Sparse Learning Based Implantable Medical Device Transmission against Eavesdropping

Tiankuo Wei*, Sicong Liu*, *Member, IEEE*
*Dept. of Information and Communication Engineering, Xiamen University, Xiamen, 361005, Fujian, China.
Email: liusc@xmu.edu.cn

***Abstract*—Due to the restrictions of computing resources and energy supply, the wireless communication security of recently emerging implantable medical devices (IMD) is still an open issue. In order to ensure privacy and security and reduce transmission power consumption, we propose a physical layer security (PLS) scheme called Sparse Learning based Encryption and Recovery (SLER) to compress and encrypt the sparse IMD sensing signal at the transmitter, and recover the sparse signal at the receiver. The encryption stage of the SLER scheme at the transmitter is conducted by a joint compression and encryption algorithm based on compressed sensing, which only requires simple matrix addition and multiplication operations. The decryption stage at the receiver adopts a pre-trained deep neural network that evolved from the conventional iterative reconstruction method, i.e., approximate message passing (AMP), to implement accurate signal recovery by learning the sparse features of the received IMD sensing signal. Simulations are performed that have verified the security performance of the SLER scheme and proved the prominent accuracy of sparse signal recovery compared with other state-of-the-art sparse approximation algorithms.**

***Index Terms*—deep learning, compressed sensing, physical layer security, eavesdropping, sparse recovery, implantable medical device**

I. Introduction

With the rapid development of Internet of Things (IoT) in the area of healthcare, numerous IoT medical devices have been applied in hospitals, clinics, and healthcare institutions to offer timely, convenient and comprehensive service. Benefit from remarkable miniaturization of basic elements and development of high-performance integrated circuits, implantable medical devices (IMD) are emerging. IMDs can be surgically implanted into the body, providing many various functions such as physiological data collection, remote health monitoring and medical treatment. Comparing with traditional medical devices, it has many advantages, such as portability, immediacy and proactivity. However, wireless communications used for data transmission tend to expose the IMDs to malicious attacks, which may lead to privacy information leakage and even life-threaten software tampering.

To handle with the potential risk of eavesdropping attacks threatening security and privacy of the patients, several solutions have been presented, such as biometric authentication methods [1], distance-based methods [2] and the external-device-dependent methods [3], [4]. However, most of the existing methods rely on external agent devices or require massive computation resources and auxiliary hardware modules. Extra embedded sensors, memories, and the execution of complicated softwares will increase the IMD energy consumption inevitably, which is unfriendly to a battery-charged and long-term-intended IMD device [5].

Therefore, physical layer security (PLS) techniques without requiring too much computational resources can be considered, which can enhance IMD security while reducing the implementation costs. Exploiting the emerging theory of compressed sensing (CS), the compression of the sparse IMD sensing signal can be implemented, and meanwhile the IMD signal can be encrypted in the framework of CS in a manner of PLS [6]–[8]. Exploiting the inherent sparsity of the IMD sensing signal, the spectral efficiency can be improved and the power consumption can be reduced to extend the life of IMDs. Specifically, a randomly generated measurement matrix can be adopted for accurate sparse recovery of the IMD sensing signal. It can be regarded as a symmetric encryption key to establish a secure communication link. In this way, a joint operation of sparse IMD signal compression and encryption are implemented simultaneously.

In the sparse recovery stage at the receiver, e.g., the programmer or a controller of a doctor, the compressed IMD signal should be accurately recovered using sparse recovery algorithms. There have been several traditional sparse recovery algorithms, such as CS-based ones like Orthogonal Matching Pursuit (OMP) [9] and Subspace Pursuit (SP) [10], and iterative sparse approximation algorithms like Approximate Message Passing (AMP) [11]. To further improve the recovery performance, the deep learning architecture is introduced to extract and learn about the sparse feature in the measured signal. For instance, learned AMP (LAMP) [12] is a deep learning based algorithm, which utilizes a deep neural network to emulate the unfolded iterations of the AMP algorithm. The deep learning based algorithms can improve the inference accuracy and accelerate the inference process comparing with traditional iterative methods.

