sensors

MDPI

Article

Performance Analysis of Wireless Information Surveillance in Machine-Type Communication at Finite Blocklength Regime

Ruonan Dong, Baogang Li * and Binyang Yan

Department of Electronic and Communication Engineering, North China Electric Power University, No. 619, Yong Hua Street, Baoding 071003, China

* Correspondence: baogangli@ncepu.edu.cn; Tel.: +86-137-2223-1981

Received: 11 May 2019; Accepted: 6 July 2019; Published: 9 July 2019

Abstract: The Internet of Things (IoT) will feature pervasive sensing and control capabilities via the massive deployment of machine-type communication devices in order to greatly improve daily life. However, machine-type communications can be illegally used (e.g., by criminals or terrorists) which is difficult to monitor, and thus presents new security challenges. The information exchanged in machine-type communications is usually transmitted in short packets. Thus, this paper investigates a legitimate surveillance system via proactive eavesdropping at finite blocklength regime. Under the finite blocklength regime, we analyze the channel coding rate of the eavesdropping link and the suspicious link. We find that the legitimate monitor can still eavesdrop the information sent by the suspicious transmitter as the blocklength decreases, even when the eavesdropping is failed under the Shannon capacity regime. Moreover, we define a metric called the effective eavesdropping rate and study the monotonicity. From the analysis of monotonicity, the existence of a maximum effective eavesdropping rate for a moderate or even high signal-to-noise (SNR) is verified. Finally, numerical results are provided and discussed. In the simulation, we also find that the maximum effective eavesdropping rate slowly increases with the blocklength.

Keywords: wireless information surveillance; proactive eavesdropping; finite blocklength; channel coding rate; IoT; machine-type communication

1. Introduction

The vision of the Internet of Things (IoT) promises to bring wireless connectivity to anything ranging from tiny static sensors to vehicles and unmanned aerial vehicles (UAVs) [1–3]. Meanwhile, short packets are the typical form of traffic generated by sensors and exchanged in machine-type communications [4]. In these scenarios, the Shannon capacity, which assumes the infinite blocklength, is no longer achievable. In comparison to the Shannon capacity regime, reference [5] developed a pioneering framework and identified a tight bound of the channel coding rate at the finite blocklength regime, which presents many new research opportunities with a wide range of applications.

The IoT can offer many benefits for daily life; however, machine-type communications, such as vehicle to vehicle communication and UAV communication among others, can be illegally used (e.g., by criminals or terrorists), which is difficult to monitor, thus presenting new challenges with respect to public security [6]. Thus, legitimate eavesdropping by legitimate parties should be necessary to effectively discover and prevent the information transmitted between the suspicious users. Further, proactive eavesdropping has recently attracted much interest in research as an approach to improve eavesdropping performance.

1.1. Related Works

Conventional wireless security studies generally assume wireless communication is rightful, i.e., the eavesdropper is treated as an adversary, and aim to preserve their confidentiality and prevent malicious eavesdropping [7,8]. In the presence of a malicious eavesdropper, the network of point-to-point [7], relaying [8,9], multi-user [10,11], and cognitive radio [12] were investigated. In contrast, legitimate eavesdropping or wireless information surveillance is a paradigm shift of wireless security, where the monitor is regarded as a legitimate eavesdropper.

In general, there are two approaches for wireless information surveillance, including passive eavesdropping and proactive eavesdropping. With passive eavesdropping, the legitimate monitor only listens to the wireless channels of the suspicious users. This approach can't change the eavesdropping performance. However, proactive eavesdropping can generally improve the eavesdropping performance via jamming or relaying. Note that there is not much research on the legitimate proactive eavesdropping in the literature, where the legitimate monitor eavesdrops a single suspicious link [13–21], multiple suspicious links [22,23], or a suspicious relaying link [24–26]. A legitimate surveillance scenario where a legitimate monitor aimed to eavesdrop a point-to-point suspicious communication link via jamming [13] and cognitive jamming [14,15] was investigated, and the eavesdropping rate at the legitimate monitor was studied. In [16], the author studied the legitimate surveillance system consisting of two legitimate monitors. In [17,18], the legitimate monitor was equipped with multiple antennae and acted as a fake relay to eavesdrop the suspicious transmitter–receiver pair. In [19–21], the author studied a new spoofing approach to change the communicated information of the suspicious link. The work in [22] investigated the wireless surveillance of multiple suspicious links, and maximized weighted sum eavesdropping rate of multiple suspicious links. The work in [23] studied the wireless surveillance of multiple suspicious communication links and proposed a cooperative eavesdropping scheme. The eavesdropping rate [24], the eavesdropping mode [25], and the eavesdropping non-outage probability [26] were studied where the legitimate monitor aims to eavesdrop a suspicious relaying communication link.

1.2. Contributions and Organizations

As a common point, all the above studies are under the Shannon capacity regime, where the length of the block is assumed to be infinite. The Shannon capacity is not achievable when the information transmitted in short packets. To our best knowledge, there is no research on the legitimate proactive eavesdropping under the finite blocklength regime. Therefore, this paper analyzes the performance of a legitimate surveillance system via proactive eavesdropping at the finite blocklength regime. In the system, there is a suspicious transmitter-receiver pair, which may be two stationary UAVs etc, and a legitimate monitor. The legitimate monitor operates in a full-duplex mode with simultaneous information reception and relaying. The main contributions are summarized as follows.

