Robust Relay in Narrow-Band Communications for Ubiquitous IoT Access

Qinghe Du,1,2 Nan Lu,1,2 Li Sun,1,2 Xuelin Zhang,3 and Bo Sun3

1Department of Information & Communications Engineering, Xi’an Jiaotong University, Xi’an, China
2Shaanxi Smart Networks and Ubiquitous Access Research Center, Shaanxi, China
3ZTE Corporation, Xi’an, China

Correspondence should be addressed to Qinghe Du; duqinghe.xjtu@gmail.com

Received 13 January 2017; Revised 3 April 2017; Accepted 6 April 2017; Published 27 April 2017

Academic Editor: Fanli Meng

Copyright © 2017 Qinghe Du et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We propose a robust wireless relay scheme in narrow-band communications for IoT access, which matches the typical features of IoT often carrying relatively low data rate with limited bandwidth. This framework is towards offering robustness in QoS guarantees with emphases on security and/or reliability, and we use the security-assured network as the typical scenario. In particular, we consider a dual-hop relay network including a transmitter, a receiver, an amplify-and-forward (AF) untrusted relay, and a jamming node. The jamming node is treated as a helper. Specifically, the jammer broadcasts artificial noise (AN), which in fact pollutes both the untrusted relay and the destination node’s signals. However, we show that such AN can be effectively mitigated after the destination node obtains the forwarded signal from the relay, while the untrusted relay node cannot do so. The core idea for robustness assurance is to exploit higher signal dimensions at the receiver over the untrusted relay node. Simulations and analyses are also conducted to demonstrate that our proposed scheme can make the performance at the untrusted relay an interference-limited manner while completely removing the interferences at the receiver, therefore corroborating our claim in robustness in terms of security and reliability.

1. Introduction

In the Internet of Things (IoT) vision, every physical object plays the role in both providing and consuming diverse service resources, making the wireless networks efficiently connected yet highly heterogeneous [1]. In a typical wireless access framework for IoT, heterogeneous wireless networks often coexist, especially when the mobile communications evolve to the 5th generation (5G) era. In 5G network, diverse networks, such as macro/small cellular networks [2, 3], vehicular and transportation networks [4, 5], cognitive radio networks [6, 7], and device-to-device networks [8–10], all need to be effectively integrated to implement seamless communications in future wireless networks. Such an interconnection will bring unprecedented convenience for users as well as economical opportunities for market, but it will also require robust and sophisticated approaches to ensure quality of service (QoS) requirements for services, especially on the security and reliability. On the one hand, the physical accessibility to the large amount of objects and the openness of wireless channels make security assurance for IoT much more challenging than the traditional network. Consequently, a great deal of research efforts have been dedicated to the security of IoT, which cover all protocol layers [11–15]. Among diverse security techniques, physical-layer security (PLS), which can take advantage of wireless channels’ features to protect secrecy, has become a research hotspot [16–20]. On the other hand, cooperative communications have been widely recognized as a key component to increase the capacity and enhance the reliability for wireless communication systems [21–23]. Thus, security and reliability enhancement via physical-layer technologies over cooperative networks have attracted special interests [10, 18–20, 23–29] in the research community.

While diverse techniques have been developed for security and reliability enhancement [10, 18–20, 23–29], applying these existing techniques for IoT access still faces the major challenge. Because IoT access often involves low-cost nodes
with limited wireless-connecting capability, too much information exchange and too complicated cooperation protocols are hard to implement. This issue imposes the urgent needs on robust and lightweight approaches in cooperative IoT access scenarios with QoS provisioning on reliability as well as security.

To address this problem, we propose a simple yet robust wireless relay scheme with a coexisting jamming node for the narrow-band communications scenario. The narrow-band communications well fit the features of IoT. As IoT communications typically deal with services having relatively low traffic load, narrower bandwidths are often assigned to users so that more simultaneous accesses can be accommodated. Furthermore, unlike the wide-band communications, the narrow-band assignment is immune to the frequency-selective fading, thus benefiting the implementation of low-cost equipment with low processing complexity. In our framework, there are four nodes in the network where the source can potentially utilize an amplify-and-forward (AF) relay to augment the direct link to the destination. In the meantime, there is another node who broadcasts jamming signals (can be also characterized as interfering signals) and actually degrades the quality of the relay’s and destination’s channels. Because the destination is able to obtain high signal dimensions from both direct link and relay transmissions, the jamming signals can be well suppressed.

