IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 12, Issue 3 Ver. II (May – June 2017), PP 118-123
www.iosrjournals.org

Efficient Anti-Jamming Technique Based on Detecting a Hopping Sequence of a Smart Jammer

Yongchul Kim[1], Jungho Kang[2]
[1](Department of Electrical Engineering / Korea Military Academy, Korea)
[2](Department of Computer Science / Korea Military Academy, Korea)

Abstract:*Military wireless communications have always been involved in the improvement of secured tactical Communications. However, securing such networks on a battlefield is far from being simple since wireless jamming attack can be easily done by emitting a continuous radio signal. Especially, a smart jammer is able to send back-to-back packets on the detected channel after scanning all of the channels. Finding a perfect way to avoid jamming is a utopia, but one of the well-knownsolutionsto mitigate jamming attacks is a channel-hopping scheme.In this paper, we consider an existing channel-hopping scheme under smart jammer attacks, and propose an efficient anti-jamming technique that canprotect users from jamming attack by finding outthe hopping sequence of a jammer.Through numerical analysis, we show that the proposed anti-jamming scheme can significantly improve the throughput performance.*

Keywords: *Anti-Jamming, Channel Hopping Scheme, Smart Jamming, WLAN*

I. Introduction

IEEE 802.11 WLAN is the most widely used standard for providing last-hop wireless access to user terminals.It is very useful technology for the operational environment where the installation of a wired network is impractical, and provides high bandwidth to users in a limited geographical area. The Army has always been involved in the improvement of WLAN technologies, to be able to use it on military operations.The US Army uses secure wireless local area network (SWLAN) [1]based on IEEE 802.11 for their Tactical Operation Center's (TOC) communications. SWLAN is considered to be one of the key subsystems of the command, control, communications, computer, and intelligence (C4I) system. Although the SWLAN is efficient, it cannot fully avoid a jamming attack sent by an opponent, especially if this jammer is considered as smart, because a smart jammer is able to attack ongoing data communications by sending send back-to-back packets on the detected channel after scanning all of the channels. Generally, a jamming attack is achieved by introducing a source of noise, strong enough to significantly reduce the capacity of the channel, i.e., a jamming attack could disrupt a wireless network. There is also an 802.11 based jammer that can disguise itself as a legitimate station. Many different types of jammers are introduced in the literature [2, 3]. One of the well-known techniques for mitigating jamming attack is a channel-hopping scheme. This scheme is a sequence-based approach that periodically hops to the next channel by changing the operating frequency and has been widely used in many technologies such as Bluetooth, WLAN, and WirelessHART [4].Navda et al. [5] show how to protect 802.11 networks from jamming attacks by having the legitimate transmission hop among channels to hide the transmission from the jammer. Jeong et al. [6] propose a new channel-hopping scheme based on IEEE 802.11h dynamic frequency selection (DFS) mechanism which enables hopping to a best channel with full channel measurement. Lee et al. [7] propose a randomized channel-hopping scheme that can be used in various jamming attack environments. Generally, channel-hopping schemes can be categorized into two groups: proactive channel hopping [8] and reactive channel-hopping [9]. In the proactive channel hopping schemes, every node periodically hop to the next channel regardless of the presence of jamming attacks and the status of channels. Thus the effectiveness of proactive scheme might be significant under the frequent jamming attackenvironment while the channel efficiency will degrade due to unnecessary hopping. In contrast, in the reactive channel hopping schemes, nodes do not hop to the next channel unless there is a noticeable difference in channel status. This reactive channel-hopping scheme can be very efficient when there is no jamming attack, however it can be easily detected by a smart jammer due to long channel duration.Khattab et al. [10] analyze the both proactive and reactive channel-hopping schemes in terms of single radio and multi radio systems, respectively. They also show that the both schemes have almost the same performance when energy efficiency is considered as a performance metric. Jeung et al. [11] propose a deception mechanism to mitigate smart jamming attack by deceiving the jammer to attack an inactive channel. Whenever the smart jammer starts jamming after detecting the current channel, every node except one that is currently using the channel will hop to the next channel to avoid jamming attack. That is, only one node sacrifices itself to protect the rest of nodes from the jamming attack. However the damage of the sacrificial node can be significant and it may not be acceptable for the

military communications where every node must be equally guaranteed to transmit data. To overcome this problem, we propose a new anti-jamming technique based on finding the hopping sequence of a smart jammer to prevent all users from the jamming attack.