In this paper, under the finite blocklength regime, we analyze the channel coding rate of the eavesdropping link and the suspicious link. Meanwhile, we find that the legitimate monitor can still eavesdrop the information sent by the suspicious transmitter as the blocklength decreases, even when the eavesdropping is failed under the Shannon capacity regime. Moreover, we define a metric called the effective eavesdropping rate and analyze the monotonicity. From the analysis of monotonicity, the existence of a maximum effective eavesdropping rate for moderate or even high signal-to-noise (SNR) is verified. Finally, numerical results are provided and discussed. In the simulation, we also find that the maximum effective eavesdropping rate slowly increases with the blocklength, and the increment is almost negligible when the blocklength reaches a relatively large value.

The rest of this paper is organized as follows. The system model and assumptions are described in Section 2. Section 3 analyzes the performance of the legitimate surveillance system at finite blocklength. Numerical results are presented in Section 4. Finally, the paper is concluded in Section 5.

2. System Model and Assumptions

As shown in Figure 1, we consider a legitimate surveillance system consisting of a suspicious transmitter-receiver pair (i.e., *S*-*D*) and a full-duplex legitimate monitor *E*. *S* transmits information to *D* during n channel uses, in this way, we consider that each block spans over n channel uses. We assume that both *S* and *D* are unaware of the presence of *E* and the decode-and-forward (DF) relaying is adopted by *E*. If *E* decodes the block received from *S* successfully, it forwards the block to *D*, which aims to enhance eavesdropping the suspicious link. *S* and *D* are each equipped with a single antenna, and *E* is equipped with two antennae, one for eavesdropping (receiving) and the other for relaying (transmitting). *S* can adaptively adjust its transmission rate. The self-interference from the relaying antenna to the eavesdropping antenna at the legitimate monitor is assumed to be perfectly cancelled by using advanced analog and digital self-interference cancellation methods [13]. DF can be assumed here as in [8,27]. In addition, *E* can act as a fake relay and thus obtain the channel state information and the symbol format of the suspicious link, and synchronize with *S* and *D* [19,20].

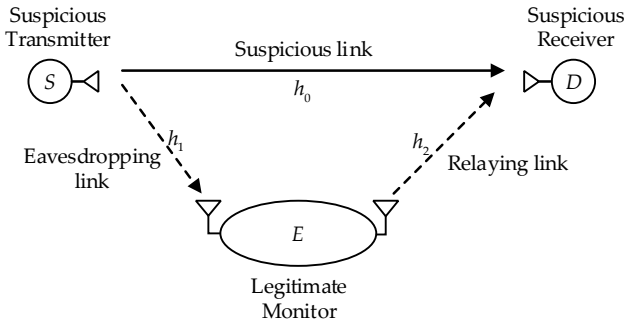

Figure 1. System model of the considered legitimate surveillance system.

We consider a Rayleigh quasi-static block-fading channel [28], where fading process is considered to be constant over the transmission of a block and independently and identically distributed from block to block. Let h_0, h_1 and h_2 denote channel coefficients from the suspicious transmitter to the suspicious receiver, from the suspicious transmitter to the eavesdropping antenna of the legitimate monitor, and from the relaying antenna of the legitimate monitor to the suspicious receiver, respectively. The corresponding channel gains are defined as $g_0 = |h_0|^2$, $g_1 = |h_1|^2$ and $g_2 = |h_2|^2$. In addition, we assume that *E* perfectly knows the channel state information of all links, which can be obtained by utilizing the methods given in the literature [14,17,19,20].

Channel Coding Rate for Finite Blocklength

For a given decoding error probability ε, the channel coding rate R (in bits per channel use) with blocklength n is [28,29]

$$R = C - \sqrt{\left(1 - 1/(1+\gamma)^2\right)/n} \cdot Q^{-1}(\varepsilon) \log_2 e \tag{1}$$

where $Q^{-1}(.)$ is the inverse Q-function and as usual the Q-function is given by $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-t^2/2} dt$. In addition, $C = \log_2(1+\gamma)$ is Shannon capacity function of the SNR γ. Note that Equation (1) is a very tight approximation when $n \geq 100$, i.e., the difference from the exact value can be neglected [28,29]. Thus, we consider $n \geq 100$ in this paper and use equal sign in Equation (1). Based on the above results, R can be transformed into

$$R = C - \sqrt{(1 - 2^{-2C})/n} \cdot Q^{-1}(\varepsilon) \log_2 e \tag{2}$$

Equivalently, for a given channel coding rate R, the decoding error probability ε can be given by

$$\varepsilon = Q\left(\frac{C-R}{\sqrt{\left(1-1/(1+\gamma)^2\right)/n}\cdot\log_2 e}\right) = Q\left(\frac{C-R}{\sqrt{(1-2^{-2C})/n}\cdot\log_2 e}\right) \tag{3}$$

3. Performance at Finite Blocklength

In this section, under the finite blocklength regime, we first analyze the performance of the legitimate surveillance system in terms of the channel coding rate of the eavesdropping link and the suspicious link in comparison with the Shannon capacity regime. Afterwards, we define a metric called the effective eavesdropping rate and analyze the monotonicity. From the analysis of monotonicity, the existence of a maximum effective eavesdropping rate for moderate or even high SNR is also verified.

