IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received December 1, 2019, accepted December 10, 2019, date of publication December 18, 2019,
date of current version December 31, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2960603

Study on Secrecy Capacity of Wireless Sensor Networks in Internet of Things Based on the Amplify-and-Forward Compressed Sensing Scheme

JIAN-LAN GUO[1], YU-QIANG CHEN[1], HUAI-DE YANG[1], CHIEN-MING CHEN[2], YEH-CHENG CHEN[3], HUIYU ZHANG[4], AND ZHIYU ZHANG[5]

[1]Department of Computer Engineering, Dongguan Polytechnic, Dongguan 523808, China
[2]College of Computer Science and Engineering, Shandong University of Science and Technology, Shandong 266510, China
[3]Department of Computer Science, University of California, Davis, CA 95616, USA
[4]Department of Electronic Information Engineering, Liangjiang International College, Chongqing University of Technology, Chongqing 401135, China
[5]College of Mechanical and Electrical Engineering, Jilin Institute of Chemical Technology, Jilin 132022, China

Corresponding author: Chien-Ming Chen (chienmingchen@ieee.org)

This work was supported in part by the National Natural Science Foundation of China under Grant 61170305 and Grant 61106019, in part by the Science and Technology Research in Department of Education of Guangdong Province under Grant 2017GKTSCX104 and Grant 2018GKTSCX070, in part by the Guangdong Philosophy and Social Sciences Project under Grant GD18CSH01, in part by the Guangzhou Science and Technology Project under Grant 201904010095, in part by the Dongguan Polytechnic Research Fund Project under Grant 2018a01, and in part by the Science and Technology Project of Guangdong Province 2014A010103002.

ABSTRACT The wireless sensor networks is a new technology for information acquisition and processing, which includes the techniques of sensor, computer, Internet of Things and network. Due to the fragility of wireless sensor networks, the security issue has become a prevalent concern in the wireless communication for Internet of Things . This paper offers a deep insight to the secrecy capacity of wireless sensor network and a calculable threshold of capacity based on the amplify-and-forward (AF) compressed sensing scheme. Moreover, we provide a feasible algorithm based on augmented Lagrange method for source reconstruction for the legitimate nodes and un-authorized nodes. Furthermore, we also discuss the impact of the numbers of active sensor nodes, relay nodes and eavesdropper nodes to the secrecy capacity. Simulation results demonstrate the correctness of the derived secrecy capacity.

INDEX TERMS Internet of Things, wireless sensor networks, physical layer security, compressed sensing, distributed strategy.

I. INTRODUCTION

The wireless sensor network is a comprehensive network system [1]–[5] (Wireless Sensor Networks, WSN), which has the characteristics of distributed that connects the network by letting physical sensors spread wireless communication in different areas. WSN can effectively realize the physical data real-time acquisition and transmission management, which is widely used in aerospace, intelligent transportation, environmental monitoring, health care and other fields. Generally, WSN sensor is limited in the power energy, communication ability and the node calculation ability. In addition, WSN has a large number of sensor nodes, wide range of distribution, strong network dynamics, large perceived data transmission flow, which brings great challenges to its basic theory and engineering research.

The WSN has been widely used in military, industrial and agricultural, commercial, environmental science, and many other fields. Many of these field are for security, security has become a wireless sensor network is one of the main obstacles toward practical application, caused the wide attention of researchers both at home and abroad [6]–[9].

How the node calculation speed, the power energy, communication ability and storage space are very limited, through the design of security mechanism, provide confidentiality protection and authentication function, prevent all kinds of

The associate editor coordinating the review of this manuscript and approving it for publication was Mu-Yen Chen.

malicious attacks, for WSN to create a relatively safe work environment [17]–[22], is a relationship to the wireless sensor network can truly practical key issues. Recently developed gradually compressed perception technology [10], [11] showed that: If its signal characteristics of compressible or sparse transformation can be used a small amount of random linear observation to reconstruct signal. Therefore, it is a feasible and effective means to improve the quality of service QOS in use of data compression perception technology processing node data collecting. At the same time, the use of compression perception technology can realize the wireless sensor network secure communication on the physical plane, the encryption algorithm based on compressed sensing technology, also known as compressed wireless sensing technology [12]–[16]. Specifically, the technology will be taken by each sensor node in the WSN's perception of the data compression late-development sent to the data fusion center, unified by the data fusion center to deal with data.

At first, some traditional compression methods are used to optimize the WSN network data acquisition and transmission, but the efficiency is not high. In order to improve the efficiency, in recent years, some people try to use the theory of compressed sensing (CS) to solve this problem [6], [8], [17]–[42]. The compressed wireless sensing method proposed by l. Baraniukrg *et al.* [8] and Agrawal and Vishwanath [6] must encrypt and decrypt the wireless network communication process by exchanging the sensing matrix as the secret key. The disadvantage of this strategy is that once the eavesdropper steals the sensing matrix information, the security of the whole communication will not be guaranteed. Jahanshahi *et al.* [31] presented a novel compressed sensing (CS)acquisition and joint recovery of spatiotemporal correlated signals algorithm for effective data collection and precise sensors data streams reconstruction in wireless sensor networks. Zhang *et al* [32] proposed a data collection algorithm to reduce energy consumption and resist packet loss, Each cluster head formulates a sparsest random measurement matrix (SRMM) via the received data to avoid the measurement of the lost node and decrease the number of measurements, which reconstructs the entire network data to reduce energy consumption, but the time correlation of node readings is not considered. Singh *et al.* [33] proposed a new data acquisition scheme which is based on compressed sensing (CS) with on-demand explosion of random walks (RWs) for improving the lifespan of wireless sensor networks (WSNs) without compromising its detection capability, but this scheme is only suitable for large WSN, and the improvement is not obvious for small sensor network. Li *et al.* [34] proposed a new detection method, which sends the forged data nodes to the fusion center according to its own observation results, thus improving the detection effect of distributed sparse signals. Zhang *et al.* [35] discussed the design of compressed sensing matrix with multiple measurement vectors, and then proposed three different design methods of sensing matrix, but which only applied to small vehicle network. Caione *et al.* [36] proposed a new distributed compressed sensing method, which provides a new idea for data compression and sampling in WSNs. Xie *et al.* [37] proposed the semi-tensor compression sensing, which breaks through the traditional compression-aware dimension matching limitation and greatly reduces the storage space. Maheshwari *et al.* [38] proposed a secure communication and firewall architecture for Internet of things applications. Unfortunately, they only upload a single data analysis to the data source node, and apply the CS technology to the intermediate node, which is not used in the leaf node. Moreover, the relationship between node energy loss, network delay, CS compression rate and average packet arrival rate is not discussed.

