This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2919743, IEEE Internet of Things Journal

RAV: Relay Aided Vectorized Secure Transmission in Physical Layer Security for Internet of Things Under Active Attacks

Ning Zhang, *Senior Member, IEEE*, Renyong Wu, *Member, IEEE*,
Shenglan Yuan, Chao Yuan, and Dajiang Chen, *Member, IEEE*

***Abstract*—Internet of Things (IoT) security becomes of great importance, as IoT is the foundation for many emerging services. To safeguard IoT security, cryptosystems at upper layer relying on sophisticated key management alone can face many challenges due to the massive deployment of resource constrained machine-type communication devices. Physical layer (PHY) security can complement and enhance IoT security, by exploiting the characteristics of the bottom layer. In PHY security, channel state information (CSI) estimated through reverse pilot training is essential for the sender to select appropriate beamforming/precoder, which however is also vulnerable to adversaries. An adversary can actively launch pilot contamination attacks to affect the channel estimation and improve its signal reception quality. In this paper, we propose a relay-aided vectorized (RAV) secure transmission scheme, to safeguard the downlink communication in IoT networks under potential pilot contamination attacks. The proposed scheme does not distinguish the pilot sequences sent from an adversary and the receiver; and the sender utilizes what it receives to estimate the CSI for beamforming/precoder design. Then, a set of data symbols are pre-superposed using a random complex matrix to form signal vectors to send. Through cooperation with a relay, the signal vectors can be recovered by the intended receiver whereas the adversary or the relay cannot, as proved through security analysis. Simulation results also demonstrate that the bit error rate (BER) of the adversary is 0.5 regardless of its channel quality, indicating perfect secrecy is achieved.**

Keywords — Internet of Things, Physical layer security, Pilot contamination attack, active attack.

I. Introduction

Internet of Things (IoT) expects to connect massive physical devices and allow them to interact with each other to collect and analyze data for decision making [1]. By incorporating massive machine-type communication (MTC) devices, such as sensors, controllers, and actuators, IoT is envisaged as the enabling platform for many emerging applications such as intelligent transportation systems and smart city [2]. Along with the great benefits from IoT are the security concerns [3]–[6]. With IoT, adversaries can launch various attacks to the physical world in addition to the cyber domain. Therefore, it is crucial to protect the IoT security, which is yet very challenging due to the limited capacity of MTC devices in terms of computation and energy [7]. Conventionally, the security is protected using key-based cryptosystems at upper layers [8], [9]. However, the conventional approaches at upper layer alone can have some limitations as follows: i) it requires sophisticated key generation and management, which can complicate the system, especially considering the massive deployment of MTC devices. and ii) only computational security can be provided, where the system is at a risk of being broken as the computing capacity of adversaries increases.

As a promising solution, physical layer security can supplement and enhance IoT security to achieve unconditional security without keys [10]–[12]. It mainly exploits the inherent random characteristics of physical channels, rather than using pre-shared keys, to guarantee the data confidentiality against eavesdropping. It is found that information can be securely transmitted to the desired receiver while the eavesdropper learns nothing, if the eavesdropper's channel is degraded than the main channel [13]. Moreover, cooperative relaying and multi-antenna capacities can be leveraged to further enhance security [14], [15], where appropriate coding [16] or signal processing techniques are utilized, e.g., beamforming [17], [18], and artificial noise [19], [20]. However, in these schemes, full or partial knowledge of both channels is usually required for selecting the beamforming/precoder and the secrecy heavily relies on the accuracy of the CSI. Beamformer based on inaccurate CSI can easily leads to information leakage to eavesdroppers [21], [22]. Therefore, in addition to passive eavesdropping, an adversary can launch active attacks by sending signals to influence the normal operations [23].

The CSI is generally estimated based on the reverse pilot sequence according to the reciprocity principle. However, this also provides opportunities for an adversary to launch intelligent attacks since precise CSI is essential for the legitimate beamforming design. Adversaries can send the same pilot sequences in the reverse training phase to mimick the legitimate receiver, which is referred to as pilot contamination attack. By doing so, the transmit beamformer selected based on the incorrect estimated CSI can direct the main beam to the eavesdropper or other unwanted destinations, rather than the desired receiver. As a result, the eavesdropper can improve its own received signal quality or degrade the desired receiver's signal quality in the subsequent data transmission phase.

To deal with the pilot contamination attack, existing works propose to introduce a random pilot or a random orthogonal pilot sequence in channel estimation phase [24], [25].

N. Zhang is with Texas A&M University at Corpus Christi, USA. Email:ning.zhang@tamucc.edu.

R. Wu, S. Yuan, and C. Yuan are with Hunan University, China. Email:{wurenyong, yuan2011ysl,hnu025}@hnu.edu.cn.

D. Chen is with University of Electronic Science and Technology of China, China. Email: djchen@uestc.edu.cn.

2327-4662 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2919743, IEEE Internet of Things Journal

For instance, two sequences of newly-designed random PSK symbols are used to replace the normal pilot sequence so as to identify the pilot contamination attack through comparing the phase difference in the two sequences. However, firstly, modification is required to the structure of the normal pilot sequences and the channel estimation process. As is well known, the practical pilot sequences are not only designed for channel estimation but subject to other constraints like the orthogonality restriction. Secondly, a priori knowledge of pilot is required in practical systems for normal operation, whereas random pilot sequence based solutions may be infeasible. In addition, the existing schemes mainly focus on detection of pilot contamination attacks and seldom consider how to perform secure transmission under potential pilot contamination attacks.

In this work, we make an effort to safeguard the downlink communication in IoT networks under potential pilot contamination attacks by proposing a relay-aided vectorized (RAV) secure transmission scheme. The RAV secure transmission scheme does not distinguish whether the pilot sequence is sent from the legitimate receiver or an eavesdropper, and it can still help transmit data securely under potential pilot contamination attacks. Specifically, the received pilot sequence from an eavesdropper is equivalently processed as the legitimate one, i.e., without distinguishing active eavesdroppers from the legitimate receiver. The sender will utilize received pilot signals to estimate the CSI of the equivalent 'main' channel for the beamforming/precoder design. In the data transmission phase, instead of sending a symbol over each antenna at a time, a set of data symbols are pre-overlapped and superposed through a random complex matrix to form signal vectors to be sent at a time. According to the principle of maximum entropy, in order to correctly recover the symbol by Bob, each symbol vector with dimension L should be sent repeatedly at least L times. At each time of transmission, Alice uses a different random scrambling matrix. To eliminate the interference caused by the eavesdropper, the transmitter and a relay cooperatively transmit the signals to help the intended receiver to recover the initially transmitted information, while guaranteeing the eavesdroppers or the relay cannot decode the information. Security analysis is provided, which proves that the intended receiver can recover the information signals under potential pilot contamination attack, whereas neither the adversary nor the relay can. Simulation results also demonstrate that the BER of the adversary is 0.5, regardless of its channel quality, indicating perfect secrecy is achieved.

The remainder of this paper is organized as follows. Section II reviews the literature. Section III presents the system model and the signal processing process which is the foundation of the proposed strategy. In Section IV, we elaborate the proposed transmission scheme in details, followed by the security analysis in Section V. Simulation results are provided in Section VI. Finally, Section VII concludes this paper.

$Notation$: The term block represents either a symbol/signal block or its corresponding channel block in time domain, and a signal vector in mathematics represents a superposition signal in physics. Function $\mathrm{rank}(\cdot)$ represents matrix rank, and $[\,\cdot\,]^*$, $[\,\cdot\,]^T$ and $[\,\cdot\,]^H$ denote complex conjugation, transposition, and Hermitian transposition, respectively. $\mathbb{c}^{m\times n}$ denotes the complex space of a matrix with dimension $m \times n$. The distribution of a circularly symmetric complex Gaussian random variable with zero-mean and variance σ^2 is denoted by $\mathcal{CN}\left(0, \sigma^2\right)$ for convenience.

II. Related Works

Physical layer security can help safeguard the communication in IoT networks. Wyner shows that information can be transmitted at a positive secrecy rate while eavesdroppers learn nothing [13], by exploiting the characteristics of the bottom layer. In physical layer security, the adversary can not only perform passive eavesdropping but also active attacks. Based on the phases when the active attack occurs, the active attacks can been classified into two categories: correlated jamming [26], [27] and pilot contamination attack [28], [29]. For the former, the interference signals are generated by the adversary during the data transmission phase. For the latter, the adversary can affect the channel estimation by sending the same pilot sequences to mimic the legitimate receiver during the reverse training phase. As a result, the received pilot signals at the transmitter will be a sum of two synchronous pilot sequences. By doing so, the eavesdropper can improve its own received signal quality while degrading the desired receiver's signal quality since the transmit beamformer based on the incorrect estimated CSI incorrectly directs the main beam to the eavesdropper or other unwanted destinations, rather than the receiver.

In the literature, pilot contamination attack is first introduced in [28], which mainly focuses on the negative effects of this attack and there is a lack of feasible solutions. As a matter of fact, it is even very challenging to detect the pilot contamination attack. To address this issue, the random pilot idea is proposed in [24], whereby the pilot sequence is replaced by two random newly-generated sequences. By comparing the phase difference in the two sequences, the pilot contamination attack can be effectively detected. In [25], a random orthogonal pilot sequence is introduced in the system and sent occasionally by the receiver, and in most of time the normal pilot sequence is used. This scheme can work well without knowing the pattern for sending the random pilot, even though the random pilot sequence is public. However, the price is longer training time and higher implementation complexity. To simplify implementation, [30] proposes to superimpose the random sequence on the normal pilot sequence. As a result, a fraction of the transmission power is allocated to the random sequence, leading to poor estimation performance.

