

Friendly-Jamming: An Anti-Eavesdropping Scheme in Wireless Networks

Xuran Li and Hong-Ning Dai

Macau University of Science and Technology, Macau SAR

lxrget@163.com; hndai@ieee.org

Abstract—This paper proposes a novel anti-eavesdropping scheme by introducing artificial noise caused by friendly jammers deployed in wireless networks. In particular, we propose an analytical model to quantify the eavesdropping risk of wireless network with friendly jammers. Our approach considers both large-scale path loss and Rayleigh fading. Our numerical results show that the eavesdropping risk of wireless networks can be significantly reduced with the aid of friendly jammers.

Index Terms—Security; Anti-eavesdropping; Wireless Networks

I. INTRODUCTION

Since the data transmission in wireless networks are highly vulnerable to eavesdropping attacks due to the broadcast nature of wireless medium, the security and privacy of wireless communication has arisen an increasing attention. Traditionally, encryption schemes are typically adopted to protect communication systems. However, the encryption protocols are not perfectly secure because they only hide the meaning of the information being transmitted but not the information itself. Moreover, the hardware constraints such as the inferior computational capability and the limited power of wireless users causes the encryption infeasible to some wireless networks [1].

Therefore, the physical layer security as the alternative paradigm received lots of attention. *Protective jamming* is a physical layer technique which can potentially enhance the network security while not leading to modifications on legitimate users in wireless networks [2]–[5]. The main idea of protective jamming is to deploy friendly jammers to emit artificial noise so that eavesdroppers will be interfered from wiretapping the confidential legitimate transmissions. However, most of these schemes can only be applied to specific scenarios. For example, the work of [2] only considers using at most 2 jammers while [3] makes an assumption on Gaussian channel that is not realistic in wireless networks. Besides, the jamming scheme proposed in [4] can only be used in Wireless Local Area Networks (WLANs).

To the best of our knowledge, there is a lack of protective schemes, which can be applied to various scenarios. In this paper, we propose a Friendly-Jamming (Fri-Jam) Anti-Eavesdropping Scheme to mitigate eavesdropping activities in wireless networks. The goal of this paper is to model the performance of Fri-Jam scheme in wireless networks. In particular, we compare the eavesdropping probability of wireless network with friendly jammers with that without

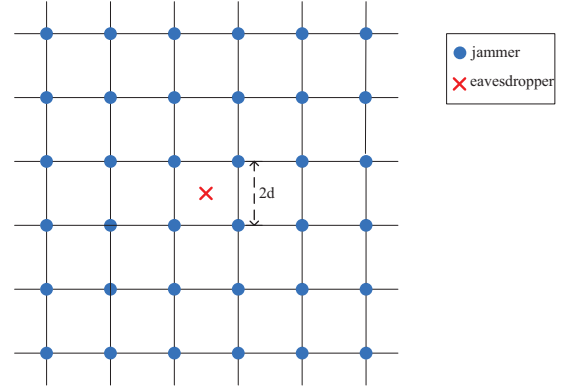


Fig. 1. Fri-Jam Scheme: every jammer is placed at a gray square. Note that we only show a part of the whole network.

friendly jammers. We find that *deploying friendly jammers in the wireless network can reduce the eavesdropping probability significantly*. Our results also show that to deploying the friendly jammers in the wireless network appropriately will reduce the eavesdropping probability while only slightly decreasing the transmission probability.

II. PROBLEM FORMULATION

In this paper, we consider a network placed in a torus [6]. We assume that the legitimate users are distributed in the torus according to homogeneous Poisson point process (PPP). Due to the symmetry of the torus, we place the eavesdropper at the center of the network, which is similar to [7]. We consider the friendly jammers are regularly deployed in a grid manner as shown in Fig. 1.

In order to determine whether the transmission from a certain legitimate user can be snooped by the eavesdropper, we define the *eavesdropping condition* as follows.

Definition 1: Eavesdropping Condition. A confidential transmission will be wiretapped by the eavesdropper if and only if the *Signal to Interference plus Noise Ratio (SINR)* of the eavesdropper is high enough, i.e., $\gamma > T$, where γ denote the SINR and T is the received power threshold that an eavesdropper can decode the transmission successfully.