Currently popular compression wireless sensing method [13] must be through the exchange of perception matrix as the secret key to decrypt the encrypted wireless network communication process, it is disadvantage that once the eavesdropper steal to the perceived matrix information, the security of the whole process of communication will not be guaranteed. In addition, the use of compression perception technology to realize point-to-point wireless sensor network security communication research has conducted more thorough, but the technology for distributed mass sensor with wireless network is not enough in-depth research. Based on the analysis of the above two points, this paper tries to from the communication perspective, the physical first wireless sensor network model is given and the necessary assumptions. Next to analysis of three phase bring noise amplifier forward under the circumstance of compressed sensing strategy of a detailed, the perception, projection and reconstruction phase. In particular, in view of the signal reconstruction stage is given based on augmented Lagrangian optimization methods of reconstruction algorithm. Finally, the wireless network communication compressed sensing strategy under the security capacity of quantitative analysis, the secrecy capacity of the upper and lower estimate formula is given. In the simulation experiments, it detailed discussion secrecy capacity threshold method of calculated, and to explore the safety of the compressed sensing strategy under different parameter Settings in the quantification of secrecy capacity.

The paper is organized as followsčž the first part is a brief introduction of WSN and compressed sensing theory; the second part discusses the system modeling; the third part discusses the compression of WSN network security capacity sensing strategy; the fourth part has made the corresponding simulation experiments, and to analyze and discuss the performance index. The conclusion is given in the end.

II. SYSTEM MODEL

A. CS THEORY

The traditional framework of compression theory is showed in Figure 1. The data source needs to sample the complete signal information and then transmit it to the destination. Obviously, the traditional compression process is based on the full information sampling, so it needs a large amount

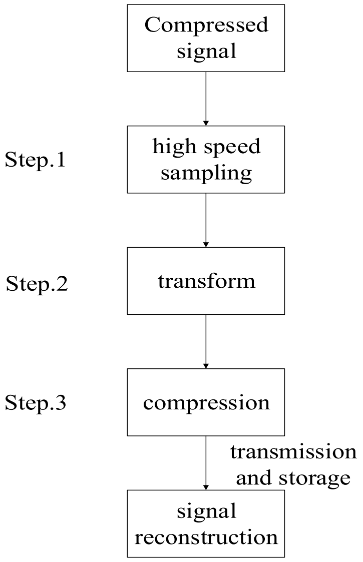

FIGURE 1. The traditional framework of compression theory.

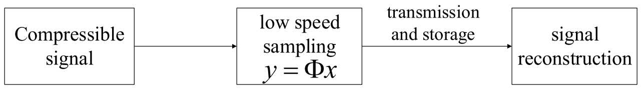

FIGURE 2. Compressed sensing theory framework.

of sampling resources. It is not desirable for the WSN data source node with limited energy and storage capacity.

In recent years, CS technology has been a research hotspot of the field of signal processing. The rate of acquisition of the original signal is much less than that of Nyquist. The sampling and compression of information are combined into one step, and the compression of the signal is obtained directly, which is not necessary for the Nyquist sampling. The CS theoretical framework is shown in figure 2.

First, the signal x ∈ RN is transformed by sparse:

$$x = \sum_{i=1}^{N} z_i G_i \quad or\ x = Gz \tag{1}$$

The sparse representation of the original signal is z ∈ RN, where G is the sparse domain of the signal, only K components is important in the Z; Find a suitable M * N dimensional perception matrix A, the Z matrix multiplication to obtain the X compression sampling value:

$$y = Az \tag{2}$$

The combined mode (1) and (2) can obtain the low speed compression sampling mode:

$$y = AGTx = \Phi x \tag{3}$$

where $\Phi = AGT$ called CS measurement matrix, Φ and G are best not related with each other.

The generation method of Φ are shown in the relevant literature [1]–[3]. One of the most common ways is to randomly generate a M x N matrix of mean 0, variance matrix Gauss random distribution of 1 /M as measuring array diameter. Sparse matrix G can be a Fourier orthogonal transform matrix but also a wavelet orthogonal transform matrix.

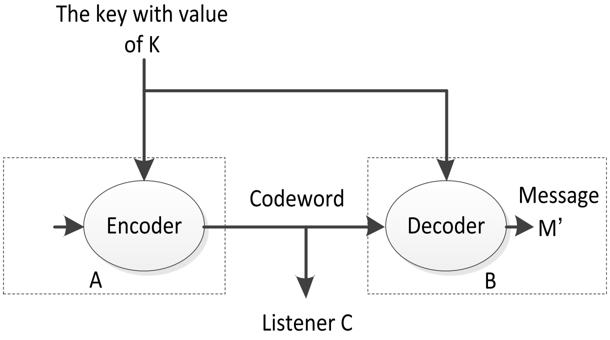

FIGURE 3. Shannon model of secrecy system.

B. APPLICATION OF COMPRESSED SENSING IN WIRELESS SENSOR NETWORKS

The WSN workflow is that the leaf node is responsible for collecting the raw data and transmitting it to the forwarding node (Upper node). The Upper node not only collects the data transmitted by its subordinate nodes (Leaf nodes and the lower Upper nodes), but also collects the data of its own region, and then transfers it to the Sink node. The central idea of this model is to reduce the length of the data acquisition and transmission by using the CS compression technology in the data source node (including the leaf nodes and intermediate forwarding nodes). Finally, the compressed data of each source node is transmitted to the data convergence center through the intermediate forwarding node, and then the original data sequence of each node is restored by CS reconstruction technique.

C. THE SYSTEM MODEL

Generally speaking, the secret communication contains two meanings: the receiving end of the target receives and recovers the sending information without error, and also ensures that other users can not obtain any information. The basic principles of secure communication is shown in Figure 3 which was elaborated by Shannon in 1949 for the first time. A is trying to send a message M which was encoded as codeword X to the legitimate receiver B. However the codeword X have been monitored completely by C. In other words, the wiretap channel is an error free channel, which is the worst case of secure communications. In the actual communication system, the noise always exists in various forms, but through strong error correction mechanism, we can ensure that the message is recovered at the receiver with any small error probability.

