A Secure Hybrid Duplex Relay System with Adaptation of Finite Blocklength and Transmission Power

Jiahe Zhao*, Xu Zhu†, Yufei Jiang*, Zhongxiang Wei‡, and Xin Wan*
∗ School of Electronic and Information Engineering, Harbin Institute of Technology, Shenzhen, China
† School of Electrical Engineering and Electronics, University of Liverpool, Liverpool, UK
‡School of Electrical Engineering and Electronics, University College London, London, UK
Emails: 18s052119@stu.hit.edu.cn, xuzhu@liverpool.ac.uk, jiangyufei@hit.edu.cn,
zhongxiang.wei@ucl.ac.uk, 18s052112@stu.hit.edu.cn

***Abstract*—As mission-critical Internet of Things (MC-IoT) is expected to carry important and private information, its high quality of service (QoS) and high physical layer (PHY) security are indispensable. Nevertheless, most existing PHY security related work is built on the assumption of infinite blocklength, which is not applicable to finite blocklength (FBL) transmission, a typical scenario in MC-IoT such as factory automation. In this paper, we address the PHY security issue of a hybrid duplex relay aided MC-IoT system with FBL. Closed-form expressions for statistical secrecy throughput of full-duplex (FD) and half-duplex (HD) relay systems are derived, respectively, which are verified by numerical results. Based on the closed-form secrecy throughput, joint optimization of blocklength and transmission powers at source and relay is conducted for FD and HD relay systems, respectively. A hybrid duplex relaying scheme is also proposed by selecting the duplex mode with a higher achievable secrecy throughput. Numerical results show that, together with the hybrid relaying scheme, the proposed relay system with joint power allocation and blocklength adaptation, relay mode selection achieves much higher secrecy throughput over the conventional sole FD or HD mode relaying systems. Also, it is revealed that increasing blocklength or transmitting power may not always lead to a higher secrecy throughput and energy efficiency (EE).**

***Index Terms*—Physical layer security, secrecy throughput, statistical finite blocklength, hybrid duplex relay, mission-critical Internet of Things.**

I. Introduction

Due to the broadcast nature of wireless communications, eavesdropping inflicts an unprecedented vulnerability to cybercrime, and high level of security has become indispensable in mission-critical Internet of Things (MC-IoT). In order to improve the secrecy performance of MC-IoT system, physical layer (PHY) security is adopted as a complement to higher layer techniques, such as authentication and encryption [1].

This work was supported in part by the National Natural Science Foundation of China under Grants 61901138 and 61801145, in part by the Natural Science Foundation of Guangdong Province under Grants 2018A030313344 and 2018A030313298, in part by the Guangdong Science and Technology Planning Project under Grant 2018B030322004, and in part by Shenzhen Science and Technology Program under Grants JCYJ20180306171800589 and KQTD20190929172545139.

There has been extensive research on PHY security. The design principle is to utilize the intrinsic PHY randomness of wireless channels, such as channel fading and interference, to transmit data confidentially to legitimate users (LUs) while degrading the receiving quality of potential Eves. By preventing the signal detectability at Eves directly, it does not rely on limitations of Eves' computational resources.

In the past years, the related works have been conducted in the areas of beamforming design, artificial noise, cooperative jamming, and PHY key distribution. Also, there has been fruitful research on the analysis performance, such as secrecy throughput and outage probability. However, the most of the PHY security related works are built on the assumption of infinite blocklength, which may not be applicable to the communication networks that are characterized by finite blocklength (FBL) transmission, such as ultra-reliable and low-latency communications (URLLC). The achievable rate with finite blocklength was revealed in Gaussian channel [2], and later the authors in [3] further studied the capacity of finite blocklength in relaying systems, where security is not taken into account. To further investigate the security performance with finite blocklength transmission, the authors in [4] and [5] derived the tightest bounds of second-order coding rate in Gaussian wiretap channels. In [6], average secrecy throughput of MC-IoT system was investigated with a simple system configuration, where a transmitter communicates with an LU in the presence of an eavesdropper (Eve).

Nevertheless, there still are open challenges in securing FBL transmissions. 1) The existing FBL based PHY security work are presented with simple designs, such as solely optimizing the length of block with prefixed power allocation, or allocating transmission power with preset block length [6]. How to jointly optimize power allocation and block length adaptation is still unknown. 2) Also, the investigated scenarios are based the basic three-node setup, i.e., one transmitter, one LU and one Eve. Evidently, in MC-IoT networks, relaying is an important approach for assisting the weak link between transmitter and destinations, which helps alleviate the detrimental impact of high path loss (PL) and blockage [7]–[9].

Recently, full-duplex (FD) has attracted much attention, which has potential to double spectral efficiency by transmitting and receiving simultaneously in the same frequency band, compared with half-duplex (HD) [10]. However, FD system is subjected to undesired self-interference, and hence there has been extensive works on trading-off FD and HD, based on the self-interference cancellation performance by FD [11]–[13]. Also, the PHY security performance of relaying systems, especially with FBL transmission, is still unknown.

In this paper, we motivated by the aforementioned opening challenges, investigate secure FBL design in a wiretap MC-IoT hybrid duplex relay system, based on the information-theoretic bounds on finite-blocklength constraints. The main contributions of this work are summarized as follows.

