A Lightweight and Energy Efficient Secrecy Outage Probability-based Friendly Jamming

Okan Yaman
Department of Computer Engineering
Izmir Institute of Technology
Izmir, TURKEY
okanyaman@iyte.edu.tr
ORCID: 0000-0001-7292-2344

Tolga Ayav
Department of Computer Engineering
Izmir Institute of Technology
Izmir, TURKEY
tolgaayav@iyte.edu.tr
ORCID: 0000-0003-1426-5694

Yusuf Murat Erten
Department of Computer Engineering
Izmir University of Economics
Izmir, TURKEY
yusuf.erten@ieu.edu.tr
ORCID: 0000-0001-9537-7414

2023 11th International Symposium on Digital Forensics and Security (ISDFS) | 979-8-3503-3698-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISDFS58141.2023.10131740

***Abstract*—Third parties and legitimate entities can reach and process users' private data through most wireless networks. However, attackers such as intruders and eavesdroppers may also try to exploit this property in communication. Hence, wireless networks are intrinsically more vulnerable to threats, unlike their wired alternatives. Cryptographic techniques are the conventional approaches to deal with that weakness. Nevertheless, they still need to meet the requirements of contemporary technologies, including IoT nodes with energy and processing power constraints. In that respect, friendly jamming (FJ) is one of the encouraging countermeasures to overcome the mentioned susceptibility since it has an energy-efficient and computation-friendly nature. However, that promising approach brings another challenge, applicability. Although various models exist against this issue, a lightweight scheme compliant with novel technologies is needed. Hence, we propose a more straightforward FJ model evaluated on cellular network-based simulations in this study. Moreover, introducing a lightweight secrecy outage probability definition increases robustness and energy efficiency.**

Keywords*—*Physical layer security, Friendly jamming, Secrecy outage probability

I. Introduction

According to many historians, we have been passing through the information age. Hence, data is one of the most valuable entities today, and current technologies try to provide data to users continuously wherever they reside. In this sense, an extensive infrastructure is required, similar to a supply chain with an invisible road network. Since air is the transmission medium for wireless networks, we are all surrounded by this ocean of data. However, that wide availability brings some severe security and privacy concerns. Intrinsically, it is easier for attackers to intrude on the system and gather some private information belonging to network users.

Cryptographic approaches are among the traditional techniques for providing wireless network security. Although achieving high levels of protection, the main drawback is their excessive usage of computation and energy sources. Due to physical limitations, new technologies require resource-efficient methods. Moreover, society and authorities demand eco-friendly solutions due to increasing awareness of global warming and climate change. Here, friendly jamming (FJ) emerges as a promising alternative. When implemented by an attacker, it is a threat and relies on disrupting transmission by reducing signal-to-noise ratio (SNR) by emitting additional noise to the network. However, we can employ that threat to thwart illegitimate transmission and thus provide security of the system to some extent, depending on the FJ precision.

Thanks to its resource-efficient performance, various networks utilize FJ, including Wireless Sensor Networks (WSN) [1], IoT (Internet of Things) [2], Industrial IoT [3], and 5G [4, 5]. Nevertheless, they must address some challenges as much as possible, including fulfilling real-life requirements, achieving maximum performance with minimum adverse effects, and consuming energy efficiently. Our previous study [6] has proposed a more straightforward and flexible model than its counterparts in the literature to suffice the mentioned challenges. However, it needs to be extended for various threats that will improve the robustness of the proposed model.

In this study, we introduce a novel and lightweight secrecy outage probability (SOP) definition compared to current models in the literature. In our previous work, based on continuous FJ, we have not considered sophisticated attackers who know when FJ is performed. Thus, intermittent FJ is the center of the model proposed in this paper, leading to a saving in energy consumption compared to its continuous alternative. We have demonstrated through cellular network simulations that it is possible to deceive the attacker that the jammed part of the message results from natural effects such as routine data loss.

This study has two main contributions:

- Introduction of a novel and lightweight SOP definition
- Improvement of our previous model by considering more sophisticated attackers, and thus gathering more robust and energy efficient countermeasure

The paper is organized as follows: the related work on FJ and SOP is presented in Section 2. Section 3 states the system and attacker model, and the results and discussion are provided in Section 4. Finally, the paper is concluded in Section 5.

