INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
O. Yaman et al., Vol.12, No.1, pp.13-20.
https://doi.org/10.55859/ijiss.1194643

A Lightweight Self-Organized Friendly Jamming

Okan YAMAN[1] , Tolga AYAV [1], Yusuf Murat ERTEN [2]

[1]Dept. of Computer Engineering, Izmir Institute of Technology, Izmir, TURKEY
[2]Dept. of Computer Engineering, Izmir University of Economics, Izmir, TURKEY
Corresponding Author: okanyaman@iyte.edu.tr

Research Paper Received: 26.10.2022 Revised: 24.12.2022 Accepted: 25.01.2023

Abstract—Wireless networks are inherently more susceptible to attacks than their wired counterparts. Our personal information transmitted over a wide range of networks, from wireless local area networks (WLAN) to wireless wide area networks (WWAN), can easily be accessed and used by third parties. The simplicity of transmitting and receiving messages for legitimate users also makes it possible for intruders to access these networks easily. Hence traditionally, cryptographic methods have been exploited to provide security and privacy against this. However, these approaches still need to fulfill the needs of current technologies, such as IoT devices with limited computation and energy sources, and friendly jamming (FJ) emerges as a promising solution to this problem due to being a computationally cheap and energy-efficient operation. Many studies have tried to cope with one of the challenges of FJ, its viability, but they are complicated and focus on old technologies. Many technologies, including 5G, IoT, Mobile Ad-hoc Networks (MANETs), and Wireless Sensor Networks (WSNs), also utilize the FJ mechanism. However, they face some restrictions, such as fulfilling real-world effects, blocking illegitimate transmission to a maximum extent, affecting legitimate transmission to a minimum extent, and consuming energy efficiently. This study proposes a more lightweight and flexible FJ scheme to address these tradeoffs. We also demonstrate that our model has the same performance parameters as other studies in this area but offers a solution more straightforwardly.

Keywords—Jamming, friendly jamming, security, privacy, mobility, wireless networks, cellular networks

1. Introduction

Using an open and shared medium is both a blessing and a curse for wireless networks. They constitute a large-scale communication infrastructure from home-based internet to satellites that can be considered an advantage. However, this limitless growth of gathering, processing, and transmitting personal private data brings severe security and privacy concerns. Moreover, this open and shared nature of wireless networks render them more susceptible to attacks than their wired alternatives.

Conventionally, the security of wireless networks is based on cryptographic techniques. However, these consume significant computational power and energy. Thus, current resource-constraint technologies require more efficient solutions. In this regard, friendly jamming is considered by researchers to be a promising defense mechanism, although it can be considered a threat from the attacker's perspective. The main idea of jamming is communication disruption by decreasing signal to noise ratio (SNR) due to the introduction of external noise. This attack can also be exploited for defensive purposes if it disrupts illegitimate communication, such as eavesdroppers.

Due to its efficiency in terms of computation and energy, various emerging technologies, such

as 5G [1], [2], Industrial IoT (Internet of Things) [3], IoT [4], Visible Light Communication (VLC) [5], [6], and Wireless Sensor Networks (WSNs) [7] exploit the friendly jamming approach. However, the mentioned models above have to tackle the following challenges

- Compliance with real-world conditions, such as Rayleigh fading and shadowing
- Maximum performance (disrupting illegitimate communication as much as possible)
- Minimum side-effect (disrupting legitimate communication as little as possible)
- Energy efficiency

Although some studies try to meet real-world requirements [8], [9], they are complicated models and need to be updated for new technologies. Therefore, our primary motivation and the contribution in this study is to propose a mechanism that is well-posed to meet real-world needs with the following features

- simplicity
- flexibility

In this study, we are dealing with generating jamming signals based on the received signal power. It is claimed that not only energy efficient but also more realistic solution to the generation of optimum jamming power problem can be provided by utilizing the received signal (see Section 3). If other parameters are kept constant, wireless signals attenuate proportional to the path loss exponent specific to each medium. Although finding the free space path loss is straightforward, determining a more realistic solution needs a comprehensive effort. Our motivation behind using the received power is the properties inherent in its nature exposed to real-world effects.

