Learning-Based Efficient Sparse Sensing and Recovery for Privacy-Aware IoMT

Tiankuo Wei, Sicong Liu, *Senior Member, IEEE,* and Xiaojiang Du, *Fellow, IEEE*

***Abstract*—Due to the inherent openness of wireless channels and the restriction of communication resources and energy supply, the privacy protection of the sensing data transmission in security-critical Internet of Medical Things (IoMT) has become a great challenge. In order to guarantee the privacy of IoMT sensing and transmission in a wireless wiretap channel and reduce the power consumption, a privacy-aware sensing and transmission scheme with the name of Sparse Learning based Encryption and Recovery (SLER) is proposed. The sparse sensing signal is compressed and encrypted at the IoMT devices in the encryption stage, and transmitted to the network coordinator or edge devices, where the sparse signal is accurately recovered via sparse learning in the decryption stage. The encryption stage is conducted based on compressed sensing. The decryption stage utilizes a model-based sparsity-aware deep neural network to accurately recover the sensing signal, whose sparse features are extracted to decrease the required size of measurement signals and increase the spectrum efficiency. The secrecy performance of the proposed SLER algorithm is theoretically analyzed. Experiments of electrocardiogram (ECG) signal transmission are performed as a typical IoMT application. The experimental results show that the proposed scheme can effectively guarantee the transmission secrecy against eavesdropping, while improving the spectrum efficiency and energy efficiency compared to other existing methods.**

***Index Terms*—sparse learning, compressed sensing, privacy, Internet of Medical Things (IoMT), eavesdropping.**

I. Introduction

As an important branch of the Internet of things (IoT), the Internet of Medical Things (IoMT) is expansively deployed in hospitals and nursing affiliations to provide prompt, comprehensive, and convenient service [1]. An IoMT may consist of various connected devices, especially implantable and wearable medical devices embedded with sensing, storage and communication modules [2]. The IoMT devices can realize physiological data collection using sensors, and then transmit the sensing data through wireless channels to the doctor's computing terminal for immediate diagnosis and treatment.

This work is supported in part by the National Natural Science Foundation of China (No. 61901403), in part by the Science and Technology Key Project of Fujian Province, China (No. 2019HZ020009), in part by the Natural Science Foundation of Fujian Province of China (No. 2019J05001), and in part by the Youth Innovation Fund of Natural Science Foundation of Xiamen (No. 3502Z20206039). *(Corresponding Author: Sicong Liu.)*

Tiankuo Wei and Sicong Liu are with the Department of Information and Communication Engineering, School of Informatics, Xiamen University, Xiamen 361005, China (e-mail: liusc@xmu.edu.cn).

Xiaojiang Du is with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, USA (e-mail: dxj2005@gmail.com).

In recent years, the privacy and security challenge in smart healthcare has been the focus of public attention. Sensitive and private medical information must be well protected and separated from public access in consideration of data privacy of the patients [3], [4]. Therefore, in order to guarantee the privacy of the patients, it is required to incorporate adequate protection mechanisms in the IoMT to deal with security attacks like eavesdropping. Unfortunately, due to the openness of wireless channels, data transmission of IoMT devices is exposed to malicious attackers [5].

To combat against the threat of eavesdropping and protect the confidentiality of IoMT transmission, compressed sensing (CS) [6] can serve as an efficient alternative to enhance secrecy and reduce the communication costs [7]–[9]. In fact, the most physiological signals collected by sensors in IoMT, such as the electrocardiogram (ECG) and electroencephalogram (EEG), are sparse in the specific basis. Exploiting the inherent sparsity of these sensing signals, the CS framework can facilitate the encryption and compression of them. For example, a joint operation of the sparse compression and encryption of the sensing signal is implemented simultaneously based on CS, where a shared observation matrix is adopted as a symmetric encryption key [10], [11]. Utilizing CS, the IoMT sensing signal can be transmitted in a compressed format with only a few measurements, which improves the spectral efficiency and reduces the power consumption of communication, thus extending the service life of IoMT devices [9]. Wei *et al.* [12] proposed a CS-based encryption and sparse recovery scheme for privacy protection and sensing signal compression.

In the CS framework, the sparse sensing signal should be accurately recovered from the received observation signal. Since the recovery accuracy and the compression ratio are critical to the IoMT system performance, the sparse recovery method is an important issue, which has been widely investigated. Among the classical methods are several iterative sparse recovery algorithms, including CS-based algorithms such as Orthogonal Matching Pursuit (OMP) [13] and Subspace Pursuit (SP) [14], and iterative algorithms such as Approximate Message Passing (AMP) [15]. Recently, the emerging deep learning technology has demonstrated its outperformance in learning data features, and has been widely applied in various fields [16]. The deep learning architecture is exploited to learn the sparse characteristics of the measured signals to further improve the recovery performance [17]–[23]. For example, a deep neural network is used to unfold the AMP algorithm for sparse recovery [23].

To deal with eavesdropping and improve the communication efficiency in the process of sensing signal transmission for

IoMT, in this paper, we propose a sparse learning based encryption and recovery (SLER) method. CS is adopted in the encryption of sensing signals, and sparse learning is introduced to improve the accuracy of the sensing signal recovery while improving the spectrum and energy efficiency. The privacy of the IoMT signal is well protected by the proposed scheme, which is verified by theoretical analysis and experiments. It is verified that the recovery performance of the proposed scheme outperforms the state-of-art sparse recovery algorithms via experiments. To summarize, the contributions of this paper are as follows:

- A privacy-protecting sensing and transmission scheme, i.e., SLER, is proposed for IoMT, which can enhance the data confidentiality with lower cost of communication and energy resources.
- A CS-based compression and encryption method is devised to resist eavesdropping attacks, which improves the spectrum efficiency.
- A deep sparse learning based algorithm is proposed to further improve the spectrum and energy efficiency by fully exploiting the inherent sparse characteristics of the sensing signals.

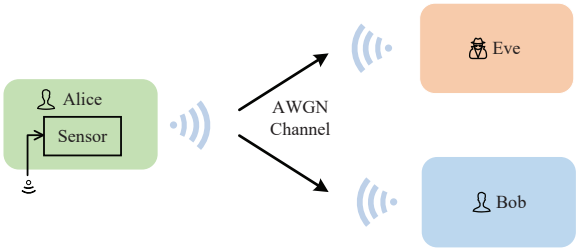
The remainder of this paper is structured as follows. The related work is reviewed in Section II. The system model of signal sensing and transmission in the IoMT is described in Section III. Section IV shows the proposed SLER scheme. The secrecy performance of the proposed SLER scheme is theoretically analyzed in Section V. Experimental results are demonstrated in Section VI, followed by the conclusions in Section VII.

II. Related Work

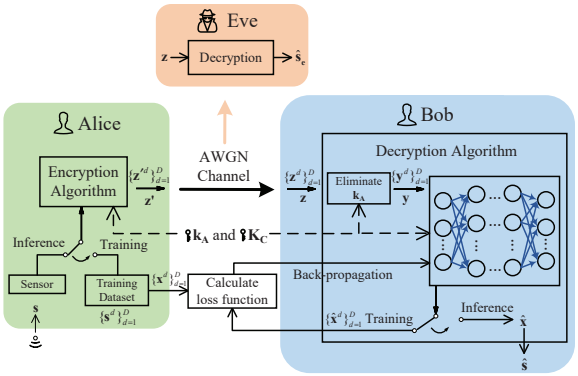
Some solutions to the privacy protection issue in IoMT have been studied. To protect the sensitive and private information of patients, Shen *et al.* [24] proposed a blockchain based medical image retrieval scheme. Sun *et al.* [25] designed a mutual authentication mechanism for the communication between mobile devices and the server to resist the black-hole attack. To avoid information leakage in the profile matching process, Qian *et al.* [26] proposed a private set intersection scheme to implement fine-grained profile matching. Yao *et al.* [27] proposed an ECG-based lightweight key agreement scheme.

As a promising method, the CS technique has been studied to protect the private and sensitive information in data transmission. Peng *et al.* [28] proposed a chaotic CS-based encryption mechanism for body-to-body networks. Chi *et al.* [8] proposed a scheme to secure the access of implantable medical devices based on CS. Liu *et al.* [29] designed a CS-based physical layer security scheme for OFDM-based IoT systems.

Moreover, CS has been used in IoMT and Wireless Body Area Networks (WBANs) as an effective alternative for the acquisition and transmission of sensing signals. Zhang *et al.* [30] designed a CS-based EEG telemonitoring scheme. Lalos *et al.* [31] exploited CS for signal compression and distributed cooperation. Wang *et al.* [32] designed a CS-based biomedical



(a) Direct transmission without encryption



(b) Secure transmission with the proposed SLER scheme

Fig. 1. System model for IoMT sensing signal encryption, transmission and recovery in the presence of eavesdropping.

signal acquisition scheme with a data-driven Boolean sampling matrix to reduce the energy consumption.

Deep learning [16] has been applied for the sparse recovery in several areas such as compressed image recovery, sparse channel estimation, and compressive random access. Mousavi *et al.* [33] developed a framework for sensing and recovery of structured signals utilizing the stacked denoising autoencoders to learn the statistical correlation in signals for accurate recovery. Some convolutional neural network based frameworks were proposed to reconstruct images from CS measurements, such as ReconNet [19] composed of both convolutional layers and fully connected layers. Moreover, some model-driven sparse learning methods were evolved from basic structures of iterative recovery algorithms. Gregor *et al.* proposed the learned iterative shrinkage thresholding algorithm (LISTA) [20] and trained the layer-wise parameters via supervised learning. Inspired by the AMP and vector AMP (VAMP) algorithms, Borgerding *et al.* proposed the learned AMP and learned VAMP framework [23].

III. System Model

The sensing and communication model in a typical IoMT scenario in the presence of eavesdropping is illustrated in Fig. 1, where Fig. 1(a) and 1(b) depict direct transmission without encryption and the secure transmission with the proposed SLER scheme, respectively. The system consists of two legitimate communication entities, i.e., the transmitter (Alice) and the legitimate receiver (Bob), and an adversary, i.e., the eavesdropper (Eve), whose details are introduced as follows.