II. Related Work

An SOP-based analysis exists on FJ selection-aided multiuser scheduling in [7]. The authors propose random and optimum FJ selection-aided multiuser scheduling models. Stationary and mobile unmanned aerial vehicle (UAV) FJ schemes are introduced in [8]. They employ SOP for the air-to-ground channel model through a novel boundary coverage algorithm considering the minimum number of UAVs. The authors of [9] provide physical layer security (PLS) for single-input-multiple-output (SIMO) wiretap channel through uncoordinated cooperative

979-8-3503-3698-6/23/$31.00 ©2023 IEEE

Authorized licensed use limited to: ULAKBIM UASL - IZMIR YUKSEK TEKNOLOJI ENSTITUSU. Downloaded on September 01,2023 at 06:47:38 UTC from IEEE Xplore. Restrictions apply.

jamming. They also try to address the power allocation for the secrecy rate maximization problem with a modified difference of convex function programming technique. Another SOP analysis in the downlink for wireless networks through spatially distributed eavesdropping is included in [10]. Half-duplex and full-duplex mode receiving user equipment (UE) cases were examined. The authors in [11] investigate the effect of cooperative and friendly jamming on the SOP of a quasi-static wiretap fading channel. Three jamming methods are analyzed based on channel state information (CSI) and security metrics, jamming coverage and efficiency. There is a Rayleigh fading-based formal secrecy outage and interception probability analysis for multiple-input and multiple-output (MIMO) wireless system in [12]. The model in [13] is designed considering jamming coverage and efficiency-based security level in a quasi-static fading environment through SOP. There is also various CSI-based jamming analysis. A new method based on minimizing compromised secrecy region is proposed in [14].

Path loss and fading channel effects determine the secrecy region and its corresponding SOP. Moreover, a novel optimization principle is introduced regardless of the randomly deployed eavesdropper position. The authors in [15] discussed radio frequency energy harvesting in a WSN for multiple eavesdroppers. The best relay and jammer are determined and analyzed based on key system factors on SOP, such as the number of eavesdroppers. A wireless-powered communication network is equipped with an energy-harvesting jammer and an eavesdropper in [16]. The authors analyze the scheme on how to minimize SOP for given CSI.

The authors in [17] propose FJ-based MAC protocol scenarios and routing protocols considering intermittent jamming. Another study presents a jamming approach for PLS in Visible Light Communication (VLC) [18]. Their main contribution is the energy-friendly nature of their model. It is described as an implementation of FJ on Internet of medical things (IoMT) [19]. There is also an analysis and discussion through two case studies. A JF-based model is proposed to improve the secrecy sum-rate for cooperative Non-Orthogonal Multiple Access (NOMA) networks [20]. The extension of [6] examines the problem of location privacy in cellular networks [21]. It proposes the FJ to address that issue.

III. Model

In this section, we define the system and attacker models that are extensions of our previous study [6].

A. System Model

In this paper, we perform intermittent FJ to minimize the effects stated in the attacker model. Moreover, there is a novel and lightweight SOP definition that can also be considered as the secrecy exposure probability. The duration of FJ and communication have inverse proportionality. Then, the SOP can be defined simply as follows

$$SOP = 1 - (T_J \ / \ \mathrm{T_C}) \tag{1}$$

where T_J *and* T_C *are durations of FJ and communication, respectively.*

TABLE I. Some Key Features of related work

Reference	SOME KEY FEATURES		
	Medium	***Threat***	***Solution***
[7]	Uplink Network	Eavesdropping (E)	FJ
[8]	UAV Network	E	UAV Jamming
[9]	Cellular Uplink	E	UCJ[A]
[10]	Wireless Downlink	E	FJ
[11]	QSWFC[B]	E	CFJ[C]
[12]	MIMO	E and Jamming	TWU[D]
[13]	QSRFC[E]	E	FJ
[14]	RFC[F]	E	CFJ
[15]	WSN	E	FJ
[16]	WPCN[G]	E	EHJ[H]
[17]	MANET[I]	E	FJ
[18]	VLC	E	FJ
[19]	IoMT	E	FJ
[20]	NOMA	E	FJ
[21]	Cellular Network	E	FJ

[A] Uncoordinated Cooperative Jamming

[B] Quasi-Static Wiretap Fading Channel

[C] Cooperative Friendly Jamming

[D] Transmit Waveform Update

[E] Quasi-Static Rayleigh Fading Channel

[F] Rayleigh Fading Channel

[G] Wireless Powered Communication Network

[H] Energy Harvesting Jamming

[I] Mobile Ad-Hoc Network

B. Attacker Model

Let N be the number of nodes in a wireless network. Let L and A be the number of legitimate and attacker nodes, respectively. For simplicity, we assume only one attacker in the network; hence, A = 1. We also anticipate two kinds of threats, internal and external. The mechanism of the former takes place by intruders through compromising legitimate nodes. The latter is directly performed against the network totally or partially. The goal of attackers for both threats is to gather the transmitted data over the network without damaging legitimate communication. Therefore, man in the middle and eavesdropping are possible types of attacks. We also consider levels of threats regarding their attacking power (see Section 4).

