The Effect of Increasing the Number of Transceivers in an Anti-jamming Channel-Hopping Scheme

Yongchul Kim[1] and Mihail L. Sichitiu[2]
[1] Korea Military Academy, Seoul, South Korea
[2] North Carolina State University, Raleigh, USA
Email: kyc6454@gmail.com; mlsichit@ncsu.edu

Abstract —In this paper, we analyze a channel-hopping scheme under a smart jamming attack in wireless military communication systems. In particular, we focus on the effect of using multiple transceivers in channel-hopping schemes and compare them with the case of a single transceiver. To evaluate the performance of the multiple transceiver system, we present an analytical model that can calculate the average jammed time when a channel is detected by a smart jammer; consequently network throughput can also be computed. The numerical results show that the multiple transceiver system achieves a significantly higher throughput than the single transceiver system. It is also shown that the effect of increasing the number of transceivers in anti-jamming channel-hopping scheme improves network throughput.

Index Terms—MIMO, channel-hopping scheme, military communications, smart jamming, etc

I. Introduction

As the demand for smart phones and portable devices increases, providing secure wireless communication services becomes crucial. In military environments, wireless technology plays an important role in managing real time data communications between the sensors, weapons and the command control center. A large number of wireless technologies are employed to provide security and reliability for military communications systems. For example, the U.S. Army developed a Secure Wireless Local Area Network (SWLAN) [1] based on IEEE 802.11 standard for their military communications. SWLAN provides enhanced service quality and extended coverage for user devices by using state of the art technologies such as a robust synchronization scheme, antenna diversity, and adaptive forward error correction (FEC). SWLAN is considered to be one of the key subsystems of the command, control, communications, computer, and intelligence (C4I) system. However, jamming attacks from adversaries cannot be fully avoided due to the characteristics of wireless systems: smart jammers scan all of the channels to be able to detect the one that is currently used for data transmissions. A smart jammer attacks ongoing data communications by sending back-to-back semi-valid packets when the channel currently in use is successfully detected. There are many other different types of jammers in the literature [2], [3]. In the context of mitigating damage from jamming attacks, much of the work to date has focused on channel-hopping schemes. Channel hopping is a technique that periodically changes the operating frequency of the communication channel and has been embraced by many technologies and standards such as Bluetooth, WLAN, and WirelessHART [4]. The authors in [5] introduce a channel-hopping scheme to increase 802.11 resilience to jamming attacks, and the work in [6] proposes a measurement based channel-hopping scheme that can choose the best channel to hop instead of hopping to a predetermined channel. In order to bypass the need for pre-key establishment, Lee *et al*. [7] present a randomized channel-hopping scheme.

In general, channel-hopping schemes can be divided into two categories: proactive channel-hopping schemes [8] and reactive channel-hopping schemes [9]. In a proactive channel-hopping scheme, every node in a network has to hop to a new channel periodically regardless of the existence of a jamming attack or channel status. This is useful for the situation where frequent jamming attacks exist, but it will degrade channel efficiency when there is no jamming attack. In contrast, a reactive channel-hopping scheme employs hopping only when a jamming attack is detected or the channel status is significantly degraded. This is beneficial for channel efficiency but the vulnerability to jamming attacks increases since the system uses a channel for an extended period. In this paper we consider a proactive channel-hopping scheme under a smart jamming attack scenario. Jeung *et al.* [10] suggest a deception mechanism in which only one node deceives a smart jammer in a current channel while the rest of nodes hop to a next channel to avoid jamming. The sacrificial node in the deception mechanism has a serious throughput degradation compared to the rest of the nodes. In order to overcome this fairness problem in the deception mechanism, another mechanism that can enhance fairness at the expense of a small throughput degradation was proposed in [11]. This scheme allows every node to hop to the next channel without the deception process. Most of the channel-hopping schemes assume systems with a transceiver where every node uses only one transceiver (radio) for both transmitting and receiving. Channel-hopping schemes with multiple transceivers have not yet

Manuscript received January 12, 2017; revised May 26, 2017.
doi:10.12720/jcm.12.5.279-284

been extensively considered in the literature. In this paper we are addressing the impact of multiple transceivers on the performance of a channel-hopping scheme under a smart jamming attack scenario. We first focus on a double transceiver system to analyze the throughput in comparison with single transceiver based channel-hopping schemes. We then explore the generalization to multiple transceivers and examine the resulting increase in efficiency.

