Li, X., Dai, H.-N., Wang, Q., Imran, M., Li, D. and Imran, M. A. (2020) Securing internet of medical things with friendly-jamming schemes. *Computer Communications*, 160, pp. 431-442.

(doi: 10.1016/j.comcom.2020.06.026)

This is the Author Accepted Manuscript.

There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

https://eprints.gla.ac.uk/219227/

Deposited on: 29 June 2020

Enlighten – Research publications by members of the University of Glasgow
http://eprints.gla.ac.uk

Securing Internet of Medical Things with Friendly-Jamming Schemes

Xuran Li, Hong-Ning Dai, *Senior Member, IEEE*, Qubeijian Wang, Muhammad Imran, *Senior Member, IEEE*, Dengwang Li, Muhammad Ali Imran *Senior Member, IEEE*

Abstract*—The Internet of Medical Things (IoMT)-enabled e-healthcare can complement traditional medical treatments in a flexible and convenient manner. However, security and privacy become the main concerns of IoMT due to the limited computational capability, memory space and energy constraint of medical sensors, leading to the in-feasibility for conventional cryptographic approaches, which are often computationally-complicated. In contrast to cryptographic approaches, friendly jamming (Fri-jam) schemes will not cause extra computing cost to medical sensors, thereby becoming potential countermeasures to ensure security of IoMT. In this paper, we present a study on using Fri-jam schemes in IoMT. We first analyze the data security in IoMT and discuss the challenges. We then propose using Fri-jam schemes to protect the confidential medical data of patients collected by medical sensors from being eavesdropped. We also discuss the integration of Fri-jam schemes with various communication technologies, including beamforming, Simultaneous Wireless Information and Power Transfer (SWIPT) and full duplexity. Moreover, we present two case studies of Fri-jam schemes in IoMT. The results of these two case studies indicate that the Fri-jam method will significantly decrease the eavesdropping risk while leading to no significant influence on legitimate transmission.

***Index Terms*—Internet of medical things; network security; friendly jamming**

I. Introduction

WITH the rapid technological advances in big data, cloud computing, machine learning/deep learning and Internet of Things, more powerful and convenient applications become available [1]–[5]. Among all the applications in different fields, the Internet of Medical Things (IoMT) as an ecosystem consisting of connected medical sensors, computing systems and clinical systems has drawn extensive attention in recent years due to the significant improvements in efficiency and quality of healthcare services [6], [7]. In IoMT system, the medical sensors collect the physiological data of patients and send them to a database repository, in which the authorized health practitioners (e.g., doctors, nurses) can access and take corresponding medical measures according to the collected physiological data of patients [8]–[11]. IoMT can be used to provide remote real-time health monitoring, studying the effect of treatment, and offering elderly healthcare in hospitals and even at home. Therefore, the IoMT is believed to be a promising solution to the absence of medical resource and avoid unnecessary hospitalizations. Compared with traditional healthcare services, the IoMT will reduce the medical cost and promote the scale and flexibility to enable the reliable and qualified healthcare services [12], [13]. Moreover, with the help of IoMT system, the frequency of close face-to-face contact between patients and healthcare providers (e.g., doctors, nurses) shall be significantly reduced. This manner is beneficial to prevent the spread of infectious diseases like new corona-virus (i.e., COVID-19) [14].

Although IoMT system provides effective and reliable healthcare services for patients and doctors, it faces serious security challenges due to the vulnerabilities of leaking the patients' sensitive medical information [15]–[17]. In particular, the sensitive medical information collected by medical sensors is transmitted to data servers via the open wireless channel connected to the Internet. During this process, malicious users may wiretap (or eavesdrop) the confidential and sensitive information, thereby leading to the serious information leakage of patients [18], [19]. Conventional cryptographic techniques have been commonly employed to protect the security of wireless communications. The current approaches to protect the security of medical data in IoMT are mainly relying on cryptographic techniques, such as identity authentication [20]–[23], access control [24]–[30] and data encryption [31]–[33]. Nevertheless, the computational-resource requirements for most cryptographic schemes are not feasible for medical sensors which are limited in computational capability, memory space and energy capacity [34], [35].

In contrast to computational-complex cryptographic approaches, physical layer security provides a cost efficient way to protect the wireless communications by exploiting the inherent characteristics of the wireless channel [36]. Among all the methods of physical layer security, Friendly jamming (Fri-jam) is an efficient and effective method to reduce the received Signal-to-Interference-and-Noise Ratio (SINR) at the eavesdropper while having no requirement on Internet of Things devices [37]. The Fri-jam is a method that injects Fri-jam signals to increase the noise level at the eavesdropper, and the eavesdropper is unable to successfully decode the confidential messages. The benefits of this method include low computational capability requirement, low implementation complexity, few exchanges of coordination messages and no processing of the information bearing messages [38]. On the other hand, in

X. Li and Dengwang Li are with Shandong Key Laboratory of Medical Physics and Image Processing, School of Physics and Electronics, Shandong Normal University, Jinan, Shandong, China (email: lxrget@163.com; dengwang@sdnu.edu.cn).

H.-N. Dai and Q. Wang are with the Faculty of Information Technology, Macau University of Science and Technology, Macau SAR (email: hndai@ieee.org; qubeijian.wang@gamil.com).

M. Imran is College of Applied Computer Science, King Saud University, Riyadh, Saudi Arabia (email: dr.m.imran@ieee.org).

M. A. Imran is with School of Engineering, University of Glasgow, Glasgow, U.K. (email: Muhammad.Imran@glasgow.ac.uk).

TABLE I
TABLE OF ACRONYMS

Acronyms	Terms	Acronyms	Terms
AES	Advanced Encryption Standard	MISO	Multiple-Input Single-Output
BLE	Bluetooth Low Energy	NFC	Near-Field Communication
BS	Base Station	NOMA	Non Othogonal Multiple Access
CPU	Central Processing Unit	OFDMA	Orthogonal Frequency Division Multiple Access
CRN	Cognitive Radio Network	PCO	Probability of the connection outage
CSI	Channel State Information	PSO	Probability of the secrecy outage
D2D	Device-to-Device	PPP	Poisson Point Process
ECG	Electrocardiogram	RFID	Radio Frequency Identification
FD	Full Duplex	SINR	Signal-to-Interference-and-Noise Ratio
Fri-jam	Friendly Jamming	SWIPT	Simultaneous wireless information and power transfer
HD	Half Duplex	SOR	Secrecy outage region
IC	Integrated Circuit Chip	SIC	Successive Interference Cancellation
IoMT	Internet of Medical Things	UAV	Unmanned Aerial Vehicle

conventional Fri-jam schemes, the power allocation between the legitimate information signal and the Fri-jam signal at the transmitter is a critical problem to be solved, revealing the trade off between enhancing the legitimate channel by increasing the power allocated to information-bearing signal and degrading the eavesdropper's channel by allocating more power to the Fri-jam signal [39]. In this paper, the power allocation problem can be solved by introducing friendly jammers into the IoMT individually, leading to no power consumption on the legitimate transmitters in this network. As a result, the proposed Fri-jam methods are feasible for resource-constrained wireless devices especially for medical sensors in IoMT.

To the best of our knowledge, there are few studies on protecting the communication security of IoMT with Fri-jam schemes. To fill this gap, this paper aims to present an overview on using Fri-jam schemes in IoMT. The main contributions of this paper are summarized as follows:

- We analyze the medical information security of IoMT. To be specific, we illustrate a 3-layer architecture of IoMT system consisting of data collection layer, data management layer and medical server layer. We then evaluate current security schemes to IoMT and identify the main security challenges in IoMT.
- Considering security challenges in IoMT, we propose Fri-jam schemes to secure the confidential medical data of patients collected by medical sensors. We also discuss the integration of Fri-jam schemes with other communication technologies such as Simultaneous Wireless Information and Power Transfer (SWIPT), beamforming and full duplexity so as to further improve the performance.
- We also introduce two case studies to verify the effectiveness of Fri-jam schemes. The results of these two case studies indicate that Fri-jam methods can significantly reduce the success probability of eavesdropping behaviour while leading to no significant influence on legitimate transmission when they are properly designed.

The rest of this paper is organized as follows: Section II provides security analysis on IoMT. Section III introduces Fri-jam schemes for protecting the medical data of IoMT. Section IV presents case studies of Fri-jam schemes. The conclusions and future work of this paper are given in Section V. Table I summarizes the main terms as well as their acronyms in this article.

II. SECURITY ANALYSIS ON IOMT

In this section, we provide a security analysis on IoMT. Specifically, we first present an illustration on the system architecture of IoMT. We then introduce some current security schemes for IoMT. At last, we discuss the security challenges in IoMT.

A. System Architecture of IoMT

Figure 1 illustrates the IoMT system architecture considered in this paper. This IoMT system architecture consists of three layers: data collection layer, data management layer and medical server layer, similar to recent studies such as [8], [40]–[42]. The medical sensors in data collection layer collect the physiological data of patients and send the collected data to the data servers located in data management layer after necessary preprocessing at edge servers, which are depolyed in approximation to patients. The data servers in data management layer store, process and analyze the collected medical data with a provision of the access interfaces to the authorized healthcare providers (such as doctors) in medical server layer. After processing and analyzing physiological information of patients at medical server layer, the healthcare providers as well as practitioners (e.g., medical doctors and nurses) can offer the professional advice to patients or take emergency measures. We then introduce the three layers of IoMT in details.

