IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 5, 2018, accepted May 10, 2018, date of publication May 16, 2018, date of current version June 5, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2837059

Energy Efficiency of Proactive Eavesdropping for Multiple Links Wireless System

BAOGANG LI[1], **(Member, IEEE), YUANBIN YAO**[1], **HAIJUN ZHANG**[2], **(Senior Member, IEEE), YABO LV**[1], **AND WEI ZHAO**[1]

[1]Department of Electronic and Communication Engineering, North China Electric Power University, Baoding 071003, China
[2] Beijing Engineering and Technology Research Center for Convergence Networks and Ubiquitous Services, University of Science and Technology Beijing, Beijing 100083, China

Corresponding author: Baogang Li (baogangli@ncepu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61501185 and Grant 61601182, in part by the Hebei Province Natural Science Foundation under Grant F2016502062, in part by the Fundamental Research Funds for the Central Universities under Grant 2016MS97, Grant 2015MS95, Grant 2015MS95, and Grant 2015MS125, and in part by the Beijing Natural Science Foundation under Grant 4164101.

ABSTRACT In this paper, we investigate the legitimate surveillance of wireless communication system, which includes multiple suspicious links. We propose a novel objective of eavesdropping energy efficiency (EEE) to value the performance of eavesdropping. Our general objective is to maximize EEE while all the suspicious links are eavesdropped, which can be accomplished through either jamming or assisting each suspicious link at a suspicious receiver under the consideration of many practical limitations, such as transmission strategy of a suspicious transmitter, power budget of legitimate monitor (LM), and eavesdropping ratio of a whole system. The formulated problem leads to a challenging mixed-integer nonlinear programming (MINLP) problem. To solve this problem, we propose a novel eavesdropping scheme by the special characteristic of eavesdropping, and the complex MINLP problem can be transformed to a concave optimization problem by a series of transformations, which can be solved by the Lagrange multiplier method. Considering the infeasibility of our proposed eavesdropping scheme when the power of LM is insufficient to eavesdrop all the suspicious links, we propose a heuristic algorithm to obtain a tradeoff between EEE and eavesdropping ratio. Numerical results show that our proposed eavesdropping schemes outperform the proactive jamming scheme and the average-power eavesdropping scheme.

INDEX TERMS Legitimate surveillance, eavesdropping energy efficiency, proactive eavesdropping, MINLP, eavesdropping ratio.

I. INTRODUCTION

Due to the broadcast nature of radio propagation, the wireless air interface is open and accessible to both authorized and illegitimate users [1]. It is significant to improve wireless communications security to fight against illegitimate users. A lot of researches exploit sophisticated signal processing techniques to increase the secrecy capacity, such as the artificial-noise-aided security [2], security-oriented beamforming [3], [4]. It is noted that almost all existing works often consider the eavesdropping process and jamming process as illegitimate attacks [5], [6], which are prohibited from a national security point of view. However, some legitimate eavesdropping accredited by the government can effectively discover, ascertain and prevent the information transmitted between suspicious users, which is a new research direction of wireless communication security.

There have been a little works in legitimate eavesdropping [7]–[13], a new approach namely proactive eavesdropping via cognitive jamming emerges, in which legitimate monitor (LM) purposely sends jamming signals to suspicious link for eavesdropping successfully [7]–[10]. In addition, [11] and [12] proposed a spoofing relay scheme to intervene a suspicious link. Note that all the aforementioned works focus on a single suspicious link. It is significant to extend the proactive eavesdropping technology into more practical scenarios. Reference [13] studied a multiple-input multiple-output (MIMO) legitimate surveillance system which improved the eavesdropping non-outage probability compared to single antenna LM. Reference [14] investigated proactive monitoring via jamming over MIMO Rayleigh fading channels. Meanwhile, [15] and [16] studied the proactive eavesdropping of two-hop suspicious communication link.

Since multiple links communication is more and more widely adopt, (e.g. orthogonal frequency division multiplexing (OFDM)). The security of multiple links communication system is crucial, whereas there are few studies of eavesdropping multiple suspicious links yet. Thus we propose a proactive eavesdropping scheme of multiple links communication system in this paper to fill this gap.

For multiple links communication system, especially OFDM-based system, the suspicious communication link is divided into multiple suspicious sub-links, which increases the difficulty of monitoring. In this paper, we propose a proactive eavesdropping scheme to eavesdrop multiple suspicious communication links efficiently. Specifically, LM contains two parts, eavesdropping part and intervention part. The former is responsible for eavesdropping and obtaining the information of suspicious transmitter (ST), the latter can adjust multiple jamming signal to suspicious receiver (SR) to guarantee the eavesdropping capability or work as a relay to forward the signal from ST to SR for a higher eavesdropping rates.

Jamming and relay power are great energy consumptions for LM. Generally, the monitor device is mobile, portable, or vehicle-mounted, the power may be only battery with limited capacity. However large-scale eavesdropping may be a necessary mission. In this case, the energy utilization is important for the constrained monitor. In this paper, we introduce a novel objective of eavesdropping energy efficiency (EEE) to evaluate the energy utilization of monitor. EEE can be defined as the improved eavesdropping rate for unit utilized power of LM. There has been much research about the energy efficiency of the wireless communication system. But to our knowledge, there is no research of energy efficiency about proactive eavesdropping system. Thus we formulate a EEE maximization problem under different transmission strategies of ST (i.e. fixed-power transmission and adaptive power transmission). Since multiple suspicious links include suspicious links have eavesdropped and suspicious links have not. Our proposed optimization problem is proposed to obtain the maximum EEE while guaranteeing all the suspicious links can be eavesdropped, which makes our proposed optimization problem to be a mixed-integer nonlinear programming (MINLP) problem. To address this issue, we utilize the characteristic of proactive eavesdropping to transform this complex optimization problem to a simplified form, which can be solved by Lagrange multiplier method finally. However, there exists the case when LM has not enough power to eavesdrop all the suspicious links, which makes our problem to be infeasible. Considering global eavesdropping scheme for our proposed model, we propose a heuristic algorithm to obtain a near optimal solution of this case, which considers a trade-off between EEE and eavesdropping ratio.

The rest of this paper is organized as follows. In section II, we present the system model and formulate the optimization problem. In section III, we solve the MINLP problem in the case when LM has enough power by the characteristic of eavesdropping. In section IV, heuristic algorithm is proposed to solve the infeasible case of optimization problem when the power of LM is insufficient. Section V shows the numerical results of our proposed eavesdropping schemes. Finally, we conclude this paper at section VI.

II. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig. 1, we consider a legitimate surveillance scenario, including one pair of ST and SR, meanwhile a full-duplex LM with one eavesdropping antenna and one intervention antenna. There are $N \geq 1$ suspicious links simultaneously in the communication system, e.g. OFDM-based suspicious system works on N orthogonal sub-channels. The LM can eavesdrop and jam/relay simultaneously for the full-duplex ability, which aims to successfully eavesdrop multiple suspicious links via jamming/assisting SR.

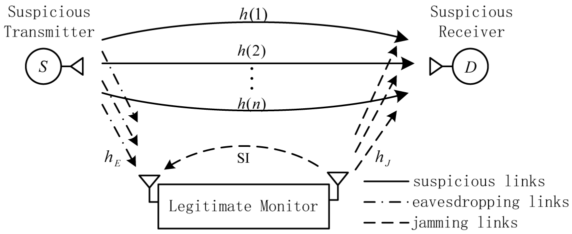


FIGURE 1. The proactive eavesdropping model of multiple links communication system.

We consider a Rayleigh block fading channel, which remains constant during each time block and is independent with each other. Furthermore, we assume the channel state information (CSI) of all links are perfectly known at the monitor by the method given in [11], so as to reveal the fundamental limit of multi-link legitimate eavesdropping.

For the nth suspicious communication link, let $h(n)$, $h_E(n)$ and $h_J(n)$, $n \in [1, 2, \cdots, N]$ denote channel coefficient from ST to SR, channel coefficient from SR to eavesdropping antenna of LM and channel coefficient from jamming antenna of LM to SR respectively. All the above channel coefficients obey the complex Gaussian distribution respectively, the corresponding channel power gains can be defined as $g(n) = |h(n)|^2$, $g_E(n) = |h_E(n)|^2$ and $g_J(n) = |h_J(n)|^2$, respectively.

We consider that ST transmits information with power $p(n)$ of nth suspicious link, while the jamming/relay power $q(n)$ of LM sent to jam/assist nth suspicious link will change to facilitate the eavesdropping. Let Q denotes the maximum power supplied by the legitimate monitor for jamming and relay, P denotes the maximum transmit power of suspicious transmitter, thus we have

$$\sum_{n=1}^{N} q(n) \leq Q, \tag{1}$$

$$\sum_{n=1}^{N} p(n) \leq P. \tag{2}$$

Now, according to the data rate of suspicious link $R_D(n)$ and the data rate of eavesdropping link $R_E(n)$, we can divide the suspicious links into two categories, which are non-eavesdropped suspicious links set Ω_1 and eavesdropped suspicious links set Ω_2, respectively.

For the first suspicious links set Ω_1, $R_E(n) < R_D(n)$, all the suspicious links have not got eavesdropped successfully. LM will work as a jammer, only by reducing the data rate of suspicious link $R_D(n)$, can LM successfully eavesdrop the suspicious link. For the second suspicious links set Ω_2, $R_E(n) \geq R_D(n)$, all the suspicious links have got eavesdropped successfully. LM will work as a relay to enhance the performance of eavesdropping.

We assume that the message transmitted by the nth ST is $s(n)$, and the corresponding signal of LM is $x(n)$, so after LM jamming the suspicious links at Ω_1, the signal received by SR via nth suspicious link is

$$y_{D1}(n) = \sqrt{p(n)}h(n)s(n) + \sqrt{q(n)}h_J(n)x(n) + n_{D1}(n), \quad (3)$$

the message eavesdropped by LM is

$$y_{E1}(n) = \sqrt{p(n)}h_E(n)s(n) + n_{SI}(n) + n_{E1}(n), \quad (4)$$

As for the suspicious links set Ω_2, the signals receives by SR via nth suspicious link after LM forwarding message to SR is

$$y_{D2}(n) = \sqrt{p(n)}h(n)s(n) + \sqrt{q(n)}h_J(n)x(n) + n_{D2}(n), \quad (5)$$

the message eavesdropped by LM is

$$y_{E2}(n) = \sqrt{p(n)}h_E(n)s(n) + n_{SI}(n) + n_{E2}(n), \quad (6)$$

where $n_{Di}(n)|_{i=1,2}$ and $n_{Ei}(n)|_{i=1,2}$ with zero mean and variances $\sigma^2(n)$ denote the additive white Gaussian noises (AWGNs) at SR and eavesdropping antenna of LM, respectively. $n_{SI}(n)$ denotes the SI of LM, which is assumed to be perfectly canceled by using advanced analog and digital self-interference cancellation schemes similar to [7]. $\beta(n)$ denotes the amplification of LM as $\beta(n) = \sqrt{\frac{q(n)}{\phi(n)(p(n)g_E(n)+\sigma^2(n))+\sigma^2(n)}}$. Besides, $\phi(n) \in [0, 1]$ denotes the signal splitting ratio that divides the signal into signal for the AF relay and signal for eavesdropping. Accordingly, we can get the signal-to-interference-plus-noise ratio (SINR) at SR and the eavesdropping antenna of LM

$$\begin{cases} \gamma_{D1}(n) = \dfrac{g(n)p(n)}{g_J(n)q(n) + \sigma^2(n)}, \\ \gamma_{E1}(n) = \dfrac{g_E(n)p(n)}{\sigma^2(n)}, \end{cases} \quad (7)$$

$$\begin{cases} \gamma_{D2}(n) = \dfrac{(\phi(n)\beta^2(n)g_E(n)g_J(n) + g(n))p(n)}{(\beta^2(n)g_J(n) + \phi(n) + 1)\sigma^2(n)}, \\ \gamma_{E2}(n) = \dfrac{(1 - \phi(n))g_E(n)p(n)}{(2 - \phi(n))\sigma^2(n)}, \end{cases} \quad (8)$$

accordingly, we can get the data rate of the suspicious link and eavesdropping link based on Shannon formula as

$$R_{Di}(n) = log_2(1 + \gamma_{Di}(n)), \quad i = 1, 2, \quad (9)$$

$$R_{Ei}(n) = log_2(1 + \gamma_{Ei}(n)), \quad i = 1, 2. \quad (10)$$

We introduce an indicator function to denote LM has eavesdropped successfully or has not:

$$\alpha(n) = \begin{cases} 1, & if\ \gamma_E(n) \geq \gamma_D(n), \\ 0, & otherwise. \end{cases} \quad (11)$$

For the suspicious links at Ω_1 with $\gamma_{E1}(n) < \gamma_{D1}(n)|_{q(n)=0}$, we denote the achievable eavesdropping rate after jamming this suspicious link as $r_{eav1}(n)$. For the suspicious links at Ω_2 with $\gamma_{E2}(n) \geq \gamma_{D2}(n)|_{q(n)=0,\phi(n)=0}$, we denote the achievable eavesdropping rate of this suspicious link as $r_{eav2}(n)$.