In general, the physical layer security problem of a particular WSN model is studied. Firstly, the security capacity of the network is analyzed theoretically, and the security capacity area of the network is obtained. The security capacity is defined as the maximum achievable communication rate that the confidential information is reliably received by the target receiver and the illegal receiver cannot obtain any useful information. In the non-degenerate discrete channel, it is equivalent to the difference between the communication channel capacity and the wiretap channel capacity. The analysis of wireless channel security capacity is the basis of physical layer security research, which will provide theoretical basis for further research. Information theory is the basis of analyzing and studying information, information entropy, communication system, data transmission, cryptography, data compression and so on.

This article will discuss wireless sensor network model and its communication security, which is composed of many sensors placed in the spatial distribution of a wireless network, These devices using sensors at different location of the collaborative monitoring of physical or environmental conditions (such as temperature, sound, vibration, pressure, etc.). Wireless sensor network has the organization way of working, this is decided by the characteristics of the wireless sensor itself. Due to unable to determine the position of the wireless sensor nodes in advance, also cannot clear relationship between the location of the nodes around it, As a result, some nodes in the work is likely to lose effectiveness because of energy shortage, the other nodes will be added in make up for the failure of nodes, There are some nodes were adjusted to a dormant state, these factors determine the self-organization mode of wireless sensor networks.

Specifically, the setting of wireless sensor network model is shown in figure 4, including, S sensor nodes, K a number of sensor nodes, R relay node number and E the passive eavesdropping malicious node number. we denoted by $K(n)$ discrete time n the number of sensors in the activation conditions, At this point the sensor value is marked $x_K(n)$, only $K(n)$ elements are nonzero, The rest of the elements $Q(n) = S - K(n)$ are zero, there are $Q(n)$ sensor nodes keep sleep. In this paper, considering:

(I) Data fusion center has n time accurate channel between the sensor node $K(n)$ and relay node R information. The channel information can generally through the design training pilot sequences and through channel estimation. In addition, hacking node set ε is not the channel information, On the contrary, the eavesdropper $K(n)$ only a weakening of the channel matrix with node collection information.

(II) Data fusion center to be interested in the signal of the second order statistics. At the same time the information was used to estimate channel training phase, the eavesdropper cannot acquire adequate access to information. measured value $x(n)$ Satisfy the Gaussian distribution $x(n) \sim N(0, \sigma^2 I_S)$, and irrelevance $E(x^T(n)x(n-1)) \neq 0$, There is an relevance between adjacent elements $E(x_i(n)x_j(n)) \neq 0$, $i, j \in S$.

Assumption I from the perspective of the physical layer to ensure the data fusion center than hacking nodes have better channel conditions. Assumption II Describes with the statistical features of spatial and temporal correlation sensors, this feature ensures a sensor through a few $K(n)$ information acquisition can real-time reflect the current state of the environment, Improve the sensor energy utilization, and simplifies the network complexity, improve the performance of wireless sensor network communication.

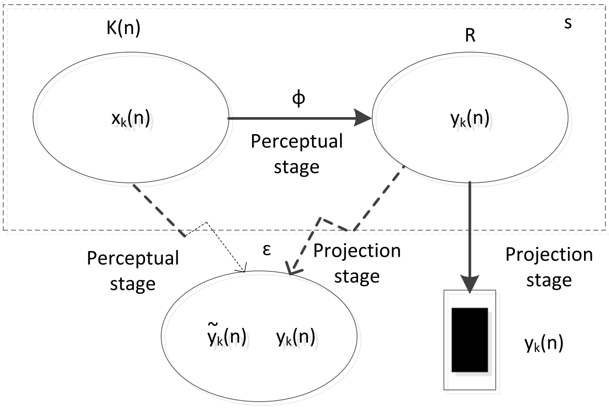

FIGURE 4. MAC scenario including $K(n)$ note of activate, R relay node, E hacking node and a data fusion center.

III. ZOOM FORWARD COMPRESSED SENSING STRATEGY PROBLEM OF WIRELESS SENSOR NETWORK SECURITY CAPACITY

A. ZOOM FORWARD COMPRESSION STRATEGY PERCEPTION

Based on the amplification forward compression perception strategy includes three phases:

(I) perception stage: sensor nodes collect data, perception based on intrinsic time correlation method [8] to select an available distributed cognitive nodes which are most relevant readings. The collected readings d sparse characteristics, that is, only a sensor in working state, the rest of the sensor is dormant. This sensor data collected will be in the form of time synchronization and sent to the relay node. In this phase, it is assumed that access to the perception of the matrix of hacking node $\hat{\Phi} \in R^{E \times S}$.

(II) The projection phase: because the channel has multiple access (MAC), so that each relay node receives is linear aliasing signal $x_K(n)$, the aliasing modeling is multiple access channel (MAC) matrix $\Phi \in R^{R \times S}$. Forwarding (AF) relay node to amplify the orthogonal way to send forward (such as frequency division multiplexing) signals to the data fusion center. For system security is very high at this stage, although the eavesdropper can fully obtained by signal sent by a relay, but these signals are actually have perceived matrix coding, so the eavesdropper Φ in unknown circumstances will not be able to decode the useful signal.Send a linear combination of signals actually provides a spontaneous protection mechanism, the earliest to as for network coding mechanism, and made full discussion in [8], [9].

This paper focused on the perceptual stage of disables the discussion.

(III) Reconstruction phase: data collected for vector fusion center for processing, in general, can by solving the minimum norm:

$$P1 \quad \min_{x(n)\in R^K} \|x(n)\|_0 \qquad s.t.\ y(n) = \Phi x(n) + e(n) \tag{4}$$

To realize the signal $x(n)$ recovery, among $e_0(n)$ for white Gaussian noise signal. In order to ensure the accuracy signal can be restored, model (4) must meet the limited nature of isometric (RIP) [7], [8] the constraint conditions:

$$(1-\delta_K)\,\|x(n)\|^2 \le \|\Phi x(n)\|^2 \le (1+\delta_K)\,\|x(n)\|^2 \tag{5}$$

Among $\delta_K \in [0, 1]$, the conditions of (5) the results of the equivalent to require all symmetric $\Omega = \Phi\Phi^T$ matrix $[1-\delta_K, 1+\delta_K]$ eigenvalue interval values.