IV. Results and discussion

In this section, we analyze the proposed SOP definition. Then the results are discussed for one-minute Monte Carlo simulations through our own PYTHON script with no additional library or tool. As mentioned in Section 3, the main parameter for SOP is the duration of FJ, and their relation is illustrated in Figure 1. As expected, SOP decreases for increasing FJ Duration, since it would be harder for an attacker to listen to the channel (see (1)). We can extend that plot by reconsidering the FJ Duration as a novel parameter, the number of jammed words. Assume that a legitimate node transmits one word per second. Hence, finding the plot in Figure 2 is straightforward. The more

Authorized licensed use limited to: ULAKBIM UASL - IZMIR YUKSEK TEKNOLOJI ENSTITUSU. Downloaded on September 01,2023 at 06:47:38 UTC from IEEE Xplore. Restrictions apply.

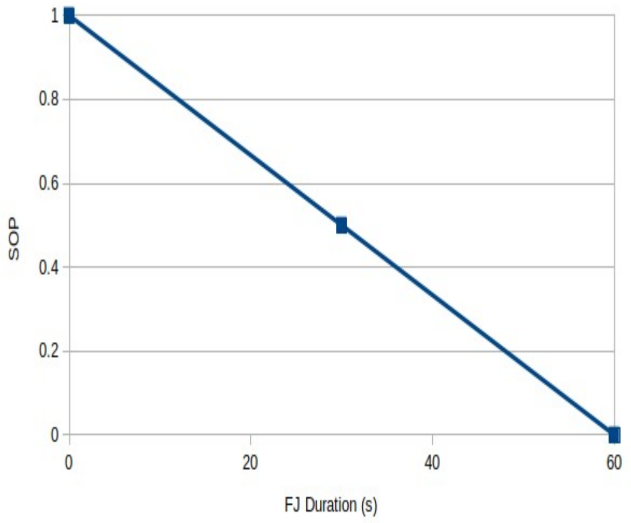

Fig. 1. Effect of FJ Duration on SOP.

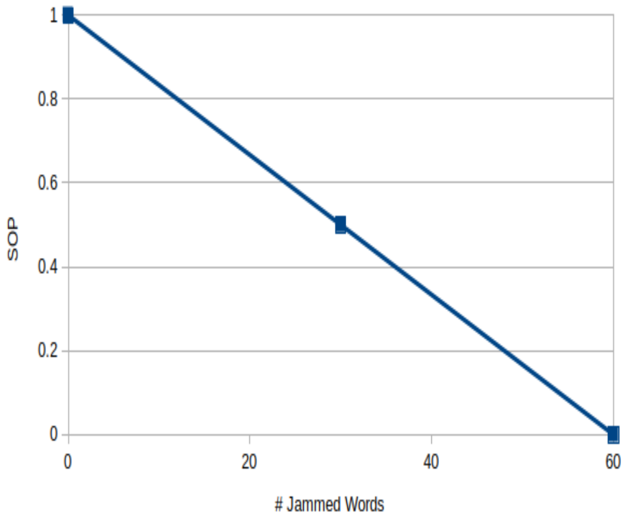

Fig. 2. Relation between number of jammed words and SOP.

jammed words infer a fall in SOP, since it would be more challenging for an adversary to deduce words. Thus, that result is not a surprise, either.

We assume that the attackers' strength is constant for the first two results. However, our last analysis will investigate the robustness of our system for varying levels of threats. By "level of threat," we mean the capability of the attacker to detect the instance of FJ.

In Figure 3, three attackers are considered. The first and also with the least power is called poor. He can detect the operation of FJ with 100% certainty after 75% of the words are jammed. The second, moderate attacker, can realize that the communication is hidden by checking the number of understandable words. We assume that the threshold of the moderate attacker is 50% of the whole communication. The last case is for the sophisticated attacker. As the name implies, it is the most challenging for our countermeasure and can harm the system the most compared to other cases.