3.1. Analysis of Channel Coding Rate

According to Equation (2), the channel coding rate of the eavesdropping link can be obtained as

$$R_E = C_E - \sqrt{(1-2^{-2C_E})/n}\cdot Q^{-1}(\varepsilon_E)\log_2 e \tag{4}$$

where $C_E = \log_2(1+\gamma_E)$, $\gamma_E = g_1P_1/{\sigma_E}^2$ is the SNR at E, P_1 is the transmit power at S, ${\sigma_E}^2$ is the power of noise at E, and ε_E is the decoding error probability at E. Likewise, the effective channel coding rate of the suspicious link can be obtained as

$$R_D = C_D - \sqrt{(1-2^{-2C_D})/n}\cdot Q^{-1}(\varepsilon_D)\log_2 e \tag{5}$$

where $C_D = \log_2(1+\gamma_D)$, $\gamma_D = (g_0P_1+g_2P_2)/{\sigma_D}^2$ is the effective SNR at D, P_2 is the transmit power at E, ${\sigma_D}^2$ is the power of noise at D, and ε_D is the decoding error probability at D. E can act as a fake relay and alter the effective channel of the suspicious link from S to D [17]. Thus, we use effective channel coding rate, which includes the suspicious link and the relaying link. ε_D results from the error probability of each link and is given by

$$\varepsilon_D = \varepsilon_0[\varepsilon_E + (1-\varepsilon_E)\varepsilon_2] \tag{6}$$

where ε_0 and ε_2 are the decoding error probabilities of the suspicious link and the relaying link, respectively.

Since $(1-\varepsilon_E)(1-\varepsilon_2) \geq 0$, it is straightforward to know that $\varepsilon_E + \varepsilon_2 - \varepsilon_E\varepsilon_2 \leq 1$. Thus, we immediately have $\varepsilon_D \leq \varepsilon_0$. Besides we consider that $\varepsilon_E \geq \varepsilon_2$, in this way, we have $\varepsilon_D = \varepsilon_0\varepsilon_E(1-\varepsilon_2) + \varepsilon_0\varepsilon_2 \leq \varepsilon_0\varepsilon_E + \varepsilon_0\varepsilon_2 \leq 2\varepsilon_0\varepsilon_E$. In summary, we can obtain as follows

$$\varepsilon_D \leq \varepsilon_0 \cdot \min\{2\varepsilon_E, 1\} \tag{7}$$

It can be known that $Q(x) < 0.5$ when $x > 0$. So according to Equation (3), $\varepsilon < 0.5$. In this way, we immediately have $\varepsilon_E < 0.5$. Thus, we can derive $\varepsilon_D < \varepsilon_E$ from Equation (7).

When $\varepsilon_E < \varepsilon_2$, we can obtain $\varepsilon_D < \varepsilon_2$. But, we consider $\varepsilon_E \geq \varepsilon_2$ is more reasonable. The reasons mainly include the following: ε_2 decreases as the transmission rate of E decreases; ε_2 decreases as the transmit power of E increases; meanwhile, as the transmit power of E increases, ε_E increases. Overall, ε_2 can be controlled at a very small value by reducing the transmission rate of E or increasing the transmit power of E.

In general, under the Shannon capacity regime, the Shannon capacity of the eavesdropping link is C_E, accordingly, the effective Shannon capacity of the suspicious link is C_D, as in [17]. Next, we give the following proposition.

Proposition 1: *$R_E > R_D$ when $C_E > C_D$, i.e., under the finite blocklength regime, E can eavesdrop the information sent by S the same as the condition under the Shannon capacity regime.*

Proof: See detailed proof of Proposition 1 in Appendix A. The corresponding simulation is shown in Figure 2. □

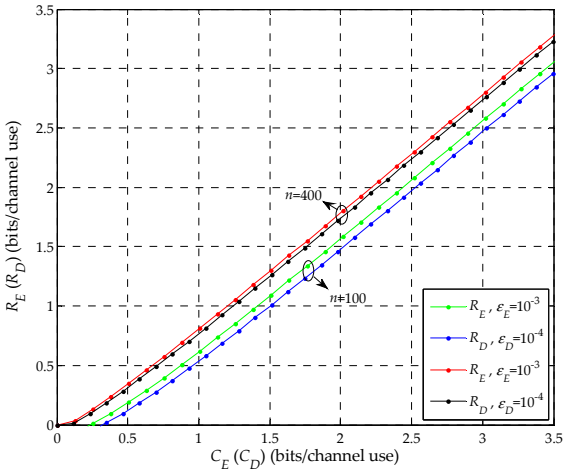

Figure 2. R_E vs C_E and R_D vs C_D.

