





Network Coding Assisted Secure Transmission in Full-Duplex Relay Networks

Hongliang He , Shanxiang Lyu , Qinghao He ,
and Dongyang Xu 

Abstract—Secure transmission in full-duplex relay networks is considered in this paper. To ensure security, we propose a network coding assisted relaying scheme, where all the messages are encoded by the transmitter and the full-duplex relay respectively. Specifically, the encoding at the transmitter makes sure that all the coded messages are required to decode a private message. Consequently, security is achieved if the eavesdropper loses one or more coded messages. The encoding at the relay is operated by introducing a public auxiliary message, which changes the eavesdropper's decoding method from combining-before-decoding to combining-after-decoding, and thus decreases the eavesdropper's signal-noise-ratio (SNR) obviously. Intercept probability is used to measure the security, and results show that the proposed scheme can significantly improve the security performance of full-duplex relay networks.

Index Terms—Full-duplex, physical-layer security, network coding.

I. INTRODUCTION

With the rapid development of wireless communication techniques, using wireless media for information interaction has become ubiquitous. However, due to the openness of wireless channels, data transmission is vulnerable to eavesdropping by illegitimate eavesdroppers. This brings security challenges especially when the data are private or confidential. To ensure the secure delivery of information, a promising method called physical-layer security has been extensively studied recently, which exploits the inherent randomness of wireless channels, such as fading, noise, and interference, and achieves keyless security [1]–[3]. The study of physical-layer security was originated with Shannon, who showed that perfect secrecy can be achieved if the key is as long as the confidential message. Subsequently, Wyner demonstrated that if the legitimate channel is better than the eavesdropper's channel, security can be achieved without using the key. Based on this result,

Manuscript received April 1, 2020; revised May 28, 2020; accepted June 8, 2020. Date of publication June 12, 2020; date of current version August 13, 2020. This work was supported in part by the Key-Area Research and Development Program of Guangdong Province under Grant 2019B010137005, in part by the National Natural Science Foundation of China under Grant 61972178, in part by the Guangdong Basic and Applied Basic Research Foundation under Grants 2017A030313334 and 2019A1515011753, in part by the Science and Technology Program of Guangzhou of China under Grant 201802010061, in part by the Fundamental Research Funds for the Central Universities under Grant 21620432, in part by the National Natural Science Foundation of China under Grant 61902149, in part by the Fundamental Research Funds for the Central Universities under Grant 21620438, and in part by the Fundamental Research Funds for the Central Universities under Grant 21620350. The review of this article was coordinated by Dr. C. Yuen. (*Corresponding author: Shanxiang Lyu.*)

Hongliang He and Shanxiang Lyu are with the College of Information Science and Technology, and the College of Cyber Security, Jinan University, Guangzhou 510632, China (e-mail: hehongliang@stu.xjtu.edu.cn; shanxianglyu@gmail.com).

Qinghao He is with the Department of Intelligent Manufacturing, Dongguan Technician College, Dongguan 523808, China (e-mail: qinghaohe@outlook.com).

Dongyang Xu is with the School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: xudongyang@xjtu.edu.cn).

Digital Object Identifier 10.1109/TVT.2020.3001871

substantial work has been conducted to achieve the physical-layer security, such as multiple antenna techniques, cooperative communications techniques, and jamming techniques.

Full-duplex (FD) relaying is an attractive cooperative communication method since it enables simultaneous transmitting and receiving on the same frequency. Recently, people have begun to study its potential to improve security. In [4], the authors obtained the upper bound of the eavesdropping capacity when the relay exploits FD mode, and analyzed the secrecy outage probability. For the scenario with multiple full-duplex relays and multiple users, authors in [5] investigated the relay selection problem to maximize the minimum secrecy rate in all source-destination pairs. The security performance of the multi-antenna full-duplex relay was discussed in [6], where the optimal beamforming is employed to maximize the secrecy rate. In [7], full-duplex is combined with jamming, and the authors demonstrated that secrecy rate can be improved by appropriately allocating power to the jamming and the private information. The application of full-duplex in cognitive radio networks was discussed in [8], where secure primary transmission was considered. The application of full-duplex in non-orthogonal multiple access (NOMA) system was considered in [9], where the secrecy outage probability was derived. In [10], the authors investigated the security performance of a wireless-powered network when the relay exploits full-duplex mode, and obtained the asymptotic average secrecy rates.