The aforementioned methods have the following limitations: i) it is required to modify the structure of the normal pilot sequences and the channel estimation process; and ii) random pilot sequence based solutions might be applicable because a priori knowledge of pilot is usually required in practical systems for normal operation. To deal with this issue, an energy ratio detector (RED) is proposed in [31] by exploiting the asymmetry property of the received signal power levels, where only the normal pilot sequence is applied. However, since both the uplink and downlink training phases are involved, it becomes more complicated and time-consuming. To further simplify the detection process, an improved method

2327-4662 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2919743, IEEE Internet of Things Journal

TABLE I
SUMMARY OF IMPORTANT NOTATIONS.

Symbol	Definition
M	The number of antennas
N	The block duration
L	The dimension of the symbol vector
$\mathbf{h}_{AB}$	The channel vector from Alice to Bob
$\mathbf{h}_{AE}$	The channel vector from Alice to Eve
$\mathbf{h}_{AR}$	The channel from Alice to Relay
$\mathbf{w}(n)$	The random weighting coefficient vector
$\mathbf{x}$	L-dimensional symbol vector
$\mathbf{W}^l$	The random matrix for l-th transmission
$\widehat{\mathbf{h}}$	The estimation of channel $\mathbf{h}$
$\mathbf{x}_p$	The pilot sequence
P_B	The transmission power of Bob
P_E	The transmission power of Eve
n_E	The Gaussian noise at Eve
σ^2	The variance of noise
λ	The coefficient for the linear equations
y_R	The received signal vectors at Relay
y_B	The received signal vectors at Bob

proposed in [32] adopts the minimum description length algorithm, where only the uplink training phase is involved in the detection. On the other hand, the existing schemes mainly focus on detection of pilot contamination attacks and seldom consider how to ensure secure transmission under pilot contamination attacks. Different from existing works, we propose a vectorized transmission scheme to safeguard information delivery under potential pilot contamination attack. Instead of detection alone, the proposed scheme can still help transmit data securely under pilot contamination attacks, without distinguishing whether the pilot sequence is sent from the legitimate receiver or an eavesdropper

III. SYSTEM MODEL

We mainly focus on the security of downlink communication (e.g., from controllers to actuators) in IoT networks, as shown in in Fig. The controller (Alice) with *M* antennas

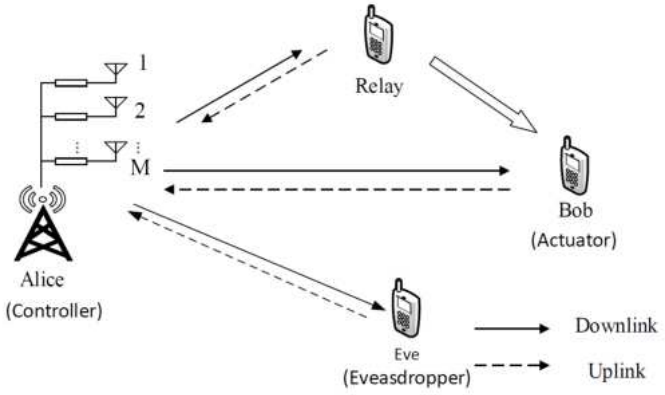


Fig. 1. Secure transmission in IoT networks.

intends to send confidential messages to the actuator (Bob) with single-antenna, while at the same time an eavesdropper (Eve) with single-antenna exists.

Suppose that all the channels are independent and identically distributed (i.i.d.) block Rayleigh fading channels. The CSI of each channel is unknown even to both Alice and Eve before channel estimation. Denote by N the block duration. Let $\mathbf{h}_{AB} = (h_{A_1B}, h_{A_2B}, \cdots, h_{A_MB})^T$ denote the channel from Alice to Bob. According to the reciprocity principle, we have $\mathbf{h}_{AB} = \mathbf{h}_{BA}^T$. Similarly, the channel from Alice to Eve is denoted by $\mathbf{h}_{AE} = (h_{A_1E}, h_{A_2E}, \cdots, h_{A_ME})^T$, and $\mathbf{h}_{AE} = \mathbf{h}_{EA}^T$. In this paper, all the symbols $\{x(n)\}$ to be transmitted are i.i.d. with zero-mean and unit variance. The key notations are given in Table 1.

A. Secure Transmission against Passive Eavesdropping

Physical layer security is to exploit the channel characteristics to protect information, while the channel advantage of Bob relative to Eve is not always satisfied in practice. In such scenarios, secure beamforming can be employed to deteriorate the received signals at Eve more seriously than that at Bob.

Denoting the random weighting coefficient vector by $\mathbf{w}(n) = (w_1(n), w_2(n), \cdots, w_M(n))^T$, the signal received by Bob in the n-th symbol interval can be expressed as

$$y_B(n) = \mathbf{h}_{AB}^H \mathbf{w}(n) x(n) + n_B(n), \tag{1}$$

where $n_B(n)$ is Gaussian noise at Bob with zero-mean and variance σ^2. Similarly, the signal $y_E(n) =$ received by Eve is given as belows;

$$y_E(n) = \mathbf{h}_{AE}^H \mathbf{w}(n) x(n) + n_E(n), \tag{2}$$

where $n_E(n)$ is Gaussian noise with zero-mean and variance σ^2 at Eve. According to [33], the random scrambling vector $\mathbf{w}(n)$ should be designed to satisfy the constraint

$$\mathbf{h}_{AB}^H \mathbf{w}(n) = ||\mathbf{h}_{AB}||, \tag{3}$$

where $||\mathbf{h}_{AB}|| = \sqrt{\sum_{i=1}^{M} |h_{A_iB}|^2}$ is the 2-norm of $\mathbf{h}_{AB}$. Thus, $||\mathbf{w}(n)|| = 1$ and Eq. (1) can be re-expressed as

$$y_B(n) = ||\mathbf{h}_{AB}|| x(n) + n_B(n). \tag{4}$$

It can be seen that, the detection capability of Bob is not deteriorated by the generated random noise while Eve will receive a series of randomly and rapidly varying signals.

B. Secure Transmission against Active Pilot Contamination Attack

Alice needs to estimate the CSI of the main channel (i.e., the channel from Alice to Bob) based on the received pilot sequence sent by Bob in reverse link, in order to design the transmission strategy (i.e., beamforming weights). However, in this reverse training phase, Eve may also send the identical pilot sequence to Alice, to pretend to be the legitimate receiver. This behavior is referred to as pilot contamination attack, which is feasible and can be easily performed in reality, given the structure of the reverse training sequence has been publicly known to all terminals. Then, the CSI estimated by Alice is a weighted sum of Bob-to-Alice and Eve-to-Alice CSIs.

Define the following two hypotheses: H_0 representing that there is no pilot contamination attack, and H_1 indicating that Alice is under pilot contamination attack. Only under H_1, Eve broadcasts the identical pilot sequence during the reverse

2327-4662 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2919743, IEEE Internet of Things Journal

training phase. Then, the received pilot signals at Alice can be expressed as

$$\begin{cases} H_0: & \mathbf{Y}_A = \sqrt{P_B}\mathbf{h}_{BA}\mathbf{x}_p + \mathbf{N}_A \\ H_1: & \mathbf{Y}_A = \sqrt{P_B}\mathbf{h}_{BA}\mathbf{x}_p + \sqrt{P_E}\mathbf{h}_{EA}\mathbf{x}_p + \mathbf{N}_A, \end{cases} \tag{5}$$

where $\mathbf{x}_p$ refers to the pilot sequence with length $\tau = \mathbf{x}_p\mathbf{x}_p^H$, $\mathbf{N}_A$ is the matrix of noise at Alice where all elements follow iid Gaussian distribution with zero-mean and variance σ^2, P_B and P_E denote the transmission power of Bob and Eve, respectively.

Given the Linear Minimum Mean Square Error (LMMSE) estimation factor [34] $\mathbf{e} = \frac{\mathbf{x}_p^H}{\sqrt{P_B}\sigma^2}\left(\frac{1}{P_B} + \frac{\mathbf{x}_p\mathbf{x}_p^H}{\sigma^2}\right)^{-1}$, the estimate of the main channel is

$$\begin{cases} H_0: & \widehat{\mathbf{h}}_{BA} = (\sqrt{P_B}\mathbf{h}_{BA}\mathbf{x}_p + \mathbf{N}_A)\mathbf{e} \\ H_1: & \widehat{\mathbf{h}}_{BA} = (\sqrt{P_B}\mathbf{h}_{BA}\mathbf{x}_p + \sqrt{P_E}\mathbf{h}_{EA}\mathbf{x}_p + \mathbf{N}_A)\mathbf{e}. \end{cases} \tag{6}$$

Obviously, under pilot contamination attack, Alice may obtain an erroneous estimate of the uplink channel. Without loss of generality, given an unbiased estimate, the above equations can be further simplified as

$$\begin{cases} H_0: & \widehat{\mathbf{h}}_{BA} = \mathbf{h}_{BA} + \varepsilon_u \\ H_1: & \widehat{\mathbf{h}}_{BA} = (\mathbf{h}_{BA} + \varepsilon_u) + \widehat{\mathbf{h}}_{EA}, \end{cases} \tag{7}$$

where the subscript u refers to the uplink channel and ε_u is a Gaussian estimate error vector with zero mean and covariance matrix $\sigma_u^2\mathbf{I}_M$, $\widehat{\mathbf{h}}_{EA} = \sqrt{P_E}\mathbf{h}_{EA}\mathbf{x}_p\mathbf{e}$. From the matrix inversion lemma [35], we have

$$\sigma_u^2 = \frac{\sigma^2}{\sigma^2 + P_B\mathbf{x}_p\mathbf{x}_p^H}. \tag{8}$$

Similarly, the downlink training sequence is sent to Bob, so the channel estimate can be expressed as

$$\widehat{\mathbf{h}}_{AB} = \mathbf{h}_{AB} + \varepsilon_d, \tag{9}$$

where the subscript d refers to the downlink channel, ε_d is a Gaussian estimate error vector with zero-mean and covariance matrix $\sigma_d^2\mathbf{I}_M$. Similarly, $\sigma_d^2 = \frac{\sigma^2}{\sigma^2 + P_A\mathbf{x}_p\mathbf{x}_p^H}$.