Our proposed relay scheme with coexisting interferences can be applied in the following two typical cases towards the robustness of security and reliability provisioning, respectively, for IoT access. (1) Security assurance: the transmitted messages need to be kept confidential to the relay that is also termed untrusted relay [23–27], even though it fulfils the source’s request by forwarding signals to the destination. The node who broadcasts jamming signals, often modeled by artificial noise (AN), can be seen as a friendly but noncooperative jammer. The friendliness comes from the fact that the jamming signals prevent the untrusted relay from decoding the confidential data. The noncooperation implies that jamming strategy does not vary with the channel state information (CSI). We further assume that the CSI of the network, thus making the protocol simpler and more practical.

(2) Interference suppression: for this case, the node broadcasting interfering signals play the role of transmitter of a coexisting link within the same radio band. The destination node can exploit signal dimensions obtained from both direct link and relay link to remove the interference, such that the system is not interference-limited and can successfully fulfill the reliability requirements. In this sense, our scheme is capable of offering robustness in terms of both reliability and security assurance. For convenience, in this paper we use security assurance as the typical framework to present our design.

The rest of this paper is organized as follows. Section 2 describes the system model for our framework towards robust IoT access, with security assurance as the typical scenario. Section 3 studies three detection approaches for our robust relay framework. Section 4 analyzes the upper and/or lower bounds of ergodic secrecy throughput (EST) under diverse detection approaches. In Section 5, we show some simulation results and meaningful discussions. The paper concludes with Section 6.

Some notations used in this paper are summarized as follows. Bold uppercase and bold lowercase letters denote matrices and vectors, respectively. Transpose operation, conjugate transpose, and inverse operation for matrices are denoted by $(\cdot)^\top$, $(\cdot)^\dagger$, and $(\cdot)^{-1}$, respectively. $A_{mn}$ is the element $(m, n)$ of matrix $A$, $a_n$ is the $n$th element in vector $a$, and $\hat{a}$ is the estimation of $a$. $I_n$ is the identity matrix of order $n$ and $\mathbf{0}$ is the zero matrix. The subscript on $I_n$ is neglected when the size is obvious from the context. The notation $\cdot \mid \cdot$ represents Euclidean norm. $\log(\cdot)$ is logarithm of base $e$. $E(\cdot)$ is the expectation operator. $\text{Var}\{\cdot\}$ denotes the variance of a random variable, and $[x]^+ = \max(0, x)$.

2. System Model

A two-hop wireless relay network is considered in this paper, as depicted in Figure 1(a), where there are four nodes in the network, including one source ($A$), one relay ($B$), one destination ($C$), and one jammer ($D$). Each node has only a single transmit antenna and a single receive antenna and operates in the half-duplex fashion. There exists the direct link between the source and destination. In the meantime, the relay node uses the amplify-and-forward (AF) mechanism to assist the source to deliver the data to the destination. The transmit power of each node is set equal to $P$.

As aforementioned, we concentrate on narrow-band communications, and thus wireless channels can be modeled as flat-fading channels. The channel between node $i$ and node $j$ is characterized by a multiplicative coefficient $h_{ij}$, which is a zero-mean circularly symmetric complex Gaussian random variable. Note that for $h_{ij}$, the subscripts $i$ and $j$ could be $A$, $B$, $C$, and $D$, representing different nodes, but $i$ and $j$ cannot be the same node simultaneously. All channel coefficients remain constant within one time frame with a fixed length but vary independently from one frame to another. The additive thermal noise at each receiver is characterized by a zero-mean complex Gaussian random variable with variance $\sigma^2$. Throughout this paper, we define $\gamma_{ij} = P|h_{ij}|^2/\sigma^2$ as channel state information (CSI). We further assume that the CSI of all links illustrated in Figure 1(a) can be accurately estimated and are known to the destination node $C$. This assumption is rational as all four users are neighbours to each other within one network. They can periodically exchange CSI to maintain connections to each other and thus all channel coefficients are known to node $C$. The accuracy of channels can be obtained by applying sophisticated and advanced estimation algorithms such as [30, 31]. However, it is worth noting that, in practical systems, the CSI and the corresponding rate adaptation are usually quantified to simplify implementation. Also, the exchange of CSI often introduces considerable overhead. Therefore, in practical systems, the actual performance will tradeoff with the resolution of system adaptation as well as the amount of introduced overhead.

