sensors

Article

The Physical Layer Security Experiments of Cooperative Communication System with Different Relay Behaviors

Yishan Su [1,2], Guangyao Han [2], Xiaomei Fu [1,2,*], Naishen Xu [2] and Zhigang Jin [2]

[1] School of Marine Science and Technology, Tianjin University, 300072 Tianjin, China; yishan.su@tju.edu.cn

[2] School of Electrical Automation and Information Engineering, Tianjin University, 300072 Tianjin, China; hanguangyao@tju.edu.cn (G.H.); xunaishen@126.com (N.X.); zgjin@tju.edu.cn (Z.J.)

[*] Correspondence: fuxiaomei@tju.edu.cn

Academic Editor: Yuh-Shyan Chen

Received: 10 January 2017; Accepted: 31 March 2017; Published: 6 April 2017

Abstract: Physical layer security is an attractive security mechanism, which exploits the randomness characteristics of wireless transmission channel to achieve security. However, it is hampered by the limitation of the channel condition that the main channel must be better than the eavesdropper channel. To alleviate the limitation, cooperative communication is introduced. Few studies have investigated the physical layer security of the relay transmission model. In this paper, we performed some experiments to evaluate the physical layer security of a cooperative communication system, with a relay operating in decode-and-forward (DF) cooperative mode, selfish and malicious behavior in real non-ideal transmission environment. Security performance is evaluated in terms of the probability of non-zero secrecy capacity. Experiments showed some different results compared to theoretical simulation: (1) to achieve the maximum secrecy capacity, the optimal relay power according to the experiments result is larger than that of ideal theoretical results under both cooperative and selfish behavior relay; (2) the relay in malicious behavior who forwards noise to deteriorate the main channel may deteriorate the eavesdropper channel more seriously than the main channel; (3) the optimal relay positions under cooperative and selfish behavior relay cases are both located near the destination because of non-ideal transmission.

Keywords: physical layer security; different relay behavior; experiment

1. Introduction

When it comes to the secure transmission of information, cryptographic algorithms are traditionally employed as the security technology to achieve information confidentiality [1]. Information encryption usually involves the use of a key to encrypt and decrypt the messages. Unlike conventional wired communication that uses wired media (optical cable, copper, etc.) for data transmission, the broadcast nature of wireless channels allows an illegal receiver to wiretap legal messages easily during the transmission from the source to the destination. Moreover, with the development of cryptography, new algorithms and methods to decipher traditionally encrypted messages have been developed, which means old encryption methods are faced with higher risk of being cracked. Cryptographic methods face numerous risks due to the rapid development of the computing capabilities of eavesdroppers [2]. Besides, complex cryptographic algorithms require devices capable of dealing with heavy computing loads, leading to high power and resource costs. The physical layer security adopts the physical characteristics of wireless channels to guarantee its security through coding and signal processing, in which confidential message can be decoded only by their legitimate receiver and avoid complex computing. In this way, physical layer security has been proposed to safeguard wireless transmission, for instance, 5G wireless communication networks and heterogeneous cellular networks [3,4].

Physical layer security was first introduced by Wyner [5], who adapted Shannon's concepts of entropy and equivocation [6] to investigate the physical layer security. The achieved maximum transmission rate of confidential message communication is defined by Wyner as the secrecy capacity. However, the feasibility of physical layer security is hampered by the limitation when the channel between the source and the destination (the main channel) is worse than that between the source and the eavesdropper (the wiretap channel). An effective way to improve the main channel condition is cooperative communication with a relay's help [7].

Cooperative relays can enhance the secrecy capacity of wireless communications by exploiting decode and forward (DF), amplify and forward (AF) [8]. In the DF and AF cooperative strategies, the relay utilizes its overheard information to reinforce the transmitting signal of the source [9–11]. In [12–14], the physical layer security is improved by the advantages of large scale MIMO arrays of relays with AF and DF strategies. In [15,16], the optimal transmission with maximized secrecy rate under energy harvesting requirements is investigated, where the secrecy capacity is sensitive to the position among the nodes. It was found that the distance from the source to the relay has an important influence on secrecy capacity. Therefore, to find the optimal relay location is an important requirement to achieve maximum secrecy capacity [17]. In this paper, we investigated a cooperative communication system with one source, one relay, one destination and one eavesdropper with experiments for further discussion.

In practical applications, relays may not always select a cooperative strategy because of its own benefits. Some research has investigated the secrecy capacity with untrusted relays. In [18,19] the authors discussed the case of untrusted relays with both a cooperator and an eavesdropper. The secrecy capacity in a selfish behavior relay scheme in which the relay wants to save its own resources [20,21] was also discussed.

Theoretical analysis usually guides the real implementation with simplified or ideal physical factors, while applying them in practice may lead to different results. The authors in [22] firstly analyzed the physical layer security with the probability of a non-zero secrecy capacity ($P(C_S > 0)$) of a wiretap channel by experimental measurements. It was found that the shadowing deviation can influence the security, which was seldom considered by theoretical analysis. The results from [23] can only be applied in a point-to-point network scenario. To investigate the physical layer security of multiple point relay transmission models, in this paper, we establish a cooperative communication testbed based on a software-defined radio (SDR) platform [24]. Based on this platform, we investigate the physical layer security with different relay behavior (cooperation, selfishness, maliciousness) with DF scheme in real non-ideal wireless transmission environment. The $P(C_S > 0)$ was calculated to evaluate physical layer security in an actual outdoor environment. We obtain some different results which is ignored by theoretical or simulation analysis.