IV. Relay Aided Vectorized Secure Transmission

This work aims at achieving secure transmission under pilot contamination attacks. To this end, in this section, a novel relay aided vectorized secure transmssion scheme is proposed to combat pilot contamination attacks. In this scheme, Alice is not required to make a mandatory distinction between Bob and Eve, or even know any priori knowledge of the main channel or wiretap channel. Together with the legitimate pilot sequence, the received pilot sequence from Eve is applied to estimate the CSI of the equivalent 'main' channel (not the real physical main channel) if active attack is launched, to design the transmission precoder. As a result, Bob and Eve are completely symmetric from the perspective of Alice. To enable Bob can still recover the information signals under potential pilot contamination attacks, Alice will cooperate with a single-antenna operator-deployed relay for secure transmission.

Let $\mathbf{h}_{AR} = (h_{A_1R}, h_{A_2R}, \cdots, h_{A_MR})^T$ be the channel from Alice to Relay. Its unbiased estimate $\widehat{\mathbf{h}}_{AR}$ is considered to be known by Alice and Relay before secure transmission. It is reasonable to assume that Relay 'pushes' the estimate $\widehat{\mathbf{h}}_{AR}$ and all his received data signals to Bob in some way while Bob does not send any signal to him. Eve only attempts to misguide Alice to deduce error channel estimates, while Eve can still overhear Relay and Bob. In what follows, we will elaborate the vectorized secure transmission scheme with a cooperative relay in details.

A. Reverse Training Phase

In the reverse training phase, Alice might receive pilot sequences from both Bob and Eve, under potential pilot contamination attack. The received signal can be a transposition of two received sequences, as follows:

$$\mathbf{Y}_{AB} = \sqrt{P_B}\mathbf{h}_{AB}^T\mathbf{x}_p + \mathbf{N}_A, \tag{10}$$

$$\mathbf{Y}_{AE} = \sqrt{P_E}\mathbf{h}_{AE}^T\mathbf{x}_p + \mathbf{N}_A. \tag{11}$$

Obviously, without prior knowledge of the main channel, Alice cannot distinguish the sequence sent from Bob or Eve. Instead, Alice can estimate the respective channels as follows:

$$\widehat{\mathbf{h}}_{AB}^T = \frac{\mathbf{Y}_{AB}\mathbf{x}_p^H}{\sqrt{P_B}\sigma^2}\left(\frac{1}{P_B} + \frac{\mathbf{x}_p\mathbf{x}_p^H}{\sigma^2}\right)^{-1}, \tag{12}$$

$$\widehat{\mathbf{h}}_{AE}^T = \frac{\mathbf{Y}_{AE}\mathbf{x}_p^H}{\sqrt{P_E}\sigma^2}\left(\frac{1}{P_E} + \frac{\mathbf{x}_p\mathbf{x}_p^H}{\sigma^2}\right)^{-1}. \tag{13}$$

For convenience, we can denote the combined CSI of the 'equivalent' main channel by

$$\widetilde{\mathbf{h}}_{AB} = \widehat{\mathbf{h}}_{AB} + \widehat{\mathbf{h}}_{AE}, \tag{14}$$

where $\widetilde{\mathbf{h}}_{AB} = (\widetilde{h}_{A_1B}, \widetilde{h}_{A_2B}, \cdots, \widetilde{h}_{A_MB})^T$.

B. Data Transmission Phase

1) At the transmitter: Alice arranges every L symbols to send into a L-dimensional symbol vector as follows:

$$\mathbf{x} = (x(1), x(2), \cdots, x(L))^T. \tag{15}$$

In order to correctly recover the symbol by Bob, each L-dimensional symbol vector should be sent repeatedly at least L times[1]. At each time of transmission, Alice performs random scrambling on the symbol vector. For the l-th transmission, the random scrambling process is shown in Fig. 2. With the random matrix $\mathbf{W}^l$, these L symbols will be superposed at each individual antenna. For different transmissions, a different random scrambling matrix will be utilized. Without loss of generality, given N is a multiple of L, all the L times of

[1]This is based on the principle of maximum entropy.

2327-4662 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2919743, IEEE Internet of Things Journal

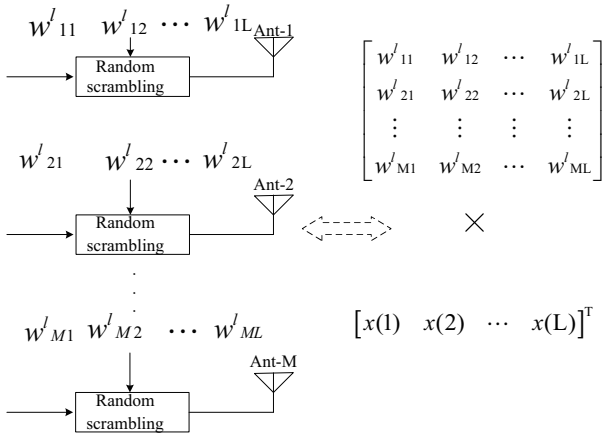


Fig. 2. The random scrambling process

transmission can be fulfilled in the same block. For the l-th transmission, the l-th random matrix is given as follows:

$$\mathbf{W}^l = \begin{bmatrix} w_{11}^l & w_{12}^l & \cdots & w_{1L}^l \\ w_{21}^l & w_{22}^l & \cdots & w_{2L}^l \\ \vdots & \vdots & \ddots & \vdots \\ w_{M1}^l & w_{M2}^l & \cdots & w_{ML}^l \end{bmatrix}. \quad (16)$$

Note that the random scrambling matrix $\mathbf{W}^l$ is generated based on $\widetilde{\mathbf{h}}_{AB}$ and $\widehat{\mathbf{h}}_{AR}$. To ensure the received signals can be detected correctly by Bob, the random matrix is generated such that the following linear constraints are satisfied:

$$\begin{cases} \widetilde{\mathbf{h}}_{AB}^H \mathbf{W}^1 & = (\lambda_{11}||\widehat{\mathbf{h}}_{AR}||, \lambda_{12}||\widehat{\mathbf{h}}_{AR}||, \cdots, \lambda_{1L}||\widehat{\mathbf{h}}_{AR}||) \\ \widetilde{\mathbf{h}}_{AB}^H \mathbf{W}^2 & = (\lambda_{21}||\widehat{\mathbf{h}}_{AR}||, \lambda_{22}||\widehat{\mathbf{h}}_{AR}||, \cdots, \lambda_{2L}||\widehat{\mathbf{h}}_{AR}||) \\ & \vdots \\ \widetilde{\mathbf{h}}_{AB}^H \mathbf{W}^L & = (\lambda_{L1}||\widehat{\mathbf{h}}_{AR}||, \lambda_{L2}||\widehat{\mathbf{h}}_{AR}||, \cdots, \lambda_{LL}||\widehat{\mathbf{h}}_{AR}||), \end{cases} \quad (17)$$

where $||\widehat{\mathbf{h}}_{AR}|| = \sqrt{\sum_{i=1}^{M} |\widehat{h}_{A_i R}|^2}$, the L coefficients $\lambda_{11}, \lambda_{12}, \cdots, \lambda_{LL}$ are only introduced to ensure that $\lambda_{11}||\widehat{\mathbf{h}}_{AR}||, \lambda_{12}||\widehat{\mathbf{h}}_{AR}||, \cdots, \lambda_{LL}||\widehat{\mathbf{h}}_{AR}||$ are sufficiently different from each other. The corresponding generation algorithm of $\mathbf{W}^l$ is given in Algorithm 1. As a result, the generated signal vectors are linearly independent of each other.

From Eq. (17), we have

$$\widetilde{\mathbf{h}}_{AB}^H \mathbf{W} = (\beta_1||\widehat{\mathbf{h}}_{AR}||, \beta_2||\widehat{\mathbf{h}}_{AR}||, \cdots, \beta_L||\widehat{\mathbf{h}}_{AR}||), \quad (18)$$

where $\mathbf{W} = \Sigma_{l=1}^{L} \mathbf{W}^l$, $\beta_l = \Sigma_{l'=1}^{L} \lambda_{l'l}$, $l = 1, 2, \cdots, L$.

2) At the receiver: The signal vector received by Bob in the l-th transmission, i.e., $y_B(l) =$ can be given by

$$y_B(l) = \mathbf{h}_{AB}^H \mathbf{W}^l \mathbf{x} + n_B(l), \quad (19)$$

where $n_B(l)$ is Gaussian noise at Bob with zero-mean and variance σ^2. Summing up all the L received signal vectors,

Algorithm 1 Algorithm for generating the random matrices.

Require:
Dimension of signal vector, L;
Number of transmitting antennas, M;
Ensure:
Scrambling matrices, from $\mathbf{W}^1$ to $\mathbf{W}^L$;
1: **for** each $l \in [1, L]$ **do**
2: **for** each $l' \in [1, L]$ **do**
3: **for** each $m \in [1, M-1]$ **do**
4: Randomly generate each element $w_{ml'}^l$;
5: **end for**
6: $w_{Ml'}^l = \frac{\lambda_{ll'}||\widehat{h}_{AR}|| - \Sigma_{i=1}^{M-1} \widetilde{h}_{A_i B} w_{il'}^l}{\widetilde{h}_{A_M B}}$;
7: **end for**
8: **end for**

corresponding to the same symbol vector, yields

$$\begin{aligned} y_B &= (\mathbf{h}_{AB}^H \mathbf{W}^1 + \mathbf{h}_{AB}^H \mathbf{W}^2 + \cdots + \mathbf{h}_{AB}^H \mathbf{W}^L)\mathbf{x} + n_B \quad (20) \\ &= \mathbf{h}_{AB}^H (\mathbf{W}^1 + \mathbf{W}^2 + \cdots + \mathbf{W}^L)\mathbf{x} + n_B \\ &= \mathbf{h}_{AB}^H \mathbf{W}\mathbf{x} + n_B, \end{aligned}$$

where $\mathbf{W} = \Sigma_{l=1}^{L} \mathbf{W}^l$, $n_B = \Sigma_{l=1}^{L} n_B(l)$.