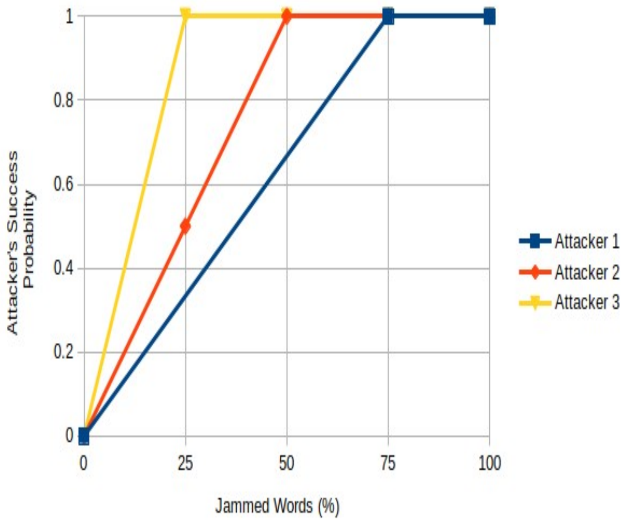

Fig. 3. Impact of jammed words percentage on attacker's success

When he can not identify 25% of the words in the channel, he realizes that the system exposes him.

For the following analyses, we utilized the FJ Power for a cellular network case of our former study, -24 dBm ≈ 0.004 mW [6]. In Figure 4, we deduce similar results to Figure 3. Since 75% is the jamming word threshold of the sophisticated attacker, 75% of 0.004 mW is the minimum required FJ power to perform the maximum level of damage. 50% and 25% of 0.004 mW are the FJ power thresholds for moderate and poor attackers, respectively.

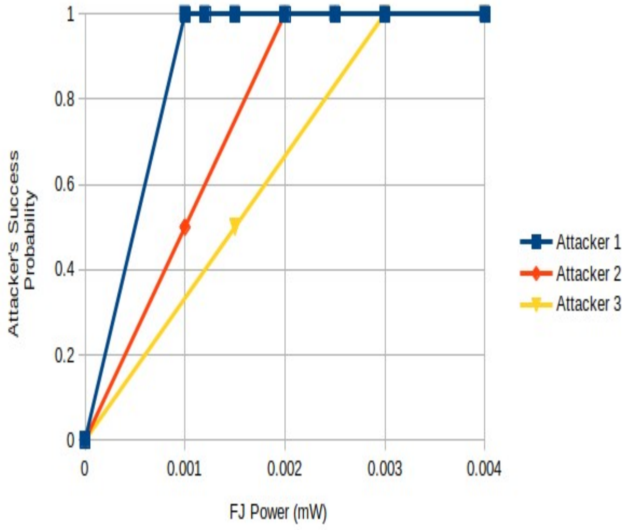

Fig. 4. Relation between fj power and success probability

The threshold values found in Figure 4 are the optimum FJ powers to eliminate the threats for corresponding attackers. They are illustrated in Figure 5.

The final result validates our claim on energy efficiency. Therefore, it is the most significant output of this study. If we performed continuous FJ, the power would be 0.004 mW (see [6]). For eliminating the poor attacker, 0.001 mW is sufficient, as illustrated in Figure 5. Hence, the saved power for that attacker is 0.003. Similarly, 0.002 and 0.001 mW can

Authorized licensed use limited to: ULAKBIM UASL - IZMIR YUKSEK TEKNOLOJI ENSTITUSU. Downloaded on September 01,2023 at 06:47:38 UTC from IEEE Xplore. Restrictions apply.