- **Alice** is the transmitter, i.e., the IoMT device such as a wearable or implantable device, which is equipped with

sensing, computing and communication modules. The physical signals in the real world are collected by sensors, probably and favorably compressed to save the spectrum efficiency and communication cost, and transmitted to Bob via the wireless channel. Due to the constrained power supply and hardware size, Alice is equipped with limited computing resource, and cannot perform complex calculations.

- **Bob** is the receiver, such as a wireless access point or an edge node in the IoMT, which receives the sensing signal sent by Alice for analyzing and processing. Different from Alice, the receiver Bob is usually equipped with sufficient computing and storage resources, and is able to support complex computations like the training and inference in deep learning.
- **Eve** is an adversary attempting to eavesdrop on the sensing signal intended for Bob by wiretapping the open wireless channel. Eve is assumed to be equipped with rationally moderate computing power, i.e., Eve can implement normal computing and processing tasks, but can not solve too complicated problems like performing exhaustive searches. More specifically, the ciphertext-only attack is considered, i.e., Eve can acquire the transmitted ciphertext signal, but can not acquire the plaintext or the secret keys.

We consider a typical sensing and transmission process in an IoMT. A length-N sensing signal $\mathbf{s} = [s_1, s_2, \cdots, s_N]^T$, which can be non-sparse, is collected by the sensors of the transmitter Alice. The non-sparse original sensing signal $\mathbf{s}$ can be sparsely represented using a certain sparse representation matrix $\mathbf{\Psi}$, which can be expressed as

$$\mathbf{s} = \mathbf{\Psi}\mathbf{x}, \tag{1}$$

where $\mathbf{\Psi}$ is an inverse discrete cosine transform (IDCT) matrix with size of $N \times N$, in the case that the original sensing signal $\mathbf{s}$ is an ECG signal. Thus, the sensing signal $\mathbf{s}$ can be represented as a k-sparse signal $\mathbf{x}$, $k \ll N$, where k is the sparsity level, i.e. the number of nonzero entries, of the sparse signal $\mathbf{x}$. Then, we can implement encryption with a secret key $\mathbf{k}_{\mathrm{A}}$ and a secret observation matrix $\mathbf{K}_{\mathrm{C}}$. Firstly, the original sensing signal $\mathbf{s}$ is converted to the private sensing signal $\mathbf{s}'$ by mixing up with the secret key $\mathbf{k}_{\mathrm{A}}$, which is then encrypted using the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ to generate the ciphertext signal $\mathbf{z}'$. Note that the secret key and the secret observation matrix have been shared in advance between Alice and Bob, which is not accessible by Eve.

Then, the ciphertext signal $\mathbf{z}'$ is transmitted from Alice to Bob through an open wireless channel, which is modeled by a transparent channel with additive white Gaussian noise (AWGN). The received signal is thus given by

$$\mathbf{z} = \mathbf{z}' + \boldsymbol{\omega}, \tag{2}$$

where $\boldsymbol{\omega}$ is the AWGN vector. At the legitimate receiver Bob, the original sensing signal $\mathbf{s}$ is reconstructed using the proposed decryption and recovery algorithm based on sparse deep learning, which is introduced in detail in the next section. Specifically, the corresponding component of the secret key $\mathbf{k}_{\mathrm{A}}$ in the received signal $\mathbf{z}$ is firstly eliminated, and thus the sparse observation signal $\mathbf{y}$ can be obtained. Subsequently, using the proposed sparse deep learning based method, i.e., the SLER scheme, we can solve for the sparse sensing signal $\mathbf{x}$ from the sparse observation signal $\mathbf{y}$. Finally, the original sensing signal $\mathbf{s}$ can be obtained from the sparse sensing signal $\mathbf{x}$ via the sparse representation given by (1).

In the system model adopted in this paper, the inherent sparsity of the medical sensing signal of interest facilitates both the compressive encryption and sparse recovery processes. Fortunately, in the realistic IoMT, due to the inherent temporal correlation of physical sensing signals, such as ECG signals, we can express the original sensing signal can be represented as a sparse vector in a transform domain using a sparse representation matrix, which can be an IDCT matrix for ECG signals. In the proposed SLER method, the sparsity of the sensing signals are fully exploited to guarantee the compressive encryption and the sparse recovery.

IV. Sparse Learning Based Encryption and Recovery Method for IoMT

In this section, we introduced the details of the proposed SLER scheme. As shown in Fig. 2, the proposed method contains two parts: 1) a compressive encryption algorithm in the compressed sensing framework at the transmitter; 2) a decryption and sparse recovery algorithm based on deep learning at the legitimate receiver, containing both training and inference stages.

A. Compressive Encryption of the Sensing Signal in the Compressed Sensing Framework

The encryption method of the proposed SLER method contains two processes, namely key addition and compressive encryption. In the first process, the secret key $\mathbf{k}_{\mathrm{A}}$ is firstly generated with each entry $\mathbf{k}_{\mathrm{A}}$ following a i.i.d. uniform distribution $\mathrm{U}(-\xi\frac{r_2-r_1}{2}, \xi\frac{r_2-r_1}{2})$. Then, the original sensing signal $\mathbf{s}$ is encrypted using the secret key $\mathbf{k}_{\mathrm{A}}$, and thus the private sensing signal $\mathbf{s}'$ is obtained by

$$\mathbf{s}' = \mathbf{s} + \mathbf{k}_{\mathrm{A}}, \tag{3}$$

where ξ presents the scale parameter for adjusting the signal power of $\mathbf{k}_{\mathrm{A}}$, and each entry of the original sensing signal $\mathbf{s}$ is bounded within the interval $[r_1, r_2]$.

In the second process, compression and encryption are jointly implemented with a simple operation, i.e., a matrix multiplication of the private sensing signal $\mathbf{s}'$ and the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ with size of $M \times N$, $M<N$, which is given by

$$\mathbf{z}' = \mathbf{K}_{\mathrm{C}}\mathbf{s}', \tag{4}$$

where each entry of $\mathbf{K}_{\mathrm{C}}$ is randomly generated following an i.i.d. Gaussian distribution, i.e., $K_{\mathrm{C}}^{(m,n)} \sim \mathcal{N}(0, 1/M)$, $m = 1, \cdots, M, n = 1, \cdots, N$. Thus, the N-dimensional private sensing signal $\mathbf{s}'$ is compressed to a ciphertext signal $\mathbf{z}'$ of length-M, with a compression ratio $\gamma = M/N \times 100\%$.

It can be noted that the computational complexity of the compressive signal sensing and encryption process is only

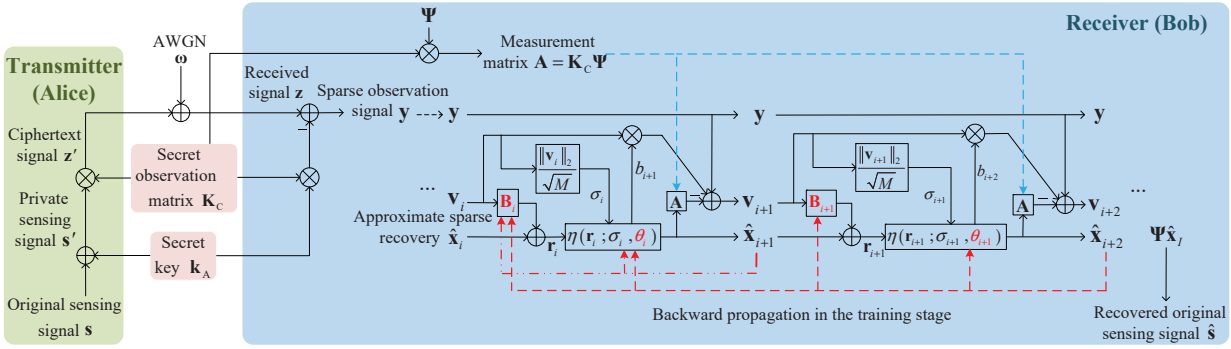


Fig. 2. Illustration of the proposed SLER scheme including compressed encryption of the sensing signal based on compressed sensing, and decryption and sparse recovery based on deep learning.

involved with simple operations of matrix additions and multiplications, which is moderate and thus it is suitable for medical devices, especially implantable devices with restricted computing resource in the IoMT. Meanwhile, sufficient secrecy performance is guaranteed, which is theoretically analyzed in Section V and verified by experiments in Section VI.

B. Deep Learning Based Decryption and Sparse Recovery

During the wireless transmission, the ciphertext signal $\mathbf{z}'$ suffers from the noise interference, obtaining the received signal $\mathbf{z}$ in (2) at the receiver Bob. Then, Bob decrypts the received signal $\mathbf{z}$ by eliminating the corresponding component of the secret key, and thus the sparse observation signal $\mathbf{y}$ is formulated, which is used to reconstruct the sparse sensing signal $\mathbf{x}$ with the deep sparse learning networks. Therefore, the decryption method consists of two phases, namely key removal and sparse reconstruction.

In the key removal phase, using both the secret key $\mathbf{k}_{\mathrm{A}}$ and the secret observation matrix $\mathbf{K}_{\mathrm{C}}$, the corresponding component of the secret key $\mathbf{k}_{\mathrm{A}}$ is removed from the received ciphertext signal $\mathbf{z}'$ for the purpose of decryption, expressed as

$$\mathbf{y} = \mathbf{z}' + \boldsymbol{\omega} - \mathbf{K}_{\mathrm{C}}\mathbf{k}_{\mathrm{A}}. \tag{5}$$

Subsequently, the sparse observation signal $\mathbf{y}$ containing the information of both the original sensing signal $\mathbf{s}$ and the sparse sensing signal $\mathbf{x}$ is given by

$$\mathbf{y} = \underbrace{\mathbf{K}_{\mathrm{C}}\boldsymbol{\Psi}}_{\mathbf{A}}\mathbf{x} + \boldsymbol{\omega}, \tag{6}$$

where $\mathbf{A}$ represents an $M \times N$ under-determined measurement matrix in the CS framework. The unknown sparse sensing signal $\mathbf{x}$ can be derived from the sparse observation signal $\mathbf{y}$ by solving the under-determined linear inverse problem formulated in (6). Different from the sparse reconstruction methods like CS-based methods or iterative methods, in the proposed SLER scheme, a deep neural network is incorporated for sparse recovery, to learn the sparse feature of the sensing signal and improve the recovery accuracy.