Hence, in order to combat against malicious eavesdropping attacks on IMDs to protect the privacy and safety of the patients, in this paper, we propose a secure wireless transmission scheme for IMDs, which guarantees the privacy using the CS-based encryption and improves the transmission efficiency and

This work is supported in part by the National Natural Science Foundation of China under grants 61901403, 61971366, 61971365 and 62006201, in part by the Natural Science Foundation of Fujian Province of China under grant 2019J05001, and in part by the Youth Innovation Fund of Xiamen under grant 3502Z20206039. (*Corresponding author: Sicong Liu.*)

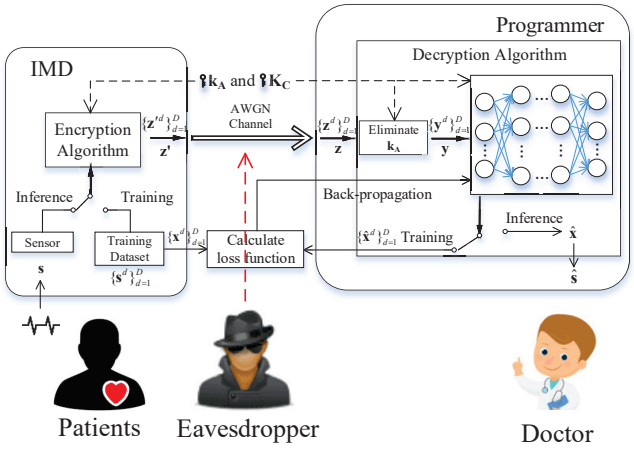

Fig. 1. IMD data transmission model with the proposed SLER scheme in the presence of eavesdropping.

recovery accuracy using sparse learning. Utilizing CS and deep learning in the encryption and sparse recovery is an efficient approach to overcome the limitation of computing and energy resources of the IMDs. The contributions of this paper are summarized as follows:

- A sparse learning based encryption and recovery (SLER) scheme is proposed, which can resist eavesdropping attacks via lightweight encryption in the framework of CS.
- A deep learning based decryption and sparse recovery algorithm is presented for accurate recovery of the original sparse IMD sensing signal, which outperforms state-of-the-art CS-based and iterative sparse approximation algorithms.

The remainder of this paper is structured as follows. The system model of the IMD sensing signal transmission system is presented in Section II. The proposed SLER scheme is introduced in Section III. Subsequently, simulation results are reported and discussed about in Section IV, followed by the conclusion in Section V.

II. System Model

The system model of IMD signal transmission considering the presence of eavesdropping in a typical healthcare scenario is illustrated in Fig. 1, where the proposed SLER scheme is utilized. There are two legitimate communication entities in the system: an IMD of the patient and a programmer at the receiver of the doctor.

- **IMD**: IMD is a small medical device implanted inside or on the body of the patient, which is embedded with modules for sensing, computing, storage and communication. The physiological data of the patient is collected by sensors, and sent to the programmer via wireless communication techniques, probably and favorably after data compression to save the costs of transmission energy and spectrum. Constrained by the power consumption and hardware size, the available computing resource of an IMD is much limited and thus complicated calculations cannot be supported.
- **Programmer**: The programmer is a portable device held by the doctor, which receives the signal containing the physiological data sent by the IMD and analyzes it for diagnosis and treatment. Different from the IMD, the programmer usually contains sufficient computing and storage resources, so that complicated calculations such as the training and inference with deep neural networks can be supported.

The adversaries are assumed to be able to eavesdrop on the medical data of the patient by wiretapping the signal transmitted in the wireless channel. The eavesdropper is assumed to be equipped with normal and limited computational capability, so the private information cannot be decoded using exhaustive methods. To be more specific, in this paper, we consider about the ciphertext-only attack (COA), i.e., the adversaries can only obtain the ciphertext, but no other information about the plaintext or the secret key can be obtained by the adversaries.

