Friendly-Jamming Schemes to Secure Ultra-Reliable and Low-Latency Communications in 5G and Beyond Communications

Xuran Li[a], Hong-Ning Dai[b,*], Mahendra K. Shukla[c], Dengwang Li[a], Huaqiang Xu[a], Muhammad Imran[d]

[a] *School of Physics and Electronics, Shandong Normal University, Jinan, Shandong, China; sdnulxr@sdnu.edu.cn; dengwang@sdnu.edu.cn; xuhq@sdnu.edu.cn*

[b] *Faculty of Information Technology, Macau University of Science and Technology, Macau SAR; hndai@ieee.org*

[c] *Department of Electrical and Computer Engineering, University of Saskatchewan, Canada; mahendra.iiitm@gmail.com*

[d] *College of Applied Computer Science, King Saud University, Riyadh, Saudi Arabia; dr.m.imran@ieee.org*

Abstract

The security vulnerabilities are becoming the major obstacle to prevent the wide adoption of ultra-reliable and low latency communications (URLLC) in 5G and beyond communications. Current security countermeasures based on cryptographic algorithms have a stringent requirement on the centralized key management as well as computational capabilities of end devices while it may not be feasible for URLLC in 5G and beyond communications. In contrast to cryptographic approaches, friendly jamming (FJ) as a promising physical layer security method can enhance wireless communications security while it has less resource requirement on end devices and it can be applied to the full distribution environment. In order to protect wireless communications, FJ signals are introduced to degrade the decoding ability of eavesdroppers who maliciously wiretap confidential information. This article presents a state-of-the-art survey on FJ schemes to enhance network security for IoT networks with consideration of various emerging wireless technologies and different types of networks. First, we present various secrecy performance metrics and introduce the FJ method. The interference caused by FJ signals on legitimate communication is the major challenge of using FJ schemes. In order to overcome this challenge, we next introduce the integration of FJ schemes with various communication technologies, including beamforming, multiple-input multiple-output, full duplex, and relay selection. In addition, we also integrate FJ schemes with different types of communication networks. Finally, a case study of FJ schemes is illustrated and future research directions of FJ schemes have been outlined.

Keywords: Beyond 5G communications, ultra-reliable and low-latency communications, friendly jamming, physical layer security

1. Introduction

As one of the critical application scenarios to support time-critical applications in 5G and beyond communications, the URLLC technologies have received extensive attention recently [1, 2, 3, 4]. There are a number of studies on the applications of URLLC, such as in industrial Internet of Things (IoT) networks [5, 6], vehicular networks [7, 8, 9, 10], UAV communication systems [11, 12], virtual reality networks [13] and remote healthcare systems [14]. On the one hand, the proliferation of URLLC enables a diversity of applications which have high requirements in reliability and latency. On the other hand, the wide adoption of URLLC in 5G and beyond communications is also facing some challenges, especially in the security and privacy aspects. For example, URLLC links are often vulnerable to eavesdropping (or wiretapping) behaviours due to the openness of radio channels. Following eavesdropping activities, other malicious attacks, such as man-in-the-middle, spoofing, and falsification attacks may occur as in [15, 16, 17, 18].

Hence, the countermeasures to secure URLLC have to be enforced to protect the massive amount of confidential data from malicious attacks, especially for eavesdropping attacks. However, identifying the eavesdropping activities is difficult since malicious nodes often passively eavesdrop the confidential data without disclosing their locations [19, 20].

Traditionally, cryptographic techniques are most commonly employed to protect the security of wireless communications [21, 22, 23, 24, 25]. Nevertheless, cryptographic schemes require a proper key generation, distribution, and management while it may not be feasible for URLLC, which has a strict requirement of ultra-low latency. Meanwhile, the relatively short channel block-length also limits the usage of complicated encryption algorithms in URLLC [26].

Different from computational-complex cryptographic techniques, physical layer security (PLS) is able to offer a less computational-complex solution to the security of URLLC by generating artificial noise or designing lightweight

[*] Corresponding author
Email address: `hndai@ieee.org` (Hong-Ning Dai)

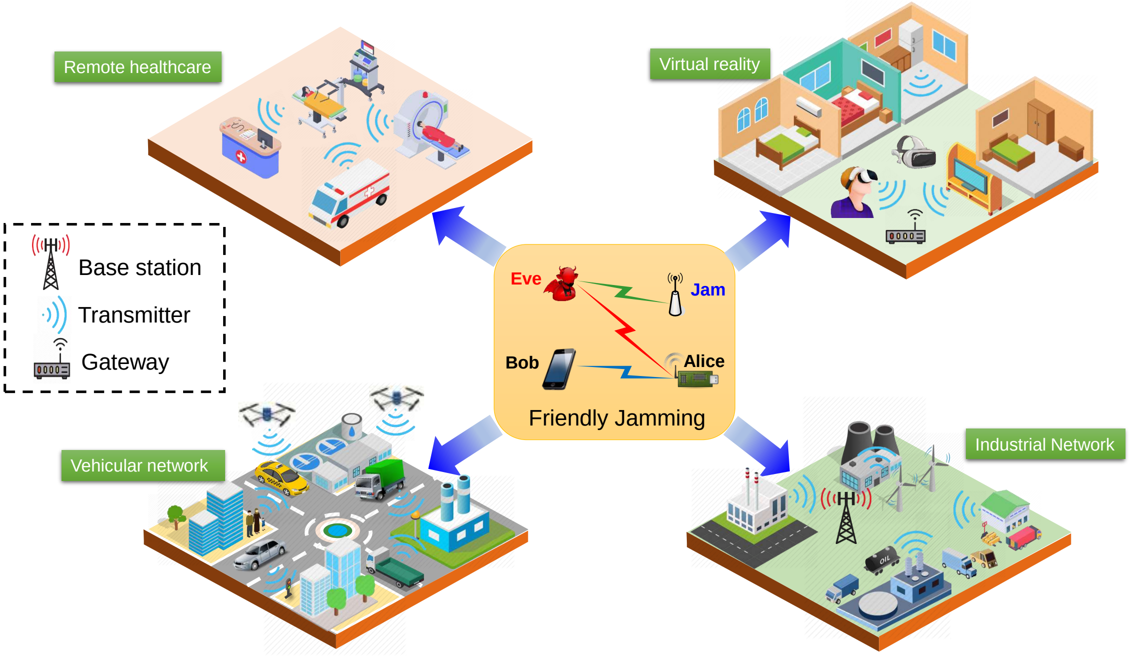


Figure 1: Applications of Friendly Jamming in beyond 5G Networks.

encryption schemes through leveraging the intrinsic randomness of wireless channels. One merit of PLS techniques for URLLC is that the key distribution and encryption/decryption process are not required [18, 26, 27].

Among all the approaches of PLS, exploiting noise and interference signals is an efficient and effective approach to confuse the eavesdropper and strengthen network security [28, 29, 30]. The most appealing designs by exploiting the advantage of artificial noise signals to thwart eavesdroppers are artificial-noise schemes and cooperative-jamming schemes. Specifically, artificial-noise signals are transmitted together with the confidential signals by the legitimate transmitter itself whereas jamming signals in cooperative jamming schemes are generated by external helping nodes [31, 32, 33]. In recent studies, the artificial-noise signals generated by relay nodes or additional users are also considered in artificial-noise schemes [34, 35, 36]. In this paper, we refer both cooperative jamming schemes and artificial noise-aided schemes to *friendly-jamming* (FJ) schemes since both of them are used for the same objective and they have similar noise-generation methods.

The FJ method essentially injects FJ signals into the wireless channels of the eavesdroppers so that the eavesdroppers are not able to decode the confidential information signals successfully due to the minimized Signal-to-Interference-and-Noise Ratio (SINR). The main merits of FJ methods are the low computational load and low implementation complexity [37]. Moreover, the coordination messages exchanging and extra processing of the legitimate information signals are unnecessary in FJ schemes. In Figure 1, we show several application domains of FJ schemes to secure URLLC, e.g., remote healthcare systems, vehicular networks, virtual reality (VR) networks, and industrial IoT networks.

On the other hand, in conventional FJ schemes, the interference management is a critical problem to be solved. In particular, the impact of FJ interference on legitimate transmissions needs to be minimized. Meanwhile, the power of FJ signals should be limited to be lower than a certain threshold. Moreover, the FJ devices should be feasible for most common communication protocols. Furthermore, the effectiveness of the FJ method is challenging in a dynamic environment. These restrictions limit the wide application of FJ schemes in URLLC of 5G and beyond networks.

Recently, there are extensive attentions on integrating FJ methods with other wireless techniques to deal with the challenges of FJ schemes. For example, the integration of FJ with beamforming concentrates the jamming power to increase the interference at the eavesdropper [38, 39, 40, 41, 42, 43]. Moreover, the integration of FJ with MIMO technique improves secrecy performance with the extra spatial degrees of freedom [44, 45, 46, 47, 48, 49]. The full-duplex technique allows legitimate receivers or relay devices to transmit FJ signals [28, 50]. With relay selection techniques, the desired relay device transmits information signal while other relay devices transmit FJ signals [51, 52, 53]. When network coding is integrated with FJ, the effectiveness of FJ to enhance the secrecy performance is improved [54, 55]. The integration of FJ with game theory provides the decisions in choosing the proper chance to conduct jamming [56, 57].

Furthermore, FJ schemes can be applied to different types of communication networks to further enhance network security. The representative communication networks

Table 1: Terms and abbreviations

Acronyms	Terms	Acronyms	Terms
5G	Fifth generation	MIMO	Multiple-Input Multiple-Output
AN	Artificial Noise	MISO	Multiple-Input Single-Output
BS	Base Station	PLS	Physical Layer Security
CRN	Cognitive Radio Network	PU	Primary User
CSI	Channel State Information	RF	Radio Frequency
D2D	Device-to-Device	SDR	semidefinite relaxation
COP	Connection Outage Probability	SIC	Successive Interference Cancellation
FD	Full Duplex	SINR	Signal-to-Interference-and-Noise Ratio
FJ	Friendly Jamming	SOP	Secrecy Outage Probability
HD	Half Duplex	SU	Secondary User
HetNet	Heterogeneous Network	SWIPT	Simultaneous wireless information and power transfer
IC	Integrated Circuit	UAV	Unmanned-Aircraft Vehicles
IoT	Internet of Things	URLLC	Ultra-Reliable Low Latency Communications

include cognitive radio networks [58, 59], heterogeneous networks [60], Device-to-Device (D2D) networks [61, 62], UAV-aided networks [63, 64], IoT networks [65, 66] while the effectiveness of FJ schemes differs from each other in various network environments.

However, there are few papers that summarize the research issues in FJ schemes, which are potentially feasible for URLLC. To the best of our knowledge, only two recent papers present overviews of FJ schemes. In particular, the authors in [67] gave a brief introduction to FJ schemes from the view of information theory while the authors in [68] introduced the integration of FJ methods with three techniques: multiple-input multiple-output (MIMO), game theory, and energy harvesting. There is no comprehensive survey on FJ schemes for URLLC, especially on the integration with other wireless techniques and discussion on the applications of FJ schemes.

Therefore, this paper aims to present a comprehensive introduction to FJ schemes for URLLC. The main objective of this paper is to introduce the FJ methods and to introduce the approaches to overcome the shortcomings of FJ schemes according to the analysis of the FJ methods. The approaches include the integration of FJ with other emerging communication technologies and the diverse applications of FJ schemes as shown in Figure 1.

Our main contributions are summarized as follows:

- We introduce the theoretical fundamentals of friendly-jamming schemes. To be specific, performance metrics for evaluating the information security are presented, and a general wireless network with applications of friendly-jamming schemes is illustrated and analyzed. In addition, the challenges of applying FJ schemes in URLLC of 5G and beyond networks are illustrated.

- We review the integration of FJ schemes with various cutting-edge communication technologies, including beamforming, MIMO, full duplex, relay selection, network coding, and game theory. The integration of FJ schemes with these emerging communication technologies is helpful for improving the secrecy efficiency and effectiveness of FJ schemes.

- We also summarize the integration of FJ schemes with various network architectures, including cognitive radio networks, heterogeneous networks, IoTs, D2D networks, and UAV-aided networks. Owing to the characteristics of these networks, FJ signals shall be sufficiently utilized and the impact of FJ methods on legitimate transmission shall be mitigated. We also provide a case study to demonstrate the effectiveness of FJ scheme and outline the future directions in FJ schemes.