Firstly, a sparsity-aware deep neural network mimicking the iterative AMP method is formulated, which is learning the sparse feature of the sensing signal with the training data. Then, the trained network is exploited to accurately recover the sparse sensing signal $\mathbf{x}$ in the inference stage. More specifically, as shown in Fig. 2, the I layers of the proposed network are evolved from the I iterations of the AMP. The operation in the ith network layer is given by

$$\hat{\mathbf{x}}_{i+1} = \eta(\hat{\mathbf{x}}_i + \mathbf{B}_i\mathbf{v}_i; \sigma_i, \theta_i), \tag{7}$$

$$\mathbf{v}_{i+1} = \mathbf{y} - \mathbf{A}\hat{\mathbf{x}}_{i+1} + b_{i+1}\mathbf{v}_i, \tag{8}$$

where $\hat{\mathbf{x}}_i$ represents the recovered sparse vector of layer-i, and $\mathbf{v}_i$ is the residual measurement error of layer-i. $\mathbf{B}_i$ is a parameterized matrix evolved from the measurement matrix $\mathbf{A}$, which is a learned parameter of layer-i. The operator $\eta(\cdot)$ represents a shrinkage function fed by the pseudo-measurement vector $\mathbf{r}_i \triangleq \hat{\mathbf{x}}_i + \mathbf{B}_i\mathbf{v}_i$, the standard deviation of the measurement error $\sigma_i = \frac{\|\mathbf{v}_i\|_2}{\sqrt{M}}$, and an i-dependent learnable threshold parameter θ_i. The shrinkage function $\eta(\mathbf{r}_i; \sigma_i, \theta_i)$ plays a role of a sparsity-inducing function, which is defined as $[\eta(\mathbf{r}_i; \sigma_i, \theta_i)]_t = \mathrm{sgn}(r_{i,t})\max(|r_{i,t}| - \theta_i\sigma_i, 0), t = 1, ..., N$, which removes the noise components in $\mathbf{r}_i$ whose magnitude is smaller than the given threshold σ_i, θ_i, while it keeps and imposes a shrinkage on the nonzero entries larger than the threshold, which yields the sparse vector $\hat{\mathbf{x}}_{i+1}$. The term $b_{i+1}\mathbf{v}_i$ is the Onsager correction term which makes $\mathbf{r}_i$ modeled as the sparse sensing signal $\mathbf{x}$ mixed with a Gaussian noise with variance σ_i^2 [34], where b_{i+1} is given by

$$b_{i+1} = \frac{1}{M}\sum_{t=0}^{N}\frac{\partial[\eta(\mathbf{r}_i; \sigma_i, \theta_i)]_t}{\partial r_{i,t}}. \tag{9}$$

Exploiting the sparsity-aware deep neural networks, the sparse feature, i.e., the positions of nonzero entries, of the sparse sensing signal $\mathbf{x}$, can be extracted to facilitate sparse recovery, and the recovery accuracy can be improved. Specifically, the proposed method consists of two stages, i.e. the training stage shown in **Algorithm 1**, and the inference stage shown in **Algorithm 2**, with the detailed procedures described as follows.

In the training stage as shown in **Algorithm 1**, the training set $\{\mathbf{x}^d, \mathbf{y}^d\}_{d=1}^{D}$ consists of D data samples, of which each contains a sparse observation signal $\mathbf{y}^d$ and the sparse sensing signal $\mathbf{x}^d$, is utilized to train the learnable network parameters $\boldsymbol{\Theta} = \{\mathbf{B}_i, \theta_i\}_{i=0}^{I-1}$. Specifically, normalized mean square error

Algorithm 1 Sparse Learning based Encryption and Recovery (SLER) Scheme: Training Stage

Input:

1) Training dataset $\left\{\mathbf{x}^d, \mathbf{y}^d\right\}_{d=1}^{D}$ with size of D, each data sample containing a sparse observation signal $\mathbf{y}^d$ and the corresponding ground-truth sparse sensing signal $\mathbf{x}^d$

2) Measurement matrix $\mathbf{A}$ defined in (6)

Initialize $i \leftarrow 0$, $\mathbf{v}_0 \leftarrow \mathbf{y}$, $\hat{\mathbf{x}}_0 \leftarrow \mathbf{0}$

(For layer-i in the deep neural network)

repeat

  Initialize parameters for layer-i: $\mathbf{B}_i \leftarrow \mathbf{A}^T$, $\theta_i \leftarrow 1$

  Compute the pseudo-measurement vector $\mathbf{r}_i = \hat{\mathbf{x}}_i + \mathbf{B}_i\mathbf{v}_i$ and the standard deviation of the measurement error $\sigma_i = \frac{\|\mathbf{v}_i\|_2}{\sqrt{M}}$

  Estimate the sparse vector $\hat{\mathbf{x}}_{i+1}$ by (7) and obtain the value of b_{i+1} by (9)

  Update the residual measurement error $\mathbf{v}_{i+1}$ by (8)

  Compute the loss function $\mathcal{L}_i$ based on (10) and update the learnable parameters $\mathbf{\Theta}_i = \{\mathbf{B}_i, \theta_i\}$ using back propagation

  Set $i = i + 1$

until $\mathcal{L}_i \geq \mathcal{L}_{i-1}$

Set the total number of network layers as $I = i - 1$

Output:

Trained parameters $\mathbf{\Theta} = \{\mathbf{B}_i, \theta_i\}_{i=0}^{I-1}$

Algorithm 2 Sparse Learning based Encryption and Recovery (SLER) Scheme: Inference Stage

Input:

1) Sparse observation signal $\mathbf{y}$

2) Trained parameters $\mathbf{\Theta} = \{\mathbf{B}_i, \theta_i\}_{i=0}^{I-1}$

Initialize the estimated sparse sensing signal as $\hat{\mathbf{x}}_I \leftarrow 0$

Conduct one feedforward operation in the trained deep neural network to infer the final estimated sparse sensing signal $\hat{\mathbf{x}}_I = \eta(\mathbf{r}_{I-1}; \sigma_{I-1}, \theta_{I-1})$

Acquire the recovered original sensing signal $\hat{\mathbf{s}} = \mathbf{\Psi}\hat{\mathbf{x}}_I$

Output:

Recovered original sensing signal $\hat{\mathbf{s}}$

(NMSE) is used as the loss function $\mathcal{L}_i$, which is calculated by

$$\mathcal{L}_i = \frac{1}{D}\sum_{d=1}^{D}\frac{\left\|\hat{\mathbf{x}}_i^d(\mathbf{y}^d; \mathbf{\Theta}_i) - \mathbf{x}^d\right\|_2^2}{\|\mathbf{x}^d\|_2^2}, \tag{10}$$

where $\hat{\mathbf{x}}_i^d(\mathbf{y}^d; \mathbf{\Theta}_i)$ denotes the output of layer-i with the input $\mathbf{y}^d$ and the learnable parameters $\mathbf{\Theta}_i = \{\mathbf{B}_k, \theta_k\}_{k=0}^{i}$ for the 0 through i layers. When training the learnable parameters in the ith layer, all the previous layers are exploited for the calculation of the loss function $\mathcal{L}_i$ given in (10). The learnable parameters are updated with the Adam optimizer and back propagation (BP) by minimizing the loss function $\mathcal{L}_i$. The layer-wise training process is repeated until $\mathcal{L}_i \geq \mathcal{L}_{i-1}$, which means the loss function does not decrease with the number of layers, to avoid possible over-fitting due to excessive layers and network parameters. Finally, the total number of network layers is finalized as $I = i - 1$ when the loop halts.

In the inference stage as shown in **Algorithm 2**, using the trained deep neural network, the legitimate receiver Bob can recover the original sparse sensing signal $\mathbf{s}$ transmitted by Alice. Specifically, the sparse observation signal $\mathbf{y}$ is fed to the network with the learned parameters $\mathbf{\Theta}$ to estimate the final sparse sensing signal $\hat{\mathbf{x}}_I$. Then, the legitimate receiver Bob can acquire the recovered original sensing signal $\hat{\mathbf{s}} = \mathbf{\Psi}\hat{\mathbf{x}}_I$. Exploiting the deep neural network, the proposed method can accurately recover the original sensing signal for the IoMT, which helps guarantee reliable diagnosis and proper treatment. Moreover, leveraging the good capability of sparse recovery, the compression ratio γ can be decreased at a specific target level of reconstruction error, thereby further improving the spectral efficiency of the IoMT sensing and transmission system.

V. Secrecy Performance Analysis and Evaluation

In this section, the secrecy performance of the proposed SLER scheme is theoretically analyzed and evaluated, from the compressive encryption, computational attack, and key addition perspectives of view.

A. Secrecy Performance Analysis of Compressive Encryption

1) Perfect Secrecy Analysis: In the compressive encryption process expressed by (4), the private sensing signal $\mathbf{s}'$ is encrypted into the ciphertext signal $\mathbf{z}'$ with the secret observation matrix $\mathbf{K}_{\mathrm{C}}$. For a cryptographic encryption system, Shannon proposed a method to measure its secrecy performance from the statistical characteristic perspective of view, called perfect secrecy [35]. Perfect secrecy is achieved if the posterior probability of $\mathbf{s}'$ in condition of any $\mathbf{z}'$ is equal to the prior probability of $\mathbf{s}'$, i.e., $P(\mathbf{s}'|\mathbf{z}') = P(\mathbf{s}')$, which means that the ciphertext $\mathbf{z}'$ does not contain any information of the plaintext $\mathbf{s}'$. Generally, it also indicates that there is zero mutual information between $\mathbf{s}'$ and $\mathbf{z}'$, i.e. $I(\mathbf{s}'; \mathbf{z}') = 0$. Based on this, the perfect secrecy of the compressive encryption process in the proposed scheme is analyzed as follows.