Assume that hacking sensors can through collaboration eavesdropping, hacking can also signal l_0 is acquired through the node of minimum norm optimization to achieve $x(n)$ recovery:

$$P2 \quad \min_{x(n)\in R^K} \|x(n)\|_0 \qquad s.t.\ y_1(n) = (\hat{\Phi}+\Sigma)x(n) + e_1(n) \tag{6}$$

Type (6) of the MAC matrix perception, says there is estimation error of the random matrix, it meet the zero mean and variance of the Gaussian distribution, to Gaussian white noise signal. Corresponding to the ground, to ensure the signal accurately, the optimization model (6) also need to satisfy the constraints of the limited nature of equidistant (RIP):

$$(1-\hat{\delta}_K)\,\|x(n)\|^2 \le \left\|(\hat{\Phi}+\Sigma)x(n)\right\|^2 \le (1+\hat{\delta}_K)\,\|x(n)\|^2 \tag{7}$$

One of $\hat{\delta}_K \in [0, 1]$. Conditions (7) the results of the equivalent to the requirements of symmetric matrix $\hat{\Omega} = \hat{\Phi}\hat{\Phi}^T$ all the characteristics of the value within $[1-\hat{\delta}_K, 1+\hat{\delta}_K]$ the interval values.

B. APPLICATION ZOOM FORWARD COMPRESSION UNDER THE STRATEGY OF SIGNAL RECONSTRUCTION

For legitimate end and illegal end, all need by solving the model (3) and (4) reconstruction signals, because the norm optimization model is a np-hard problem, signal could not be gotten by direct solution, so this article USES the flabby optimization techniques, such as augmented Lagrangian method to implement the accurate reconstruction of signals. Augmented Lagrangian method [12] is modified algorithm of Lagrange function. Usually require the outer penalty function method for broadening factor gradually tends to infinity, the objective function of hazen matrix tend to be morbid, destabilize the calculation results. The augmented Lagrangian function method by constructing exact penalty function, the choice of augmented factor by its greater than some positive number (threshold value) can ensure minimization function converge to the optimal solution of the original optimization problem. Multiplier method on convergence of iterations also significantly less than the general penalty function method, the theory and practical application show that multiplier method is a good method to solve the optimization problem. In legal side, for example, reconstruction model (4) to:

$$P1 \quad \min_{x(n)\in R^K} \|x(n)\|_p \qquad s.t.\ y(n) = \Phi x(n) + e(n) \tag{8}$$

In view of the optimization model (8), we can be converted into sequence for solving unconstrained optimization model

$$\min_{x(n)} F(x(n), \lambda, C_k) = \sum_{i=1}^{n} |x_i(n)|^p + \lambda^T (y(n) - \Phi x(n)) + \frac{C_k}{2}\,\|y(n) - \Phi x(n)\|_2^2 \tag{9}$$

To approximate solution of original problem. Type (9) of the introduction of the augmented factor C_k can be understood as to punishment of noise arising from the model, in order to achieve the goal of noise suppression. To (9) about $x(n)$ the optimization of gradient direction:

$$\frac{\partial F}{\partial x(n)} = \frac{\partial J(S)}{\partial x(n)} + \Phi^T\lambda + C_k\Phi^T(\Phi x(n) - y(n)) \tag{10}$$

Through mathematical deduction, can get the following equations of expression:

$$x(n) = \frac{1}{C_k}(\frac{p}{C_k}\Pi(x(n)) + \Phi^T\Phi)^{-1}\Phi^T(C_k y(n) - \lambda) \tag{11}$$

Among them $\Pi(x(n)) = \mathrm{diag}(|x_1(n)|^{p-2} \cdots\cdots |x_n(n)|^{p-2})$ Because, $K \ll S$ have the following result is derived:

$$(\frac{p}{C_k}\Pi(x(n)) + A^TA)^{-1}A^T = \frac{C_k}{p}\Pi^{-1}(x(n))\Phi^T[\frac{C_k}{p}\Phi\Pi^{-1}(x(n))\Phi^T + I]^{-1} \tag{12}$$

We through the matrix transformation optimization iteration method to solve:

$$x^{(k+1)}(n) = \frac{1}{C_k}\Pi^{-1}(x^{(k)}(n)) \cdot \Phi^T \cdot G_k^{-1} \cdot b_k \tag{13}$$

Among them

$$G_k = \Phi\Pi^{-1}(x^{(k)}(n))\Phi^T + \frac{p}{C_k}I \qquad b_k = \lambda_k - C_k y(n) \tag{14}$$

As you can see from the type (13), a matrix G_k is a symmetrical positive definite reversible phalanx, based on the augmented Lagrangian function method, augmented factor G_k values just take an incremental but limited regular real can make type (13) converge to the optimal solution, as follows:

$$C_{k+1} = C_0 + \alpha k, \quad \alpha > 0 \tag{15}$$

Lagrange multiplier vector by means of iterative also won:

$$\lambda_{k+1} = \lambda_k + C_k(\Phi x^{(k)}(n) - y(n)) \tag{16}$$

Illegal end also can use the same algorithm for signal reconstruction, however due to illegal end on perception matrix can only get a poor version, thus reconstruction effect is poorer, and the section will discuss quantitative signal reconstruction after the whole wireless sensor the security capacity of the network.

C. BASED ON THE ZOOM FORWARD SECRECY CAPACITY IS DERIVED UNDER COMPRESSION PERCEPTION STRATEGY

Analysis according to the first two sections, you can see that in order to ensure the security of wireless network communication, using the eavesdropper cannot get accurate perception of the matrix that physical characteristics effectively provides a spontaneous protection mechanism, the encoding mechanism to the network coding at the earliest. This set out from the physical layer security mechanism to the extent to which the safety of the wireless network transmission, this need through quantitative analysis of tumble zoom forward secrecy capacity under compressed sensing strategy, to get the general situation of wireless sensor network security capacity. To this end, we derive the following theorem is given.