1) Data collection layer: The data collection layer is composed of medical sensors, mobile devices and edge servers. The medical sensors are sensor devices that implanted, worn or connected to daily items such as clothes. Medical sensors collect multi-source physiological data of patients, such as temperature, blood glucose, blood pressure, blood oxygenation, heart rate, breathing rate, pulse rate, movement and electrocardiogram (ECG) [43]–[45].

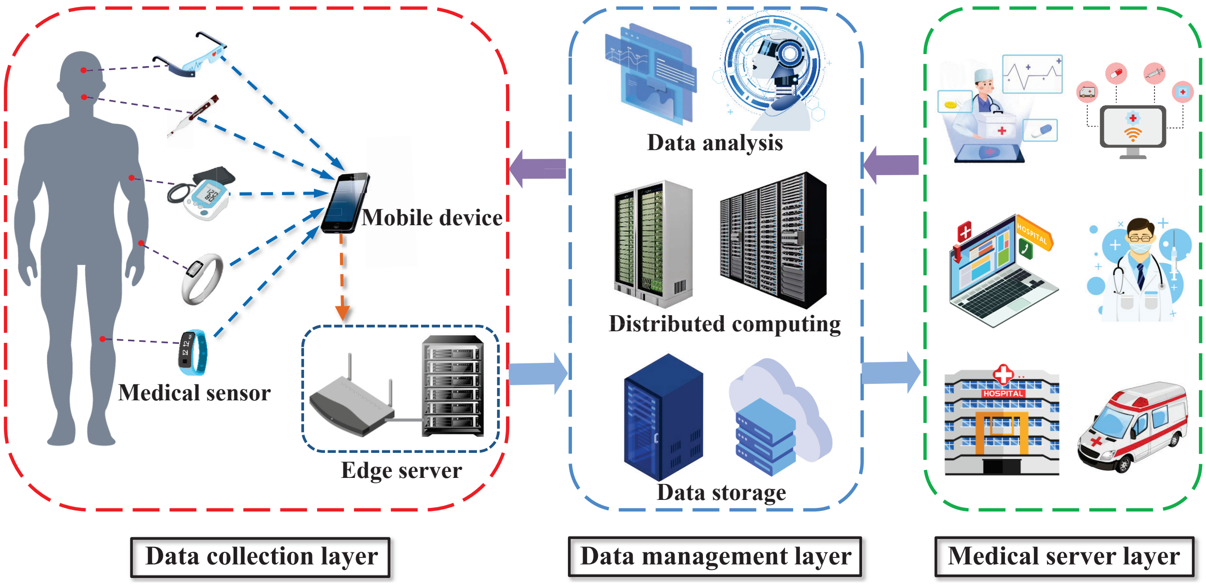


Fig. 1. System architecture of IoMT.

In emergency scenarios, strict monitoring will be performed. The medical sensors will continuously collect the important physiological data, which will be temporarily stored at a mobile device (such as smart phones, laptops and tablets). While in normal scenarios, intermittent monitoring will be performed according to the request of the authorized persons (e.g., patient, doctor or nurse, etc.). The medical sensors will collect patient data at frequent intervals. Each medical sensor is wirelessly connected to a dedicated mobile device via the low-power wireless technologies, such as Near-Field Communication (NFC), RFID and Bluetooth Low Energy (BLE) [46]. After preprocessing the collected data, the mobile device will transmit the data to the edge server, which is usually deployed close to patients.

The edge servers that are typically mounted at wireless accessing devices (such as wireless routers, IoT gateways and base stations) and interact with different types of local networks compatibly [8]. At the edge server, the original heterogeneous data in different structures and formats have been preprocessed and aggregated locally before sending to the next layer [47]. Compared with medical sensor devices and mobile devices, edge servers have much stronger computational capability and sufficient power supply. Therefore, edge servers can provide the secure data transmission between data collection layer and data management layer with stronger encryption algorithms. In addition, with the consent of patient, the applications for early diagnosis and rehabilitation progress assessment can be performed on the edge server. The edge servers can also generate alarm signals to alert the patient or doctor when any vital physiological parameter reaches a threshold.

Both security and privacy in the data collection layer pose challenges especially due to the limitations of computational capability and power supply of the medical sensor devices and mobile devices. Therefore, the security methods of this layer are required to be less computationally-complex and cause less communication overhead. We will present the explicit discussion on data collection layer in Section II-C.

2) Data management layer: The main aim of data management layer is to uniformly manage the received heterogeneous data from data collection layer. The received medical data should be processed and analyzed according to the timeliness of medical data and the priority of analysis tasks. In this layer, storage resources and computing facilities are provided to store, process, and analyze the collected physiological data.

In order to process huge volumes of medical data, most of studies adopt the distributed processing models in the data management layer, such as [8], [9], [30], [40]. Those distributed mechanisms for efficient data processing, analysis and storage are typically integrated with big data, cloud computing and storage technologies. Consequently, the data analysis based on cloud computing will significantly reduce the computing time and the data storage on the cloud will bring the ubiquitous convenience of accessing data anytime and anywhere.

The data security and patient privacy are important issues since patients' physiological data is stored at the data servers for a long time. Therefore, the data must be encrypted when being stored at the data management layer. Based on the strong computational-capability of data management facilities (like clouds), complicated and strong data encryption algorithms can be adopted to protect the data security and patient privacy. In addition, some identity authentication and access control mechanisms are also feasible to this layer. The details of these methods are introduced in Section II-B.

3) Medical server layer: In this layer, the healthcare professionals (e.g., doctors, nurses) which have authentication and authorization credentials are able to access patients' physiological data. After the process and analysis on the physiological data of patients in data management layer, the healthcare professionals are provided by visual data analytical results in this layer.

When the physiological data of patient is changing, the healthcare professionals can immediately discover it and take corresponding measures. The professional advice from hospitals and medical research centers to patients may reduce the number of visits to doctors and examinations. In addition, the recovery procedure of a patient can be traced by healthcare professionals. It is helpful for treatment optimization.

The main requirement of protecting the security of patients' data in the medical server layer is that only the authorized healthcare professionals can access the data. Therefore, the access control mechanisms (such as signatures or certificates) can be established to ensure that only authenticated users with access rights can access the data. The policies on health data sharing to avoid the leakage of patients' privacy information are implemented in this layer, too.

B. Current security schemes for IoMT

Security is one of the most important concerns in IoMT because the privacy sensitive physiological data of patients can be easily leaked or misused during the whole life cycle of medical data. The exposure of these data may lead to data abuse and even social discrimination against patients. The current approaches used for protecting the security of medical data in IoMT mainly include identity authentication, access control and data encryption.

Access control is the method to prevent illegal access to resources by unauthorized users and to determine the appropriate level of authority for authorized users. The authors in [20] proposed a lightweight glass-breaking access control system which contains two access modes: attribute-based access and glass-breaking access. The attribute-based access is used for fine-grained access control in normal situation while the glass-breaking access is used in emergency situation. In their proposed system, the collected medical data is encrypted by the patients themselves. A similar research is given in [21], where a two-fold flexible access control mechanism is designed for an IoMT data storage system. This access control mechanism is self-adaptive for normal scenario and emergency scenario, which protect the privacy of patients as well as guarantee the first-aid treatment to the patient when emergency situation occurs. In [22], the authors proposed a ciphertext-policy attribute-based encryption algorithm to build an access control system in IoMT. In this research, the authors addressed patient privacy issue by hiding the addressed data and encrypting the medical records. In research [23], a practical data collection framework is proposed for preventing insider attacks and protecting the privacy of patient. The proposed framework of IoMT utilized a secret sharing scheme based on Slepian-Wolf-coding algorithm. In this framework, a patient access control scheme is designed to prevent the data storage servers from revealing of patients' privacy.

Identity authentication is a method to validate the identity of each other and prevent unauthorized entity from accessing the sensitive medical data. The research [24] investigated a lightweight IoMT storage system. In this lightweight storage system, they designed a concrete data integrity verification scheme to verify the identity of patient and the integrity of the sensitive physiology data. In [25], the authors provided an authentication and key agreement protocol, and also provided an access control mechanism to enhance the information security and the privacy of patients and doctors. Moreover, the ownership transfer of the patient and doctor in IoMT system can be addressed with their proposed protocol. In [26], an end-to-end scheme for securing IoMT system is designed based on the handshake process and session resumption technique. In this scheme, the authentication and authorization architecture is built and the mobility of medical sensors in IoMT is considered. The research [27] introduced a secure IoMT system with privacy-aware aggregate authentication and access control mechanism. In this system, the authentication mechanism is designed with an anonymous certificateless aggregate signature scheme, and the access control mechanism is enabled by anonymous attribute-based encryption. The authors of research [28] proposed an update mechanism which can be used to update both authentication keys and session keys with two-way identity authentication method. This method can be used to identify and authenticate the legality of heterogeneous medical sensors. The identity authentication is achieved by the mechanism of the elliptic curve encryption algorithm signature as well as symmetric encryption algorithm of session key. An anonymous authentication scheme to prevent the authenticated patients from untrusted authentication server is proposed in [29], where the rotating group signatures based on elliptic curve cryptosystem is utilized in this scheme. The authors of [30] first proposed a lattice-based secure cryptosystem and then designed a mutual authentication scheme based on this cryptosystem. In addition, they proposed a data encryption scheme for data storage servers in data management layer on the foundation of their proposed cryptosystem.

Data encryption is a security method that both sides of communication transform information according to the agreed rules. The authors in [31] designed a group send-receive model and AES based key distribution scheme to realize the secure data transmission in IoMT. In addition, a homomorphic encryption based on matrix scheme is proposed in this research to enable a privacy-preserving strategy. A secure data collection scheme for enhancing the security of data acquisition and data transmission is proposed in [32]. This data collection scheme is designed based on two algorithms, one is light-weight FPGA hardware-based cipher algorithm and the other is secret cipher share algorithm. In [33], the authors proposed a D2D-assist data transmission protocol to guarantee the confidentiality and integrity of the medical data transmission in IoMT. This protocol is designed based on certificateless generalized signcryption technique.