The rest of this paper is organized as follows: Section 2 gives a brief introduction to FJ schemes. Section 3 introduces the integration of FJ with other communication techniques. Section 4 then discusses the integration of FJ with different types of network architectures. A case study of FJ scheme is provided in Section 5. Section 6 outline future research directions. Section 7 concludes this paper. The acronyms used in this paper are summarized in Table 1.

2. Overview of friendly-jamming techniques

In this section, we briefly introduce the security analysis of FJ schemes and the challenges of applying FJ schemes in URLLC of 5G and beyond networks.

2.1. Performance metrics

We first introduce the commonly adopted security performance metrics in wireless networks.

2.1.1. Secrecy Capacity

Secrecy capacity is a primary security performance metric, which describes the maximal achievable secure transmission rate. The secrecy capacity is generally considered as the upper bound of the transmission rate which satisfies the requirements of both reliability and secrecy. This metric is determined by the differentiation between the Shannon capacity of the legitimate link and Shannon capacity of the eavesdropping link [69, 70, 71].

Mathematically, the secrecy capacity C_s is derived by the following expression,

$$C_s \triangleq [C_r - C_e]^+ , \tag{1}$$

where $C_r = \log_2(1+\xi_r)$ is the Shannon capacity of legitimate link and $C_e = \log_2(1+\xi_e)$ is the Shannon capacity of eavesdropping link, ξ_r represents the SINR at the legitimate receiver, and ξ_e represents the SINR at the eavesdropper.

In realistic network environment, the value of ξ_r is determined by the information-decoding sensitivity at the legitimate receiver, and the value of ξ_e is determined by the information decoding sensitivity at the eavesdropper.

2.1.2. SOP and COP

Obtaining the instantaneous SINR of eavesdropper ξ_e is difficult because passive eavesdroppers which seldom emit signals are hardly been detected. Therefore, the security metric secrecy outage probability (SOP) is employed to analyze the eavesdropping activities [72, 73]. The SOP is the probability that secrecy outage (SO) event occurs when the received SINR at the eavesdropper is above a given threshold. To derive the SOP, only statistical knowledge of ξ_e is required and the instantaneous knowledge of ξ_e is not necessary. Mathematically, the SOP can be expressed by the following expression,

$$P_{SO} = \Pr\left(\xi_e \geq \xi_{th}^e\right) = 1 - F_{\xi_e}\left(\xi_{th}^e\right). \tag{2}$$

where $F(\cdot)$ represents the cumulative distribution function.

Similarly, the metric connection outage probability (COP) is used to describe the probability that a connection outage (CO) event occurs when the SINR at the legitimate receiver cannot reach the given minimal threshold value. The expression of COP is given by

$$P_{CO} = \Pr\left(\xi_r < \xi_{th}\right) = F_{\xi_r}\left(\gamma_{th}\right). \tag{3}$$

The SOP is considered to be the probability that the transmission fails to reach the perfect secrecy while the COP is considered to be the probability of an unsuccessful transmission. The goal of deploying friendly jammers in wireless networks is to minimize the SOP while maintaining the COP low enough, i.e., to improve the secrecy performance and meanwhile guaranteeing the reliability of wireless communication.

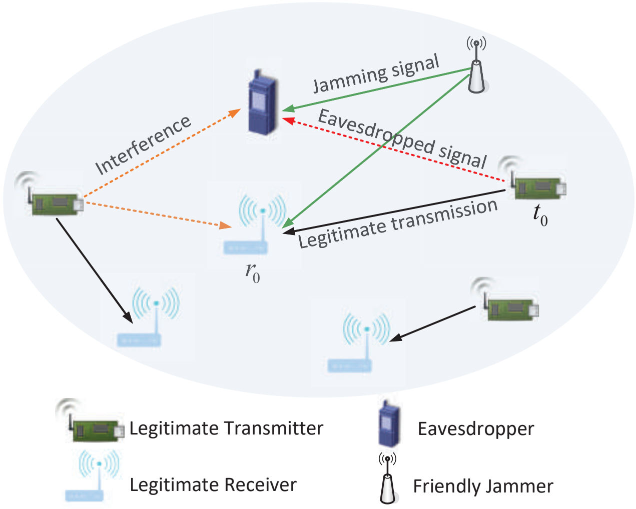


Figure 2: Network model.

2.2. Friendly-jamming schemes

The aforementioned security performance metrics have been extensively adopted in recent studies. From the illustration of performance metrics, we can find the information security of wireless networks is heavily determined by the SINR of the eavesdropper and that of the legitimate receiver. Therefore, we analyze the effectiveness of the FJ scheme according to the SINR of the eavesdropper and that of the legitimate receiver.

2.2.1. Security analysis without FJ schemes

We consider a general wireless network as shown in Figure 2. In this network, multiple legitimate transmitters transmit confidential information to the corresponding legitimate receivers, and an eavesdropper in this network attempts to wiretap the transmitted legitimate information. The eavesdropper is assumed to be passive and does not transmit signals to avoid being discovered by legitimate users. If the eavesdropper generates signals, the appearance eavesdropper can be easily discovered and be located with multiple technologies. The number of legitimate transmitters is M and legitimate transmitters are denoted by by $\{t_0, t_1, \ldots, t_{M-1}\}$. We assume all the devices in this network are equipped with the omnidirectional antenna in this section.

Without loss of generality, we focus on the transmission link between legitimate transmitter t_0 and the corresponding legitimate receiver r_0 as shown in Figure 2. The legitimate information signal emitted by transmitter t_0 may potentially be wiretapped by an eavesdropper E. Based on the statistical channel state information, the SINR at the eavesdropper is given by [72, 28] as follows,

$$\xi_e = \frac{P_T h_{e0}^2 d_{e0}^{-\alpha}}{\sigma^2 + I_{te}}, \tag{4}$$

where P_T is the transmitting power of legitimate transmitters, d_{e0} is the Euclidean distance between eavesdropper E and transmitter t_0, h_{e0} is the fading coefficients of the channel between eavesdropper E and legitimate transmitter t_0, $I_{te} = \sum_{m=1}^{M-1} P_T h_{em}^2 d_{em}^{-\alpha}$ represents the cumulative interference from legitimate transmitters to eavesdropper E, h_{em} is the fading coefficients of the channel between eavesdropper E and legitimate transmitter t_m, d_{em} is the Euclidean distance between eavesdropper E and transmitter t_m, α denotes the path loss factor, σ^2 represent the additive white Gaussian noise.

The SINR at the desired legitimate receiver r_0 can be derived by

$$\xi_{r_0} = \frac{P_T h_{r0}^2 d_{r0}^{-\alpha}}{\sigma^2 + I_{tr}}, \tag{5}$$

where h_{r0} is the fading coefficients of the channel between legitimate receiver r_0 and legitimate transmitter t_0, d_{r0} is the Euclidean distance between receiver r_0 and legitimate transmitter t_0, $I_{tr} = \sum_{m=1}^{M-1} P_T h_{rn}^2 d_{rn}^{-\alpha}$ represents the cumulative interference from legitimate transmitters to legitimate receiver r_0, h_{rm} is the fading coefficients of the channel between legitimate receiver r_0 and legitimate transmitter t_m, d_{rm} is the Euclidean distance between receiver r_0 and legitimate transmitter t_m.

2.2.2. Security analysis with FJ scheme

To protect the security of legitimate communications in this network, we introduce friendly jammers to emit jamming signals. The jamming signals confound the eavesdropper and prevent the eavesdropper from successfully decoding the legitimate messages. The number of friendly jammers is N, and the friendly jammers are denoted by $\{ j_1, j_2, \cdots, j_N\}$.

After deploying FJ schemes in wireless networks, the SINR at the eavesdropper can be expressed by the following equation [65]

$$\xi_e^{'} = \frac{P_T h_{e0}^2 d_{e0}^{-\alpha}}{\sigma^2 + I_{te} + I_{je}}, \tag{6}$$

where P_J denotes the transmitting power of friendly jammers, $I_{je} = \sum_{n=1}^{N} P_J h_{en}^2 d_{en}^{-\alpha}$ is the cumulative interference from friendly jammers to the eavesdropper E, h_{en} is the fading coefficients of the channel between the eavesdropper E and the friendly jammer j_N, d_{en} is the Euclidean distance between the eavesdropper E and the friendly jammer j_N.

The SINR of desired legitimate receiver r_0 becomes

$$\xi_{r_0}^{'} = \frac{P_T h_{r0}^2 d_{r0}^{-\alpha}}{\sigma^2 + I_{tr} + I_{jr}}, \tag{7}$$

where $I_{jr} = \sum_{n=1}^{N} P_J h_{rn}^2 d_{rn}^{-\alpha}$ is the cumulative interference from friendly jammers to receiver r_0, h_{rn} is the fading coefficients of the channel between legitimate receiver r_0 and friendly jammer j_N, d_{rn} is the Euclidean distance between the receiver r_0 and the friendly jammer j_N.

2.3. Challenges of applying friendly jamming

Although FJ schemes are effective in protecting the security of wireless information transmission, there are several challenges that remain to be solved before adopting FJ schemes in URLLC of 5G and beyond networks.

First, interference management is important for FJ methods. From the security analysis on FJ schemes in Section 2.2.2, we find that FJ schemes introduce the interference to both the eavesdropper and the legitimate receiver. To guarantee the reliability of legitimate communication, the impact of FJ noises on legitimate communication should be minimized. The FJ noises need to be concentrated on the eavesdropper based on various techniques and strategies.

In addition, deploying FJ schemes needs to be pervasive for resource-limited wireless networks. Applying friendly jamming at low cost should be available and the power of FJ signals should be limited. The FJ devices should be feasible for the most common communication protocols such as Wi-Fi (IEEE 802.11).

Furthermore, the effectiveness of the FJ method is challenging in a dynamic environment when the impacts of multi-path effects, attenuation, and fast channel fading are considered [74]. FJ schemes that satisfy the high mobility requirement in URLLC of 5G and beyond networks are highly expected.

3. Integration of friendly jamming with other techniques

Friendly jamming is a promising approach to protect legitimate communication from being wiretapped. Nevertheless, FJ signals also have interference on legitimate receivers [75]. In order to satisfy the high-quality communication of URLLC, the integration of multiple communication techniques with FJ schemes is investigated.

3.1. Friendly Jamming with Beamforming

Beamforming is a technique that concentrates transmitting power on the desired direction. This technique can be used to concentrate FJ signals to eavesdroppers rather than to legitimate receivers, as shown in Figure 3. Hence, this technique is helpful to reduce the interference from FJ schemes on legitimate communications.