Table 1. Symbols Description.

h_{SD}	the channel fading coefficients from S to D (source to destination)
h_{SR}	the channel fading coefficients from S to R (source to relay)
h_{RD}	the channel fading coefficients from R to D (relay to destination)
P_{off}	the probability in the Off-State
$P(C_S > 0)$	the probability of Non-zero secrecy capacity
γ_M	the average SNR of the main channel
γ_W	the average SNR of the wiretap channel
γ_{SD}	the average SNR of the S to D channel (source to destination)
γ_{SRD}	the average SNR of the main channel which consists of channel from S to R and R to D
γ_{SE}	the average SNR of the S to E path
γ_{SRE}	the average SNR of the wiretap channel which consists of channel from S to R, and R to E
P_{SR}	the BER at S-R hop
P_{RD}	the BER at R-D hop
P_{SRD}	the BER of the two-hop S-R-D channel

The paper is structured as follows: Section 2 introduces the system model and different relays' behavior; Section 3 presents experimental results of bit error rate (BER) in a system with different relay behavior; Section 4 discusses the security performance under different relay behavior; finally, Section 5 presents our conclusions. The symbols used in this paper are described in Table 1.

2. System Description

2.1. System Model

A relay transmission system model consists of a source (S), a destination (D), a relay (R) and an eavesdropper (E), as depicted in Figure 1. S wants to communicate with D in the presence of E. The S broadcasts signals with average power P_S. R receives signals from S with DF strategy.

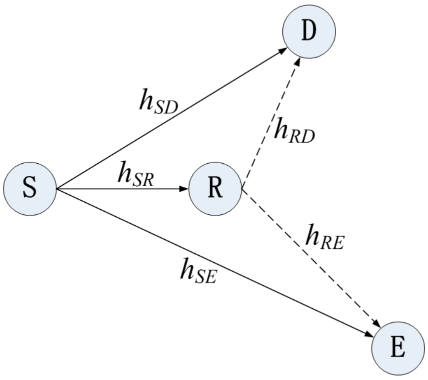

Figure 1. Relay transmission model with one eavesdropper, where h_{SD}, h_{SR}, h_{RD} denote the channel fading coefficients from S to D, R, and from R to D. They are modeled as follows: $h_{SD} \sim CN(0, \sigma_{SD}^2)$, $h_{SR} \sim CN(0, \sigma_{SR}^2)$, $h_{RD} \sim CN(0, \sigma_{RD}^2)$, with $\sigma_{SD}^2 = E\{|h_{SD}|^2\}$, $\sigma_{SR}^2 = E\{|h_{SR}|^2\}$, $\sigma_{RD}^2 = E\{|h_{RD}|^2\}$.

2.2. Different Behaviors of Relay

In this paper, three types of relay behaviors are discussed:

1. Cooperative Behavior: The relay decodes the received signal and forwards it to the destination.
2. Selfish Behavior: The relay refuses to cooperate with probability P_{off} [14], while selecting to cooperate with probability P_{on} $\left(P_{on} = 1 - P_{off}\right)$.
3. Malicious Behavior: The relay forwards random noise instead of the received signals of the source.

2.3. The Probability of Non-Zero Secrecy Capacity with Different Behavior

To investigate the physical layer security in experiment, we adopted the theories and equations in [8] with the wiretap communication model without relay, as shown in Figure 2. Then, we investigate the scenario of a relay cooperative case. Suppose a k-length message m^k sent from source is coded to n-length codeword $x^n (x^n = [x(1), x(2), \ldots, x(n)])$, chosen from codebook $\mathcal{X}^n (x^n \in \mathcal{X}^n)$, the main channel and the wiretap channel output is described as:

$$y_M(i) = h_{SD}(i)x(i) + n_{SD}, \tag{1}$$

$$y_W(i) = h_{SE}(i)x(i) + n_{SE}, \tag{2}$$

where h_{SD}, h_{SE} denote the channel fading coefficients of the main channel and wiretap channel respectively with complex Gaussian distribution. Notations n_{SD}, n_{SE} denote the mean circularly symmetric complex Gaussian noise in the main channel and wiretap channel respectively, and $n_{SD} \sim CN(0, N_M)$, $n_{SE} \sim CN(0, N_W)$.

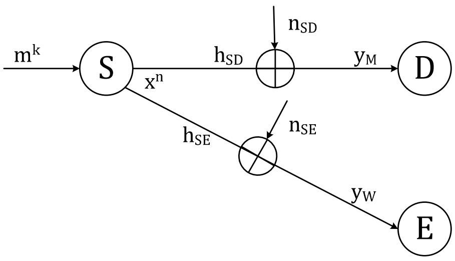

Figure 2. Wiretap communication model without relay.