Table II summarizes the related studies on incumbent security schemes for IoMT. The current security schemes are effective for data manage layer and medical server layer in the 3-tier IoMT healthcare architecture, where the powerful computing facilities can support computation-complicated and energy-consumed tasks such as encryption, decryption and data analytics. However, the security of data collection layer in IoMT is vulnerable in contrast to data manage layer and medical server layer. Due to the extensive amount of medical data generated in IoMT, even light-weight encryption methods

TABLE II
CURRENT SECURITY SCHEMES FOR IOMT

References	Objectives	Approach	Data collection layer	Data management layer	Medical server layer
[20]	Designing a lightweight glass-breaking access control system for IoMT	Access control	×	×	✓
[21]	Designing a self-adaptive access control mechanism for IoMT data storage system	Access control	×	×	✓
[22]	Proposing a privacy-aware IoMT access control system	Access control	×	×	✓
[23]	Proposing a practical data collection framework of IoMT to prevent collusion attacks and data leakage	Data collection, access control	×	✓	✓
[24]	Proposing an IoMT storage system to verify the identity of patient and the integrity of patients' data	ID authentication	×	✓	×
[25]	Proposing a lightweight authentication and ownership transfer protocol	ID authentication, access control	×	✓	✓
[26]	Proposing an authentication and authorization architecture where the mobility of IoMT is considered	ID authentication	✓	✓	✓
[27]	Proposing an privacy-aware aggregate authentication and access control mechanism for IoMT system	ID authentication, access control	×	✓	✓
[28]	Designing an update mechanism to update the authentication keys and session keys	ID authentication	×	×	✓
[29]	Designing an anonymous authentication scheme to prevent the authenticated patients from untrusted authentication server	ID authentication	×	✓	×
[30]	Designing a mutual authentication scheme with a lattice-based secure cryptosystem	ID authentication, data encryption	×	✓	✓
[31]	Proposing a group send-receive model based key distribution scheme to enhance the security of data transmission	Data encryption	✓	×	✓
[32]	Proposing a secure data collection scheme to guarantee the security of data acquisition and data transmission	Data encryption	✓	✓	×
[33]	Proposing a light-weight data transmission protocol to guarantee the security and primacy of D2D-assist IoMT system	Data encryption	✓	✓	×

will lead to the significant cost at resource-strained medical sensors. Meanwhile, the communication delays introduced by encryption methods may be disastrous for patients especially in emergency situations. Therefore, the current access control, data encryption and authentication mechanisms may not be feasible for securing the data collection layer due to the limited computational capability, memory space and energy supply of the medical sensors.

C. Challenges in security schemes of IoMT

The security challenges in IoMT system may exhibit in all the layers in the three-layer IoMT architecture while the security vulnerabilities at data collection layer are more serious than other two layers. The limitations of medical sensors in computational capability, memory space and energy supply are the main root cause for security vulnerabilities. In addition, the characteristics of medical sensors in variety and mobility lead to the extra difficulty for designing the feasible security schemes.

Medical sensors usually have small form factors (e.g., size and volume). On the one hand, the portable size of medical sensors brings the convenience of medical applications and reduce the cost of sensors. However, the portability of medical sensors, on the other hand, also leads to the limited computing capability, memory space and power capacity. For example, their memory is not enough to perform complicated security protocols, because it will take a long time to perform complex computing operations and lead to significant delay in data transmission, which is nevertheless dangerous for patients. Therefore, most of the current security algorithms are not suitable for normal operation under the condition of limited resources. The security scheme suitable for this device should occupy as few computing and storage resources as possible, and the requirements for the computing power and storage space of the medical sensors should be low enough while not affecting the operation of the sensors.

Although medical sensors have a certain processing capacity, they will choose to use less energy in most cases due to the limited battery power. When there is no critical information to process, they will run at a lower CPU speed to save energy. When it is not necessary to report sensor readings, such devices will turning on power saving mode to save energy. In addition, for some chips (i.e., ICs) implanted into the human body, replacing them for the lack of power will result in both pain and high cost. Therefore, the energy constraint of medical sensor leads to the design challenges of the security schemes.

There are various types of medical sensors, from mature PC devices to RFID tags, and even chips embedded in the body. The computing capability, function, memory, and embedded software of each type of sensor are different. Therefore, designing a security scheme that can accommodate even the devices with weakest capability is another challenge.

In general, medical sensors are not static but mobile. The mobility of medical sensors improves the applicability of IoMT. For example, patients can conduct physical exercises activities in restricted medical area while being continuously monitored. In addition, mobility enables patients to move from their living rooms to other rooms for medical examination without interrupting the continuously medical monitoring. In addition, medical sensors may connect or leave the IoMT network at any moment, thereby leading to the dynamic changes of the network topology accompanied by difficulties in the central management or secret key distribution. Therefore, it is also a serious challenge to design a security scheme that satisfies the mobility requirement.

III. Application of Fri-jam scheme in IoMT

The main idea of Fri-jam schemes is to introduce a certain number of friendly jammers to wireless networks to produce jamming signal to the transmission channels to prevent the eavesdroppers from successfully wiretapping the legitimate transmissions. In Fri-jam schemes, there is no requirement of computing capability, memory space and energy supply at medical sensors. Even those medical sensors with the weakest capability can be protected by friendly jammers. In addition, Fri-jam schemes can also be applied to mobile scenarios of IoMT, where the mobility of medical sensors has little impact on the performance of Fri-jam schemes as long as their mobility is limited in a finite area. Moreover, friendly jammers can be switched off to save the energy when there is no sensitive medical data transmissions to be protected in the IoMT. Therefore, Fri-jam schemes are also flexible to be applied to diverse scenarios. In this section, we introduce the applications of Fri-jam schemes in IoMT. Specifically, we first introduce the system of Fri-jam based IoMT. We next quantify the security of Fri-jam schemes to IoMT. At last, we summarize the researches on integration of Fri-jam methods with other techniques to mitigate the interference on legitimate communication.

A. System Model of Fri-jam Schemes in IoMT

The general IoMT scenario is illustrated in Figure 2, where multiple medical sensors intend to transmit confidential physiological data of patients to the corresponding mobile devices in the presence of eavesdroppers. We assume the eavesdropper is passive and non-colluding all the time, they attempt to wiretap the messages sent by medical sensors. This assumption is reasonable since it is easy to discover and locate the eavesdroppers if the eavesdroppers are active in transmission.

In order to protect the communication security of wireless network, we deploy friendly jammers at a boundary around the data transmission region in this network to emit jamming signals to prevent eavesdroppers from successfully decoding the legitimate messages. In this section, each device in the network is equipped with a single omnidirectional antenna. The number of medical sensors and the number of friendly jammers are denoted by N_T and N_J, respectively. The medical sensors are denoted by $\{t_0, t_1, \dots, t_{N_T-1}\}$ and the friendly jammers are denoted by $\{j_1, j_2, \dots, j_{N_T}\}$. Without loss of generality, we focus on the transmission link between medical sensor t_0 and mobile device r_0 as shown in Figure 2. The information signal transmitted from transmitter t_0 may potentially be eavesdropped by an eavesdropper E. When the large-scale fading is considered in the wireless channels [37], [48], [49], the received signal at the desired mobile device r_0 is given by

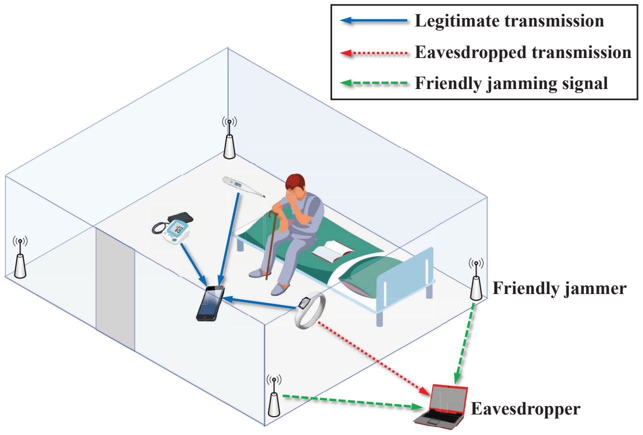


Fig. 2. Application scenario of Fri-jam scheme in IoMT.

$$y_{r_0} = \frac{\sqrt{P_T} h_{r0} x_0}{d_{r0}^{\alpha/2}} + \sum_{n=1}^{N_T-1} \frac{\sqrt{P_T} h_{rn} x_n}{d_{rn}^{\alpha/2}} + \sum_{m=1}^{N_J} \frac{\sqrt{P_J} h_{rm} z_m}{d_{rm}^{\alpha/2}} + \mathbf{n}_0, \tag{1}$$

where P_T is the transmitting power of medical sensors, P_J is the transmitting power of friendly jammers, h_{rn} denotes fading coefficients of the channel between mobile device r_0 and medical sensor t_n, h_{rm} denotes fading coefficients of the channel between mobile device r_0 and friendly jammer j_m, x_n denotes the information-bearing signal sent by transmitter t_n with unit power where $\mathbb{E}\left[|x_n|^2\right] = 1$, z_m denotes the Fri-jam signals sent by the m-th friendly jammer with unit power where $\mathbb{E}\left[|z_m|^2\right] = 1$, d_{rn} is the Euclidean distance between mobile device r_0 and medical sensor t_n, d_{rm} is the Euclidean distance between mobile device r_0 and friendly jammer j_m, α is the path loss factor, and $\mathbf{n}_0$ denotes the complex additive white Gaussian noise.

