International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 5965-5970
© Research India Publications
http://www.ripublication.com

Jamming-Resistent Frequency Hopping for Cognitive Radio Networks Security: Survey

K.Karunambiga [1], M.Sundarambal [2], S.Saranya Rubini [3]

[1] Department of CSE, College of Engineering Guindy, Chennai.
Email : karunambiga.cse12@gmail.com
[2] Department of EEE, [3] CSE&IT,
Coimbatore Institute of Technology, Coimbatore

Abstract

Wireless devices are used in a wide range of real world practical applications which typically operate in unlicensed ISM band that leads to spectrum scarcity. Cognitive Radio Networks (CRN) is an emerging technology used for improving spectrum utilization. One of the key challenges of CRN is to perform reliable control information exchange with the coordinator, which ensures availability of the network. This issue can be addressed using frequency hopping (FH) technique. Frequency Hopping is the easiest method that provides protection against interference and jamming. This paper analyses various existing frequency hopping schemes for wireless network and its scope towards secure communication in cognitive radio networks.

Keywords- Cognitive Radio; jamming; Spectrum sensing; DSSS; Frequency Hopping; Uncoordinated FH

I. INTRODUCTION

Wireless services greatly increase the demand for advancement in wireless technology that introduced several devices such as Wi-Fi, Wi-Max, Bluetooth, Wireless sensors, RFID and so on. This exponential growth of wireless devices has caused the frequency spectrum to become crowded. Hence Wireless devices undergo spectrum scarcity which can be resolved using CRN.

A. *Cognitive Radio Network*

Cognitive radio network enables the opportunistic use of licensed frequency band. Opportunistic spectrum usage means a band of frequencies that are not being used by the primary user of that band at a particular time in a particular geographic area [1].

CRN must guarantee interference free primary user’s operation in licensed spectrum. To achieve this cognitive radio (CR) has to periodically sense the electromagnetic environment to detect the primary user’s activity in the licensed spectrum and other CR’s operations. Primary users seize their frequency at anytime while the secondary user with cognitive radio is operating on their band. In order to prevent the interference with the licensed user, the sensing method of CR should detect the presence of primary user within a short duration.

B. *Spectrum Sensing and Dynamic Spectrum Access*

Spectrum sensing is the ability of CR to collect the channel usage pattern to guide the Dynamic Spectrum Access (DSA). DSA is a protocol used to identify the white space in spectrum for secondary user communication. DSA can be implemented in centralized or distributed Architecture. In centralized protocol, a single CR node coordinate control information exchange and decide the spectrum selection, but in the distributed protocol cluster heads make its own decision for spectrum access with the exchanged control information. In spite of the architecture, DSA protocols seamlessly blend on the exchange of sensing information with the coordinator. Those control information can be exchanged using two ways: i) Cognitive Pilot Channel (CPC) [2] or Common Control Channel (CCC) and ii) Time slotted sensing phase and transmission phase in a single channel. Ensuring reliable sensing information exchange is mandatory to assure secure dynamic spectrum access for secondary users without interrupting primary user’s operation.

C. *Challenges in Reliable Control Messages Broadcast*

Time slotted sensing phase and CCC facilitate the cooperation among the cognitive radio secondary user’s to share the opportunistic licensed band. Common control channel jamming, selective jamming of sensing phase particularly devastates the cognitive radio network availability, because of their cooperative nature. Jamming is an attack launched by the malicious node to block the access to the medium. Interference and jamming attacks have been analyzed and addressed as a degradation of obtaining the accurate view of the spectrum usage pattern and performance in CRN.

Frequency Hopping (FH) is an effective technique for frequency diversity and interference diversity. Frequency hopping is a channel switching technique which hops from one frequency spectrum to another. It has been employed in order to avoid the interference and to overcome the jamming attack [3]. This survey focuses on analyzing the jamming resistant frequency hopping methods and the reliability provided by those channel switching techniques for cognitive radio network.

II. IMPACT OF FHSS TECHNIQUES ON JAMMING

Jamming is the easiest attack launched in the wireless environment. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DHSS) are two commonly adapted spread spectrum techniques to counteract jamming attack. The use of FHSS and DSSS methods make the jamming attack more difficult to launch. DSSS works in a wideband which can be used for short range wireless communication.

In cognitive radio network the spectrum is accessed in opportunistic manner, which cannot guarantee the wideband for communication. FHSS uses the narrow band carrier frequency for communication which best suits CRN. Transmitter and receiver CRs have to hop between the frequency spectrum and transfer data. Traditionally, frequency hopping is considered as solution for jamming attack [5]. Even, if the current channel is interfered by jammer, frequency hopping technique sends the message successfully once the CR switches to a new frequency band. To resolve the jamming problem in the CRN the frequency hopping techniques can be applied. The most efficient frequency hopping techniques for jamming are proactive and reactive frequency hopping.