The channel power is limited by average transmit signal power P:

$$\frac{1}{n}\sum_{i=1}^{n} E[|x(i)|^2] \leq P. \tag{3}$$

The average *SNR* of the main channel is given by:

$$\gamma_M = P \times E[|h_{SD}|^2]/N_M. \tag{4}$$

Similarly, the average *SNR* of the wiretap channel is described as:

$$\gamma_W = P \times E[|h_{SE}|^2]/N_W. \tag{5}$$

The secrecy capacity in this model is defined as $C_S = C_M - C_W$:

$$C_S = \begin{cases} \log\left(1 + \frac{|h_{SD}|^2 P}{N_M}\right) - \log\left(1 + \frac{|h_{SE}|^2 P}{N_W}\right) & , if\ \gamma_M > \gamma_W \\ 0 & , if\ \gamma_m \leq \gamma_W \end{cases} \tag{6}$$

We denote the instantaneous *SNR* of the main channel and wiretap channel by ${\gamma_M}'$ and ${\gamma_W}'$, [25]:

$${\gamma_M}' = P \times E[|h_{SD}(i)|^2]/N_M, \tag{7}$$

$${\gamma_W}' = P \times E[|h_{SD}(i)|^2]/N_W, \tag{8}$$

from which we can see that γ (regardless of the footnote in different channels) is exponentially distributed as $\gamma \propto |h|^2$. Then:

$$p(\gamma) = \frac{1}{\bar{\gamma}} exp\left(-\frac{\gamma}{\bar{\gamma}}\right), \tag{9}$$

and the probability of $C_S > 0$ (denoted by $P(C_S > 0)$) is calculated in [8], specifically:

$$P(C_S > 0) = \int_0^\infty \int_0^{\gamma_M} p(\gamma_M)p(\gamma_W)d\gamma_W d\gamma_M = \frac{\gamma_M}{\gamma_M + \gamma_W}. \tag{10}$$

Then, we derive $P(C_S > 0)$ in relay transmission model for different relay behaviors:

(1) $P(C_S > 0)$ under cooperative behavior: The relay cooperatively decodes and forwards the received signal to D (or E). The destination combines the received signals from S and R by maximum ratio combining (MRC). The main channel consists of the S-R-D path and S-D path, and the wiretap channel includes the S-E and S-R-E path. $\gamma_M = \gamma_{SRD} + \gamma_{SD}$ is the SNR of the main channel, and $\gamma_W = \gamma_{SRE} + \gamma_{SE}$ is the *SNR* of the eavesdropper channel. Therefore, according to (10), the $P(C_S > 0)$ is given by:

$$P_C(C_S > 0) = \frac{\gamma_{SRD} + \gamma_{SD}}{\gamma_{SRD} + \gamma_{SD} + \gamma_{SRE} + \gamma_{SE}}, \tag{11}$$

where γ_{SD} is the average SNR of S to D channel, γ_{SRD} is the average SNR of the main channel which consists of S to R, and R to D path. The average SNR of the S to E path is denoted as γ_{SE}, and γ_{SRE} is the average SNR of the wiretap channel which consists of S to R, and R to E path.

(2) $P(C_S > 0)$ under selfish behavior: If the relay is selfish with the probability P_{off}, then, $\gamma_M = \gamma_{SD}$ and $\gamma_W = \gamma_{\text{SE}}$, while the relay uses cooperative behavior with the probability $(1 - P_{off})$. Then, $P(C_S > 0)$ is given by:

$$P_S(C_S > 0) = \left(1 - P_{off}\right) \times \frac{\gamma_{SRD} + \gamma_{SD}}{\gamma_{SRD} + \gamma_{SD} + \gamma_{SRE} + \gamma_{SE}} + P_{off} \times \frac{\gamma_{SD}}{\gamma_{SD} + \gamma_{SE}}. \tag{12}$$

(3) $P(C_S > 0)$ under malicious behavior: The received signal from the malicious relay at D and E is considered as a noise. $\gamma_M = \gamma_{SD}/(1 + \gamma_{RD})$ and $\gamma_W = \gamma_{SE}(1 + \gamma_{RE})$, $P(Cs > 0)$ is given by:

$$P_M(C_S > 0) = \frac{\gamma_{SD}(1 + \gamma_{RE})}{\gamma_{SD}(1 + \gamma_{RE}) + \gamma_{SE}(1 + \gamma_{RD})}. \tag{13}$$

2.4. Equivalent Signal-To-Noise Ratio from Source to the Destination

In theoretical analyses, most of the existing work considers the forward process as completely ideal in the DF strategy [10,11,24], in which the relay correctly decodes and forwards the received messages. However, A few researchers consider this a non-ideal scenario. Due to possible errors at the relay, the S-R-D channel is clearly non-linear and non-Gaussian. However, one can think of the BER in S-R-D channel as the error probability at the receiver of an equivalent one-hop AWGN link. The BER of the two-hop S-R-D channel is given by [26]:

$$P_{SRD} = (1 - P_{SR}) \times P_{RD} + (1 - P_{RD}) \times P_{SR} \tag{14}$$

where P_{SR} and P_{RD} are the BER at source to relay (S-R) hop and relay to destination (R-D) hops, respectively. The equivalent SNR from the measured BER is applied to describe this non-ideal DF transmission scenario. Then the equivalent SNR is obtained.