The received signal vector by the relay in the l-th transmission, $y_R(l)$ is

$$y_R(l) = \mathbf{h}_{AR}^H \mathbf{W}^l \mathbf{x} + n_R(l). \quad (21)$$

Similarly, by accumulating all the L received signal vectors, we have

$$\begin{aligned} y_R &= (\mathbf{h}_{AR}^H \mathbf{W}^1 + \mathbf{h}_{AR}^H \mathbf{W}^2 + \cdots + \mathbf{h}_{AR}^H \mathbf{W}^L)\mathbf{x} + n_R \quad (22) \\ &= \mathbf{h}_{AR}^H (\mathbf{W}^1 + \mathbf{W}^2 + \cdots + \mathbf{W}^L)\mathbf{x} + n_R \\ &= \mathbf{h}_{AR}^H \mathbf{W}\mathbf{x} + n_R, \end{aligned}$$

where $n_R = \Sigma_{l=1}^{L} n_R(l)$.

Since Alice does not distinguish Bob and Eve in reverse training phase, Bob needs to fuse the received signal vector y_R with y_B to decode the transmitted signal vectors correctly. Considering all the channels are estimated accurately for simplicity, the following holds:

$$\begin{cases} y_B & = \widehat{\mathbf{h}}_{AB}^H \mathbf{W}\mathbf{x} + n_B \\ y_R & = \widehat{\mathbf{h}}_{AR}^H \mathbf{W}\mathbf{x} + n_R \\ (\widehat{\mathbf{h}}_{AB}^H + \widehat{\mathbf{h}}_{AE}^H)\mathbf{W} & = (\beta_1||\widehat{\mathbf{h}}_{AR}||, \beta_2||\widehat{\mathbf{h}}_{AR}||, \cdots, \beta_L||\widehat{\mathbf{h}}_{AR}||). \end{cases} \quad (23)$$

To simplify the derivation process, we first solve $\mathbf{W}\mathbf{x}$ as an intermediate solution, instead of $\mathbf{x}$. Given $\widehat{\mathbf{h}}_{AR}^H$ is a full row-rank matrix, $\widehat{\mathbf{h}}_{AR}^H \widehat{\mathbf{h}}_{AR}$ is reversible. According to matrix theory [36], $\mathbf{W}\mathbf{x} = (\widehat{\mathbf{h}}_{AR}^H)^{-1}(y_R - n_R)$ if and only if $\widehat{\mathbf{h}}_{AR}^H (\widehat{\mathbf{h}}_{AR}^H)^{-1} \widehat{\mathbf{h}}_{AR}^H = \widehat{\mathbf{h}}_{AR}^H$.

In addition, the right pseudo-inverse matrix of $\widehat{\mathbf{h}}_{AR}^H$ can be given by

$$\left(\widehat{\mathbf{h}}_{AR}^H\right)^{\dagger} = \widehat{\mathbf{h}}_{AR} \left(\widehat{\mathbf{h}}_{AR}^H \widehat{\mathbf{h}}_{AR}\right)^{-1}, \quad (24)$$

It also follows that $\widehat{\mathbf{h}}_{AR}^H \left(\widehat{\mathbf{h}}_{AR}^H\right)^{\dagger} \widehat{\mathbf{h}}_{AR}^H = \widehat{\mathbf{h}}_{AR}^H$, and thus the

2327-4662 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2919743, IEEE Internet of Things Journal

intermediate solution can be given as

$$\mathbf{W}\mathbf{x} = \left(\widehat{\mathbf{h}}_{AR}^H\right)^\dagger (y_R - n_R). \tag{25}$$

Denoting $\varphi_{AR} = (\beta_1||\widehat{\mathbf{h}}_{AR}||, \beta_2||\widehat{\mathbf{h}}_{AR}||, \cdots, \beta_L||\widehat{\mathbf{h}}_{AR}||)$ for convenience, we have

$$\begin{aligned}\varphi_{AR}\mathbf{x} &= \left(\widehat{\mathbf{h}}_{AB}^H + \widehat{\mathbf{h}}_{AE}^H\right)\mathbf{W}\mathbf{x} \\ &= \widehat{\mathbf{h}}_{AB}^H\mathbf{W}\mathbf{x} + \widehat{\mathbf{h}}_{AE}^H\mathbf{W}\mathbf{x} \\ &= y_B - n_B + \widehat{\mathbf{h}}_{AE}^H\mathbf{W}\mathbf{x}.\end{aligned} \tag{26}$$

Thus, the first equation of (23) can be re-written as

$$y_B = \varphi_{AR}\mathbf{x} - \widehat{\mathbf{h}}_{AE}^H\left(\widehat{\mathbf{h}}_{AR}^H\right)^\dagger (y_R - n_R) + n_B. \tag{27}$$

In what follows, we will discuss how to recover the information symbols for the two cases with and without active attacks.

3) Under active attacks: Denoting $\phi_{AR}^l = (\lambda_{l1}||\widehat{\mathbf{h}}_{AR}||, \lambda_{l2}||\widehat{\mathbf{h}}_{AR}||, \cdots, \lambda_{lL}||\widehat{\mathbf{h}}_{AR}||)$ and $\eta = \widehat{\mathbf{h}}_{AE}^H(\widehat{\mathbf{h}}_{AR}^H)^\dagger$ for convenience, there are totally $L+1$ equations related to the transmitted signal vector as below:

$$\begin{cases} y_B(1) &= \phi_{AR}^1\mathbf{x} - \eta y_R(1) + \eta n_R(1) + n_B(1) \\ y_B(2) &= \phi_{AR}^2\mathbf{x} - \eta y_R(2) + \eta n_R(2) + n_B(2) \\ &\vdots \\ y_B(L) &= \phi_{AR}^L\mathbf{x} - \eta y_R(L) + \eta n_R(L) + n_B(L) \\ y_B &= \varphi_{AR}\mathbf{x} - \eta y_R + \eta n_R + n_B, \end{cases} \tag{28}$$

which can be re-written as Eq. (29).

Obviously, the equation has the form

$$\widetilde{\mathbf{y}} = \widetilde{\mathbf{\Lambda}}\widetilde{\mathbf{x}} + \widetilde{\mathbf{n}}, \tag{30}$$

where $\widetilde{\mathbf{y}} = (y_B(1), y_B(2), \cdots, y_B(L), y_B)^T$, $\widetilde{\mathbf{n}} = (\eta n_R(1) + n_B(1), \eta n_R(2) + n_B(2), \cdots, \eta n_R(L) + n_B(L), \eta n_R + n_B)^T$, $\widetilde{\mathbf{x}} = (x(1), x(2), \cdots, x(L), -\eta)^T$ and

$$\widetilde{\mathbf{\Lambda}} = \begin{bmatrix} \lambda_{11}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{12}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{1L}||\widehat{\mathbf{h}}_{AR}|| & y_R(1) \\ \lambda_{21}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{22}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{2L}||\widehat{\mathbf{h}}_{AR}|| & y_R(2) \\ \vdots & \vdots & \cdots & \vdots & \\ \lambda_{L1}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{L2}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{LL}||\widehat{\mathbf{h}}_{AR}|| & y_R(L) \\ \beta_1||\widehat{\mathbf{h}}_{AR}|| & \beta_2||\widehat{\mathbf{h}}_{AR}|| & \cdots & \beta_L||\widehat{\mathbf{h}}_{AR}|| & y_R \end{bmatrix}. \tag{31}$$

From Eq. (17), we have $rank(\widetilde{\mathbf{\Lambda}}) = L$, and thus $\widetilde{\mathbf{\Lambda}}$ is a singular matrix. By applying Tikhonov regularization method in [37], we can derive the solution. Because of the additive noise component, the regularized least squares cost function can be constructed as

$$\boldsymbol{J}(\widetilde{\mathbf{x}}) = \frac{1}{2}(||\widetilde{\mathbf{\Lambda}}\widetilde{\mathbf{x}} - \widetilde{\mathbf{y}}||^2 - \lambda||\widetilde{\mathbf{x}}||^2), \tag{32}$$

where $\lambda \geq 0$ is the regularization parameter. Then,

$$\frac{\partial \boldsymbol{J}(\widetilde{\mathbf{x}})}{\partial \widetilde{\mathbf{x}}^H} = \widetilde{\mathbf{\Lambda}}^H\widetilde{\mathbf{\Lambda}}\widetilde{\mathbf{x}} - \widetilde{\Lambda}^H\widetilde{\mathbf{y}} - \lambda\widetilde{\mathbf{x}}. \tag{33}$$

With the regularization, we can have a numerical solution. Thus, an explicit solution, $\widehat{\mathbf{x}} = (\widehat{x}(1), \widehat{x}(2), \cdots, \widehat{x}(L), -\widehat{\eta})^T$, can be derived:

$$\widehat{\mathbf{x}} = (\widetilde{\mathbf{\Lambda}}^H\widetilde{\mathbf{\Lambda}} - \lambda\mathbf{I})^{-1}\widetilde{\mathbf{\Lambda}}^H\widetilde{\mathbf{y}}. \tag{34}$$

Given the singular value decomposition $\widetilde{\mathbf{\Lambda}} = \boldsymbol{U}\Sigma\boldsymbol{V}^H$, the solution is re-expressed as

$$\begin{aligned}\widehat{\mathbf{x}} &= (\widetilde{\mathbf{\Lambda}}^H\widetilde{\mathbf{\Lambda}} + \delta_{min}^2\mathbf{I})^{-1}\widetilde{\mathbf{\Lambda}}^H\widetilde{\mathbf{y}} \\ &= \boldsymbol{V}(\Sigma^2 + \delta_{min}^2\mathbf{I})^{-1}\Sigma\boldsymbol{U}^H\widetilde{\mathbf{y}},\end{aligned} \tag{35}$$

where δ_{min} denotes the lowest nonzero singular value of $\widetilde{\mathbf{\Lambda}}$.