To derive the SINR γ , we assume the channel is mainly experiencing the Rayleigh fading and large-scale path loss. Then the received power of a receiver (i.e., a legitimate user

or the eavesdropper) at a distance r from a legitimate user (or friendly jammer) is $\xi r^{-\alpha}$, where α is the path loss factor and the Rayleigh fading factor ξ is a random variable which follows the exponential distribution with mean $\frac{1}{\mu}$, which could be denoted as $\xi \sim \exp(\mu)$.

Then we have the SINR γ expressed as

$$\gamma = \frac{\xi r^{-\alpha}}{\eta + I_t + I_j}, \quad (1)$$

where η is the noise power, $I_t = \sum_{i \in \Omega/t_0} \xi_i R_i^{-\alpha}$ denotes the cumulative interference from legitimate users, Ω denotes the set of legitimate users and I_j denotes the cumulative interference generated by friendly jammers.

The definition of the *eavesdropping probability* denoted by $\mathbb{P}(E)$ is then given as follows.

Definition 2: Eavesdropping Probability is the probability that at least one transmission can be eavesdropped

We denote $\mathbb{P}_e$ as the probability that one transmission has been eavesdropped. We next express $\mathbb{P}(E)$ by $\mathbb{P}_e$ as follows,

$$\mathbb{P}(E) = 1 - (1 - \mathbb{P}_e)^N, \quad (2)$$

where N is the expected number of legitimate users in the network.

Another objective of this paper is to investigate the influence of our Fri-Jam scheme on the legitimate transmissions. So, we also investigate the transmission probability denoted by $\mathbb{P}(C)$. As shown in [8], we have $\mathbb{P}(C) \triangleq \mathbb{P}(\gamma > \beta)$, where β is the threshold value of the SINR of the legitimate receiver for a successful reception.

III. MAIN RESULT

The Non-Jam scheme is denoted to be the conventional scheme without friendly jammers in contrast to our proposed Fri-Jam scheme. Then we will state our main result with Non-Jam Scheme and Fri-Jam Scheme separately.

A. Result of Non-Jam Scheme

We need to derive the eavesdropping probability $\mathbb{P}_e$ that one transmission has been wiretapped according to the definition of the eavesdropping probability $\mathbb{P}(E)$. In particular, we get $\mathbb{P}_e$ of wireless networks in Non-Jam scheme as follows.

Theorem 1: In Non-Jam scheme, the eavesdropping probability $\mathbb{P}_e$ is calculated as

$$\mathbb{P}_e = \int_{r>0} e^{-\mu T r^\alpha \eta - \pi r^2 \lambda (\rho(T, \alpha) + 1)} 2\pi \lambda r dr, \quad (3)$$

where $\rho(T, \alpha) = T^{-2/\alpha} \int_{T^{-2/\alpha}}^{\infty} \frac{1}{1 + \mu^\alpha/2} d\mu$.

The proof of Theorem 1 can be found in [5]. Theorem 1 indicates that $\mathbb{P}_e$ is heavily influenced by the channel status (such as the path loss and Rayleigh fading).

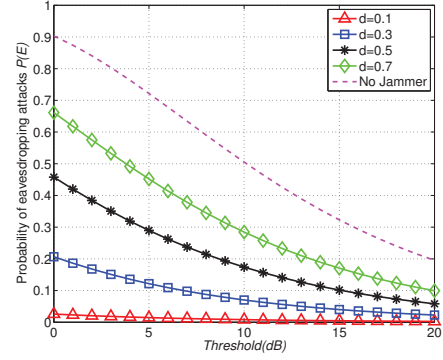


Fig. 2. Probability of eavesdropping attacks $\mathbb{P}(E)$ with Fri-Jam scheme versus Non-Jam scheme when $\alpha = 4$ with SINR threshold T ranging from 0dB to 20dB.

B. Result of Fri-Jam Scheme

We denote $E[I_j]$ by the expectation of the cumulative interference generated by jammers. We then derive the probability $\mathbb{P}_e$, which is shown in the Theorem 2.