1) The closed-form expressions of statistical secrecy throughputs of FD and HD relay systems in the FBL regime are derived, respectively, and verified by numerical results, to allow low-complexity system optimization towards high security and high QoS.
2) Based on the closed-form expressions of secrecy throughput derived, we propose a novel design that maximizes the secrecy throughput by jointly optimizing the blocklength as well as the transmission power at source and relay. Based on the optimized throughputs, we further propose an hybrid relaying mode, where the relay is enabled to switch between FD and HD mode for achieving higher secrecy throughput.
3) The inherent impact of blocklength on secrecy throughput and energy efficiency (EE) in the FBL regime is revealed: i) Increasing blocklength or transmitting power may not always lead to a higher secrecy throughput and EE. In particular, FD relaying mode needs a larger blocklength for achieving its optimal secrecy throughput and EE, compared to its HD counterpart. ii) For FD relaying mode, both secrecy throughput and EE performances are affected by the self-interference cancelation ability of FD, and HD relaying mode is preferable to FD relaying mode with a relatively weak self-interference cancelation ability.

The rest of the paper is organized as follows: In Section II, the system model of the investigated secure relaying system in FBL regime is presented. In Section III, we analyze the system with HD or FD relay and derived the closed-form expressions of secrecy throughput. In Section IV, we investigate the optimization method and a hybrid duplex scheme. In Section V the numerical simulations and performance comparison are presented and we conclude this study in Section VI.

II. System Model

A. Channel Model

We consider a wiretap MC-IoT relaying system where a decode-and-forward (DF) relay is deployed, as depicted in Fig. 1. There are five channels in the system: two legitimate channels from transmitter S to relay R and from R to legitimate receiver D: $h_{sr} = d_{sr}^{-\frac{\alpha}{2}} g_{sr}$, $h_{rd} = d_{rd}^{-\frac{\alpha}{2}} g_{rd}$,

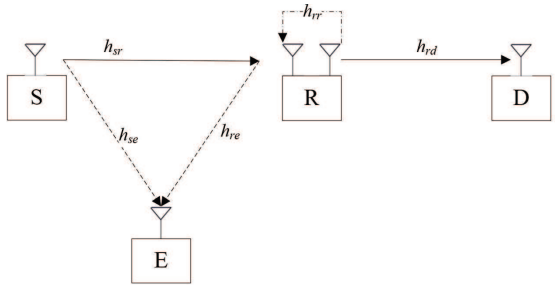


Fig. 1. A simplified secure relaying system with FBL transmission. The confidential communication between S and D is assisted by a relay node, under the presence of a passive Eve.

two eavesdropping channels from S to eavesdropper E and from R to E: $h_{se} = d_{se}^{-\frac{\alpha}{2}} g_{se}$, $h_{re} = d_{re}^{-\frac{\alpha}{2}} g_{re}$, and one self-interferencing channel for FD relay: $h_{rr} = \sigma_{rr} g_{rr}$, where α is the large scale path-loss exponent, for all $m \in \{s, r\}$ and $n \in \{r, d, e\}$, d_{mn} denotes the distance from m to n and g_{mn} is independent small-scale block fading and follows $\mathcal{CN}(0, 1)$. Assume there is no direct link between S and D, due to high PL or blockage in MC-IoT systems [11]. We assume that the CSI of legitimate channels and self-interferencing channel can be known by channel estimation, while only the Eve's CSI can only be statistically known [6].

We assume there are a total number of N time slots consisting of one blocklength, and N_{max} is the maximum tolerable blocklength. Let $s[i]$ denote the signal transmitted by the transmitter in the i-th $(i = 0, 1, ...N-1)$ time index. The information-bearing signal is written as $\mathbf{s} = [s[1]\ s[2]\ \cdots\ s[N]]$ with normalized power.

B. Signal to Interference Plus Noise Ratio Analysis of FD and HD Relaying

We now present signal to interference plus noise ratio (SINR) analysis for the FD and HD relayings, respectively.

1) FD relay: Write the transmitted signal at the i-th slot as $\mathbf{x}[i] = \sqrt{P_s}\mathbf{s}[i]$. Then the received signal at R is given

$$\mathbf{y}_{\mathrm{r}}^{\mathrm{FD}}[i] = h_{sr}\mathbf{x}_{\mathrm{s}}[i] + h_{rr}\mathbf{z}^{\mathrm{FD}}[i] + \mathbf{n}_{\mathrm{r}}[i], \tag{1}$$

where the forwarded signal $\mathbf{z}^{\mathrm{FD}}[i] = \sqrt{P_r}\mathbf{s}[i-1]$ acts the self-interference to the relay node, and $\mathbf{n}_{\mathrm{r}} \sim \mathcal{CN}(\mathbf{0}, \sigma_r^2\mathbf{I}_N)$ denotes the receive noise at the relay node.