For multiple suspicious links include eavesdropped links and non-eavesdropped links, we not only jam suspicious links to enable successfully eavesdropping but also forward for suspicious receiver to acquire higher eavesdropping rate. Therefore, the eavesdropping rate is

$$R_{eav} = \sum_{n\in\Omega_1} \alpha(n)r_{eav1}(n) + \sum_{n\in\Omega_2} r_{eav2}(n). \quad (12)$$

We introduce the system EEE for multiple suspicious links to evaluate the above performance, which is defined as follows

$$\eta = \frac{R_{eav} - R_{eav}^{(0)}}{\sum_{n=1}^{N} q(n)}, \quad (13)$$

which implies the improved system eavesdropping rate per unit power of LM. $R_{eav}^{(0)} = \sum_{n\in\Omega_2} R_{D2}^{(0)}(n)$ is the initial eavesdropping rate of suspicious links at Ω_2 before relay.

For the multiple suspicious links communication system, we study the allocation of jamming and relay power to maximize EEE and guarantee a reliable eavesdropping ratio as well. We form the problem of maximizing system EEE as follows

$$(P1): \ \max \ \eta$$

$$s.t. \sum_{n=1}^{N} \alpha(n)q(n) \leq Q, \quad (14)$$

$$R_E(n) \geq R_D(n), \quad \forall n. \quad (15)$$

where (14) is to guarantee the power constraint of the monitor, (15) is the eavesdropping ratio constraint which ensures all the eavesdropping links being eavesdropped, since larger number of eavesdropped suspicious links means higher eavesdropping ratio of legitimate monitor. To solve the problem (P1), we first check the feasibility of of the problem (P1). We have a theorem of successfully eavesdropping a single suspicious link as follows

Theorem 1: The maximum eavesdropping rate of eavesdropping a single suspicious link n is obtained if and only if $R_D(n) = R_E(n)$, the eavesdropping rate $r_{eav}(n) = R_D(n)$. For suspicious links at Ω_1, the optimal jamming power $q^*(n)$ is the power consumed to reduce $R_D(n)$ to $R_E(n)$.

$$q^*(n) = \frac{1}{g_J(n)}\Big(\frac{g(n)\sigma^2(n)}{g_E(n)} - \sigma^2(n)\Big), \quad n \in \Omega_1. \quad (16)$$

Proof: The eavesdropping rate of suspicious link at Ω_1 is $R_D(n), n \in \Omega_1$ if and only if $R_E(n) \geq R_D(n)$, $n \in \Omega_1$, or the eavesdropping rate is 0. When the jamming power $q(n) \geq q^*(n), n \in \Omega_1$, the eavesdropping rate $R_D(n), n \in \Omega_1$ starts to reduce. For the eavesdropping rate of suspicious links at Ω_2, $R_E(n) \geq R_D(n), n \in \Omega_2$. There exists a peak of the eavesdropping rate when $R_E(n) = R_D(n), n \in \Omega_2$, since $R_D(n), n \in \Omega_2$ is increasing and $R_E(n), n \in \Omega_2$ is decreasing during the relay from LM to SR. So that the maximum eavesdropping rate of eavesdropping a single suspicious link n is obtained if and only if $R_D(n) = R_E(n), n \in \Omega_1 \cup \Omega_2$. ■

Generally, the monitor is an energy constraint node. The finite jamming power is hoped to produce more eavesdropping rate. According to theorem 2.1, the LM cannot stop jamming SR until $\gamma_{E1}(n) = \gamma_{D1}(n)$, then the suspicious information can be eavesdropped. We denote the achievable eavesdropping rate after jamming this suspicious link as $r_{eav1}(n) = R_{D1}(n)$. For the suspicious links at Ω_2 with $\gamma_{E2}(n) \geq \gamma_{D2}(n)|_{q=0,\phi=0}$, the relay power and signal splitting ratio should be also adjusted until $\gamma_{E1}(n) = \gamma_{D1}(n)$, which means the peak of the eavesdropping rate. Then we denote the achievable eavesdropping rate of this suspicious link as $r_{eav2}(n) = R_{D2}(n)$.

For our proposed optimization problem, when the power of LM is enough for jamming all the suspicious links at Ω_1 to get eavesdropped, the LM will jam the non-eavesdropped suspicious links preferentially. According to theorem 2.1, we denote the jamming power that just meets the requirement of eavesdropping all the suspicious links at Ω_1 as $Q_l = \sum_{n\in\Omega_1} q^*(n)$. When $Q \geq Q_l$, the problem (P1) is feasible, i.e. all the suspicious links will get eavesdropped with a jamming power consumption Q_l of LM. Then LM will utilize the extra power to improve the performance of relay to reach higher eavesdropping rate, which is the main study task and contribution of this paper.

When $Q \leq Q_l$, the problem (P1) is infeasible, which means the power of LM cannot afford to eavesdrop all the non-eavesdropped suspicious links. In this case, LM will tend to eavesdrop as many suspicious links as possible for the constraint (15) and try to achieve higher EEE as well.

To further analyze the problem (P1), we study the power allocation of LM according to the power constraint Q and solve the MINLP problem (P1) by utilizing the theorem 2.1 of successfully eavesdropping a suspicious link, which is the characteristic of proactive eavesdropping.

III. THE SOLUTION OF LEGITIMATE MONITOR WITH ENOUGH POWER

In this section, LM has enough power to eavesdrop all the suspicious links, our task is to obtain the highest EEE. Since all the non-eavesdropped suspicious links can get eavesdropped, which means $\alpha(n) = 1, n \in \Omega_1$, problem (P1) can be expanded as

$$
\begin{aligned}
(P2): \quad & \max_{\substack{q(n)\geq 0\\ 0\leq\phi(n)\leq 1}} \frac{\sum\limits_{n\in\Omega_1} r_{eav1}(n) + \sum\limits_{n\in\Omega_2} r_{eav2}(n) - R_{eav}^{(0)}}{\sum\limits_{n\in\Omega_1} q(n) + \sum\limits_{n\in\Omega_2} q(n)} \\
& s.t. \sum_{n\in\Omega_1} q(n) + \sum_{n\in\Omega_2} q(n) \leq Q(n) \\
& \quad (15).
\end{aligned} \tag{17}
$$

Next, we start to solve the problem (P2) under different transmission strategies of ST, which are fixed power transmission and adaptive power transmission.