In order to exemplify our model, a cellular network scenario is selected where all nodes have the same transmission power. If we are asked to block all the communication inside the desired range, we need to generate a signal whose power matches the signal received from the furthest node in the region. Blocking all the communication can be performed by adding transmit power to the power lost due to that distance according to the classical lost-power centric models. Nevertheless, those models have two drawbacks: (i) determining the exact loss is not possible since all the real-world effects cannot be calculated precisely; (ii) that calculation is cumbersome, as can be seen in [10] and also in the following sections. However, we can measure them exactly where the core of our model lies. In our model, the lost power is substituted with the difference between the transmitted power and the received power, giving rise to the same results. We eliminated the first issue above by measuring the exact real-life data that is the received signal. Furthermore, we do not need to calculate anything since we can measure it. Therefore, the abovementioned issues are eliminated by our model.

The remainder of the paper is organized as follows: other models in the literature are reviewed in Section 2, the proposed model is stated and proven in Section 3, and in Section 4, the evaluation part which is comprised of model validation via simulations is discussed, and the paper is concluded in Section 5.

2. Related Work

The authors of [11] propose a friendly jammer scheme to increase the secrecy sum rate for the Non-Orthogonal Multiple Access (NOMA). There are novel secrecy capacity (SC) schemes and assessments of the FJ efficiency in [12]. Authors have an optimal power allocation approach exploiting FJ for PLS by increasing the secrecy outage probability (SOP) [13].

The effect of cooperative and FJ on the security of wireless networks is investigated in [14]. The authors proposed a full-duplex jammer protocol with a half-duplex version for energy harvesting and security [15]. A novel scheme, ally-friendly jamming, is also proposed for authentic communication through secret keys [16]. A game-theoretic scheme is presented to exploit non-altruistic users as cooperative jammers for secure communication in[17]. The amount of confidentiality gathered by exploiting FJs is evaluated in [18]. They consider an attacker with multiple antennas. An FJ-based security model is proposed in [19], and analysis for different channel state information (CSI) is presented to provide optimal jamming.

3. System Model

Our first step in attacking the problem is optimizing the power of the jamming signal. We have utilized a well-defined mathematical function concerning distance. It is the summation of transmission power and the lost power on the path. However, we substituted the lost power with the difference between the transmit power and the received power. In this way, we both have the received power approach, which is our contribution, and guarantee to provide the received signal equal to the transmission power sufficient to jam the sources at the given distance.

In the following theorem, we state our model formally and claim that all the nodes inside the desired range will be jammed.

Theorem 1 (Optimum Jamming Power) *Let n be the number of nodes in a cellular network, T be the transmission power and T(k) be the transmission power of the k^{th} nearest node where $1 \leq k \leq n$. Assume T = T(k) for all k. Let J be the optimum jamming power and d be the desired distance to jam. Let $C = (\frac{v}{4.pi.f})^2$ where v is the speed of light, f is the carrier frequency and γ is the path loss exponent such that $2 \leq \gamma \leq 6$. The optimum power to jam the distance d is*

$$J(d) = T - 10.log_{10}C + 10.\gamma.log_{10}d \quad (1)$$

Proof: Let R be the received power. According to the simple path loss model, the received power from the k^{th} nearest node is

$$R(k) = 10.log_{10}C - 10.\gamma.log_{10}d + T \quad (2)$$

Let L be the lost power and L(k) be the lost power of the k^{th} nearest node. Since the largest one is sufficient to jam the network, the optimum jamming power is

$$J = max(J(d_1), J(d_2), ..., J(d_n)) \quad (3)$$

The received power from the jammer has to be T and in order to compensate the path loss it has to be added. Thus,

$$J = max(T + L(1), T + L(2), ..., T + L(n)) \quad (4)$$

Since the lost power of the n^{th} nearest node is larger than all the others, then