Several recent researches focused on designing the proper beamforming strategies for FJ schemes. In [82], the authors proposed a semi-adaptive beamforming strategy for FJ schemes in Multiple-Input Single-Output (MISO) channels. When the communication rate is a fixed value, this

Table 2: Friendly Jamming with Beamforming

References	Network Environment	Beamforming Deployment	Jamming Deployment	CSI of eavesdropper	Design Objectives
[76]	MISO NOMA CR network with SWIPT	Primary BS and cognitive BS	Primary BS and cognitive BS	Imperfect	Improving the security of the primary network
[69]	MISOME wiretap channel	Transmitter	Transmitter	Statistical	Maximizing the secrecy rate under an SOP and power constraint
[77]	Multi-cast multiuser directional system	BS	BS	Perfect	Achieving a secure transmission
[78]	MISO CR network with SWIPT	Cognitive BS	Cognitive BS	Imperfect	Guaranteing secure communication and energy harvesting
[79]	Underlay CR MISO system	Secondary transmitter	Secondary transmitter	Statistical	Improving the secrecy rate of secondary system
[80]	MISOME wiretap channel	Transmitter	Transmitter	Statistical	Maximizing the secrecy rate under the SOP constraint
[81]	MISO wiretap channel	Transmitter	Transmitter	Statistical	Maximizing the ergodic secrecy capacity
[60]	Two-tier 5G heterogeneous network	Marco BS	Marco BS	Imperfect	Optimizing the secrecy rate of a marco user in a macrocell
[82]	FJ aided MISO system	Transmitter	Transmitter	Statistical	Maximizing the secrecy throughput under the requirement of reliable and secure transmission
[83]	FJ aided MISO system	Transmitter and Friendly jammer	Friendly jammer	No or Perfect	Solving the robust QoS based secure transmission design problem
[84]	FJ aided MISO system	Transmitter and Friendly jammer	Friendly jammer	No	Maximizing the power of FJ signals under the constraint of reliability at the legitimate receiver
[85]	Large scale spectrum sharing network	Secondary transmitter	Secondary transmitter	Perfect	Characterizing the impact of beamforming and FJ on network
[86]	Cellular network with hierarchical security structure	BS	BS	Perfect	Maximizing the higher level information security performance under the constraint low level information secrecy rate
[87]	Cooperative relay network	Relay node	Friendly jammer	Statistical or Perfect	Improving the secrecy rate by allocating the power optimally

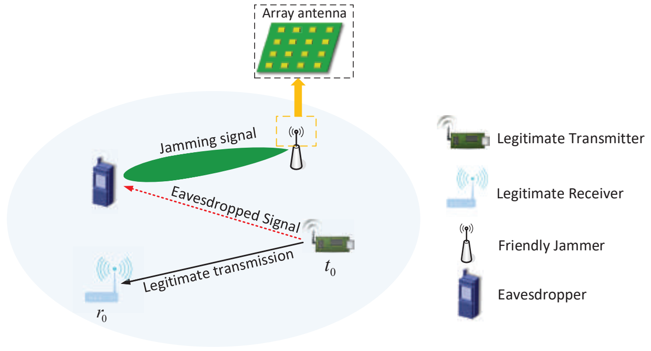


Figure 3: Integration of friendly jamming with beamforming techniques.

strategy is helpful in maximizing the secrecy rate. The authors in [60] studied the beamforming enabled FJ schemes in a 5G HetNet and designed a secrecy transmission algorithm for optimizing the secrecy rate. In research [85], a beamforming enabled FJ scheme is proposed for large scale Cognitive Radio Networks (CRNs). In this scheme, the secondary transmitters emit directional FJ signals to eavesdroppers to enhance the information security of the CRN. Similarly, a beamforming-enabled FJ scheme for CRNs is studied in [79], where the secondary transmitters emit directional FJ signals to improve the security performance of the secondary network.

In order to allocate the total transmitting power between the FJ signal and the information signal, the research [69] proposed an optimal power allocation strategy for their beamforming enabled FJ scheme. In [80], the authors investigated a beamforming enabled FJ scheme in the MISO channel. In this research, an optimal power allocation strategy is designed according to the imperfect CSI of the eavesdropper.

In the above researches, the perfect or imperfect CSI of eavesdroppers is assumed to be known. However, in a realistic communication environment, even knowing the statistical channel information of eavesdroppers is difficult since the eavesdroppers are usually passive and the locations of eavesdroppers are unknown. In [83], the authors investigated the scenario that CSI of eavesdroppers is unavailable. In this scenario, semi-definite relaxation (SDR) approach is required to solve the optimal power allocation problem. The research [76] proposed a beamforming enabled FJ scheme for MISO-NOMA based CRNs, where the secondary BS emits the directional FJ signals to assist the primary BS for maximizing the secrecy rate of the primary network. When the scenario that CSI of eavesdroppers is imperfect is considered, an SDR algorithm is proposed for minimizing the transmission power. In [78], the beamforming enabled FJ scheme and power splitting design in MISO based CRNs are investigated. In this research, the SDR is also used for solving the optimization problem.

Table 2 presents a summary corresponding to studies of integrating FJ schemes with beamforming techniques.

3.2. Friendly Jamming with MIMO

MIMO is a technique to improve the spectral and energy efficiencies by exploiting the benefits of multiple antennas. In PLS, MIMO is an effective technique to improve secrecy performance with the extra spatial degrees of freedom.

Consider a wireless network model as shown in Figure 2, where each of legitimate transmitters and receivers is equipped with q antennas. For simplicity, each eavesdropper is also equipped with q antennas while each friendly jammer is equipped with a single antenna. In this new scenario, the received signal of the legitimate receiver r_0 is shown by the following expression,

$$\mathbf{y}_{r_0}=\sqrt{P_T}\mathbf{H}_{qq0}\mathbf{x}_0+\sum_{n=1}^{N_T-1}\sqrt{P_T}\mathbf{H}_{qqn}\mathbf{x}_n+\sum_{m=1}^{N_J}\sqrt{P_J}\mathbf{H}_{qm}\mathbf{z}_m+\mathbf{n}_0, \tag{8}$$

where $\mathbf{H}_{qq0}$ denotes the $q \times q$ channel matrix between the legitimate transmitter t_0 and legitimate receiver r_0, $\mathbf{H}_{qqn}$ denotes a $q \times q$ channel matrix between the nth legitimate transmitter and legitimate receiver r_0, $\mathbf{H}_{qm}$ denotes the $q \times 1$ channel vector between the m-th jammer and the legitimate receiver r_0, $\mathbf{x}_n$ is the $q \times q$ information signal matrix sent by the legitimate transmitter t_n with unit power, $\mathbf{z}_m$ is the $q \times 1$ information signal transmitted by the m-th FJ jammer, $\mathbf{n}_0$ is the $q \times 1$ information signal vector with unit power vector of additive Gaussian noise.

With a similar approach, we derive the received signal expression of eavesdropper E in the following,

$$\mathbf{y}_e=\sqrt{P_T}\mathbf{H}^e_{qq0}\mathbf{x}^e_0+\sum_{n=1}^{N_T-1}\sqrt{P_T}\mathbf{H}^e_{qqn}\mathbf{x}^e_n+\sum_{m=1}^{N_J}\sqrt{P_J}\mathbf{H}^e_{qm}\mathbf{z}^e_m+\mathbf{n}_e, \tag{9}$$

where $\mathbf{H}^e_{qq0}$ denotes the $q \times q$ channel matrix between the legitimate transmitter t_0 and eavesdropper E, $\mathbf{H}^e_{qqn}$ denotes the $q \times q$ channel matrix between the n-th legitimate transmitter and eavesdropper E, $\mathbf{H}^e_{qm}$ denotes the $q \times 1$ channel vector between the m-th friendly jammer and and eavesdropper E, $\mathbf{x}^e_n$ is the $q \times q$ information signal matrix sent by legitimate transmitter t_n with unit power, $\mathbf{z}^e_m$ is the $q \times 1$ information signal sent by the mth friendly jammer with unit power, $\mathbf{n}_e$ is the $q \times 1$ information signal vector with unit power vector of additive Gaussian noise.

For improving the secrecy rate of a MIMO untrusted relay network, in which the legitimate receivers also serve as friendly jammers, the authors of [88] designed an alternating iterative optimization algorithm. This optimization algorithm is constrained by total source, FJ power, and relaying power together. Meanwhile, the authors in [36] studied the secrecy rate in a Gaussian MIMO system considering the help of a friendly jammer. In this research, the authors also analyzed the impact of eavesdropper's CSI on secrecy performance.

Another research investigates the impact of eavesdropper's CSI on secrecy performance of MIMO system is [89]. This research investigated maximizing the secrecy rate of MIMO untrusted two-way relay system under the cases that perfect and imperfect CSI is known. In this article, an iterative algorithm based on the constrained concave-convex procedure is designed when perfect CSI is known, and a weighted minimum mean square error based method is proposed when imperfect CSI is known. In [90], the authors analyzed the impact of eavesdroppers' locations on the secrecy performance in the MIMO Rician channel. Moreover, [91] studied an FD MIMO relay network, where the FD friendly jammer is charged purely from RF energy-harvesting. In this research, a sufficient condition of self-energy recycling is derived to guarantee enough power supply at friendly jammers.

3.3. Friendly Jamming with Full Duplex

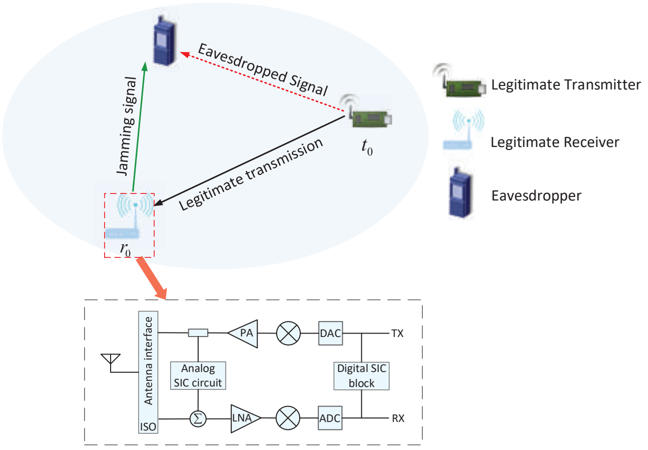


Figure 4: Integration of friendly jamming with full duplex technique. ISO:isolation; PA: power amplifier; SIC: self- interference cancellation; LNA: low-noise amplifier; ADC: analog-to-digital converter; DAC: digital-to-analog converter.

Comparing with HD communications, FD communications are feasible for 5G due to the high spectral efficiency.

Table 3: Friendly Jamming with Full duplex

References	Network Environment	Full Duplex Deployment	Jamming Deployment	CSI of eavesdropper	Objectives
[28]	Two-tier heterogeneous decentralized wireless network	Receiver in the overlaid tier	Receiver in the overlaid tier	Statistical	Maximizing the network-wide secrecy throughput
[50]	Wireless communication system	Transmitter	Transmitter and receiver	Perfect	Maximizing the secrecy rate and the SOP
[92]	Energy harvesting wireless network	Friendly jammer	Friendly jammer	No	Maximizing the SOP of wireless communications
[91]	Full-duplex MIMO relay channel	Relay and friendly jammer	Friendly jammer	No	Securing the legitimate transmissions
[93]	Full-duplex relaying system	Relay	Transmitter and relay	Imperfect	Maximizing the ergodic achievable secrecy rate
[94]	Multihop wireless network	Transmitter, receiver and relay	Transmitter, receiver and relay	No	Maximizing the secure connection probability
[95]	Full-duplex jamming SWIPT system	Receiver	Receiver	No	Maximizing the COP, SOP, reliable secure probability and secrecy throughput

In Figure 4, we show a scenario that FD technology is integrated with the FJ scheme. The legitimate receiver works in FD mode emit FJ signals to confound the eavesdropper.

Several studies have recently investigated the integration of FD technology with FJ schemes. In [28], the authors proposed the FD enabled FJ scheme for protecting the confidential information in a two-tier decentralized communication network. In the overlaid tier of this network, the legitimate receiver in FD mode receives information signals and emits FJ signals simultaneously. The research [50] proposed a two-phase FD-enabled FJ scheme to maximize the secrecy rate of the communication system. In this scheme, after two phases' transmission and signal processing, FJ signals at the legitimate receiver are cancelled but FJ signals at the eavesdropper are still effective.

Some studies concentrate on the integration of SWIPT with FD enabled FJ schemes. The work [95] investigates an FD and SWIPT system, in which the legitimate receiver also plays the role of energy-limited friendly jammer. The legitimate receiver receives the information signals as well as the wireless power from the legitimate transmitter, and then radiate FJ signals in FD mode. In the FD enabled FJ scheme proposed in [92], the legitimate receiver is also assumed to accumulate the energy form the legitimate transmitter first and then emit FJ signals to the eavesdropper. In [91], the FD friendly jammer is assumed to be self-energy recycled, which harvests energy from the ambient RF transmissions.

The integration of relaying system with FD enabled FJ schemes has been investigated in a substantial body of researches. In [93], the authors investigated an FD-enabled FJ scheme in a relaying system. In this system, the FD relay node radiates FJ signals to the eavesdropper. The authors [94] proposed an FJ scheme in a multihop relaying system. In this scheme, both legitimate receiver and relay nodes emit FJ signals to the colluding eavesdroppers.

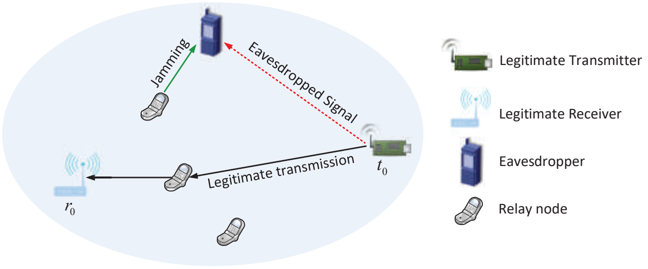


Figure 5: Integration of friendly jamming with relay selection technique.