Let us consider a typical sensing interval of the IMD, and a length-N sensing signal containing the physiological data collected by the sensors in the IMD is generated, which can be modeled as $\mathbf{s} = [s_1, s_2, \cdots, s_N]^T$. Using a certain sparse representation matrix, the original non-sparse sensing signal $\mathbf{s}$ can be sparsely represented as

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

where $\mathbf{\Psi}$ is the sparse representation matrix, which can be, for instance, an $N \times N$ inverse discrete cosine transform (DCT) matrix for sparse representation of electrocardiogram (ECG) signals. Then, we can represent the sensing signal $\mathbf{s}$ using a sparse signal $\mathbf{x}$, which is the sparse representation of the original sensing signal $\mathbf{s}$. Then, using some encryption algorithm with the private key $\mathbf{k}_\mathrm{A}$ and the private measurement matrix $\mathbf{K}_\mathrm{C}$, the original sensing signal $\mathbf{s}$ is first mixed up with the private key $\mathbf{k}_\mathrm{A}$ to generate the private sensing signal $\mathbf{s}'$, and then converted to a ciphertext signal $\mathbf{z}'$ using the private measurement matrix $\mathbf{K}_\mathrm{C}$. Note that the private keys have been shared in advance between the IMD and programmer so that the eavesdropper has no access to them.

Subsequently, the ciphertext signal $\mathbf{z}'$ is transmitted from the IMD to the programmer via a wireless channel, which can be simply modeled by a transparent channel with additive white Gaussian noise (AWGN), without loss of generality. Therefore, the received signal can be expressed as

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

where $\boldsymbol{\omega}$ represents the AWGN. In the programmer at the receiver, the original sensing signal $\mathbf{s}$ is recovered utilizing the deep learning based decryption and reconstruction algorithm. Specifically, the received signal $\mathbf{z}$ is firstly decrypted to generate the sparse measurement vector $\mathbf{y}$ by eliminating the private key $\mathbf{k}_\mathrm{A}$. Then, the sparse sensing signal $\mathbf{x}$ can be obtained from the sparse measurement vector $\mathbf{y}$ using a sparse deep learning based method proposed in this paper, i.e., the

SLER scheme. And thus the original sensing signal $\mathbf{s}$ can be derived from the sparse sensing signal $\mathbf{x}$.

In the system model above, the sparsity of the signal of interest is very important for the purpose of both signal compression and sparse recovery. Fortunately, owing to the temporal correlation of many physiological signals, such as ECG as a common example, the original sensing signals can usually be represented as a sparse signal in some transform domain with a basis matrix, which is a DCT matrix in the case of ECG signals. The sparsity of physiological signals can be fully exploited in the proposed SLER scheme to facilitate the signal compression at the IMD and the sparse recovery at the receiver, which is described in detail in Section III.

III. Sparse Learning based Encryption and Recovery Scheme for Secure IMD Transmission

In this section, we describe the proposed SLER scheme in detail, which contains a joint compression and encryption algorithm in the framework of compressed sensing at the IMD, and a sparse recovery algorithm based on deep learning including both training and inference stages at the receiver. The block diagram of the proposed SLER scheme is illustrated in Fig. 2.

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

The encryption algorithm consists of two components, i.e. private key addition and compressive encryption. In the key addition process, a pseudo-random signal $\mathbf{k}_\mathrm{A}$ whose each entry follows a uniform distribution $U(\xi\frac{r_1-r_2}{2}, \xi\frac{r_2-r_1}{2})$ is generated as the private key, which is used to encrypt the original sensing signal $\mathbf{s}$ to generate the private sensing signal $\mathbf{s}'$ given by

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

where r_2 and r_1 denote the maximum and minimum entry in original sensing signal $\mathbf{s}$, respectively. And the signal power of $\mathbf{k}_\mathrm{A}$ can be adjusted by the scale parameter ξ.