A common assumption in the work discussed above is that private messages sent from the transmitter are independent. In this case, the loss of a private message at the eavesdropper does not prevent it from decoding other private messages. Another common feature of the existing work is that they generally use secrecy capacity or secrecy outage probability to measure security performance. Once the legitimate channel is worse than the eavesdropper's channel, security cannot be achieved. Moreover, the eavesdropper in the existing work can combine the received signals from both the transmitter and the relay before decoding. This greatly enhances the decoding capabilities of the eavesdropper. Our work is different from the existing work because of the use of network coding. First, we use network coding at the transmitter to relate the private messages in different slots, so the loss of a coded message prevents the eavesdropper from decoding any private messages. Second, we use intercept probability instead of secrecy outage probability. Thus, even the legitimate channel is worse than the eavesdropper's channel, security still can be achieved. Third, the network coding used at the relay prevents the eavesdropper from combining the received signals before decoding. Thus, the eavesdropper can only combine the signals after decoding, which obviously decreases the eavesdropper's SNR.

Network coding is generally exploited to improve the throughput of networks, but it recently showed its potential to improve security. In [12], the authors exploited the fountain code to improve security. They showed that if the legitimate destination can decode the private file before the eavesdropper, security can be achieved. Subsequently, the fountain code was extended to the scenario that the channel coefficients in different slots are not independent [14]. Different from the work in [12] and [14] that consider direct transmission, authors in [15] jointed the network coding and the relay selection to improve the security in the cooperative communication. However, the eavesdropper in their work can only overhear the information from the relays, which is relatively weak. In order to improve both the security and the reliability, network coding is recently combined with automatic-repeat-request

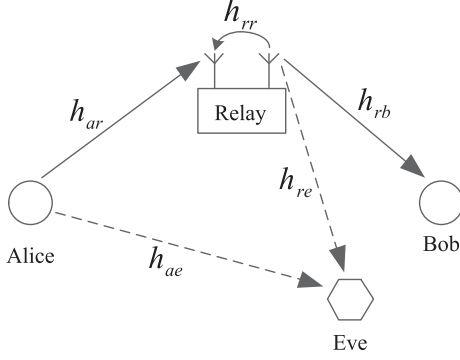


Fig. 1. System Model.

(ARQ) scheme [13]. Although all these works have shown the effectiveness of network coding in improving security, all of them use the half-duplex technique. To the best of our knowledge, this paper is the first work to investigate the security performance of the network coding in full-duplex relay networks.

The remainder of this paper is organized as follows. Section II provides the system model and the capacity of the eavesdropper's channel when network coding is not used. Section III analyzes the security performance when network coding is used at the transmitter and the relay. Simulation results and conclusions are provided in Sections IV and V.

II. SYSTEM MODEL AND COMBINING-BEFORE-DECODING AT THE EAVESDROPPER

A. System Model

We consider a full-duplex relay network, as shown in Fig. 1, which consists of a source, noted as Alice, a legitimate destination, noted as Bob, and a full-duplex relay. The source Alice intends to transmit private information to the destination Bob via the full-duplex relay, but the information is overheard by a passive eavesdropper, noted as Eve. The relay exploits decoding-and-forward (DF) protocol and is equipped with two antennas, i.e., one transmitting antenna and one receiving antenna, but other nodes have only one antenna. There is no direct communication link between Alice and Bob because of the long distance and high attenuation of signals, but the eavesdropper can intercept the information from both the source and the relay.