3. Experimental Setup

Software defined radio (SDR) is a rapidly emerging concept in wireless communication system. The main SDR involves using GNU Radio and universal software radio peripheral (USRP) in an Ubuntu system [18]. The experimental setup is shown in Figure 3, where each node is equipped with a laptop running GNU Radio connected to a USRP in the experiment.

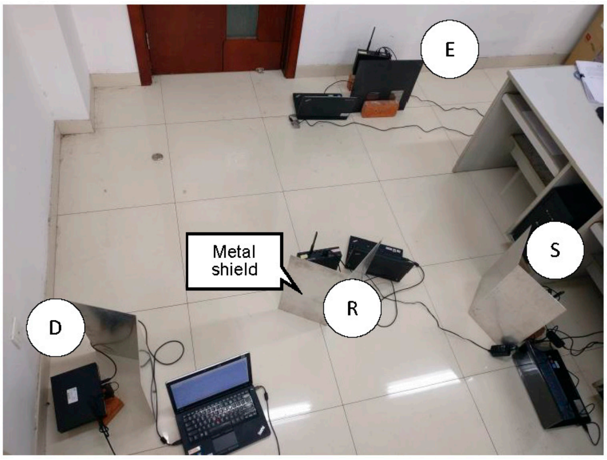

Figure 3. Experimental setup.

Metal shields are placed between nodes to help attenuate any line-of-sight path. The distance between every two points of S, R and D is 2 m. The noise power is measured about −60 dBm. The source power is fixed on −39 dBm and relay power changes from −51 dBm to −39 dBm (all the power presented in dBm is measured from the experiment). Figure 4 illustrates the different steps of signal processing at the transmitter and relay designed by the authors.

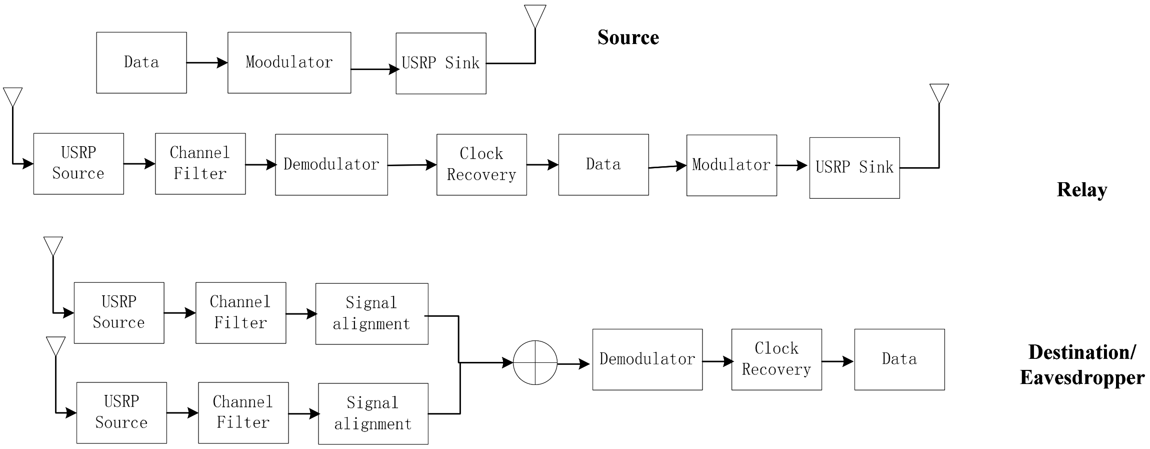

Figure 4. Signal processing at each node.

3.1. Source Operations

We use a USRP sink in the GNU Radio platform to transmit a binary bit stream. Messages are first encoded in the laptop to baseband signals. Then the USRP sink broadcasts the signal at 2.45 GHz with GMSK. A Python program is used to process the signals. We transmit 12,144 bits each time and repeat every situation 25 times to exclude an accident case. The signal's power is defined in the software part by limiting the signal amplitude to a certain voltage.

3.2. Relay Operations

In this paper, we experiment on different relay strategy, forward power, and locations to discuss the influence on secrecy capacity. In general, the main task of a relay is to receive the signal from the source, decode and forward them to the destination. After received desired signal, it saves the complex signal for further processing and finally transmit processed signal in a certain power.

3.3. Data Receiving and Processing

The USRP both in destination and eavesdropper node operates in the same way. They monitor at the frequency of 2.45 GHz and save received complex signals to the laptop. Thanks to the extensive GNU Radio platform and the stable USRP hardware, we have little worries about how to generate a baseband bit stream and shifting it to a high frequency is much more easy and there is no carrier frequency offset problem compared to a traditional transmission device. The difficult part in the experiment however is processing the received data. The data are all saved in a complex signal form which can be read from MATLAB. We have to determine which part of the data is the desired signal and leave out the white noise. Besides, complex signals received at the destination and eavesdropper consists of the two parts received from the source and relay, respectively. Synchronization is required to combine these two parts and after synchronization, two different parts of the complex signal are combined using the maximum ratio combining (MRC) method.