A summary of the literature on integrating FJ schemes with full duplex technique is given in Table 3.

3.4. Friendly Jamming with Relay Selection

Relay selection is an effective method to improve energy efficiency by selecting one or multiple relays from a group of relays to forward information [51]. It may be beneficial to let the remaining relays to generate FJ signals interfere with eavesdroppers. Figure 5 presents a scenario that one relay device serves as a friendly jammer to emit FJ signals to interfere with the eavesdropper.

Several recent studies such as [96, 97, 52, 98] take advantage of relays to generate FJ signals to confound eavesdroppers. In [96], Choi and Lee studied an FJ technique to minimize the SOP of an amplify-and-forward relay network with multiple relays. In this network, both legitimate transmitters and legitimate receivers transmit jamming signals in different transmission phases by jointly allocate the power and select the relays. In [97], an FJ-aided two-way opportunistic relay selection scheme is proposed to enhance the communication security of the legitimate transmitters pair. The legitimate transmitters are relayed by multiple two-way relays with a decode-and-forward protocol. Their proposed scheme outperforms traditional direct transmission schemes according to the performance of the SOP and intercept probability. In [52], the authors proposed a secure buffer-aided relay selection scheme to improve the performance of SOP and end-to-end packet delay by allowing a subset of legitimate transmitters, relay devices, and legitimate receivers to transmit FJ signals cooperatively.

Jia *et al.* proposed an FJ aided cooperative relay selection scheme, where one cognitive relay is selected to forward the confidential information signal and the rest of the relays generate FJ signals to confound eavesdroppers [98]. In this research, the closed-form expression of SOP for their proposed scheme is derived with consideration of various system parameters. In an energy-harvesting cooperative communication system, Mabrouk *et al.* investigated an FJ technique to prevent the confidential data from being intercepted by untrusted relays [51]. In this research, the jamming signals are emitted by the legitimate transmitters and a relay selection scheme considering the battery power is proposed to reduce the power consumption.

3.5. Friendly Jamming with Physical Network Coding and Game Theory

A possible solution to avoid the interference of FJ schemes at legitimate transmission is to combine the jamming signal and information with physical network coding, and then extract the information signal from the mixed signals at the legitimate receiver. There are several attempts in integrating FJ method with physical network coding. In [99], random binary messages are integrated into the FJ signals by applying the physical layer network coding method while the legitimate receiver can obtain the message from mixed signals with the FJ seed from the communication protocol. Moreover, the work of [100] proposed an explicit and low-complexity polar coding scheme where the FJ strategies are implemented with polar codes. In [101], an FJ-aided message authentication codes (MACs) is developed to enhance the security of computation and information. In this approach, the FJ signals are used to prevent the eavesdropper from obtaining the key. Furthermore, the authors in [102] proposed an FJ-aided physical layer phase challenge-response authentication scheme to enhance the security of orthogonal frequency division multiplexing transmission. In this scheme, the FJ signals are introduced to the phase-modulated key to avoid potential key recovery behaviour.

Game theory is helpful for friendly jammers to choose the proper jamming opportunity to maximize energy efficiency under the constraints of transmission secrecy. In [103], Lu *et al.* investigated a scenario that the hybrid BS in a cellular network serves as both a power source and a friendly jammer for the Device-to-device (D2D) transmitter. In this scenario, an energy trading-based Stackelberg game is proposed to allocate the power for D2D devices and the BS optimally. Meanwhile, the work of [104] investigated a MIMO wiretap interference network, where FJ signals and information signals are transmitted jointly. Besides, a non-convex game approach is proposed to enhance the information security of each transmission link. Furthermore, the authors in [105] studied an FJ-aided CR network. In this research, the Stackelberg game is investigated to model the scenario, where the primary transmitter attempts to maximize its secrecy rate while the secondary transmitter attempts to maximize its energy efficiency. In [106], friendly jammers that are assumed to be selfishly are desired to obtain profits from generating jamming signals. In this research, a Bertrand game is introduced to help to offer the optimal pricing schemes for friendly jammers. In [107], the authors introduced the concept of social tie to present the jammer's willingness to contribute to FJ. In this work, a social tie-based FJ game is investigated based on a pure Nash equilibrium.

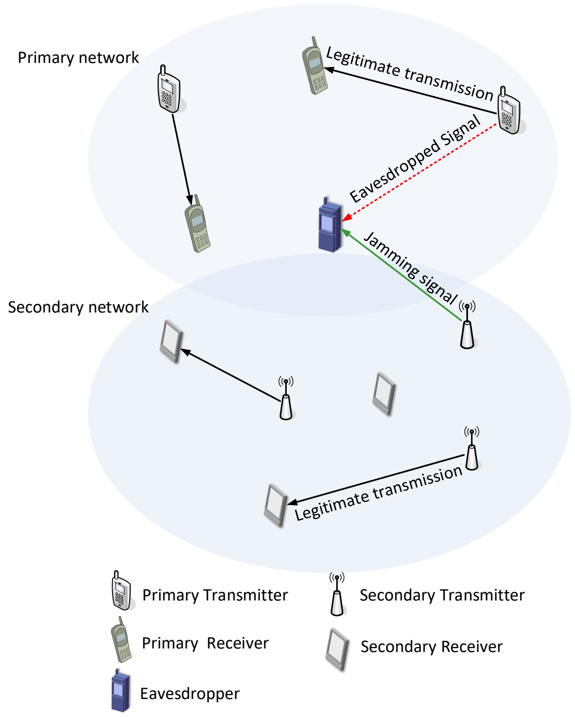


Figure 6: FJ scheme in Cognitive Radio Network.

4. Integration of Friendly Jamming with Various Network Architectures

FJ schemes are promising to protect the security of existing wireless networks without extra security countermeasures at either infrastructure or wireless devices. This section discusses the integration of FJ schemes with diverse wireless network architectures.

4.1. Friendly Jamming in Cognitive Radio Networks

CRN has widely been recognized as a dynamic spectrum access network layout to make sufficient usage of radio spectrum resources. Figure 6 shows a scenario that a secondary transmitter serves as a friendly jammer to improve the transmission security of primary users in a CRNs [85, 79, 37, 59]. In this case, FJ signals emitted by the desired secondary transmitter degrade the SNR level of the eavesdropper. On the other hand, compared with conventional wireless communication systems, the information security of CR networks is more challenging due to the strict requirement for QoS of the primary network, the overall interference, and the extra reliability of SUs to security threats. Therefore, a number of recent studies focused on investigating the application of FJ schemes in CRNs [76, 78, 79, 85, 87, 37, 59, 108, 109, 105, 98, 41], which have been reviewed individually in Section 3.

4.2. Friendly Jamming in Heterogeneous Networks

Heterogeneous network (HetNet) is a kind of modular, flexible, and extensible network architecture. On one hand, this architecture offers a platform to support various emerging wireless technologies, such as MIMO and NOMA; on the other hand, the rich diversity of communication devices and applications leads to the risks of communication security. In order to make full usage of this architecture to protect the legitimate transmission, friendly jammers have been extensively investigated in literature.

In particular, the authors in [28] proposed the FD FJ schemes in a two-tier decentralized HetNet. In the underlying tier of this network, the legitimate transmitter radiates information signals to the HD legitimate receiver. While in the overlaid tier, the legitimate transmitter sends confidential signals to the FD legitimate receiver, which radiates FJ signals and receives the desired signal simultaneously. Moreover, the optimal deployment density of the overlaid tier was investigated to improve the network-wide secrecy throughput under the constraints of communication performance in the underlaid tier. Moreover, in [60], FJ schemes are investigated in a two-tier 5G HetNet, which consists of macrocell tier and local cell tier. In this literature, three secrecy transmission algorithms employing beamforming, power allocation, and joint optimization methods are designed to fulfill different security requirements. Moreover, the secrecy transmission algorithms were proposed to enhance the information security with consideration of imperfect CSI and collusive eavesdroppers.

Some researches utilized the modified Poisson hole process to model the locations of the active friendly jammers. In [110], the authors proposed a friendly jammer selection scheme to protect the confidential downlink transmission of HetNets from being wiretapped by eavesdroppers. In their scheme, the friendly jammers are selected to be active if their interference on legitimate communication is lower than a threshold. Furthermore, they investigated a scenario in which both friendly jammer selection and FD receivers are used to protect the downlink transmission of HetNets in [111]. Moreover, the FD receivers generate jamming signals to interfere with eavesdroppers when the friendly jammers in the guard zones are silent.

The authors in [86] proposed an FJ-aided optimal beamforming scheme to guarantee layered information security based on a hierarchical security structure. They designed a convex approximation-based algorithm to solve the nonconvexity of the optimal beamforming problem. Moreover, they proposed a low complexity zero-forcing beamforming scheme to improve computational efficiency. Furthermore, [112] investigated the performance of the FJ method to protect the communication security in the heterogeneous the D2D underlaying cellular networks. This work proposed both a non-coordinated jamming strategy and a coordinated jamming strategy to reduce the compromised secrecy region. Meanwhile, the security problem of D2D link instead of the cellular link is considered due to the lack of high layer security strategies of the D2D link.

4.3. Friendly Jamming in D2D Communications

The merit of Device-to-device (D2D) communication is to reuse the spectrum resources between the devices located in short distances without the network infrastructure. Compared with the conventional infrastructure-based networks, D2D communications can enhance radio spectrum reuse and reduce the delay [113].

Aiming to archive the maximal secrecy throughput of a wireless D2D network under the constraint of SOP, [61] proposed a switched FD/HD mode adaptive FJ transmission scheme with low complexity. In [57], Chu *et al.* investigated a scenario that a wireless D2D communication system that was wirelessly-powered by hybrid BSs in a cellular network, in which BSs also generate FJ signals to confuse the eavesdropper. An interaction between BS and D2D users can be modeled by two Stackelberg games depending on energy trading or without energy trading. A similar network environment was investigated in [103], which presented a Stackelberg game based energy trading scheme with consideration of the quadratic energy cost model. The authors also derived the closed-form Stackelberg equilibria of the formulated games through analyzing the social welfare optimization problem.

Wang *et al.* investigated a D2D communication system with the existence of multiple friendly jammers and eavesdroppers in [114], in which, both the optimal friendly jammer selection and the transmitting power allocation are investigated to protect the security of D2D links. The optimization problem is solved by their proposed heuristic genetic algorithm. Moreover, in [115], Wang *et al.* focused on the security of clustered D2D communications underlay in cellular networks. To protect the communication security of clustered D2D users, the authors proposed an optimization scheme for relay and friendly jammer selection. A Dinkelbach-type algorithm based fractional programming method is designed to solve the optimization problem.

D2D Communication usually coexist with other types of networks. In [116], the authors studied a scenario of

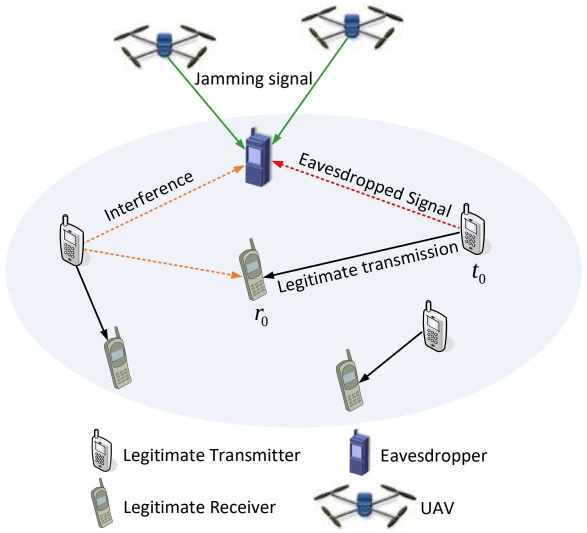


Figure 7: Friendly Jamming in UAV-aided Networks.