Corollary 1: Assume that the private sensing signal $\mathbf{s}'$ follows the discrete uniform distribution on an alphabet set $\mathcal{S}'$. Then, when the original sensing signal $\mathbf{s}'$ is not a null signal, i.e., $P_{\mathcal{S}'}(\mathbf{0}) = 0$, the compressive encryption process can achieve perfect secrecy if the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ satisfies the Restricted Isometric Property (RIP) [6] with $M \geq 2k$.

Proof: Please refer to Appendix A.

Remark 1: In [11], Rachlin *et al.* proved that when $\mathbf{s}' = \mathbf{0}$, a observation matrix enabled cryptographic system will leak the information of the transmitted data, making it impossible to achieve perfect secrecy. However, in realistic IoMT scenarios, a null signal is meaningless and unlikely to occur. Except for trivial null signals, we have proved that the compressive encryption process of the proposed scheme can achieve perfect secrecy, as demonstrated in *Corollary 1*.

2) Computational Attack Analysis: The attack on the compressive encryption process of the proposed SLER scheme from an adversarial eavesdropper can be regarded as trying to *guess* the actual secret observation matrix $\mathbf{K}_{\mathrm{C}}$. According

to Theorem 1 in [11], if the eavesdropper uses a observation matrix different from the actual secret observation matrix $\mathbf{K}_{\mathrm{C}}$ in CS recovery, the eavesdropper will obtain an M-sparse solution which is completely different from the actual k-sparse sensing signal $\mathbf{x}$. Therefore, only if the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ is completely compromised can the eavesdropper acquire the correct transmitted signal. One possible approach for the eavesdropper is trying to continuously reconstruct $\mathbf{x}$ by exhaustively searching for the correct $\mathbf{K}_{\mathrm{C}}$ in a brute-force manner until the eavesdropper gets a satisfactory k-sparse signal. However, the brute-force search is computationally intolerable. Specifically, suppose that the step size of the exhaustive search grid is 10^{-4}. Since each entry of the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ follows a Gaussian distribution, i.e., $K_{\mathrm{C}}^{(m,n)} \sim \mathcal{N}(0, 1/M)$, its confidence probability over the interval $(-3/\sqrt{M}, 3/\sqrt{M})$ is 0.9973. Thus, most entries fall into this interval, which can be selected as the search space of the eavesdropper. For each entry in $\mathbf{K}_{\mathrm{C}}$, the size of the search space is $2\times 3/\sqrt{M}/10^{-4} = 6\times 10^4/\sqrt{M}$. Therefore, cracking the entire secret observation matrix $\mathbf{K}_{\mathrm{C}}$ needs to perform a grid search on the space with size of $(6 \times 10^4/\sqrt{M})^{MN}$. That is, in total, $(6 \times 10^4/\sqrt{M})^{MN}$ matrix candidates should be used as the guessed secret observation matrix to perform sparse recovery one by one until the desired result is obtained. For instance, when $N = 500$ and $M = 250$, assuming the computational complexity of the sparse recovery algorithm is N_S, the computational complexity of the brute-force search cracking method is $\mathcal{O}(10^{4.5\times 10^5} N_S)$, which far exceeds the computing capability of a normal eavesdropper.

Remark 2: It is observed from the analysis above that, the computational complexity of the sparse signal reconstruction is large, so it requires a high computational cost. When searching for $\mathbf{K}_{\mathrm{C}}$ by gridding, as the length of the original sensing signal increases, the computational complexity of brute force cracking will increase exponentially, which is normally unbearable for a common eavesdropper equipped with limited computing resource.

B. Secrecy Performance Analysis of Key Addition Process

The key addition process of the proposed SLER scheme further improves the secrecy protection ability by jeopardizing the sparsity of the sensing signal, making it almost impossible to implement correct sparse recovery even if the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ is compromised by the eavesdropper. Specifically, in the extreme condition that the $\mathbf{K}_{\mathrm{C}}$ is known by the eavesdropper, the attack scenario can be formulated as solving an equivalent sparse recovery problem expressed as

$$\begin{aligned}\mathbf{y} &= \mathbf{K}_{\mathrm{C}}(\mathbf{s} + \mathbf{k}_{\mathrm{A}}) \\ &= \mathbf{K}_{\mathrm{C}}\mathbf{\Psi}\mathbf{x} + \mathbf{K}_{\mathrm{C}}\mathbf{k}_{\mathrm{A}} \\ &= \mathbf{A}\mathbf{x} + \mathbf{u},\end{aligned} \tag{11}$$

where $\mathbf{u} = \mathbf{K}_{\mathrm{C}}\mathbf{k}_{\mathrm{A}}$ represents an equivalent noise which disturbs the signal reconstruction of the eavesdropper. The aim of the eavesdropper is to solve for the unknown sparse sensing signal $\mathbf{x}$ from the received observation signal $\mathbf{y}$ disturbed by the equivalent noise $\mathbf{u}$ in the equivalent sparse reconstruction problem given by (11). In order to quantify the impact of key addition on the sparse reconstruction performance for the eavesdropper, the approximate statistical properties of the equivalent noise $\mathbf{u}$ in (11) are analyzed as follows.

Corollary 2: The key addition process utilizes the key $\mathbf{k}_{\mathrm{A}}$ to add an equivalent noise $\mathbf{u}$, of whom each entry $u^{(m)}$ obeys an i.i.d. Gaussian distribution given by

$$u^{(m)} \sim \mathcal{N}\left(0, \frac{\xi^2 N}{12M}(r_2 - r_1)^2\right), m = 1, \cdots, M \tag{12}$$

to hinder the illegal reconstruction of Eve, where ξ is the scale parameter of the secret key $\mathbf{k}_{\mathrm{A}}$ in (3), and r_1 and r_2 denote the lower and upper bounds of the uniform distribution of the secret key $\mathbf{k}_{\mathrm{A}}$, respectively.

Proof: Please refer to Appendix B.

Remark 3: Assuming that the original sensing signal $\mathbf{s}$ obeys a uniform distribution with the variance of $\sigma_s^2 = (r_2 - r_1)^2/12$, the variance of the equivalent noise can be expressed as

$$\sigma_u^2 = \xi^2 \frac{N}{M}\sigma_s^2 = \xi^2 \frac{1}{\gamma}\sigma_s^2. \tag{13}$$

From (13) it can be observed that, the noise power varies with the scale parameter ξ of the secret key $\mathbf{k}_{\mathrm{A}}$ and the compression ratio γ. This means that the amount of measurement data and the power of the secret key have an influence on the secrecy performance of the key addition process, which is further investigated by experiments in Section VI-B.

According to the CS theory, the RIP of the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ is an important aspect to ensure the sparse recovery performance [6]. The k-order RIP of a certain matrix $\mathbf{A}$ can be expressed as

$$\begin{aligned}&\exists \delta_k \in (0,1), \text{s.t. } \forall k\text{−sparse } \mathbf{x}, \\ &(1-\delta_k)\|\mathbf{x}\|^2 \le \|\mathbf{A}\mathbf{x}\|^2 \le (1+\delta_k)\|\mathbf{x}\|^2.\end{aligned} \tag{14}$$

In order to demonstrate that the key addition process can make the eavesdropper unable to achieve accurate sparse recovery by imposing significant error gain on the eavesdropper, we now present Corollory 3 as follows to quantitatively provide the error gain due to key addition, before which, a lemma in [36] utilizing the RIP property is firstly introduced as follows.

Lemma 1: If the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ satisfies the $2k$-order RIP with $\delta_{2k} < \sqrt{2} - 1$, the error gain caused by the equivalent noise $\mathbf{u}$ constrained by $\|\mathbf{u}\|_2 \le \epsilon$ can be expressed as

$$\Delta_{\text{Eve}} \triangleq \|\hat{\mathbf{x}}_{\mathrm{e}} - \mathbf{x}\|_2 \le C_1\epsilon + C_2\frac{\|\mathbf{x} - \mathbf{x}_k\|_1}{\sqrt{k}}, \tag{15}$$

where the coefficients are given by $C_1 = \frac{2}{1-\delta_{2k}-\sqrt{2}\delta_{2k}}$ and $C_2 = \frac{2-2\delta_{2k}+2\sqrt{2}\delta_{2k}}{1-\delta_{2k}-\sqrt{2}\delta_{2k}}$, the vector $\mathbf{x}_k \in \mathbb{R}^N$ represents a k-sparse vector whose nonzero entries are the largest k entries in $\mathbf{x}$, and the vector $\hat{\mathbf{x}}_{\mathrm{e}} \in \mathbb{R}^N$ denotes the sparse signal estimated by the eavesdropper.

Assuming that $\mathbf{x}$ is k-sparse, the second item on the right-hand side in (15) becomes 0, and we have

$$\Delta_{\text{Eve}} \le C_1\epsilon. \tag{16}$$

Utilizing the result in (16), the error gain caused by the key addition process on the illegal signal recovery of the

TABLE I
THE EVALUATION METRIC FOR RECOVERY QUALITY OF ECG SIGNALS [40]

PRD Range (%)	Quality Level
0-2	"Very good"
2-9	"Good"
9-16	"Not good"
16-60	"Bad"

eavesdropper can be obtained, as given by the following corollary.

Corollary 3: For the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ satisfying the $2k$-order RIP with $\delta_{2k} < \sqrt{2}-1$ and the k-sparse sensing signal $\mathbf{x}$, the error gain caused by the key addition process imposed on the unauthorized eavesdropper is given by

$$\Delta_{\mathrm{Eve}} \leq \frac{\sigma_0^2 + 2\alpha\sigma_0}{1-\delta_{2k}-\sqrt{2}\delta_{2k}}, \tag{17}$$

with $\sigma_0 = \sqrt{\frac{N}{6}}\xi\,(r_2 - r_1)$.