Denote a signal vector with the same dimension as $\mathbf{x} = (x(1), x(2), \cdots, x(L))^T$, which is a L-dimension vector. Each component $x(l), l = 1, 2, \cdots, L$, has its own constellation diagram $\mathbf{S}(l)$. Bob can detect the received signal vectors as

$$\widehat{\mathbf{x}}_{ML} \cong arg \min_{x(l)\in\mathbf{S}(l)} ||\widehat{\mathbf{x}}_{Tik} - \mathbf{x}||^2, \tag{36}$$

where $\widehat{\mathbf{x}}_{Tik} = (\widehat{x}(1), \widehat{x}(2), \cdots, \widehat{x}(L))^T$.

4) Under passive eavesdropping: If Eve is only a passive eavesdropper, i.e., $\mathbf{Y}_{AE} = \mathbf{0}$ and $\widehat{\mathbf{h}}_{AE}^H = \mathbf{0}$, then the received signal vectors become

$$\begin{cases} y_B(1) = \mathbf{h}_{AB}^H\mathbf{W}^1\mathbf{x} + n_B(1) \\ y_B(2) = \mathbf{h}_{AB}^H\mathbf{W}^2\mathbf{x} + n_B(2) \\ \vdots \\ y_B(L) = \mathbf{h}_{AB}^H\mathbf{W}^L\mathbf{x} + n_B(L), \end{cases} \tag{37}$$

which can be re-written as Eq. (38).

Similarly, the equation has the form of

$$\overline{\mathbf{y}} = \overline{\mathbf{\Lambda}}\overline{\mathbf{x}} + \overline{\mathbf{n}}, \tag{39}$$

where $\overline{\mathbf{y}} = [y_B(1), y_B(2), \cdots, y_B(L)]^T$, $\overline{\mathbf{x}} = [x(1), x(2), \cdots, x(L)]^T$, $\overline{\mathbf{n}} = [n_B(1), n_B(2), \cdots, n_B(L)]^T$ is a Gaussian noise vector with zero-mean and variance $\sigma^2\mathbf{I}$, and

$$\overline{\mathbf{\Lambda}} = \begin{bmatrix} \lambda_{11}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{12}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{1L}||\widehat{\mathbf{h}}_{AR}|| \\ \lambda_{21}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{22}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{2L}||\widehat{\mathbf{h}}_{AR}|| \\ \vdots & \vdots & \cdots & \vdots \\ \lambda_{L1}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{L2}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{LL}||\widehat{\mathbf{h}}_{AR}|| \end{bmatrix}. \tag{40}$$

Note that the matrix $\overline{\mathbf{\Lambda}}$ is a nonsingular square matrix since all the L row vectors $\phi_{AR}^l, l = 1, 2, \cdots, L$, are linearly independent with each other.

The core idea of the ordinary least square (OLS) method [38] is that the solution vector can minimize the sum of squared errors on both sides of the matrix equation, so the optimization problem is

$$\widehat{\mathbf{x}}_{OLS} = arg \min_{\mathbf{x}} ||\overline{\mathbf{\Lambda}}\mathbf{x} - \overline{\mathbf{y}}||^2. \tag{41}$$

Denoting $\mathbf{\Gamma} = (\overline{\mathbf{\Lambda}}\mathbf{x} - \overline{\mathbf{y}})^H(\overline{\mathbf{\Lambda}}\mathbf{x} - \overline{\mathbf{y}})$ for convenience, we can

2327-4662 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2919743, IEEE Internet of Things Journal

$$\begin{bmatrix} y_B(1) \\ y_B(2) \\ \vdots \\ y_B(L) \\ y_B \end{bmatrix} = \begin{bmatrix} \lambda_{11}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{12}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{1L}||\widehat{\mathbf{h}}_{AR}|| & y_R(1) \\ \lambda_{21}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{22}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{2L}||\widehat{\mathbf{h}}_{AR}|| & y_R(2) \\ \vdots & \vdots & \cdots & \vdots & \\ \lambda_{L1}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{L2}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{LL}||\widehat{\mathbf{h}}_{AR}|| & y_R(L) \\ \beta_1||\widehat{\mathbf{h}}_{AR}|| & \beta_2||\widehat{\mathbf{h}}_{AR}|| & \cdots & \beta_L||\widehat{\mathbf{h}}_{AR}|| & y_R \end{bmatrix} \begin{bmatrix} x(1) \\ x(2) \\ \vdots \\ x(L) \\ -\eta \end{bmatrix} + \begin{bmatrix} \eta n_R(1) + n_B(1) \\ \eta n_R(2) + n_B(2) \\ \vdots \\ \eta n_R(L) + n_B(L) \\ \eta n_R + n_B \end{bmatrix}. \quad (29)$$

$$\begin{bmatrix} y_B(1) \\ y_B(2) \\ \vdots \\ y_B(L) \end{bmatrix} = \begin{bmatrix} \lambda_{11}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{12}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{1L}||\widehat{\mathbf{h}}_{AR}|| \\ \lambda_{21}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{22}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{2L}||\widehat{\mathbf{h}}_{AR}|| \\ \vdots & \vdots & \cdots & \vdots \\ \lambda_{L1}||\widehat{\mathbf{h}}_{AR}|| & \lambda_{L2}||\widehat{\mathbf{h}}_{AR}|| & \cdots & \lambda_{LL}||\widehat{\mathbf{h}}_{AR}|| \end{bmatrix} \begin{bmatrix} x(1) \\ x(2) \\ \vdots \\ x(L) \end{bmatrix} + \begin{bmatrix} n_B(1) \\ n_B(2) \\ \vdots \\ n_B(L) \end{bmatrix}. \quad (38)$$

write the expansion of $\mathbf{\Gamma}$ as

$$\mathbf{\Gamma} = \mathbf{x}^H \overline{\mathbf{\Lambda}}^H \overline{\mathbf{\Lambda}} \mathbf{x} - \mathbf{x}^H \overline{\mathbf{\Lambda}}^H \overline{\mathbf{y}} - \overline{\mathbf{y}}^H \overline{\mathbf{\Lambda}} \mathbf{x} + \overline{\mathbf{y}} \overline{\mathbf{y}}^H. \quad (42)$$

The first order derivative of $\mathbf{\Gamma}$ on $\mathbf{x}$ is

$$\frac{\mathrm{d}\mathbf{\Gamma}}{\mathrm{d}\mathbf{x}} = 2\overline{\mathbf{\Lambda}}^H \overline{\mathbf{\Lambda}} \mathbf{x} - 2\overline{\mathbf{\Lambda}}^H \overline{\mathbf{y}}. \quad (43)$$

Forcing $\frac{\mathrm{d}\mathbf{\Gamma}}{\mathrm{d}\mathbf{x}} = 0$, we have the following solution:

$$\widehat{\mathbf{x}}_{OLS} = (\overline{\mathbf{\Lambda}}^H \overline{\mathbf{\Lambda}})^{-1} \overline{\mathbf{\Lambda}}^H \overline{\mathbf{y}}. \quad (44)$$

Similarly, Bob can detect the received signal vectors as

$$\widehat{\mathbf{x}}_{ML} \cong arg \min_{x(l) \in \mathbf{S}(l)} ||\widehat{\mathbf{x}}_{OLS} - \mathbf{x}||^2. \quad (45)$$

V. Security Analysis

In this section, we conduct security analysis for single and multiple eavesdroppers, respectively. Through theoretical analysis, we demonstrate that the single eavesdropper cannot recover the transmitted signal. Moreover, for multiple eavesdroppers, even when each has the same receiving condition as Bob, it is also impossible for the eavesdroppers to recover the transmitted signal vectors.

1) With Single Eavesdropper: In the *l*-th transmission, for Eve, the received signal vector is

$$y_E(l) = \mathbf{h}_{AE}^H \mathbf{W}^l \mathbf{x} + n_E(l), l = 1, 2, \cdots, L, \quad (46)$$

Given $\mathbf{W}^l = (\mathbf{w}_1^l, \mathbf{w}_2^l, \cdots, \mathbf{w}_L^l)$, $\mathbf{h}_{AE}^H \mathbf{W}^l$ can be re-written as

$$\mathbf{h}_{AE}^H \mathbf{W}^l = (\mathbf{h}_{AE}^H \mathbf{w}_1^l, \mathbf{h}_{AE}^H \mathbf{w}_2^l, \cdots, \mathbf{h}_{AE}^H \mathbf{w}_L^l). \quad (47)$$

Then, all the *L* received signal vectors can be expressed as

$$\begin{bmatrix} y_E(1) \\ y_E(2) \\ \vdots \\ y_E(L) \end{bmatrix} = \begin{bmatrix} \mathbf{h}_{AE}^H \mathbf{w}_1^1 & \mathbf{h}_{AE}^H \mathbf{w}_2^1 & \cdots & \mathbf{h}_{AE}^H \mathbf{w}_L^1 \\ \mathbf{h}_{AE}^H \mathbf{w}_1^2 & \mathbf{h}_{AE}^H \mathbf{w}_2^2 & \cdots & \mathbf{h}_{AE}^H \mathbf{w}_L^2 \\ \vdots & \vdots & \cdots & \vdots \\ \mathbf{h}_{AE}^H \mathbf{w}_1^L & \mathbf{h}_{AE}^H \mathbf{w}_2^L & \cdots & \mathbf{h}_{AE}^H \mathbf{w}_L^L \end{bmatrix} \begin{bmatrix} x(1) \\ x(2) \\ \vdots \\ x(L) \end{bmatrix} + \begin{bmatrix} n_E(1) \\ n_E(2) \\ \vdots \\ n_E(L) \end{bmatrix}. \quad (48)$$

Similarly, all the *L* received signal vectors can be summed up

$$\begin{aligned} y_E &= (\mathbf{h}_{AE}^H \mathbf{W}^1 + \mathbf{h}_{AE}^H \mathbf{W}^2 + \cdots + \mathbf{h}_{AE}^H \mathbf{W}^L)\mathbf{x} + n_E \quad (49) \\ &= \mathbf{h}_{AE}^H \mathbf{W} \mathbf{x} + n_E. \end{aligned}$$

where $n_E = \Sigma_{l=1}^L n_E(l)$.