D2D link underlying a cellular network, where an eavesdropper attempts to eavesdrop the confidential signal. In this research, the D2D users are considered to serve as friendly jammers and a power allocation scheme is proposed to improve the secrecy performance. Furthermore, the authors in [117] introduced a UAV-aided D2D communication system, where the D2D receivers working in FD mode generate FJ signals to confuse the eavesdroppers. The results showed that the secure capacity of this system can be improved by adjusting the UAV's position and coverage.

4.4. Friendly Jamming in UAV-aided Networks

The Unmanned Aerial Vehicles (UAVs)-enabled mobile communication has drawn extensive attention due to the rapid growth of UAVs. In particular, UAVs can serve as friendly jammers to protect wireless communication. Figure 7 shows a scenario, in which UAVs serve as friendly jammers and emit FJ signals to confuse the eavesdropper.

The research [118] presented a UAV-aided communication system, in which a UAV acts as the air-to-ground friendly jammer whereas an eavesdropper tries to wiretap the legitimate confidential transmission. In this research, both the influence of UAV jamming power as well as its 3D spatial deployment on the secrecy performance have been analyzed. Meanwhile, the work of [63] considered a case that a mobile UAV served as a friendly jammer to opportunistically interfere with the eavesdropper to safeguard the information security of ground transmission channel. In this research, an iterative algorithm was proposed to jointly optimize the jamming power and UAV's trajectory with consideration of the constraints of finite transmit power and the UAV's mobility.

In some researches, a part of UAVs serve as legitimate user while the rest of UAVs serve as friendly jammer. In [119], the authors have investigated a UAV-ground communication system, where a UAV serves as BS and emits confidential information signals to legitimate ground users, and an idle UAV serves as a friendly jammer whereas multiple ground eavesdroppers with unknown position information attempt to eavesdrop the confidential signals. In this work, the authors designed an algorithm to optimize the flying trajectories and transmitting power for both UAVs to maximize secrecy performance. A similar network environment is considered in [120], where one UAV sends information signals to a legitimate ground user while the other UAVs generate FJ noise signals to confound a suspicious eavesdropper on the ground. This research essentially concentrates on optimizing the UAVs' trajectories to improve the secrecy performance of the communication system. Besides, the work [121] investigated a problem in which one mobile UAV tries to send confidential information signals to legitimate receivers on the ground while another cooperative UAV transmits the FJ signal. An algorithm is designed to jointly optimize the transmit power, the trajectory of the UAVs, and the scheduling sequence of legitimate receivers.

Some studies focused on the scenario that the UAVs act as eavesdropper. In [122], the authors considered a network in which a group of UAVs serves as friendly jammers while the other UAVs are eavesdroppers. The legitimate ground transmissions are protected by friendly UAVs from the eavesdropping attacks of UAV eavesdroppers. In this literature, the probability of line-of-sight channels for the air-to-ground links is approximated by their proposed piecewise function. Moreover, in [123], a UAV-aided MISO system in which multiple eavesdroppers exist is investigated. In this research, a UAV acts as a friendly jammer and safeguard the information security against multiple eavesdroppers when the CSI is imperfect. In particular, the authors investigated the beamforming of FJ signals, the optimal UAV placement strategy and the optimal power allocation between information signals, and FJ signals.

4.5. Friendly Jamming in IoT

IoT is vulnerable to the eavesdropping attacks due to the limitations of IoT devices in terms of the size, power, and computational capability [124]. The FJ schemes have been adopted to improve the security of IoT systems.

In particular, the authors in [65] investigated the security of IoT networks, where sensors, controllers, and actuators coexist. The security of downlink message transmission from a controller to an actuator can be enhanced by introducing FJ signals to confound the eavesdroppers. Meanwhile, in [125], an anti-eavesdropping scheme is applied to protect the information security of the wireless network of things. In this study, both the impact of various channel conditions and placement schemes of friendly jammers on secrecy performance are investigated. Moreover, in [126], Kim and Choi studied an IoT network where the transmitter generates FJ signal and information signal simultaneously under an optimal power allocation strategy without the receiver's CSI. In this network, cancellation

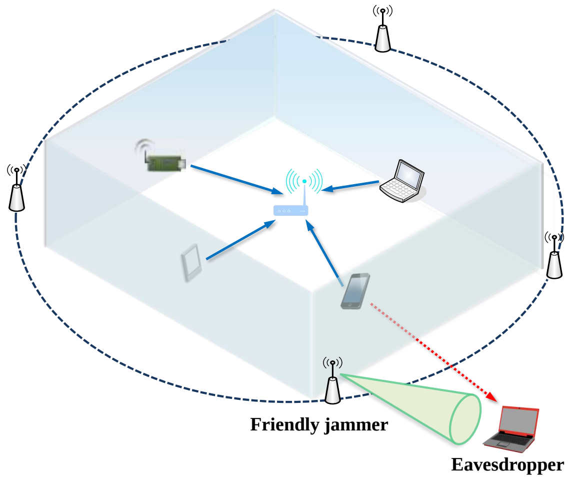


Figure 8: Beamforming-assisted FJ.

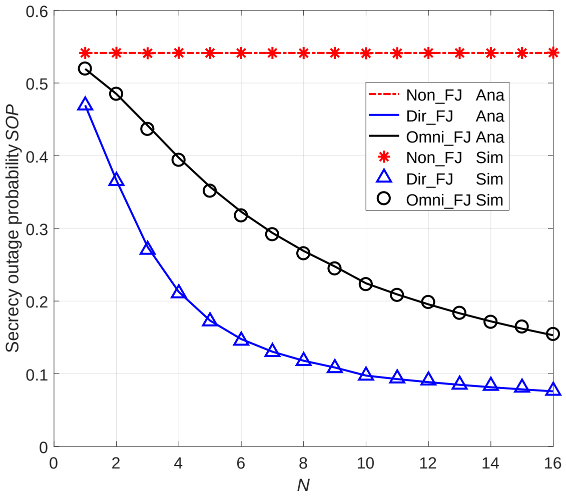


Figure 9: Number of friendly jammers N ranges from 1 to 16.

capability is required at the receiver to cancel the jamming interference from transmitter aided by shared secret keys.

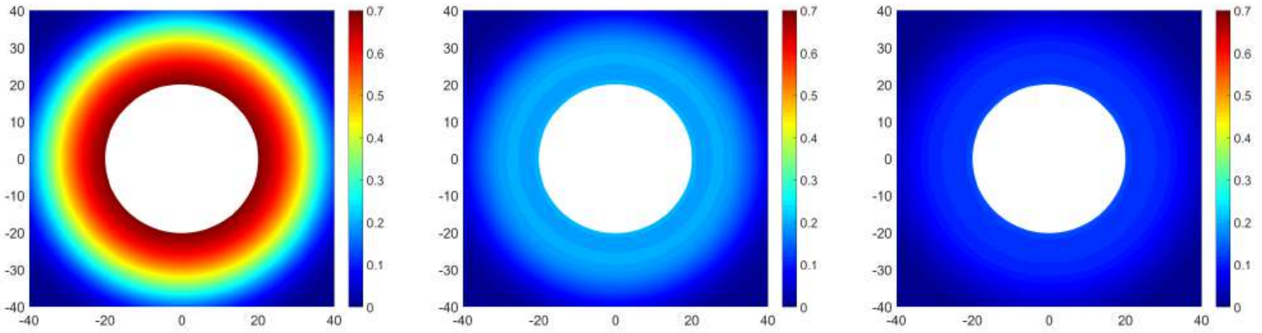
The research [127] investigated the security of a Cognitive IoT network, where sensors and actuators acting as secondary users and access the licensed spectrum bands provided by primary users. To enhance the security of this network, a number of secondary users harvest energy transmitted by the legitimate transmitter and generate FJ signals to confuse the eavesdroppers with the harvested energy. Moreover, in [128], the authors proposed a secrecy transmission protocol for the cognitive IoT network. In particular, two selection schemes are designed to select one SU to transmit secondary signals and select another one to transmit FJ signals against eavesdropping. In addition, the work of [129] focused on enhancing the security of industrial IoT with the UAV-enabled FJ scheme. In this work, UAV friendly jammers (each of which is equipped with a directional antenna) generate FJ signals to interfere with eavesdroppers outside of the factory.

5. Case study

In this section, we introduce a case study of applying beamforming-assisted FJ scheme to protect the communication security in a limited circular region [130]. As shown in Figure 8, legitimate users in the network communicate with each other in a limited region (such as factory, laboratory, hospital, etc.). Legitimate transmitters transmit confidential information to legitimate receivers within the transmission region. At the same time, an eavesdropper outside the communication region may eavesdrop the confidential signals due to the openness of wireless channels. The eavesdropper that is assumed to be passive does not transmit signals to avoid being discovered. Due to the absence of authenticated permission to enter this area, the eavesdropper cannot enter the communication region. We assume that legitimate transmissions are conducted inside the circular communication area with radius R. The locations of M legitimate transmitters are randomly distributed according to the homogeneous Poisson Point Process. The eavesdropper appears outside of the communication region. The distance between the eavesdropper and the boundary of the communication region is D. Each device except friendly jammers is assumed to be equipped with an omnidirectional antenna.

To protect the wireless transmission inside of the limited circular region, we deploy N friendly jammers at the boundary of the communication region to generate FJ signals. In this scheme, the beamforming technology is applied, because applying the directional antenna can concentrate the jamming signal on the potential eavesdropped area rather than the legitimate communication region. Therefore, we propose the Dir-FJ scheme where friendly jammers are equipped with the directional antenna. For comparison, we consider the Omni-FJ scheme where friendly jammers are equipped with the omnidirectional antenna. We also consider the Non-FJ scheme, in which no friendly jammer is deployed. In this case, we adopt the information security performance metric SOP introduced in Section 2.

We first present SOP results of three types of schemes: Dir-FJ scheme, Omni-FJ scheme, and Non-FJ scheme with the varied number of friendly jammers N, as shown in Figure 9. In this figure, the curves represent the analytical results and the dots represent the simulation results. The analytical results and simulation results match well, verifying the accuracy of the analytical result. As shown in Figure 9, deploying friendly jammers will lead to a significant decrease in the SOP of the network, especially when there are more than 2 friendly jammers deployed. For instance, when the number of friendly jammers $N = 6$, the SOP of Omni-FJ scheme is 0.2221 reduced (i.e., 40.96% reduction) compared to that of Non-FJ scheme, and the SOP of Dir-FJ scheme is 0.3937 reduced (i.e., 72.72% reduction) compared to that of Non-FJ scheme. On the other



(a) Eavesdropping area without FJ scheme. (b) Eavesdropping area with Omni-FJ scheme. (c) Eavesdropping area with Dir-FJ scheme.

Figure 10: Secrecy outage probability (SOP) distribution in the eavesdropping area.

hand, we find that deploying a large number of friendly jammers may also be unnecessary. When the number of friendly jammers N is larger than 8, increasing the number of friendly jammers will not lead to a significant decrease in the SOP. In the Dir-FJ scheme, the curve of SOP drops rapidly as long as we deploy a few friendly jammers.

From Eq.(4) shown in Section 2.2, we find that the distance D plays a critical role in the SINR of the eavesdropper, heavily affecting the SOP of the network. To demonstrate the effect of FJ schemes on the geometrical distribution of SOP according to the location of the eavesdropper, we provide experimental results shown in Figure 10. As shown in Figure 10, we demonstrate the 2D distribution of SOP in wireless networks for each location of the eavesdropper. We assume that the radius of the limited circular communication region R is 20. Meanwhile, the distance D between the eavesdropper and the boundary of the communication region varies from 0 to 20. The white empty area in the center of each subfigure in Figure 10 represents the protected circular legitimate communication region, where the eavesdropper cannot enter due to the lack of authenticated permission. Figure 10(a) illustrates the SOP distribution without deploying friendly jammers, the dark red area represents the most dangerous area that the legitimate information from transmitter t_0 is potentially wiretapped with high probability (around 70%), and the dark blue area represents the safest area that the legitimate information is potentially wiretapped with low probability (less than 10%). Figure 10(b) illustrates the SOP distribution of the network with Omni-FJ scheme. We find that the SOP at the majority surrounding area outside the legitimate communication region is around 25%. When the beamforming technology is applied on friendly jammers, as shown in Figure 10(c), the SOP at the majority area where the eavesdropper may appear is reduced to be around 10%.