The relay procedures are illustrated in Figure 1(b) and the physical-layer signal model is described as follows. Each time frame is divided equally into two phases. During the first phase, node $A$ transmits signal $x$ with power $P$. In the meantime, node $D$ functioning as a noncooperative jammer broadcasts the artificial noise (AN) denoted by $n_D$, which is
the zero-mean complex Gaussian white noise with variance $P$. Evidently, the artificial noise will disturb both the relay node $B$ and the destination node $C$. The signals received by node $B$ and node $C$ in the first phase are denoted by $y_{1B}$ and $y_{1C}$, respectively, which can be written by

$$y_{1B} = \sqrt{P|h_{AB}|^2}x + \sqrt{P|h_{DB}|^2}n_D + n_{1B}, \quad (1)$$

$$y_{1C} = \sqrt{P|h_{AC}|^2}x + \sqrt{P|h_{DC}|^2}n_D + n_{1C} \quad (2a)$$

$$= \sqrt{P|h_{AC}|^2}x + n', \quad (2b)$$

where $n_{1B}, n_{1C} \sim \mathcal{CN}(0, \sigma^2), n_D \sim \mathcal{CN}(0, 1), n' \sim \sqrt{P|h_{DC}|^2}n_D + n_{1C}$ and thus $n' \sim \mathcal{CN}(0, P|h_{DC}|^2 + \sigma^2)$. Here $\mathcal{CN}(\cdot, \cdot)$ denotes the circularly symmetric complex Gaussian random variable, where the first parameter denotes the mean and the second is the variance.

In the second phase, node $B$ amplifies and forwards the received signal. Meanwhile, it attempts to decode the received signal to retrieve the confidential information. Therefore, node $B$ is actually an untrusted relay node. For security requirements, the task of our design is to prevent $B$ from successfully decoding while enhancing the destination node $C$’s QoS, such as secrecy, throughput, and bit error rate (BER). The signal received by node $C$ in the second phase is given by

$$y_{2C} = \beta h_{BC} y_{1B} + n_{2C}, \quad (3)$$

where $\beta \equiv \sqrt{|P|h_{AB}|^2 + P|h_{DB}|^2 + \sigma^2}$ is to normalize the transmit power to $P$. For convenience, we define $\tilde{\beta} \equiv P|h_{AB}|^2 + P|h_{DB}|^2 + \sigma^2$. By substituting $\beta$ and (1) into (3), we have

$$y_{2C} = \frac{P h_{AB} h_{BC}}{\sqrt{\tilde{\beta}}} x + \frac{P h_{DB} h_{BC}}{\sqrt{\tilde{\beta}}} n_D + \frac{\sqrt{P} h_{DC} n_{1B} + n_{2C}}{\sqrt{\tilde{\beta}}} \quad (4a)$$

$$= \frac{P h_{AB} h_{BC}}{\sqrt{\tilde{\beta}}} x + \sqrt{\tilde{\beta}} n_D + n'' \quad (4b)$$

$$= \frac{P h_{AB} h_{BC}}{\sqrt{\tilde{\beta}}} x + n'' \quad (4c)$$

From the above equations, we can readily obtain $n'' \sim \mathcal{CN}(0, (P|h_{BC}|^2/\tilde{\beta} + 1)\sigma^2)$ and $n'' \sim \mathcal{CN}(0, P|h_{DB}|^2|h_{BC}|^2/\tilde{\beta} + (P_B|h_{BC}|^2/\tilde{\beta} + 1)\sigma^2)$.

We assume that node $D$ remains idle in the second phase, and thus the received signal $y_{2C}$ is not polluted by the artificial noise. As aforementioned, our framework can be applied to the cases for security and reliability assurance. For the security assurance case, node $D$ plays a role of helper but with limited cooperation. This is because the artificial noise can disturb the untrusted relay $B$, such that it cannot successfully decode the data. The limited cooperation comes from the fact the artificial noise does not adapt with the CSI of any links. In the reliability assurance case, node $D$ can be treated as the transmitter of another existing link within the same bandwidth. Correspondingly, our target would be how to suppress the interference at the destination by combining the signals received in the two phases. As the two cases share the same model, we in this paper mainly use the security assurance case as the typical case to study and analyze our design.

3. Detection Schemes at the Destination Node

The core idea for security assurance is to exploit higher signal dimensions at the legitimate destination user, that is, node $C$, over the untrusted relay $B$. Specifically, we can see from (2b) and (4c) that the destination node $D$ can receive two versions of the signals with independent channel fading in two phases. In contrast, the untrusted relay node $B$ has only the signals received in the first phase. This promises that $C$ is able to suppress the interferences, that is, the artificial noise broadcast by $D$ in the first phase, but $B$ cannot do so.
Where procedures. By combining (4b) with (2a), we arrive at

detailed ZF detection for our case is derived by the following

known for complete elimination of the interferences. The

3.1. Zero Forcing (ZF) Detection. Zero forcing detector is

known for complete elimination of the interferences. The
detailed ZF detection for our case is derived by the following

procedures. By combining (4b) with (2a), we arrive at

\[ y'_{IC} = \sqrt{p_{AC}} x + \sqrt{p_{DC}} n_D + n_{IC} \]
\[ y'_{SC} = \frac{1}{\sqrt{\beta}} p_{AB} b_{BC} x + \frac{1}{\sqrt{\beta}} p_{DB} h_{BC} n_D + n'' \].