$$J(d_n) = T + L(n) \quad (5)$$

Since the lost power is the difference between T and R(n), it follows that

$$J(d_n) = T + (T - R(n)) \quad (6)$$

Substitute equation 2, then

$$J(d_n) = T - 10.log_{10}C + 10.\gamma.log_{10}d_n \quad (7)$$

Without loss of generalization

$$J(d) = T - 10.log_{10}C + 10.\gamma.log_{10}d \quad (8)$$

□

Corollary 1.1 (Finding Path Loss Exponent) *Let d be the present distance to jam and γ be*

the regarding path loss exponent. Let d' be the desired distance to jam. Then the regarding path loss exponent is

$$\gamma' = \gamma.\frac{log_{10}d}{log_{10}d'} \tag{9}$$

provided that

$$J(d) = J(d') \tag{10}$$

Proof: Let J be the optimum jamming power and J(d) be the optimum power to jam the distance d. According to Theorem 1

$$J(d) = T - 10.log_{10}C + 10.\gamma.log_{10}d \tag{11}$$

In the same manner,

$$J(d') = T - 10.log_{10}C + 10.\gamma'.log_{10}d \tag{12}$$

Since

$$J(d) = J(d') \tag{13}$$

It follows that

$$\gamma' = \gamma.\frac{log_{10}d}{log_{10}d'} \tag{14}$$

□

Corollary 1.2 (Center of d and γ) *Let n be the number of nodes in a cellular network, d_i be the distance to the i^{th} node and γ_i be the path loss exponent of the i^{th} node where $1 \leq i \leq n$. Let d_c be the center of distance to jam and γ_c be the center of path loss exponent to jam. Then,*

$$d_1{}^{\gamma_1}.d_2{}^{\gamma_2}...d_n{}^{\gamma_n} = d_c{}^{n.\gamma_c} \tag{15}$$

Proof: Let J be the optimum jamming power, $J(d_i)$ be the optimum power to jam the distance d_i such that $1 \leq i \leq n$ and $J(d_c)$ be the optimum power to jam the center of distances. It follows that

$$J(d_1) + ...J(d_n) = n.J(d_c) \tag{16}$$

According to Theorem 1

$$J(d_i) = T - 10.log_{10}C + 10.\gamma_i.log_{10}d_i \tag{17}$$

Substituting eq.17 into eq.16 we get

$$log_{10}(d_1{}^{\gamma_1}.d_2{}^{\gamma_2}...d_n{}^{\gamma_n}) = log_{10}d_c{}^{\gamma_c.n} \tag{18}$$

Therefore,

$$d_1{}^{\gamma_1}.d_2{}^{\gamma_2}...d_n{}^{\gamma_n} = d_c{}^{n.\gamma_c} \tag{19}$$

□

4. Evaluation

In this section, the proposed model is validated using Monte Carlo simulations in MATLAB, and simulations were run 1000 times (see Algorithm 1). Moreover, the results of our approach and the proposed model in [10] were compared and discussed using the same parameters shown in Table 1.

Table 1.
Parameters of the [10]

PARAMETER	VALUE	UNIT
SNR_{MIN}	9	dB
$Power_{MAX}$	-15	dBm
Frequency(f)	1880	MHZ
Distance(d)	10	m
Free Space Loss	58	dB

By its definition, SNR is as follows

$$SNR(dB) = Signal(dB) - Noise(dB) \tag{20}$$

Here, Noise is the jamming power at the receiver, input power.

$$9 = -15 - Noise(dB) \tag{21}$$

$$Noise(dB) = -24dBm \tag{22}$$

It follows that we have to add the path loss to find the output power (jamming power),