In the compressive encryption process, compression and encryption can be conducted in a single operation by multiplying the signal by an $M \times N$ private measurement matrix $\mathbf{K}_\mathrm{C}$ with $M<N$, which can be expressed as

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

where the private measurement matrix $\mathbf{K}_\mathrm{C}$ is randomly generated and follows an i.i.d. Gaussian distribution, i.e., $\mathbf{K}_\mathrm{C} \sim \mathcal{N}(0, 1/M)$. Thus, the length-$N$ private sensing signal $\mathbf{s}'$ is compressed into an M-dimensional ciphertext signal $\mathbf{z}'$. The compression ratio (CR) γ for this signal compression is defined as $\gamma = (1 - M/N) \times 100\%$ in percentage.

The complexity of both steps are moderate, only involved with simple matrix addition and multiplication, which doesn't requires for massive computing resource.

B. Deep Learning Based Decryption and Sparse Recovery

As shown in equation (2), the ciphertext signal $\mathbf{z}'$ is disturbed by AWGN during transmission in the wireless channel, yielding the received signal $\mathbf{z}$ given by (2) at the programmer. After receiving the signal $\mathbf{z}$, the programmer decrypts the private key by removing the corresponding key component in the sparse measurement vector $\mathbf{y}$, and reconstructs the sparse sensing signal $\mathbf{x}$ via deep learning. Thus, the process at the receiver is composed of two steps, i.e., key elimination and sparse recovery.

In the key elimination process, the private key $\mathbf{k}_\mathrm{A}$ and the private measurement matrix $\mathbf{K}_\mathrm{C}$ are utilized for the purpose of key removing and decryption, which is given by

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

Then, the sparse measurement vector $\mathbf{y}$ that contains the information of the original sensing signal $\mathbf{s}$ and its corresponding sparse sensing signal $\mathbf{x}$ based on (1) can be obtained, which is given by

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

where $\mathbf{A}$ is an under-determined $M \times N$ observation matrix utilized in the deep neural networks of the proposed SLER scheme as a parameterized matrix. Then, according

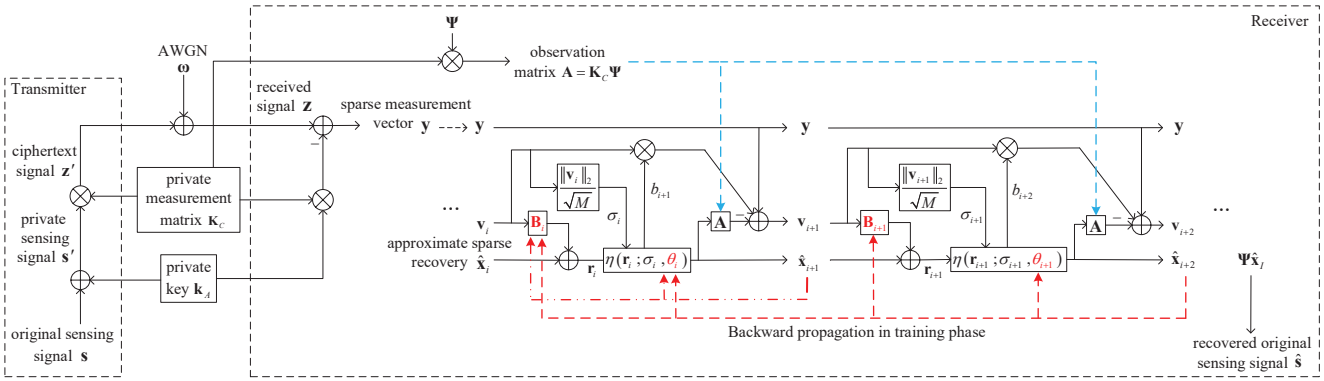

Fig. 2. The block diagram of the proposed SLER scheme.

to the sparse measurement model in (6), which is an underdetermined linear inverse problem since $M<N$, the sparse sensing signal $\mathbf{x}$ can be recovered using sparse recovery methods such as CS-based algorithms. In this paper, in order to better extract the sparse feature of the sensing signal and improve the recovery performance in severe conditions, we propose the SLER scheme based on sparse deep learning to conduct sparse recovery.