A. FIXED POWER TRANSMISSION

For the fixed power transmission, the transmit power of ST is constant, i.e. $p(n) = p_{cons}$. Then the adjustment of tradeoff between the whole eavesdropping rate and EEE depends entirely on the power allocation of LM.

Since all the suspicious links have got eavesdropped successfully, which means the eavesdropping rate for the suspicious links at Ω_1 achieves the peak and remain constant, we denote the eavesdropping rate of eavesdropping suspicious links at Ω_1 as $\sum_{n\in\Omega_1} r_{eav1}(n)|_{p=p_{cons}} = R_{eav1}$. Besides, the jamming power allocated to eavesdrop the non-eavesdropped suspicious links is also a constant value Q_l. Accordingly, we can transform problem (P2) as

$$
\begin{aligned}
(P2.1): \quad & \max_{\substack{q(n)\geq 0\\ 0\leq\phi(n)\leq 1}} \frac{\sum\limits_{n\in\Omega_2} r_{eav2}(n) + R_{eav1} - R_{eav}^{(0)}}{Q_l + \sum\limits_{n\in\Omega_2} q(n)} \\
& s.t. \sum_{n\in\Omega_2} q(n) + Q_l \leq Q \\
& \quad (15).
\end{aligned} \tag{18}
$$

By introducing an auxiliary variable y_1, the problem (P2.1) can be expressed as follows and can be solved by Lagrangian multiplier method.

$$
\begin{aligned}
(P2.2): \quad & \max_{\substack{q(n)\geq 0\\ 0\leq\phi(n)\leq 1}} \; y_1 \\
& s.t. \; (15) \; and \; (18) \\
& \quad \sum_{n\in\Omega_2} r_{eav2}(n) + R_{eav1} - R_{eav}^{(0)} \\
& \quad - y_1\Big(Q_l + \sum_{n\in\Omega_2} q(n)\Big) \geq 0
\end{aligned} \tag{19}
$$

The Lagrangian function of problem (P2.2) is denoted as

$$
\begin{aligned}
& \mathcal{L}(q(n), \phi(n), y_1, \lambda_1, \mu_1, \{\nu_1(n)\}_{n=1}^{N}) \\
& = y_1 - \lambda_1\Big(\sum\nolimits_{n\in\Omega_2} r_{eav2}(n) + R_{eav1} - R_{eav}^{(0)} \\
& \quad - y_1\big[Q_l + \sum\nolimits_{n\in\Omega_2} q(n)\big]\Big) \\
& \quad + \mu_1(\sum\nolimits_{n\in\Omega_2} q(n) + Q_l - Q) \\
& \quad + \sum\nolimits_{n=1}^{N} \nu_1(n)(\gamma_E(n) - \gamma_D(n))
\end{aligned} \tag{20}
$$

$$\frac{\partial \mathcal{L}}{\partial \phi(n)} = \frac{-\lambda_1\ g_E(n)\sigma^2(n)p_{cons}}{\ln 2[(1-\phi(n))(g_E(n)P+\sigma^2(n))+\sigma^2(n)][(1-\phi(n))\sigma^2(n)+\sigma^2(n)]} - \nu_1(n)\Big(-\sigma^2(n)g(n)+\frac{g_E(n)g_J(n)q(n)\sigma^2(n)(g_E(n)p_{cons}+3\sigma^2(n))}{[(\phi(n)g_E(n)p_{cons}+\sigma^2(n))+\sigma^2(n)]^2}+g_E(n)\sigma^2(n)\Big), \tag{21}$$

$$\frac{\partial \mathcal{L}}{\partial q(n)} = -\nu_1(n)(2\phi(n)-1)\frac{g_E(n)g_J(n)\sigma^2(n)}{\phi(n)(g_E(n)p_{cons}+\sigma^2(n))+\sigma^2(n)} - \lambda_1 y_1 - \mu_1, \tag{22}$$

$$\phi(n) = \frac{(\nu_1(n)g_E(n)g_J(n)-\lambda_1 y_1-\mu_1)\sigma^2(n)}{2\nu_1(n)g_E(n)g_J(n)\sigma^2(n)+(\mu_1-\lambda_1 y_1)(g_E(n)p_{cons}+\sigma^2(n))}, \tag{23}$$

$$q(n) = \frac{\big[(1-\phi(n))(g_E(n)-g(n)\sigma^2(n))-g(n)\sigma^2(n)\big]\big[\phi_1(n)(g_E(n)p_{cons}+\sigma^2(n))+\sigma^2(n)\big]}{g_E(n)g_J(n)[\phi_1(n)(\sigma^2(n)+1)-1]}. \tag{24}$$

where $\lambda_1, \mu_1, \{\nu_1(n)\}_{n=1}^N > 0$ are Lagrange multipliers, then the gradient of $\mathcal{L}(x)$ and the optimal solution $q(n)$ and $\phi(n)$ are gave in (21)-(24), as shown at the top of this page.

B. ADAPTIVE POWER TRANSMISSION

We have studied the eavesdropping scheme of LM when ST transmits with a constant transmit power. In this part, we will focus on a more practical problem that ST will adjust its transmit power of each suspicious link, i.e. increases the transmit power after being assisted by LM and decreases the transmit power after being jammed by LM.

To achieve the highest data rate, the ST applies this adaptive power transmission strategy, which can be denoted as

$$(P3): \max_{q(n)\geq 0} \sum_{n\in\Omega_1} R_{D1}(n) + \sum_{n\in\Omega_2} R_{D2}(n) \quad s.t.\ (2)$$

where $R_{D1}(n) = \log_2(1+\frac{g(n)}{g_J(n)q^*(n)+\sigma^2(n)}p(n)), n \in \Omega_1$ and $R_{D2}(n) = \log_2(1+\frac{(1-\phi(n))g_E(n)}{\sigma^2(n)}p(n)), n \in \Omega_2$. We classify the two formulas into one formulas as $R_D(n) = \log_2(1+\overline{\gamma}(n)p(n))$, since we only focus on optimizing the variable $p(n)$. $\overline{\gamma}(n)$ is the unit SNR of the suspicious link, which denotes as

$$\overline{\gamma}(n) = \begin{cases} \overline{\gamma}_1(n) = \dfrac{g(n)}{g_J(n)q^*(n)+\sigma^2(n)}, & n\in\Omega_1 \\ \overline{\gamma}_2(n) = \dfrac{(1-\phi(n))g_E(n)}{\sigma^2(n)}, & n\in\Omega_2 \end{cases} \tag{25}$$