Rewriting (5) in a matrix form, we get

\[ y = \sqrt{\beta} R b + n \]

where \( y = (y_{IC}, y_{SC})^T \), \( b = (x, n_D)^T \), \( n = (n_{IC}, n'')^T \), and \( R \) is
denoted by

\[ R = \begin{bmatrix} h_{AC} & h_{DC} \\ \frac{1}{\sqrt{\beta}} p_{AB} h_{BC} & \frac{1}{\sqrt{\beta}} p_{DB} h_{BC} \end{bmatrix} \].

In this section, we apply ZF detector at node C to suppress
the interference. Node C will judge transmitted signal \( x \)
based on the result of received signal vector \( y \) multiplied
with the matrix \( L_{ZF} \), where \( L_{ZF} = R^{-1} \) according to the zero

forcing criterion. The estimation of transmitted signal \( \hat{x} \) is
determined by

\[ \hat{x} = \arg \min_x \{ \|(L_{ZF} y)_1 - \hat{x}\|^2 \}. \]

After using (6), we have

\[ L_{ZF} y = \sqrt{\beta} b + R^{-1} n \].

According to the principal of ZF detector which aims to
eliminate the interference in \( b \), we reach the conclusion that

\( (L_{ZF} y)_1 \) is the sufficient statistics of the transmitted signal \( x \).

\( (L_{ZF} y)_1 \) can be written as

\[ (L_{ZF} y)_1 = \sqrt{\beta} x + \frac{R_{22} n_{IC} - R_{12} n''}{R_{11} R_{22} - R_{12} R_{21}} = \sqrt{\beta} x + \bar{n}, \]

where

\[ \bar{n} \sim CN \left( 0, \frac{R_{22} \text{Var} \{n_{IC}\} - R_{12} \text{Var} \{n''\}}{(R_{11} R_{22} - R_{12} R_{21})^2} \right) . \]

Noticing that \( n_{IC} \) and \( n'' \) are independent, we obtain the
instantaneous signal-to-interference plus noise ratio (SINR)
at node C is given by

\[ \text{SINR}_{C}^{ZF} = \frac{Y_{AC} Y_{DB} - (Y_{AB} Y_{DC})^2}{\gamma_{DB} Y_{BC} + Y_{DC} (Y_{BC} + Y_{AB} + Y_{DB} + 1)} . \]

In order to make it concise, we hereby denote all the SINRs’
subscripts \( AB, AC, BC, DB, DC \) as the index 1, 2, 3, 4, 5,
respectively. After using the following definitions:

\[ \mathcal{A} = \gamma_2 \sqrt{Y_4 - \sqrt{Y_2 Y_5}}, \]
\[ \mathcal{B}' = y_1 + y_4 + 1, \]
\[ \mathcal{B} = \frac{\mathcal{B}'}{\gamma_5} \]

SINR\(_{C}^{ZF}\) can be further rewritten as

\[ \text{SINR}_{C}^{ZF} = \frac{\mathcal{A}^2}{(y_4 + Y_5 \mathcal{B})} . \]

3.2. Minimum Mean-Square Error (MMSE) Detection. For
MMSE, the detector matrix \( L_{MMSE} \) meets

\[ L_{MMSE} = \arg \min_L \{ \| b - L y \|^2 \} . \]

By using the Projection Theorem, we obtain the following
equation:

\[ E \{ by^H - L_{MMSE} y^H \} = 0. \]

After a series of simplification, the detector matrix \( L_{MMSE} \) is
given by

\[ L_{MMSE} = \sqrt{\beta} (P R + \sigma^2 I (R^H)^{-1})^{-1}, \]

where \( R \) is defined in (7) and \( I' \) is defined as

\[ I' = \begin{bmatrix} 1 & 0 \\ 0 & m \end{bmatrix} . \]

where \( m = y_{BC} / (y_{AB} + y_{DB} + 1) + 1. \) Similar to the ZF detection,
we focus on the first element of \( \hat{b} \) to adjudicate \( x \). Moreover, \( \hat{b}_1 \)
is given by

\[ \hat{b}_1 = L'_{11} y'_{1} + L'_{12} y'_2, \]