4. The Physical Layer Security Performance of the Relay Transmission Model

Considering the model depicted in Figure 5, S, D and E are located at fixed two-dimensional normalized coordinates (0; 0), (1; 0) and (0; 1). R is located along a horizontal line with S and D.

We execute the experiments and simulate the theoretical formulas according to Equations (11)–(13) for comparison.

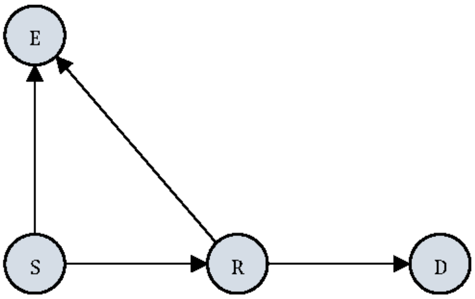

Figure 5. The system model.

4.1. The Influence of the Relay Power for P(Cs > 0)

4.1.1. Simulation Results with Various Relay Power

Figure 5 is a typical cooperative relay communication model adopted from [7], with source, destination and eavesdropper nodes fixed and relay node's location changing between the source and destination. The difference in this paper is that the relay has different relay behaviors. We simulate the $P(C_S > 0)$ verses P_r/P_s under different relay behaviors, where P_r and P_s are the power in relay and source, respectively, and the SNR of the source to destination (S-D) channel is 5dB. The path loss in the simulation is $1/d^2$, where d is the distance between two nodes.

The relay's normalized location is fixed at (0.5; 0) (the middle of S and D) and source power P_S is fixed at -40 dBm. Relay power P_r is changed from -70 dBm to -20 dBm. We simulate the $P(C_S > 0)$ under three different relay behavior according to (11), (12) ($P_{off} = 50\%$) and (13) as shown in Figure 6. We find that there exists an optimal relay power $P_r = P_s$, where $P(C_S > 0)$ would reach a peak value in cooperative and selfish scenario. When the relay power P_r increases beyond P_s, the $P(C_S > 0)$ decreases. We also notice that increasing the malicious relay power always decreases the $P(C_S > 0)$.

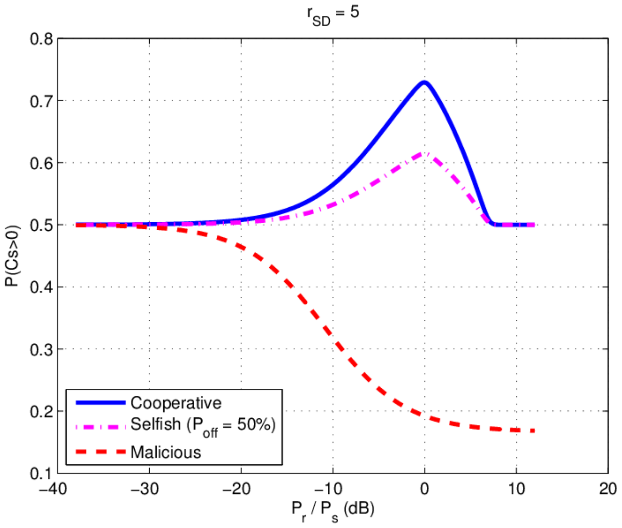

Figure 6. Simulation results: $P(C_S > 0)$ versus P_r/P_S under different behavior.

4.1.2. Experimental Results with Various Relay Power

In the experiment, S, R, D and E are located at fixed two-dimensional coordinates (0; 0), (1.8 m; 0), (3.6 m; 0) and (0; 3.6 m), respectively. In both D and E node, BER of both main channel and wiretap channel are obtained by combining the complex signal from S and R using maximum-ratio-combining (MRC), which a weighted superposition of the source and relay signals arriving at the destination are collected with the maximum available diversity order. We calculate $P(C_S > 0)$ by SNR according to (11), (12) and (13). The relay power is changed about 3 dBm every step and the source power is fixed at -39 dBm. In malicious behavior case, pseudo random noise is forwarded by the relay, in which there are 5972 error bits in all 12,144 bits.

The experimental data of cooperative relay and malicious relay are shown in Tables 2 and 3 respectively, where P_D is the BER at the destination and P_E is the BER at the eavesdropper. In Table 2, $\gamma_M = \gamma_{SRD} + \gamma_{SD}$ is the SNR of the main channel, and $\gamma_W = \gamma_{SRE} + \gamma_{SE}$ is the SNR of the eavesdropper channel. The last row of Table 2 is the calculated probability of $C_S > 0$ (denoted by $P(C_S > 0)$. In Table 3, $\gamma_M = \gamma_{SD}/(1 + \gamma_{RD})$ is the SNR of the main channel, and $\gamma_W = \gamma_{SE}(1 + \gamma_{RE})$ is the SNR of the eavesdropper channel. The graphic experimental results are shown in Figure 7.

