Cognitive Radio Based Jamming Resilient Multi-channel MAC Protocol for Wireless Network

Zaw Htike, Choong Seon Hong
Department of Computer Engineering, Kyung Hee University,
1 Seocheon,Giheung, Yongin, Gyeonggi, 449-701 Korea
htike@networking.khu.ac.kr
cshong@khu.ac.kr

Abstract

Radio jamming attack is the most effective and easiest Denial-of –Service (DOS) attack in wireless network. In this paper, we proposed a multi-channel MAC protocol to mitigate the jamming attacks by using cognitive radio. The Cognitive Radio (CR) technology supports real-time spectrum sensing and fast channel switching. By using CR technologies, the legitimate nodes can perform periodic spectrum sensing to identify jamming free channels and when the jamming attack is detected, it can switch to un-jammed channel with minimum channel switching delay. In our proposed protocol, these two CR technologies are exploited for thwarting the jamming attacks.

1. Introduction and Motivation

In wireless network, jamming is quite easy since the devices use single channel communication. Attackers need no or basic knowledge of MAC and PHY layers to launch radio jamming attacks. The adversaries can simply transmit radio signals or forge packets to disturb the transmissions of legitimate users which lead to denial of service (DOS).

In this paper, a multi-channel MAC protocol has been proposed for thwarting the jamming attacks and it exploits the Cognitive Radio (CR) technology which supports real-time spectrum sensing and fast channel switching [1]. Real-time spectrum sensing allows the devices to perform periodic spectrum sensing to identify unused channels and when jamming is detected fast channel switching will allow the devices to switch among different channels with minimum delay.

Many multi-channel schemes for thwarting the jamming attacks have been proposed in [4] [5] [6] [7]. In most of multi-channel concepts, the channel hopping sequence used by legitimate communication is pre-defined by a pseudo-random sequence and the channel hopping is performed periodically with or without jammers [3]. It can contribute to un-necessary hopping and as a result it will increase the channel switching time. Moreover, there is no guarantee that all pre-defined channels are totally available for communication. For example, some of pre-defined channels already have been jammed by attackers and it is possible for the legitimate nodes to switch to the jammed channels. Thus, this will degrade the average throughput of the network if the number of pre-defined channels which already have been jammed is high.

This work was supported by the IT R&D program of MKE/KEIT. [2009-S-014-01, on the development of Sensing based Emotive Service Mobile Handheld Devices] Dr. CS Hong is corresponding author.

3. Cognitive Radio Based Channel Switching Mechanism

In our scheme, both sender and receiver sense all available channels and build their own free channel list (FCL) according to the power sensed by each of them. For example, the channel with lowest power level will be the top of the list.

After building a FCL, the sender sends it to the receiver. The receiver checks its own FCL and matches the common channels available to both nodes in order to create a common free channel List (C-FCL). The C-FCL will be sent back to the sender. It will be maintained and used by both nodes. Both nodes, sender and receiver, will perform the above operation periodically to update the C-FCL. If the sender has data packets to send, it will send it instead of CFL and the receiver will acknowledge with AKC as shown in Figure 1.

Updating the C-FCL mechanism serves not only for channel selection but also for assuring the currently used channel is reliable. Updating the C-FCL is performed by exchanging the channel selection packets (CFL and C-FCL) of two communication parties. Thus, the channel is safe as long as the channel selection packets can be exchanged periodically which implies updating the C-FCL is performed successfully. Otherwise, we can assume that the current channel is not reliable although the channel selection packets

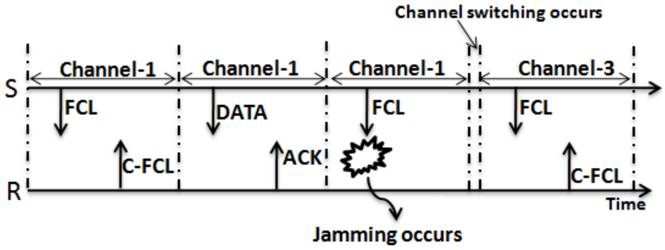

Fig.1 After detection a jamming attack at currently used channel, channel 1, both nodes will migrate to un-jammed channel, channel-3

absences occur accidentally or intentionally

When the jamming attack occurs the channel selection packets of both nodes cannot be exchanged successfully as show in Figure 1. Therefore, when no FCL from sender is received within a definite time interval, the receiver will monitor the current channel. If it senses the high power level, it will determine that the currently used channel is being jammed because high power level should correspond to high throughput. Thus, it will switch to an un-jammed channel, one of the free channels, according to the C-FCL it maintains. From the sender side, it sends its FCL to receiver and waits for C-FCL. If it does not receive C-FCL within definite time interval, it will also monitor the power level of current channel. The sender will also determine that the current channel is being jammed if it senses the high power level. Otherwise both nodes will stay at the current channel and try to perform channel selection mechanism at next time slot. But it does not guarantee that the jamming signal will last long enough to be sensed by both nodes. Thus, if the channel updating cannot be done within two time slots, both nodes will migrate to un-jammed channel at the beginning of next time slot even though they did not sense any high power level. To maintain synchronization between two nodes, we defined both nodes to perform channel switching only at the beginning of time slots.

After migrating to an un-jammed channel, the nodes will perform the channel selection mechanism and update C-FCL. This current channel will be used for any communication between two nodes till next jamming attack is detected.

4. Discussion and Conclusion

It is obvious that the impact of jamming attacks depends on total number of available channels in the network. The more channels it uses, the more difficult for the attacker to jam all channels.

As a drawback, using more channels can cause higher channel sensing time. All legitimate nodes have to sense every available channel to create their own FCL. No data packet can be sent while channel sensing is performed. Thus, longer channel sensing time can degrade average throughput of the network. However, this can be traded off according to the jammer's behaviors. For example, if the jammer is lacking in knowledge of CR technology, the network can use only few channels.

Jamming attacks are serious threat in any kind of wireless network. In this paper, we proposed a multi-channel concept based on the next generation Cognitive Radio (CR) technology to mitigate the jamming attacks. According to our proposed protocol, if there is only one available channel for both nodes, any communication can be performed well like communicating in jamming free environment.

REFERENCE

[1] Sampath, A. Hui Dai Haitao Zheng Zhao, B.Y., "Multi-channel Jamming Attacks using Cognitive Radios" Computer Communications and Networks, 2007. ICCCN 2007

[2] Kaigui Bian and Jung-Min Park, "MAC-Layer Misbehaviors in Multi-Hop Cognitive Radio Networks" Wireless Personal Communications Symposium , 2006

[3] Sherif Khattab, Daniel Mosse and Rami Melhem, "Jamming Mitigation in Multi- Radio Wireless Networks: Reactive or Proactive?" Proceedings of the 4th international conference on Security and privacy in communication networks, 2008

[4] G. Alnifie and R. Simon, "A multi-channel defense against jamming attacks in wireless sensor networks," in 3rd ACM workshop on QoS and security for wireless and mobile networks, 2007, pp. 95-104.

[5] L. Lazos, S. Liu, and M. Krunz, "Mitigating control-channel jamming attacks in multi-channel ad hoc networks," in second ACM conference on Wireless network security, 2009, pp. 169-180.

[6] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in 3rd ACM workshop on Wireless security, 2004, pp. 80-89.

[7] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks,"in IEEE INFOCOM 2007, 2007, pp. 2526-2530.