The rest of this paper is organized as follows. In the next section, we present channel-hopping models of user nodes for both single and double transceiver systems and the smart jammer model. In Section III, we present an analytical model for a normalized network throughput under a smart jamming attack. Numerical results and analysis for both single and multiple transceiver systems are shown in Section IV. Section V concludes this paper.

II. Channel Hopping Schemes

In this paper, we consider a proactive channel-hopping scenario under a smart jamming attack, i.e., every node must hop periodically regardless of the existence of a jammer.

A. System Model for a Single Transceiver System

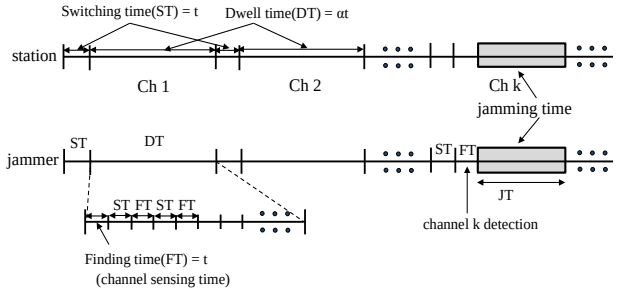


Fig. 1. Channel hopping model of user nodes (above) and channel finding model of smart jammer (below) for a single transceiver system.

We denote with DT (dwell time) the time duration for the actual data transmission at every hop, while the time duration for switching the channels is denoted by ST (switching time). The ST is assumed to be a constant value, while the DT varies according to the jamming situation, hence affecting the network throughput performance. If there is no jamming attack in a network, the longer the DT period, the higher the network throughput. However if there is a jammer in a system, the throughput degradation will be significant as a result of using a long DT period. Fig. 1 shows the channel-hopping model of user nodes and channel finding model of smart jammer for a single transceiver system. The time duration that the smart jammer is sensing a channel is denoted by FT (finding time). If a smart jammer fails to find a channel during the first FT period, it has to change a channel and try to sense again in the second FT period, thus ST is spent between consecutive FTs. We assume that the scanning sequence of a smart jammer is random and all channels are randomly distributed. After successfully detecting an occupied channel, the smart jammer starts jamming until the end of the DT period. We denote with JT (jamming time) the time duration of the jamming interval. Since we assume that the smart jammer has a single transceiver, only one channel can be detected and jammed at a time. In a single transceiver system, none of the user nodes can transmit data when a smart jammer jams the current channel as depicted in Fig. 1.

B. System Model for a Two Transceiver System

If the user nodes have two transceivers, two parallel data communications are made possible by using two different channels simultaneously. Fig. 2 shows the channel hopping model of user nodes and channel finding model of a smart jammer for a two transceiver system. In every DT period two channels are used, thus the achievable network throughput is doubled by comparison with a single transceiver system. However we assume that the smart jammer model is the same as with a single transceiver system in order to compare the effect of increasing the number of transceivers against an equivalent jamming attack. During a DT period, only one channel can be detected and jammed by the smart jammer, i.e., at least one channel is always available for data transmission under the jamming attack as depicted in Fig. 2. From the smart jammer's point of view, it is more likely to find a channel during a DT period because two different channels are simultaneously active.