Over slot t , the source transmits signal $x[t]$ and the relay forwards $z[t]$. The received signal at the relay is

$$y_r[t] = \sqrt{p_a}h_{ar}[t]x[t] + \sqrt{p_r}h_{rr}[t]z[t] + n_r[t]. \quad (1)$$

Here, the signals $x[t]$ and $z[t]$ are with unit power. The transmit power at Alice is p_a , and the transmit power at the relay is p_r . Notation $h_{ar}[t]$ denotes the channel coefficient from Alice to the relay over slot t , which is modeled as a circularly symmetric complex Gaussian variable with zero mean and variance σ_{ar}^2 , noted as $h_{ar}[t] \sim \mathcal{CN}(0, \sigma_{ar}^2)$. Notation $h_{rr}[t]$ denotes the residual self-interference channel of the full-duplex relay over slot t , which also be considered as a complex Gaussian variable with zero mean and variance σ_{rr}^2 (See [16] and the references therein). Notation $n_r[t] \sim \mathcal{CN}(0, 1)$ denotes the additive white complex Gaussian noise (AWGN) at the relay over slot t . The received signal at Bob is

$$y_b[t] = \sqrt{p_r}h_{rb}[t]z[t] + n_b[t], \quad (2)$$

where $h_{rb} \sim \mathcal{CN}(0, \sigma_{rb}^2)$ denotes the channel coefficient from the relay to Bob, and $n_b[t] \sim \mathcal{CN}(0, 1)$ is the complex AWGN at Bob. The

received signal at the eavesdropper is

$$y_e[t] = \sqrt{p_a}h_{ae}[t]x[t] + \sqrt{p_r}h_{re}[t]z[t] + n_e[t], \quad (3)$$

where $h_{ae} \sim \mathcal{CN}(0, \sigma_{ae}^2)$ denotes the channel coefficient from the source to Eve, $h_{re} \sim \mathcal{CN}(0, \sigma_{re}^2)$ denotes the channel coefficient from the relay to Eve, and $n_e[t] \sim \mathcal{CN}(0, 1)$ is the complex AWGN at Eve. We assume that the channel coefficients $h_{ar}[t]$, $h_{rb}[t]$, and $h_{rr}[t]$ remain unchanged over one slot but are independently identically distribution (i.i.d.) in different slots. However, the eavesdropper's channel coefficients, $h_{ae}[t]$ and $h_{re}[t]$, remain unchanged in multiple slots because of the less mobility of the eavesdropper.

Throughout this paper, we denote $\Gamma_{ae}[t] = p_a|h_{ae}[t]|^2$, $\Gamma_{re}[t] = p_r|h_{re}[t]|^2$, $\Gamma_{ar}[t] = p_a|h_{ar}[t]|^2$, $\Gamma_{rb}[t] = p_r|h_{rb}[t]|^2$, and $\Gamma_{rr}[t] = p_r|h_{rr}[t]|^2$. The random variable $\Gamma_{mn}[t]$ is exponentially distributed with mean $\lambda_{mn} = 1/(p_m\sigma_{mn}^2)$, so its probability density function (p.d.f.) is

$$f(x) = \lambda_{mn}e^{-\lambda_{mn}x}, \quad x > 0. \quad (4)$$

B. Combining-Before-Decoding at the Eavesdropper

We now consider the eavesdropper's capacity to decode the message $x[t]$ when the network coding is not used at the relay, and obtain the upper bound of the eavesdropper's capacity.

First, it is worth noting that due to the power limitation and the processing delay at the full-duplex relay, the relationship between $z[t]$ and $x[t]$ is

$$z[t] = x[t - \tau], \quad (5)$$

where τ is an integer multiple of the time slot representing the processing delay at the relay to make sure that the signal transmitted at the relay is uncorrelated from the simultaneously received signal. In this paper, we assume one slot, i.e., $\tau = 1$ slot, is long enough to meet this requirement, so the relationship between $z[t]$ and $x[t]$ is further expressed as

$$z[t] = x[t - 1], \quad (6)$$

and the eavesdropper's received signal can be further expressed as

$$y_e[t] = \sqrt{p_a}h_{ae}[t]x[t] + \sqrt{p_r}h_{re}[t]x[t - 1] + n_e[t]. \quad (7)$$