Proof: Please refer to Appendix C.

Remark 4: The key addition process significantly increases the estimation error of the eavesdropper by imposing an intensive noise on sparse recovery. The error gain is derived in Corollary 3, which proves that the secrecy is well protected by the key addition process.

VI. EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section, extensive experiments have been conducted to investigate the anti-eavesdropping and sparse reconstruction performance of the proposed method in IoMT sensing and transmission scenarios. The sensing signals from the ECG experimental records in the MIT-BIH arrhythmia database [37], [38] are adopted, with the sampling rate of 360 Hz. We set the length of the original sensing signal $\mathbf{s}$ in a typical interval as $N = 500$. For sake of fair comparison, the compression ratio is set as $\gamma = 50\%$, and the signal-to-noise ratio (SNR) is set as 20dB unless explicitly stated otherwise. The scale parameter of the secret key $\mathbf{k}_{\mathrm{A}}$ is set as $\xi = 1$. An $N \times N$ IDCT matrix is exploited as the sparse representation matrix $\mathbf{\Psi}$. In the training stage, the Adam optimizer is used to optimize learnable parameters, and the learning rate is set as 10^{-3}. Moreover, the depth of the network is adjusted using a validation dataset to prevent the possible over-fitting during training.

The performance of recovery accuracy of the experimental results is evaluated with percentage root-mean square difference (PRD), which is a commonly adopted to measure recovery quality of ECG signals [39]. For the original sensing signal $\mathbf{s}$ and recovered sensing signal $\hat{\mathbf{s}}$, the PRD λ is defined as

$$\lambda = \frac{\|\hat{\mathbf{s}} - \mathbf{s}\|_2}{\|\mathbf{s}\|_2} \times 100\%. \tag{18}$$

In addition, Zigel *et al.* proposed an evaluation metric based on the PRD value, which has been widely adopted to evaluate the subjective recovery quality of ECG signals [40], as shown in Table I, and thus it is also adopted in this paper.

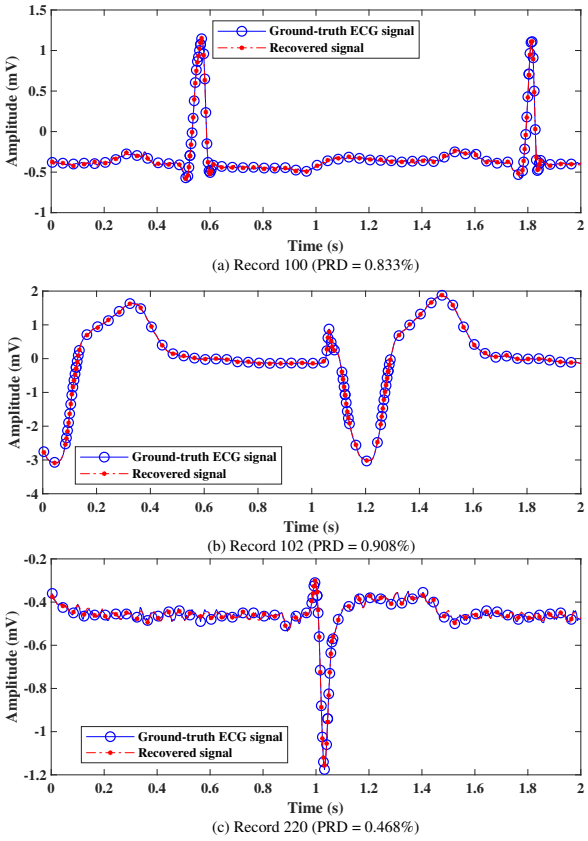


Fig. 3. The recovery results of three ECG sensing signals from the MIT-BIH arrhythmia database.

First, the recovered results of some typical ECG sensing signals from the MIT-BIH arrhythmia database using the proposed SLER scheme are reported in Fig. 3, in which the PRDs of them are 0.833%, 0.908% and 0.468%, respectively. Although the signal quality slightly degrades due to wireless transmission, the recovery performance still reaches the "very good" level. Moreover, when we look at the sparse recovery performance in the discrete cosine transform (DCT) domain as shown in Fig. 4, the NMSE for sparse recovery of the three ECG signals is -30.4dB, -34.9dB and -34.6dB, respectively, which indicates that the sparsity and integrity of the sensing signal are well exploited and preserved using the proposed SLER scheme. In the following, we evaluate the performance of IoMT signal sensing and sparse recovery in the metric of recovery accuracy, spectral efficiency, as well as secrecy protection capability, via extensive experimental results.

A. Sparse Recovery Performance

The performance of sparse reconstruction of the proposed scheme is evaluated and compared with some benchmark schemes including the CS-based greedy algorithms of OMP [13] and SP [14], and the iterative sparse approximation algorithm of AMP [15]. To evaluate the accuracy performance of sparse recovery of sensing signals, the PRD performance with respect to compression ratio is shown in Fig. 5. As illustrated in Fig. 5, compared with other benchmark schemes, the recovery error of the proposed SLER scheme is much

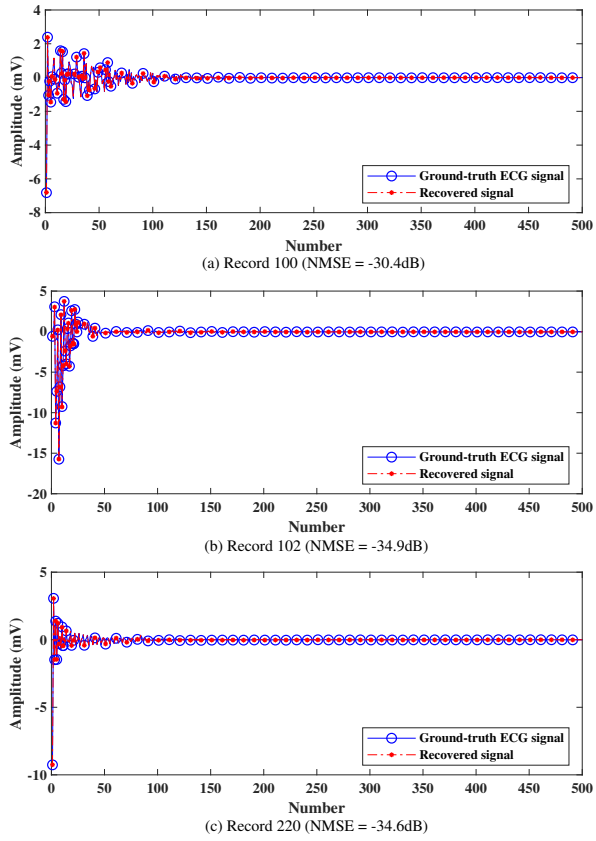


Fig. 4. The recovery results of ECG signals from the MIT-BIH arrhythmia database in the DCT domain.

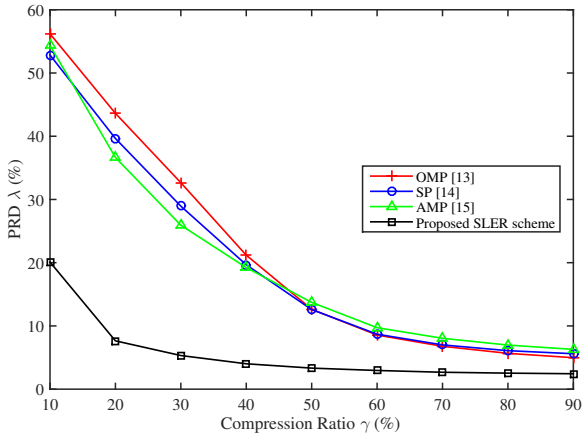


Fig. 5. PRD performance of the proposed SLER scheme and other benchmark schemes with respect to compression ratio in sparse recovery of IoMT sensing signals.

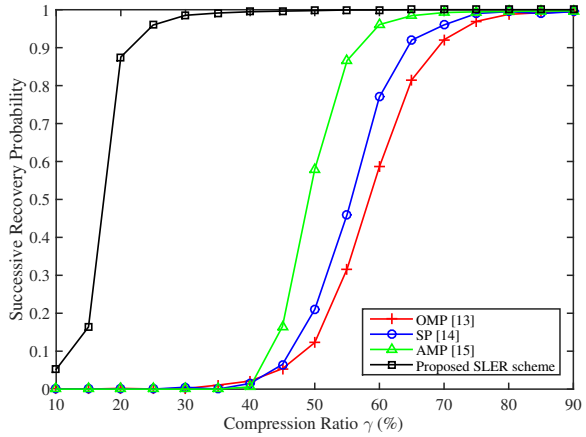


Fig. 6. Successive recovery probability of the proposed SLER scheme and other benchmark schemes with respect to compression ratio in sparse recovery of IoMT sensing signals.

lower for different compression ratios. Specifically, the PRD of the SLER scheme at the compression ratio of 20% is close to that of the SP and OMP algorithms at the compression ratio of 70%. The successive recovery probability, i.e. the probability that the recovery NMSE <-10dB, is adopted as an alternative metric to measure the recovery error in the DCT domain and demonstrate the successive recovery capability, as reported in Fig. 6. It can be observed from Fig. 6 that, at a quite low compression ratio of 25% which indicates that the original long sensing signal is compressed into only a quarter of its original size to transmit, a successive recovery probability of no less than 0.9 can still be achieved, much higher than the other benchmark schemes. The experimental results indicate that by effectively learning and fully exploiting the sparse feature of the sensing signal, the proposed scheme can obtain better performance of recovery accuracy and spectrum efficiency in IoMT signal transmission and recovery, even if the original sensing signal is heavily compressed with a very low compression ratio. This makes it possible to significantly save the amount of data to be transmitted in wireless communication between the IoMT sensor and the post-processing receiver, thus also greatly saving the transmission energy and spectrum costs.