First, a sparsity-aware deep neural network emulating the iterative sparse approximation algorithm of AMP is trained using the training data obtained in advance in the training stage. Then, in the inference stage, the well-trained sparsity-aware deep neural network is utilized to find the accurate support for the sparse sensing signal $\mathbf{x}$. Specifically, as illustrated in Fig. 2, the proposed sparsity-aware deep network is actually a deep neural network with I layers evolved from the AMP algorithm with I iterations. The ith layer of the proposed deep neural network can be expressed as

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

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

where $\mathbf{v}_i$ represents residual measurement error of the ith layer, and $\hat{\mathbf{x}}_i$ is the reconstructed approximate result of the ith layer. $\eta(\cdot)$ denotes the shrinkage function used to infer the sparse vector $\hat{\mathbf{x}}_{i+1}$, which is fed by the residual measurement error calculated by $\mathbf{r}_i = \hat{\mathbf{x}}_i + \mathbf{B}_i\mathbf{v}_i$, a layer-dependent learnable tuning parameter θ_i, and the standard deviation of the measurement error σ_i that can be expressed as $\sigma_i = \frac{\|\mathbf{v}_i\|_2}{\sqrt{M}}$. Moreover, $b_{i+1}\mathbf{v}_i$ is an Onsager correction bypass which is used to decouple different layers in the network. Here, b_{i+1} can be calculated as

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

Utilizing the deep learning methods over the sparsity-aware deep neural networks in the proposed SLER scheme, the support of the sparse sensing signal $\mathbf{x}$, i.e. the locations of nonzero entries, can be learnt and recovered effectively, and the accuracy of the sparse recovery can be improved significantly. The proposed SLER scheme is composed of two stages, i.e. the training stage and the inference stage, as described in **Algorithm 1** and **Algorithm 2**, respectively. The detailed procedures of the two stages are as follows.

In the training stage, the training set $\left\{\mathbf{x}^d, \mathbf{y}^d\right\}_{d=1}^{D}$ composed of D data samples, with each including the sparse measurement vector $\mathbf{y}^d$ and its corresponding sparse sensing signal $\mathbf{x}^d$, is used for the training of the learnable parameters $\mathbf{\Theta} = \{\mathbf{B}_i, \theta_i\}_{i=0}^{I}$ in the neural network. The normalized mean square error (NMSE) is utilized as the loss function given 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 $\hat{\mathbf{x}}_i^d(\cdot)$ represents the output of the ith-layer with the input of $\mathbf{y}^d$ and parameters of $\mathbf{\Theta}_i$. For the training of learnable parameters in each layer, the previous layers with well-trained parameters are used as a whole to calculate the loss function $\mathcal{L}_i$. The parameters are updated by using the Adam optimizer and back propagation (BP) to minimize the loss, and the training error is gradually reduced until the loss function does not decrease with the number of layers, i.e., $\mathcal{L}_i \geq \mathcal{L}_{i-1}$, to avoid over-fitting caused by too many layers and parameters. Consequently, the total number of layers is set to $I = i - 1$.

In the inference stage, with the well-trained deep network, we can estimate the original sparse sensing signal $\mathbf{s}$ generated by the IMD. Firstly, the sparse measurement vectors $\mathbf{y}$ is input into the network with the already learnt parameters $\mathbf{\Theta}$ to infer the final estimated sparse sensing signal $\hat{\mathbf{x}}_I$. Then, we acquire the support of the original IMD sensing signal by $\hat{\mathbf{s}} = \mathbf{\Psi}\hat{\mathbf{x}}_I$. With the aid of the sparsity-aware deep networks, the proposed SLER scheme can reconstruct the original sensing signal with high accuracy, and achieve higher compression rate with the same reconstruction error, which is verified by the simulation results in Section IV.