Theorem 1: In the case of passive eavesdropping, zoom forward compression perception strategy under the secrecy capacity of wireless sensor network:

$$I(y(n), \hat{y}(n)) = \frac{1}{2}log_2\{\frac{det[\sigma_0^2 I_R + \sigma^2\Phi\Phi^T]}{det[\sigma_0^2 I_E + \sigma^2\hat{\Phi}\hat{\Phi}^T]}\} \tag{17}$$

The capacity of wireless sensor network security are limited to:

$$I(y(n), \hat{y}(n)) \le \frac{1}{2}log_2\frac{[\sigma_0^2 + \sigma^2(1+\sqrt{K/R})^2]R}{[\sigma_0^2 + \sigma^2(1-\sqrt{K/E})^2]E} \tag{18}$$

The lower limit of wireless sensor network security capacity as follows:

$$I(y(n), \hat{y}(n)) \ge \frac{1}{2}log_2\frac{[\sigma_0^2 + \sigma^2(1-\sqrt{K/R})^2]R}{[\sigma_0^2 + \sigma^2(1+\sqrt{K/E})^2]E} \tag{19}$$

Proof: first of all, we carried out on the perceived matrix eigenvalue analysis of necessary. For relay nodes, might as well assume that perception matrix of the Wishart matrix, the eigenvalue of the matrix satisfies the following Marcenko - Pasur [9] distribution, the probability density function is:

$$f_\Omega(\lambda) = (1 - \frac{1}{\alpha})^+\delta(\lambda) + \frac{\sqrt{(\lambda - \lambda_{\min}) \times (\lambda_{\max} - \lambda)^+}}{2\pi\alpha\lambda} \tag{20}$$

Among them, $\lambda_{\min} = (1 - \sqrt{\alpha})^2\lambda_{\max} = (1 + \sqrt{\alpha})^2$ for the set up and down it $f_\Omega(\lambda)$, and $\alpha = \lim_{K,R\to 0} K/_R$. Similarly, $\hat{\Phi}$ for hacking nodes, assuming that perception matrix of the Wishart matrix, characteristic value of matrix satisfies the following distribution $f_{\hat{\Omega}}(\hat{\lambda})$, there is $\hat{\lambda}_{\min} = (1 - \sqrt{\hat{\alpha}})^2$, $\hat{\lambda}_{\max} = (1+\sqrt{\hat{\alpha}})^2 f_{\hat{\Omega}}(\hat{\lambda})$ for a set of upper and lower boundary truly, and $\hat{\alpha} = \lim_{K,E\to 0} K/_E$. According to the definition of the secrecy capacity [11], can be deduced in this paper, the model of the secrecy capacity type are as follows:

$$\begin{aligned} I(y(n), \hat{y}(n)) &= \frac{1}{2}log_2\{\frac{det[\sigma_0^2 I_R + \sigma^2\Phi\Phi^T]}{det[\sigma_0^2 I_E + \sigma^2\hat{\Phi}\hat{\Phi}^T]}\} \\ &= \frac{1}{2}log_2\{det[\sigma_0^2 I_R + \Phi R_{x_K(n)}\Phi^T]\} \\ &\quad - \frac{1}{2}log_2\{det[\sigma_0^2 I_E + \hat{\Phi} R_{x_K(n)}\hat{\Phi}^T]\} \\ &= \frac{1}{2}log_2\{\frac{det[\sigma_0^2 I_R + \sigma^2\Phi\Phi^T]}{det[\sigma_0^2 I_E + \sigma^2\hat{\Phi}\hat{\Phi}^T]}\} \end{aligned} \tag{21}$$

By using the distribution and the type of matrix eigenvalue perception (8) the supremum of secrecy capacity was derived:

$$\begin{aligned} I(y(n), \hat{y}(n)) &\le \frac{1}{2}log_2\{[\sigma_0^2 + \sigma^2\lambda_{\max}]R\} \\ &\quad - \frac{1}{2}log_2\{[\sigma_0^2 + \sigma^2\hat{\lambda}_{\min}]E\} \\ &= \frac{1}{2}log_2\frac{[\sigma_0^2 + \sigma^2(1+\sqrt{K/R})^2]R}{[\sigma_0^2 + \sigma^2(1-\sqrt{K/E})^2]E} \end{aligned} \tag{22}$$

Similarly, produces infimum secrecy capacity:

$$\begin{aligned} I(y(n), \hat{y}(n)) &\ge \frac{1}{2}log_2\{[\sigma_0^2 + \sigma^2\lambda_{\min}]R\} \\ &\quad - \frac{1}{2}log_2\{[\sigma_0^2 + \sigma^2\hat{\lambda}_{\max}]E\} \\ &= \frac{1}{2}log_2\frac{[\sigma_0^2 + \sigma^2(1-\sqrt{K/R})^2]R}{[\sigma_0^2 + \sigma^2(1+\sqrt{K/E})^2]E} \end{aligned} \tag{23}$$

By using the theorem, which can be quantified analysis of sensor network nodes affect communication security capacity. For example, by type (13), (14) can be seen that when the number of active sensor nodes K must increase the number of relay nodes can improve the secrecy capacity of wireless sensor network, the number of nodes at the same time increase tapped decreases the secrecy capacity of wireless sensor network, and vice versa. The theoretical derivation results place network on how to optimize the number of nodes, maximize has guiding significance for increasing the safety of the wireless sensor network communication.

IV. SIMULATION

Through two examples to illustrate the proposed amplifier and forwarded compression strategy in wireless sensor network communication ideas of secrecy capacity.

Assuming that perception nodes for $S = 200$, active node to perception set to $E = 10$, change the interval is set to the number of relay nodes $R = [60, 150]$; Then a fixed number

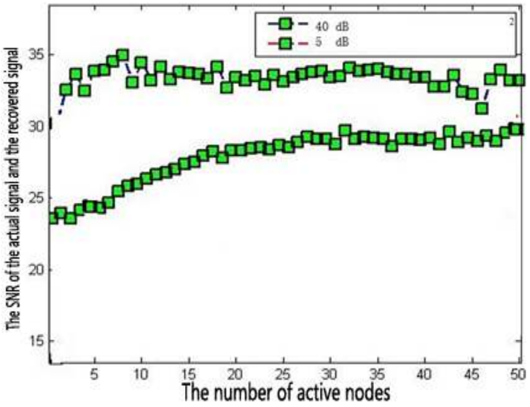

FIGURE 5. The SNR of the actual signal and the recovered signal.

of relay nodes $R = 60$, is active perception nodes $K = 10$, of hacking nodes change area $K = [10, 30]$, a relay node $R = [60, 150]$ for eavesdroppers number $E = [10, 110]$ for agv.MAC perception matrix are assumed to be gaussian distribution. Considering the noise existing situation, we [12] used SNR formula to measure the effect of the reconstructed signal:

$$\begin{aligned} SNR &= 10 \log_{10} \frac{\|x_K(n)\|}{\|e(n)\|} \\ &= 10 \log_{10} \frac{\left\|\hat{x}_K(n)\right\|}{\left\|\hat{e}(n)\right\|} = 10 \log_{10} \frac{\sigma^2}{\sigma_0^2} \end{aligned} \tag{24}$$

First, we present the noise $5dB, 40dB$, active sensor node number under the change of signal reconstruction signal-to-noise ratio effect. As shown in figure 5, you can see, the use of augmented Lagrangian algorithm proposed in this paper reconstructs the signal, in the case of 5 db can achieve an average of 25 db reconstruction precision, in addition, and in the case of 40 db even reached an average of 30 db signal reconstruction precision. In addition, you can be seen from the diagram, the accuracy of signal reconstruction with the change of number of active sensors, thus it can be seen that reconstruction algorithm is proposed in this paper is effective and robust. Next, we can be fixed with different parameter Settings, concrete analysis network parameter is set to the capacity of wireless network security. To do this, you can set the following parameters: fixed active perception between the number of nodes $K = 10$, to eavesdrop on nodes $E = [10, 110]$; finally fixed relay nodes $E = 10$ is the number of the nodes in hacking of active perception nodes $K = [10, 30]$ change interval. In addition, consider the range is: the noise [5 dB, 40 dB].