Furthermore, the recovery accuracy performance with respect to SNR is reported in Figs. 7 and 8. It can be observed from Fig. 7 that compared with the benchmark schemes, the PRD of the SLER scheme is only 1.63% at the SNR of 30dB, which outperforms the OMP, SP and AMP algorithms by 6.50%, 4.78% and 4.35%, respectively. It is also noted from Fig. 7 that, the slope of the curve for the SLER scheme is much lower than other methods in the low SNR region, which indicates that the recovery performance of the proposed scheme is much more robust to intensive noise disturbance. From Fig. 8 it is observed that, in the region of SNR $\geq$ 20dB, the proposed SLER scheme can achieve almost 100% successive recovery probability, but other methods still have a performance gap even in the high SNR region. In a wide SNR region between 5dB to 30dB, the proposed SLER scheme greatly outperforms the benchmark schemes, which shows the effectiveness, reliability and robustness of the proposed IoMT sensing and transmission system even in the harsh communication environment contaminated by intensive noise.

B. Secrecy Protection Performance

Due to the openness of the wireless transmission channel, it is probable that the eavesdropper may wiretap the transmitted encrypted signal and try to recover the original sensing signal via *guessing* or even intelligently learning the statistical

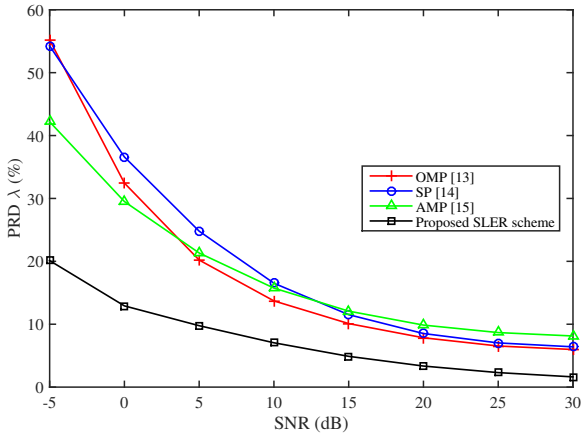


Fig. 7. PRD performance of the proposed SLER scheme and other benchmark schemes with respect to SNR in sparse recovery of IoMT sensing signals.

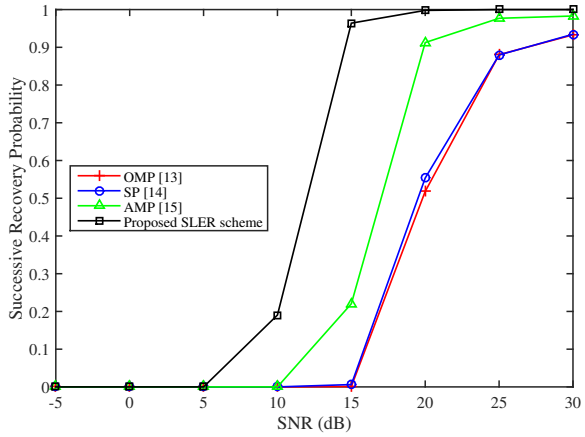


Fig. 8. Successive recovery probability of the proposed SLER scheme and other benchmark schemes with respect to SNR in sparse recovery of IoMT sensing signals.

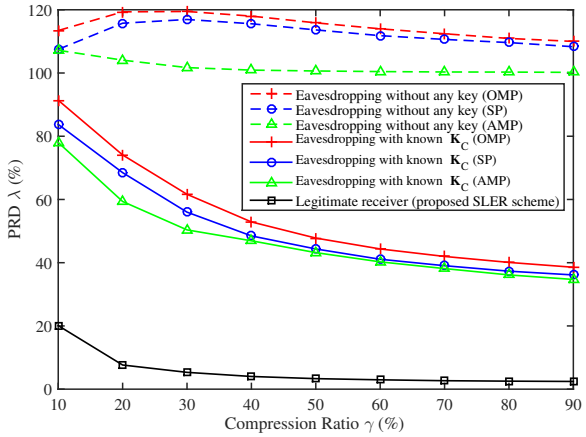


Fig. 9. Recovery PRD performance of the eavesdropper with respect to compression ratio in condition of either knowing the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ or not knowing any secret keys, with the performance of the legitimate receiver also compared.

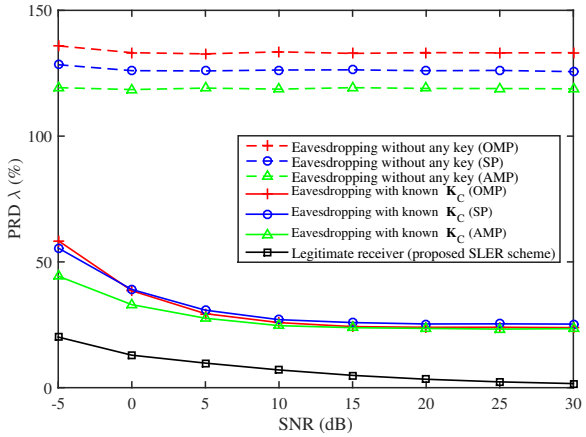


Fig. 10. Recovery PRD performance of the eavesdropper with respect to SNR in condition of either knowing the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ or not knowing any secret keys, with the performance of the legitimate receiver also compared.

characteristics of the secret keys, which might cause damage to information secrecy. Similarly, the PRD performance of the eavesdropper's illegal sparse recovery of the sensing signal is used as a metric to quantify the secrecy information leakage. Specifically, a higher PRD value for the eavesdropper, indicating a more severe recovery error of the sensing signal, implies that it is more difficult for the eavesdropper to recover the accurate original secrecy information, and thus the IoMT system has a better secrecy protection performance. The illegal wiretapping performance of the eavesdropper using different sparse recovery algorithms including OMP, SP and AMP are evaluated through experiments, in the condition that either the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ is compromised by the eavesdropper, or no secret key is leaked at all. For comparison, the sparse recovery performance of the legitimate receiver using the proposed SLER scheme is investigated via experiments with respect to different values of compression ratio, SNR and the scale parameter ξ of the secret key, and the results are reported and compared along with those of the illegal wiretapping performance of the eavesdropper in Figs. 9, 10 and 11, respectively.

From Figs. 9 and 10, it is noted that when both the secret key $\mathbf{k}_{\mathrm{A}}$ and the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ are unavailable to the eavesdropper, the PRD of the signal recovered by the eavesdropper is higher than 100% as illustrated by the dashed lines, which is much worse than the "bad" PRD quality level, indicating that the eavesdropper can hardly obtain the accurate secrecy information. In comparison, it is observed that the PRD performance of the legitimate receiver using the proposed SLER scheme is almost in the "good" or "very good" quality level, which shows the superior secrecy performance of the IoMT system in anti-eavesdropping. In the extreme case that the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ is completely compromised by the eavesdropper, the recovery PRD performance of the eavesdropper is still worse than the "bad" quality level, as illustrated by the solid curves. It is also observed that, the gap of the recovery PRD performance between the eavesdropper and the legitimate receiver is even much larger in the low SNR region or with a lower compression ratio. Therefore, it is verified that the proposed SLER scheme is able to achieve a high secrecy protection performance with high spectral and energy efficiency in the presence of wiretapping.

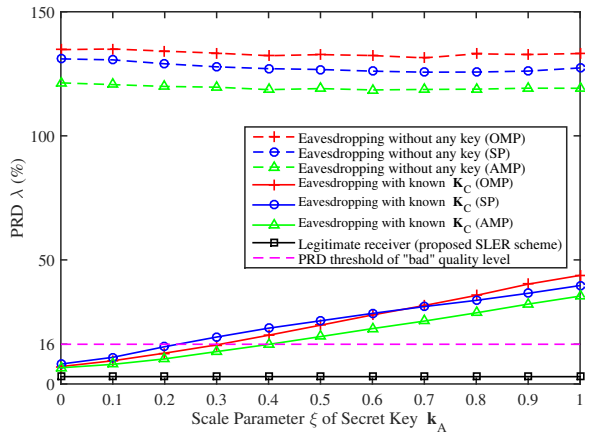


Fig. 11. Recovery PRD performance of the eavesdropper with respect to the scale parameter ξ of the secret key $\mathbf{k}_{\mathrm{A}}$, in condition of either knowing the secret observation matrix $\mathbf{K}_{\mathrm{C}}$ or not knowing any secret keys, with the performance of the legitimate receiver also compared.

Moreover, in order to investigate the influence of the power of the secret key $\mathbf{k}_{\mathrm{A}}$ on the secrecy performance, the recovery PRD performance with respect to the scale parameter ξ of the secret key $\mathbf{k}_{\mathrm{A}}$ is reported in Fig. 11. It can be observed from the black solid curve that the recovery performance of the legitimate receiver using the proposed scheme is independent of the variation of the scale parameter ξ, since the secret key is known to the legitimate receiver and thus completely removed before sparse recovery. On the contrary, the recovery performance of the eavesdropper gets worse with the increase of the scale parameter, which indicates that a better secrecy performance can be achieved using a secret key with larger power to prevent from illegal recovery. However, larger power consumption jeopardizes the energy efficiency, so a tradeoff between energy efficiency and anti-eavesdropping capability is an open issue which can be investigated to guarantee some target information confidentiality while improving the energy efficiency, thus extending the lifetime of IoMT devices. Here we show a toy example to this: assuming a "bad" PRD quality level, i.e. a PRD value greater than the threshold of 16 as illustrated by the magenta dashed line in Fig. 11, is the target recovery performance of the eavesdropper subject to a certain secrecy constraint, the minimum value of the scale parameter ξ can be obtained at the intersection point with the green solid curve, i.e. around 0.4, which can be a good tradeoff point between information confidentiality protection and power consumption.