$$Power_{Jamming} = FreeSpaceLoss + Noise \tag{23}$$

$$Power_{Jamming} = 58 + (-24) \tag{24}$$

Algorithm 1 The MATLAB algorithm of simulations

1: $simcnt = 1000$ (Simulation count)
2: $Pt = 10^{-2.4}$ (Transmit power in mW)
3: $PtdBm = 10 * log_{10}Pt$; (Transmit power in dBm)
4: $f = 1.88 * 10^9$; (Frequency in Mhz)
5: $Gt = 1$ (Transmitting antenna gain)
6: $Gr = 1$ (Receiving antenna gain)
7: $gamma = 2$ (Path loss exponent)
8: $wavelength = 2.99 * 10^8/f$ (Wavelength in Mhz)
9: $C = Gt*Gr*(wavelength/(4*\pi))^2$ (Constant based on selected wavelength)
10: $r1 = 1:1:15$ (Distance)
11: $OurPr = C*Pt*(r_1)^{-2}$ (Our received transmit power in mW)
12: $OurPrdBm = 20*(log_{10}(2.99*10^8) - log_{10}4 - log_{10}\pi - log_{10}r1 - log_{10}f) + PtdBm$ (Our Pr in dBm)
13: $OurJ = 2 * Pt - OurPr$ (Our jamming power in mW)
14: $OurJrdBm = 20*(log_{10}(2.99*10^8) - log_{10}4 - log_{10}\pi - log_{10}r1 - log_{10}f) + OurJdBm$ (Our received J in dBm)
15: $PaperFspldBm = 32.44 + 20 * log_{10}(r1 * 10^{-3}) + 20 * log_{10}1880$ (Free space loss of [10] in dBm)
16: $PaperJdBm = PaperFspldBm + PtdBm$ (Jamming power of [10] in dBm)
17: $PaperRdBm = PaperJdBm - PaperFspldBm$ (Received power of [10] in dBm)
18: $OurCounter = OurJrdBm \geq PtdBm$ (Condition for coverage probability)
19: $OurSimulation = Ourcounter/simcnt$ (Our coverage probability)
20: $PaperCounter = PaperRdBm \geq PtdBm$ (Condition for coverage probability of [10])
21: $PaperSimulation = PaperCounter/simcnt$ (Coverage probability of [10])

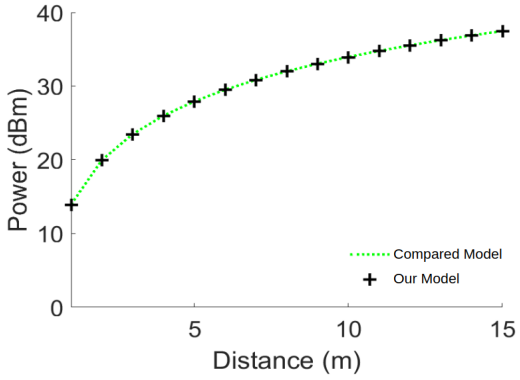

Figure 1. Jamming power comparison with respect to distance

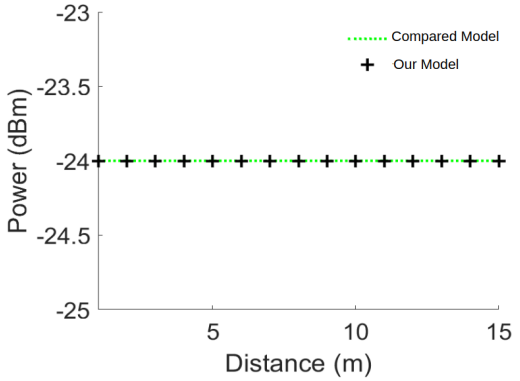

Figure 2. Received jamming power comparison with respect to distance

$$Power_{Jamming} = 34dBm \tag{25}$$

In Figure 1, we compared the jamming powers of the two models. Since the jamming of longer distances needs much more power, an increasing curve can be observed as expected. However, the most significant deduction is the overlapping of two models, which implies that our model performs as well as the model of [10] in free space.