Table 2. Experimental results with different transmit power under cooperative relay.

Transmit Power (dBm)	**-51**	**-49**	**-46.5**	**-44**	**-41.5**	**-39**	**-36**	**-34**	**-31**	**-28.5**
P_D	0.3383	0.2472	0.1873	0.113	0.061	0.0196	0.0026	0.0002	0.0001	0.0000
γ_M	0.0974	0.2614	0.4415	0.825	1.3386	2.3814	4.3727	7.1942	8.1577	∞
P_E	0.3472	0.2639	0.2096	0.152	0.1118	0.0692	0.0226	0.0054	0.0005	0.0000
γ_W	0.0864	0.2231	0.3652	0.593	0.8293	1.2289	2.2451	3.6327	6.1224	∞
$P(C_S > 0)$	0.5299	0.5394	0.5473	0.582	0.6175	0.6596	0.6608	0.6645	0.5713	0.5

Table 3. Experimental results with different transmit power under malicious relay.

Transmit Power (dBm)	**-51**	**-49**	**-46.5**	**-44**	**-41.5**	**-39**	**-36**	**-34**	**-31**	**-28.5**
P_D	0.3670	0.3810	0.4017	0.4198	0.4358	0.4459	0.4635	0.4811	0.4878	0.4918
γ_M	0.0647	0.0513	0.0343	0.0229	0.0146	0.0104	0.0047	0.0013	0.0005	0.0002
P_E	0.3609	0.3725	0.3902	0.4104	0.4251	0.4359	0.4530	0.4685	0.4847	0.4918
γ_W	0.0710	0.0592	0.0416	0.0287	0.0200	0.0146	0.0078	0.0035	0.0010	0.0002
$P(C_S > 0)$	0.4767	0.4624	0.4519	0.4438	0.4231	0.4155	0.3761	0.2652	0.3333	0.5

In our experimental setup, the results from Figure 7 indicate that the optimal relay power value is larger than the sources power ($P_r/P_s = 5$ dB), which means the relay need more power to achieve the optimal security performance in real non ideal DF environment. Therefore, generally speaking, in practice we can assume, the source to destination(S-D) channel is not ideal, the more relay power will be needed to achieve the same results as that in the ideal S-D channel.

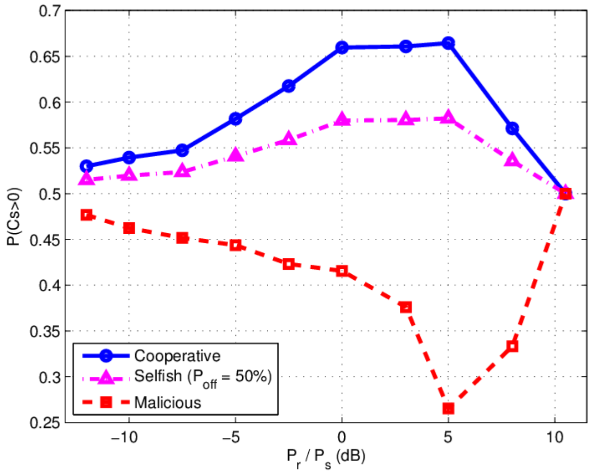

Figure 7. Experimental results: $P(C_S > 0)$ versus P_r/P_s under different behavior.

Moreover, in malicious relay behavior case, $P(C_S > 0)$ increases when P_r/P_s is beyond 5 dB, which is different to theoretical simulation result. It indicates that when the malicious relay forwards noise power high enough, the eavesdropper channel will be deteriorated more heavily than the main channel. As for the influence of relay power, it can be found that there exists a maximum value of $P(C_S > 0)$ for different relay powers.

4.2. *Influence of Relay Location for P(C_S > 0)*

4.2.1. Simulation Results with Various Relay Location

We assume P_r equals P_s, and $x(x = d_{SR}/d_{SD})$ is the normalized distance from S to R. Let x change from 0 to 1. The simulation result of $P(C_S > 0)$ is shown in Figure 8. There exists an optimal relay location where $P(C_S > 0)$ would reach a peak value in both cooperative and selfish behavior of a relay.

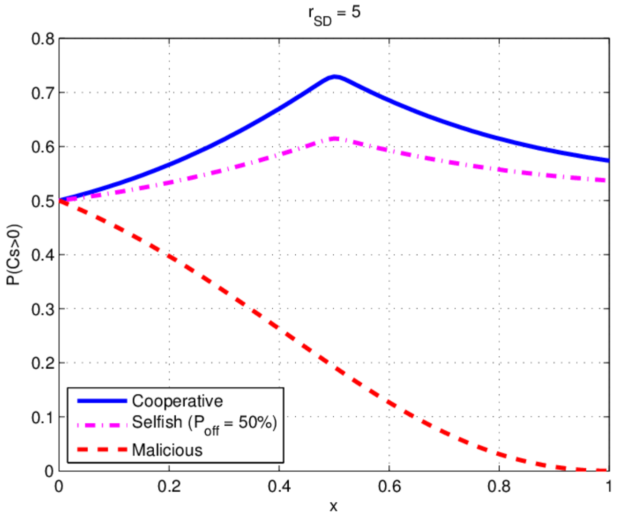

Figure 8. Simulation results: $P(C_S > 0)$ versus relay location under various behaviors.