Consider that Alice transmits L successive codewords, i.e., $\mathbf{x} = (x[1], \dots, x[L])^T$. The eavesdropper's channels keep constant in the transmission of these L codewords. Based on (7), the eavesdropper can combine the signals from Alice and the relay to form a vector:

$$\mathbf{y}_e = \mathbf{H}_e \mathbf{x} + \mathbf{n}_e, \quad (8)$$

where $\mathbf{y}_e = (y_e[1], \dots, y_e[L + 1])^T$, $\mathbf{n}_e = (n_e[1], \dots, n_e[L + 1])^T$, and \mathbf{H}_e is the equivalent matrix of the eavesdropping channels, which is a $(L + 1) \times L$ matrix given by

$$\mathbf{H}_e = \sqrt{p_a}h_{ae} \begin{bmatrix} \mathbf{I}_L \\ \mathbf{0}_{1 \times L} \end{bmatrix} + \sqrt{p_r}h_{re} \begin{bmatrix} \mathbf{0}_{1 \times L} \\ \mathbf{I}_L \end{bmatrix}, \quad (9)$$

with $\mathbf{0}_{1 \times L}$ denoting $1 \times L$ zero vector and \mathbf{I}_L denoting $L \times L$ unit matrix. Because Eve combines \mathbf{x} before decoding it, we call this method as **combining-before-decoding**.

From (8), we can see that the capacity of the eavesdropper's channel is equivalent to the capacity of a multiple-input and multiple-output (MIMO) channel, which is expressed as

$$C_E = \frac{1}{L} \log_2 \det\{\mathbf{I}_L + \mathbf{H}_e^\dagger \mathbf{H}_e\}. \quad (10)$$

Based on the result given in [4], we can obtain the upper bound of C_E in (10) as $C_E^{\text{UB}} = \log_2(1 + \Gamma_{ae} + \Gamma_{re})$. For the convenience of analysis, we assume the eavesdropper's capacity is equal to its upper bound, i.e.,

$$C_E = \log_2(1 + \Gamma_{ae} + \Gamma_{re}). \quad (11)$$

From (11), we can find that the use of combining-before-decoding makes the SNR at the eavesdropper close to the result using maximal-ratio combining (MRC), which improves the eavesdropper's SNR significantly [4]. To prevent this situation from happening, we use network coding, which is discussed in the following section.

III. APPLICATION OF THE NETWORK CODING

In this section, we discuss the specific encoding and decoding method at Alice and the relay. Intercept probability is used to measure the security performance of the proposed scheme, and we analyze it in theory.

A. Encoding at Alice

First, we discuss the network coding method used by Alice. Assume Alice intends to transmit $L - 1$ private messages to the legitimate destination Bob, noted as $s[1], s[2], \dots, s[L - 1]$. When L is even, the encoding method used by Alice is given by

$$\begin{aligned} x[1] &= s[0] \oplus s[1], \\ x[2] &= s[0] \oplus s[2], \\ &\vdots \\ x[L - 1] &= s[0] \oplus s[L - 1], \\ x[L] &= s[1] \oplus s[2] \oplus \dots \oplus s[L - 1], \end{aligned} \quad (12)$$

where \oplus denotes the XOR operation. When L is odd, the encoding method used by Alice is given by

$$\begin{aligned} x[1] &= s[0] \oplus s[1], \\ x[2] &= s[0] \oplus s[2], \\ &\vdots \\ x[L - 1] &= s[0] \oplus s[L - 1], \\ x[L] &= s[0] \oplus s[1] \oplus s[2] \oplus \dots \oplus s[L - 1]. \end{aligned} \quad (13)$$

Here, $s[0]$ is a helper message, which does not contain private information but to assist the secure transmission. Observing the encoding method at Alice, we can find that when $t = 1, 2, \dots, L - 1$, the encoding is $x[t] = s[0] \oplus s[t]$; when $t = L$, the encoding is $x[L] = s[1] \oplus \dots \oplus s[L - 1]$ for even L and $x[L] = s[0] \oplus s[1] \oplus \dots \oplus s[L - 1]$ for odd L .