The problem (P3) can be transformed into a concave optimization as

$$(P3.1): \max_{p(n)\geq 0} \sum_{n\in\Omega_1\bigcup\Omega_2} \log_2(1+\overline{\gamma}(n)p(n)) \quad s.t.\ (2)$$

For solving the problem (P3.1), we employ Lagrangian function with multiplier $\zeta \geq 0$ to solve it as

$$\mathcal{L}(p(1), p(2), \cdots, p(n), \zeta) = \sum_{n\in\Omega_1\bigcup\Omega_2} \log_2(1+\overline{\gamma}(n)p(n)) - \zeta\Big(\sum_{n\in\Omega_1\bigcup\Omega_2} p(n) \leq P\Big) \tag{26}$$

Thus, we get the optimal transmit power of ST by setting $\partial\mathcal{L}/\partial p(n) = 0$ as

$$\hat{p}(n) = \frac{1}{\zeta\ln 2} - \frac{1}{\overline{\gamma}(n)} = \begin{cases} \frac{1}{\zeta\ln 2} - \dfrac{1}{\overline{\gamma}_1(n)}, & n\in\Omega_1 \\ \frac{1}{\zeta\ln 2} - \dfrac{1}{\overline{\gamma}_2(n)}, & n\in\Omega_2 \end{cases} \tag{27}$$

where $\upsilon = \frac{1}{\zeta\ln 2}$ is the water level, which is associated with the power constraint $\sum_{n\in\Omega_1\bigcup\Omega_2} p(n) = P$ at ST, so that we can get the water level υ as

$$\upsilon = \frac{P + \sum\limits_{n\in\Omega_1} \log_2 \frac{1}{\gamma_1(n)} + \sum\limits_{n\in\Omega_2} \log_2 \frac{1}{\gamma_2(n)}}{N} \tag{28}$$

Accordingly, the optimal transmit power can be transformed as

$$\hat{p}(n) = \begin{cases} \hat{p}_1(n) = \dfrac{P + \sum\limits_{n\in\Omega_1} \frac{g_J(n)q^*+\sigma^2(n)}{g(n)} + \sum\limits_{n\in\Omega_2} \frac{\sigma^2(n)}{(1-\phi(n))g_E(n)}}{N} - \dfrac{g_J(n)q^*(n)\ +\ \sigma^2(n)}{g(n)}, & n\in\Omega_1 \\ \hat{p}_2(n) = \dfrac{P + \sum\limits_{n\in\Omega_1} \frac{g_J(n)q^*+\sigma^2(n)}{g(n)} + \sum\limits_{n\in\Omega_2} \frac{\sigma^2(n)}{(1-\phi(n))g_E(n)}}{N} - \dfrac{\sigma^2(n)}{(1-\phi(n))g_E(n)}, & n\in\Omega_2 \end{cases} \tag{29}$$

The adaptive power transmission of ST will influence the power policy of LM. Different from the fixed power transmission, adaptive power transmission promotes the power allocation of LM becomes a more complex problem, which we will study below.

Same as the solution for fixed power transmission, we still solve the problem at two cases according to the power constraint Q of LM.

When $Q \geq Q_l$, in this case, all the suspicious links get eavesdropped successfully. The EEE of LM is

$$\eta(q(n), \phi(n)) = \frac{\varphi(q(n), \phi(n)) - R_{eav}^{(0)}}{\sum\limits_{n\in\Omega_1\bigcup\Omega_2} q(n)} \tag{30}$$

where $\varphi(q(n), \phi(n)) = \sum_{n\in\Omega_1} \log_2(\upsilon\overline{\gamma}_1(n)) + \sum_{n\in\Omega_2} \log_2(\upsilon\overline{\gamma}_2(n))$, accordingly, we transform the problem (P1) as

$$(P4): \quad \max_{\substack{q(n)\geq 0\\ 0\leq\phi(n)\leq 1}} \quad \eta(q(n), \phi(n))$$
$$s.t.\ (1)\ and\ (15).$$

To solve the above fractional programming, we introduce an auxiliary variable y_2, the problem (P4) is equivalently as

$$(P4.1): \quad \max_{\substack{q(n)\geq 0\\ 0\leq\phi(n)\leq 1}} \quad y_2$$
$$s.t.\ \varphi(q(n), \phi(n)) - y_2 \sum_{n\in\Omega_2} q(n) \geq 0$$
$$(1)\ and\ (15)$$

We employ Lagrange multipliers $\lambda_2, \mu_2, \{\nu_2(n)\}_{n=1}^{N} > 0$ to solve the concave optimization problem (P4.1), the Lagrange function is

$$\begin{aligned}&\mathcal{L}(q(n), \phi(n), y_2, \lambda_2, \mu_2, \{\nu_2(n)\}_{n=1}^{N})\\ &= y_2 - \lambda_2\Big(\varphi(q(n), \phi(n)) - y_2 \sum_{n\in\Omega_2} q(n)\Big)\\ &\quad + \mu_2\Big(\sum_{n\in\Omega_1\cup\Omega_2} q(n) - Q\Big)\\ &\quad + \sum\nolimits_{n=1}^{N} \nu_2(n)(\gamma_E(n) - \gamma_D(n)) \qquad (31)\end{aligned}$$

the solution are gave in (32)-(34), as shown at the bottom of this page.

IV. THE SOLUTION OF LEGITIMATE MONITOR WITHOUT ENOUGH POWER

As we have introduced in section II, In this section, we study the infeasible case of the problem (P1). When $Q < Q_l$, there is not enough power for LM to guarantee constraint (15), which means LM cannot guarantee to eavesdrop all the non-eavesdropped suspicious links. However, it is a practical problem we must solve: how to allocate the limited power of LM to guarantee a highest eavesdropped ratio with a higher EEE. So it is significant to develop a scheme, which decides the non-eavesdropped suspicious links get eavesdropped first efficiently.

A. FIXED POWER TRANSMISSION

For the case that transmit power of ST is fixed as we analyzed above, we proposed a heuristic algorithm to solve the infeasible case of problem (P1).

Since we differentiate suspicious links as non-eavesdropped suspicious links and eavesdropped links. We can also divide the EEE into two parts, which are jamming energy efficiency (JEE) η_J and relay energy efficiency (REE) η_R as follows

$$\eta_J = \frac{\sum_{n\in\Omega_1} \alpha(n) r_{eav1}(n)}{\sum_{n\in\Omega_1} \alpha(n) q(n)} \qquad (35)$$

$$\eta_R = \frac{\sum_{n\in\Omega_2} r_{eav2}(n) - R_{eav}^{(0)}}{\sum_{n\in\Omega_2} q(n)} \qquad (36)$$

We first maximize these two energy efficiencies respectively, and then decide the power allocation of LM by heuristic algorithm to make a trade-off between whole eavesdropping rate, successfully eavesdropping ratio and EEE.