Similarly, the received signal at the eavesdropper E is given by

$$y_e = \frac{\sqrt{P_T} h_{ej} x_0}{d_{e0}^{\alpha/2}} + \sum_{n=1}^{N_T-1} \frac{\sqrt{P_T} h_{en} x_n}{d_{en}^{\alpha/2}} + \sum_{m=1}^{N_J} \frac{\sqrt{P_J} h_{em} z_m}{d_{em}^{\alpha/2}} + \mathbf{n}_e, \tag{2}$$

where d_{en} is the Euclidean distance between eavesdropper E and medical sensor t_n, d_{em} is the Euclidean distance between eavesdropper E and friendly jammer j_m, $\mathbf{n}_e$ denote complex additive white Gaussian noise.

After deriving the received signal at a mobile device (or an IoT gateway), we can calculate the SINR, which is closely related with performance metrics of information security. The

SINR of desired edge server r_0 [50] is given by

$$\gamma_{r_0} = \frac{P_T h_{r0}^2 d_{r0}^{-\alpha}}{\sigma^2 + I_{tr} + I_{jr}}, \tag{3}$$

where $I_{tr} = \sum_{n=1}^{N_T-1} P_T h_{rn}^2 d_{rn}^{-\alpha}$ represents the cumulative interference from medical sensors to mobile device r_0, $I_{jr} = \sum_{m=1}^{N_J} P_J h_{rm}^2 d_{rm}^{-\alpha}$ represents the cumulative interference from friendly jammers to mobile device r_0.

The SINR at the eavesdropper is given by

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

where $I_{te} = \sum_{n=1}^{N_T-1} P_T h_{en}^2 d_{en}^{-\alpha}$ represents the cumulative interference from medical sensors to eavesdropper E, $I_{je} = \sum_{m=1}^{N_J} P_J h_{em}^2 d_{em}^{-\alpha}$ represents the cumulative interference from friendly jammers to eavesdropper E.

B. Security Analysis of Fri-jam Schemes

We next introduce the common performance metrics of communication security in Fri-jam aided wireless networks.

1) Secrecy Capacity/Rate: In physical layer security, a principal communication security metric is *secrecy capacity*, which is used to describe the largest amount of information that can be confidentially communicated between a legitimate transmitter and a legitimate receiver from the information-theoretic secrecy perspective.

Specifically, the definition of secrecy capacity is the difference between the legitimate link capacity and the eavesdropping link capacity [51]–[54], where the legitimate link capacity is the capacity between a legitimate transmitter and a legitimate receiver, the eavesdropping link capacity is the capacity between the legitimate transmitter to the eavesdropper. The secrecy capacity denoted by C_s is expressed as follows

$$C_s \triangleq [C_r - C_e]^+, \tag{5}$$

where $C_r = \log_2(1+\gamma_r)$ denotes the legitimate link capacity and $C_e = \log_2(1+\gamma_e)$ denotes the eavesdropping link capacity. The difference between two capacities essentially determines the secrecy capacity.

In practice, the value of γ_e depends on the information decoding sensitivity at an eavesdropper. When γ_e decreases, the less information can be wiretapped by the eavesdropper. Once γ_e is below the information decoding sensitivity, no information can be wiretapped by the eavesdropper.

The physical meaning of secrecy capacity can be expressed as the upper bound of the transmission rate which satisfy the condition of reliability and secrecy.

2) PCO and PSO: For the assumption that eavesdroppers are passive and seldom transmit signals, the instantaneous knowledge of γ_e is difficult to be obtained. The perfect secrecy capacity is unavailable if the instantaneous knowledge of γ_e is absent. Therefore, research studies employ probability of the connection outage (PCO) and probability of the secrecy outage (PSO) to measure the security [49], [55], [56]. PCO and PSO are corresponding to the connection outage (CO) event and the secrecy outage (SO) event, respectively. The CO event occurs when the receiving SINR at the legitimate receiver is lower than a given threshold γ_{th} while the SO event occurs when the receiving SINR at the eavesdropper is above a given threshold γ_{th}^e [57]–[59].

Mathematically, the PCO can be calculated as

$$P_{CO} = \Pr(\gamma_r < \gamma_{th}) = F_{\gamma_D}(\gamma_{th}), \tag{6}$$

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

Similarly, the PSO can be calculated as

$$P_{SO} = \Pr(\gamma_e \geq \gamma_{th}^e) = 1 - F_{\gamma_E}(\gamma_{th}^e). \tag{7}$$

To derive the PSO, the statistical knowledge instead of instantaneous knowledge of γ_e is required. The physical meaning of PCO is the probability of a unsuccessful transmission, while the physical meaning of PSO is the probability that the transmission fails to reach the perfect secrecy. The goal of introducing Fri-jam signals to wireless networks is to reduce the PSO while maintaining the PCO low enough, i.e., to enhance the security along with the reliability guarantee of wireless communication.

3) Secrecy Outage Region: The placement strategies of friendly jammers are investigated to improve the secrecy efficiency in recent studies including [48], [60], [61]. In these schemes, the area of secure regions and unsecured regions are secrecy metrics to evaluate the transmission security of the network.

In particular, in [48], secrecy outage region (SOR) is proposed to investigate the influence of geometric locations of eavesdroppers on secrecy outage event. In [60], the metric audible region is a region in which any eavesdropper located inside will lead to $\gamma_e \geq \gamma_{th}^e$ if no jammer is introduced; jamming region is a region where any eavesdropper located inside will lead to $\gamma_e < \gamma_{th}^e$ if jamming signal is introduced. In [61] the authors proposed Fri-jam strategy based on their defined jamming region and masking region. The physical meaning of secrecy outage region is the amount of area where secrecy outage event occurs.

Summary. The above security metrics have been widely adopted in recent studies. In particular, the secrecy capacity, secrecy rate and probability of secrecy outage mainly focus on the analysis from the perspective of information theory while secrecy outage region concentrate on the locations of the eavesdroppers. From the illustration of performance metrics, we find the information security of wireless network heavily depends on the SINR of eavesdropper and that of legitimate receiver.

C. Integration of Fri-jam Schemes with Other Techniques in IoMT

Fri-jam is a promising approach to protect the confidential information of legitimate communications from being wiretapped by eavesdroppers. Nevertheless, from the expressions of SINR at legitimate receiver and at eavesdropper in Eq. (3), we find that the Fri-jam signals also bring interference at legitimate users. Therefore, multiple techniques are investigated to integrate with Fri-jam schemes for the purpose of mitigating the impact of jamming signals on legitimate transmissions or to make sufficient usage of Fri-jam signals (e.g., harvesting energy).

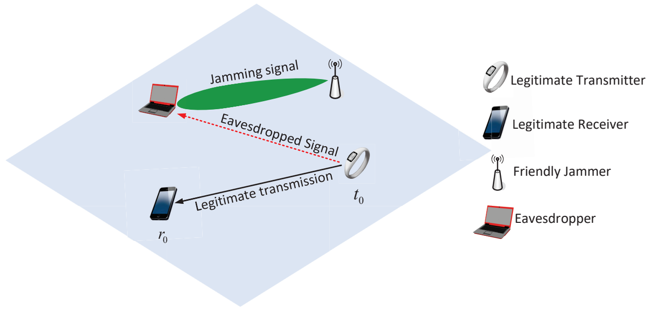


Fig. 3. Integration of Fri-jam with Beamforming.

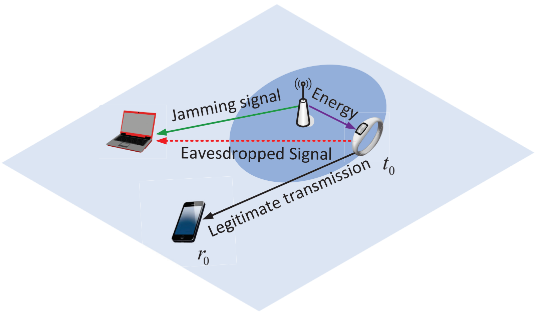


Fig. 4. Integration of Fri-jam with SWIPT.

1) Integration of Fri-jam with Beamforming: Compared with conventional omni-directional transmissions, beamforming concentrates the signals to the desired direction by taking advantage of spatial degrees of freedom. Figure 3 shows a scenario in which Fri-jam is integrated with beamforming techniques. In this scenario, the power of Fri-jam signal is concentrated on the eavesdropper so that the interference of the friendly jammer on legitimate transmission is reduced.

Several recent studies attempt to investigate the joint impact of beamforming and Fri-jam. In particular, the influence of beamforming and Fri-jam on large scale spectrum sharing networks was investigated in [39], in which the exact analytical expressions of average secrecy rate and SOP are derived and the results are helpful for designing the optimal power allocation strategy. Meanwhile, the research [51] investigated Fri-jam aided beamforming scheme in multi-input single-output multi-eavesdropper (MISO-ME) wiretap channel. Their results on secrecy outage proved that null-space Fri-jam is an optimal solution when the number of antennas equipped by eavesdropper is arbitrary. In [62], the authors jointly designed Fri-jam aided beamforming and power splitting technique to protect the security of legitimate data transmission and minimize the transmitting power in a MISO CR network with SWIPT. The secrecy rate constraint, interference constraint and EH constraint are considered in this design. Furthermore, Nguyen *et al.* [63] proposed the joint optimization strategy of the information signals and beamforming of Fri-jam signals to maximize the secrecy rate considering MISO broadcast channel in an underlay cognitive radio network (CRN). In this optimal beamforming design, the secondary user eliminated the interference of friendly jammers with zero-forcing method.

