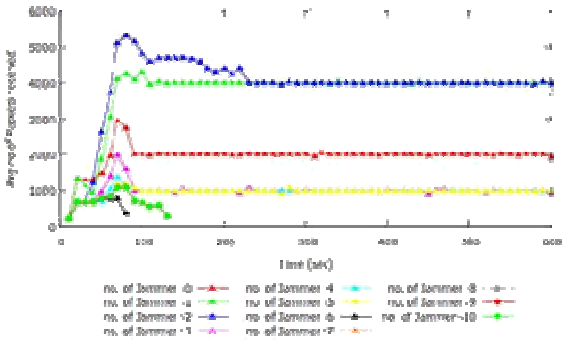

Fig. 3: SCS – Throughput

The scenario of 12 different clusters with three nodes in each is implemented. One AP is placed in each cluster. To resemble the internet traffic of Wi-Fi network, downlink traffic load is kept high from AP to STA. The three non-overlapping bands of 24MHZ width are used. The number of jammer is varied from 0 to n, where n is the number of channels including ISM band and licensed band. The throughput of the network under jamming attack with the number of jammer varying from 0 to 10 is illustrated in figure.2, 3 and 4.The channel switching latency parameter is used to analyze the overhead of the channel switching phase in terms of latency. The latency is recorded immediately after detection of PU or jammer presence in the channel until the successful selection of data channel for communication. The percentage of channel switching latency overhead is shown in the Table.5. It shows that Cognitive Wi-Fi network using PRCS and RCS is survived in all the cases but the throughput of SCS throughput reaches almost lower bound. When the neighbor clusters also follow the SCS strategy then there is a possibility

that all the clusters in the same transmission region end up with the same channel, which leads to the degradation of performance in terms of throughput. But the RCS is completely random and PRCS is partially random, so the possibility of choosing the same channel by neighbor cluster is reduced. The throughput of the PRCS is better than RCS after all 10 channels are attacked, until that case the RCS and PRCS produces near about same throughput.

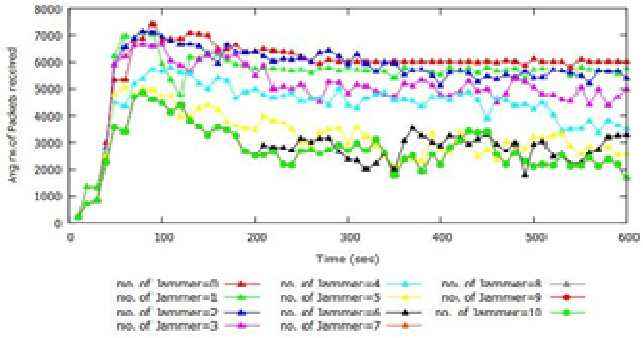

Fig. 4: PRCS - Throughput

Table 5: Channel Switching Latency

Number of Jammer	Latency Ratio		
	SCS	PRCS	RCS
0	0.06	0.082	0.09
1	0.059	0.22	0.23
2	0.06	0.064	0.06
3	0.057	0.07	0.1
4	0.057	0.07	0.07
5	0.06	0.62	0.16
6	0.06	0.09	0.125
7	0.06	0.099	0.13
8	0.06	0.099	0.13
9	0.06	0.099	0.13
10	0.06	0.099	0.13

Conclusion:

The weight based channel selection and Partial Random Channel Selection Strategies are discussed in detailed for a system model of cognitive Wi-Fi network. According to the experimental result it is concluded that the two proposed strategies excludes the overhead due to monitor and maintenance of information about the neighbors in other cluster and traffic created by other clusters. Since the SCS do not depend on the random selection, it does not experiences the channel switching delay due to randomness but it is not efficient in terms of throughput. Similarly the RCS is efficient in terms of throughput, while in terms of channel switching latency the PRCS is better than RCS. Since PRCS is implemented using the partial randomness, it acquired the efficiency in terms of both high throughput during jamming and reduced channel switching latency.

REFERENCES

Alex Chia-Chun Hsu, David S.L. Wei and C.C. Jay Kuo, 2007. "A Cognitive MAC Protocol Using Statistical Channel Allocation for Wireless Ad-hoc Networks", IEEE Communications Society Conference Proceedings of WCNC.

An Liu, Peng Ning, Huaiyu Dai, Yao Liu, 2010. "USD-FH : Jamming-resistant Wireless Communication using Frequency Hopping with Uncoordinated Seed Disclosure", IEEE International conference on Mobile Adhoc and Sensor Systems.

Baldini, G. and *et al*., 2012. "Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead", IEEE Communications Surveys & Tutorials, 14: 2.

Ejaz Ahmed, Muhammad Shiraz, Abdullah Gani, 2013. " Spectrum-aware Distributed Channel Assignment for Cognitive Radio Wireless Mesh Networks", Malaysian Journal of Computer Science, 26: 3.

Hai Su, Qian Wang, Kui Ren and Kai Xing, 2011. "Jamming-Resilient Dynamic Spectrum Access for Cognitive Radio Networks", IEEE ICC.

Hu, W., T. Wood, W. Trappe and Y. Zhang, 2004. "Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service", in ACM Workshop on Wireless Security.

Konstantios Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy, 2011. "Denial of Service Attacks in Wireless Networks: The Case of Jammers", in IEEE Communication Survey & Tutorials, 13: 3.

Mubashir Husain Rehmani, Aline Carneiro Viana, Hicham Khalife, Serge Fdida, 2013. "SURF: A distributed channel selection strategy for data

dissemination in multi-hop cognitive radio networks", Computer Communications., 36: 1172-1185.

Qurratul-Ain Minhas, Mohamed A. Tawhid and Hasan Mahmood, 2014. “Efficient Power and Channel Allocation Strategies in Cooperative Potential Games for Cognitive Radio Sensor Networks”, International Journal of Distributed Sensor Networks.

Rohit Negi, Arjunan Rajeswaran, 2005. " DoS analysis of reservation based MAC protocols",IEEE.

Wang, L.-C., C.-W. Wang, F. Adachi, 2011. "Load-balancing spectrum decision for cognitive radio networks", IEEE Journal on Selected Areas in Communications., 29(4): 757-769.

Wenjing Wang, Shameek Bhattacharjee, Mainak Chatterjee, Kevin Kwiat, 2013. “Collaborative jamming and collaborative defense in cognitive radio networks”, Pervasive and Mobile Computing.

Xu, W., K. Ma, W. Trappe and Y. Zhang, 2006. “Jamming sensor networks: attack and defense strategies,” Network, IEEE, 20(3): 41-47.

Yongle Wu, Beibei Wang, K.J. Ray Liu and T. Charles Clancy, 2012. " Anti-Jamming Games in Multi-Channel Cognitive Radio Networks", IEEE Journal On Selected Areas In Communications, 30: 1.

Yu, F.R. and *et al*., 2009. “Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios”, IEEE Military Communication Conference.

Yuhua Xu, Alagan Anpalagan, Qihui Wu, Liang Shen, Zhan Gao and Jinglong Wang, 2013. “Decision-Theoretic Distributed Channel Selection for Opportunistic Spectrum Access: Strategies, Challenges and Solutions”, IEEE Communications Surveys & Tutorials, 15: 4.