For JEE, LM takes a strategy to eavesdrop the non-eavesdropped suspicious, which guarantees to eavesdrop as many non-eavesdropped suspicious links as possible and obtain the highest JEE simultaneously. As we have already analyzed in theorem 2.1, the jamming power requested by each non-eavesdropped suspicious links to get eavesdropped is fixed as $q^*(n), n \in \Omega_1$, we denote the JEE of a single suspicious link n as

$$\eta_j(n) = \frac{r_{eav1}(n)}{q(n)}, \quad n \in \Omega_1 \qquad (37)$$

With the JEE of each suspicious link at Ω_1, we can sort them from highest to the lowest and constitute a task table for LM.

For the REE of eavesdropped suspicious links at Ω_2, we can easily employ Lagrange multipliers method to obtain the optimal power $q(n)$ and $\phi(n)$ like (P2.1).

$$\begin{aligned}\frac{\partial\mathcal{L}}{\partial\phi(n)} &= \frac{-\lambda_2\, g_E(n)\hat{p}_2(n)\sigma^2(n) + (\sigma^2(n) + \sigma^2(n)/(1-\phi(n)))(1/N-1)\sigma^2(n)}{\ln 2[(1-\phi(n))(g_E(n)\hat{p}_2(n) + \sigma^2(n)) + \sigma^2(n)][(1-\phi(n))\sigma^2(n) + \sigma^2(n)]}\\ &\quad - \nu_1(n)\Big(-\sigma^2(n)g(n) + \frac{g_E(n)g_J(n)q(n)\sigma^2(n)(g_E(n)\hat{p}_2(n) + 3\sigma^2(n))}{[\phi(n)(g_E(n)\hat{p}_2(n) + \sigma^2(n)) + \sigma^2(n)]^2} + g_E(n)\sigma^2(n)\Big), \qquad (32)\end{aligned}$$

$$\frac{\partial\mathcal{L}}{\partial q(n)} = -\nu_2(n)(2\phi(n)-1)\frac{g_E(n)g_J(n)\sigma^2(n)}{\phi(n)(g_E(n)\hat{p}_2(n) + \sigma^2(n)) + \sigma^2(n)} - \lambda_2 y_2 - \mu_2, \qquad (33)$$

$$q(n) = \frac{\big[(1-\phi(n))(g_E(n) - g(n)\sigma^2(n)) - g(n)\sigma^2(n)\big]\big[\phi(n)(g_E(n)\hat{p}_2(n) + \sigma^2(n)) + \sigma^2(n)\big]}{g_E(n)g_J(n)(\phi(n)(\sigma^2(n)+1) - 1)}. \qquad (34)$$

After solving the two sub-problems of optimizing JEE and REE, we back to analyze the heuristic algorithm of the infeasible case of the primal problem (P1). For the influence of constraint (15), the most important task of LM is successfully eavesdropping suspicious links, we focus on contributing to eavesdrop as many suspicious links as possible and maintain the highest EEE as well under this circumstance. The heuristic algorithm is described at algorithm 1.

Algorithm 1 Heuristic Algorithm for LM When $Q < Q_l$

```
Set $L = \{1, 2, \dots, N\}$,$n = 1$ to $N$.
for all $n = 1$ to $N$ do
    if $\gamma_E(n) < \gamma_D(n)$ then
        $n \in \Omega_1$
    else
        $n \in \Omega_2$
    end if
end for
resort $\Omega_1$ in descending order of $\eta_j(n)$
for all $n$ in $\Omega_1$ do
    if $Q \geq q^*(n)$ then
        update $Q = Q - q^*(n)$
        eavesdrop nth suspicious link
        $n = n + 1$
    else
        Break
    end if
end for
for all $n$ in $\Omega_2$ do
    Update $R_D(n)$ with $q(n)$ and $\phi(n)$ via (23) and (24)
end for
return result
```

B. ADAPTIVE POWER TRANSMISSION

The power allocation scheme of ST has been studied at section III, we have already got the optimal transmit power $\hat{p}(n)$. The transmit power is influenced by the jamming power $q(n)$. As we have studied above, for the case that the problem (P1) is infeasible in this case when $Q < Q_l$, LM cannot eavesdrop all the suspicious links, LM will take the strategy that eavesdrops as many suspicious links as possible and try to reach a higher EEE simultaneously. Accordingly, the LM will utilize all the limited power Q to jam the non-eavesdropped suspicious links at Ω_1. Thus we can denote the problem as follows

$$(P5): \max_{q(n)\geq 0} \frac{R^{(ad)} - R^{(0)}_{eav}}{Q}$$

$$s.t. \sum_{n\in\Omega_1} \alpha(n)q(n) \leq Q(n) \tag{38}$$

$$\alpha(n) \in \{0, 1\} \tag{39}$$

where $\alpha(n)q(n)$ is the jamming power that LM jams the nth suspicious link, $R^{(ad)} = \sum_{n\in\Omega_1} \alpha(n)\log_2 \left(1 + \frac{g_E(n)\hat{p}_1(n)}{\sigma_s^2(n)+\sigma^2(n)}\right) + \sum_{n\in\Omega_2} \log_2\left(1 + \frac{g(n)\hat{p}_1(n)}{\sigma^2(n)}\right)$ is the eavesdropping rate after the power allocation scheme.