where \( L' \equiv (R' (R'^H)^{-1})^{-1}, \mathcal{R}' \equiv \mathcal{R} / \sigma, \) and \( y' \equiv y / \sigma \). From
(21) we have the distribution of \( \hat{b}_1 \), which is omitted due to
the lack of space. Finally, we have the SINR of node C which can
be expressed as

\[ \text{SINR}_{C}^{MMSE} \]
\[ = \frac{(y_2 (\mathcal{A} / \mathcal{A}') + \mathcal{A}')^2}{y_5 y_2 (\mathcal{A} / \mathcal{A}')^2 + (\sqrt{y_2 + \sqrt{Y_2 (\mathcal{A} / \mathcal{A})^2}} + y_5 \mathcal{B})} , \]

where \( \mathcal{A} \) and \( \mathcal{B} \) are defined in (13) and (15), respectively.
3.3. Maximum Likelihood (ML) Detection. In this subsection, we have the new simultaneous equations:

\[
\begin{bmatrix}
y_{YC} \\
y_{ZC}
\end{bmatrix} = \left[ \frac{\sqrt{p}p_{AC}}{\sqrt{B}}, B \right] x + \left[ \begin{array}{c} n' \\ n'' \end{array} \right],
\]

(23)

by combining (2b) with (4c). Transforming (23) into a matrix form, we obtain

\[
y = \mathbf{H}x + \mathbf{n},
\]

(24)

where \( \mathbf{H} \) and \( \mathbf{n} \)'s definition can be easily get by comparing (23) with (24). Since it is easy to analyze the covariance matrix of the noise vector \( \mathbf{n} \), we directly give \( \mathbb{E}[\mathbf{n}\mathbf{n}^T] = \sigma^2 \mathbf{N} \) where \( \mathbf{N} \) is defined by

\[
\mathbf{N} = \begin{bmatrix}
\gamma_{xc} + 1 & \frac{\gamma_{xy} \gamma_{zc}}{\beta} \\
\frac{\gamma_{xc} \gamma_{zy}}{\beta} & \frac{\gamma_{xy} \gamma_{yc}}{\beta} + m
\end{bmatrix},
\]

(25)

with \( m = \gamma_{zc}/(\gamma_{zc} + 1) + 1 \).

Based on noise-whiting method and \( \mathbf{N} \)'s unitary decomposition \( \mathbf{N} = \sigma^2 \mathbf{A} \mathbf{u} \mathbf{u}^T \), whitening matrix \( \mathbf{M} \) is given by \( \mathbf{M} = (1/\sigma) \sqrt{\mathbf{N}^{-1}} \). Therefore, we have

\[
\mathbf{\tilde{y}} = \mathbf{M} \mathbf{H} x + \mathbf{M} \mathbf{n} = \mathbf{\tilde{H}} x + \mathbf{\tilde{n}}',
\]

(26)

where \( \mathbf{\tilde{H}} = \mathbf{M} \mathbf{H} \) and \( \mathbf{\tilde{n}}' = \mathbf{M} \mathbf{n} \). Obviously, \( \mathbb{E}[\mathbf{\tilde{n}}' \mathbf{\tilde{n}}'] = \sigma^2 \mathbf{I} \) holds. According to the principle of maximal ratio combining (MRC), the output is a weighted sum of all branches and the weights should be proportional to the branch SINRs. Thus, the SINR of the combiner output is the sum of SINRs on each branch. After using MRC of \( \mathbf{\tilde{y}} \), the judgment result \( \mathbf{\tilde{x}} \) from \( \mathbf{\tilde{y}} \) naturally meets \( \mathbf{\tilde{x}} = \arg \min_{\mathbf{x}} ||\mathbf{\tilde{y}} - \mathbf{\tilde{H}} x||^2 \). Intuitively, the output SINR of ML detection can be expressed as

\[
\text{SINR}_{\text{ML}} = \mathbf{\tilde{H}}_1^2 + \mathbf{\tilde{H}}_2^2.
\]

(27)

The analytical expression of \( \text{SINR}_{\text{ML}} \) cannot be obtained, caused by the complexity of unitary decomposition of symbolic expression in (25). But luckily and unexpectedly, we will find that \( \text{SINR}_{\text{ML}} \) is equal to \( \text{SINR}_{\text{MMSE}} \) in Section 4.4. Furthermore, this result will be confirmed through numerical simulations in Section 5.