6. Future Research Directions

In Section 3 and Section 4, we introduce the studies on the integration of FJ schemes with multiple communication technologies as well as the applications of FJ schemes in different types of wireless networks. However, there are still a number of research efforts expected in the future to overcome the drawbacks of FJ schemes while maximizing the advantages of them. As shown in Figure 11, we summarize the future directions in the following aspects.

6.1. Placement Strategies of Friendly Jammers

The integration of beamforming and FJ schemes is beneficial since the beamformed FJ signal will concentrate their power on the eavesdropper rather than at legitimate receivers. However, it is a prerequisite to obtain accurate CSI before applying beamforming FJ while it is challenging to obtain the CSI of eavesdroppers, especially for passive eavesdroppers who remain quiet. Therefore, it is still a challenge to deploy friendly jammers to minimize the interference at legitimate receivers while maximizing the interference at eavesdroppers when CSI at eavesdroppers is difficult to be obtained.

One of the potential solutions is designing the proper placement strategies of friendly jammers without accurate CSI of eavesdroppers. In particular, friendly jammers can be deployed in an area to directionally interfere the unsecured area where eavesdroppers may exist while there is no interference in other regions where legitimate communications take place. In this way, the security of legitimate communications will be significantly improved while the impact on normal communications will be mitigated. For example, some of the recent studies such as [130] propose to place directional friendly jammers in a circle where the legitimate communications occur within the circular area while the eavesdroppers are located outside the circular area. In this way, the impacts on legitimate communications are minimized while the eavesdroppers are interfered with.

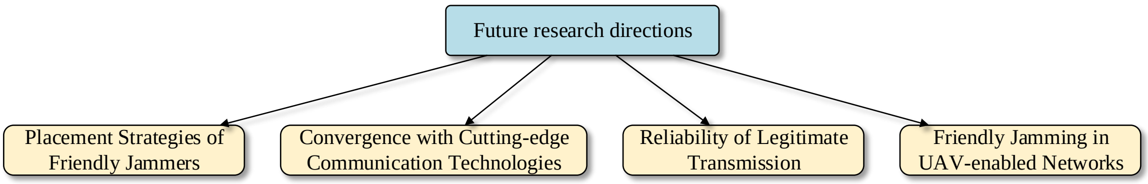

Future research directions
Placement Strategies of Friendly Jammers
Convergence with Cutting-edge Communication Technologies
Reliability of Legitimate Transmission
Friendly Jamming in UAV-enabled Networks

Figure 11: Future research directions for friendly jamming.

As a key technology for 5G or 6G wireless networks, MIMO is often integrated with beamforming technologies while it also has high CSI requirements on legitimate communications. However, in the dynamic network environments, the acquisition of CSI of legitimate devices and illegal devices is a nontrivial task. Therefore, the difficulty to obtain the CSI should be considered when designing the FJ schemes for MIMO systems. The potential solutions include designing secure and robust CSI feedback mechanisms and proposing proper placement strategies of friendly jammers.

6.2. Convergence with Cutting-edge Communication Technologies

An FJ scheme alone cannot work well for 6G networks. It is expected to integrate the FJ scheme with other cutting-edge communication technologies. In particular, SWIPT is a method that greatly improves the energy efficiency and the integration of SWIPT and FJ method makes full use of the FJ signals. However, low energy transfer efficiency results in a short energy harvest distance. According to the previous analysis, the legitimate transmitter is required to be placed close to friendly jammers to harvest the energy because the energy harvesting circuitry is not that sensitive as information decoding circuitry. In this case, the information signals are mixed with FJ signals. So, low energy harvest efficiency is still the key obstacle on the way to prevent SWIPT from being widely adopted in 6G networks [131]. In addition, the integration of network coding and SWIPT in FJ schemes may be a promising research direction that can be helpful in solving such problems. If legitimate receivers could decode the useful information from the mixed signal based on the prior knowledge while eavesdroppers could not, the secrecy performance is improved in this network environment.

In addition, full duplex technology enables the simultaneous receiving process and transmitting process to be integrated into one device. With this technology, the friendly jammers can be acted by relay devices or legitimate receivers in FJ schemes, consequently reducing the network complexity. However, when this technology is applied in FJ schemes, the self-interference mitigation method is important. Hardware imperfections such as non-linear distortions, phase noise, and non-ideal frequency responses of circuits will significantly degrade the performance of full duplex. Despite the rapid advances in the self-interference suppression approaches for FD devices, the current analog cancellation circuits are still too bulky for the Internet of Things [132]. The mitigation of unwanted interference of FJ signals on the relay devices or legitimate receivers should be further explored to avoid the received signals' quality decrement.

6.3. Reliability of Legitimate Transmission

CRN is a promising network technology to improve spectral efficiency. As introduced in Section 3, multiple techniques are studied to be integrated with FJ schemes under the CR network environment. In CR works, the secondary transmitters serve as friendly jammers to protect the security of the primary transmission. In this scenario, the reliability of primary transmission should be considered in security objectives, because the FJ schemes may degrade the performance of primary transmission. Therefore, when designing the FJ schemes for the CRN system, the constraints of security and reliability of primary transmission should be jointly taken into account. The global optimization with the joint considerations of security and reliability is still open to be explored.

When designing the effective FJ schemes in IoT, the limited battery, computation ability, and the low-cost hardware of most IoT devices should be considered. On one hand, applying FJ schemes in IoT requires no change of the original network, which is feasible to the characteristics of IoT devices. On the other hand, the aforementioned constraints of IoT devices require the mitigation of friendly jammers' interference on legitimate transmission. The IoT devices may fail to decode the useful information from the received mixed signals if the received FJ signal is strong, because the signal processing requirements for low-powered IoT devices besides normal communication should be treated as an extra burden. The technique such as beamforming should be integrated with FJ schemes to minimize the interference of FJ signals on legitimate transmissions in the IoT.

6.4. Friendly Jamming in UAV-enabled Networks

Due to the rapid growth of UAV applications in the military and civilian environment, applying UAVs to emit FJ signals has been extensively investigated in recent studies. However, different from conventional wireless networks that have often been analyzed in a two-dimensional (2D) plane, UAV-enabled networks require the analysis through the whole 3D space. In contrast to 2D networks, the 3D air-ground wireless communication environment is more complicated. Thus, different channel models need to consider. Another important characteristic of UAV-aided communication is mobility. With the consideration of UAV's mobility, building the 3D wireless communication model to analyze the performance of FJ schemes in UAV-enabled networks still deserves to be explored.

Meanwhile, UAVs may play a role as a malicious user instead of the friendly jammer. In particular, in IoT networks, some sensor devices are mounted on the top of the buildings. For example, the sensors in some smart healthcare networks are equipped at the roof of the house to monitor the health status of the patients while a malicious UAV intruder may wiretap the confidential and sensitive information from the patents. In the future, it is worthwhile to investigate the countermeasure to these malicious attacks. For example, we may place a friend jammer on top of the build to mitigate the eavesdropping activities from the air. When we investigate to protect the security of wireless transmission in such IoT networks with FJ schemes, the height from the devices to the floor should not be ignored.

7. Conclusion

The wide adoption of URLLC in 5G and beyond communications is facing some challenges, especially in the security aspect. In contrast to the conventional cryptographic methods that have a stringent computational requirement on end devices, FJ schemes neither require end devices to conduct computationally-complex operations nor alterations on current communication/networking infrastructures, thereby exhibiting strengths in assuring security of URLLC. There are a number of studies on FJ schemes in wireless communications. In this article, we present a comprehensive review on existing studies of FJ schemes. We first give an overview of FJ schemes as well as performance metrics. We then discuss that FJ schemes can be integrated with diverse communication technologies such as beamforming, multiple-input multiple-output, full duplex, and relay selection. We next discuss the applications of FJ schemes in different networks, including cognitive radio networks, heterogeneous networks, Internet of things, D2D networks, and UAV aided networks. To demonstrate the effectiveness of FJ schemes, we also provide a case study of the beamforming assisted FJ scheme. Finally, the future research directions of FJ schemes are also summarized.

References

[1] P. Popovski, J. J. Nielsen, C. Stefanovic, E. d. Carvalho, E. Strom, K. F. Trillingsgaard, A. Bana, D. M. Kim, R. Kotaba, J. Park, R. B. Sorensen, Wireless access for ultra-reliable low-latency communication: Principles and building blocks, IEEE Network 32 (2) (2018) 16–23.

[2] P. Popovski, C. Stefanovic, J. J. Nielsen, E. de Carvalho, M. Angjelichinoski, K. F. Trillingsgaard, A. Bana, Wireless access in ultra-reliable low-latency communication (urllc), IEEE Transactions on Communications 67 (8) (2019) 5783–5801.

[3] Z. Hou, C. She, Y. Li, L. Zhuo, B. Vucetic, Prediction and communication co-design for ultra-reliable and low-latency communications, IEEE Transactions on Wireless Communications 19 (2) (2020) 1196–1209.

[4] L. U. Khan, I. Yaqoob, M. Imran, Z. Han, C. S. Hong, 6g wireless systems: A vision, architectural elements, and future directions, IEEE Access 8 (2020) 147029–147044.

[5] H. Yang, A. Alphones, W. Zhong, C. Chen, X. Xie, Learning-based energy-efficient resource management by heterogeneous rf/vlc for ultra-reliable low-latency industrial iot networks, IEEE Transactions on Industrial Informatics 16 (8) (2020) 5565–5576.

[6] G. Hampel, C. Li, J. Li, 5g ultra-reliable low-latency communications in factory automation leveraging licensed and unlicensed bands, IEEE Communications Magazine 57 (5) (2019) 117–123.

[7] H. Yang, K. Zheng, K. Zhang, J. Mei, Y. Qian, Ultra-reliable and low-latency communications for connected vehicles: Challenges and solutions, IEEE Network 34 (3) (2020) 92–100.

[8] H. Yang, K. Zhang, K. Zheng, Y. Qian, Joint frame design and resource allocation for ultra-reliable and low-latency vehicular networks, IEEE Transactions on Wireless Communications 19 (5) (2020) 3607–3622.

[9] M. K. Abdel-Aziz, S. Samarakoon, C. Liu, M. Bennis, W. Saad, Optimized age of information tail for ultra-reliable low-latency communications in vehicular networks, IEEE Transactions on Communications 68 (3) (2020) 1911–1924.

[10] S. A. A. Shah, E. Ahmed, M. Imran, S. Zeadally, 5g for vehicular communications, IEEE Communications Magazine 56 (1) (2018) 111–117.

[11] C. She, C. Liu, T. Q. S. Quek, C. Yang, Y. Li, Ultra-reliable and low-latency communications in unmanned aerial vehicle communication systems, IEEE Transactions on Communications 67 (5) (2019) 3768–3781.

[12] K. Chen, Y. Wang, Z. Fei, X. Wang, Power limited ultra-reliable and low-latency communication in uav-enabled iot networks, in: 2020 IEEE Wireless Communications and Networking Conference (WCNC), 2020, pp. 1–6.

[13] M. S. Elbamby, C. Perfecto, M. Bennis, K. Doppler, Toward low-latency and ultra-reliable virtual reality, IEEE Network 32 (2) (2018) 78–84.

[14] G. J. Sutton, J. Zeng, R. P. Liu, W. Ni, D. N. Nguyen, B. A. Jayawickrama, X. Huang, M. Abolhasan, Z. Zhang, E. Dutkiewicz, T. Lv, Enabling technologies for ultra-reliable and low latency communications: From phy and mac layer perspectives, IEEE Communications Surveys& Tutorials 21 (3) (2019) 2488–2524.

[15] L. Li, G. Xu, L. Jiao, X. Li, H. Wang, J. Hu, H. Xian, W. Lian, H. Gao, A secure random key distribution scheme against node replication attacks in industrial wireless sensor systems, IEEE Transactions on Industrial Informatics 16 (3) (2020) 2091–2101.

[16] X. Li, G. Xu, X. Zheng, K. Liang, E. Panaousis, T. Li, W. Wang, C. Shen, Using sparse representation to detect anomalies in complex wsns, ACM Transactions on Intelligent Systems and Technology (TIST) 10 (6) (2019) 1–18.

[17] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. A. Latif, F. M. Al-Turjman, L. Mostarda, Cyber security threats detection in internet of things using deep learning approach, IEEE Access 7 (2019) 124379–124389.