The security performance of the proposed scheme can be

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

Input:

1) Training dataset of size-D, including the sparse measurement vectors $\{\mathbf{y}^d\}_{d=1}^{D}$ and the corresponding ground-truth sparse sensing signal $\{\mathbf{x}^d\}_{d=1}^{D}$

2) Observation matrix $\mathbf{A}$

Initialize $\mathbf{v}_0 = \mathbf{0}$, $\hat{\mathbf{x}}_0 = \mathbf{0}$, $\mathbf{B} = \mathbf{A}^T$, $\theta_i = 1$, $i = 0$

repeat

  (For each layer in the neural network)

  Obtain the input to shrinkage function $\mathbf{r}_i = \hat{\mathbf{x}}_i + \mathbf{B}_i\mathbf{v}_i$ and compute the value of b_{i+1} by (9)

  Calculate the value of $\hat{\mathbf{x}}_{i+1}$ and $\mathbf{v}_{i+1}$ by (7) and (8)

  Compute loss function $\mathcal{L}_i$ in (10) and update learnable parameters $\mathbf{\Theta}_i = \{\mathbf{B}_k, \theta_k\}_{k=0}^{i}$ with 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 $\mathbf{\Theta} = \{\mathbf{B}_i, \theta_i\}_{i=0}^{I}$

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

Input:

1) Sparse measurement vector $\mathbf{y}$

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

Initialize $\mathbf{v}_0 = \mathbf{0}$, $\hat{\mathbf{x}}_0 = \mathbf{0}$

Perform a single-trip feedforward operation using the trained network and obtain the final estimated value of $\hat{\mathbf{x}}_I = \eta(\mathbf{r}_{I-1}; \sigma_{I-1}, \theta_{I-1})$

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

Output:

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

theoretically guaranteed from the following two perspectives of view. For one thing, it has been proved that *measurement as a key* can achieve Maurer-sense perfect security [13], i.e., when N approaches infinity, the mutual information between the original sensing signal and the eavesdropped signal is zero, i.e., $\lim_{N\to\infty} I(\mathbf{s};\mathbf{z}) = 0$. On the other hand, it is also verified that the computational security is guaranteed, i.e., when an eavesdropper uses exhaustive methods to guess the key using an incorrect key, the probability of getting a wrong reconstruction result is 1 [14]. Moreover, the key addition process further improves the confidentiality performance through destroying the sparseness of the plaintext, making it almost impossible to achieve accurate signal reconstruction even if the private measurement matrix $\mathbf{K}_{\mathrm{C}}$ is known by the adversaries. This is because the $\mathbf{K}_{\mathrm{C}}$-known eavesdropping scenario can be approximately regarded as a sparse reconstruction problem given by $\mathbf{y} = \mathbf{K}_{\mathrm{C}}(\mathbf{s} + \mathbf{k}_{\mathrm{A}}) = \mathbf{A}\mathbf{x} + \mathbf{n}_0$ with a white noise $\mathbf{n}_0 = \mathbf{K}_{\mathrm{C}}\mathbf{k}_{\mathrm{A}}$, and the noise power is related with the private key $\mathbf{k}_{\mathrm{A}}$. It can be noted that the sparse recovery error is doomed to be unacceptable due to the intensive noise power.

IV. Simulation Results and Discussions

To evaluate the anti-eavesdropping and sparse recovery performance of the proposed SLER scheme, simulations are performed using ECG signals as the IMD sensing signal in the scenario of compressive encryption, wireless transmission and sparse recovery. The ECG signals are obtained from the experimental record 100 in the MIT-BIH Arrhythmia database [15], with a sampling rate of 360 Hz. The ECG signal in the record is firstly divided into several length-500 signals that are used as the original sensing signal $\mathbf{s}$ as described in (1) in Section II. They are then used to generate the training and test datasets.

For the training dataset, we can obtain a training data sample pair composed of a sparse sensing signal $\mathbf{x}$ and the corresponding sparse measurement vector $\mathbf{y}$ using (1) through (5), where the AWGN $\boldsymbol{\omega}$ is generated using standard Gaussian distribution with zero mean and variance of one, and then scaled to represent different values of SNR. By repeating this process 1000 times, we can generate the training set with 1000 samples, i.e., $\{\mathbf{y}^d, \mathbf{x}^d\}_{d=1}^{D}$, $D = 1000$. The test set is also generated in a similar way. The training process is implemented in a computing platform with a CPU of Intel Xeon E5-2620 v4 and a GPU of GeForce GTX 1080Ti running Tensorflow 1.14.0 in Python. The Adam optimizer and the gradient descent algorithm are used for the training of the deep network, and the initial learning rate is 10^{-3}. In order to further improve the fitting accuracy of the network, the learning rate is gradually refined by a ratio of 0.5, 0.1 and 0.01, respectively. Moreover, to prevent over-fitting during training, the depth of the proposed sparsity-aware deep neural network is adjusted with a validation set.