Obviously,

$$\mathbf{h}_{AE}^H \mathbf{W} = \begin{bmatrix} \mathbf{h}_{AE}^H \Sigma_{l'=1}^L \mathbf{w}_1^{l'} & \mathbf{h}_{AE}^H \Sigma_{l'=1}^L \mathbf{w}_2^{l'} & \cdots & \mathbf{h}_{AE}^H \Sigma_{l'=1}^L \mathbf{w}_L^{l'} \end{bmatrix}, \quad (50)$$

where $\mathbf{h}_{AE}^H \Sigma_{l'=1}^L \mathbf{w}_l^{l'} = \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m E} w_{ml}^{l'}\}$. According to Eq. (18), we have

$$\widehat{\mathbf{h}}_{AE}^H \mathbf{W} = \varphi_{AR} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}. \quad (51)$$

Therefore,

$$\mathbf{h}_{AE}^H \Sigma_{l'=1}^L \mathbf{w}_l^{l'} = \Sigma_{l'=1}^L \lambda_{l'l} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{ml}^{l'}\}. \quad (52)$$

Replacing Eq. (52) into Eq. (50), we have

$$y_E = \begin{bmatrix} \Sigma_{l'=1}^L \lambda_{l'1} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{m1}^{l'}\} \\ \Sigma_{l'=1}^L \lambda_{l'2} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{m2}^{l'}\} \\ \vdots \\ \Sigma_{l'=1}^L \lambda_{l'L} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{mL}^{l'}\} \end{bmatrix}^T \begin{bmatrix} x(1) \\ x(2) \\ \vdots \\ x(L) \end{bmatrix} + n_E. \quad (53)$$

Note that both $\widehat{\mathbf{h}}_{AB}$ and $\widehat{\mathbf{h}}_{AR}$ are unknown to Eve. With

2327-4662 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2919743, IEEE Internet of Things Journal

the random variation of the scrambling coefficient $w_{ml}^{l'}$, $\mathbf{h}_{AE}^H \Sigma_{l'=1}^L \mathbf{w}_l^{l'}$ will also vary randomly. Thus it is impossible for the eavesdropper to recover the transmitted signal vectors.

2) With Multiple Eavesdroppers: Suppose that there are *K* eavesdroppers. One of them, e.g., the *p*-th eavesdropper, launches pilot contamination attack, while the others just overhear Alice. According to Eq. (17), we have

$$\begin{cases} (\widehat{\mathbf{h}}_{AB}^H + \widehat{\mathbf{h}}_{AE_p}^H)\mathbf{W}^1 &= \phi_{AR}^1 \\ (\widehat{\mathbf{h}}_{AB}^H + \widehat{\mathbf{h}}_{AE_p}^H)\mathbf{W}^2 &= \phi_{AR}^2 \\ & \vdots \\ (\widehat{\mathbf{h}}_{AB}^H + \widehat{\mathbf{h}}_{AE_p}^H)\mathbf{W}^L &= \phi_{AR}^L, \end{cases} \tag{54}$$

where $\widehat{\mathbf{h}}_{AE_p}^H$ is the CSI of the *p*-th eavesdropper. The signal vectors received by all *K* eavesdroppers can be expressed as

$$\mathbf{Y}_E = \begin{bmatrix} y_{E_1}(1) & y_{E_1}(2) & \cdots & y_{E_1}(L) \\ y_{E_2}(1) & y_{E_2}(2) & \cdots & y_{E_2}(L) \\ \vdots & \vdots & \ddots & \vdots \\ y_{E_K}(1) & y_{E_K}(2) & \cdots & y_{E_K}(L) \end{bmatrix}, \tag{55}$$

where $y_{E_k(l)} = \widehat{\mathbf{h}}_{AE_k}^H \mathbf{W}^l \mathbf{x} + n_{E_k}(l), \quad k = 1, 2, \cdots, K.$

Similarly, according to Eq. (24) and (25), the received signal vectors $y_{E_p}(l)$ and $y_{E_k}(l)$ are

$$\begin{cases} y_{E_p}(l) = \phi_{AR}^l \mathbf{x} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}^l \mathbf{x} + n_{E_p}(l) \\ y_{E_k}(l) = \mathbf{h}_{AE_k}^H (\mathbf{h}_{AE_p}^H)^\dagger (y_{E_p}(l) - n_{E_p}(l)) + n_{E_k}(l), \end{cases} \tag{56}$$

where $(\mathbf{h}_{AE_p}^H)^\dagger$ is the right pseudo inverse matrix of $\mathbf{h}_{AE_p}^H$. Then, at the *k*-th eavesdropper, the received signals of *L* transmissions can be expressed as

$$\begin{cases} y_{E_k}(1) &= \mathbf{h}_{AE_k}^H (\mathbf{h}_{AE_p}^H)^\dagger (\phi_{AR}^1 \mathbf{x} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}^1 \mathbf{x}) + n_{E_k}(1) \\ y_{E_k}(2) &= \mathbf{h}_{AE_k}^H (\mathbf{h}_{AE_p}^H)^\dagger (\phi_{AR}^2 \mathbf{x} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}^2 \mathbf{x}) + n_{E_k}(2) \\ & \vdots \\ y_{E_k}(L) &= \mathbf{h}_{AE_k}^H (\mathbf{h}_{AE_p}^H)^\dagger (\phi_{AR}^L \mathbf{x} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}^L \mathbf{x}) + n_{E_k}(L). \end{cases} \tag{57}$$

Obviously, by summing up the received signal vectors, it is easy to obtain all the signal vectors

$$\begin{cases} y_{E_1} &= \mathbf{h}_{AE_1}^H (\mathbf{h}_{AE_p}^H)^\dagger (\varphi_{AR} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}) \mathbf{x} + n_{E_1} \\ y_{E_2} &= \mathbf{h}_{AE_2}^H (\mathbf{h}_{AE_p}^H)^\dagger (\varphi_{AR} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}) \mathbf{x} + n_{E_2} \\ & \vdots \\ y_{E_K} &= \mathbf{h}_{AE_K}^H (\mathbf{h}_{AE_p}^H)^\dagger (\varphi_{AR} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}) \mathbf{x} + n_{E_K}, \end{cases} \tag{58}$$

where $y_{E_k} = \Sigma_{l=1}^L y_{E_k}(l)$ and $n_{E_k} = \Sigma_{l=1}^L n_{E_k}(l)$. Especially, for the *p*-th eavesdropper who launched the pilot contamination attack, it is known that

$$y_{E_p} = (\varphi_{AR} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}) \mathbf{x} + n_{E_p}. \tag{59}$$

Eq. (58) can be re-written as

$$\begin{bmatrix} y_{E_1} \\ y_{E_2} \\ \vdots \\ y_{E_K} \end{bmatrix} = \begin{bmatrix} \mathbf{h}_{AE_1}^H (\mathbf{h}_{AE_p}^H)^\dagger (\varphi_{AR} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}) \\ \mathbf{h}_{AE_2}^H (\mathbf{h}_{AE_p}^H)^\dagger (\varphi_{AR} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}) \\ \vdots \\ \mathbf{h}_{AE_K}^H (\mathbf{h}_{AE_p}^H)^\dagger (\varphi_{AR} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}) \end{bmatrix} \begin{bmatrix} x(1) \\ x(2) \\ \vdots \\ x(L) \end{bmatrix} + \begin{bmatrix} n_{E_1} \\ n_{E_2} \\ \vdots \\ n_{E_K} \end{bmatrix}. \tag{60}$$

Denoting $\eta_{E_k} = \mathbf{h}_{AE_k}^H (\mathbf{h}_{AE_p}^H)^\dagger$, then we have $\mathbf{h}_{AE_k}^H (\mathbf{h}_{AE_p}^H)^\dagger (\varphi_{AR} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W}) = \eta_{E_k} (\varphi_{AR} - \widehat{\mathbf{h}}_{AB}^H \mathbf{W})$.