In the investigation of joint beamforming and Fri-jam schemes, the Channel State Information (CSI) is important and it is assumed to be known or unknown. In this aspect, the article [64] proposed a semi-adaptive scheme, where the secrecy rate will be adaptively adjusted following the CSI of legitimate channel under the fixed transmission rate. In [65], the authors investigated secure transmission designs to jointly optimize the beamforming vector and the covariance matrix of jamming signals. In this research, authors also analyze two different cases of eavesdroppers' CSI being known and unknown. Moreover, the article [66] investigate to maximize the secrecy rate in the worst-case in a Fri-jam aided amplify-and-forward relay network when the CSI of eavesdroppers is imperfect. Zhang *et al.* [67] proposed a Fri-jam aided optimal beamforming scheme in a two-layer physical layer security model. This model can be used for protecting the security of higher level information while satisfying the low-level information secrecy rate constraint.

2) Integration of Fri-jam with SWIPT: As one of the most promising technologies to extend the operation time of low-power networks with constrained energy (e.g., IoMT), SWIPT enables the devices to obtain information and acquire energy from the same signal [68]–[70]. On the other hand, Fri-jam schemes are suitable to wireless networks in which wireless devices are limited in low battery power and poor computational capability so that the computational-complex encryption algorithms cannot be used. The integration of SWIPT with Fri-jam may potentially improve the security of wireless networks while extending life time of wireless networks [71].

Figure 4 illustrates a scenario of integrating Fri-jam with SWIPT. In this scenario, friendly jammers also serve as power providers for legitimate transmitters. When the legitimate transmitters are located close to the friendly jammers, the energy in the Fri-jam signals is harvested by legitimate transmitters. In addition, the legitimate transmitters can also act as power providers for friendly jammers, as in [70], [72]. The related studies of integration of Fri-jam with SWIPT can be roughly categorized into two types according to their transmission protocols.

(a) Harvest-then-jam protocols. In [70] and [72], friendly jammers are considered as energy-constrained nodes without embedded power supply, they firstly harvest radio frequency (RF) energy from emitted by the legitimate transmitters according to the proposed protocols, and then utilize the acquired energy to interfere with the eavesdropper. Specifically, the secrecy performances of two types of legitimate receivers are studied in [72], where the first type of receivers could cancel the jamming interference with prior knowledge while the other type of receivers could not.

In [49], the authors proposed a SWIPT based full-duplex self-jamming (SWIPT-FDSJ) scheme in energy-constrained SWIPT networks. In this scheme, the legitimate receiver first harvests energy from legitimate transmitters with the maximal ratio transmission protocol and then sends jamming signals to prevent the eavesdropping behaviour. Compared with no self-jamming scheme with half-duplexity, SWIPT-FDSJ scheme promoted the COP and SOP performance simultaneously,

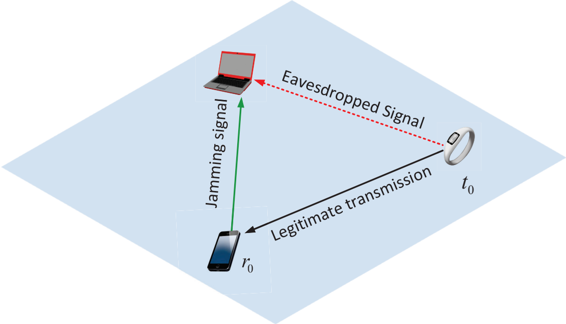


Fig. 5. Integration of Fri-jam with Full duplex.

leading to the improvement of secrecy throughput.

In a Fri-jam aided secure OFDMA system with SWIPT, [69] designed a Fri-jam aided transmission strategy in frequency-domain to optimally allocate both power and subcarrier to derive the maximal weighted sum value of information receivers' secrecy rate. This strategy is designed on the condition of individual energy receivers' minimum harvested power. The work of [73] investigates a wireless-powered sensor network, in which the access point transmits energy signals to supply the power to sensor nodes and friendly jammer. With the harvested energy, friendly jammer then sends jamming signals to confuse eavesdropper. In this research, the security performance of wireless sensor network considering Nakagami-m channels are studied since the transmission distance in wireless sensor network is short.

In a multiple-Input Single-Output based non-orthogonal multiple access (MISO-NOMA) cognitive radio network relying on SWIPT, Zhou *et al.* [74] proposed a Fri-jam aided cooperative jamming scheme to enhance the communication security of the primary network. In this work, the practical non-linear energy harvesting model was considered, rather than the ideally linear energy harvesting model. The non-linear EH model is also employed by the Fri-jam aided multi-cell coordinated beamforming scheme to secure SWIPT transmitting schemes in [68]. The centralized and distributed versions were individually designed to guarantee the security of legitimate users' information and the requirements of energy harvesting.

(b) Harvest-then-relay-and-jam protocols. In [75] and [76], the harvest-then-relay-and-jam protocols are employed for the wireless transmission. In the first transmission phase, each relay receives the wireless information and wireless power simultaneously from legitimate transmitters. In the second transmission phase, the relay nodes split the harvested power into two parts: one part is used to relay the legitimate information signal and another part is used to transmit the Fri-jam signals to the eavesdroppers. Specifically, semi-definite relaxation-based algorithms are designed to derive the maximal value of the achievable secrecy rate at the legitimate receiver as in [75], [76]. In particular, in [75], the centralized case with global CSI and the distributed case with only local CSI of relays are investigated. The joint optimization of covariance matrix of Fri-jam and the beamforming vector when the CSI is perfect and the worst-case robust optimization when the CSI is imperfect is investigated in [76].

In [52], Lee *et al.* investigated a Fri-jam aided wireless-powered relay network, where the legitimate receivers act as friendly jammers and relay nodes receive the energy from both legitimate transmitters and legitimate receivers to forward data signal simultaneously. Harnessing power splitting and time switching techniques, Lee *et al.* proposed two relaying schemes which are effective for practical environments under the condition that the CSI of eavesdropper is unknown.

3) Integration of Fri-jam with Full duplexity: Full duplex (FD) technology has attracted much attention in physical layer security due to the high spectral efficiency compare with the conventional half duplex (HD) communications. Figure 5 shows a scenario that Fri-jam is integrated with full duplex communications. In this case, the FD legitimate receiver transmits Fri-jam signals and receives the information signals simultaneously.

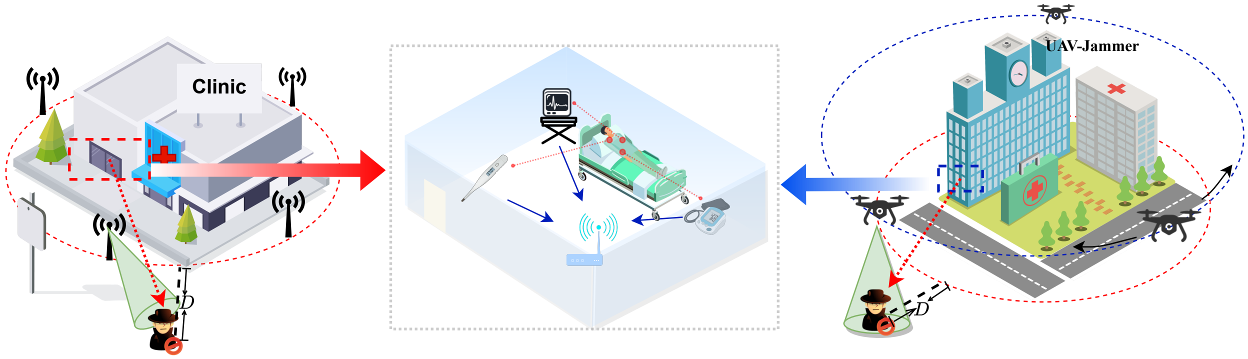
Integrating Fri-jam schemes with FD technology has been studied in recent research studies. In [37], Zheng *et al.* studied a decentralized wireless network where the FD legitimate receivers generate jamming signals to confound eavesdroppers and receive the signals from legitimate transmitters simultaneously. In this network, a spatial Successive Interference Cancellation (SIC) strategy for deploying the FD receivers optimally is proposed to derive the maximal value of network-wide secrecy. The accurate integral expressions and analytical approximations for COP and SOP are provided based on a stochastic geometry framework. In [77], a precoded Fri-jam signal injection scheme is designed for an FD MIMO relay channel. In this scheme, the friendly jammer is an FD device and the ambient radio-frequency transmissions supply the power for the friendly jammer.

Hu *et al.* [78] proposed a two-phase Fri-jam aided secure transmission scheme. In the first phase of this scheme, a FD transmitter transmits Fri-jam signals and receives another independent Fri-jam signals from a HD receiver simultaneously. In the second phase of this scheme, the transmitter superimposes the confidential information signal with the received Fri-jam signals from the receiver, then transmits the composed signals which can be decoded by the receiver only while the eavesdropper cannot. The average secrecy rate and the SOP of this scheme are analyzed under the Rayleigh block-fading channel.

Bi and Chen [70] considered to secure the communication with a wireless powered FD friendly jammer, which harvests energy and generates jamming signals simultaneously. In this work, an accumulate-and-jam protocol is designed to maximize the amount of harvested energy of the FD jammer. Similarly, Li [79] proposed Fri-jam aided precoding strategy, where the multiple-antenna legitimate transmitter transmits confidential information signals and the Fri-jam signals simultaneously.