We evaluate the simulation results with a metric called percentage root-mean square difference (PRD), which is an important indicator of the reconstruction quality of ECG signals. The PRD denoted by λ between the original sensing signal $\mathbf{s}$ and recovered sensing signal $\hat{\mathbf{s}}$ is defined as

$$\lambda = \frac{\|\hat{\mathbf{s}} - \mathbf{s}\|_2}{\|\mathbf{s}\|_2} \times 100\%. \tag{11}$$

Moreover, we adopt a PRD-based evaluation metric proposed by Zigel *et al* to reflect the subjective recovery performance, which classifies the PRD value below 9% as "good", and "bad" otherwise [16].

In order to verify the effectiveness and confidentiality of the proposed SLER scheme, comparative experiments using SLER and other benchmark schemes including CS-based algorithms such as OMP [9] and SP [10], and iterative sparse approximation algorithms like AMP [11], are conducted in a wireless IMD transmission system in the presence of an eavesdropper. The reconstruction accuracy with the private key scale parameters $\xi = 1$ and $\xi = 0.5$ are recorded in Figs. 3 and 4, respectively, where the compression rate is $\gamma = 50$. The solid lines represent the signal recovery error of the legitimate user, while the dashed lines and dotted-dashed lines represent the accuracy of the signal recovered by the eavesdropper when the private measurement matrix $\mathbf{K}_{\mathrm{C}}$ is unknown and known to the receiver, respectively. Here, without loss of generality, we assume that the eavesdropper can learn the statistical characteristics of the private keys and use a random guess of the private keys to perform sparse recovery. Since the adversary can hardly obtain the confidential personal medical data of the patients for the purpose of training, it is very difficult for the adversary to generate the training dataset with sufficient amount of training data. Thus, the eavesdropper cannot train a deep neural network eligible for sparse recovery. Only existing benchmark schemes, including CS-based ones and iterative sparse approximation, can be used by the eavesdropper.

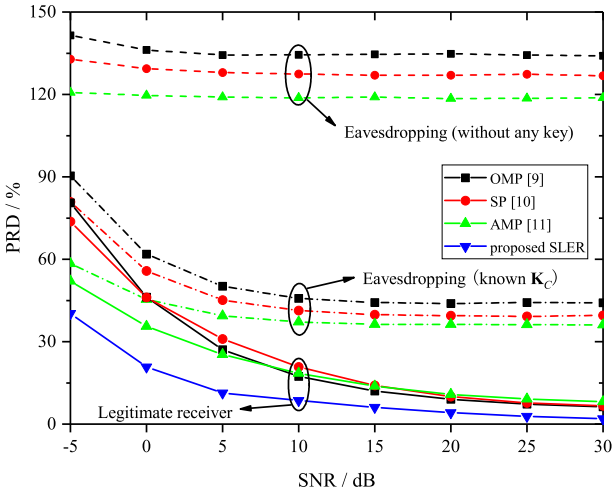

Fig. 3. Reconstruction accuracy of legitimate receiver and eavesdropper using the proposed SLER and other benchmark schemes with the private key scale parameter $\xi = 1$.

To evaluate the sparse recovery performance, the reconstruction accuracy in terms of PRD of the proposed SLER scheme