The received signals at D and E at the i-th slot are given by

$$\mathbf{y}_{\mathrm{d}}^{\mathrm{FD}}[i] = h_{rd}\mathbf{z}^{\mathrm{FD}}[i] + \mathbf{n}_{\mathrm{d}}[i], \tag{2}$$

$$\mathbf{y}_{\mathrm{e}}^{\mathrm{FD}}[i] = h_{se}\mathbf{x}_{\mathrm{s}}[i] + h_{re}\mathbf{z}^{\mathrm{FD}}[i] + \mathbf{n}_{\mathrm{e}}[i], \tag{3}$$

where $\mathbf{n}_{\mathrm{d}}[i] \sim \mathcal{CN}(0, \sigma_d^2)$ and $\mathbf{n}_{\mathrm{e}}[i] \sim \mathcal{CN}(0, \sigma_e^2)$ denote the receive noise at the destination and relay, respectively. Based on the received signal, the SINR at the destination is written as $\gamma_d^{\mathrm{FD}} = \min\left\{\gamma_{rd}^{\mathrm{FD}}, \gamma_{sr}^{\mathrm{FD}}\right\}$, where $\gamma_{rd}^{\mathrm{FD}} = \frac{P_r d_{rd}^{-\alpha}}{\sigma_d^2} |g_{rd}|^2$ and $\gamma_{sr}^{\mathrm{FD}} = \frac{P_s d_{sr}^{-\alpha} |g_{sr}|^2}{\sigma_r^2 + P_r \sigma_{rr}^2 |g_{rr}|^2}$.

We now calculate the SINR at the Eve. The intercepting strategy of the Eve is to decode $s[i]$ from the S by successive

interference cancellation (SIC), and then at the $(i+1)$-th slot the Eve turns to decode $s[i]$ again from the relay node. Since the confidential signal $s[i]$ is decoded by the Eve twice, the SINR of Eve is written as $\gamma_e^{\mathrm{FD}} = \max\left\{\gamma_{se}^{\mathrm{FD}}, \gamma_{re}^{\mathrm{FD}}\right\}$, where $\gamma_{se}^{\mathrm{FD}} = \frac{P_s d_{se}^{-\alpha}}{\sigma_e^2}|g_{se}|^2$ and $\gamma_{re}^{\mathrm{FD}} = \frac{P_r d_{re}^{-\alpha}|g_{re}|^2}{\sigma_e^2 + P_s d_{se}^{-\alpha}|g_{se}|^2}$.

2) HD relay: When the relay works in HD mode, there is no self-interferece at the relay node, *e.g.* $\sigma_{rr} = 0$. For total N slots, the source and relay need two time slots for transmitting signal from the source to destination. Hence, assume $i_o = 2i-1, i_e = 2i$, and S transmits signal $\mathbf{x}[i_o] = \sqrt{P_s}\mathbf{s}[i_o]$ only at slot i_o. Hence, the received signals at R, D and E are given by

$$\mathbf{y}_{\mathrm{r}}^{\mathrm{HD}}[i_o] = h_{sr}\mathbf{x}_{\mathrm{s}}[i_o] + \mathbf{n}_{\mathrm{r}}[i_o], \tag{4}$$

$$\mathbf{y}_{\mathrm{d}}^{\mathrm{HD}}[i_e] = h_{rd}\mathbf{z}^{\mathrm{HD}}[i_e] + \mathbf{n}_{\mathrm{d}}[i_e], \tag{5}$$

$$\mathbf{y}_{\mathrm{e}}^{\mathrm{HD}}[i_o] = h_{se}\mathbf{x}_{\mathrm{s}}[i_o] + \mathbf{n}_{\mathrm{e}}[i_o], \tag{6}$$

$$\mathbf{y}_{\mathrm{e}}^{\mathrm{HD}}[i_e] = h_{re}\mathbf{z}[i_e] + \mathbf{n}_{\mathrm{e}}[i_e], \tag{7}$$

where the forwarded signal by the HD relay is given as $\mathbf{z}^{\mathrm{HD}}[i_e] = \sqrt{P_r}\mathbf{s}[i_o]$. Then the SINRs of legitimate and wiretap channels are given as $\gamma_d^{\mathrm{HD}} = \min\left\{\gamma_{rd}^{\mathrm{HD}}, \gamma_{sr}^{\mathrm{HD}}\right\}$ and $\gamma_e^{\mathrm{HD}} = \max\left\{\gamma_{se}^{\mathrm{HD}}, \gamma_{re}^{\mathrm{HD}}\right\}$ respectively, where $\gamma_{mn}^{\mathrm{HD}} = \frac{P_m d_{mn}^{-\alpha}}{\sigma_n^2}|g_{mn}|^2$, $mn \in \{sr, rd, se, re\}$.