Although the encoding methods are different when L is odd and even, their decoding methods are the same, which is

$$\begin{aligned} s[t] &= x[1] \oplus x[2] \oplus \dots \oplus x[L] \oplus x[t] \\ &= x[1] \oplus \dots \oplus x[t - 1] \oplus x[t + 1] \oplus \dots \oplus x[L], \end{aligned} \quad (14)$$

where $t = 1, 2, \dots, L - 1$. From (14), we can see that the decoding of $s[t]$ requires $L - 1$ coded messages, i.e., $x[1], x[2], \dots, x[L]$ except $x[t]$. The loss of any coded messages in $\{x[1], x[2], \dots, x[t - 1], x[t + 1], \dots, x[L]\}$ will prevent the eavesdropper from decoding all the private messages, i.e., $s[t]$ with $i = 1, 2, \dots, L - 1$. In this case, the security of $s[t]$ is related to all the coded messages in $\{x[1], x[2], \dots, x[t - 1], x[t + 1], \dots, x[L]\}$.

B. Encoding at the Relay

We now consider the network coding method at the relay. It is given by

$$z[t] = r[0] \oplus x[t - 1], \quad (15)$$

where $t = 1, 2, \dots, L$, and $r[0]$ is a public message known by Bob and Eve. Note that the selection of $r[0]$ should satisfy $r[0] \oplus x[t - 1] \neq x[t - 1]$. In this case, the received signal at the eavesdropper is no longer the same as (7). In fact, it is the same as (3) but $z[t] \neq x[t - 1]$. Due to the existence of $z[t] \neq x[t - 1]$, Eve cannot use the signal processing method given in (8) any more, so the received signal in (3) is similar to the output of intersymbol interference (ISI) channel, i.e., $x[t]$ and $z[t]$ interference each other.

As discussed before, the eavesdropper can receive each signal twice, one is from Alice and the other is from the relay. Then he/she can combine both of them to decode the information. Using the coding scheme in (15), we can find that if the eavesdropper intends to combine $x[t - 1]$ from Alice and the relay, he/she has to decode $z[t]$ first, which means that the combining-before-decoding method used in (8) cannot be employed anymore.

C. Capacity of the Eavesdropper's Channel

Observing (3), we find that the eavesdropper has two ways to decode a coded message $x[t - 1]$. The first way is to view $z[t - 1]$ as interference and decode $x[t - 1]$ directly. Note that $x[t - 1]$ in this case is from Alice. The second way is to decode $x[t - 1]$ based on $z[t] = r[0] \oplus x[t - 1]$. In this case, $z[t] = r[0] \oplus x[t - 1]$ is from the relay, and $x[t]$ is viewed as interference. For the first way, the signal-to-interference-plus-noise-ratio (SINR) at Eve is

$$\gamma_{e1} = \frac{\Gamma_{ae}}{\Gamma_{re} + 1}. \quad (16)$$

For the second way, the SINR at Eve is

$$\gamma_{e2} = \frac{\Gamma_{re}}{\Gamma_{ae} + 1}. \quad (17)$$

The eavesdropper can use **combining-after-decoding** scheme to select the best way in (16) and (17) to decode $x[t - 1]$. In this case, we can obtain the SINR at the eavesdropper to decode $x[t - 1]$ as

$$\gamma_e = \max(\gamma_{e1}, \gamma_{e2}). \quad (18)$$

Comparing $\max(\gamma_{e1}, \gamma_{e2})$ in the combining-after-decoding scheme with $\Gamma_{ae} + \Gamma_{re}$ in the combining-before-decoding scheme, we find that the SINR in the combining-after-decoding scheme is obviously less than that in the combining-before-decoding scheme, i.e., $\max(\gamma_{e1}, \gamma_{e2}) < \Gamma_{ae} + \Gamma_{re}$. In this respect, the network coding method used at the relay decreases the capacity of the eavesdropper's channel, which is given by

$$C_e = \log_2(1 + \max(\gamma_{e1}, \gamma_{e2})). \quad (19)$$

D. Capacity of the Legitimate Channel

Based on the received signals given in (1) and (2), the capacity of the legitimate channel to decode $z[t]$ is obtained as

$$C_b = \log_2 \left(1 + \min \left\{ \frac{\Gamma_{ar}[t]}{\Gamma_{rr}[t] + 1}, \Gamma_{rb}[t] \right\} \right). \quad (20)$$