In the simulation $\gamma_{SD} = 5$ is the SNR of S to D channel, the optimal location is in the middle of source and destination $(x = d_{SR}/d_{SD} = 0.5)$. $P(C_S > 0)$ will decreases quickly when R moves towards D with a malicious behavior relay.

4.2.2. Experimental Results with Various Relay Location

In this experiment, the transmit power of S and R both are fixed at −39 dBm. S, D and E are located at fixed two-dimensional coordinates (0, 0), (3.6 m, 0) and (0, 3.6 m), respectively. The coordinate of R changes from (1.2 m, 0), (1.8 m, 0) to (2.4 m, 0). The experimental results table are shown in Tables 4 and 5 respectively. The graphic experimental result is shown in Figure 9.

Table 4. Experimental results with various relay locations of cooperative behavior.

Relay Location	Left (1.2 m, 0)	Middle (1.8 m, 0)	Right (2.4 m, 0)
P_D	327.08	237.84	383.27
γ_M	2.081	2.3814	1.9336
P_E	625.71	840.78	1174.15
γ_W	1.488	1.2289	0.9472
$P(C_S > 0)$	0.5831	0.6596	0.6712

It can be seen that the experimental $P(C_S > 0)$ value in Figure 9 is different from the theoretical curves in Figure 8. The optimal location of the relay is a nearer the destination in experiment with non ideal DF case, whereas in theoretical ideal DF analysis, the location is in the middle of the Source to destination link. That phenomenon is also appeared in selfish relay case. For malicious behavior, the near destination malicious relay deteriorates the main channel seriously, but it is not as serious as that in theoretical simulation.

Table 5. Experimental results with different relay location of malicious behavior.

Relay Location	Left (1.2 m, 0)	Middle (1.8 m, 0)	Right (2.4 m, 0)
P_D	0.441	0.4459	0.4535
γ_M	0.0123	0.0104	0.0076
P_E	0.4382	0.4359	0.4302
γ_W	0.0135	0.0146	0.0173
$P(C_S > 0)$	0.4763	0.4155	0.3063

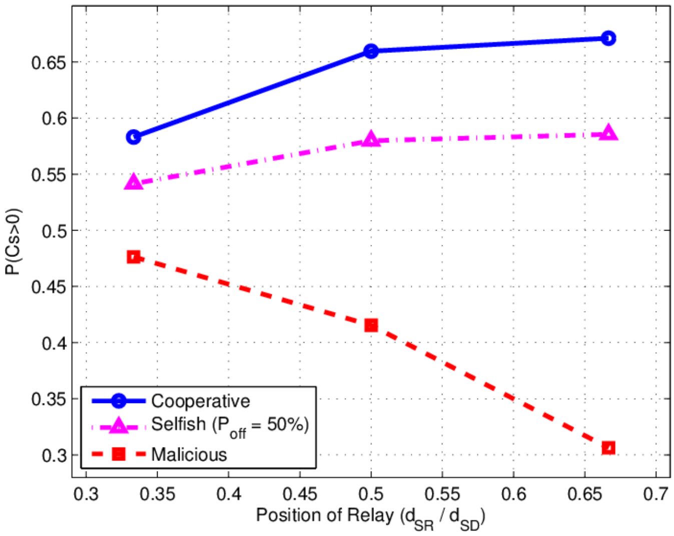

Figure 9. Experimental results: $P(C_S > 0)$ versus relay location under various behavior.

5. Conclusions

In this paper, we implement several experiments to investigate the physical layer security of a relay transmission model with different relay behaviors. Experimental results are compared with a theoretical analysis. We find a gap between the ideal theoretical simulations and the non-ideal real experiments:

(1) The relays need more power to achieve the maximum-security performance in a real environment. In the experiment, the optimal relay power is larger than the source power in both cooperative and selfish behavior relay scenarios because of the non-ideal source to destination (S-D) channel;

(2) In the malicious behavior relay case, the experimental value of $P(C_S > 0)$ is different from the ideal theoretical simulation result when the relay power is larger than the critical power ($P_r/P_S = 5$ dB), which indicates that when s malicious relay forwards high enough noise power, the eavesdropper channel is deteriorated more seriously than the main channel;

(3) Optimal relay location in both cooperative and selfish behavior of relay is in the middle of source and destination ($d_{SR}/d_{SD} = 0.5$) in the ideal theoretical simulation. However, in the experiment, the optimal relay location is nearer to the destination because of the non-ideal source to relay and to destination (S-R-D) channel.

Acknowledgments: This work is supported by the National Natural Science Foundation of China (61571323) (61571318), and the Guangxi Science and Technology Project AC16380094.

Author Contributions: X.F. conceived and designed the study. Y.S., G.H. and N..X performed the experiments. Z.J. gave some very important suggestions in the study. Y.S. and N.X. wrote the paper. X.F. and G.H. reviewed and edited the manuscript. All authors read and approved the manuscript.