VII. Conclusion

In this paper, a privacy-aware sensing and transmission scheme named SLER is proposed for the IoMT system with limited processing capability, communication resource and energy supply, to improve the secrecy protection performance while preserving the spectrum and energy efficiency. The scheme includes a compressive encryption process and a decryption and sparse recovery algorithm based on deep learning. The compressive encryption algorithm can effectively prevent the eavesdropper from wiretapping the confidential information, even if the secret observation matrix is compromised by an intelligent adversary. A model-driven deep neural network mimicking the AMP algorithm is utilized to learn the sparse characteristics of the IoMT sensing signal for accurate sparse recovery, especially in severe conditions such as low SNR and insufficient measurement data. Theoretical analysis and extensive experimental results have verified that the proposed SLER scheme significantly outperforms state-of-the-art benchmark schemes in sparse recovery performance, and the secrecy protection performance of the IoMT system is greatly improved while preserving the energy and spectrum efficiency. Furthermore, it is also promising for the proposed scheme to be applied in other resource-constrained IoT scenarios with confidentiality requirements.

Appendix A
Proof of Corollary 1

Proof: For any secret observation matrix $\mathbf{K}_{\mathrm{C}}$, there is only one unique mapping between $\mathbf{s}'$ and $\mathbf{z}'$, so $P_{\mathcal{Z}'}(\mathbf{0}) = 0$, where $\mathcal{Z}'$ is the alphabet of $\mathbf{z}'$. Thus, the mutual information between $\mathbf{s}'$ and $\mathbf{z}'$ can be expressed as

$$\begin{aligned} I(\mathbf{s}';\mathbf{z}') &= H(\mathbf{s}') - H(\mathbf{s}'|\mathbf{z}') \\ &= H(\mathbf{s}') - \sum_{\boldsymbol{\zeta}\in\mathcal{Z}'} P_{\mathcal{Z}'}(\mathbf{z}'=\boldsymbol{\zeta}) H(\mathbf{s}'|\mathbf{z}'=\boldsymbol{\zeta}) \\ &= H(\mathbf{s}') - P_{\mathcal{Z}'}(\mathbf{z}'=\mathbf{0}) H(\mathbf{s}'|\mathbf{z}'=\mathbf{0}) \\ &\quad - \sum_{\boldsymbol{\zeta}\in\mathcal{Z}',\boldsymbol{\zeta}\neq\mathbf{0}} P_{\mathcal{Z}'}(\mathbf{z}'=\boldsymbol{\zeta}) H(\mathbf{s}'|\mathbf{z}'=\boldsymbol{\zeta}) \\ &= H(\mathbf{s}') - \sum_{\boldsymbol{\zeta}\in\mathcal{Z}',\boldsymbol{\zeta}\neq\mathbf{0}} P_{\mathcal{Z}'}(\mathbf{z}'=\boldsymbol{\zeta}) H(\mathbf{s}'|\mathbf{z}'=\boldsymbol{\zeta}) \\ &= \log(|\mathcal{S}'|-1) - \frac{1}{|\mathcal{S}'|-1} \sum_{\boldsymbol{\zeta}\in\mathcal{Z}',\boldsymbol{\zeta}\neq\mathbf{0}} \mathrm{H}(\mathbf{s}'|\mathbf{z}'=\boldsymbol{\zeta}). \end{aligned} \tag{19}$$

Since $\mathbf{K}_{\mathrm{C}}$ satisfies the RIP condition and $M \geq 2k$, $\mathbf{s}'$ has an unique projection on $\mathbf{z}'$. Therefore, $\mathbf{z}'$ follows a discrete uniform distribution on the alphabet $\mathcal{Z}' - \{\mathbf{0}\}$, and

$$H(\mathbf{s}'|\mathbf{z}'=\boldsymbol{\zeta}) = H(\mathbf{s}') = \log(|\mathcal{S}'|-1), \forall \boldsymbol{\zeta} \in \mathcal{Z}' - \{\mathbf{0}\}. \tag{20}$$

Substituting (20) into (19), we have

$$\begin{aligned} I(\mathbf{s}';\mathbf{z}') &= \log(|\mathcal{S}'|-1) \\ &\quad - \frac{1}{|\mathcal{S}'|-1} \cdot (|\mathcal{S}'|-1)\log(|\mathcal{S}'|-1) \\ &= 0. \end{aligned} \tag{21}$$

Therefore, the compressive encryption process can achieve perfect secrecy. ■

Appendix B
Proof of Corollary 2

Proof: First, each entry $u^{(m)}, m = 1, \cdots, M$, of the equivalent noise vector $\mathbf{u}$ can be regarded as a linear combination of i.i.d. Gaussian random variables $K_{\mathrm{C}}^{(m,n)}$, which can be expressed as

$$u^{(m)} = \sum_{n=1}^{N} k_{\mathrm{A}}^{(n)} K_{\mathrm{C}}^{(m,n)}, \tag{22}$$

where $k_{\mathrm{A}}^{(n)}$ and $K_{\mathrm{C}}^{(m,n)}$ are the entries of the secret key vector $\mathbf{k}_{\mathrm{A}}$ and the secret observation matrix $\mathbf{K}_{\mathrm{C}}$, respectively. Using the property of linear combination of Gaussian random variables, it can be derived that $u^{(m)}$ follows a Gaussian distribution $\mathcal{N}(\mu_u, \sigma_u^2)$ with the mean $\mu_u = 0$, and the variance σ_u^2 can be calculated using the variance of $K_{\mathrm{C}}^{(m,n)}$ as

$$\sigma_u^2 = \sum_{n=1}^{N} k_{\mathrm{A}}^{(n)2} \cdot \frac{1}{M}. \tag{23}$$

Based on the Khinchin's law of large numbers, it can be derived that

$$\forall \epsilon > 0, \lim_{N\to\infty} \left\{ \left| \frac{1}{N} \sum_{n=1}^{N} k_{\mathrm{A}}^{(n)2} \right| - \mathbb{E}\left[k_{\mathrm{A}}^{(n)2}\right] < \varepsilon \right\} = 1, \tag{24}$$

where $\mathbb{E}[\cdot]$ denotes the statistical expectation operator. Then, since each entry of the secret key $\mathbf{k}_{\mathrm{A}}$ follows a uniform distribution, i.e., $k_{\mathrm{A}}^{(n)} \sim \mathrm{U}(-\xi\frac{r_2-r_1}{2}, \xi\frac{r_2-r_1}{2})$, as the length of the original sensing signal $\mathbf{s}$, i.e., N, approaches infinity, the variance of $u^{(m)}$ in (23) can be given by

$$\begin{aligned} \lim_{N\to\infty} \sigma_u^2 &= \frac{N}{M}\mathbb{E}\left[k_{\mathrm{A}}^{(n)2}\right] \\ &= \frac{N}{M}\left\{ \mathrm{Var}\left[k_{\mathrm{A}}^{(n)}\right] + \left(\mathbb{E}\left[k_{\mathrm{A}}^{(n)}\right]\right)^2 \right\} \\ &= \frac{\xi^2 N}{12M}\left(r_2 - r_1\right)^2, \end{aligned} \tag{25}$$

where $\mathrm{Var}[k_{\mathrm{A}}^{(n)}]$ denotes the variance of $k_{\mathrm{A}}^{(n)}$. This means that when the length of the sensing signal is sufficiently large, the variance of $u^{(m)}, m = 1, \cdots, M$, can be asymptotically approaching $\frac{\xi^2 N}{12M}\left(r_2 - r_1\right)^2$. ■

Appendix C
Proof of Corollary 3

Proof: The energy of the equivalent noise $\mathbf{u}$ can be represented as $\|\mathbf{u}\|_2^2 = \sum_{m=1}^{M} u^{(m)2}$. Since $\{u^{(m)}\}_{m=1}^{M}$ are i.i.d. Gaussian random variables, $\|\mathbf{u}\|_2^2$ follows a chi-square distribution with the mean of $\sigma^2 M$ and the variance of $2\sigma^2 M$. According to the concentration inequalities, when the coefficient α in (17) is relatively large, i.e., typically $\alpha = 3$, the probability that $\|\mathbf{u}\|_2^2$ falls into the interval $\left(\mathbb{E}[\|\mathbf{u}\|_2^2] - \alpha\sqrt{\mathrm{Var}[\|\mathbf{u}\|_2^2]}, \mathbb{E}[\|\mathbf{u}\|_2^2] + \alpha\sqrt{\mathrm{Var}[\|\mathbf{u}\|_2^2]}\right)$ will asymptotically approach 1. Therefore, the bound of $\|\mathbf{u}\|_2^2$ denoted by ϵ^2 can be approximately calculated as

$$\begin{aligned} \epsilon^2 &= \mathbb{E}[\|\mathbf{u}\|_2^2] + \alpha\sqrt{\mathrm{Var}[\|\mathbf{u}\|_2^2]} \\ &= \sigma_u^2 M + \alpha\sqrt{2M}\sigma_u. \end{aligned} \tag{26}$$

Substituting (13) into (26), we have

$$\begin{aligned} \epsilon^2 &= \frac{\xi^2 N}{12M}\left(r_2 - r_1\right)^2 \cdot M \\ &\quad + \alpha\sqrt{2M}\sqrt{\frac{N}{12M}}\xi\left(r_2 - r_1\right) \\ &= \frac{\xi^2 N}{12}\left(r_2 - r_1\right)^2 + \alpha\sqrt{\frac{N}{6}}\xi\left(r_2 - r_1\right) \\ &= \frac{1}{2}\sigma_0^2 + \alpha\sigma_0. \end{aligned} \tag{27}$$

Thus, combining (16) and (27), we have (17). ■

References

[1] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the Internet-of-Medical-Things (IoMT) systems security," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8707–8718, Jun. 2021.

[2] J. Andreu-Perez, D. R. Leff, H. M. D. Ip, and G.-Z. Yang, "From wearable sensors to smart implants--toward pervasive and personalized healthcare," *IEEE Trans. Biomed. Eng.*, vol. 62, no. 12, pp. 2750–2762, Dec. 2015.

[3] Z. Zhou, H. Zhang, X. Du, P. Li, and X. Yu, "Prometheus: Privacy-aware data retrieval on hybrid cloud," in *Proc. IEEE INFOCOM*, Turin, Italy, Apr. 2013, pp. 2643–2651.