The remainder of the paper is structured as follows: section II represents the system models and introduces deception mechanism. After introducing the proposed anti-jamming technique in section III, performance results and findings are subsequently presented in Section VI. Finally conclusions are drawn in Section V.

II. Channel Hopping Schemes

In this paper, we focus on proactive channel-hopping system to analyze the efficiency of anti-jamming performance under a smart jamming attack environment. In general, every useris allowed to hop to the next channel after certain amount of time regardless of channel status. We define this time duration as a Dwell Time (DT). And a time needed to hop is called switching time (ST) as shown in Fig. 1. That is, a user node transmits frames during a DT period and hops to the predetermined channel during an ST. An ST is a constant value but a DT period can vary according to the jamming intensityand has an impact on network throughput. Figure 1 shows a station and a jammer model in this system. When a jammer scans one channel, it takes one finding time (FT) and one ST. Let ST and FT be the same *t* seconds to simplify our model. Thus a DT can be expressedas αt,where $\alpha$is called DT slot.We assume that a smart jammer recognizes both ST and DT periods but does not recognize the channel-hopping sequence. Thus it scans all of the channels by its own random sequence to detect the currently used channel. When the jammer detects a channel *k*, it starts jamming by sending back-to-back packets. Generally, the smart jammer is able to jam the channel until the end of current DT period. However, the smart jammer checks whether or not the channel is still being used aftera jamming time (βt). Ifthe channel is still used by stations, the smart jammer re-jam the channel for another βt, but if the channel isnot used anymore after a βt, the jammer switches to another channel and restarts its scan process.

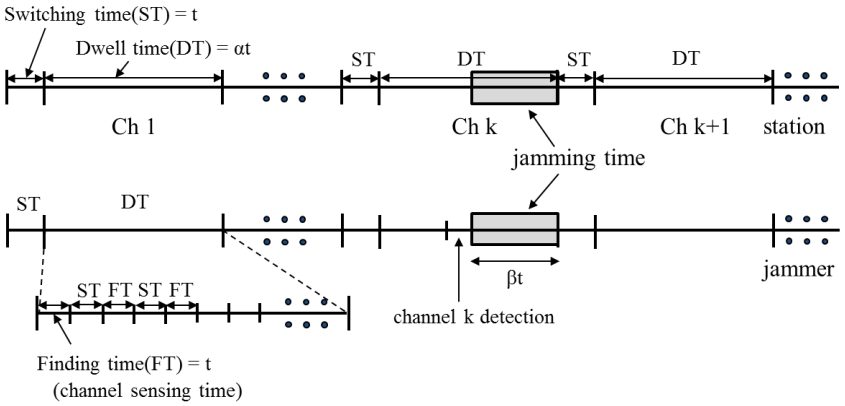


Fig.1: Station and jammer models

The deception mechanism proposed in [11] takes advantage of the characteristics of a smart jammer. When the channel is detected by a smart jammer, only one user node that is using the current channel must remain in the channel aftera βt and deceives the jammer to re-jam the channel until the end of the DT period while the rest of users hop to the next channel and continue to transmit data without jamming attack. Therefore, the deception mechanism can be significantly effective when the number of users in a network is high. To analyze the performances of the deception mechanism, we examine the network throughput by varying some parameters such as DT,βt, and the number of stations. The normalized achievable throughput under no jamming attack can be expressed as:

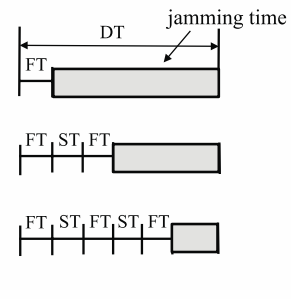
$$Throughput_1 = \frac{DT}{ST + DT}.$$

The whole time of the DT periodis used for data transmission and only ST periodisnot used for the transmission. Hence, the longer the DT period, the higher throughput can be achieved. In other words, even if there is no jamming attack, a short DT period can lead to throughput degradation. When a smart jammer exists in the considered system, the normalized achievable throughput will be degraded. In addition, the probability of detecting channel varies according to the duration of DT. In a short DT case, the probability of detecting channel will be lower, but for a long DT case the detecting probability by the jammer increases. A smart jammer

takes FT+ST times to scan one channel, thus if we denote with *N* the number of channels that the jammer scans during one DT period, *N* can be computed by:

$$\square = \frac{DT}{FT + ST}.$$

We also denote the total number of channels in the system and the probability that the jammer can detect the channel after scanning an $n_{th}(1,2,\dots,N)$ channel by L and p_n respectively (i.e., $p_n = 1/L$). Figure 2 shows the derivation of the channel detecting probabilityp_n.



$$n = 1,\ p_1 = \frac{1}{L}$$

$$n = 2,\ p_2 = \frac{L-1}{L} \times \frac{1}{L-1} = \frac{1}{L}$$

$$n = 3,\ p_3 = \frac{L-1}{L} \times \frac{L-2}{L-1} \times \frac{1}{L-2} = \frac{1}{L}$$

Fig.2: Channel detecting probability of a smart jammer

Therefore, the average jammed time during DT period can be expressed as:

$$E(t) = \sum_{n=1}^{N} (DT - nFT - (n-1)ST) \times p_n.$$

When a smart jammer starts jamming after detecting the channel, none of the users can transmit data through the channel until the end of the DT period. Thus the normalized achievable throughput under the smart jamming attack can be expressed as:

$$Throughput_2 = \frac{DT - E(t)}{ST + DT}.$$

The deception mechanism minimizes the damage from the jammer by allowing every node excluding one to hop to the next channel when the smart jammer successfully detected the current channel. The jammed node will remain on the same channel to deceive the jammer to stay until the end of the DT period. Hence the normalized throughput will be significantly enhanced when the many nodes in the system. Let γt be a summation of jamming detection, announcement, and switching time. Let also σ_n and k_n denote the time duration of jammed station and un-jammed station can actually use within a DT period respectively. Then the normalized achievable throughput of the deception mechanism is expressed as:

$$Throughput_3 = \frac{1}{M}\left(\frac{\sum_{n=1}^{N} \sigma_n p_n + DT(L-N)/L}{ST + DT} + \frac{\sum_{n=1}^{N} k_n p_n + DT(L-N)/L}{ST + DT} \times (M-1)\right),$$

Where *M* is the total number of users in the system. Even if the throughput enhancement can be achieved by the deception mechanism, the jamming attack cannot be fully avoided and also the effectiveness of the deception method is negligible when *M* is very small. In an extreme case, where there is only one node in a network, this mechanism is useless. To overcome this limitation, we introduce a fundamental solution for the smart jamming attack by detecting the sequence of a jammer.

III. Proposed Anti-Jamming Technique

The main idea of avoiding smart jamming attack is finding out the hopping sequence of the jammer. The user nodes and access point (AP) have their own predetermined hopping sequences to protect data transmission under jamming attacks, and the jammer also has its own predetermined hopping sequence to detect and jam the channel. The hopping sequence of a jammer is a set of numbers, and each number corresponding to a channel. In general, it is not feasible to find out the hopping sequence of a jammer. We made a reasonable assumption that there are two possible ways of scanning process of a jammer. First, the jammer restarts its sequence from the beginning whenever it detects a channel successfully within a DT period. Second, the jammer follows its sequence in order regardless of detecting a channel within a DT period. Figure 3 describes the first method with an example sequence of the jammer $\{3,5,1,4,8,7,6,2\}$and $L = 8$. This method prevents itself from scanning the whole channels with the same frequency, i.e., the latter parts of the sequence are less used for

scanning than the former parts. In contrast, the second method will use every channel equally for scanning as described in Figure 4. Thus we assume that a smart jammer performs the second method of hopping sequence.