[18] R. Chen, C. Li, S. Yan, R. Malaney, J. Yuan, Physical layer security for ultra-reliable and low-latency communications, IEEE Wireless Communications 26 (5) (2019) 6–11.

[19] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, M. Imran, Perception layer security in internet of things, Future Generation Computer Systems 100 (2019) 144 – 164.

[20] J. M. Batalla, E. Andrukiewicz, G. P. Gomez, P. Sapiecha, C. X. Mavromoustakis, G. Mastorakis, J. Zurek, M. Imran, Security risk assessment for 5g networks: National perspective, IEEE Wireless Communications 27 (4) (2020) 16–22.

[21] C. Thirumalai, S. Mohan, G. Srivastava, An efficient public

key secure scheme for cloud and iot security, Computer Communications 150 (2020) 634 – 643.

[22] B. D. Deebak, F. Al-Turjman, M. Aloqaily, O. Alfandi, An Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT, IEEE Access 7 (2019) 135632–135649.

[23] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, S. E. Venegas-Andraca, Secure Data Encryption Based on Quantum Walks for 5G Internet of Things Scenario, IEEE Transactions on Network and Service Management 17 (1) (2020) 118–131.

[24] W. Yaokumah, M. Rajarajan, J.-D. Abdulai, I. Wiafe, F. Katsriku, Modern Theories and Practices for Cyber Ethics and Security Compliance, IGI Global, 2020.

[25] A. Yeboah-Ofori, J.-D. Abdulai, F. Katsriku, Cybercrime and risks for cyber physical systems, International Journal of Cyber-Security and Digital Forensics 8.

[26] H. Ren, C. Pan, Y. Deng, M. Elkashlan, A. Nallanathan, Resource allocation for secure urllc in mission-critical iot scenarios, IEEE Transactions on Communications (Early Access) (2020) 1–1.

[27] J. M. Hamamreh, E. Basar, H. Arslan, Ofdm-subcarrier index selection for enhancing security and reliability of 5g urllc services, IEEE Access 5 (2017) 25863–25875.

[28] T. Zheng, H. Wang, Q. Yang, M. Lee, Safeguarding decentralized wireless networks using full-duplex jamming receivers, IEEE Transactions on Wireless Communications 16 (1) (2017) 278–292.

[29] R. Zhao, Y. Huang, W. Wang, V. Lau, Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming, IEEE Transactions on Wireless Communications 15 (4) (2016) 2537–2551.

[30] K. Cao, B. Wang, H. Ding, L. Lv, R. Dong, T. Cheng, F. Gong, Improving physical layer security of uplink noma via energy harvesting jammers, IEEE Transactions on Information Forensics and Security 16 (2021) 786–799.

[31] Y. Liu, J. Xu, R. Zhang, Exploiting interference for secrecy wireless information and power transfer, IEEE Wireless Communications 25 (1) (2018) 133–139.

[32] M. T. Mamaghani, Y. Hong, Improving phy-security of uav-enabled transmission with wireless energy harvesting: Robust trajectory design and communications resource allocation, IEEE Transactions on Vehicular Technology 69 (8) (2020) 8586–8600.

[33] W. Wang, X. Li, M. Zhang, K. Cumanan, D. W. Kwan Ng, G. Zhang, J. Tang, O. A. Dobre, Energy-constrained uav-assisted secure communications with position optimization and cooperative jamming, IEEE Transactions on Communications 68 (7) (2020) 4476–4489.

[34] I. Bang, S. Kim, D. Sung, Artificial noise-aided user scheduling from the perspective of secrecy outage probability, IEEE Transactions on Vehicular Technology 67 (8) (2018) 7816–7820.

[35] C. Liu, N. Yang, R. Malaney, J. Yuan, Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers, IEEE Transactions on Wireless Communications 15 (11) (2016) 7444–7456.

[36] X. Yang, A. Swindlehurst, Limited rate feedback in a mimo wiretap channel with a cooperative jammer, IEEE Transactions on Signal Processing 64 (18) (2016) 4695–4706.

[37] Y. Sarikaya, O. Ercetin, O. Gurbuz, Control of cognitive networks with friendly jamming as a service, IEEE Transactions on Cognitive Communications and Networking 4 (2) (2018) 299–313.

[38] C. Wang, H. Wang, Robust joint beamforming and jamming for secure af networks: Low-complexity design, IEEE Transactions on Vehicular Technology 64 (5) (2015) 2192–2198.

[39] S. Wang, X. Xu, K. Huang, X. Ji, Y. Chen, L. Jin, Artificial noise aided hybrid analog-digital beamforming for secure transmission in mimo millimeter wave relay systems, IEEE Access 7 (2019) 28597–28606.

[40] N. Ouyang, X. Jiang, E. Bai, H. Wang, Destination assisted jamming and beamforming for improving the security of af relay systems, IEEE Access 5 (2017) 4125–4131.

[41] Y. Huang, Z. Li, F. Zhou, R. Zhu, Robust an-aided beamforming design for secure miso cognitive radio based on a practical nonlinear eh model, IEEE Access 5 (2017) 14011–14019.

[42] B. Li, Z. Fei, H. Chen, Robust artificial noise-aided secure beamforming in wireless-powered non-regenerative relay networks, IEEE Access 4 (2016) 7921–7929.

[43] X. Yu, Y. Hu, Q. Pan, X. Dang, N. Li, M. Shan, Secrecy performance analysis of artificial-noise-aided spatial modulation in the presence of imperfect csi, IEEE Access 6 (2018) 41060–41067.

[44] Y. Zhang, J. Zhang, H. Yu, Physically securing energy-based massive mimo mac via joint alignment of multi-user constellations and artificial noise, IEEE Journal on Selected Areas in Communications 36 (4) (2018) 829–844.

[45] T. Zheng, H. Wang, Optimal power allocation for artificial noise under imperfect csi against spatially random eavesdroppers, IEEE Transactions on Vehicular Technology 65 (10) (2016) 8812–8817.

[46] R. Eletreby, H. Rahbari, M. Krunz, Supporting phy-layer security in multi-link wireless networks using friendly jamming, in: 2015 IEEE Global Communications Conference (GLOBECOM), 2015, pp. 1–6.

[47] Z. Li, T. Jing, X. Cheng, Y. Huo, W. Zhou, D. Chen, Cooperative jamming for secure communications in mimo cooperative cognitive radio networks, in: 2015 IEEE International Conference on Communications (ICC), 2015, pp. 7609–7614.

[48] S. Iwata, T. Ohtsuki, P. Kam, A lower bound on secrecy capacity for mimo wiretap channel aided by a cooperative jammer with channel estimation error, IEEE Access 5 (2017) 4636–4645.

[49] M. Ahmed, L. Bai, Secrecy capacity of artificial noise aided secure communication in mimo rician channels, IEEE Access 6 (2018) 7921–7929.

[50] X. Hu, C. Kai, S. Zhang, Z. Guo, J. Gao, To establish a secure channel from a full-duplex transmitter to a half-duplex receiver: An artificial-noise-aided scheme, IEEE Wireless Communications Letters 8 (2) (2019) 480–483.

[51] A. Mabrouk, A. Shafie, K. Tourki, N. Al-Dhahir, An-aided relay-selection scheme for securing untrusted rf-eh relay systems, IEEE Transactions on Green Communications and Networking 1 (4) (2017) 481–493.

[52] R. Nakai, S. Sugiura, Physical layer security in buffer-state-based max-ratio relay selection exploiting broadcasting with cooperative beamforming and jamming, IEEE Transactions on Information Forensics and Security 14 (2) (2019) 431–444.

[53] M. H. Khoshafa, T. M. N. Ngatched, M. H. Ahmed, A. Ibrahim, Secure transmission in wiretap channels using full-duplex relay-aided d2d communications with outdated csi, IEEE Wireless Communications Letters 9 (8) (2020) 1216–1220.

[54] J. Kang, J. Yang, J. Ha, I. Kim, Joint design of optimal precoding and cooperative jamming for multiuser secure broadcast systems, IEEE Transactions on Vehicular Technology 66 (11) (2017) 10551–10556.

[55] H. Long, W. Xiang, Y. Li, Precoding and cooperative jamming in multi- antenna two-way relaying wiretap systems without eavesdropper's channel state information, IEEE Transactions on Information Forensics and Security 12 (6) (2017) 1309–1318.

[56] P. Siyari, M. Krunz, D. Nguyen, Price-based friendly jamming in a miso interference wiretap channel, in: IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, 2016, pp. 1–9.

[57] Z. Chu, H. Nguyen, T. Le, M. Karamanoglu, D. To, E. Eve, F. Al-Turjman, A. Yazici, Game theory based secure wireless powered d2d communications with cooperative jamming, in: 2017 Wireless Days, 2017, pp. 95–98.

[58] X. Hu, X. Zhang, H. Huang, Y. Li, Secure transmission via jamming in cognitive radio networks with possion spatially

distributed eavesdroppers, in: 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2016, pp. 1–6.

[59] Y. Wen, T. Jing, Y. Huo, Z. Li, Q. Gao, Secrecy energy efficiency optimization for cooperative jamming in cognitive radio networks, in: 2018 International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 795–799.

[60] Y. Huo, X. Fan, L. Ma, X. Cheng, Z. Tian, D. Chen, Secure communications in tiered 5g wireless networks with cooperative jamming, IEEE Transactions on Wireless Communications 18 (6) (2019) 3265–3280.

[61] H. Wang, B. Zhao, T. Zheng, Adaptive full-duplex jamming receiver for secure d2d links in random networks, IEEE Transactions on Communications 67 (2) (2019) 1254–1267.

[62] M. H. Khoshafa, T. M. N. Ngatched, M. H. Ahmed, On the physical layer security of underlay relay-aided device-to-device communications, IEEE Transactions on Vehicular Technology 69 (7) (2020) 7609–7621.

[63] A. Li, Q. Wu, R. Zhang, Uav-enabled cooperative jamming for improving secrecy of ground wiretap channel, IEEE Wireless Communications Letters 8 (1) (2019) 181–184.

[64] H. Lei, D. Wang, K. Park, I. S. Ansari, J. Jiang, G. Pan, M. Alouini, Safeguarding uav iot communication systems against randomly located eavesdroppers, IEEE Internet of Things Journal 7 (2) (2020) 1230–1244.

[65] L. Hu, H. Wen, B. Wu, F. Pan, R. Liao, H. Song, J. Tang, X. Wang, Cooperative jamming for physical layer security enhancement in internet of things, IEEE Internet of Things Journal 5 (1) (2018) 219–228.

[66] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, W. Dou, Complementing iot services through software defined networking and edge computing: A comprehensive survey, IEEE Communications Surveys & Tutorials 22 (3) (2020) 1761–1804.

[67] Y. Huo, Y. Tian, L. Ma, X. Cheng, T. Jing, Jamming strategies for physical layer security, IEEE Wireless Communications 25 (1) (2018) 148–153.

[68] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, G. K. Karagiannidis, Physical layer security jamming: Theoretical limits and practical designs in wireless networks, IEEE Access 5 (2017) 3603–3611.

[69] B. Wang, P. Mu, Z. Li, Artificial-noise-aided beamforming design in the misome wiretap channel under the secrecy outage probability constraint, IEEE Transactions on Wireless Communications 16 (11) (2017) 7207–7220.

[70] K. Lee, J. Hong, H. Choi, M. Levorato, Adaptive wireless-powered relaying schemes with cooperative jamming for two-hop secure communication, IEEE Internet of Things Journal 5 (4) (2018) 2793–2803.

[71] J. Giti, A. Sakzad, B. Srinivasan, J. Kamruzzaman, R. Gaire, Secrecy capacity against adaptive eavesdroppers in a random wireless network using friendly jammers and protected zone, Journal of Network and Computer Applications 165 (2020) 102698.

[72] X. Tang, Y. Cai, Y. Deng, Y. Huang, W. Yang, W. Yang, Energy-constrained swipt networks: Enhancing physical layer security with fd self-jamming, IEEE Transactions on Information Forensics and Security 14 (1) (2019) 212–222.

[73] G. Li, X. Sheng, J. Wu, H. Yu, Securing transmissions by friendly jamming scheme in wireless networks, Journal of Parallel and Distributed Computing 144 (2020) 260 – 267.