III. PROACTIVE FREQUENCY HOPPING

In proactive frequency hopping (PFH) the set of transceivers hop channels for every n seconds irrespective of jammer in the current channel and hopping channel. Since channel hopping takes place for every n seconds it is difficult for the jammer to identify the current channel of the CR. It is robust when appropriate n value is chosen and high hidden probabilistic frequency hopping sequence is designed. Figure 1 and 2 shows the typical steps in frequency hopping sender and receiver that depend on the Pseudo Noise (PN). Pre-shared secret key controlled pseudo-random used for frequency hopping pattern, in the wireless environment is referred as pseudo noise [8].

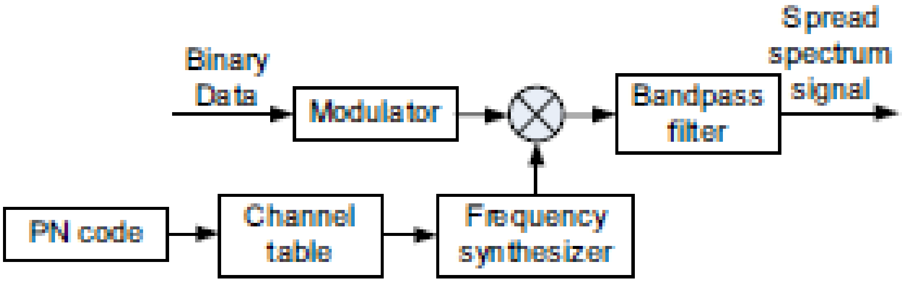

Figure 1. **Frequency Hopping Sender**

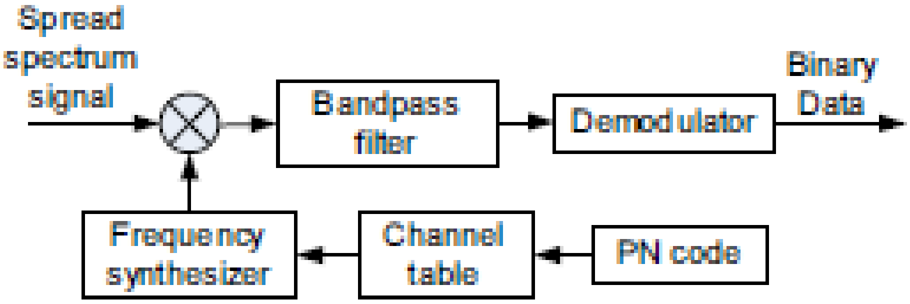

Figure 2. **Frequency Hopping Receiver**

Navda *et al* [4] use pseudo random with PFH, to generate the same set of frequency hopping sequence by the sender and receiver. It makes the sender and receiver to synchronize in the same frequency band for communication. But the jammer energy between the adjacent orthogonal channels is not considered. Konstantios *et al* [5] proposed a measurement driven, analytical framework proactive frequency hopping to cope with jamming. Game theoretic framework was provided to capture the interactions between the legitimate communication link and a jammer. The link chooses its channel randomly, using a probability distribution *x*, while the jammer picks its channel as per a probability distribution *y*. The expected link throughput is

$$v = x^T A y \tag{1}$$

The payoff matrix *A*, is the percentage of jamming-free throughput that the legitimate link obtained when the jammer do not resides on the channel. The success of anti-jamming depends on the payoff matrix. These conventional anti-jamming has the performance penalty due to the periodic channel switching in the absences of jammer.

IV. REACTIVE FREQUENCY HOPPING

Channel hopping will take place in the reactive frequency hopping scheme, when the jammer interferes with the current channel [6]. The Synchronization between the pair of communication devices is the great challenge in reactive frequency hopping. When the wireless device detects the jamming attack, immediately it switches to a new available channel without giving any information about the channel switching to other devices. Pair-wise Uncoordinated frequency hopping (UFH) was proposed in [9] as an anti-jamming technique. It is based on rapid channel switching over a large frequency range. But this method has to send each packet multiple times due to the uncoordinated channel selection between the legitimate sender and receiver. Efficiency of the wireless communication is low in UFH–based techniques.

The basic idea of USD-FH is to transmit each key establishment message that use a one-time pseudo-random hopping pattern and disclose the seed of the pattern in an uncoordinated manner. In [10], USD-FH scheme was used to convey the frequency hopping pattern information between the wireless nodes, that frequency pattern was later used for data transmission under coordinated frequency hopping. This method helps in hiding frequency hopping pattern for data communication from the jammer. This method improves efficiency and robustness of communication between a pair of nodes but there is a possibility for more than one pair selecting the same frequency hopping pattern for data transmission. This conflict is overcome using the collaborative UFH-based broadcast approach [7].

The main objective of the collaborative UFH-based broadcast approach is to allow the group of nodes that already received the message to relay the same to other receivers that expects those broadcast message. This process starts slowly but it accelerates the speed of broadcast when more number of nodes joins the group. Unlicensed frequency hopping and collaborative unlicensed freq hopping are the major solutions for jamming attack that do not depend on pre shared secret key. UFH scheme directly broadcasted information from the source node to the destination node. The relay based broadcast was implemented in the collaborative UFH for successful communication as shown in the figure 3 [11].