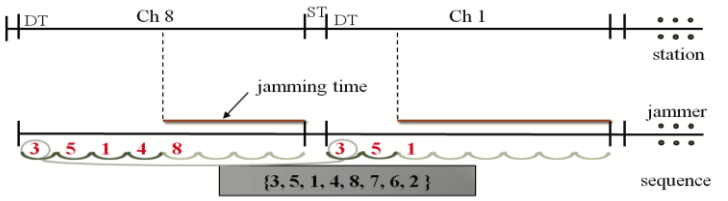


Fig.3: A smart jammer hopping sequence process 1

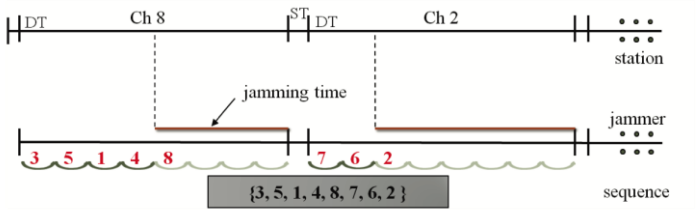


Fig.4: A smart jammer hopping sequence process 2

Our proposed anti-jamming technique provides how to find out the sequence of the smart jammer. When the number of scanning channels N is equal to the total number of channels L, then the jammer will be able to scan all the channelswithin a DT period. Since the jammer's hopping sequence includes all the channels, the jammer will detect the current channel successfully in every DT. The exact time when the jammer detects the channel is recorded by the AP, i.e., the time and channel information will be saved in the AP. In the next DT period, another time and detected channel information will be added. Consequently, the whole sequence of the jammer will be detected after $L \times DT$ periods.For example, as shown in Figure 5, channel 8 is used in the first DT period for every users and the AP. The next hopping channel for the users and the AP is channel 2. The jammer detects channel 8 in the 5^{th} scanning process and starts jamming until the end of the first DT period. In the next DT period, the jammer detects channel 2 in the 3^{rd} scanning process. Therefore, the two elements 8 and 2 are revealed in the hopping sequence of the jammer. The time that is needed to find the hopping sequence of the jammer is $L \times (DT + ST)$. After detecting the sequence of the jammer, the AP can modify the hopping sequence of the users in the system to avoid jamming attack from the smart jammer. Then the normalized achievable throughput will be enhanced as will be shown in the next section. When the DT period is short, i.e., $N < L$, this sequence finding method is also applicable. Figure 6 shows an example of how to find the hopping sequence of the jammer when $N < L$. Channel 2 is used in the first DT period for every users and the AP. The next hopping channel for the users and the AP is channel 6. The jammer detects channel 2 in the 5^{th} scanning process and starts jamming until the end of the first DT period. Thus, the AP knows that 4 channels have been scanned before channel 2 is detected. Therefore, channel 2 is the 5^{th} element of the hopping sequence of the jammer. In the next DT period, the jammer detects channel 6 in the 5^{th} scanning process. Hence the 5^{th} element from the previous detected element (channel 2) is channel 6. To find the whole elements of this sequence, the process is the same as in Figure 5.

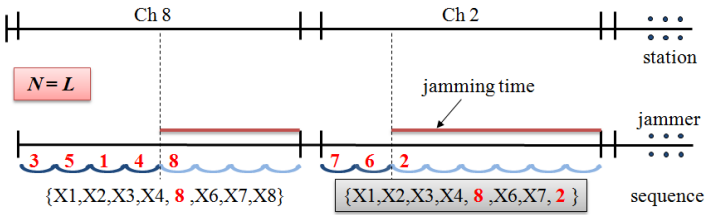


Fig.5: An example of how to find the hopping sequence of a jammer ($N = L$).