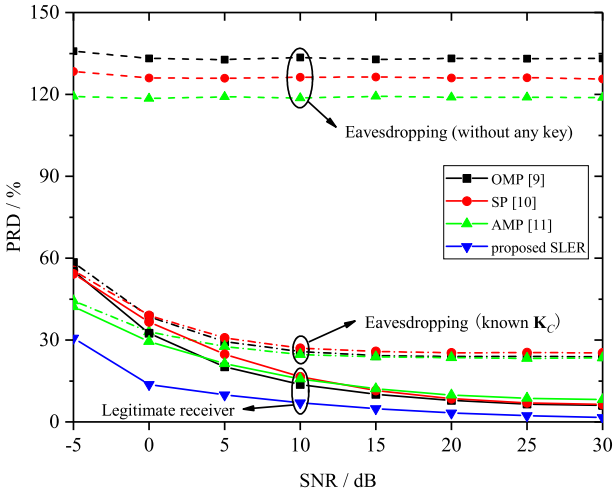

Fig. 4. Reconstruction accuracy of legitimate receiver and eavesdropper using the proposed SLER and other benchmark schemes with the private key scale parameter $\xi = 0.5$.

and the existing benchmark schemes indicated by PRD are compared in Figs. 3 and 4, with different scales of the private key. It can be seen that compared with the existing methods, the PRD of the proposed SLER scheme is reduced to less than 2% at the SNR of 30. Therefore, in harsh communication environments with intensive background noise, the proposed SLER scheme can achieve higher reconstruction accuracy.

To evaluate the security performance of the proposed SLER scheme against eavesdropping, it can be seen from the dashed lines in Figs. 3 and 4 that the recovery error of the eavesdropper without knowing any keys exceeds 110%, which is far higher than the "bad" criterion, which shows that the eavesdropper cannot acquire the accurate original sensing signal. As an obvious contrary, the recovery accuracy of the proposed SLER scheme is shown to be significantly higher, which verifies the security performance of the legitimate receiver against eavesdropping. Subsequently, we assume that the private measurement matrix $\mathbf{K}_{\mathrm{C}}$ has been revealed to the eavesdropper, and the quality of illegally received signal is still "bad". Moreover, comparing Fig. 3 and 4, it can be observed that the encryption using a private key with larger scale ξ will increase the recovery error of the eavesdropper, which means the confidentiality is improved using a private key signal with more power. This leads to an open problem that we can seek for a tradeoff between the key signal power and the anti-eavesdropping confidentiality, and thus improving the energy efficiency while protecting the security.

V. Conclusion

In this paper, a physical layer security scheme called SLER based on sparse deep learning is proposed for secure IMD sensing signal compression and wireless transmission against eavesdropping, which significantly improves the confidentiality and spectral efficiency. The scheme is composed of a lightweight compressive encryption algorithm and a decryption and recovery algorithm based on sparse learning. Joint compression and encryption are achieved by exploiting the inherent time correlation and the sparse feature of the sensing signal in the DCT domain, and accurate sparse recovery is implemented by learning the sparse feature of the sensing signal. Simulation results show that the proposed SLER scheme can resist eavesdropping attacks effectively and improve the recovery accuracy compared with existing CS-based and iterative sparse approximation algorithms. Furthermore, the proposed SLER scheme is promising in other communication systems, especially for the resource-constrained scenarios like IoT applications.

References

[1] X. Hei and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," in *2011 Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011, pp. 346–350.

[2] B. Kim, J. Yu, and H. Kim, "In-vivo NFC: Remote monitoring of implanted medical devices with improved privacy," in *Proc. 10th ACM Conf. Embedded Netw. Sensor Syst.*, Toronto, Ontario, Canada, Nov. 2012, pp. 327–328.

[3] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *2011 Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011, pp. 1862–1870.

[4] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: New directions for implantable medical device security," in *Proc. USENIX HotSec*, San Jose, CA, USA, Jul. 2008, pp. 1–7.

[5] H. Zhang, M. Feng, K. Long, G. K. Karagiannidis, V. C. M. Leung, and H. V. Poor, "Energy efficient resource management in SWIPT enabled heterogeneous networks with NOMA," *IEEE Transactions on Wireless Communications*, vol. 19, no. 2, pp. 835–845, 2020.

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

[7] N. Wang, T. Jiang, W. Li, and S. Lv, "Physical-layer security in internet of things based on compressed sensing and frequency selection," *IET Commun.*, vol. 11, no. 9, pp. 1431–1437, Jun. 2017.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[14] 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.

[15] 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.

[16] 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.