Similarly, Eq. (53) can be re-expressed as

$$y_{E_k} = \begin{bmatrix} \eta_{E_k}[\Sigma_{l'=1}^L \lambda_{l'1} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{m1}^{l'}\}] \\ \eta_{E_k}[\Sigma_{l'=1}^L \lambda_{l'2} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{m2}^{l'}\}] \\ \vdots \\ \eta_{E_k}[\Sigma_{l'=1}^L \lambda_{l'L} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{mL}^{l'}\}] \end{bmatrix}^T \begin{bmatrix} x(1) \\ x(2) \\ \vdots \\ x(L) \end{bmatrix} + n_{E_k}. \tag{61}$$

Thus, the coefficient matrix of Eq. (60) will become

$$\begin{bmatrix} \eta_{E_1}[\Sigma_{l'=1}^L \lambda_{l'1} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{m1}^{l'}\}] & \cdots \\ \eta_{E_2}[\Sigma_{l'=1}^L \lambda_{l'1} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{m1}^{l'}\}] & \cdots \\ \vdots & \vdots \\ \eta_{E_K}[\Sigma_{l'=1}^L \lambda_{l'1} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{m1}^{l'}\}] & \cdots \\ \eta_{E_1}[\Sigma_{l'=1}^L \lambda_{l'L} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{mL}^{l'}\}] \\ \eta_{E_2}[\Sigma_{l'=1}^L \lambda_{l'L} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{mL}^{l'}\}] \\ \vdots \\ \eta_{E_K}[\Sigma_{l'=1}^L \lambda_{l'L} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L \{\sum_{m=1}^M h_{A_m B} w_{mL}^{l'}\}] \end{bmatrix} \tag{62}$$

Since $\widehat{\mathbf{h}}_{AB}$ and $||\widehat{\mathbf{h}}_{AR}||$ are unknown to eavesdroppers, $\eta_{E_k}[\Sigma_{l'=1}^L \lambda_{l'l} ||\widehat{\mathbf{h}}_{AR}|| - \sum_{l'=1}^L (\sum_{m=1}^M h_{A_m B} w_{ml}^{l'})]$ will vary randomly with different *k* and *l*. From Eq. (62), it is impossible for eavesdroppers to resolve the equation with a random and unknown coefficient matrix.

3) Security of Relay: At Relay, it is known that

$$\begin{cases} \phi_{AR}^l = (\widehat{\mathbf{h}}_{AB}^H + \widehat{\mathbf{h}}_{AE}^H)\mathbf{W}^l \\ y_R(l) = \widehat{h}_{AR}^H \mathbf{W}^l \mathbf{x} + n_R(l). \end{cases} \tag{63}$$

Thus, we can obtain

$$y_R(l) = \widehat{\mathbf{h}}_{AR}^H (\widehat{\mathbf{h}}_{AB}^H + \widehat{\mathbf{h}}_{AE}^H)^\dagger \phi_{AR}^l \mathbf{x} + n_R(l). \tag{64}$$

Similarly, summing up *L* signal vectors yields

$$y_R = \widehat{\mathbf{h}}_{AR}^H (\widehat{\mathbf{h}}_{AB}^H + \widehat{\mathbf{h}}_{AE}^H)^\dagger \varphi_{AR} \mathbf{x} + n_R. \tag{65}$$

Clearly, it is impossible for Relay to recover the transmitted signals alone since both $\widehat{\mathbf{h}}_{AB}$ and $\widehat{\mathbf{h}}_{AE}$ are unknown and φ_{AR} is random.

VI. Simulation Results

In this section, we provide the simulation results to validate the analysis and evaluate the performance of the proposed scheme. For simulations, we have the following settings. Alice

2327-4662 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2919743, IEEE Internet of Things Journal

is equipped with 4 antennas, and there are 1 relay node and 6 eavesdroppers both with single antenna. The channels among Alice, relay, and all eavesdroppers, are independently generated as complex Gaussian random variables with zero mean and unit variance. The channels remain constant within a block while varying independently across blocks. The block length N is set to 8. Each data symbol is uniformly selected from $\{1+i, 1-i, -1+i, -1-i\}$. Average received SNR ranges from 3dB to 13dB. Both Bob and Eve detect the received signal vectors according to Eq. . Bit error rate (BER) is adopted as the major performance metric. Simulation result is obtained by performing 10^4 times Monto Carlo experiments.

Fig. 3 shows the BER performance of Bob and Eve with different signal vector dimensions. It can be seen that the transmitted information can hardly be intercepted by eavesdroppers. The BER of eavesdroppers is around 0.5, and in practical scenarios such as fading channels, achieving BER of 0.5 at eavesdroppers can be considered for perfect secrecy. Moreover, Eve's BER always maintain fixed, approximately equal to 0.5, regardless of SNR. This implies that perfect security is achievable.

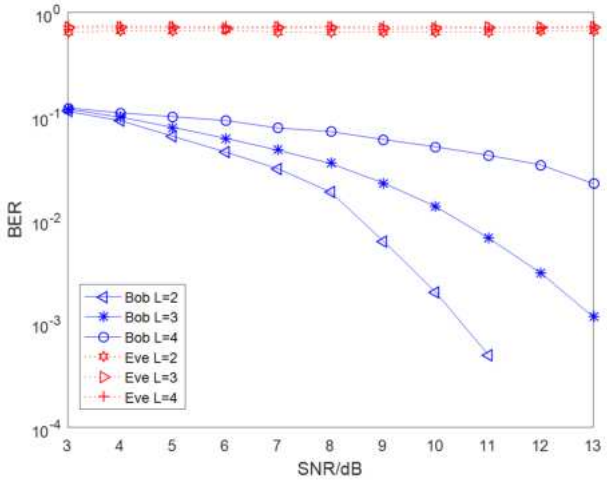


Fig. 3. BER VS. SNR with different dimension L

To a great extent, the successful signal detection mainly depends on whether there exists distinguished difference between the coefficient terms, which should satisfy the constraints (17) and can be used as weights of the corresponding components of the same symbol vector in turn. Thus, they can be regarded as a type of order information of signal components. On the other hand, as L keeps increasing, more degrees of freedom can be used to calculate the 2-norm, which will increase the possibility that two different signal vectors have the same 2-norm.

Since the physical channels $\mathbf{h}_{AB}$, $\mathbf{h}_{AR}$ and $\mathbf{h}_{AE}$ are independent, unique and different from each other, it is difficult for Eve to obtain the knowledge of $\mathbf{h}_{AB}$ and $\mathbf{h}_{AR}$. According to Eq. (53) and (62), the received signals at Eve can vary randomly, making Eve difficult to recover the transmitted signal vectors. At the same time, Bob also has the same problem if no Relay's help when the CSI from Alice to Eve is not available. Combining the received signals of Relay with his own signals, Bob can eliminate the negative effects of the interference introduced by Eve during the reverse training phase. Fig. 3 demonstrates that the proposed secure scheme is effective under pilot contamination attack.

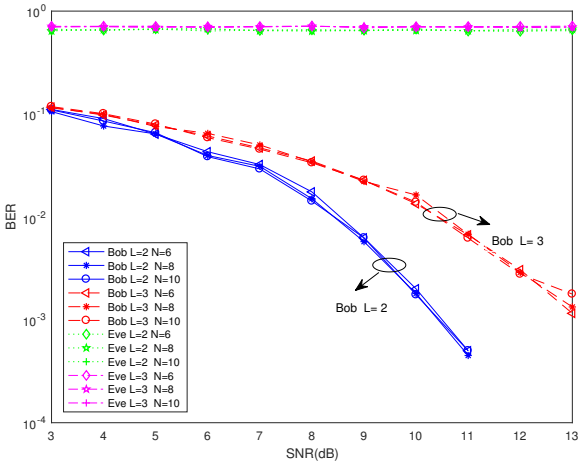


Fig. 4. BER VS. SNR with different block length N.

It can also be seen that as L keeps increasing, Bob's reception performance decreases and BER increases. The reason is as follows. According to Eq. (36), if Alice increases the dimension of signal vectors, more components from the received random signal vectors, each vector representing a superposition signal, need to be recovered by Bob. It also implies that the signal observation space is expanded and its structure becomes much more complicated with increasing of L. Besides, cumulative noise and extra estimate error are introduced into detection process when estimating the parameter η, making more difficulties for Bob in successfully recovering the signal vectors.

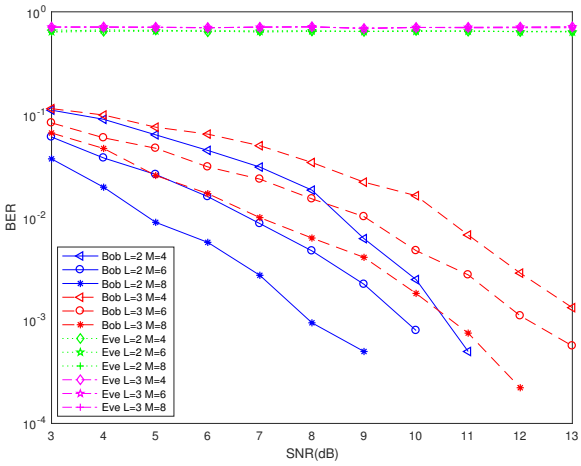


Fig. 5. BER VS. SNR with different antenna number M.

Fig. 4 shows the BER performance of Bob with respect to different block length N. It can be seen that, Bob's BER curves

2327-4662 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2919743, IEEE Internet of Things Journal

with different N almost coincide. Thus, the impact of block length N on Bob's BER is nearly negligible.

As shown in Fig. 5, Bob's BER keeps decreasing as M increases from 4 to 8. It can be seen that Bob's receiving performance is closely related to the number of transmitting antenna at Alice. The BER of Bob can be improved by employing more antenna while guaranteeing that the BER of adversary is still 0.5 (i.e., perfect secrecy is guaranteed).

VII. Conclusions

In this paper, we have investigated secure downlink communication in IoT networks under potential pilot contamination attacks. A relay aided vectorized secure transmission strategy has been proposed, which does not distinguish the pilot sequences sent from the eavesdropper and the legitimate. A set of data symbols are superposed using a random complex matrix to form signal vectors to send. Through cooperation with the relay, the intended receiver is able to recover the information signals under potential pilot contamination attack, whereas the eavesdropper or the relay cannot. Through security analysis, it is proved that the proposed scheme is effective and secure. Simulation results demonstrate that the proposed scheme can ensure secure communication under potential pilot contamination attacks. In the future work, we will study how to achieve secure communication where eavesdroppers are intelligent and smart to choose the best strategies under different scenarios.

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5):1125–1142, 2017.

[2] H. Omar, W. Zhuang, A. Abdrabou, and L. Li. Performance evaluation of vemac supporting safety applications in vehicular networks. *IEEE Transactions on Emerging Topics in Computing*, 1(1):69–83, 2013.