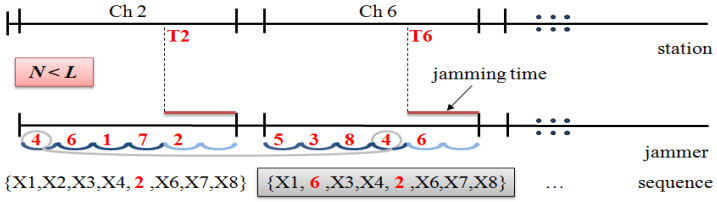


Fig.6: An example of how to find the hopping sequence of a jammer ($N < L$).

IV. Performance Analysis

In order to show the effectiveness of the proposed anti-jamming technique, we run the simulation to examine the normalized achievable throughput by varying DT periods. The total number of channels is 12 and the number of users varies from 1 to 10 ($L = 12, M = 1{\sim}10$). For the simplicity, we assume that the ST and FT are equal to $t = 5ms$. Thus the maximum value of the α is 24 ($L \times (FT + ST) = 24t$). We also assume that $\gamma t = 2t$ and $\beta t = 3t$. Figure 7 shows the normalized throughput results for different schemes as a function of the DT slot(α). The throughput Th_1 represents no jamming attack scenario. When there is no smart jamming attack, the throughput increases as the α increases. In contrast, the throughput Th_2 shows the result from the jamming attack. No additional hopping is allowed until the end of the current DT period leading to a significant damage when the DT slot α increases. The normalized throughput results between Th_1 and Th_2 represents the deception mechanism performances (Th_3). In an extreme case ($M = 1$), there is no throughput enhancement from the deception mechanism. However, when the number of user nodes increases ($M = 3{\sim}10$), the throughput enhancement also increases. The throughput enhancement is not proportional to the number of users in a network and converges to a certain level. When we run the simulation with $M = 50$, the throughput result was very similar to the Th_3 with$M = 10$. Although many other nodes are taking advantages from deception mechanism, one sacrificial node must suffer from the jamming attack. Therefore, more than 10% damages are inevitable compare to the no jamming attack scenario.

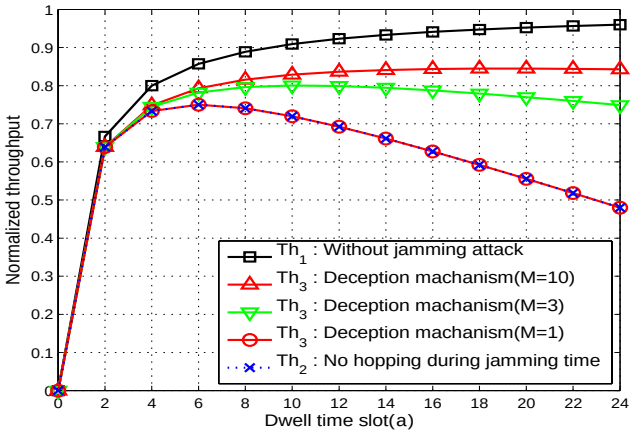


Fig. 7: Normalized throughputsfor different schemes as a function of DT slot

To overcome the limitation of the deception mechanism, we proposed a new anti-jamming technique by detecting jammer's hopping sequences. Figure 8 shows the normalized throughput result of the proposed scheme. After$L \times DT$ periods, the AP finds out the whole hopping sequence of the smart jammer, hence the throughput is significantly increased as depicted in Figure 8. When we run the simulation for 10 times longer than the finding sequence periods ($10 \cdot (L \times DT)$), the average normalized throughput of the proposed anti-jamming technique is as close as to the highest normalized throughput Th_1. As the simulation time increases, the result will be more effective. Therefore, the proposed anti-jamming technique can be considered as the best channel-hopping scheme that can minimize the damage from the smart jamming attack.