Using the results of the theorem 1, in view of parameters: the number of relay nodes, hacking node number, the number of active nodes, and the noise changes, in turn, to painting the secrecy capacity change with network node number of the diagram, the figure 6, figure 7, figure 8 and figure 9. Can be seen from the figure 6, when the number of active sensor nodes K must increase the number of relay nodes can improve the secrecy capacity of wireless sensor network, on the contrary, to reduce the number of relay nodes can reduce network traffic is secrecy capacity; Can be seen from

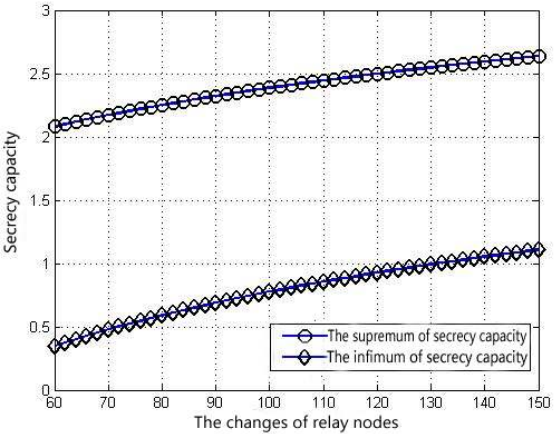

FIGURE 6. The noise 20*dB*, the relay sensor node number of the secrecy capacity of up and down on the change of the world.

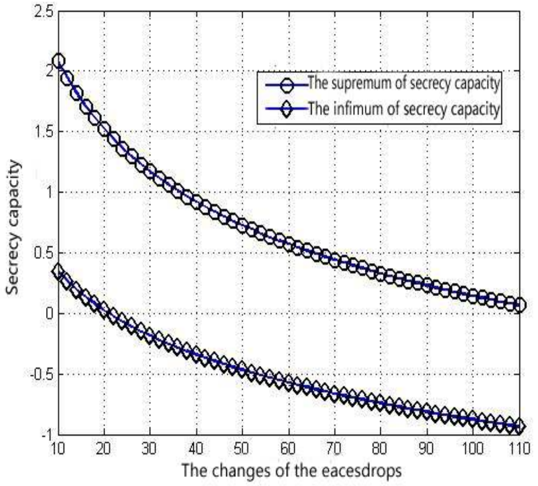

FIGURE 7. The noise 20*dB*, hacking sensor node number of the secrecy capacity of up and down on the change of the world.

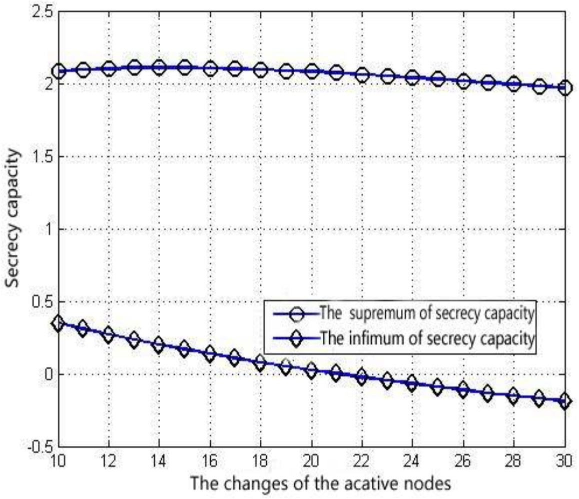

FIGURE 8. The noise 20*dB*, the number of active sensor nodes under the change of secrecy capacity is bound up and down.

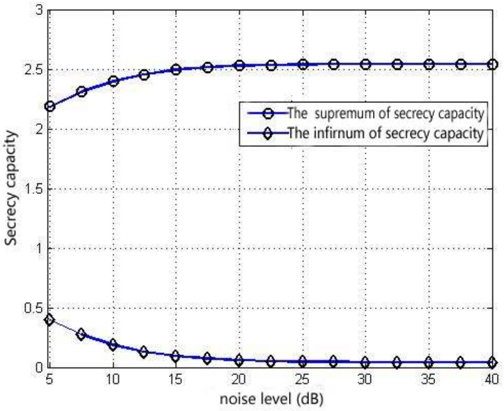

FIGURE 9. Under different noise levels and infimum on secrecy capacity.

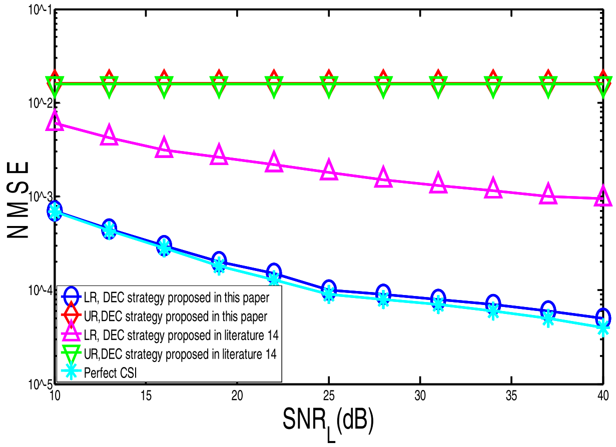

FIGURE 10. Different SNR levels of the channel NMSE $\gamma = 0.03$ based MIMO system.

the figure 7, increasing tapping the number of nodes to reduce the secrecy capacity of wireless sensor network, but the decline is not obvious, such as node number increased to 40 node needs to be tapped to secrecy capacity dropped to 1 unit. Figure 8 shows the active if the increase in the number of sensor nodes will slightly increase secrecy capacity of wireless sensor networks, due to the number of active nodes are random changes over time, according to the result of simulation shows that active node parameter's influence on secrecy capacity is not big, and confidential policy of robustness. Finally, figure 9 shows the secrecy capacity curve under different SNR, you can see when the signal-to-noise ratio reaches more than 15 db, the proposed wireless network compression perception strategy secrecy capacity will achieve the stable value, and in extreme cases 5 db, secrecy capacity can still achieve two units. The simulation results of the effective signal to verify the proposed algorithm and the effectiveness of the lower limit on secrecy capacity is derived.