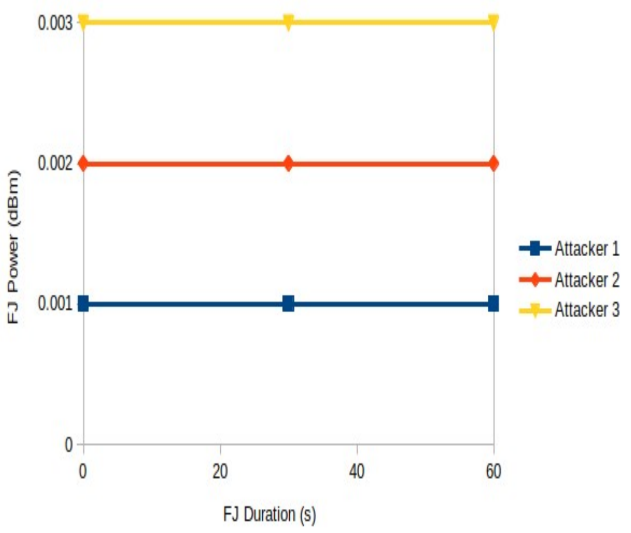

Fig. 5. Relation between fj power and duration of varying attackers

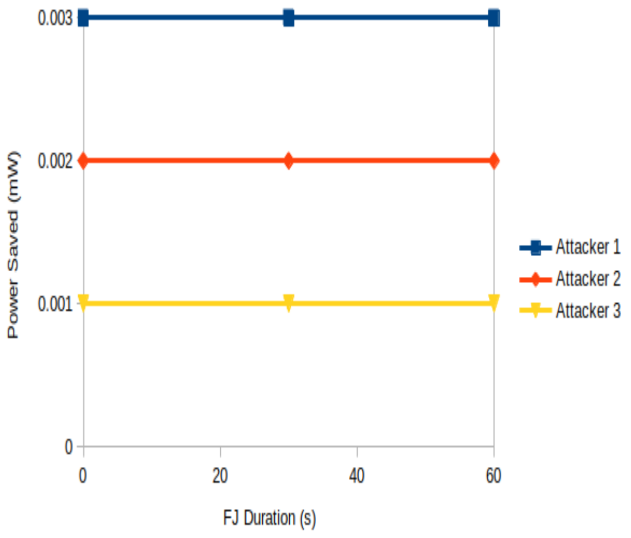

Fig. 6. Impact of fj duration on saved power for attackers

be found for the moderate and the sophisticated attackers, respectively.

Finally, we assume that all the attackers can detect words used in messages they hear, and they can calculate the number of possible words to be sent by exploiting elapsed time. We consider the following as future research:

- Case of simultaneous attack by multiple attackers and utilizing some density estimators [22]
- Determining weight factors for some keywords

V. Conclusion

Due to their widely available and easily accessible properties, wireless networks are undoubtedly a blessing in terms of communication. It is easy to send and receive a wide range of data, one of which is our personal information, whenever and wherever we desire. Thus, these key features will probably lead us to exploit that technology in the foreseeable future. However, attackers might abuse that environment broadly covering us. Traditional solutions generally rely on cryptography that inefficiently exploits resources, such as energy and computation power. Nevertheless, they can not fulfill the requirements of new networks, including IoT and 5G, that are operable with physically restricted entities.

Furthermore, those techniques can easily be breached by a sufficiently equipped attacker. In that respect, FJ emerges as a brilliant remedy against the problem owing to its energy and computation-friendly nature. Apart from benefits, FJ has some drawbacks, including viability. In this study, we introduce a lightweight and energy-efficient FJ model. The outputs of the simulations demonstrate the improved robustness and savings in FJ power and hence energy. As future research, we plan to improve this study by introducing a weight factor for each word.

Acknowledgment

The first author of this study is a 100/2000 YOK Ph.D. Scholar.

References

[1] *I. Martinovic, P. Pichota and JB. Schmitt, ”Jamming for good: a fresh approach to authentic communication in WSNs,” in Proceedings of the ACM Conf. on Wireless Network Sec., Zurich, Switzerland, 2009, doi: 10.1145/1514274.1514298.*

[2] 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, doi: 10.1109/JIOT.2022.319975.

[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, doi: 10.1109/JCN.2019.000042.

[4] 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, doi: 10.1109/TWC.2019.2912611.

[5] 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, doi: 10.1109/MWC.2019.1800458.

[6] O. Yaman, T. Ayav and Y. M. Erten, “A Lightweight Self-Organized Friendly Jamming,” International Journal of Information Security Science, vol. 12, no:1, pp. 13-20, 2023, doi: 10.55859ijiss.1194643.

[7] B. Li et al. “Secrecy Outage Probability Analysis of Friendly Jammer Selcetion Aided Multiuser Scheduling for Wireless Networks,” IEEE Trans. on Comm., vol. 67, no. 5, pp. 3482-3495, 2019, doi: 10.1109/TCOMM.2019.2894824.

[8] Y. Zhou et al. “Secrecy Outage Probability and Jamming Coverage of UAV-enabled Friendly Jammer,” in Proceedings of the International Conf. on Signal Processing and Comm. Systems, Surfers Paradise, Australia, 2017, doi: 10.1109/ICSPCS.2017.8270455.

[9] P. Mu, X. Hu, B. Wang and Z. Li, “Secrecy Rate Maximization with Uncoordinated Cooperative Jamming by Single-Antenna Helpers Under Secrecy Outage Probability Constraint,” IEEE Comm. Letters, vol. 19, no. 12, pp. 2174-2177, 2015, doi: 10.1109/LCOMM.2015.2490138.