Theorem 2: In Fri-Jam scheme, the probability P_e that one transmission has been eavesdropped is

$$\mathbb{P}_e = \int_{r>0} e^{-\mu T r^\alpha (\eta + E_j) - \pi r^2 \lambda (\rho(T, \alpha) + 1)} 2\pi \lambda r dr, \quad (4)$$

where $\rho(T, \alpha) = T^{-2/\alpha} \int_{T^{-2/\alpha}}^{\infty} \frac{1}{1 + \mu^\alpha/2} d\mu$ and $E[I_j]$ is given in the following equation,

$$E[I_j] = \frac{1}{\mu} \sum_{m=1}^n E[I_j(m)], \quad (5)$$

where $I_j(n)$ is calculated as

$$I_j(n) = 4 \left\{ 2 \cdot \sum_{k=1}^n \left(d \cdot \sqrt{(2k-3)^2 + (2k-1)^2} \right)^{-\alpha} + \left(d \cdot \sqrt{2(2k-1)^2} \right)^{-\alpha} \right\}.$$

The proof of Theorem 2 please refer to our previous paper [5]. Theorem 2 indicates that $\mathbb{P}_e$ is heavily influenced by the placement parameter d , the Rayleigh fading factor μ , the path loss factor α and the noise η .

According to the definition of the probability of eavesdropping attack $\mathbb{P}(E)$, we have

$$\mathbb{P}(E) = 1 - (1 - \mathbb{P}_e)^N,$$

where $\mathbb{P}_e$ is given by Theorem 1, Theorem 2 in Non-Jam scheme, Fri-Jam scheme, respectively. In next section, we will show the numerical results of $\mathbb{P}(E)$ based on the two schemes.

IV. NUMERICAL STUDY

We calculate the probability of eavesdropping attacks $\mathbb{P}(E)$ of Non-Jam scheme and that of Fri-Jam scheme. Fig. 2 presents the numerical results. Note that the dash curve represents the results of Non-Jam scheme and the solid curves

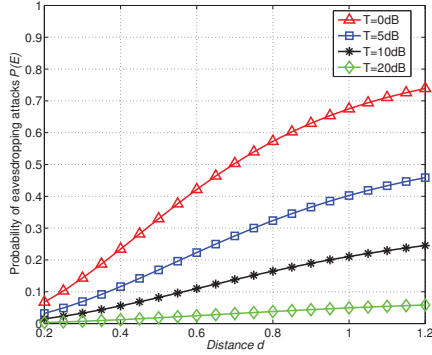


Fig. 3. Probability of eavesdropping attacks $\mathbb{P}(E)$ when $T = 0, 5, 10, 20\text{dB}$ and $\alpha = 3$ with distance d ranging from 0.2 to 1.2.

with markers denote the results of Fri-Jam scheme, where we choose the different values of placement distance d . We find that in contrast to the Non-Jam scheme, deploying friendly jammers will always reduce the eavesdropping probability.

Moreover, it is shown in Fig. 2 that $\mathbb{P}(E)$ is heavily influenced by placement parameter d . Specifically, from Fig. 3 we find that the probability of eavesdropping attack $\mathbb{P}_E$ increases with the increased values of d , implying that *the performance of mitigating eavesdropping attacks can be further improved by deploying more jammers* while too many jammers can also mitigate the legitimate communications (so there is a trade-off in deploying jammers). Taking Fig. 2 as an example again, when $\alpha = 4$ and the threshold $T = 5\text{dB}$, $\mathbb{P}(E)$ of Non-Jam scheme is 0.719 while $\mathbb{P}_E$ of Fri-Jam scheme is reduced to 0.117 with placement distance $d = 0.3$.

Another objective is to investigate whether friendly jammers will have significant impact on the legitimate communications. We define the *eavesdropping deviation* $\mathbb{D}_E$ and the *transmission deviation* $\mathbb{D}_C$ to distinguish the influence of Fri-Jam scheme and Non-Jam scheme in terms of the eavesdropping probability and the transmission probability separately, which is shown as follows.