Due to the importance of channel estimation in the perceptual phase, we increase the channel estimation training process and compare it with the literature [14]. It is assumed that both the legitimate user and the illegal user can use the training sequence signal for channel estimation, and the illegal user can also acquire the training sequence. Through comparison, after 100000 times of operation, the NMSE channel estimation is shown in Figure 10 which is respectively obtained for the threshold value of $\gamma = 0.03$. It can be seen from the figures that while ensuring the channel estimation of illegal receiver exceeds the preset error threshold, the bi-directional training estimation strategy can ensure that the channel estimation accuracy of legal receiver remains at 10^{-3} DB under different SNR. Moreover, with the decrease of noise interference intensity, the channel estimation accuracy of this kind of legal receiver increases linearly with SNR. As a result of comparison, it can be seen that the accuracy of the algorithm proposed in literature [14] is about 10^{-2} dB. Therefore, the algorithm proposed in this paper has better differentiation for channel estimation of legitimate receiver and illegal receiver, which make the WSN secure communication effect better.

V. CONCLUSION

This article considers the wireless sensor network security problems of amplification and forwarded compressed sensing strategy under the theory, from a new view we derived the wireless sensor network security capacity of amplification compression the transfer strategy. At the same time, considering the problem of difficult signal reconstruction phase signal recovery, under is given based on augmented Lagrange method of signal reconstruction algorithm. Finally, combining with the analysis of the simple example, it is concluded that the zoom forward compression transmission strategy important position in the wireless sensor network security. These research results can be further applied to smart grid, smart home network, Internet of vehicles and 5G network applications in the future, which will bring huge economic benefits.

REFERENCES

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

[2] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Sep. 2008, pp. 813–817.

[3] W. Bajwa, J. Haupt, A. Sayeed, and R. Nowak, "Compressive wireless sensing," in *Proc. 5th Int. Conf. Inf. Process. Sensor Netw.*, Apr. 2006, pp. 134–142.

[4] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Optimization of the amplify-and-forward in a wireless sensor network using compressed sensing," in *Proc. 19th Eur. Signal Process. Conf. (EUSIPCO)*, Barcelona, Spain, Aug. 2011, pp. 363–367.

[5] G.-P. Chen, "Distributed online algorithm of node selection in sensor network," *Comput. Eng.*, vol. 38, no. 10, pp. 101–104, 2012.

[6] S. Agrawal and S. Vishwanath, "Secrecy using compressive sensing," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 2011, pp. 563–567.

[7] E. J. Candes and T. Tao, "Decoding by Linear Programming," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

[8] R. Baraniuk, M. Davenport, R. DeVore, and M. Wakin, "A simple proof of the restricted isometry property for random matrices," *Constructive Approximation*, vol. 28, pp. 253–263, Jan. 2008.

[9] M. Debbah, H. El-Gamal, H. V. Poor, and S. Shamai (Shitz), "Wireless physical layer security," *EURASIP J. Wireless Commun. Netw.*, vol. 20, no. 9, pp. 1–2, 2009.

[10] G. N. Shirazi and L. Lampe, "A compressive sensing approach for secret key agreement based on UWB channel reciprocity," in *Proc. IEEE Int. Conf. Ultra-Wideband (ICUWB)*, Sep. 2012, vol. 17, no. 20, pp. 135–139.

[11] M. R. Hestenes, "Multiplier and gradient methods," in *Proc. 2nd Int. Conf. Comput. Methods Optim. Problems*, San Remo, Italy, 1968.

[12] D. P. Kumar, T. Amgoth, and C. S. R. Annavarapu, "Machine learning algorithms for wireless sensor networks: A survey," *Inf. Fusion*, vol. 49, no. 9, pp. 1–25, 2019.

[13] S. Alam and D. De, "Bio-inspired smog sensing model for wireless sensor networks based on intracellular signalling," *Inf. Fusion*, vol. 49, no. 9, pp. 100–119, 2019.

[14] Y. Chen, X. G. Xu, and Y. Wang, "Wireless sensor network energy efficient coverage method based on intelligent optimization algorithm," *Discrete Continuous Dyn. Syst.-S*, vol. 12, no. 4, pp. 887–900, 2019.

[15] W. Guo, J. Li, G. Chen, Y. Niu, and C. Chen, "A PSO-optimized real-time fault-tolerant task allocation algorithm in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 12, pp. 3236–3249, Dec. 2015.

[16] Z. Shen, P. P. C. Lee, J. Shu, and W. Guo, "Encoding-aware data placement for efficient degraded reads in XOR-coded storage systems: Algorithms and evaluation," *IEEE Trans. Parallel Distrib. Syst.*, vol. 29, no. 12, pp. 2757–2770, Dec. 2018.

[17] Y. Cheng, H. Jiang, F. Wang, Y. Hua, D. Feng, W. Guo, and Y. Wu, "Using high-bandwidth networks efficiently for fast graph computation," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 5, pp. 1170–1183, May 2019.

[18] X. Huang, W. Guo, G. Liu, and G. Chen, "FH-OAOS:A fast 4-step heuristic for obstacle-avoiding octilinear architecture router construction," *ACM Trans. Des. Automat. Electron. Syst.*, vol. 21, no. 3, Art. no. 48, 2016.

[19] B. Lin, W. Guo, N. Xiong, G. Chen, A. V. Vasilakos, and H. Zhang, "A pretreatment workflow scheduling approach for big data applications in multicloud environments," *IEEE Trans. Netw. Service Manage.*, vol. 13, no. 3, pp. 581–594, Sep. 2016.

[20] W. Zhu, W. Guo, Z. Yu, and H. Xiong, "Multitask allocation to heterogeneous participants in mobile crowd sensing," *Wireless Commun. Mobile Comput.*, vol. 2018, 2018, Art. no. 7218061.