III. Statistical Analysis of Secrecy Throughput

In this section, the closed-form expressions of the secrecy throughput for FD and HD relay systems are derived. Before we present the secrecy throughput performance, we have to first calculated the block error rate probability (BLEP). Denote B as the number of total information bits during N slots time. Then the first-order approximation for block error probability (BLEP) [6] calculated as the function of SINR as

$$\epsilon_{\gamma_d|\gamma_e}(\gamma) \approx \begin{cases} 1, & \gamma < \gamma_m, \\ \frac{1}{2} - a\left(\gamma - \gamma_0\right), & \gamma_m \le \gamma \le \gamma_M, \\ 0, & \gamma > \gamma_M, \end{cases} \tag{8}$$

where $\gamma_m = -\frac{1}{2a} + \gamma_0$, $\gamma_M = \frac{1}{2a} + \gamma_0$, $\gamma_0 = \exp\left\{\frac{V_e}{N}Q^{-1}(\delta) + \frac{B}{N}\ln 2\right\}(1+\gamma_e) - 1$, $a = \sqrt{\frac{N}{2\pi\gamma_0(\gamma_0+2)}}$. In particular, δ is the *information leakage*, which measures information leakage probability. $Q^{-1}(\cdot)$ is the inverse function of complementary cumulative distribution function (CCDF) of standard Gaussian distribution $Q(t) = \int_t^\infty \exp(-x^2/2)\,dx$ [5], $V_e = 1 - (1+\gamma_e)^{-2}$. γ_d and γ_e are the received SINR at receiver or eavesdropper respectively.

A. Secrecy Throughput with FD Relaying

When relay R works in FD mode, we get the average secrecy throughput as

$$T^{\mathrm{FD}} = \frac{B}{N}\left(1 - \mathbb{E}_{\gamma_d,\gamma_e}\epsilon^{\mathrm{FD}}\right). \tag{9}$$

where $\mathbb{E}_{\gamma_d,\gamma_e}\epsilon^{\mathrm{FD}}$ denotes the expectation of BLER with respect to the SINR of the destination γ_d and Eve γ_e. To obtain the value of $\mathbb{E}_{\gamma_d,\gamma_e}\epsilon^{\mathrm{FD}}$, we first calculate the cumulative distribution function (CDF) of the SINR γ_d and γ_e as

$$F_{\gamma_d^{\mathrm{FD}}}(x) = 1 - \frac{P_s d_{sr}^{-\alpha}}{P_s d_{sr}^{-\alpha} + P_r\sigma_{rr}^2 x}\exp\left\{-x\left(\frac{\sigma_r^2}{P_s d_{sr}^{-\alpha}} + \frac{\sigma_d^2}{P_r d_{rd}^{-\alpha}}\right)\right\}, \tag{10}$$

$$F_{\gamma_e^{\mathrm{FD}}}(y) = 1 - \exp\left\{-\frac{\sigma_e^2 y}{P_s d_{se}^{-\alpha}}\right\} - \frac{P_r d_{re}^{-\alpha}}{P_r d_{re}^{-\alpha} + y P_s d_{se}^{-\alpha}} \cdot \left(\exp\left\{-\frac{\sigma_e^2 y}{P_s d_{se}^{-\alpha}}\right\} - \exp\left\{\frac{\sigma_e^2}{P_s d_{se}^{-\alpha}}y + \frac{\sigma_e^2}{P_r d_{re}^{-\alpha}}\left(y + y^2\right)\right\}\right). \tag{11}$$

Since γ_d and γ_e are independent, we have

$$\mathbb{E}_{\gamma_d,\gamma_e}\epsilon^{\mathrm{FD}} = \int_{-\infty}^{+\infty}\Theta^{\mathrm{FD}}(y)\, f_{\gamma_e}(y)dy, \tag{12}$$

and

$$\begin{aligned}\Theta^{\mathrm{FD}}(y) &= \int_{-\infty}^{+\infty} f_{\gamma_d}(x)\,\epsilon^{\mathrm{FD}}(x,y)\,dx, \\ &\approx \int_{\gamma_m}^{\gamma_M} a F_{\gamma_d}(x)\,dx, \\ &= 1 - \frac{a e^{\tilde{\omega}_1} P_s d_{sr}^{-\alpha}}{P_r\sigma_{rr}^2}\left[E_1(\tilde{\omega}_1\tilde{x}_m) - E_1(\tilde{\omega}_1\tilde{x}_M)\right],\end{aligned} \tag{13}$$

where $E_1(x) = \int_x^{+\infty}\frac{e^{-t}}{t}dt$ is an exponential integral, $f_{\gamma_d}(y)$ and $f_{\gamma_e}(y)$ are the probability distribution function (PDF) of γ_d and γ_e respectively, $\tilde{\omega}_1 = \frac{P_s d_{sr}^{-\alpha}}{P_r\sigma_{rr}^2}\left(\frac{\sigma_r^2}{P_s d_{sr}^{-\alpha}} + \frac{\sigma_d^2}{P_r d_{rd}^{-\alpha}}\right)$, $\tilde{x}_m = \frac{P_s d_{sr}^{-\alpha}}{P_r\sigma_{rr}^2}\gamma_m + 1$, and $\tilde{x}_M = \frac{P_s d_{sr}^{-\alpha}}{P_r\sigma_{rr}^2}\gamma_M + 1$.