Next, we give the following proposition, which is different from the results under the Shannon capacity regime where the legitimate monitor can eavesdrop the information sent by the suspicious transmitter only when $C_E \geq C_D$.

Proposition 2: *E can still eavesdrop the information sent by S as n decreases even though in some conditions of $C_E < C_D$, i.e., when n decreases, $R_E \geq R_D$ can still be achieved even in some conditions of $C_E < C_D$.*

Proof: Based on Equation (A1), it is known that $R_E - R_D > 0$ when $C_E = C_D$. Further, according to Equation (A1), the value of $R_E - R_D$ decreases with n because n is in the denominator. Therefore, the value of $R_E - R_D$ increases as n decreases. In this way, in some conditions of $C_E < C_D$, $R_E \geq R_D$ can still be achieved as n decreases, which is investigated by simulation in Figure 3. Thus, E can still eavesdrop the information sent by S as n decreases even though in some conditions of $C_E < C_D$. □

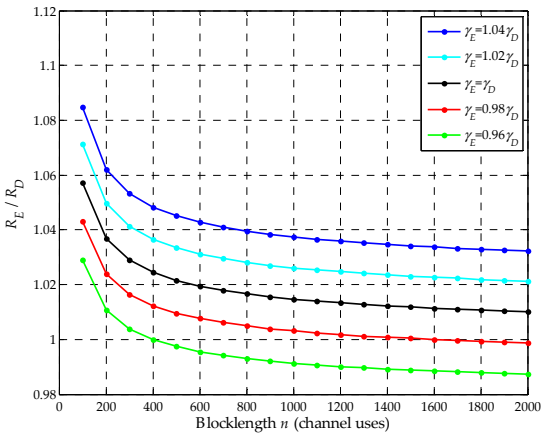

Figure 3. The ratio of R_E and R_D as a function of the blocklength n.

3.2. Analysis of Effective Eavesdropping Rate

When $R_E > R_D$, there is always a potential chance, such as increasing the relaying power of the legitimate monitor, to improve the eavesdropping rate by increasing R_D until $R_E = R_D$, which means that R_D reaches the optimal value. Then, any more improvement of R_D will lead to $R_E < R_D$, which means the failure of eavesdropping. So, when the suspicious link is eavesdropped with optimal eavesdropping rate, the relation of $R_E = R_D$ is always realized.

Next, under the finite blocklength regime, we define a metric called effective eavesdropping rate to analyze the system performance. Mathematically, the effective eavesdropping rate is given by

$$R_{eff} = R_{eav}(1 - \varepsilon_E) \tag{8}$$

where R_{eav} is the eavesdropping rate, and $R_{eav} = R_D = R_E$. According to Equation (3), we can reformulate Equation (8) as a function of R_{eav} as

$$R_{eff} = R_{eav}\left(1 - Q\left(\frac{a - R_{eav}}{b}\right)\right) \tag{9}$$

where $a = C_E = \log_2(1 + \gamma_E)$, and $b = \sqrt{\left(1 - \frac{1}{(1+\gamma_E)^2}\right)/n} \cdot \log_2 e$. Next, we study Equation (9), for which we have the following lemma.

Lemma 1: *Under the finite blocklength regime, the effective eavesdropping rate R_{eff} is monotonically increasing over $[0, R^*_{eav}]$ and monotonically decreasing over (R^*_{eav}, a) for moderate or even high SNR, where R^*_{eav} is the eavesdropping rate that maximizes the effective eavesdropping rate R_{eff}.*

Proof: See detailed proof of Lemma 1 in Appendix B. □

Base on the proof of Lemma 1, we prove that there exists a maximum effective eavesdropping rate, R^*_{eff}, corresponding to R^*_{eav}. However, unfortunately, the general closed-form for R^*_{eav} cannot be derived. Therefore, it is investigated by simulation in Figure 4. Furthermore, we consider the optimal eavesdropping rate $R^{opt}_{eav} = \max(R^*_{eav}, R_0)$, where R_0 is the channel coding rate of the suspicious link with no relaying power. Here, we first simply explain it as follows. We consider the eavesdropping rate $R_0 \le R_{eav} < a$. First, consider the case when $R^*_{eav} \ge R_0$. In this case, the legitimate monitor should use a positive relaying power to facilitate the eavesdropping, such that the effective channel coding rate R_D of the suspicious link is improved from R_0 to R^*_{eav}, thus, we have $R^{opt}_{eav} = R^*_{eav}$ and the optimal effective eavesdropping rate $R^{opt}_{eff} = R^*_{eff}$. Next, consider $R^*_{eav} < R_0$. In this case, we have $R^{opt}_{eav} = R_0$, which means that no relaying is required for the legitimate monitor to obtain its optimal effective eavesdropping rate.