The received jamming powers of the two models are illustrated in Figure 2, which is another expected result. According to the assumptions of both models, transmit powers are all the same and independent of the distance. If optimized jamming powers are lost due to the path, received powers have to be equal to

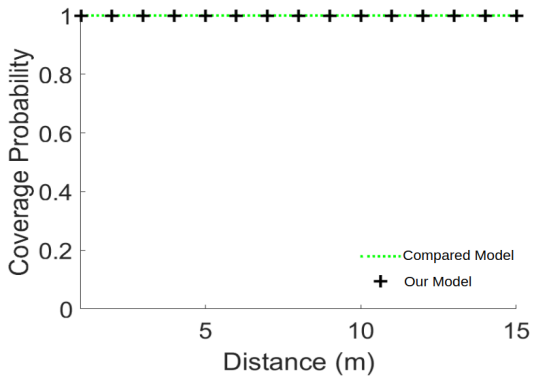

Figure 3. Coverage probability comparison with respect to distance

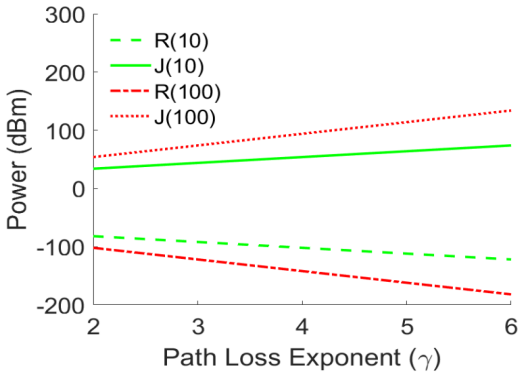

Figure 4. Received and jamming power comparison with respect to path loss exponent

the transmit power of target nodes preventing them from hearing each other.

Figure 3 depicts that two models cover any desired region with perfect performance. By composing the abovementioned analyses, it is not surprising, either. As the first result shows a case where, jamming power is optimized. It follows that the received power is the same as the noise, which means that the two models perform perfectly. Thus, nodes cannot hear each other since there is a noise with their communication level. Therefore we can infer that $\%100$ jamming coverage is provided for the desired range on top of the first two simulations. After determining path loss exponents, calculations of the optimized jamming power become straightforward. As expected, the received power from 10 m is higher than the received power from 100 m, and hence the jamming power of 100 m is higher than the jamming power of 10 m, too (see Figure 4).

Last but not least is the side effects of our model, basically disrupting legitimate communication. To minimize that effect, we have to choose the desired range to jam as the diameter of the corresponding cell in which the attacker resides. Thus, only the transmission inside that cell will be affected. Moreover, the network's density should be considered for improving the effectiveness by exploiting some models, such as [20].

5. Conclusion

The nature of wireless networks is a double-edged sword. On the one hand, it is possible to easily share and reach information, including our private data, anywhere and anytime, provided that we are in the coverage area. On the other hand, attackers can also exploit the convenience of this prevailing world. They inherently devise unprecedented attacks with new toolsets for each novel technology. Most conventional methods against these attacks are based on cryptography, which consumes significant energy and computing power. However, these techniques fail to meet the requirements of some current technologies, such as 5G and IoT, since eligible devices for them have energy and computing power constraints.

Moreover, any attacker with significant resources can make these methods ineffective. Therefore, friendly jamming (FJ) is a promising solution to these challenges due to its operability with considerably low energy and computation sources. Besides the advantages, there are also disadvantages of FJ,

such as the applicability. Although some models are proposed to tackle that issue, they are not straightforward and must be updated for new technologies. In this paper, we propose a lightweight and flexible FJ model that is well-posed for the mentioned drawbacks of the studies. It is also clearly illustrated that our model has the same performance as one of the mentioned studies above in a more straightforward way. Therefore, the proposed model in this study is energy-efficient and computationally cheap, which is also viable for new technologies. However, there are some limitations of our research:

- Although we have mathematically proved our model, it needs to be implemented physically to observe its viability on various types and sizes of networks
- Testing the model for different attackers will increase its robustness
- Last but not least is the issue of legal restrictions. Since each government has different regulations on jamming, such as permitted hardware and frequency, they must be considered while performing FJ

As future research, we aim to study the first two limitations.

Acknowledgment

The first author of this study is a 100/2000 YOK PhD scholar.

References

[1] Y. Huo, et al. "Secure communications in tiered 5G wireless networks with cooperative jamming," IEEE Trans. on Wireless Comm., vol. 18, no. 6, pp. 3265-3280, 2019.