This indicates that the capacity of the legitimate channel depends on the weak link in the Alice-Relay link and the Relay-Bob link. Since $z[t] = r[0] \oplus x[t - 1]$ holds, the capacity of the legitimate channel to

decode $x[t-1]$ is the same as that to decode $z[t]$. For presentation convenience, we define

$$\gamma_b = \min \left\{ \frac{\Gamma_{ar}[t]}{\Gamma_{rr}[t] + 1}, \Gamma_{rb}[t] \right\} \quad (21)$$

E. Intercept Probability

We use intercept probability to measure the security performance of the proposed scheme. The intercept probability is defined as the probability that the eavesdropper decodes the message successfully [12], [17], [18]. If the transmission rate is $R_0 = C_b$, the intercept probability of $x[t-1]$ is

$$\begin{aligned} P_{int,x} &= \Pr(R_0 \leq C_e) \\ &= \Pr(\gamma_b \leq \gamma_e) \\ &= \Pr \left(\min \left\{ \frac{\Gamma_{ar}[t]}{\Gamma_{rr}[t] + 1}, \Gamma_{rb}[t] \right\} \leq \max(\gamma_{e1}, \gamma_{e2}) \right). \end{aligned} \quad (22)$$

Since $\Gamma_{mn}[t]$ is i.i.d. in different slots, we suppress the index t for ease of presentation.

Defining $X = \Gamma_{ar}/(\Gamma_{rr} + 1)$, we can obtain its c.d.f. as

$$\begin{aligned} F_X(x) &= \int_0^\infty F_{\Gamma_{ar}}(x(y+1)) f_{\Gamma_{rr}}(y) dy \\ &= 1 - \frac{e^{-\lambda_{ar}x}}{1 + \frac{\lambda_{ar}}{\lambda_{rr}}x}. \end{aligned} \quad (23)$$

Based on (23), we can obtain the c.d.f of $\gamma_b = \min\{\Gamma_{ar}/(\Gamma_{rr} + 1), \Gamma_{rb}\}$ as

$$\begin{aligned} F_{\gamma_b}(x) &= F_X(x) + F_{\Gamma_{rb}}(x) - F_X(x)F_{\Gamma_{rb}}(x) \\ &= 1 - \frac{e^{-(\lambda_{ar} + \lambda_{rb})x}}{1 + \frac{\lambda_{ar}}{\lambda_{rr}}x}, \end{aligned} \quad (24)$$

and the p.d.f. of γ_b as

$$f_{\gamma_b}(x) = \frac{(\lambda_{ar} + \lambda_{rb} - \frac{\lambda_{ar}}{\lambda_{rr}}) e^{-(\lambda_{ar} + \lambda_{rb})x}}{\left(1 + \frac{\lambda_{ar}}{\lambda_{rr}}x\right)^2}. \quad (25)$$

Similarly, we can obtain the c.d.f. of $\gamma_e = \max(\gamma_{e1}, \gamma_{e2})$ as

$$F_{\gamma_e}(y) = \left(1 - \frac{e^{-\lambda_{ae}y}}{1 + \frac{\lambda_{ae}}{\lambda_{re}}y}\right) \left(1 - \frac{e^{-\lambda_{re}y}}{1 + \frac{\lambda_{re}}{\lambda_{ae}}y}\right). \quad (26)$$

Based on (24), (25), and (26), we can obtain the intercept probability of $x[t-1]$ as

$$\begin{aligned} P_{int,x} &= \Pr(\gamma_b \leq \gamma_e) \\ &= \int_0^\infty \int_0^y f_{\gamma_b}(x) f_{\gamma_e}(y) dx dy \\ &= \int_0^\infty f_{\gamma_e}(y) \int_0^y f_{\gamma_b}(x) dx dy \\ &= 1 - \int_0^\infty F_{\gamma_e}(y) f_{\gamma_b}(y) dy. \end{aligned} \quad (27)$$

Substituting (25) and (26) into (27), we can obtain the final result of the intercept probability of $x[t-1]$. Unfortunately, the result does not have closed-form expression.