IV. Case studies of Fri-jam scheme in IoMT

Fri-jam schemes have been widely proposed to safeguard transmissions in wireless networks. Moreover, these Fri-jam schemes can also be adopted to protect data transmissions in



(a)
Beamforming-assisted Fri-jam

(b)
UAV-assisted Fri-jam

Fig. 6. Application of Fri-jam schemes.

IoMT. As shown in Figure 6, there is usually a protection region in IoMT (e.g., the entrance requiring permissions), where the eavesdropper cannot enter. Meanwhile, if the eavesdroppers appear inside the medical-care centers (e.g., a clinic or a hospital), they can be easily identified. Therefore, eavesdroppers are typically restricted externally while they can still wiretap the confidential information due to the openness of wireless medium.

In such a scenario, we only need to consider eavesdroppers who are outside the medical center. Herein, we present two specific case studies to introduce applications of Fri-jam schemes in IoMT.

A. *Case I: Beamforming-assisted Fri-jam*

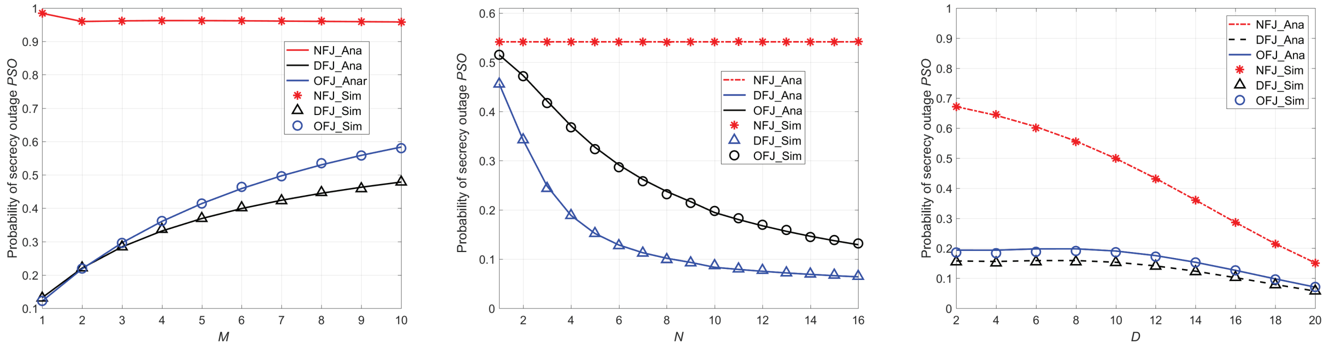
Firstly, we introduce a scheme integrated with beamforming technique firstly introduced in [80]. In particular, we consider that the medical center is surrounded by a finite circular region as shown in Figure 6(a). In this data transmission region, multiple medical sensors transmit physiological data of patients to mobile devices. The distribution of medical sensors are assumed to follow the Poisson point process (PPP), and the expectation number of medical sensors is M. The mobile devices which receive the collected data from medical sensors are assumed to locate at the center of this data transmission region. In this scenario, an eavesdropper E is trying to eavesdrop the sensitive medical information in the data transmission region. The distance between this eavesdropper and the circular boundary of data transmission region surrounded by friendly jammers is D.

Aiming at protecting the medical data of patients from being wiretapped by eavesdropper, we introduce N friendly jammers into this data transmission region. The placement strategy of friendly jammers are shown in Figure 6(a), where we place friendly jammers at the circular boundary of the data transmission region. In this case, the mobile device, the medical sensors and the eavesdropper emit signals omnidirectionally. With regard to friendly jammers, two jamming strategies are designed for this scenario: (i) OFJ scheme, where friendly jammers emit signals omnidirectionally; (ii) DFJ scheme, where friendly jammers emit directional signals with beamforming technique. A scheme named by NFJ is designed as a comparison group, in which no deployment of Fri-jam is conducted.

After deriving PSO via stochastic geometric approaches, we can obtain PSO of the above schemes. Meanwhile, we have also conducted simulations to verify the effectiveness of our analytical model. From Figure 7(a), we can find that the introduction of friendly jammers into the data transmission region will result in the reduction on PSO. For instance, when the expectation number of medical sensors M is 4, in contrast to the NFJ scheme, the decrease of PSO with OFJ scheme is 0.5988 (i.e., 62.21 $\%$ decreased). When M remains to be 4, in contrast to the NFJ scheme, the decrease of PSO with DFJ scheme is 0.6304 (i.e., 65.50% decreased). Therefore, the DFJ scheme results in the more significant reduction of PSO compared with OFJ scheme. This result indicates that applying Fri-jam schemes in the network can mitigate the success probability of eavesdropping behaviour.

As shown in Figure 7(b), the curve of PSO drops rapidly when the parameter N increases. In particular, when friendly jammers are using beamforming technique (i.e., in DFJ scheme), the decrease of PSO is even more significant. This result is helpful in verifying the effectiveness of Fri-jam schemes (i.e., OFJ and DFJ schemes) in reducing the PSO of IoMT. The results of Figure 7(b) imply that deploying too many friendly jammers in the IoMT may be unnecessary, especially in the DFJ scheme. In DFJ scheme, the PSO reduces significantly as long as a few friendly jammers is introduced. For instance, when the number of friendly jammers N is 6, in contrast to NFJ scheme, the decrease of PSO in the DFJ scheme is 0.3937 (i.e., 72.72% reduction).

Another set of simulation results are given in Figure 7(c), where the PSO values of different schemes are compared in terms of the varied distance between the eavesdropper and the network boundary denoted by D. As presented in Figure 7(c), three schemes have the rapidly-decreased PSO values. This phenomenon becomes significant especially in the NFJ scheme. This result indicates that the impact of path loss is more obvious on legitimate signal than on jamming signal.



(a) Number of medical sensors M varies from 1 to 10

(b) Number of friendly jammers N ranges from 1 to 16.

(c) Distance D varies from 2 to 20.

Fig. 7. Probability of secrecy outage (PSO) for Fri-jam scheme.

Figure 7(c) also verified the effectiveness of Fri-jam schemes in reducing the PSO of IoMT compared with the NFJ scheme.

B. Case II: UAV-assisted Fri-jam

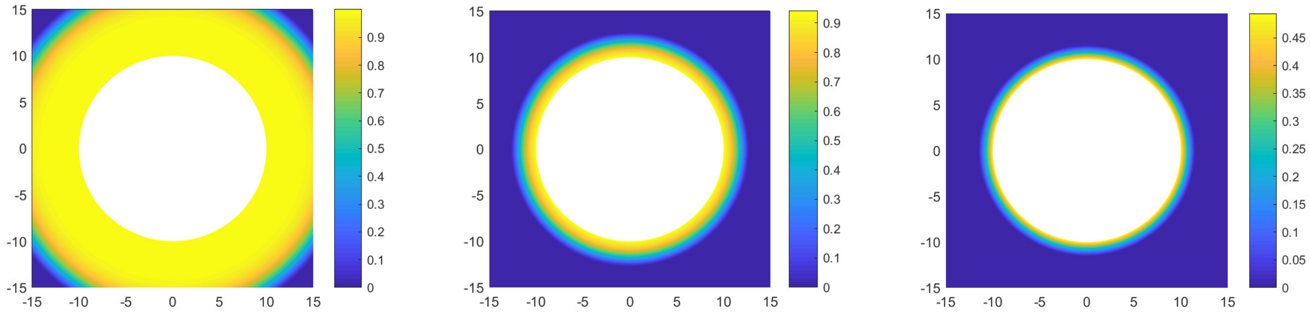
Recently, unmanned aerial vehicles (UAVs) have been widely applied in wireless communications to substitute some disrupted transmitting nodes to extend the network coverage or serve as relays [81]. UAVs can also be used as friendly jammers. In particular, a UAV-assisted Fri-jam scheme is introduced in [82], where UAVs are considered as jammers to disturb the eavesdropper. In particular, as depicted in Figure 6(b), a UAV jammer flies surrounding the protection region. A directional antenna is mounted at each UAV jammer. The jamming signal is emitted by the directional antenna from the UAV jammer toward ground to disturb the eavesdropper. Thanks to the mobility of UAV, the jamming region can flexibly move to cover the eavesdropper. Next, we evaluate the anti-eavesdropping performance of the UAV-assisted Fri-jam scheme by the PSO.

The PSO can be used to evaluate the probability of wiretapping activity for each location of the eavesdropper. Figure 8 plots PSO for UAV-assisted Fri-jam (U-FJ) scheme deployed in IoMT. As shown in Figure 8, the darkest blue stands for the lowest PSO, whereas the lightest yellow stands for the highest PSO. The color from yellow to blue implies that the intensity of the PSO decreases. The inner white circular area is the protection region where the legitimate IoMT transmissions are conducted. Figure 8(a) illustrates the PSO for IoMT when there is no UAV jammer deployed. We can find that most of the surrounding area outside the protection region are in yellow, implying that the legitimate communications in IoMT have high chance to be eavesdropped. Both Figure 8(b) and Figure 8(c) show the PSO for IoMT when UAV jammer is deployed. In particular, in Figure 8(b), the ratio of transmit power P_t of IoMT to jamming power P_j of UAV jammer is $10 : 1$. It implies that, compared with the power consumption of transmissions by medical sensors, the UAV jammer consumes less. Moreover, we find that most of the areas outside the protection region are changed from yellow to blue. It means that the eavesdropping risks are significantly reduced, although the jamming power is small. As shown in Figure 8(c), the yellow-covered areas are further reduced as the jamming power is increased to the same value of transmit power of IoMT. Consequently, we can conclude that U-FJ scheme can effectively reduce the PSO in IoMT.