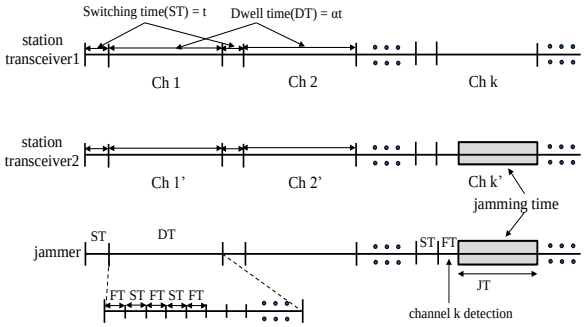


Fig. 2. Channel hopping model of user nodes and channel finding model of smart jammer for a two transceiver system.

III. Analytical Model

A. Single Transceiver System

With a proactive channel-hopping scheme, every node will hop to the next channel periodically even if there is no jamming attack. The duration of the dwell time DT is an important factor for implementing an efficient channel-hopping system. We analyze the performance of the channel-hopping schemes for both single and multiple transceiver systems. We use normalized throughput as a performance evaluation factor for both systems. We denote with Th_M^{NJ} and Th_M^{J} the normalized network throughput without and with jamming when M transceivers are used respectively. From Fig. 1, if the channel is fully utilized without any jamming attack, the

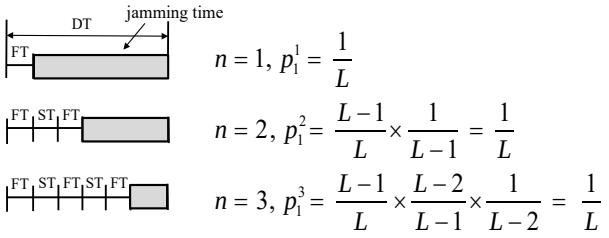
normalized throughput in a single transceiver system is expressed as:

$$Th_1^{NJ} = \frac{DT}{ST + DT} \tag{1}$$

except for the ST periods for channel switching, all of the DT periods are used for data transmission. When the DT period decreases, the normalized throughput is also reduced. When there is a smart jammer, on the other hand, the probability of detecting the channel in use by a jammer increases as the DT period grows. A smart jammer needs one FT and one ST for scanning each channel, thus the total number of trials (N) that a jammer can attempt to scan during the user dwell time is:

$$N = \left\lfloor \frac{DT}{FT + ST} \right\rfloor \tag{2}$$

where $\lfloor\ \rfloor$ is the floor function. When there are L channels in the system, we assume that N should be less than or equal to L ($N \le L$) since a smart jammer can scan all channels when N is equal to L. The probability that a smart jammer can detect the channel in the n^{th} (n=1, 2,…, N) trial during one DT period in a single transceiver system is $p_1^n = 1/L$. Fig. 3 shows the derivation of the channel detecting probability for a single transceiver system.



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

$$n = 2,\ p_1^2 = \frac{L-1}{L} \times \frac{1}{L-1} = \frac{1}{L}$$

$$n = 3,\ p_1^3 = \frac{L-1}{L} \times \frac{L-2}{L-1} \times \frac{1}{L-2} = \frac{1}{L}$$

Fig. 3. Channel detecting probability of a smart jammer in a single transceiver system.

By using the channel detecting probability of a jammer, the expected jamming time during a DT period in a single transceiver system is:

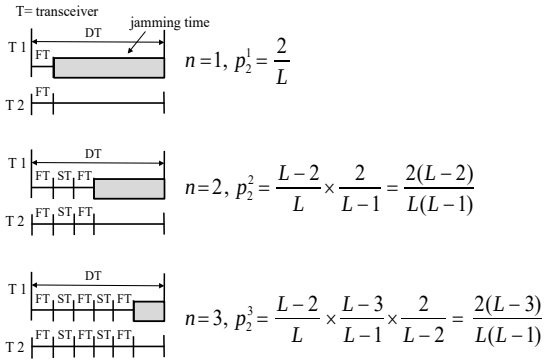
$$E_1(t) = \sum_{n=1}^{N} (DT - nFT - (n-1)ST) \times p_1^n \tag{3}$$

Under a smart jamming attack, the normalized throughput of a single transceiver system can be expressed as:

$$Th_1^J = \frac{DT - E_1(t)}{ST + DT} \tag{4}$$

B. Two Transceiver System

Unlike the single transceiver system, a double transceiver system allows user nodes to transmit data by using two different channels simultaneously.