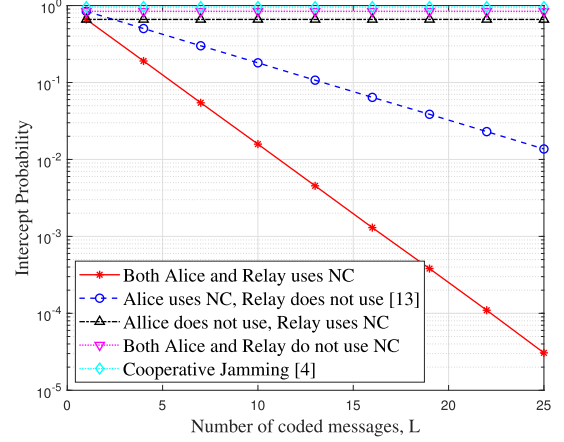


Fig. 2. Intercept probability of $s[t]$ vs. the number of coded messages, L .

Recall that the decoding of $s[t]$ requires $L-1$ coded messages, i.e., $x[1], \dots, x[t-1], x[t+1], \dots, x[L]$, so the intercept probability of $s[t]$ is obtained as

$$\begin{aligned} P_{int,s} &= (P_{int,x})^{L-1} \\ &= \left(1 - \int_0^\infty F_{\gamma_e}(y) f_{\gamma_b}(y) dy\right)^{L-1}. \end{aligned} \quad (28)$$

IV. SIMULATION RESULTS

In this section, we provide simulation results to show the security performance of the proposed scheme.

Fig. 2 exhibits the intercept probability of $s[t]$ changing with the number of coded messages, L . The simulation parameters are given as follows: $p_a = p_r = 1$, $\sigma_{ar}^2 = 2$, $\sigma_{rb}^2 = 2$, $\sigma_{ae}^2 = 1$, $\sigma_{re}^2 = 2$, and $\sigma_{rr}^2 = 0.1$. There are five cases shown in Fig. 2. The first case is that both Alice and the relay use network coding (NC); the second case is that only Alice uses network coding (shown in (12) and (13)) but the relay does not use [13]; the third case is that Alice does not use network coding but the relay uses (shown in (15)); the fourth case is that both Alice and the relay do not use network coding; the fifth case is the cooperative jamming scheme proposed in [4]. It can be seen that the proposed scheme, i.e., the first case, achieves the best security performance. In the second case, Alice uses the method given in (12) and (13), but the relay forwards $x[t-1]$ rather than $x[t-1] \oplus r[0]$. The third case is that Alice does not use network coding but the relay operates $z[t] = x[t-1] \oplus r[0]$. We can see that the second case is related to the number of coded messages, but the third case is not. Thus, when L is small, the third case is better than the second case, but with the increase of L , the second case gets better than the third case. In addition, it can be seen that the cooperative jamming scheme does not have an advantage.

Fig. 3 shows the effect of σ_{re}^2 and σ_{ae}^2 on the security performance of the proposed scheme. The parameters are given as follows: $p_a = p_r = 1$, $\sigma_{ar}^2 = 0\text{dB}$, $\sigma_{rb}^2 = 0\text{dB}$, $\sigma_{ae}^2 = \sigma_{re}^2 - 0.5$, $\sigma_{rr}^2 = 0.1$, and $L = 30$. It can be seen that the security performance decreases obviously when σ_{re}^2 and σ_{ae}^2 increase. The intercept probability of the second, the third, the fourth, and the fifth case tend to one, but the intercept probability in the first case exists an upper bound. This indicates that the network coding scheme used at the relay restricts the eavesdropper's ability to decode the private information when both σ_{ae}^2 and σ_{re}^2 are large.