Let $\mathcal{A}^{\mathrm{FD}}(y) = a\left[E_1(\tilde{\omega}_1\tilde{x}_m) - E_1(\tilde{\omega}_1\tilde{x}_M)\right] f_{\gamma_e}(y)$, and M_1 is a large number that guarantees $\int_{M_1}^{+\infty}\mathcal{A}^{\mathrm{FD}}(y)dy \approx 0$. By applying Gaussian-Chebyshev quadrature to the integral term above and substituting it into (9), we finally obtain the closed-form expression of the secrecy throughput as

$$T^{\mathrm{FD}} \approx \frac{\pi e^{\tilde{\omega}_1} B M_1 P_s d_{sr}^{-\alpha}}{2\rho_{rr} N M_2 P_r\sigma_{rr}^2}\sum_{n=1}^{M_2}\sqrt{1-z_n^2}\,\mathcal{A}^{\mathrm{FD}}\left(\frac{M_1}{2}(z_n+1)\right), \tag{14}$$

where $z_n = \cos\left(\frac{2n-1}{2M_2}\pi\right)$, M_2 is a positive integer which is related to the accuracy of Gaussian-Chebyshev quadrature.

B. Secrecy Throughput with HD Relaying

Similarly, we get the average secrecy throughput as

$$T^{\mathrm{HD}} = \frac{B}{2N}\left(1 - \mathbb{E}_{\gamma_d,\gamma_e}\epsilon^{\mathrm{HD}}\right). \tag{15}$$

With the exponentially distributed variables $\gamma_{rd}^{\mathrm{HD}}$, $\gamma_{sr}^{\mathrm{HD}}$, $\gamma_{se}^{\mathrm{HD}}$ and $\gamma_{re}^{\mathrm{HD}}$, we can calculate the CDF of γ_d^{HD} as:

$$F_{\gamma_d^{\mathrm{HD}}}(x) = 1 - \exp\left\{-\tilde{\omega}_2 x\right\}, \tag{16}$$

where $\tilde{\omega}_2 = \frac{\sigma_d^2}{P_r d_{rd}^{-\alpha}} + \frac{\sigma_r^2}{P_s d_{sr}^{-\alpha}}$ and the PDF of γ_e in is:

$$f_{\gamma_e^{\mathrm{HD}}}(y) = \frac{\sigma_e^2}{P_r e_{rd}^{-\alpha}}\exp\left\{-\frac{\sigma_e^2}{P_r e_{rd}^{-\alpha}}y\right\} + \frac{\sigma_e^2}{P_s d_{se}^{-\alpha}}\exp\left\{-\frac{\sigma_e^2}{P_s d_{se}^{-\alpha}}y\right\} - \left(\frac{\sigma_e^2}{P_r e_{rd}^{-\alpha}} + \frac{\sigma_e^2}{P_s d_{se}^{-\alpha}}\right)\exp\left\{\left(\frac{\sigma_e^2}{P_r e_{rd}^{-\alpha}} + \frac{\sigma_e^2}{P_s d_{se}^{-\alpha}}\right)y\right\}, \tag{17}$$

The expectation of BLEP in (15) is

$$\mathbb{E}_{\gamma_d,\gamma_e}\epsilon^{\mathrm{HD}} \approx \int_{-\infty}^{+\infty} \Theta^{\mathrm{HD}}(y)\, f_{\gamma_e}(y) dy, \tag{18}$$

and

$$\Theta^{\mathrm{HD}}(y) = \int_{-\infty}^{+\infty} f_{\gamma_d}(x)\, \epsilon^{\mathrm{HD}}(x,y)\, dx, \tag{19}$$

$$\approx \int_{\gamma_m}^{\gamma_M} a F_{\gamma_d}(x)\, dx, \tag{20}$$

$$= 1 - \frac{a}{\tilde{\omega}_2}\left(e^{-\tilde{\omega}_2\gamma_m} - e^{-\tilde{\omega}_2\gamma_M}\right). \tag{21}$$

Denoting $\mathcal{A}^{\mathrm{HD}}(y) = a\left(e^{-\tilde{\omega}_2\gamma_m} - e^{-\tilde{\omega}_2\gamma_M}\right) f_{\gamma_e}(y)$ and leaveraging Gaussian-Chebyshev quadrature, we have

$$T^{\mathrm{HD}} \approx \frac{\pi B M_1}{4\tilde{\omega}_2 N M_2} \sum_{n=1}^{M_2} \sqrt{1-z_n^2}\, \mathcal{A}^{\mathrm{HD}}\left(\frac{M_1}{2}(z_n+1)\right), \tag{22}$$

which serves the closed-form expression of secrecy throughput when an HD relay is selected.

IV. Joint Optimization to Transmission Power and Blocklength and Hybrid Duplex Mode Selection

A. Problem Formulation

There are three parameters that system designer could operate to improve secrecy throughtput, namely $\boldsymbol{\Xi} = [P_s\ P_r\ N]$ in two different modes, HD or FD. The optimization problem can be written as

$$\mathbf{P1}: \max_{\boldsymbol{\Xi}} T^{\xi}, \tag{23a}$$

$$\text{s.t. } C1: P_{total}^{\xi} \le P_{max}, \tag{23b}$$

$$C2: \boldsymbol{\Xi} \succeq \mathbf{0}, \tag{23c}$$

$$C3: N \le N_{max}, \tag{23d}$$

$$C4: N \text{ is an positive integer}, \tag{23e}$$

where ξ denotes the mode of FD or HD, N_{max} is the maximum tolerable blocklength, and P_{total}^{ξ} is the total power consumed in ξ duplex relaying system.