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

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

$$n = 3,\ p_2^3 = \frac{L-2}{L} \times \frac{L-3}{L-1} \times \frac{2}{L-2} = \frac{2(L-3)}{L(L-1)}$$

Fig. 4. Channel detecting probability of a smart jammer in a double transceiver system.

When there are two channels used for data transmissions in a DT period, only one of them can be jammed by a smart jammer, hence the damage from the jamming attack will be reduced but the channel detecting probability of a jammer will be increased. Fig. 4 shows the channel detecting probability of a smart jammer in a double transceiver system. Thus, the probability that a smart jammer can detect the channel in n^{th} (n=1, 2,…, N) trial during DT period is:

$$p_2^n = \frac{2(L-n)}{L(L-1)} \tag{5}$$

Using (5), the average jamming time during a DT period for the double transceiver system can be computed by (3) by replacing p_1^n with p_2^n; consequently, the normalized throughput of a double transceiver system can be expressed as:

$$Th_2^J = \frac{2DT - E_2(t)}{2(ST + DT)} \tag{6}$$

C. Multiple Transceiver System

In order to examine the impact of increasing the number of transceivers on the normalized network throughput, we explore an extension of the channel-hopping scheme to a general multiple transceiver based system. Let p_M^n be the channel detecting probability of a smart jammer in n^{th} (n=1, 2,…,N) trial during DT period when M transceivers are used for multiple data transmissions. Fig. 5 shows p_3^n in a three transceiver system case. In a similar way to the p_2^n and p_3^n described in Fig. 4 and Fig. 5, the generalized channel detecting probability of a smart jammer p_M^n can be expressed as:

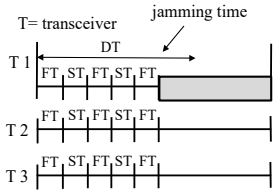
$$p_M^n = \frac{M(L-n)(L-(n+1))\cdots(L-(n+M-2))}{L(L-1)(L-2)\cdots(L-(M-1))} \tag{7}$$

If we denote with $E_M(t)$ the average jamming time for the M transceiver based system, $E_M(t)$ can be expressed as:

$$E_M(t)=\sum_{n=1}^{N}(DT-nFT-(n-1)ST)\times p_M^n \quad (8)$$

Consequently the generalized equation of Th_M^J can be written as:

$$Th_M^J=\frac{M\cdot DT-E_M(t)}{M\cdot(ST+DT)} \quad (9)$$



$$n=1,\ p_3^1=\frac{3}{L}$$

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

$$n=3,\ p_3^3=\frac{L-3}{L}\times\frac{L-4}{L-1}\times\frac{3}{L-2}=\frac{3(L-3)(L-4)}{L(L-1)(L-2)}$$

$$n=4,\ p_3^4=\frac{L-3}{L}\times\frac{L-4}{L-1}\times\frac{L-5}{L-2}\times\frac{3}{L-3}=\frac{3(L-4)(L-5)}{L(L-1)(L-2)}$$

Fig. 5. Channel detecting probability of a smart jammer in a three transceiver system.