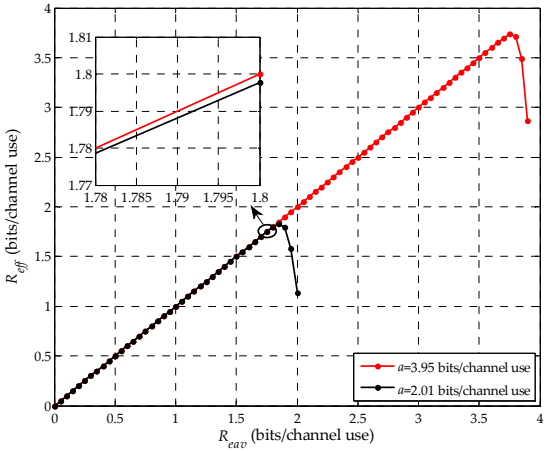

Figure 4. R_{eff} vs R_{eav} given in Equation (9).

4. Numerical Results

Next, we present numerical results obtained by simulations for the considered legitimate surveillance system. We consider the Rayleigh quasi-static block-fading channel and set the channel coefficients h_0, h_1 and h_2 to be independent circularly symmetric complex Gaussian random variables with mean zero and variance 1. Here, the transmit powers are normalized over the receiver noise powers such that we can set the noise powers at E and D to be ${\sigma_E}^2 = \sigma_D^2 = 1$. Unless otherwise stated, we set the transmit power at S as $P_1 = 20$ dB. We assume that the transmit power P_2 is large enough to facilitate the eavesdropping.

In Figure 2, R_E with C_E and R_D with C_D are shown for given blocklength n and error probability ε. Here, the transmit power P_2 is set to be 2 dB. Without loss of generality, n is set to be 100 and 400 channel uses, ε_E and ε_D are set to be 10^{-3} and 10^{-4}, respectively. As shown in the figure, when $C_E \geq C_D$, it is clear that $R_E > R_D$. Meanwhile, we can note that R_E increases with C_E, and that R_D also increases with C_D. For example, when n is 400 channel uses, for $C_E = C_D = 1.63$, $R_E - R_D = 0.04$, while for $C_E = 2.14$ and $C_D = 2.1$, $R_E - R_D = 0.09$, so $R_E - R_D > 0$ when $C_E \geq C_D$. Thus, under the finite blocklength regime, E can eavesdrop the information sent by S the same as the condition under the Shannon capacity regime, which is in line with Proposition 1.

In Figure 3, we plot the ratio of R_E and R_D with n when $\gamma_E = 1.04\gamma_D$, $\gamma_E = 1.02\gamma_D$, $\gamma_E = \gamma_D$, $\gamma_E = 0.98\gamma_D$ and $\gamma_E = 0.96\gamma_D$, where $\gamma_E = 0.98\gamma_D$ and $\gamma_E = 0.96\gamma_D$ represent some conditions of $C_E < C_D$. We set ε_E and ε_D to be 10^{-3} and 10^{-4}, respectively. As shown in the figure, we can note that when $\gamma_E \geq \gamma_D$, $R_E/R_D > 1$ and R_E/R_D decreases with n. Meanwhile, in comparison to $\gamma_E = \gamma_D$, R_E/R_D can still be larger than or equal to 1 when $\gamma_E = 0.98\gamma_D$ and $\gamma_E = 0.96\gamma_D$ as shown in the figure. For example, when $R_E/R_D = 1$, the blocklengths n of the red and green curves are respectively around 1400, 400 channel uses, thus, n decreases. So even in some conditions of $C_E < C_D$, E can still eavesdrop the information sent by S as n decreases, which demonstrates proposition 2.

Figure 4 shows the effective eavesdropping rate R_{eff} with the eavesdropping rate R_{eav} at E given in Equation (9). Here, the results are obtained when a is 2.01 and 3.95 bits per channel use, thus, we can obtain that γ_E is 4.81 dB and 11.6 dB, which are supposed to moderate SNRs. Without loss of generality, we set n to be 400 channel uses. As shown in the figure, we can note that R_{eff} is first monotonically increasing and then monotonically decreasing and there is a maximum value of the eavesdropping rate, R^*_{eav}, which is corresponding to the maximum value of the effective eavesdropping rate, R^*_{eff}. For example, R^*_{eav} is around 3.7 when γ_E is 11.6 dB. Moreover, we can also note that R_{eff} is larger when γ_E is 11.6 dB compared with γ_E is 4.81 dB. Thus, for a given blocklength n, R_{eff} increases with γ_E for the same R_{eav}. So far, the Lemma 1 is demonstrated by simulation.

In Figure 5, we plot the maximum effective eavesdropping rate R^*_{eff} with the blocklength n. Here, corresponding to Figure 4, the results are obtained when a is 2.01 and 3.95 bits per channel use. As

show in Figure 5, we can clearly note that R^*_{eff} increases with n. We can also note that the increments of the curves are almost negligible when n reaches a relatively large value. For example, the increment of the red curve is very small in the range of 1500 channel uses to 2000 channel uses. Moreover, it is easy to see that R^*_{eff} increases with a, thus, R^*_{eff} increases with γ_E.