V. Conclusions and Future Work

Traditional medical treatment methods requiring extensive resources to be concentrated on medical agencies (e.g., hospitals and clinics) cannot cater for the rising demands on healthcare especially for aging population or outbreak of epidemic diseases. The advent of IoMT can complement traditional healthcare services in a flexible and convenient manner. However, both security and privacy become the main concerns of IoMT due to vulnerabilities of IoMT devices, which have the limited computational capability, memory space and power capacity. Therefore, conventional cryptographic approaches may not be feasible for IoMT devices. Different from conventional cryptographic security countermeasures which have a strong requirement on computational capability of end devices, Fri-jam schemes have neither specific requirements on end devices nor modifications on existing network infrastructures. Therefore, there are a number studies on Fri-jam schemes in wireless networks.

In this paper, we investigate the usage of Fri-jam schemes in IoMT. In particular, we illustrated the three-layer architecture of IoMT system consisting of data collection layer, data management layer and medical server layer. We then present some current security schemes and analyzed the main security challenges of IoMT. We next propose to use Fri-jam schemes to protect the confidential medical data of patients collected by medical sensors from being eavesdropped. The secrecy performance metrics which are commonly used to evaluate the information security are also presented. Moreover, the integration of Fri-jam schemes with other communication technologies such as SWIPT, beamforming and full duplexity is also discussed. In addition, we introduce two case studies of Fri-jam schemes in IoMT. From the analytical results of these two case studies, we find that the Fri-jam method will significantly reduce the probability of secrecy outage while causing no significant influence on legitimate transmission as



(a) Without UAV jammers

(b) With UAV jammers ($P_t : Pj = 10 : 1$).

(c) With UAV jammers ($P_t : Pj = 1 : 1$).

Fig. 8. PSO for UAV-assisted Fri-jam scheme (better viewed in color).

long as friendly jammers are properly placed. We believe that the integration of Fri-jam schemes with other communication technologies (beamforming and full duplexity) can further improve the performance.

Future work will be focus on further improving the security performance of IoMT systems. Another approach to control the propagation environment to ensure that the eavesdropper does not get a change to receive the legitimate signals is to introduce intelligent reflective surfaces (IRS) [83], [84]. In line with the jamming principal, this solution will enable the walls to change their reflective and absorption properties to ensure that the wireless signal is appropriately contained within a secure environment. This approach is also a potential solution to the security challenges in data collection layer of IoMT systems since most of the legitimate communications in this layer are within an indoor environment [11]. In the future, we will explore the integration of Fri-jam schemes with IRS schemes and the joint consideration of these two schemes according to the specific IoMT communication environment.

References

[1] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. u. Rasool, and W. Dou, “Complementing iot services through software defined networking and edge computing: A comprehensive survey (early access),” *IEEE Communications Surveys Tutorials*, pp. 1–1, 2020.

[2] H. Najmul, G. Saira, A. Ejaz, Y. Ibrar, and I. Muhammad, “The role of edge computing in internet of things,” *IEEE Communications Magazine*, 2018.

[3] A. K. Sangaiah, D. V. Medhane, T. Han, M. S. Hossain, and G. Muhammad, “Enforcing position-based confidentiality with machine learning paradigm through mobile edge computing in real-time industrial informatics,” *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2019.

[4] R. M. Imran, I. Muhammad, and X. Guandong, “Big data analytics for preventive medicine,” *Neural Computing & Applications*, 2019.

[5] A. K. Sangaiah, J. S. A. Dhanaraj, P. Mohandas, and A. Castiglione, “Cognitive iot system with intelligence techniques in sustainable computing environment,” *Computer Communications*, 2020.

[6] L. Syed, S. Jabeen, S. Manimala, and A. Alsaeedi, “Smart healthcare framework for ambient assisted living using iomt and big data analytics techniques,” *Future Generation Computer Systems*, vol. 101, pp. 136 – 151, 2019.

[7] M. Asif-Ur-Rahman, F. Afsana, M. Mahmud, M. S. Kaiser, M. R. Ahmed, O. Kaiwartya, and A. James-Taylor, “Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4049–4062, 2019.

[8] J. H. Abawajy and M. M. Hassan, “Federated internet of things and cloud computing pervasive patient health monitoring system,” *IEEE Communications Magazine*, vol. 55, no. 1, pp. 48–53, 2017.

[9] T. Han, L. Zhang, S. Pirbhulal, W. Wu, and V. Albuquerque, “A novel cluster head selection technique for edge-computing based iomt systems,” *Computer Networks*, vol. 158, pp. 114 – 122, 2019.

[10] A. K. Sangaiah, M. Arumugam, and G. B. Bian, “An intelligent learning approach for improving ecg signal classification and arrhythmia analysis,” *Artificial Intelligence in Medicine*, vol. 103, 2019.

[11] W. Taylor, S. A. Shah, K. Dashtipour, A. Zahid, Q. H. Abbasi, and M. A. Imran, “An intelligent non-invasive real-time human activity recognition system for next-generation healthcare,” *Sensors*, vol. 20, no. 5, 2020.

[12] Y. Fu and J. Guo, “Blood cholesterol monitoring with smartphone as miniaturized electrochemical analyzer for cardiovascular disease prevention,” *IEEE Transactions on Biomedical Circuits and Systems*, vol. 12, no. 4, pp. 784–790, 2018.

[13] H. Ren, H. Jin, C. Chen, H. Ghayvat, and W. Chen, “A novel cardiac auscultation monitoring system based on wireless sensing for healthcare,” *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 6, pp. 1–12, 2018.

[14] F. Wu *et al.*, “A new coronavirus associated with human respiratory disease in china,” *Nature*, vol. 579, p. 265–269, 2020. [Online]. Available: https://doi.org/10.1038/s41586-020-2008-3

[15] J.-P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, “Securing internet of medical things systems: Limitations, issues and recommendations,” *Future Generation Computer Systems*, vol. 105, pp. 581 – 606, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X19305680

[16] R. Somasundaram and M. Thirugnanam, “Review of security challenges in healthcare internet of things,” *Wireless Networks*, pp. 1–7, 2020.

[17] P. Sandeep, S. Oluwarotimi, W. Wanqing, K. Arun, and L. Guanglin, “A joint resource-aware and medical data security framework for wearable healthcare systems,” *Future Generation Computer Systems*, vol. 95, 2019.

[18] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin, A. Gani, E. Ahmed, A. S. M. Nainar, N. M. Akim, and M. Imran, “Deep learning and big data technologies for iot security,” *Computer Communications*, vol. 151, pp. 495 – 517, 2020.

[19] Y. Ibrar, A. Ejaz, H. ur Rehman Muhammad, A. A., al-garadi Mohammed, I. Muhammad, and G. Mohsen, “The rise of ransomware and emerging security challenges in the internet of things,” *Computer Networks*, 12 2017.

[20] Y. Yang, X. Liu, and R. Deng, “Lightweight break-glass access control system for healthcare internet-of-things,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3610–3617, 2018.

[21] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, “Privacy-preserving smart iot-based healthcare big data storage and self-adaptive access control system,” *Information Sciences*, vol. 479, pp. 567–592, 2019.

[22] Y. Zhang, D. Zheng, and R. Deng, “Security and privacy in smart health: Efficient policy-hiding attribute-based access control,” *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

[23] E. Luo, M. Bhuiyan, G. Wang, M. Rahman, J. Wu, and M. Atiquzzaman, “Privacyprotector: Privacy-protected patient data collection in iot-based healthcare systems,” *IEEE Communications Magazine*, vol. 56, no. 2, pp. 163–168, 2018.

[24] R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, “Lightweight privacy-preserving identity-based verifiable iot-based health storage system,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8393–8405, 2019.

[25] S. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, “Laco: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in iot,” *Future Generation Computer Systems*, vol. 96, pp. 410 – 424, 2019.

[26] S. Moosavi, T. Gia, E. Nigussie, A. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, “End-to-end security scheme for mobility enabled healthcare internet of things,” *Future Generation Computer Systems*, vol. 64, pp. 108 – 124, 2016.

[27] Y. Zhang, R. Deng, G. Han, and D. Zheng, “Secure smart health with privacy-aware aggregate authentication and access control in internet of things,” *Journal of Network and Computer Applications*, vol. 123, pp. 89 – 100, 2018.

[28] X. Cheng, Z. Zhang, F. Chen, C. Zhao, T. Wang, H. Sun, and C. Huang, “Secure identity authentication of community medical internet of things,” *IEEE Access*, vol. 7, pp. 115 966–115 977, 2019.

[29] A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston, and Y. Zhang, “Anonymous authentication scheme for smart cloud based healthcare applications,” *IEEE Access*, vol. 6, pp. 33 552–33 567, 2018.

[30] R. Chaudhary, A. Jindal, G. Aujla, N. Kumar, A. Das, and N. Saxena, “Lscsh: Lattice-based secure cryptosystem for smart healthcare in smart cities environment,” *IEEE Communications Magazine*, vol. 56, no. 4, pp. 24–32, 2018.

[31] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, “Private and secured medical data transmission and analysis for wireless sensing healthcare system,” *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1227–1237, 2017.

[32] H. Tao, M. Bhuiyan, A. Abdalla, M. Hassan, J. Zain, and T. Hayajneh, “Secured data collection with hardware-based ciphers for iot-based healthcare,” *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 410–420, 2019.

[33] A. Zhang, L. Wang, X. Ye, and X. Lin, “Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 662–675, 2017.