B. Joint Optimization of Transmission Power of Source P_s, Transmission Power of Relay P_r, and Blocklength N

Since the considered problem $\mathbf{P1}$ is quasi-concave with respect to P_s, P_r and N, the problem is able to be transformed into a series of convex feasibility problems [14].

Denote T_{opt}^{ξ} as the optimal secrecy throughput in (23a), and $t \in \mathcal{R}$ be an arbitrary preset value. If the following convex problem

$$\mathbf{P2}: \min_{\boldsymbol{\Xi}} P_{total}^{\xi}, \tag{24a}$$

$$\text{s.t. } C0: T^{\xi} \ge t, \tag{24b}$$

$$C2, C3 \tag{24c}$$

where constraint $C1$ and $C4$ are removed. Hence, we can solve the convex optimization $\mathbf{P2}$ and check if the optimal result satisfies constraint $C1$ or not. If it is true, it means $T_{opt}^{\xi} \ge t$, or $T_{opt}^{\xi} < t$.

In a nutshell, for solving $\mathbf{P2}$, a standard convex problem, it can be readily solved with strict convergence. By updating the value of t with bisection method, the final value of t can be converged, which is summerized in Algorithm 1.

Algorithm 1 Bisection Search Method for Solving $\mathbf{P2}$ with HD or FD Relay

1: **initialize:** For the assumed optimal solution T_{opt}^{ξ}; lower bound $l = 0$; upper bound u satisfing $u > T_{opt}^{\xi}$; and accuracy tolerance $\varepsilon > 0$;
2: **repeat**
3: $t = (l+u)/2$;
4: Solve $\mathbf{P2}$, and obtain the minimized $P_{total}^{\xi *}$ with the corresponding $\boldsymbol{\Xi}^*$,
5: **if** $P_{total}^{\xi} \le P_{max}$ **then**
6: $l = t$;
7: **else**
8: $u = t$;
9: **until** $u - l < \varepsilon$.
10: The optimal variable $\boldsymbol{\Xi}^*$ at the last loop is obtained.

C. Hybrid Duplex Mode Selection

Based on the optimaization process above, we propose an hybrid duplex scheme. Firstly, the Algorithm 1 is used with a particular duplex mode, $\xi =$ HD or FD. Secondly, recalling the constraint $C4$ that is neglected, blocklength N has to be an integer. We choose N from $N_1 = \lceil N^{\xi *} \rceil$ and $N_2 = \lfloor N^{\xi *} \rfloor$, where $N^{\xi *}$ is the optimal blocklength by Algorithm 1, and decide the one leading a larger T^{ξ} as the blocklength. Finally, the maximum throughput can be found by comparing two duplex modes, where we set the optimal secrecy throughput T and the corresponding parameters $\boldsymbol{\Xi}^*$ as

$$T = \max_{\boldsymbol{\Xi}} \left\{ T^{\mathrm{HD}*}, T^{\mathrm{FD}*} \right\}, \tag{25}$$

$$\boldsymbol{\Xi}^* = \arg\max_{\boldsymbol{\Xi}} T. \tag{26}$$

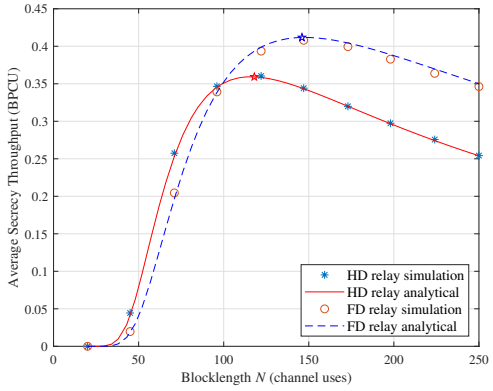


Fig. 2. Impact of blocklength on analytical and numerical optimized secrecy throughputs of FD and HD relay systems.

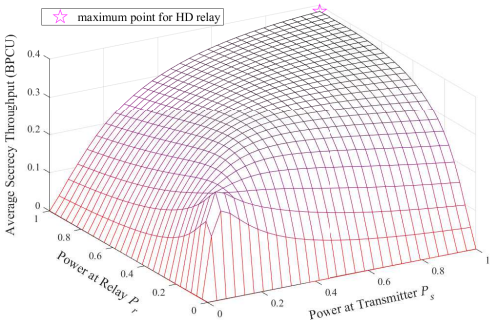


Fig. 3. Optimization impacted by power of source P_s and power of relay P_r, with HD relay aiding and $N = N_{opt}^{\mathrm{HD}}$.

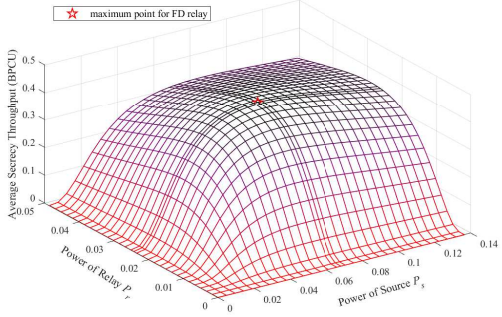


Fig. 4. Optimization impacted by power of source P_s and power of relay P_r, with FD relay aiding and $N = N_{opt}^{\mathrm{FD}}$.

