Throughput and Fairness Analysis of Channel-hopping Scheme under Smart Jammer Attacks in IEEE 802.11 WLANs

Yongchul Kim

Korea Military Academy

kye6454@kma.ac.kr

Abstract

Jamming attack in wireless networks is a severe problem and is easily accomplished by emitting a continuous radio signal. Although the perfect solution to avoid jamming attack does not exist due to the nature of the wireless shared medium, a channel-hopping scheme is considered one of the most effective ways to mitigate jamming attacks. In this paper, I consider various channel-hopping schemes under smart jammer attacks and study the issue of throughput and fairness in such networks. I provide an analytical model that can be used to evaluate the performance of channel-hopping schemes by calculating normalized network throughput. I also propose a simple channel-hopping scheme that preserves fairness among active stations under a jamming attack. The numerical results show that the proposed channel-hopping scheme enhances fairness significantly at minimal throughput degradation expense.

I. Introduction

IEEE 802.11 WLAN is the most widely used standard as portable computing and smart phone devices are becoming increasingly popular. WLAN technologies are also used for military applications, especially for Tactical Operations Centers (TOC). The U.S. Army uses secure wireless local area network (SWLAN) [1] with IEEE 802.11 standard waveforms for their TOC communications. Although the SWLAN provides secure mobile communications by integrating cryptographic techniques, the jamming attack from an adversary cannot be fully avoided since the jammer can be very smart and transmits back-to-back packets on the detected channel after randomly scanning all of the channels. In this paper, I consider various channel-hopping schemes under smart jammer attacks and study the issue of throughput and fairness in such networks.

II. Channel-hopping Schemes

In the literature, there has been a significant amount of work directed toward alleviating the effects of jamming by proposing channel-hopping methods. Navda et al. [2] present a channel-hopping scheme in order to increase 802.11 resilience in the face of jamming attacks. Traditionally, channel-hopping strategies can be divided into two categories, proactive rapid channel-hopping and reactive slow channel-hopping [3]. Since I consider a smart jammer model in this work, the reactive slow channel-hopping method is not effective because the smart jammer can easily detect and jam the hopped channel again. Therefore, I focus on a proactive rapid channel-hopping scheme in this paper. As shown in Fig. 1, every station must hop to the next channel after a dwell time (DT) period regardless of channel status. That is, a station transmits frames during a dwell time and hops to the predetermined channel during a switching time (ST). A DT period can vary according to the jamming intensity and has an impact on network throughput as will be shown in the next section. A smart jammer recognizes both ST and DT periods but does not recognize the channel-hopping sequence, hence, it quickly scans all of the channels by its own random sequence during every DT period. The jammer takes one finding time (FT) and ST to verify one channel as shown in the jammer model below. Let ST and FT be the same t to simplify our model. When the jammer detects a channel k, it jams the channel during jamming time (kt). After jamming time, it checks whether the channel is still being used. If the channel is still active it continues to jam, otherwise it switches to another channel and starts sensing again.

![Fig. 1 Station and jammer models](image)

The deception mechanism proposed in [3] takes advantage of the characteristics of a smart jammer. When a channel is detected by a jammer, every station, except one, must hop to the next channel immediately but the jammed station has to stay and deceive the jammer as if the channel is being used. This mechanism can be very effective when there are many stations in a network in terms of network throughput. However, the damage to the sacrificed station is severe and leads to a serious unfairness problem.
I propose a simple channel-hopping scheme that enhances fairness performance by allowing the sacrificed station to hop to the next channel immediately after a jamming time. The numerical analysis validates the proposed scheme in the next section.

### III. Numerical Analysis

In this section I analyze the network throughput and fairness performance by varying some parameters such as dwell time, jamming time, and the number of stations. If there is no jamming attack, the normalized throughput can be expressed as

$$Th_0 = DT / (ST + DT).$$

When a smart jammer is active, it scans $N$ channels during $DT$ period (i.e., $N = DT / (FT + ST)$). Let $L$ be the total number of channels and $p_n$ be the probability that the jammer can detect the channel after sensing an $n_{th}$ channel (i.e., $p_n = 1/L$). The average jammed time during $DT$ can be expressed as:

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

Therefore, the normalized throughput under the smart jammer without allowing any client station to hop during the jamming time can be obtained as:

$$Th_j = DT - E(t) \over ST + DT. \tag{2}$$

To compute the normalized throughput of the deception mechanism [3], let $\eta T$ be a summation of jamming detection, announcement, and switching time. Let also $\sigma_n$ and $k_n$ denote the time duration of jammed station and un-jammed station can actually use within a $DT$ period respectively. Then, the actual normalized throughput of the deception method is expressed as:

$$Th_3 = \frac{1}{M} \left( \sum_{n=1}^{N} \sigma_n p_n + DT(L-N)/L, \sum_{n=1}^{N} k_n p_n + DT(L-N)/L \right) / (ST + DT). \tag{3}$$

In an extreme case, where there is only one station in a network, this mechanism is useless. And the unfairness problem will be severe under this method. To alleviate the fairness problem, I allow a jammed station to hop to the next channel after $\beta T$. That is, there is no deceiving station, hence, a smart jammer can also start sensing directly after $\beta T$. The normalized throughput of the jammed station is obtained as:

$$Th_3 = \frac{DT}{ST + DT} \over L - N \over L + \left( \sum_{n=1}^{N} \sigma_n p_n + DT(L-N)/L, \sum_{n=1}^{N} k_n p_n + DT(L-N)/L \right) / (ST + DT). \tag{4}$$

Therefore, the normalized throughput of the proposed scheme can be computed by:

$$Th_k = \frac{Th_j + (Th_j + \beta T - \eta T) \times (M-1)}{M}. \tag{5}$$

Fig. 2 shows all performance results for the four different channel-hopping schemes as a function of dwell time slot $(\alpha)$ given $L=12, M=3, t=5ms, \beta T = 2\alpha$, $\beta T = 3\alpha$. The throughput of $Th_k$ is growing as the $DT$ period increases since there is no jamming attack. In contrast, the throughput of $Th_j$ decreases significantly as the dwell time grows, because none of the stations can hop to the other channel during the jamming time. The normalized throughput of our proposed scheme is slightly lower than that of the deception mechanism, however, the fairness performance of the proposed scheme is significantly better than that of the deception mechanism. The throughput difference between maximum and minimum value from the deception mechanism is more than five times greater than that of the proposed scheme as shown in Fig. 3 and 4.

### IV. Conclusion

In this paper I studied the channel-hopping scheme under a smart jammer attack and analyzed the network throughput and fairness performance. An analytical model was provided to calculate the normalized network throughput for different channel-hopping schemes. The numerical results show that the fairness performance of the proposed scheme was significantly enhanced at the expense of minimal throughput degradation.

### References