The problem (P5) is a MINLP problem, we redefine $\alpha(n) \in [0, 1]$. Then the objective function is jointly convex in $\{\alpha(n), q(n)\}'s$, we can solve it by employing Lagrange multiplies $\lambda_3, \mu_3(n), \{\nu_3(n)\}_{n=1}^N > 0$. The Lagrange function is

$$\mathcal{L}(q(n), \alpha(n), \lambda_3, \{\nu_3(n)\}_{n=1}^N) = \left(R^{(ad)}R^{(0)}_{eav}\right)/Q + \lambda_3\left(\sum_{n\in\Omega_1} \alpha(n)q(n) - Q\right) + \sum_{n=1}^N \nu_3(n)(\alpha(n) - 1) \tag{40}$$

Thus we can obtain the optimal solution is

$$\alpha(n) = \left(1 - \frac{1}{N}\right)\frac{g_J(n)}{Q\ln 2 g(n)(1+\lambda_3)}\left(\frac{g(n)}{g(n)\hat{p}_1(n) + \sigma^2(n)} + \frac{g_E(n)}{g_E(n)\hat{p}_1(n) + \sigma^2(n)}\right), \tag{41}$$

$$q(n) = \alpha(n)q^*(n). \tag{42}$$

V. NUMERICAL RESULTS

The performance of our proposed eavesdropping scheme is evaluated by a series of numerical experiments. Consider a multiple suspicious links communication system, where the number of suspicious links is $N = 50$ unless otherwise stated. In addition, the channel coefficients of ST to SR $h(n)$, ST to LM $h_E(n)$ and LM to SR $h_J(n)$ are independent circularly symmetric complex Gaussian (CSCG) random variables with mean value 0.5. Meanwhile, we set the fixed transmit power at ST of each suspicious link to be $p(n) = 20dB$. For the fairness of results, we set the transmit power constraint of ST as $P = 37dB$ for both two transmission strategies of ST. Here, the transmit power are normalized over the receiver noise power such that we can set the noise power to be $\sigma^2 = 1$.

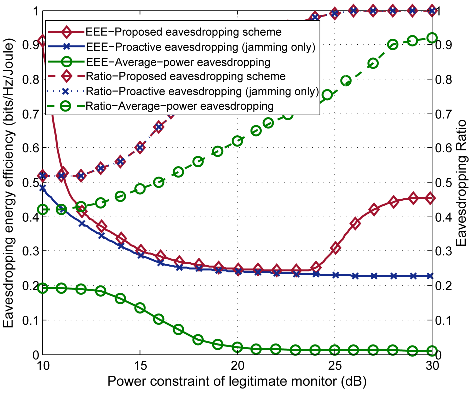


FIGURE 2. Eavesdropping energy efficiency and eavesdropping ratio versus the power constraint of legitimate monitor.

Fig. 2 shows the EEE η and eavesdropping ratio of three eavesdropping scheme versus the power constraint Q of LM, which are our proposed eavesdropping scheme, proactive jamming scheme (LM only interferes the non-eavesdropped suspicious links for eavesdropping) and average power eavesdropping scheme (LM allocates the energy to interfere or assist each of the suspicious links equally). We can observe that EEE η of LM will decrease through eavesdropping more non-eavesdropped suspicious links when Q is not enough, i.e. $Q \leq 20dB$. When all the non-eavesdropped suspicious links are eavesdropped, which means the eavesdropping ratio is 1, the EEE will increase with the rise of Q in the eavesdropping scheme we proposed. This is the advantage of assisting the eavesdropped suspicious links. Our proposed eavesdropping scheme can achieve much higher EEE than proactive jamming scheme and average-power eavesdropping scheme. Furthermore, our proposed eavesdropping scheme owns the same eavesdropping ratio as proactive jamming scheme and has higher EEE. The observation shows that our proposed scheme can not only guarantee a high eavesdropping ratio by jamming the suspicious links but also further increase the eavesdropping rate by assisting the suspicious links.

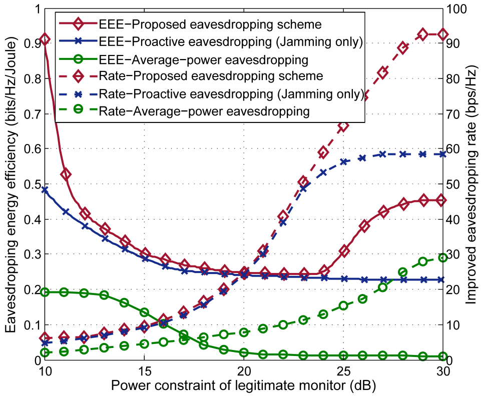


FIGURE 3. Eavesdropping energy efficiency and improved eavesdropping rate versus the power constraint of legitimate monitor.

Next, Fig. 3 shows the EEE η and the improved eavesdropping rate versus the power constraint Q of legitimate monitor. We can observe that compared with proactive jamming scheme and average-power eavesdropping scheme, LM can not only obtain the highest improvement of eavesdropping rate but also have the highest EEE by utilizing our proposed eavesdropping scheme. Moreover, the power constraint of legitimate monitor is low, the improvement of our proposed scheme on eavesdropping rate is little compared to proactive jamming, since the vast majority of energy is utilized to jam for eavesdropping non-eavesdropped suspicious links, only litter energy is allocated to assiat eavesdropped suspicious links. This is designed for achieving higher eavesdropping ratio.

According to theorem 2.1, we can obtain the power threshold Q_l of LM. When $Q > Q_l$, which means LM has enough power to eavesdrop all the suspicious links, Fig.4 shows EEE of LM with $N = 40$ and $N = 60$ when ST employs fixed power transmission and adaptive power transmission. Our proposed eavesdropping scheme can improve EEE of LM by parlaying the adaptive power transmission of ST, since the assistance to eavesdropped suspicious link from LM will lead to the rise of adaptive transmission power $p(n)$, which can lead to a higher eavesdropping rate and EEE of LM. We can also see that the improvement of EEE is higher when there exists more suspicious links, which means more eavesdropped suspicious links.

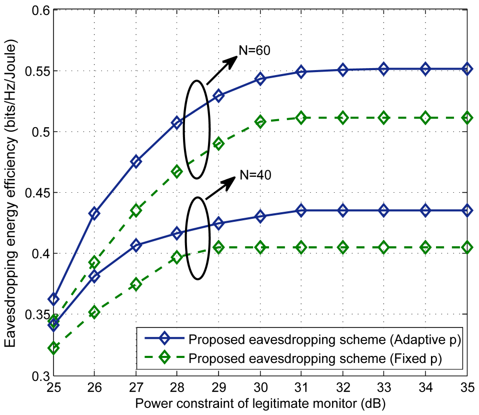


FIGURE 4. Eavesdropping energy efficiency of Legitimate monitor under fixed power transmission and adaptive power transmission with $N = 40$ and $N = 60$, $Q > Q_l$.

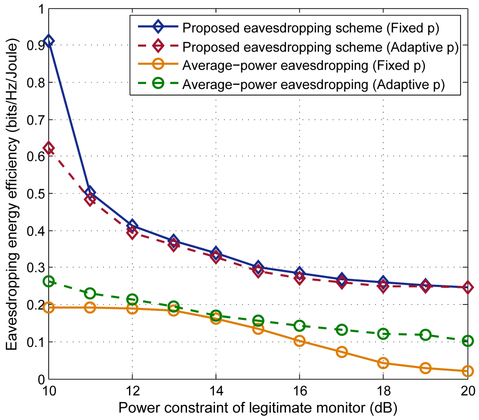


FIGURE 5. Eavesdropping energy efficiency of Legitimate monitor under fixed power transmission and adaptive power transmission in our proposed eavesdropping scheme and average-power eavesdropping scheme. $Q < Q_l$.