IV. Numerical Results

In this section, we analyze the performance of channel-hopping schemes by using the analytical models presented in the previous section. We first examine the achievable normalized network throughput by varying the DT period for different transceiver systems to compare the performances. We then explore the ratio of the average jamming time to a single DT period for different transceiver systems to analyze the impact of increasing transceivers on performance enhancement. We assume that FT and ST durations are t seconds (t=5ms) and DT duration is αt (we call α the DT slot). When the number of available channels in a network is 20, the maximum value of the DT slot is 40 to allow a smart jammer to scan 20 channels in a DT period ($20(FT+ST)=40t$). Fig. 6 shows the normalized network throughput as a function of the DT slot for different transceiver systems. When there is no jamming attack, the normalized throughput increases and approaches 1 as the DT slot increases. However with a smart jammer, the normalized throughput of a single transceiver system, Th_1^J decreases when the DT slot α>8. Because it is very likely that a jammer can detect a channel when DT period is long, the damage from a smart jammer grows as the DT slot increases. For a double transceiver system, the normalized throughput, Th_2^J, achieves better performance compared to the single transceiver system, with more than 30% higher normalized throughput achieved when the DT slot is α=40. The three and four transceiver systems also show that the Th_3^J and Th_4^J achieve better performance in comparison with the single transceiver system, but the enhancement is not as significant as for the double transceiver system. The Th_3^J and Th_4^J achieved 49% and 59% higher normalized throughput compared to Th_1^J when the DT slot is α=40.

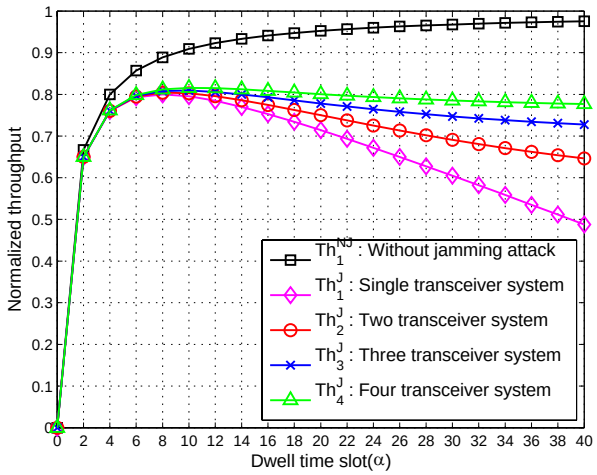


Fig. 6. Normalized throughput as a function of DT slot for systems with a different number of transceivers.

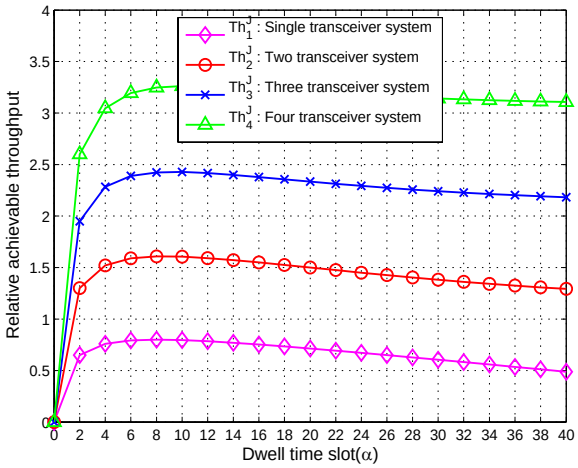


Fig. 7. Relative achievable throughput as a function of DT slot.

Although it is clear that the normalized throughput of multiple transceiver system continues to grow as the number of transceivers increases, we do not show them on the graph since implementing more than four transceivers is not realistic and would clutter the graph.

In order to examine the relative throughput enhancement in multiple transceiver channel-hopping schemes, we compare the achievable network throughputs of multiple transceiver systems with that of single transceiver system. Fig. 7 shows the relative achievable data throughput for different transceiver systems as a function of the DT slot α. When there is no jamming attack, the relative achievable data throughput converges to 1 for the single transceiver system and 2 for the double transceiver system, etc. However the actual throughput degrades due to the jamming attacks and the

degradation for the system with a high number of transceivers is the most significant. As stated in the previous section, the average jamming time $E_M(t)$ varies according to the channel detecting probability p_M^n, thus the higher the number of transceivers in a channel-hopping scheme, the longer the average jamming time.