The eavesdropping deviation $\mathbb{D}_E$ is the difference between the eavesdropping probability $\mathbb{P}(E)$ without jammers and the eavesdropping probability $\mathbb{P}(E)$ with jammers. The transmission deviation $\mathbb{D}_C$ is the difference between the transmission probability $\mathbb{P}(C)$ without jammers and the transmission probability $\mathbb{P}(C)$ with jammers. In particular, we have $\mathbb{D}_E = \mathbb{P}_{\text{Non-Jam}}(E) - \mathbb{P}_{\text{Fri-Jam}}(E)$, where $\mathbb{P}_{\text{Non-Jam}}(E)$ denotes the eavesdropping probability of Non-Jam scheme and $\mathbb{P}_{\text{Fri-Jam}}(E)$ denotes the eavesdropping probability of Fri-Jam scheme. Besides, we have $\mathbb{D}_C = \mathbb{P}_{\text{Non-Jam}}(C) - \mathbb{P}_{\text{Fri-Jam}}(C)$, where $\mathbb{P}_{\text{Non-Jam}}(C)$ denotes the transmission probability of Non-Jam scheme and $\mathbb{P}_{\text{Fri-Jam}}(C)$ denotes the transmission probability of Fri-Jam-Ran scheme.

It is shown in Fig. 4 that Fri-Jam scheme can significantly reduce the eavesdropping probability with slight influence on the legitimate communication. For example, when $d = 0.1$, eavesdropping deviation $\mathbb{D}_E = 0.497$ while the reduction of the transmission probability $\mathbb{D}_C = 0.075$; the eavesdropping

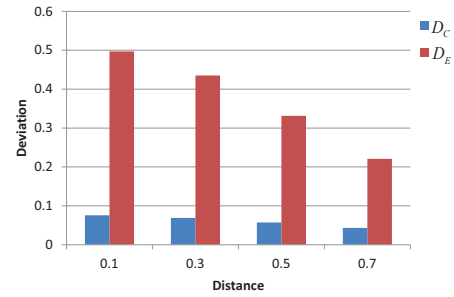


Fig. 4. Eavesdropping deviation and transmission deviation of comparing Fri-Jam scheme with Non-Jam scheme when $d = 0.1, 0.3, 0.5, 0.7$ and $T = 10\text{dB}$, $\alpha = 4$.

deviation $\mathbb{D}_E = 0.331$ and transmission deviation $\mathbb{D}_C = 0.057$ when $d = 0.5$.

V. CONCLUSION

In this paper, we introduce multiple friendly jammers in the wireless networks to mitigate the eavesdropping attacks. We find the eavesdropping risk is obviously reduced with the aid of friendly jammers. This novel anti-eavesdropping scheme requires no modification on existing wireless users and can be used in various scenarios.

One of the future directions is to improve our Fri-Jam scheme to further reducing the eavesdropping probability while maintaining the lowest impact on the legitimate transmissions, which can be achieved by integrating with other security schemes.

ACKNOWLEDGEMENT

The work described in this paper was supported by Macao Science and Technology Development Fund under Grant No. 096/2013/A3. The authors would like to thank anonymous reviewers for their constructive comments. The authors would like to express their appreciation for Gordon K.-T. Hon for his thoughtful discussions.

REFERENCES

- [1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.
- [2] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, 2011.
- [3] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polshchuk, S. Ramasubramanian, and M. Segal, "Optimization schemes for protective jamming," in *Proceedings of ACM MOBIHOC*, 2012.
- [4] Y. S. Kim, P. Tague, H. Lee, and H. Kim, "A jamming approach to enhance enterprise wi-fi secrecy through spatial access control," *Wirel. Netw.*, pp. 2631–2647, Nov. 2015.
- [5] X. Li, H.-N. Dai, and H. Wang, "Friendly-Jamming: An Anti-Eavesdropping Scheme in Wireless Nets of Things," in *IEEE Global Communications Conference (GlobeCom)*, Washington D.C., USA, 2016.
- [6] A. E. Gamal, J. Mammen, B. Prabhakar, and D. Shah, "Optimal throughput-delay scaling in wireless networks-part I: The fluid model," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2568–2592, 2006.
- [7] J.-C. Kao and R. Marculescu, "Minimizing Eavesdropping Risk by Transmission Power Control in Multihop Wireless Networks," *IEEE Transactions on Computers*, vol. 56, pp. 1009 – 1023, 2007.
- [8] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on Communications*, pp. 3122 – 3134, Nov. 2011.