Finally, Fig.5 shows EEE of LM with insufficient power in our proposed eavesdropping scheme and average-power eavesdropping scheme when ST employs fixed power transmission and adaptive power transmission. We can see that when $Q < Q_l$, which means LM cannot eavesdrop all the suspicious links, the adaptive power transmission of ST will influence EEE of LM, since jamming a suspicious link will lead to a decrease of the transmit power $p(n)$, which directly causes the decrease of eavesdropping rate and EEE. We can observe that our proposed eavesdropping scheme can handle the above concern and the gap of EEE between the two transmission method is closing with the increase of Q.

VI. CONCLUSION

In this paper, we study EEE of multiple suspicious links communication system, which is a novel objective. We consider there exists eavesdropped and non-eavesdropped suspicious links in the eavesdropping range of LM. The main task of our work is to maximize EEE of LM and maintain a high eavesdropping ratio and eavesdropping rate which is covered in the constraints of our model. The finite power of LM is used for jamming the non-eavesdropped suspicious to eavesdrop it successfully and relaying for the eavesdropped suspicious links to improve EEE. In addition, we consider the fixed power transmission and adaptive power transmission of ST for practicality. We propose eavesdropping schemes for both two transmission methods of ST. The optimization problem we proposed is a MINLP problem, which is intractable. We solve the problem by utilizing the theorem of proactive eavesdropping and simplify it to a fractional programming problem by analyzing the energy constraint of LM. Then we utilize Lagrange method to solve it, since we can transform the problem to a concave optimization problem by introducing an auxiliary variable. Numerical results show that our proposed eavesdropping schemes can achieve higher EEE and eavesdropping rate versus proactive jamming scheme and average-power eavesdropping. Furthermore, our proposed schemes are trade-offs between EEE, eavesdropping rate and eavesdropping ratio.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[2] H.-M. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[3] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 764–774, Feb. 2017.

[4] Y. Bi and H. Chen, "Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1538–1550, Dec. 2016.

[5] G. Han, L. Zhou, H. Wang, and S. Chan, "A source location protection protocol based on dynamic routing in WSNs for the social Internet of Things," *Future Gener. Comput. Syst.*, vol. 82, no. 5, pp. 689–697, 2018.

[6] G. Han, L. Liu, W. Zhang, and S. Chan, "A hierarchical jammed-area mapping service for ubiquitous communication in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 92–98, Jan. 2018.

[7] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 80–83, Feb. 2016.

[8] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2790–2806, May 2017.

[9] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 152–159, Aug. 2017.

[10] H. Tran and H.-J. Zepernick, "Proactive attack: A strategy for legitimate eavesdropping," in *Proc. IEEE ICCE*, Jul. 2016, pp. 457–461.

[11] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1449–1461, Dec. 2016.

[12] J. Xu, L. Duan, and R. Zhang, "Fundamental rate limits of physical layer spoofing," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 154–157, Apr. 2017.

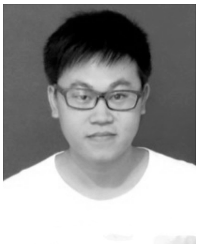
[13] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: design and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4585–4599, Jul. 2017.

[14] H. Cai, Q. Zhang, Q. Li, and J. Qin, "Proactive monitoring via jamming for rate maximization over MIMO Rayleigh fading channels," *IEEE Commun. Lett.*, vol. 21, no. 9, pp. 917–921, Sep. 2017.

[15] X. Jiang, H. Lin, C. Zhong, X. Chen, and Z. Zhang, "Proactive eavesdropping in Relaying systems," *IEEE Signal Process. Lett.*, vol. 24, no. 6, pp. 917–921, Jun. 2017.

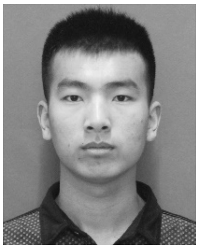
[16] G. Ma, J. Xu, L. Duan, and R. Zhang. (2017). "Wireless surveillance of two-hop communications." [Online]. Available: https://arxiv.org/abs/1704.07629

BAOGANG LI received the B.Eng. degree from North China Electric Power University, China, in 2006, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2012. From 2016 to 2017, he visited the Centre for IoT and Telecommunications, The University of Sydney, as a Visiting Scholar. He is currently an Associate Professor with the School of Electrical and Electronic Engineering, North China Electric Power University. His research interests include wireless resource management, optimization technology, energy harvesting technology, energy efficiency of wireless communications, and smart grid.



YUANBIN YAO received the B.Eng. degree in electronics and communication engineering from North China Electric Power University, Baoding, China, in 2016, where he is currently pursuing the M.S. degree in communication and information engineering. His research interests include wireless security, wireless resource management, optimization technology, and energy efficiency of wireless communications.

HAIJUN ZHANG (M'13–SM'17) was a Post-Doctoral Research Fellow with the Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver Campus, Canada. He is currently a Full Professor with the University of Science and Technology Beijing, China. He received the IEEE ComSoc Young Author Best Paper Award in 2017 and the IEEE ComSoc CSIM Technical Committee Best Journal Paper Award in 2018. He serves/served as the General Co-Chair of GameNets'16, the Symposium Chair of Globecom'19, the TPC Co-Chair of the INFOCOM'18 Workshop IECCO, the General Co-Chair of the ICC'18/ICC'17/Globecom'17 Workshop on UDN, and the General Co-Chair of the Globecom'17 Workshop on LTE-U. He serves as an Editor for the IEEE Transactions on Communications and the IEEE 5G Tech Focus. He serves/served as a Leading Guest Editor for the *IEEE Communications Magazine* and the IEEE Transactions on Emerging Topics in Computing.



YABO LV received the B.Eng. degree from the Agricultural University of Hebei, China, in 2016. He is currently pursuing the M.S. degree in communication and information engineering with North China Electric Power University, China. His research interests include deep reinforcement learning, energy harvesting, and wireless resource management.

WEI ZHAO received the B.Eng. degree from North China Electric Power University, China, in 2008, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2011. In 2011, he joined the School of Electrical and Electronic Engineering, North China Electric Power University. From 2016 to 2017, he visited the King's College London, U.K., as a Visiting Scholar. His research interests include wireless security, massive MIMO, NOMA, and energy efficiency of wireless communications.