4. Ergodic Secrecy Throughput of Three Detection Approaches

In this section, we adopt the Rayleigh fading model and derive the closed-form expressions for the lower bound and the upper bound of EST. We assume \( y_k, k = 1, \ldots, 5 \), is independent identically distributed (i.i.d) random variable and subject to exponential distribution with the same expectation \( \gamma \). In the following parts of this paper, we call \( \gamma \) the signal-to-noise ratio (SNR) of our system.

The instantaneous secrecy rate [16] of this general scheme can be written as

\[
R_S = \left[ \frac{1}{2} \log \left( 1 + \text{SINR}_C \right) - \frac{1}{2} \log \left( 1 + \text{SINR}_B \right) \right]^+.
\]

(28)

And EST is given by \( C_S = \mathbb{E}[R_S] \).

4.1. Lower Bound of ZF’s EST. For ZF, we have

\[
C_{ZF} = \mathbb{E} \left[ \frac{1}{2} \log \left( 1 + \frac{\gamma_{3,\text{ZF}}}{\gamma_{4} + \gamma_{5}} \right) \right],
\]

(29)

\[
\geq \frac{1}{2} \mathbb{E} \left[ \log \left( 1 + \frac{\gamma_{3,\text{ZF}}}{\gamma_{4} + \gamma_{5}} \right) \right] + C_{m,\text{low}}^{+ZF}
\]

where the inequality is due to the simple fact that \( \mathbb{E}[\max(X, Y)] \geq \max(\mathbb{E}[X], \mathbb{E}[Y]) \). The lower bound of EST can be characterized by

\[
C_{m,\text{low}}^{+ZF} = \left[ \frac{1}{2} \mathbb{E} \left( \log \left( 1 + \frac{\gamma_{3,\text{ZF}}}{\gamma_{4} + \gamma_{5}} \right) \right) \right]^+ - \mathbb{E} \left[ \frac{1}{2} \mathbb{E} \left( \log \left( 1 + \frac{\gamma_{3,\text{ZF}}}{\gamma_{4} + \gamma_{5}} \right) \right) \right].
\]

(30)

where \( \mathcal{A}, \mathcal{B}, \) and \( \mathcal{B}' \) are defined as before. In (30), \( C_{m}^{ZF} \) can be further lower bounded by

\[
C_{m}^{ZF} = \mathbb{E} \left( \log \left( 1 + \frac{\gamma_{3,\text{ZF}}}{\gamma_{4} + \gamma_{5}} \right) \right) + e^{\mathbb{E} \left( \log \left( 1 + \frac{\gamma_{3,\text{ZF}}}{\gamma_{4} + \gamma_{5}} \right) \right)} \geq \log \left( 1 + e^{\mathbb{E} \left( \log \left( 1 + \frac{\gamma_{3,\text{ZF}}}{\gamma_{4} + \gamma_{5}} \right) \right)} \right)
\]

(31)

\[
\approx C_{m,\text{low}}^{ZF}
\]

In (31), (a) is obtained from Jensen’s inequality and the convexity of \( \log(1+ae^x) \) for \( a > 0 \). Similarly, (b) is obtained from Jensen’s inequality and the convexity of logarithmic function. For Rayleigh fading, \( y_k \) obeys exponential distribution with the same rate parameter \( 1/\gamma \), where \( \gamma \) is the average SNR.
of our system. Recalling \(\mathcal{A}\)'s definition in (13), probability density function (PDF) of \(\mathcal{A}\) when \(\mathcal{A} > 0\) is given by

\[
h_{\mathcal{A}}(a) = \frac{16}{\pi} \int_{a}^{\infty} y_1 \text{BesselK} \left( 0, \frac{2y_1}{\sqrt{\mathcal{A}}} \right) \left( y_1 - a \right) \, dy_1,
\]

where \(\text{BesselK}[\nu, z]\) is modified Bessel function of second kind. According to the definition of \(\mathcal{A}\) given in (15) and the assumptions that all SNRs are independent and identically distributed, it is evident that the distribution of \(\mathcal{A}\) is symmetric for regions \(\mathcal{A} > 0\) and \(\mathcal{A} < 0\), leading to \(h(a) = h(-a)\).