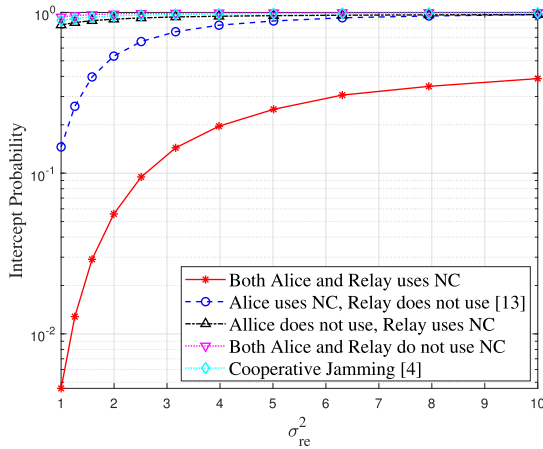


Fig. 3. Intercept probability of $s[t]$ vs. the average value of the eavesdropper's channels, i.e., σ_{re}^2 and $\sigma_{ae}^2 = \sigma_{re}^2 - 0.5$.

V. CONCLUSION

In this paper, we consider the secure transmission in full-duplex relay networks. The transmitter and the relay jointly design network coding, so that the eavesdropper cannot decode any private messages if it loses one or more than one coded messages. Especially, the network coding used at the relay prevents the eavesdropper from using the combining-before-decoding scheme, which weakens the capacity of the eavesdropper's channel. The intercept probability is employed to measure the security performance of the proposed scheme, which decreases exponentially with the increase of the number of coded messages.

REFERENCES

- [1] K. Lee, J. Hong, H. Choi, and T. Q. S. Quek, "Wireless-powered twoway relaying protocols for optimizing physical layer security," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 1, pp. 162–174, Jan. 2019.
- [2] R. Chopra, C. R. Murthy, and R. Annavajjala, "Physical layer security in wireless sensor networks using distributed co-phasing," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 10, pp. 2662–2675, Oct. 2019.
- [3] Q. Li and L. Yang, "Beamforming for cooperative secure transmission in cognitive two-way relay networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 130–143, 2020.
- [4] G. Chen, Y. Gong, P. Xiao, and J. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 3, pp. 574–583, Mar. 2015.
- [5] S. Atapattu, N. Ross, Y. Jing, Y. He, and J. S. Evans, "Physical-layer security in full-duplex multi-hop multi-user wireless network with relay selection," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1216–1232, Feb. 2019.
- [6] D. Hwang, J. Yang, E. Yoon, H. Song, and S. S. Nam, "Beamformer optimization for the full-duplex AF relay wiretap channels," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 129–132, Feb. 2019.
- [7] S. Parsaeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 10, pp. 2095–2107, Oct. 2015.
- [8] B. Chen *et al.*, "Secure primary transmission assisted by a secondary full-duplex NOMA relay," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7214–7219, Jun. 2019.
- [9] Y. Cao *et al.*, "Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5574–5587, Aug. 2019.
- [10] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 3, pp. 621–634, Jul. 2018.
- [11] B. Li, X. Li, R. Zhang, W. Tang, and S. Li, "Joint power allocation and adaptive random network coding in wireless multicast Networks," *IEEE Trans. Commun.*, vol. 66, no. 4, pp. 1520–1533, Apr. 2018.
- [12] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting fountain codes for secure wireless delivery," *IEEE Commun. Lett.*, vol. 18, no. 5, pp. 777–780, May 2014.
- [13] H. He and P. Ren, "Secure ARQ protocol for wireless communications: Performance analysis and packet coding design," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7158–7169, Aug. 2018.
- [14] L. Sun and H. Xu, "Fountain-coding-based secure communications exploiting outage prediction and limited feedback," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 740–753, Jan. 2019.
- [15] A. S. Khan and I. Chatzigeorgiou, "Opportunistic relaying and random linear network coding for secure and reliable communication," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 223–234, Jan. 2018.
- [16] T. Riihonen, S. Werner, and R. Wichman, "Optimized gain control for single-frequency relaying with loop interference," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2801–2806, Jun. 2009.
- [17] L. Sun, P. Ren, Q. Du, and Y. Wang, "Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 291–300, Feb. 2016.
- [18] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jun. 2014.