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

References

1. Schneier, B. Description of a new variable-length key, 64-bit block cipher (Blowfish). In Proceedings of the Fast Software Encryption: 7th International Workshop, FSE 2000, New York, NY, USA, 10–12 April 2000; pp. 191–204.
2. Bruce, S. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*; John Wiley & Sons, Inc.: New York, NY, USA, 1996.
3. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Di Renzo, M. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27. [CrossRef]
4. Wang, H.M.; Zheng, T.X. Physical Layer Security in Heterogeneous Cellular Network. In *Physical Layer Security in Random Cellular Networks*; Springer: Singapore, 2016; pp. 61–84.
5. Wyner, A.D. The Wire-Tap Channel. *Bell Labs Techn. J.* **1975**, *54*, 1355–1387. [CrossRef]
6. Shannon, C.E. Communication theory of secrecy systems. *Bell Labs Techn. J.* **1949**, *28*, 656–715. [CrossRef]
7. Lai, L.; El Gamal, H. The relay–eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory* **2008**, *54*, 4005–4019. [CrossRef]
8. Dong, L.; Han, Z.; Petropulu, A.P.; Poor, H.V. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875–1888. [CrossRef]
9. Bassily, R.; Ulukus, S. Deaf cooperation and relay selection strategies for secure communication in multiple relay networks. *IEEE Trans. Signal Process.* **2013**, *61*, 1544–1554. [CrossRef]
10. Bassily, R.; Ulukus, S. Deaf cooperation for secrecy with multiple antennas at the helper. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1855–1864. [CrossRef]
11. Bassily, R.; Ulukus, S. Secure communication in multiple relay networks through decode-and-forward strategies. *J. Commun. Netw.* **2012**, *14*, 352–363. [CrossRef]
12. Chen, X.; Lei, L.; Zhang, H.; Yuen, C. Large-scale MIMO relaying techniques for physical layer security: AF or DF? *IEEE Trans. Wirel. Commun.* **2015**, *14*, 5135–5146. [CrossRef]
13. Chen, X.; Zhong, C.; Yuen, C.; Chen, H.H. Multi-antenna relay aided wireless physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 40–46. [CrossRef]
14. Li, Q.; Yang, Y.; Ma, W.K.; Lin, M.; Ge, J.; Lin, J. Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks. *IEEE Trans. Signal Process.* **2015**, *63*, 206–220. [CrossRef]
15. Zhang, J.; Yuen, C.; Wen, C.K.; Jin, S.; Wong, K.K.; Zhu, H. Large system secrecy rate analysis for SWIPT MIMO wiretap channels. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 74–85. [CrossRef]
16. Salem, A.; Hamdi, K.A.; Rabie, K.M. Physical layer security with RF energy harvesting in AF multi-antenna relaying networks. *IEEE Trans. Commun.* **2016**, *64*, 3025–3038. [CrossRef]
17. Liu, Y.; Chen, H.H.; Wang, L. Physical layer security for next generation wireless networks: Theories, Technologies, and Challenges. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 347–376. [CrossRef]
18. Xiang, H.; Yener, A. Secrecy and reliable Byzantine detection in a Gaussian untrusted two-hop link. In Proceedings of the 2010 IEEE Information Theory Workshop on Information Theory (ITW 2010), Cairo, Egypt, 6–8 January 2010; pp. 1–5.
19. He, X.; Yener, A. Cooperation with an untrusted relay: A secrecy perspective. *IEEE Trans. Inf. Theory* **2010**, *56*, 3807–3827. [CrossRef]
20. Hou, L.; Fu, X. Physical layer security with dynamic behaviour cooperator based on coalitional game. *IET Commun.* **2014**, *8*, 1258–1264. [CrossRef]
21. Fu, X.; Li, L.; Zong, Q. Bayesian Coalitional Game in Physical Layer Security. *Wirel. Pers. Commun.* **2015**, *85*, 1237–1250. [CrossRef]
22. Chrysikos, T.; Dagiuklas, T.; Kotsopoulos, S. Wireless information-theoretic security in an outdoor topology with obstacles: Theoretical analysis and experimental measurements. *EURASIP J. Wirel. Commun. Netw.* **2011**, *2011*. [CrossRef]

23. Mitola, J. The software radio architecture. *IEEE Commun. Mag.* **1995**, *33*, 26–38. [CrossRef]
24. Zhang, R.; Comaniciu, C.; Poor, H.V. Outage capacity and partial secrecy for energy efficient physical layer security in Gaussian fading channels. In Proceedings of the 2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC), Atlantic City, NJ, USA, 24–27 June 2013; pp. 1–5.
25. Barros, J.; Rodrigues, M.R. Secrecy capacity of wireless channels. In Proceedings of the 2006 IEEE International Symposium on Information Theory, Honolulu, HI, USA, 9–14 July 2006; pp. 356–360.
26. Wang, T.; Cano, A.; Giannakis, G.B.; Laneman, J.N. High-performance cooperative demodulation with decode-and-forward relays. *IEEE Trans. Commun.* **2007**, *55*, 1427–1438. [CrossRef]