[4] "Health insurance portability and accountability act of 1996," *104th Congress Public Law 104-191*, 1996.

[5] L. Wu, X. Du, M. Guizani, and A. Mohamed, "Access control schemes for implantable medical devices: A survey," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1272–1283, Oct. 2017.

[6] D. L. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[7] S. Liu, F. Yang, W. Ding, and J. Song, "Double kill: Compressive-sensing-based narrow-band interference and impulsive noise mitigation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5099–5109, Jul. 2016.

[8] H. Chi, L. Wu, X. Du, Q. Zeng, and P. Ratazzi, "e-safe: Secure, efficient and forensics-enabled access to implantable medical devices," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Beijing, China, May 2018, pp. 1–9.

[9] T. Wei, D. Su, and S. Liu, "Generative adversarial network enabled sparse signal compression and recovery for Internet of Medical Things," in *Proc. ACM UbiComp'21*, Sep. 2021, pp. 678–683.

[10] Y. Zhang, Y. Xiang, L. Y. Zhang, Y. Rong, and S. Guo, "Secure wireless communications based on compressive sensing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1093–1111, Oct. 2019.

[11] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. Annu. Allerton Conf. Commun. Control Comput.*, Urbana-Champaign, IL, USA, Sep. 2008, pp. 813–817.

[12] T. Wei and S. Liu, "Sparse learning based implantable medical device transmission against eavesdropping," in *Proc. Int. Symp. Med. Inf. Commun. Technol. (ISMICT)*, Xiamen, China, Apr. 2021, pp. 70–75.

[13] J. Wen, Z. Zhou, J. Wang, X. Tang, and Q. Mo, "A sharp condition for exact support recovery with orthogonal matching pursuit," *IEEE Trans. Signal Process.*, vol. 65, no. 6, pp. 1370–1382, Mar. 2017.

[14] C. Song, S. Xia, and X. Liu, "Improved analysis for subspace pursuit algorithm in terms of restricted isometry constant," *IEEE Signal Process. Lett.*, vol. 21, no. 11, pp. 1365–1369, Nov. 2014.

[15] F. Caltagirone, L. Zdeborová, and F. Krzakala, "On convergence of approximate message passing," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jun. 2014, pp. 1812–1816.

[16] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015.

[17] S. Liu, L. Xiao, Z. Han, and Y. Tang, "Eliminating NB-IoT interference to LTE system: A sparse machine learning-based approach," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6919–6932, Aug. 2019.

[18] S. Liu, L. Xiao, L. Huang, and X. Wang, "Impulsive noise recovery and elimination: A sparse machine learning based approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2306–2315, Mar. 2019.

[19] K. Kulkarni, S. Lohit, P. Turaga, R. Kerviche, and A. Ashok, "ReconNet: Non-iterative reconstruction of images from compressively sensed measurements," in *Proc. IEEE Conf. Comput. Vis. Pattern Reconit. (CVPR)*, Las Vegas, NV, USA, Jun. 2016, pp. 449–458.

[20] K. Gregor and Y. LeCun, "Learning fast approximations of sparse coding," in *Proc. 27th Int. Conf. Mach. Learn. (ICML)*, Haifa, Israel, Jun. 2010, pp. 399–406.

[21] S. Liu, F. Yang, J. Song, and Z. Han, "Block sparse Bayesian learning-based NB-IoT interference elimination in LTE-Advanced systems," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4559–4571, Oct. 2017.

[22] S. Liu and X. Huang, "Sparsity-aware channel estimation for mmwave massive MIMO: A deep CNN-based approach," *China Commun.*, vol. 18, no. 6, pp. 162–171, Jun. 2021.

[23] M. Borgerding, P. Schniter, and S. Rangan, "AMP-inspired deep networks for sparse linear inverse problems," *IEEE Trans. Signal Process.*, vol. 65, no. 16, pp. 4293–4308, Aug. 2017.

[24] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach," *IEEE Network*, vol. 33, no. 5, pp. 27–33, Sep.-Oct. 2019.

[25] J. Sun, F. Khan, J. Li, M. D. Alshehri, R. Alturki, and M. Wedyan, "Mutual authentication scheme for the device-to-server communication in the Internet of Medical Things," *IEEE Internet Things J.*, pp. 1–1, 2021.

[26] Y. Qian, J. Shen, P. Vijayakumar, and P. K. Sharma, "Profile matching for IoMT: A verifiable private set intersection scheme," *IEEE J. Biomed. Health Inform.*, pp. 1–1, 2021.

[27] X. Yao, W. Liao, X. Du, X. Cheng, and M. Guizani, "Using bloom filter to generate a physiological signal-based key for wireless body area networks," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10 396–10 407, Dec. 2019.

[28] H. Peng, Y. Tian, J. Kurths, L. Li, Y. Yang, and D. Wang, "Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks," *IEEE Trans. Biomed. Circuits Syst.*, vol. 11, no. 3, pp. 558–573, Jun. 2017.

[29] J. Liu, Q. Hu, R. Suny, X. Du, and M. Guizani, "A physical layer security scheme with compressed sensing in OFDM-based IoT systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dublin, Ireland, Jun. 2020, pp. 1–6.

[30] Z. Zhang, T.-P. Jung, S. Makeig, and B. D. Rao, "Compressed sensing of EEG for wireless telemonitoring with low energy consumption and inexpensive hardware," *IEEE Trans. Biomed. Eng.*, vol. 60, no. 1, pp. 221–224, Jan. 2013.

[31] A. S. Lalos, A. Antonopoulos, E. Kartsakli, M. Di Renzo, S. Tennina, L. Alonso, and C. Verikoukis, "RLNC-aided cooperative compressed sensing for energy efficient vital signal telemonitoring," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 7, pp. 3685–3699, Jul. 2015.

[32] Y. Wang, X. Li, K. Xu, F. Ren, and H. Yu, "Data-driven sampling matrix boolean optimization for energy-efficient biomedical signal acquisition by compressive sensing," *IEEE Trans. Biomed. Circuits Syst.*, vol. 11, no. 2, pp. 255–266, Apr. 2017.

[33] A. Mousavi, A. B. Patel, and R. G. Baraniuk, "A deep learning approach to structured signal recovery," in *Proc. 53rd Annu. Allerton Conf. Commun. Control Comput. (Allerton)*, Monticello, IL, USA, Sep. 2015, pp. 1336–1343.

[34] M. Borgerding and P. Schniter, "Onsager-corrected deep learning for sparse linear inverse problems," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Washington, DC, USA, Dec. 2016, pp. 227–231.

[35] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[36] E. J. Candès, J. K. Romberg, and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," *Communications on Pure and Applied Mathematics*, vol. 59, no. 8, pp. 1207–1223, May 2006.

[37] G. B. Moody and R. G. Mark, "The impact of the MIT-BIH Arrhythmia Database," *IEEE Eng. Med. Biol. Mag.*, vol. 20, no. 3, pp. 45–50, May-Jun. 2001.

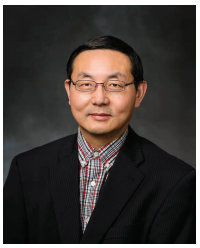
[38] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng, and H. E. Stanley, "Physiobank, physiotoolkit, and physionet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, Jun. 2000.

[39] S. Jalaleddine, C. Hutchens, R. Strattan, and W. Coberly, "Ecg data compression techniques-a unified approach," *IEEE Trans. Biomed. Eng.*, vol. 37, no. 4, pp. 329–343, Apr. 1990.

[40] Y. Zigel, A. Cohen, and A. Katz, "The weighted diagnostic distortion (WDD) measure for ECG signal compression," *IEEE Trans. Biomed. Eng.*, vol. 47, no. 11, pp. 1422–1430, Nov. 2000.

Tiankuo Wei received the B.S. degree in communication engineering from Huaqiao University, Xiamen, China in 2020. He is currently pursuing the M.S. degree with the Department of Information and Communication Engineering, Xiamen University, Xiamen, China. His research interests include compressed sensing and AI-assisted communications.

Sicong Liu (S'15-M'17-SM'22) is an Associate Professor in the Department of Information and Communication Engineering, School of Informatics, Xiamen University, China. He was a Senior Engineer in Huawei Technologies Co Ltd between 2017 and 2018. Dr. Liu received his B.S.E. and the PhD degree both in electronic engineering from Tsinghua University, Beijing, China in 2012 and 2017 with the highest honor. He was a visiting scholar in City University of Hong Kong in 2010. His current research interests are compressed sensing, AI-assisted communications, integrated sensing and communications, and visible light communications. He has authored over 60 journal and conference papers, and four monographs in the related areas. Dr. Liu won the best paper award at the ACM UbiComp 2021 CPD WS. He has served as the associate editor, TPC chair or publication chair of several IEEE and other academic journals and conferences. He is a Senior Member of IEEE, and a Senior Member of China Institute of Communications.



Xiaojiang (James) Du (S'99-M'03-SM'09-F'20) is the Anson Wood Burchard Endowed-Chair Professor in the Department of Electrical and Computer Engineering at Stevens Institute of Technology. He was a professor at Temple University between August 2009 and August 2021. Dr. Du received his B.S. from Tsinghua University, Beijing, China in 1996. He received his M.S. and Ph.D. degree in Electrical Engineering from the University of Maryland, College Park in 2002 and 2003, respectively. His research interests are security, wireless networks, and systems. He has authored over 500 journal and conference papers in these areas, including the top security conferences IEEE S&P, USENIX Security, and NDSS. Dr. Du has been awarded more than 8 million US Dollars research grants from the US National Science Foundation (NSF), Army Research Office, Air Force Research Lab, the State of Pennsylvania, and Amazon. He won the best paper award at IEEE ICC 2020, IEEE GLOBECOM 2014 and the best poster runner-up award at the ACM MobiHoc 2014. He serves on the editorial boards of three IEEE journals. Dr. Du is an IEEE Fellow, an ACM Distinguished Member, and an ACM Life Member.