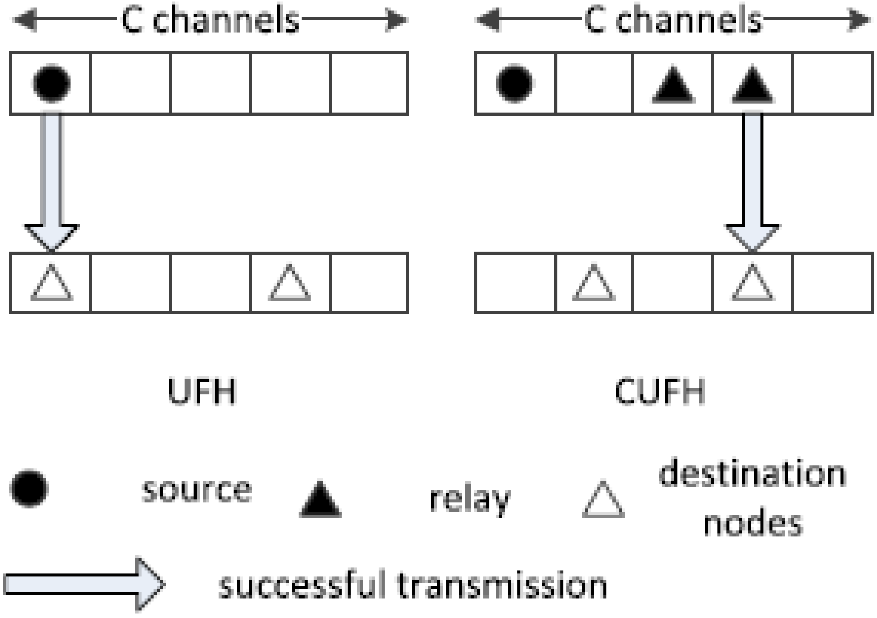

Figure 3. UFH and Collaborative UFH (CUFH)

V. ANALYSIS OF JAMMING RESISTENT FREQUENCY HOPPING FOR CRN

The performance and availability of the cognitive radio network depends on reliable sensing and secure exchange of control information about spectrum status with the coordinators. The sensing information has to be updated with the coordinator via in-band or out-band method. In the out-band scheme common control channel was deployed to send the spectrum usage pattern to the coordinator in CRN. Sensing phase in the time-slotted approach was used for exchange of control messages. The pseudo random methods and game theory based analytical framework addresses the common control channel jamming. The pre-shared secret key based pseudo random and game theory approach hides the frequency hopping pattern from the jammer. Collaborative UFH match the requirement of anti-jamming against the sensing phase selective jamming. The broadcast nature of the Collaborative UFH can resist the sensing phase jamming.

VI. CONCLUSION

Jamming resistant frequency hopping techniques for wireless communication were analyzed and its applicability for cognitive radio network was discussed. One of the key vulnerability of proactive frequency hopping is the pre-shared secret key, so research are ongoing to address this key challenge. Reactive frequency hopping has the benefit of channel switching only in the presence of jammer. But the communication efficiency is low due to uncoordinated frequency hopping. The synchronization between the communication devices is still an open issue in UFH.

REFERENCES

[1] P. Kolodzy et al., "Next generation communications: Kickoff meeting", in Proc. DARPA, Oct. 2001.

[2] J. P. Romero, O. Sallent, R.Agusti, and L. Giupponi, "A novel on- demand cognitive pilot channel enabling dynamic spectrum allocation", in 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, (DySPAN'07), April 2007, pp. 46-54.

[3] Konstantios Pelechrinis, Marios Iliofotou, and Srikanth V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers", in IEEE Communication Survey & Tutorials, Vol. 13, No.3, 2011.

[4] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using Channel Hopping to Increase 802.11 Resilience to Jamming Attacks", in IEEE INFOCOM mini-conference, 2007.

[5] Konstantios Pelechrinis, Christos Koufogiannakis, and Srikanth V. Krishnamurthy, "On the efficacy of Frequency Hopping in Coping with Jamming Attacks in 802.11 Networks", IEEE Transactions on Wireless Communications, Vol. 9, No. 10, Oct. 2010.

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

[7] Liang Xiao, Huaiyu Dai, Peng Ning, "Jamming-Resistant Collaborative Broadcast Using Uncoordinated Frequency Hopping", IEEE Transaction on Information Forensics and Security, Vol. 7, No. 1, Feb. 2012.

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

[9] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping", in Proc. IEEE symposium on security and privacy, 2008.

[10] A. Liu, P. Ning, H. Dai, and Y. Liu, "USD-FH: Jamming-resistant wireless communication using frequency hopping with uncoordinated seed disclosure." in Proc. 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems, 2010.

[11] Chengzhi Li, Huaiyu Dai, Liang Xiao, Peng Ning , "Communication Efficiency of Anti-jamming Broadcast in Large-scale Multi-Channel Wireless Networks", IEEE Transactions on Signal Processing, Vol. 60, No.10, Oct. 2012.