[74] D. Berger, F. Gringoli, N. Facchi, I. Martinovic, J. B. Schmitt, Friendly jamming on access points: Analysis and real-world measurements, IEEE Transactions on Wireless Communications 15 (9) (2016) 6189–6202.

[75] X. Li, H.-N. Dai, Q. Wang, M. Imran, D. Li, M. A. Imran, Securing internet of medical things with friendly-jamming schemes, Computer Communications 160 (2020) 431–442. doi:10.1016/j.comcom.2020.06.026.

[76] F. Zhou, Z. Chu, H. Sun, R. Hu, L. Hanzo, Artificial noise aided secure cognitive beamforming for cooperative miso-noma using swipt, IEEE Journal on Selected Areas in Communications 36 (4) (2018) 918–931.

[77] F. Shu, L. Xu, J. Wang, W. Zhu, Z. Xiaobo, Artificial-noise-aided secure multicast precoding for directional modulation systems, IEEE Transactions on Vehicular Technology 67 (7) (2018) 6658–6662.

[78] F. Zhou, Z. Li, J. Cheng, Q. Li, J. Si, Robust an-aided beamforming and power splitting design for secure miso cognitive radio with swipt, IEEE Transactions on Wireless Communications 16 (4) (2017) 2450–2464.

[79] V. Nguyen, T. Duong, O. Dobre, O. Shin, Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks, IEEE Transactions on Information Forensics and Security 11 (11) (2016) 2609–2623.

[80] B. Wang, P. Mu, Z. Li, Secrecy rate maximization with artificial-noise-aided beamforming for miso wiretap channels under secrecy outage constraint, IEEE Communications Letters 19 (1) (2015) 18–21.

[81] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, Y. Zhang, Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays, IEEE Access 5 (2017) 1658–1667.

[82] Z. Li, P. Mu, B. Wang, X. Hu, Optimal semiadaptive transmission with artificial-noise-aided beamforming in miso wiretap channels, IEEE Transactions on Vehicular Technology 65 (9) (2016) 7021–7035.

[83] H. Ma, J. Cheng, X. Wang, P. Ma, Robust miso beamforming with cooperative jamming for secure transmission from perspectives of qos and secrecy rate, IEEE Transactions on Communications 66 (2) (2018) 767–780.

[84] H. Ma, J. Cheng, X. Wang, Cooperative jamming aided robust beamforming for miso channels with unknown eavesdroppers, in: GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017, pp. 1–5.

[85] Y. Deng, L. Wang, S. Zaidi, J. Yuan, M. Elkashlan, Artificial-noise aided secure transmission in large scale spectrum sharing networks, IEEE Transactions on Communications 64 (5) (2016) 2116–2129.

[86] W. Zhang, J. Chen, Y. Kuo, Y. Zhou, Artificial-noise-aided optimal beamforming in layered physical layer security, IEEE Communications Letters 23 (1) (2019) 72–75.

[87] H. Guo, Z. Yang, L. Zhang, J. Zhu, Y. Zou, Joint cooperative beamforming and jamming for physical-layer security of decode-and-forward relay networks, IEEE Access 5 (2017) 19620–19630.

[88] J. Xiong, L. Cheng, D. Ma, J. Wei, Destination-aided cooperative jamming for dual-hop amplify-and-forward mimo untrusted relay systems, IEEE Transactions on Vehicular Technology 65 (9) (2016) 7274–7284.

[89] Q. Li, L. Yang, Artificial noise aided secure precoding for mimo untrusted two-way relay systems with perfect and imperfect channel state information, IEEE Transactions on Information Forensics and Security 13 (10) (2018) 2628–2638.

[90] J. Wang, J. Lee, F. Wang, T. Quek, Jamming-aided secure communication in massive mimo rician channels, IEEE Transactions on Wireless Communications 14 (12) (2015) 6854–6868.

[91] A. Shafie, D. Niyato, N. Al-Dhahir, Artificial-noise-aided secure mimo full-duplex relay channels with fixed-power transmissions, IEEE Communications Letters 20 (8) (2016) 1591–1594.

[92] Y. Bi, H. Chen, Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer, IEEE Journal of Selected Topics in Signal Processing 10 (8) (2016) 1538–1550.

[93] Y. Li, R. Zhao, Y. Wang, G. Pan, C. Li, Artificial noise aided precoding with imperfect csi in full-duplex relaying secure communications, IEEE Access 6 (2018) 44107–44119.

[94] J. Yao, S. Feng, Y. Liu, Secure routing in full-duplex jamming multihop relaying, in: 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–6.

[95] X. Tang, W. Yang, Y. Cai, W. Yang, Y. Huang, Security of full-duplex jamming swipt system with multiple non-colluding

eavesdroppers, in: 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), 2017, pp. 66–69.

[96] Y. Choi, J. Lee, A new cooperative jamming technique for a two-hop amplify-and-forward relay network with an eavesdropper, IEEE Transactions on Vehicular Technology 67 (12) (2018) 12447–12451.

[97] X. Ding, T. Song, Y. Zou, X. Chen, L. Hanzo, Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection, IEEE Transactions on Vehicular Technology 66 (5) (2017) 3930–3941.

[98] S. Jia, J. Zhang, H. Zhao, Y. Lou, Y. Xu, Relay selection for improved physical layer security in cognitive relay networks using artificial noise, IEEE Access 6 (2018) 64836–64846.

[99] D. Li, S. Yan, X. Zhang, Y. Shang, Combined physical network coding and friendly jamming for secure wireless cooperative communications, in: 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), 2016, pp. 1–5.

[100] R. Chou, A. Yener, Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming, IEEE Transactions on Information Theory 64 (12) (2018) 7903–7921.

[101] X. Wu, Z. Yang, C. Ling, X. Xia, Artificial-noise-aided message authentication codes with information-theoretic security, IEEE Transactions on Information Forensics and Security 11 (6) (2016) 1278–1290.

[102] X. Wu, Z. Yang, C. Ling, X. Xia, Artificial-noise-aided physical layer phase challenge-response authentication for practical ofdm transmission, IEEE Communications Letters 15 (10) (2016) 6611–6625.

[103] Z. Chu, H. Nguyen, T. Le, M. Karamanoglu, E. Ever, A. Yazici, Secure wireless powered and cooperative jamming d2d communications, IEEE Transactions on Green Communications and Networking 2 (1) (2018) 1–13.

[104] P. Siyari, M. Krunz, D. Nguyen, Friendly jamming in a mimo wiretap interference network: A nonconvex game approach, IEEE Journal on Selected Areas in Communications 35 (3) (2017) 601–614.

[105] F. Gabry, A. Zappone, R. Thobaben, E. Jorswieck, M. Skoglund, Energy efficiency analysis of cooperative jamming in cognitive radio networks with secrecy constraints, IEEE Wireless Communications Letters 4 (4) (2015) 437–440.

[106] K. Wang, L. Yuan, T. Miyazaki, S. Guo, Y. Sun, Antieavesdropping with selfish jamming in wireless networks: A bertrand game approach, IEEE Transactions on Vehicular Technology 66 (7) (2017) 6268–6279.

[107] L. Tang, H. Chen, Q. Li, Social tie based cooperative jamming for physical layer security, IEEE Communications Letters 19 (10) (2015) 1790–1793.

[108] B. Fang, Z. Qian, W. Shao, W. Zhong, Precoding and artificial noise design for cognitive mimome wiretap channels, IEEE Transactions on Vehicular Technology 65 (8) (2016) 6753–6758.

[109] Y. Jiang, Y. Zou, J. Ouyang, J. Zhu, Secrecy energy efficiency optimization for artificial noise aided physical-layer security in ofdm-based cognitive radio networks, IEEE Transactions on Vehicular Technology 67 (12) (2018) 11858–11872.

[110] W. Tang, S. Feng, Y. Ding, Y. Liu, Jammer selection in heterogeneous networks with full-duplex users, in: 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–6.

[111] W. Tang, S. Feng, Y. Ding, Y. Liu, Physical layer security in heterogeneous networks with jammer selection and full-duplex users, IEEE Transactions on Wireless Communications 16 (12) (2017) 7982–7995.

[112] S. Yan, Y. Shang, M. Zhang, Compromised secrecy region with friendly jammers in heterogeneous cellular networks, in: IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2018, pp. 848–852.

[113] A. Zhang, X. Lin, Security-aware and privacy-preserving d2d communications in 5g, IEEE Network 31 (4) (2017) 70–77.

[114] W. Li, H. Wu, Jamming partner selection for maximising the worst d2d secrecy rate based on social trust, Transactions on Emerging Telecommunications Technologies 2 (4).

[115] W. Li, C. Cao, H. Wu, Secure inter-cluster communications with cooperative jamming against social outcasts, Computer Communications 63 (2015) (2015) 1–10.

[116] J. Ouyang, M. Lin, W. Zhu, K. An, L. Wang, Improving secrecy performance via device-to-device jamming in cellular networks, in: 2016 8th International Conference on Wireless Communications Signal Processing (WCSP), 2016, pp. 1–5.

[117] Q. Zeng, Z. Zhang, The full-duplex device-to-device security communication under the coverage of unmanned aerial vehicle, KSII Transactions on Internet and Information Systems 13 (4) (2019) 1941–1960.

[118] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, R. Schober, L. Zhuo, B. Vucetic, Improving physical layer security via a uav friendly jammer for unknown eavesdropper location, IEEE Transactions on Vehicular Technology 67 (11) (2018) 11280–11284.

[119] Y. Li, R. Zhang, J. Zhang, S. Gao, L. Yang, Cooperative jamming for secure uav communications with partial eavesdropper information, IEEE Access 7 (2019) 94593–94603.

[120] C. Zhong, J. Yao, J. Xu, Secure uav communication with cooperative jamming and trajectory control, IEEE Communications Letters 23 (2) (2019) 286–289.

[121] H. Lee, S. Eom, J. Park, I. Lee, Uav-aided secure communications with cooperative jamming, IEEE Transactions on Vehicular Technology 67 (10) (2018) 9385–9392.

[122] J. Tang, G. Chen, J. P. Coon, Secrecy performance analysis of wireless communications in the presence of uav jammer and randomly located uav eavesdroppers, IEEE Transactions on Information Forensics and Security 14 (11) (2019) 3026–3041.

[123] Y. Chen, Z. Zhang, Uav-aided secure transmission in misome wiretap channels with imperfect csi, IEEE Access 7 (2019) 98107–98121.

[124] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, M. Imran, Unmanned aerial vehicle for internet of everything: Opportunities and challenges, Computer Communications 155 (2020) 66–83. doi:https://doi.org/10.1016/j.comcom.2020.03.017.
URL https://www.sciencedirect.com/science/article/pii/S0140366419318754

[125] X. Li, H. Dai, H. Wang, Friendly-jamming: An anti-eavesdropping scheme in wireless networks of things, in: 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–6.

[126] J. Kim, J. Choi, Cancellation-based friendly jamming for physical layer security, in: 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1–6.

[127] Z. Li, Zhen, T. Jing, L. Ma, Y. Huo, J. Qian, Worst-case cooperative jamming for secure communications in ciot networks, Sensors 16 (3). doi:10.3390/s16030339.

[128] P. Xie, L. Xing, H. Wu, J. Seo, I. You, Cooperative jammer selection for secrecy improvement in cognitive internet of things, Sensors 18 (4257).

[129] Q. Wang, H.-N. Dai, H. Wang, G. Xu, A. K. Sangaiah, Uav-enabled friendly jamming scheme to secure industrial internet of things, Journal of Communications and Networks 21 (5) (2019) 481–490.

[130] X. Li, Q. Wang, H.-N. Dai, H. Wang, A novel friendly jamming scheme in industrial crowdsensing networks against eavesdropping attack, Sensors 18 (6).

[131] T. Perera, D. Jayakody, S. Sharma, S. Chatzinotas, J. Li, Simultaneous Wireless Information and Power Transfer (SWIPT): Recent Advances and Future Challenges, IEEE Communications Surveys & Tutorials 20 (1) (2018) 264–302.

[132] Z. Zhang, K. Long, A. V. Vasilakos, L. Hanzo, Full-duplex wireless communications: Challenges, solutions, and future research directions, Proceedings of the IEEE 104 (7) (2016) 1369–1409.