Further letting \(\mathcal{X} = \mathcal{A}^2\), we can obtain the PDF of \(\mathcal{X}\) by

\[
h_{\mathcal{X}}(k) = \frac{16}{\pi} \int_{\sqrt{k}}^{\infty} y_1 \text{BesselK} \left( 0, \frac{2y_1}{\sqrt{\mathcal{X}}} \right) \left( y_1 - \sqrt{k} \right) \, dy_1.
\]

As shown in (31), \(I_1 = \mathbb{E}[\log \mathcal{X}]\). Thus, we have

\[
I_1 = \frac{16}{\pi} \int_{0}^{\infty} \left( \log k \right) \frac{1}{\sqrt{k}} \int_{\sqrt{k}}^{\infty} y_1 \text{BesselK} \left( 0, \frac{2y_1}{\sqrt{\mathcal{X}}} \right) \left( y_1 - \sqrt{k} \right) \, dy_1 \, dk.
\]

The double integral in (34) cannot be simplified in closed-form. We can figure out \(I_1\) by numerical integration. \(I_2\) can be solved as

\[
I_2 = \log \left( \mathbb{E} [y^3 y_4 + y_5 (y_3 + y_1 + y_4 + 1)] \right)
\]

\[
= \log \left( \mathbb{E} [y_3 y_4] + \mathbb{E} [y_5 (y_3 + y_1 + y_4 + 1)] \right) \tag{35}
\]

\[
= 2 \log (2\sqrt{\gamma}).
\]

In (35), (a) holds due to the property of mathematical expectation and (b) holds due to \(y_3, k = 1, \ldots, 5\), being i.i.d random variable and subject to exponential distribution with the expectation \(\bar{\sigma}\). In addition, it is easy to get that

\[
\mathbb{E} \{ \log y_3 \} = \log \bar{\sigma} - \kappa,
\]

where \(\kappa\) is the Euler constant defined in [32]. On the other hand,

\[
C_e = \frac{1}{\pi} \int_{y_1, y_2 > 0} \log \left( \frac{1 + y_1}{y_4} \right) e^{-\left( y_1 + y_2 \right)/\bar{\sigma}} dy_1 dy_2 = 1. \tag{37}
\]

By substituting (34), (35), (36), and (37) into (30), we can arrive at the lower bound of EST under ZF strategy:

\[
C_{S,\text{low}}^{\text{ZF}} = \max \left( \frac{\log \left( 1 + \exp (-\kappa + I_1 - \log 4\bar{\sigma}) \right) - 1}{2}, 0 \right). \tag{38}
\]

4.2. Upper Bound of ZF’s EST. The upper bound of EST for the ZF detection approach can be obtained as follows. Because \(C_{m}^{\text{ZF}}\) is the secrecy throughput and \(C_{\text{m}}^{\text{ZF}}\) represents the maximum achievable rate with malicious users (see (29)-(30) for definitions of the two notations), we can readily have

\[
C_{S}^{\text{ZF}} < C_{m}\]
Applying (45), (46), and the simple fact that the last item in the molecule of \( \alpha \) is positive into (44), we immediately have \( \alpha > 1 \). Thus Theorem 1 follows.

On the basis of Theorem 1, which indicates that MMSE has a higher instantaneous SINR, we draw the conclusion that the EST of MMSE is lower bounded by that of ZF.

4.4. Analysis of ML’s EST. Solving the EST under ML detection needs to find the exact value of \( \text{SINR}_{\text{ML}} \). In order to analyze this problem, we first introduce the following lemma.

**Lemma 2.** The result of MMSE for the initial model (6) and the noise whitening model (26) is consistent.

**Proof.** The proof of Lemma 2 is omitted for the lack of space.

**Theorem 3.** In our jamming-aided Security provisioning scheme, MMSE and ML are essentially the same. That is to say

\[
\text{SINR}_{\text{MMSE}} = \text{SINR}_{\text{ML}}.
\]

**Proof.** We rewrite (26) as

\[
\bar{y} = \bar{H}x + \bar{n}',
\]

where \( \bar{n}_1, \bar{n}_2 \sim \mathcal{CN}(0, 1) \) and \( \bar{H}_1, \bar{H}_2 \) are fixed real number. (For simplicity, we have such assumption. In fact they are complex numbers. But we can multiply the observed sample by the corresponding opposite phase to transform them into real numbers.) As given in Section 3.3,

\[
\hat{x}_{\text{ML}} = \bar{H}\bar{y}
\]

and (27) holds. On the other hand, by applying the method similar to Section 3.2, \( L_w \) which meets argmin \( \{ |x - Ly|^2 \} \) is given by

\[
L_w = H(HH^T + I)^{-1}.
\]

Then, we obtain

\[
\bar{x} = cH^T\bar{y}.
\]

By comparing (49) with (51), we find that the difference between them is a consistent which will not have any impact on the judgment. Finally, considering Lemma 2, Theorem 3 follows.

Based on Theorem 3, we draw a conclusion that the performance of ML is equal to MMSE, thus offering the potential low computational complexity. Correspondingly, EST of ML is equal to that of MMSE.