V. Numerical Results

In this section, system performance is presented by Monte-Carlo simulations. The following setups are adopted. The distances among transmitter, relay, legitimate receiver and eavesdropper are $d_{sr} = d_{rd} = 10$, $d_{re} = 20$, $d_{se} = 10\sqrt{5}$. The path-loss exponent $\alpha = 4$. Maximum power constraint $P_{max} = 1$. The variances of noise are $\sigma_r^2 = \sigma_d^2 = \sigma_e^2 = -60\mathrm{dB}$, and that of self-interference $\sigma_{rr}^2/\sigma_r^2 = 20dB$. The amount of information in one block is $B = 200$. And the information leakage is $\delta = 10^{-2}$.

In Fig. 2-4, we verify the accuracy of the closed-form expressions and the optimization results by jointly optimizing power and blocklength parameters in HD and FD relaying system. It is observed in Fig. 2 that the closed-form expressions of statistical secrecy throughput for FD and HD relaying approach the real secrecy throughput, and there exists an optimal point that maximizes average secrecy throughput, which vertifies the accuracy of the proposed closed-form expressions. Also, Fig. 3 and Fig. 4 demonstrates the validity of the proposed optimization method. In Fig. 2-4, the pentagram points depict the value of secrecy throughput and the corresponding power P_s, P_r and blocklength N, with relay working in different duplex mode.

In Fig. 5, the impact of information leakage on the secrecy

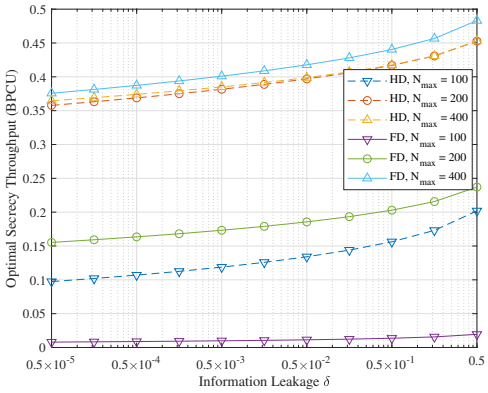


Fig. 5. The optimal throughput versus information leakage δ with HD and FD relay on various blocklength constraint N_{max}, when the amount of information per block is $B = 400\ bits$.

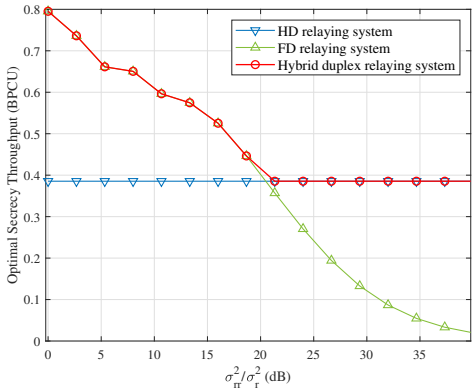
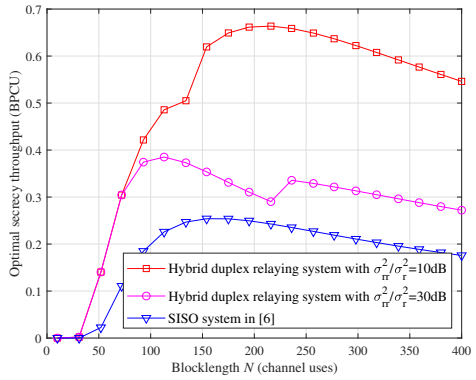


Fig. 6. The optimal secrecy throughput versus the ratio of σ_{rr}^2 to σ_r^2, when relay is working in HD, FD or hybrid duplex mode.

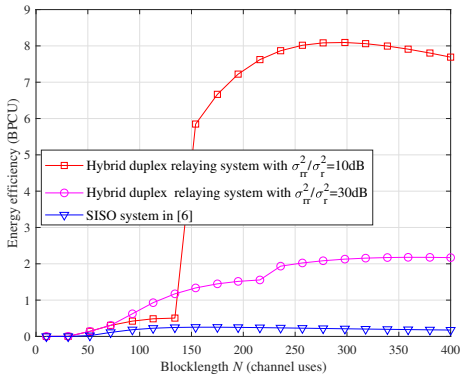
throughput is presented. We find that as δ increases, both the tolerance for information leakage and secrecy throughput increase. When relay works in HD mode, the impact of N_{max} is less significant on throughput and hence the influence of N_{max} decreases gradually with the increase of N_{max}. However, when relay works in FD mode, the influence caused by the increase of N_{max} is more pronounced, which proves that FD relaying system requires larger blocklength to reach the maximum secrecy throughput.

In Fig. 6, we compare the effects of self-interference on the secrecy performance under two different duplex modes, HD and FD. In such system, we have optimized multiple systems with different self-interference strengths. As the power of self-interference increases, the performance of the FD relay system is reduced, while the performance of the HD relay system remains unchanged. Hence by the proposed hybrid duplex system, it is able to adaptively select the duplex mode that leads to a higher secrecy throughput.