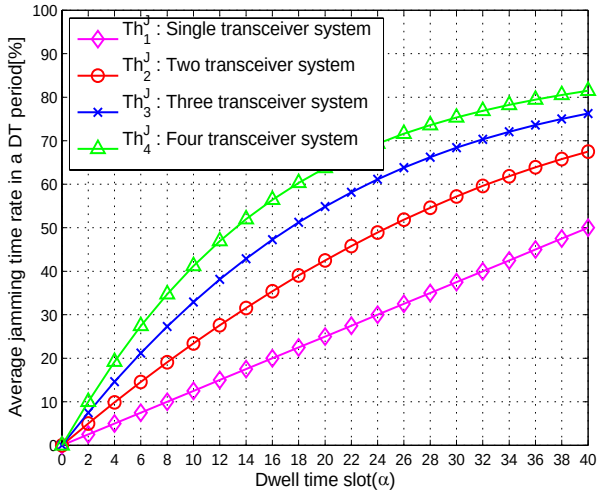


Fig. 8. Average jamming rates as a function of DT slot for different transceiver systems.

Fig. 8 shows average jamming rates within a DT period as a function of DT slot for different transceiver systems. In a single transceiver based channel-hopping scheme, the average jamming rate is linearly increasing as the DT slot increases because the channel detecting probability p_1^n is always $1/L$ in each scan period. The system with multiple transceivers shows a different characteristic. The average jamming time rates increase rapidly at first and then slowdown at high values of α; this trend occurs because the channel detecting probability is always highest value at the first scan and then diminishes as the number of trials increase. This phenomenon is more significant for the four transceiver based channel-hopping scheme as depicted in Fig. 8.

V. Conclusion

In this paper, we studied the channel-hopping scheme under a smart jamming attack in a wireless military communication environment. We focused on the effect of increasing the number of transceivers in channel-hopping scheme against jamming attacks. To compare the performance of multiple transceiver systems, we presented an analytical model and calculated the average jamming time and achievable network throughput for different transceiver systems. Our numerical results showed that the normalized network throughput increased more than 30% for the double transceiver based channel-hopping scheme in comparison with the single transceiver based system for large dwell times. However the throughput enhancement dwindled as the number of transceivers increased under a smart jamming attack.

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," in *Proc. MobiHoc'05*, Urbana-Champaign, IL, USA, May 2005, pp. 46-57.

[3] N. Sufyan, N. A. Saqib, and Z. Muhammad, "Detection of jamming attacks in 802.11b wireless networks," *EURASIP J. Wireless Commun. and Netw.*, vol. 2013, no. 208, 2013.

[4] HART Communication. [Online]. Available: 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. INFOCOM '07*, Anchorage, AK, May 2007, pp. 2526-2530.

[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. K. Lee, S. Y. Oh, and M. Gerla, "Randomized channel hopping scheme for anti-jamming communication," in *Proc. IEEE 2010 IFIP, Wireless Days (WD)*, Venice, Italy, Oct. 2010, pp. 1-5.

[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, Aug. 2007.

[9] M. S. Gast, *802.11 Wireless Networks: The Definitive Guide*, O'Reilly Publisher, 2002.

[10] J. Jeung, S. Jeong, and J. Lim, "Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN," in *Proc. IEEE MILCOM*, Baltimore, MD, Nov. 2011, pp. 1231-1236.

[11] Y. Kim, "Throughput and fairness analysis of channel-hopping scheme under smart jammer attacks in IEEE 802.11 WLANs," in *Proc. KICS Summer Conference'14*, South Korea, Jun. 2014, pp. 247-248.

Yongchul Kim received a B.E. from Korea Military Academy in 1998 and an M.S. from the University of Surrey (Surrey, UK) in 2001. He received a Ph.D. degree in Electrical and Computer Engineering from the North Carolina State University (Raleigh, USA). He is currently employed as an associate professor in the Department of Electrical Engineering at Korea Military Academy.

Mihail L. Sichitiu received a B.E. and an M.S. in Electrical Engineering from the Polytechnic University of Bucharest in 1995 and 1996 respectively. In May 2001, he received a Ph.D. degree in Electrical Engineering from the University of Notre Dame. He is currently employed as a professor in the Department of Electrical and Computer Engineering at North Carolina State University.