[2] B. Li, Z. Fei, Y. Zhang and M. Guizani, "Secure UAV communication networks over 5G," IEEE Wireless Comm., vol. 26, no. 5, pp. 114-120, 2019.

[3] Q. Wang, HN. Dai, H. Wang, G. Xu and AK. Sangaiah, "UAV-enabled friendly jamming scheme to secure industrial Internet of Things," Journal of Comm. and Networks, vol. 21, no. 5, pp. 481-90, 2019.

[4] H. Dang-Ngoc et al. "Secure swarm UAV-assisted communications with cooperative friendly jamming," IEEE Internet of Things Journal, vol. 9, no. 24, pp. 25596-25611, 2022.

[5] TV. Pham and AT. Pham, "Energy-efficient friendly jamming for physical layer security in visible light communication," presented at the IEEE International Conf. on Comm. Workshops, Montreal, QC, Canada, 2021.

[6] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," presented at the IEEE Globecom Workshops, Austin, TX, USA, 2014.

[7] I. Martinovic, P. Pichota and JB. Schmitt, "Jamming for good: a fresh approach to authentic communication in WSNs," presented at the ACM Conf. on Wireless Network Sec., Zurich, Switzerland, 2009.

[8] DS. Berger, F. Gringoli, N. Facchi, I. Martinovic and JB. Schmitt, "Friendly jamming on access points: Analysis and real-world measurements," IEEE Trans. on Wireless Comm., vol. 15, no. 9, pp. 6189-6202, 2016.

[9] DS. Berger, F. Gringoli, N. Facchi, I. Martinovic and J. Schmitt, "Gaining insight on friendly jamming in a real-world IEEE 802.11 network," presented at the ACM Conf. on Sec. and Privacy in Wireless and Mobile Networks, Oxford, U.K., 2014.

[10] DS. Madara, E. Ataro and S. Sitati, "Design and testing of a mobile-phone-jammer," Innovative systems design and engineering, vol. 7, no. 7, pp. 7-18, 2016.

[11] J. Li, X. Lei, PD. Diamantoulakis, L. Fan and GK. Karagiannidis, "Security Optimization of Cooperative NOMA Networks With Friendly Jamming," IEEE Trans. on Vehicular Tech., vol. 71, no. 12, pp. 13422-13428, 2022.

[12] R. Jin, K. Zeng and K. Zhang, "A reassessment on friendly jamming efficiency," IEEE Trans. on Mobile Computing, vol. 20, no. 1, pp. 32-47, 2019.

[13] J. Kim and JP. Choi, "Cancellation-based friendly jamming for physical layer security," presented at the IEEE Global Comm. Conf., Washington, DC, USA, 2016.

[14] JP. Vilela, M. Bloch, J. Barros and SW. McLaughlin, "Friendly jamming for wireless secrecy," presented at the IEEE International Conf. on Comm., Cape Town, S. Africa, 2010.

[15] Z. Mobini, M. Mohammadi and C. Tellambura, "Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications," IEEE Trans. on Info. Forensics and Sec., vol. 14, no. 3, pp. 621-34, 2018.

[16] W. Shen, P. Ning, X. He and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," presented at the IEEE Sym. on Sec. and Privacy, Berkeley, CA, USA, 2013.

[17] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," IEEE Trans. on Wireless Comm., vol. 12, no. 1, pp. 134-45, 2012.

[18] NO. Tippenhauer, L. Malisa, A. Ranganathan and S. Capkun, "On limitations of friendly jamming for confidentiality," presented at the IEEE Sym. on Sec. and Privacy, Berkeley, CA, USA, 2013.

[19] JP. Vilela, M. Bloch, J. Barros and SW. McLaughlin, "Wireless secrecy regions with friendly jamming," IEEE Trans. on Info. Forensics and Sec., vol. 6, no. 2, pp. 256-66, 2011.

[20] O. Yaman, A. Eroglu and E. Onur, "Density-aware cell zooming," presented at the Conf. on Innovation in Clouds, Internet and Networks and Workshops, Paris, France, 2018.