5. Simulation Results and Discussions

This section presents some numerical results to verify the previous theoretical analyses. The simulation environment is based on the system model described in Section 2. In Figures 2–5, we assumed that all channel coefficients are submitted to Rayleigh fading with the same mean, which is so-called average SNR. Without loss of generality, we assumed the power of the transmitting node \( A \) and the jamming node \( D \) is equal to 1. In Figure 2, all the nodes use QPSK modulation. In addition, ZF technique is prone to high errors as the channel coefficients cannot be estimated perfectly. The readers can refer to the rich literature to study the impact of channel estimation errors.

Figure 2 shows the simulation results of the receiving node \( C \) and the relay node \( B \)’s bit error rate (BER) with the change of the average SNR, which illustrates the reliability of our proposed network. From Figure 2, we observe that the relay node \( B \) has a significant error floor, caused by...
the jamming node $D$’s artificial noise. In high SNR regime, $\text{SNR}_B \approx \gamma_1/\gamma_4$. We immediately have $B$’s BER given by

$$\text{BER}_B = \int_0^{\infty} \frac{Q(\sqrt{\epsilon})}{(1+z)^2}dz$$

$$= \frac{1}{4} \left( 2 - \sqrt{2\pi} \text{Erfc} \left( \frac{1}{\sqrt{2}} \right) \right) \approx 0.172,$$

where Erfc($\cdot$) is complementary error function defined in [32]. But in our network, node C’s BER rapidly declines with the growth of SNR, which benefits from node C having higher signal dimensions to effectively suppress the interference. All the detectors can gather the interfered signal of the two phases and carry out a joint decision. Thus the reliability for data transmissions is assured. Additionally, the slope of the BERs of three detection approaches in high SNR regime relative to the SNR is approximately $-0.5$, which indicates our robustness provisioning scheme achieves a half-order diversity gain.

Figure 3 illustrates the change of the EST with the average SNR, from which it can be seen that, as expected, the ESTs under the three approaches increase with the increase of the average SNR. As the average SNR increases, the difference between the EST of the three detection methods becomes smaller, which is consistent with the fact that MMSE detector degenerate into ZF detector with increase of SNR. The performances of the MMSE detector and the ML detector are close to each other and have the best performances. It can be seen that the exact values and the lower bounds given in (38) agree well for high SINRs, at the same time, the exact values and the upper bound given in (41) agree well for low SNRs. As a result of inequality of (a) and (b) in (39), the difference between upper bound and exact values is large in high SNR regime.

Finally, in Figures 4 and 5 we plot the secrecy outage probability (SOP) curves with respect to the average SNR and secrecy throughput threshold, respectively. In Figure 4 secrecy throughput thresholds corresponding to the solid line and dashed line are 0 nats/s/Hz and 1 nats/s/Hz, respectively. Because solid line corresponds to a smaller threshold, solid line’s SOP is smaller than dashed line’s SOP under the same average SNR. For a fixed secrecy throughput threshold, SOP decreases as the average SINR increases. SOP under ZF detection approach is higher than it is under the other detection approaches. The main reason for this phenomenon is briefly given as follows: ZF criterion only aims to reduce the interference between signal and AN, but MMSE criterion additionally considers the character of noise. Besides, ML detector as the optimal detector certainly has the best performance, and its performance is equal to MMSE in our proposed scheme, which supports our conclusion in Section 4. In Figure 5, the average SNRs corresponding to the solid line and dashed line are 20 dB and 40 dB, respectively. SOP corresponding to each curve increases with the increase of the security throughput threshold.

6. Conclusion

In this paper, we present a comprehensive analysis of the robust relay aided by an uncooperative jamming node in narrow-band communications for ubiquitous IoT access, which is further modeled as a two-hop AF cooperative system. We first focus on the three typical detection approaches to exploit potential security and robustness in our transmission scheme and derive the lower bounds and/or the upper bounds of the ESTs. Then we reveal that, in our framework, ML detection and MMSE detection in fact are equivalent, offering the potential low computational complexity. All the theoretical contributions are validated by numerical and...
simulation results. While our study concentrates on the simple yet typical model, our future work will extend our idea to other more complicated topologies.

Conflicts of Interest
The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments
The research work reported in this paper is supported by the National Natural Science Foundation of China under Grant nos. 61461136001 and 61671371, the National Science and Technology Major Project under Grant no. 2016ZX03001016-005, Science and Technology Program of Shaanxi Province under Grant no. 2016KW-032, ZTE Industry Academic Research Cooperation Funds, and Fundamental Research Funds for the Central Universities.

References