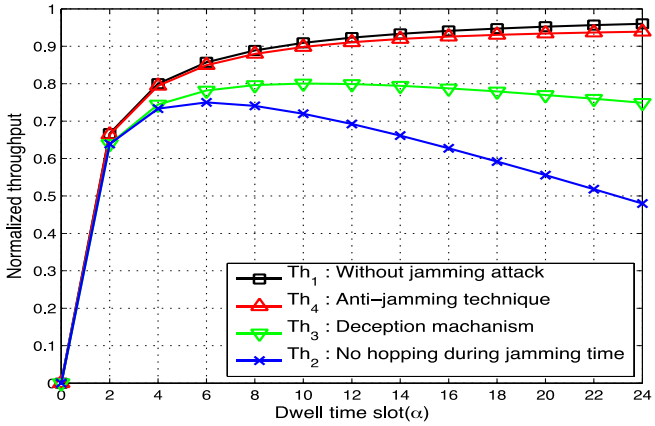


Fig. 8: Normalized throughput of the proposed anti-jamming technique

V. Conclusion

In this paper, weanalyzed the impact of smart jamming attack on a tactical wireless communication environment and emphasized the importance of avoiding the jamming attack. We first examined the drawbacks of the well-known deception mechanism by evaluating the normalized throughput under a smart jamming attack. Then we proposed our anti-jamming technique to protect user nodes from jamming attack. The key aspect of our proposed scheme is to find out the hopping sequence of a smart jammer and use that information to avoid jamming attack. Through numerical analysis, we show that the proposed anti-jamming scheme can detect the hopping sequence of a smart jammer after $L \times DT$ periods. Once the AP finds out the hopping sequence of the jammer, the average normalized throughput of a network was significantly improved.

References

[1] S. Shanken, D. Hughes, and T. Carter, "Secure wireless local area network (SWLAN)," in Proc. IEEE MILCOM, vol. 2, pp. 886-891, Nov. 2004.
[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," Proc. MobiHoc'05, pp. 46–57, Urbana-Champaign, IL, USA, May 2005.
[3] N. Sufyan, N. A. Saqib, and Z. Muhammad, "Detection of jamming attacks in 802.11b wireless networks," EURASIP Journal on Wireless Communications and Networking, vol. 2013, article 208, 2013.
[4] HART Communication. http://www.hartcomm2. org/index.html
[5] V.Navda, A.Bohra, S.Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in Proc. of INFOCOM '07, pp.2526-2530, 2007.
[6] S. Jeong, J. Jeung, and J. Lim, "Measurement-based channel hopping scheme against jamming attacks in IEEE 802.11 wireless networks," J. KICS, vol. 37, no. 4, pp. 205-213, Apr. 2012.
[7] E. Lee, S. Oh, and M.Gerla. "Randomized channel hopping scheme for anti-jamming communication." Wireless Days (WD), 2010 IFIP. IEEE, 2010.
[8] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan,"Understanding and mitigating the impact of RF interference on 802.11 networks," in Proc. IEEE SIGCOMM, vol. 37, pp. 385-396, 2007.
[9] M. S. Gast, "802.11 wireless networks: the definitive guide," O'Reilly publisher, 2002.
[10] S. Khattab, D. Mosse, and R. Melhem, "Jamming mitigation in multi-radio wireless networks: reactive or proactive?," in Proc. of the 4th international Conference on Security and Privacy in Communication Networks (SecureComm), pp.1-10, 2008.
[11] J. Jeung, S. Jeong, and J. Lim, "Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN," in Proc. IEEE MILCOM, pp. 1231-1236, 2011.
[12] C.Delattreand Y. Kim. "A study on How to Find a Hopping Sequence of a Smart Jammerin IEEE 802.11 WLANs," KICS 2014 Fall Conference, Nov. 2014.