[34] H. Asmaa, Özdemir Suat, T. Ahmet, and C. Fatih, “Security and privacy in medical internet of things and cluster-based wireless sensor networks for health care,” *Journal of Medical Imaging and Health Informatics*, vol. 10, pp. 211–222, 2020.

[35] S. Pirbhulal, N. Pombo, V. Felizardo, N. Garcia, A. H. Sodhro, and S. C. Mukhopadhyay, “Towards machine learning enabled security framework for iot-based healthcare,” in *2019 13th International Conference on Sensing Technology (ICST)*, 2019, pp. 1–6.

[36] K. H. Ali, S. Munam, K. Sangeen, A. Ihsan, and I. Muhammad, “Perception layer security in the internet of things,” *Future Generation Computer Systems*, vol. 100, p. 28, 2019.

[37] T. Zheng, H. Wang, Q. Yang, and M. Lee, “Safeguarding decentralized wireless networks using full-duplex jamming receivers,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 278–292, 2017.

[38] Y. Sarikaya, O. Ercetin, and O. Gurbuz, “Control of cognitive networks with friendly jamming as a service,” *IEEE Transactions on Cognitive Communications and Networking*, vol. 4, no. 2, pp. 299–313, 2018.

[39] Y. Deng, L. Wang, S. Zaidi, J. Yuan, and M. Elkashlan, “Artificial-noise aided secure transmission in large scale spectrum sharing networks,” *IEEE Transactions on Communications*, vol. 64, no. 5, pp. 2116–2129, 2016.

[40] Y. Zhang, M. Qiu, C. Tsai, M. M. Hassan, and A. Alamri, “Health-cps: Healthcare cyber-physical system assisted by cloud and big data,” *IEEE Systems Journal*, vol. 11, no. 1, pp. 88–95, 2017.

[41] R. Cao, Z. Tang, C. Liu, and B. Veeravalli, “A scalable multicloud storage architecture for cloud-supported medical internet of things,” *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1641–1654, 2020.

[42] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdić, “Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine,” *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3810–3822, 2018.

[43] M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, and C. Youn, “Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems,” *IEEE Communications Magazine*, vol. 55, no. 1, pp. 54–61, 2017.

[44] F. Qureshi and S. Krishnan, “Wearable hardware design for the internet of medical things (iomt),” *Sensors*, vol. 18(11), p. 3812, 2018.

[45] S. Mukhopadhyay, “Wearable sensors for human activity monitoring: A review,” *IEEE Sensors Journal*, vol. 15, no. 3, pp. 1321–1330, 2015.

[46] Y. Sun, F. Lo, and B. Lo, “Security and privacy for the internet of medical things enabled healthcare systems: A survey,” *IEEE Access*, vol. 7, pp. 183 339–183 355, 2019.

[47] H.-N. Dai, R. C.-W. Wong, H. Wang, Z. Zheng, and A. V. Vasilakos, “Big data analytics for large scale wireless networks: Challenges and opportunities,” *ACM Computing Surveys*, vol. 52, no. 5, pp. 99:1–36, 2019. [Online]. Available: https://doi.org/10.1145/3337065

[48] J. Wang, J. Lee, F. Wang, and T. Quek, “Jamming-aided secure communication in massive mimo rician channels,” *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6854–6868, 2015.

[49] X. Tang, Y. Cai, Y. Deng, Y. Huang, W. Yang, and W. Yang, “Energy-constrained swipt networks: Enhancing physical layer security with fd self-jamming,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 212–222, 2019.

[50] L. Hu, H. Wen, B. Wu, F. Pan, R. Liao, H. Song, J. Tang, and X. Wang, “Cooperative jamming for physical layer security enhancement in internet of things,” *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 219–228, 2018.

[51] B. Wang, P. Mu, and Z. Li, “Artificial-noise-aided beamforming design in the misome wiretap channel under the secrecy outage probability constraint,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7207–7220, 2017.

[52] K. Lee, J. Hong, H. Choi, and M. Levorato, “Adaptive wireless-powered relaying schemes with cooperative jamming for two-hop secure communication,” *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2793–2803, 2018.

[53] M. Ahmed and L. Bai, “Secrecy capacity of artificial noise aided secure communication in mimo rician channels,” *IEEE Access*, vol. 6, pp. 7921–7929, 2018.

[54] R. Zhao, Y. Huang, W. Wang, and V. Lau, “Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 2537–2551, 2016.

[55] S. Xu, S. Han, W. Meng, Y. Du, and L. He, “Multiple-jammer-aided secure transmission with receiver-side correlation,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, pp. 3093–3103, 2019.

[56] S. Yan, N. Yang, I. Land, R. Malaney, and J. Yuan, “Three artificial-noise-aided secure transmission schemes in wiretap channels,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3669–3673, 2018.

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

[58] X. Hu, X. Zhang, H. Huang, and 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] X. Tang, W. Yang, Y. Cai, W. Yang, and 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.

[60] J. Liu, Z. Liu, Y. Zeng, and J. Ma, “Cooperative jammer placement for physical layer security enhancement,” *IEEE Network*, vol. 30, no. 6, pp. 56–61, 2016.

[61] Z. Liu, J. Liu, N. Kato, J. Ma, and Q. Huang, “On cooperative jamming in wireless networks with eavesdroppers at arbitrary locations,” in *2016 IEEE International Conference on Communications (ICC)*, 2016, pp. 1–6.

[62] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, “Robust an-aided beamforming and power splitting design for secure miso cognitive radio with swipt,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 4, pp. 2450–2464, 2017.

[63] V. Nguyen, T. Duong, O. Dobre, and O. Shin, “Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2609–2623, 2016.

[64] Z. Li, P. Mu, B. Wang, and X. Hu, “Optimal semiadaptive transmission with artificial-noise-aided beamforming in miso wiretap channels,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7021–7035, 2016.

[65] H. Ma, J. Cheng, X. Wang, and P. Ma, “Robust miso beamforming with cooperative jamming for secure transmission from perspectives of qos and secrecy rate,” *IEEE Transactions on Communications*, vol. 66, no. 2, pp. 767–780, 2018.

[66] C. Wang and H. Wang, “Robust joint beamforming and jamming for secure af networks: Low-complexity design,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 2192–2198, 2015.

[67] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Artificial-noise-aided optimal beamforming in layered physical layer security," *IEEE Communications Letters*, vol. 23, no. 1, pp. 72–75, 2019.

[68] Y. Lu, K. Xiong, P. Fan, Z. Zhong, and K. Letaief, "Coordinated beamforming with artificial noise for secure swipt under non-linear eh model: Centralized and distributed designs," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1544–1563, 2018.

[69] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in ofdma systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 3085–3096, 2016.

[70] Y. Bi and H. Chen, "Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1538–1550, 2016.

[71] Y. Liu, J. Xu, and R. Zhang, "Exploiting interference for secrecy wireless information and power transfer," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 133–139, 2018.

[72] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless Powered Cooperative Jamming for Secure OFDM System," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1331–1346, 2018.

[73] G. Hu and Y. Cai, "Analysis and optimization of wireless-powered cooperative jamming for sensor network over nakagami- m fading channels," *IEEE Communications Letters*, vol. 23, no. 5, pp. 926–929, 2019.

[74] F. Zhou, Z. Chu, H. Sun, R. Hu, and L. Hanzo, "Artificial noise aided secure cognitive beamforming for cooperative miso-noma using swipt," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 918–931, 2018.

[75] H. Xing, K. Wong, A. Nallanathan, and R. Zhang, "Wireless Powered Cooperative Jamming for Secrecy Multi-AF Relaying Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 7971–7984, 2016.

[76] H. Xing, K. Wong, Z. Chu, and A. Nallanathan, "To harvest and jam: A paradigm of self-sustaining friendly jammers for secure af relaying," *IEEE Transactions on Signal Processing*, vol. 63, no. 24, pp. 6616–6631, 2015.

[77] A. Shafie, D. Niyato, and N. Al-Dhahir, "Artificial-noise-aided secure mimo full-duplex relay channels with fixed-power transmissions," *IEEE Communications Letters*, vol. 20, no. 8, pp. 1591–1594, 2016.

[78] X. Hu, C. Kai, S. Zhang, Z. Guo, and 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*, vol. 8, no. 2, pp. 480–483, 2019.

[79] Y. Li, R. Zhao, Y. Wang, G. Pan, and C. Li, "Artificial noise aided precoding with imperfect csi in full-duplex relaying secure communications," *IEEE Access*, vol. 6, pp. 44 107–44 119, 2018.

[80] X. Li, Q. Wang, H.-N. Dai, and H. Wang, "A novel friendly jamming scheme in industrial crowdsensing networks against eavesdropping attack," *Sensors*, vol. 18, no. 6, 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/6/1938

[81] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for internet of everything: Opportunities and challenges," *Computer Communications*, vol. 155, pp. 66 – 83, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366419318754

[82] Q. Wang, H.-N. Dai, H. Wang, G. Xu, and A. K. Sangaiah, "UAV-enabled friendly jamming scheme to secure industrial Internet of Things," *Journal of Communications and Networks*, vol. 21, no. 5, pp. 481–490, 2019.

[83] J. u. Rehman Kazim, T. J. Cui, A. Zoha, L. Li, S. Aziz Shah, A. Alomainy, M. A. Imran, and Q. H. Abbasi, "Revolutionizing Future Healthcare using Wireless on the Walls (WoW)," *arXiv e-prints*, 2020. [Online]. Available: https://ui.adsabs.harvard.edu/abs/2020arXiv200606479R

[84] Y. Liu, L. Zhang, B. Yang, W. Guo, and M. A. Imran, "Programmable wireless channel for multi-user mimo transmission using meta-surface," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.