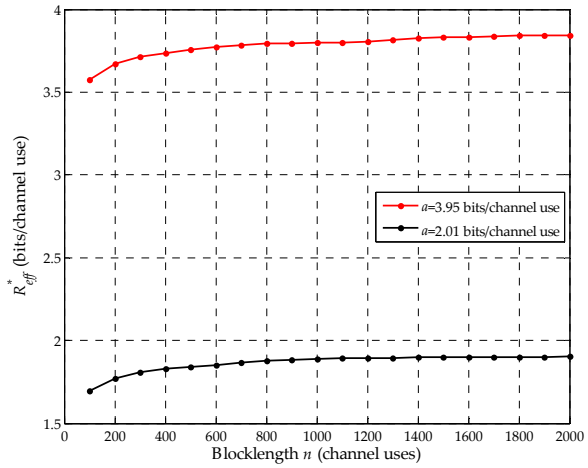

Figure 5. R^*_{eff} vs the blocklength n.

5. Conclusions

In this paper, under the finite blocklength regime, we analyze the performance of a legitimate proactive eavesdropping system, which consists of a suspicious transmitter–receiver pair and a legitimate monitor. We consider that the legitimate monitor operates in a full-duplex mode with simultaneous information reception and relaying. Moreover, we analyze the channel coding rate of the eavesdropping link and the suspicious link. We find that the legitimate monitor can still eavesdrop the information sent by the suspicious transmitter as the blocklength decreases, even when the eavesdropping is failed under the Shannon capacity regime. Furthermore, we define a metric called effective eavesdropping rate and analyze the monotonicity. From the analysis of monotonicity, the existence of a maximum effective eavesdropping rate for moderate or even high SNR is verified. Finally, numerical results are provided and discussed. In the simulation, we also find that the maximum effective eavesdropping rate slowly increases with the blocklength, and the increment is almost negligible when the blocklength is relatively large.

Author Contributions: Conceptualization, R.D., B.L. and B.Y.; Funding acquisition, B.L.; Investigation, R.D.; Methodology, R.D. and B.Y.; Project administration, B.L.; Software, R.D.; Supervision, B.L.; Validation, B.Y.; Writing–original draft, R.D.; Writing–review & editing, B.L.

Funding: This research was funded by the National Natural Science Foundation of China (61501185), and the Hebei Province Natural Science Foundation (F2016502062), and the Fundamental Research Funds for the Central Universities (2015MS125, 2016MS97), and the Beijing Natural Science Foundation (4164101), and the Shaanxi STA International Cooperation and Exchanges Project (2017KW-011). The APC was funded by the Fundamental Research Funds for the Central Universities (2015MS125).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Proof of Proposition 1

First, when $C_E = C_D$, we have

$$\begin{aligned} R_E - R_D &= C_E - \sqrt{(1-2^{-2C_E})/n} \cdot Q^{-1}(\varepsilon_E)\log_2 e \\ &\quad -\left(C_D - \sqrt{(1-2^{-2C_D})/n} \cdot Q^{-1}(\varepsilon_D)\log_2 e\right) \\ &= \sqrt{(1-2^{-2C_D})/n} \cdot Q^{-1}(\varepsilon_D)\log_2 e \\ &\quad - \sqrt{(1-2^{-2C_E})/n} \cdot Q^{-1}(\varepsilon_E)\log_2 e \\ &= \sqrt{(1-2^{-2C_D})/n} \cdot \log_2 e \cdot \left[Q^{-1}(\varepsilon_D) - Q^{-1}(\varepsilon_E)\right] \end{aligned} \tag{A1}$$

where it can be known that $\sqrt{(1-2^{-2C_D})/n} \cdot \log_2 e > 0$. We have obtained $\varepsilon_D < \varepsilon_E$, so we can derive $Q^{-1}(\varepsilon_D) > Q^{-1}(\varepsilon_E)$ by using the fact that $Q^{-1}(x)$ is the decreasing function of x. Thus, we can obtain $R_E > R_D$ when $C_E = C_D$.

Afterwards, Equation (1) can be approximated as

$$R = C - \sqrt{1/n} \cdot Q^{-1}(\varepsilon)\log_2 e \tag{A2}$$

As is shown in the Figure A1, the approximation, i.e. Equation (A2), is very tight for the range of SNR.

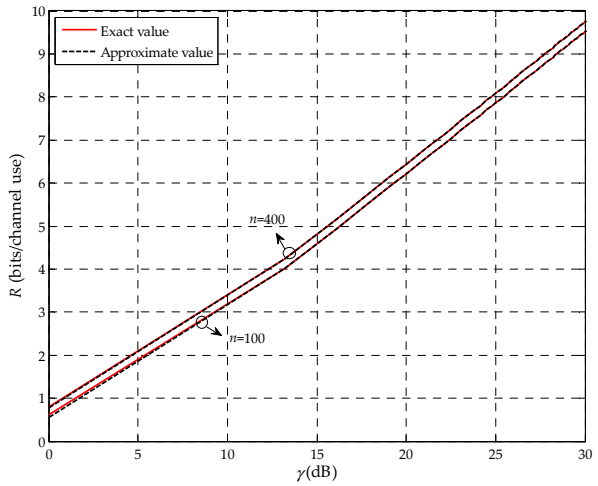

Figure A1. R with γ via Equation (1) and Equation (A2).

According to Equation (A2), it can be known that R increases with C. Thus, R_D increases with C_D, therefore, if $C_E > C_D$, which means that C_D is smaller in comparison with the condition $C_E = C_D$, R_E is definitely larger than R_D.