[3] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao. A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal*, 4(5):1250–1258, 2017.

[4] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu. Security vulnerabilities of internet of things: A case study of the smart plug system. *IEEE Internet of Things Journal*, 4(6):1899–1909, 2017.

[5] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, 2018.

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

[7] A. Mukherjee. Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints. *Proceedings of the IEEE*, 103(10):1747–1761, 2015.

[8] C. Lai, H. Li, R. Lu, and X. Shen. Se-aka: A secure and efficient group authentication and key agreement protocol for lte networks. *Computer Networks*, 57(17):3492–3510, 2013.

[9] H. Zhu, R. Lu, X. Shen, and X.Lin. Security in service-oriented vehicular networks. *IEEE Wireless Communications*, 16(4), 2009.

[10] D. Chen, N. Zhang, R. Lu, N. Cheng, K. Zhang, and Z. Qin. Channel precoding based message authentication in wireless networks: Challenges and solutions. *IEEE Network*, 33(1):99–105, 2019.

[11] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen. Physical layer security in wireless networks: A tutorial. *IEEE Wireless Commun.*, 18(2):66–74, Apr. 2011.

[12] D. Chen, N. Zhang, Z. Qin, X. Mao, Z. Qin, X. Shen, and X. Li. S2m: A lightweight acoustic fingerprints-based wireless device authentication protocol. *IEEE Internet of Things Journal*, 4(1):88–100, 2017.

[13] A. D. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, Oct. 1975.

[14] D. Rawat, T. White, M. Parwez, c. Bajracharya, and M. Song. Evaluating secrecy outage of physical layer security in large-scale mimo wireless communications for cyber-physical systems. *IEEE Internet of Things Journal*, 4(6):1987–1993, 2017.

[15] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. Mark, and X. Shen. Partner selection and incentive mechanism for physical layer security. *IEEE Transactions on Wireless Communications*, 14(8):4265–4276, 2015.

[16] D. Chen, N. Zhang, R. Lu, x. Fang, k. Zhang, Z. Qin, and X. Shen. An ldpc code based physical layer message authentication scheme with prefect security. *IEEE Journal on Selected Areas in Communications*, 36(4):748–761, 2018.

[17] H. M. Wang, T. Zheng, and X. G. Xia. Secure miso wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading. *IEEE Trans. Wireless Commun.*, 14(1):94–106, Jan. 2015.

[18] X. Wang, Z. Zhang, and K. Long. Secure beamforming for multiple-antenna amplify-and-forward relay networks. *IEEE Trans. Signal Process.*, 64(6):1477–1492, Mar. 2016.

[19] F. Jameel, S. Wyne, G. Kaddoum, and T. Duong. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Communications Surveys & Tutorials*, 2018.

[20] X. Zhang, M. R. Mckay, X. Zhou, and R. W. Heath. Artificial-noise-aided secure multi-antenna transmission with limited feedback. *IEEE Trans. Wireless Commun.*, 14(5):2742–2754, May 2015.

[21] A. Kashyap, T. Basar, and R. Srikant. Correlated jamming on mimo gaussian fading channels. *IEEE Trans. Inf. Theory*, 50(9):2119–2123, Sep. 2004.

[22] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar. On the gaussian mimo wiretap channel. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, pages 2471–2475, Jun. 2007.

[23] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor. Physical layer security in wireless networks with passive and active eavesdroppers. In *Proc. IEEE Global Commun. Conference (GLOBCOM)*, pages 4868–4873, Dec. 2012.

[24] D. Kapetanovi, G. Zheng, K. K. Wong, and B. Ottersten. Detection of pilot contamination attack using random training and massive mimo. In *Proc. IEEE Int. Symp. Pers., Indoor and Mobile Radio Commun. (PIMRC'13)*, pages 13–18, Sep. 2013.

[25] X. Hou, C. Gao, Y. Zhu, and S. Yang. Detection of active attacks based on random orthogonal pilots. In *Proc. IEEE Wireless Commun. Signal Process. (WCSP)*, pages 1–4, Oct. 2016.

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

[27] Yanpeng Guan and Xiaohua Ge. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. *IEEE Transactions on Signal and Information Processing over Networks*, 4(1):48–59, 2018.

[28] X. Zhou, B. Maham, and A. Hjorungnes. Pilot contamination for active eavesdropping. *IEEE Trans. Wireless Commun.*, 11(3):903–907, Mar. 2012.

[29] R. Wu, S. Yuan, and C. Yuan. Secure transmission against pilot contamination: A cooperative scheme with multiple antennas. *IEEE symposium on Computers and Communications (ISCC)*, pages 1–5, Jun. 2018.

[30] J. K. Tugnait. Self-contamination for detection of pilot contamination attack in multiple antenna systems. *IEEE Wireless Commun. Lett.*, 4(5):525–528, Oct. 2015.

[31] Q. Xiong, Y. C. Liang, K. H. Li, and Y. Gong. An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems. *IEEE Trans. Inf. Forensics Security*, 10(5):932–940, May 2015.

[32] K. Yuan, L. Guo, C. Dong, and T. Kang. Detection of active eavesdropper using source enumeration method in massive mimo. In *Proc. IEEE Int. Conf. Commun. (ICC)*, pages 1–5, May 2017.

[33] X. Li, M. Chen, and E. P. Ratazzi. Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy. In *Proc. IEEE Workshop on Signal Proces. Advances in Wireless Commun. (SPAWC)*, pages 811–815, Jun. 2005.

[34] S. M. Kay. *Fundamentals of Statistical Signal Processing: Estimation Theory*. PTR Prentice hall, 1993.

[35] D. J. Tylavsky and G. R. L. Sohie. Generalization of the matrix inversion lemma. *Proceedings of the IEEE*, 74(7):1050–1052, Jul. 1986.

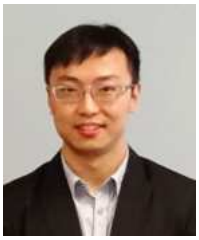
[36] R. Penrose. A generalized inverse of matrices. *Mathematical Proceedings of the Cambridge Philosophical Society*, 57(3):17–19, 1955.

[37] A. N. Tikhonov. *Solution of Incorrectly Formulated Problems and The Regularization Method*. Soviet Mathematics, 1963.

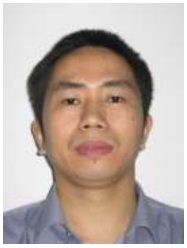
[38] K. P. Burnham. *Information and Likelihood Theory: A Basis for Model Selection and Inference*. Springer New York, 2002.

2327-4662 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2919743, IEEE Internet of Things Journal



Ning Zhang (M'12-SM'18) received B.E. degree and M.S. degree from Beijing Jiaotong University and Beijing University of Posts and Telecommunications in 2007 and 2010, respectively. He received the Ph.D degree from University of Waterloo, Canada, in 2015. From 2015 to 2017, he was a postdoc research fellow at University of Waterloo and University of Toronto, Canada, respectively. Since 2017, He has been an Assistant Professor at Texas A&M University-Corpus Christi, USA. He serves/served as an Associate Editor of IEEE Transactions on Cognitive Communications and Networking, IEEE Access and IET Communications, an Area Editor of Encyclopedia of Wireless Networks (Springer) and Cambridge Scholars. He also served as the workshop chair for MobiEdge'18 (in conjunction with IEEE WiMob 2018) and CoopEdge'18 (in conjunction with IEEE EDGE 2018), and 5G&NTN'19 (in conjunction with IEEE ICCC 2019). He is a recipient of the Best Paper Awards from IEEE Globecom in 2014, IEEE WCSP in 2015, Journal of Communications and Information Networks in 2018, IEEE Technical Committee on Transmission Access and Optical Systems in 2019, and IEEE ICC in 2019, respectively. His current research interests include next generation mobile networks, physical layer security, machine learning, and mobile edge computing.



Renyong Wu received the M.Sc. degrees in computer science from Hunan University, China, in 1998, and the Ph.D. degree in information and communication engineering from Huazhong University of Science Technology, China, in 2007. From 1998 to 2003, he was a senior telecom engineer with China Telecom. In 2011, he was a Visiting Scholar with the Department of Electrical Computer Engineering, University of Waterloo, Canada. Since 2007, he has been with the College of Computer Science and Electronic Engineering, Hunan University, where he is an Associate Professor. His research interests mainly include future wireless networks, mobile communication and multiuser signal processing.

Shenglan Yuan received the B.S. degree in electrical engineering from North China Electric Power University, China, 2015, and the M.S. degree in communication engineering from Hunan University, China, 2018, where she is currently working towards the Ph.D. degree in computer science. Her research interests include wireless communication networks and physical layer security.

Chao Yuan received the B.S. and M.S. degree in communication engineering from Hunan University, China, in 2014 and 2017, respectively. He is currently a research engineer with Ant Finanical Inc., China. His research interests include intelligent wireless communications and physical layer security

Dajiang Chen is currently an Assistant Professor in the School of information and software Engineering at University of Electronic Science and Technology of China (UESTC). He was a Post Doctoral Fellow at the University of Waterloo, Waterloo, ON, Canada, from 2015 to 2017.

He was also a Post Doctoral Fellow in the School of information and software Engineering at UESTC, from 2014 to 2017. He received the B.Sc. degree in 2005 and the M.Sc. degree in 2009 from Neijiang Normal University and Sichuan University, respectively, and the Ph.D. degree in information and communication engineering from UESTC in 2014. His current research interest includes Information Theory, Secure Channel Coding, and their applications in Wireless Network Security, Wireless Communications and other related areas. Dr. Chen serves/served as a TPC Member for IEEE Globecom, IEEE ICC, IEEE VTC, and IEEE WF-5G.

2327-4662 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.