[10] G. Chen, J. P. Coon and M. Di Renzo, “Secrecy Outage Analysis for Downlink Transmissions in the Presence of Randomly Located Eavesdroppers,” IEEE Trans. On Info. Forensics and Sec., vol. 12, no. 5, pp. 1195-1206, 2017, doi: 10.1109/TIFS.2017.2656462.

[11] J.P. Vilela, M. Bloch, J. Barros and S.W. McLaughlin, “Friendly Jamming for Wireless Secrecy,” in Proceedings of the IEEE Conf. on Comm., Cape Town, S. Africa, 2010, doi:10.1109/ICC.2010.5502606.

[12] D. B. Rawat, T. White, MD. S. Parwez, C. Bajracharya and M. Song, “Evaluating Secrecy Outage of Physical Layer Security in Large-Scale MIMO Wireless Communications for Cyber-Physical Systems,” IEEE Internet of Things Journal, vol. 4, no. 6, 2017, doi: 10.1109/JIOT.2017.2691352.

[13] J.P.Vilela, M. Bloch, J. Barros and S.W. McLaughlin, “Wireless Secrecy Regions With Friendly Jamming,” IEEE Trans. On Info. Forensics and Sec., vol. 6, no. 2, 2011, doi:10.1109/TIFS.2011.2111370.

[14] H. Li, X. Wang and W. Hou, “Security enhancement in cooperative jamming using compromised secrecy region minimization,” in Proceedings of the Canadian Workkshop on Info. Theory, Toronto, ON, Canada, 2013, doi: 10.1109/CWIT.2013.6621623.

Authorized licensed use limited to: ULAKBIM UASL - IZMIR YUKSEK TEKNOLOJI ENSTITUSU. Downloaded on September 01,2023 at 06:47:38 UTC from IEEE Xplore. Restrictions apply.

[15] V.Nhan Vo, T.G. Nguyen, C. So-in, Z.A. Baig and S. Sanguanpong, “Secrecy Outage Performance Analysis for Energy Harvesting Sensor Networks With a Jammer Using Relay Selection Strategy,” IEEE Access, vol. 6, pp. 23406-23419, 2018, doi: 10.1109/ACCESS.2018.2829485..

[16] J. Moon, H. Lee, C. Song and I. Lee, “Secrecy Outage Minimization for Wireless Poered Communication Networks with an Energy Harvesting Jammer,” in Proceedings of the IEEE Global Comm. Conf., Washington, DC, USA, 2016, doi: 10.1109/GLOCOM.2016.7842246.

[17] J. Kim et al. “Advanced protocols for the mitigation of friendly jamming in mobile ad-hoc networks,” Journal of Network and Computer Applications, vol. 181, 2021, 103037, doi: 10.1016/j.jnca.2021.103037.

[18] T. V. Pham and A. T. Pham, “Energy-efficient friendly jamming for physical layer security in visible light communication,” in Proceedings of the IEEE Int. Conf. On Comm. Workshops, Montreal, QC Canada, 2021, doi: 10.1109/ICCWorksops50388.2021.9473744.

[19] X. Li et al. “Securing Internet of Medical Things with Friendly-jamming schemes,” Computer Communications, vol. 160, pp. 431-442, 2020, doi: 10.1016/j.comcom.2020.06.026.

[20] J. Li, X. Lei, P.D. Diamantoulakis, L. Fan, and G.K. Karagiannidis, “Security Optimization of Cooperative NOMA Networks With Friendly Jamming,” IEEE Trans. On Vehicular Tech., vol. 71, no. 12, pp. 13422-13428, 2022, doi: 10.1109/TVT.2022.3200253.

[21] O. Yaman, “Location privacy in cellular networks,” Ph.D. dissertation [Online], Dept. Comp. Eng., Izmir Institute of Technology, Izmir, TURKEY, 2022, Available: https://hdl.handle.net/11147/13430.

[22] O. Yaman, A. Eroglu and E. Onur, “Density-aware cell zooming,” in Proceedings of the Conf. On Innovations in Clouds, Internet and Networks and Workshops, Paris, 2018, pp: 1-8, doi: 1109/ICIN.2018.8401612.

Authorized licensed use limited to: ULAKBIM UASL - IZMIR YUKSEK TEKNOLOJI ENSTITUSU. Downloaded on September 01,2023 at 06:47:38 UTC from IEEE Xplore. Restrictions apply.