In conclusion, $R_E > R_D$ when $C_E \geq C_D$. □

Appendix B

Proof of Lemma 1

To demonstrate there is the value of R_{eav} that maximizes the effective eavesdropping rate R_{eff}, we next examine the monotonicity and concavity of R_{eff} with respect to R_{eav}. For this purpose, we derive the first and second derivatives of R_{eff} with respect to R_{eav} respectively.

Based on the differentiation of a definite integral in terms of a parameter [30], the first derivative of R_{eff} with respect to R_{eav} is given by

$$\begin{aligned} R_{eff}{}'(R_{eav}) &= \left(1 - Q\left(\tfrac{a-R_{eav}}{b}\right)\right) + R_{eav} \cdot \left(-\tfrac{m}{b}\right) \\ &= 1 - Q\left(\tfrac{a-R_{eav}}{b}\right) - \tfrac{R_{eav}m}{b} \end{aligned} \tag{A3}$$

where $m = \frac{1}{\sqrt{2\pi}} e^{-\frac{(a-R_{eav})^2}{2b^2}}$.

Likewise, the second derivative of R_{eff} with respect to R_{eav} is obtained as

$$\begin{aligned} R_{eff}{}''(R_{eav}) &= -\tfrac{m}{b} - \left(\tfrac{m}{b} + \tfrac{R_{eav}m(a-R_{eav})}{b^3}\right) \\ &= -\tfrac{2m}{b} - \tfrac{R_{eav}m(a-R_{eav})}{b^3} \end{aligned} \tag{A4}$$

We can easily note that $a > 0$ and $b > 0$. In this way, we can immediately obtain that

$$R_{eff}{}'(0) = 1 - Q\left(\frac{a}{b}\right) > 0 \tag{A5}$$

which is due to $0 < Q\left(\frac{a}{b}\right) < 0.5$.

Besides, we can also obtain that

$$R_{eff}{}''(0) = -\frac{2m(0)}{b} < 0 \tag{A6}$$

which is due to $m > 0$.

Moreover, we find that $R''_{eff}(R_{eav}) < 0$ within $0 \le R_{eav} < a$. So, $R'_{eff}(R_{eav})$ keeps decreasing in the range of $0 \le R_{eav} < a$. We next confirm that the value of $R'_{eff}(a)$ is larger than zero or smaller than zero. According to Equation (A3), we have

$$\begin{aligned} R_{eff}{}'(a) &= 1 - Q(0) - \tfrac{am(a)}{b} \\ &= 0.5 - \tfrac{a}{b\sqrt{2\pi}} \\ &= 0.5 - \frac{\log_2(1+\gamma_E)}{\sqrt{\left(1 - \frac{1}{(1+\gamma_E)^2}\right)/n \cdot \log_2 e \cdot \sqrt{2\pi}}} \end{aligned} \tag{A7}$$

It is easy to know that the value of $R'_{eff}(a)$ decreases as γ_E increases, and also decreases as n increases. In general, the SNR is relatively small when $\gamma_E = -5$ dB. Note that Equation (3) is just an approximation when n is large enough [29], e.g. $n \ge 100$. By bringing $\gamma_E = -5$ dB and $n = 100$ channel uses into Equation (A7), we obtain that $R'_{eff}(a) < 0$. So for moderate or even high SNR, $R'_{eff}(a)$ is definitely smaller than zero with a given n.

Summarizing, $R'_{eff}(R_{eav})$ keeps decreasing within $0 \le R_{eav} < a$, meanwhile $R'_{eff}(0) > 0$ and $R'_{eff}(a) < 0$ for moderate or even high SNR. So there must exist a value R^*_{eav} of $R'_{eff}(R_{eav}) = 0$, where R^*_{eav} is the value of R_{eav} that maximizes the effective eavesdropping rate R_{eff}. So far, Lemma 1 is proved. □

References

1. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
2. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Trans. Ind. Inf.* **2018**, *14*, 4724–4734. [CrossRef]

3. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality under Resource Constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [CrossRef]
4. Durisi, G.; Koch, T.; Popovski, P. Toward massive, ultrareliable, and low-latency wireless communication with short packets. *Proc. IEEE* **2016**, *104*, 1711–1726. [CrossRef]
5. Polyanskiy, Y.; Poor, H.V.; Verdu, S. Channel coding rate in the finite blocklength regime. *IEEE Trans. Inf. Theory* **2010**, *56*, 2307–2359. [CrossRef]
6. Xu, J.; Duan, L.; Zhang, R. Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm. *IEEE Wirel. Commun.* **2017**, *24*, 152–159. [CrossRef]
7. Wang, D.; Ren, P.; Cheng, J.; Wang, Y. Achieving full secrecy rate with energy-efficient transmission control. *IEEE Trans. Commun.* **2017**, *65*, 5386–5400. [CrossRef]
8. Su, Y.; Han, G.; Fu, X.; Xu, N.; Jin, Z. The Physical Layer Security Experiments of Cooperative Communication System with Different Relay Behaviors. *Sensors* **2017**, *17*, 781. [CrossRef] [PubMed]
9. Shim, K.; Do, N.T.; An, B. Performance Analysis of Physical Layer Security of Opportunistic Scheduling in Multiuser Multirelay Cooperative Networks. *Sensors* **2017**, *17*, 377. [CrossRef] [PubMed]
10. Yang, M.; Zhang, B.; Huang, Y.; Yang, N.; Guo, D.; Gao, B. Secure Multiuser Communications in Wireless Sensor Networks with TAS and Cooperative Jamming. *Sensors* **2016**, *16*, 1908. [CrossRef]
11. Tang, X.; Cai, Y.; Yang, W.; Yang, W.; Chen, D.; Hu, J. Secure Transmission of Cooperative Zero-Forcing Jamming for Two-User SWIPT Sensor Networks. *Sensors* **2018**, *18*, 331. [CrossRef] [PubMed]
12. Sun, A.; Liang, T.; Li, B. Secrecy Performance Analysis of Cognitive Sensor Radio Networks with an EH-Based Eavesdropper. *Sensors* **2017**, *17*, 1026. [CrossRef] [PubMed]
13. Xu, J.; Duan, L.; Zhang, R. Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels. *IEEE Wirel. Commun. Lett.* **2016**, *5*, 80–83. [CrossRef]
14. Xu, J.; Duan, L.; Zhang, R. Proactive eavesdropping via cognitive jamming in fading channels. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 2790–2806. [CrossRef]
15. Xu, J.; Duan, L.; Zhang, R. Proactive eavesdropping via cognitive jamming in fading channels. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 23–27 May 2016; pp. 1–6.
16. Tran, H.; Zepernick, H. Proactive attack: A strategy for legitimate eavesdropping. In Proceedings of the 2016 IEEE Sixth International Conference on Communications and Electronics (ICCE), Ha Long, Vietnam, 27–29 July 2016; pp. 457–461.
17. Zeng, Y.; Zhang, R. Wireless information surveillance via proactive eavesdropping with spoofing relay. *IEEE J. Sel. Top. Signal Process.* **2016**, *10*, 1449–1461. [CrossRef]
18. Zhong, C.; Jiang, X.; Qu, F.; Zhang, Z. Multi-antenna wireless legitimate surveillance systems: Design and performance analysis. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 4585–4599. [CrossRef]
19. Xu, J.; Duan, L.; Zhang, R. Transmit Optimization for Symbol-Level Spoofing. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 41–55. [CrossRef]
20. Xu, J.; Duan, L.; Zhang, R. Fundamental Rate Limits of Physical Layer Spoofing. *IEEE Wirel. Commun. Lett.* **2017**, *6*, 154–157. [CrossRef]
21. Xu, J.; Duan, L.; Zhang, R. Transmit Optimization for Symbol-Level Spoofing with BPSK Signaling. In Proceedings of the 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, USA, 4–8 December 2016; pp. 1–6.
22. Li, B.; Yao, Y.; Chen, H.; Li, Y.; Huang, S. Wireless information surveillance and intervention over multiple suspicious links. *IEEE Signal Process. Lett.* **2018**, *25*, 1131–1135. [CrossRef]
23. Li, B.; Yao, Y.; Zhang, H.; Lv, Y. Energy efficiency of proactive cooperative eavesdropping over multiple suspicious communication links. *IEEE Trans. Veh. Technol.* **2019**, *68*, 420–430. [CrossRef]
24. Jiang, X.; Lin, H.; Zhong, C.; Chen, X.; Zhang, Z. Proactive eavesdropping in relaying systems. *IEEE Signal Process. Lett.* **2017**, *24*, 917–921. [CrossRef]
25. Ma, G.; Xu, J.; Duan, L.; Zhang, R. Wireless surveillance of two-hop communications (Invited paper). In Proceedings of the 2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Sapporo, Japan, 3–6 July 2017; pp. 1–5.
26. Zhang, Y.; Jiang, X.; Zhong, C.; Zhang, Z. Performance of Proactive Eavesdropping in Dual-Hop Relaying Systems. In Proceedings of the 2017 IEEE Globecom Workshops (GC Wkshps), Singapore, 4–8 December 2017; pp. 1–6.

27. Nie, Z.; Zhao, R.; Li, Y.; Xiamen, X.T. A full-duplex SWIPT relaying protocol based on discrete energy state. In Proceedings of the 2017 20th International Symposium on Wireless Personal Multimedia Communications (WPMC), Bali, Indonesia, 17–20 December 2017; pp. 500–505.
28. Yang, W.; Durisi, G.; Koch, T.; Polyanskiy, Y. Quasi-Static Multiple-Antenna Fading Channels at Finite Blocklength. *IEEE Trans. Inf. Theory* **2014**, *60*, 4232–4265. [CrossRef]
29. Hu, Y.; Schmeink, A.; Gross, J. Blocklength-limited performance of relaying under quasi-static rayleigh channels. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 4548–4558. [CrossRef]
30. Gradshteyn, I.; Ryzhik, I. *Table of Integrals, Series, and Products*; Elsevier Inc.: Cambridge, MA, USA, 2007.