Moreover, we compare the performance of proposed hybrid duplex scheme with MC-IoT communication system in [6]. The benchmark consists of one access point (AP), one actu-



(a)



(b)

Fig. 7. (a) The optimal secrecy throughput and (b) energy efficiency versus the blocklength N.

ator equipped with a single antenna, and one eavesdropper equipped with a single antenna. For fair comparison, we remove the relay from current system, and then substitute the corresponding parameters into this benchmark.

In Fig. 7, the impact of blocklength on the secrecy throughput and EE is demonstrated. EE is defined as the ratio of throughput to total power consumed. In this figure, it is observed that the proposed hybrid duplex scheme at least doubles the secrecy throughput over the SISO systems, even when the ability of self-interference cancellation is weak. In terms of EE, it is found that EE is higher than that of SISO system. It is interesting that EE of hybrid duplex scheme with $\sigma_{rr}^2/\sigma_r^2 = 10dB$ grows rapidly when N exceeds a certain threshold. The reason is that when the size of blocklength is small, the hybrid duplex scheme tends to consume all transmission power in order to maximize secrecy throughput. On the other hand, when blocklenghth is larger than the threshold the optimal power consumption will decrease rapidly, which leads to higher EE. Moreover, with $\sigma_{rr}^2/\sigma_r^2 = 30dB$, it is found that although the secrecy throughput is relatively lower than the case when self-interference is low and $50 < N < 150$, the EE is higher, which proves that when self-interference intensity is higher, the power consumption in hybrid duplex scheme will be lower.

VI. Conclusion

In this paper, we have analyzed the hybrid duplex relay MC-IoT system, where the relay may adaptively choose duplex mode between HD and FD mode in finite blocklength regime. Specifically, we have derived the closed-form expressions of statistical secrecy throughput. Based on the derived closed-form expressions, a novel optimization problem is formulated to jointly allocate transmission power at source, transmission power at relay, and blocklength to maximize the statistical secrecy throughput. The tightness of the closed-form expressions has been proved, and the performance of the proposed optimization algorithm has been demonstrated. Compared to conventional sole-FD or HD relaying and SISO systems, the proposed algorithm achieves a higher secrecy throughput and EE performance, and is robust to the self-interference cancellation ability. A promising direction in future is to to expand the application scope of the proposed scheme, such as deploying relay arrays and multi-antenna relays.

References

[1] Z. Wei, C. Masouros, F. Liu, S. Chatzinotas, and B. Ottersten, "Energy- and cost-efficient physical layer security in the era of IoT: The role of interference," *IEEE Commun. Mag.*, vol. 58, no. 4, pp. 81–87, Apr. 2020.

[2] W. Yang, G. Durisi, T. Koch, and Y. Polyanskiy, "Quasi-static multiple-antenna fading channels at finite blocklength," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 4232–4265, Jul. 2014.

[3] Y. Hu, J. Gross, and A. Schmeink, "On the capacity of relaying with finite blocklength," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1790–1794, Mar. 2016.

[4] W. Yang, R. F. Schaefer, and H. V. Poor, "Finite-blocklength bounds for wiretap channels," in *Proc. 2016 IEEE International Symposium on Information Theory (ISIT)*, Barcelona, 2016, pp. 3087–3091.

[5] W. Yang, R. F. Schaefer, and H. V. Poor, "Secrecy-reliability tradeoff for semi-deterministic wiretap channels at finite blocklength," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Aachen, Jun. 2017, pp. 2133–2137.

[6] H. Wang, Q. Yang, Z. Ding, and H. V. Poor, "Secure short-packet communications for mission-critical IoT applications," *IEEE Trans. Wirel. Commun.*, vol. 18, no. 5, pp. 2565–2578, May. 2019.

[7] C. Wang, H. Wang, D. W. K. Ng, X. Xia, and C. Liu, "Joint beamforming and power allocation for secrecy in peer-to-peer relay networks," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 6, pp. 3280–3293, Jun. 2015.

[8] Y. Zou, J. Zhu, X. Wang, and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[9] K. Shamganth and M. J. N. Sibley, "A survey on relay selection in cooperative device-to-device (D2D) communication for 5G cellular networks," in *Proc. International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Aug. 2017, pp. 42–46.

[10] Z. Kong, S. Yang, D. Wang, and L. Hanzo, "Robust beamforming and jamming for enhancing the physical layer security of full duplex radios," *IEEE Trans. Inf. Forensic Secur.*, vol. 14, no. 12, pp. 3151–3159, Dec. 2019.

[11] H. He, P. Ren, Q. Du, and L. Sun, "Full-duplex or half-duplex? Hybrid relay selection for physical layer secrecy," in *Proc. IEEE 83rd Vehicular Technology Conference (VTC Spring)*, Nanjing, May. 2016, pp. 1–5.

[12] H. Wang, B. Zhao, and T. Zheng, "Adaptive full-duplex jamming receiver for secure D2D links in random networks," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1254–1267, Feb. 2019.

[13] T. Zheng, H. Wang, J. Yuan, Z. Han, and M. H. Lee, "Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy," *IEEE Trans. Wirel. Commun.*, vol. 16, no. 6, pp. 3827–3839, Jun. 2017.

[14] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.