[21] Y. Mo, L. Xing, Y.-K. Lin, and W. Guo, "Efficient analysis of repairable computing systems subject to scheduled checkpointing," *IEEE Trans. Depend. Sec. Comput.*, to be published, doi: 10.1109/TDSC.2018.2869393.

[22] Y. Yang, X. Liu, X. Zheng, C. Rong, and W. Guo, "Efficient traceable authorization search system for secure cloud storage," *IEEE Trans. Cloud Comput.*, to be published, doi: 10.1109/TCC.2018.2820714.

[23] X. Chen, A. Li, X. Zeng, W. Guo, and G. Huang, "Runtime model based approach to IoT application development," *Frontiers Comput. Sci.*, vol. 9, no. 4, pp. 540–553, 2015.

[24] W. Guo and G. Chen, "Human action recognition via multi-task learning base on spatial-temporal feature," *Inf. Sci.*, vol. 320, pp. 418–428, Nov. 2015.

[25] K. Guo, W. Guo, Y. Chen, Q. Qiu, and Q. Zhang, "Community discovery by propagating local and global information based on the MapReduce model," *Inf. Sci.*, vol. 323, pp. 73–93, Dec. 2015.

[26] G. Liu, X. Huang, W. Guo, Y. Niu, and G. Chen, "Multilayer obstacle-avoiding X-architecture Steiner minimal tree construction based on particle swarm optimization," *IEEE Trans. Cybern.*, vol. 45, no. 5, pp. 1003–1016, May 2015.

[27] F. Luo, W. Guo, Y. Yu, and G. Chen, "A multi-label classification algorithm based on kernel extreme learning machine," *Neurocomputing*, vol. 260, pp. 313–320, Oct. 2017.

[28] S. Wang and W. Guo, "Robust co-clustering via dual local learning and high-order matrix factorization," *Knowl.-Based Syst.*, vol. 138, pp. 176–187, Dec. 2017.

[29] G. Liu, W. Guo, Y. Niu, G. Chen, and X. Huang, "A PSO-based-timing-driven octilinear Steiner tree algorithm for VLSI routing considering bend reduction," *Soft Comput.*, vol. 19, no. 5, pp. 1153–1169, 2015.

[30] Y. Niu, J. Chen, and W. Guo, "Meta-metric for saliency detection evaluation metrics based on application preference," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 26351–26369, 2018.

[31] J. A. Jahanshahi, H. Danyali, and M. S. Helfroush, "A modified compressed sensing-based recovery algorithm for wireless sensor networks," *Radioengineering*, vol. 28, no. 3, pp. 610–617, 2019.

[32] C. Zhang, O. Li, and Y. P. Yang, "Energy-efficient data gathering algorithm relying on compressive sensing in lossy WSNs," *Measurement*, vol. 149, Jan. 2020, Art. no. 107099.

[33] V. K. Singh, S. Verma, and M. Kumar, "ODECS: An on-demand explosion-based compressed sensing using random walks in wireless sensor networks," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2466–2475, Sep. 2019.

[34] C. Li, G. Li, B. Kailkhura, and P. K. Varshney, "Secure distributed detection of sparse signals via falsification of local compressive measurements," *IEEE Trans. Signal Process.*, vol. 67, no. 18, pp. 4696–4706, Sep. 2019.

[35] L. Zhang, L. Huang, B. Li, and J. Yin, "Sensing matrix design for MMV compressive sensing: An MVDR approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8601–8612, Sep. 2019.

[36] C. Caione, D. Brunelli, and L. Benini, "Distributed compressive sampling for lifetime optimization in dense wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 8, no. 1, pp. 30–40, Feb. 2012.

[37] D. Xie, H. Peng, L. Li, and Y. Yang, "Semi-tensor compressed sensing," *Digit. Signal Process.*, vol. 58, pp. 85–92, Nov. 2016.

[38] N. Maheshwari and H. Dagale, "Secure communication and firewall architecture for IoT applications," in *Proc. 10th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bengaluru, India, Jan. 2018, pp. 328–335.

[39] J.-S. Pan, C.-Y. Lee, A. Sghaier, M. Zeghid, and J. Xie, "Novel systolization of subquadratic space complexity multipliers based on toeplitz matrix–vector product approach," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 7, pp. 1614–1622, Jul. 2019.

[40] T.-Y. Wu, C.-M. Chen, K.-H. Wang, C. Meng, and E. K. Wang, "A provably secure certificateless public key encryption with keyword search," *J. Chin. Inst. Eng.*, vol. 42, no. 1, pp. 20–28, 2019.

[41] C.-M. Chen, K.-H. Wang, K.-H. Yeh, B. Xiang, and T.-Y. Wu, "Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 8, pp. 3133–3142, Aug. 2019.

[42] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for Internet of vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019.

JIAN-LAN GUO is currently an Associate Professor with the Department of Computer Engineering, Dongguan Polytechnic College. Her current research interests include network security, mobile Internet, the IoT, and cryptography.

YU-QIANG CHEN received the Ph.D. degree from the Guangdong University of Technology. He is currently a Professor with the Department of Computer Engineering, Dongguan Polytechnic College. His current research interests include network security, mobile Internet, big data, the IoT, and cryptography.

HUAI-DE YANG is currently an Associate Professor with the Department of Computer Engineering, Dongguan Polytechnic College. His current research interests include network security, mobile Internet, the IoT, and cryptography.

CHIEN-MING CHEN received the Ph.D. degree from National Tsing Hua University, Taiwan. He is currently an Associate Professor with the College of Computer Science and Engineering, Shandong University of Science and Technology, China. His current research interests include network security, mobile Internet, the IoT, and cryptography. He serves as an Executive Editor of the *International Journal of Information Computer Security*. He also serves as an Associate Editor of IEEE ACCESS.

YEH-CHENG CHEN is currently pursuing the Ph.D. degree with the Department of Computer Science, University of California, Davis, CA, USA. His research interests are radio-frequency identification (RFID), data mining, social networks, information systems, wireless networks, artificial intelligence, the IoT, and security.

HUIYU ZHANG is currently pursuing the Bachelor of Engineering degree with the Department of Electronic Information Engineering, Liangjiang International College, Chongqing University of Technology. She is very interested in the IoT and artificial intelligence.

ZHIYU ZHANG is currently pursuing the bachelor's degree with the College of Mechanical and Electrical Engineering, Jilin Institute of Chemical Technology, Jilin, China. She is very interested in intelligent manufacturing and the IoT.