

Exploring Relay Cooperation for Secure and Reliable Transmission in Two-Hop Wireless Networks

Yulong Shen^{1,2,*} and Yuanyu Zhang^{1,3}

¹School of Computer Science and Technology, Xidian University, China

²State Key Lab. of Integrated Service Network, Xi'an, Shaanxi, China

³School of Systems Information Science, Future University Hakodate, Japan

Abstract

This work considers the problem of secure and reliable information transmission via relay cooperation in two-hop relay wireless networks without the information of both eavesdropper channels and locations. While previous work on this problem mainly studied infinite networks and their asymptotic behavior and scaling law results, this paper focuses on a more practical network with finite number of system nodes and explores the corresponding exact result on the number of eavesdroppers one network can tolerate to ensure desired secrecy and reliability. We first study the scenario where path-loss is equal between all pairs of nodes and consider two transmission protocols there, one adopts an optimal but complex relay selection process with less load balance capacity while the other adopts a random but simple relay selection process with good load balance capacity. Theoretical analysis and numerical results are then provided to determine the maximum number of eavesdroppers one network can tolerate to ensure a desired performance in terms of the secrecy outage probability and transmission outage probability. We further extend our study to the more general scenario where path-loss between each pair of nodes also depends on the distance between them, for which a new transmission protocol with both preferable relay selection and good load balance as well as the corresponding theoretical analysis and numerical results are presented.

Received on 19 December 2013; accepted on 16 February 2014; published on 04 March 2014

Keywords: Two-Hop Wireless Networks, Cooperative Relay, Physical Layer Security, Transmission Outage, Secrecy Outage.

Copyright © 2014 Yulong Shen and Yuanyu Zhang, licensed to ICST. This is an open access article distributed under the terms of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/>), which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi:10.4108/sis.1.2.e2

1. Introduction

Two-hop ad hoc wireless networks, where each packet travels at most two hops (source-relay-destination) to reach its destination, have been a class of basic and important networking scenarios [1]. Actually, the analysis of basic two-hop relay networks serves as the foundation for performance study of general multi-hop networks. Due to the promising applications of ad hoc wireless networks in many important scenarios (like battlefield networks, vehicle networks, disaster recovery networks), the consideration of secrecy (and also reliability) in such networks is of great importance

for ensuring the high confidentiality requirements of these applications.

Traditionally, the information security is provided by adopting the cryptography approach, where a plain message is encrypted through a cryptographic algorithm that is hard to break (decrypt) in practice by any adversary without the key. The cryptography is acceptable for general applications with standard security requirement (like education system and public networks). Based on the cryptography, H. Wang et al. proposed a rule-based framework to identify and address issues of sharing for the global education system in [2], studied a problem of protecting privacy of individuals in large public survey rating data in [3] and proposed a privacy-aware access control model in web service environments in [4]. While these methods may not be sufficient for applications with a requirement

*Corresponding author. Email: ylshen@mail.xidian.edu.cn

of strong form of security (like military networks and emergency networks). This is because that the cryptographic approach can hardly achieve everlasting secrecy, since the adversary can record the transmitted messages and try any way to break them [5]. That is why there is an increasing interest in applying signaling scheme in physical layer to provide a strong form of security, where a degraded signal at an eavesdropper is always ensured such that the original data can be hardly recovered regardless of how the signal is processed at the eavesdropper. We consider applying physical layer method to achieve secure and reliable information transmission in the two-hop wireless networks. By now, a lot of research works have been dedicated to the study of physical layer security based on cooperative relays and artificial noise, and these works can be roughly classified into two categories depending on whether the information of eavesdroppers channels and locations is known or not.

For the case that the information of eavesdroppers channels and locations is available, to achieve the goal of maximizing the secrecy rates while minimizing the total transmit power, a few cooperative transmission schemes have been proposed in [6][7][8], and for two-hop wireless networks the optimal transmission strategies were presented in [9][10]. With respect to small networks, cooperative jamming with multiple relays and multiple eavesdroppers and knowledge of channels and locations was considered in [11][12]. Even if only local channel information rather than global channel state information is known, it was proved that the near-optimal secrecy rate can be achieved by cooperative jamming schemes [13][14]. Except channel information, the relative locations were also considered for optimizing cooperative jamming and power allocation to disrupt an eavesdropper with known location [15][16]. In addition, L. Lai et al. established the utility of user cooperation in facilitating secure wireless communications and proposed cooperation strategies in the additive White Gaussian Noise (AWGN) channel [17], R. Negi et al. showed how artificially generated noise can be added to the information bearing signal to achieve secrecy in the multiple and single antenna scenario under the constraint on total power transmitted by all nodes [18]. The physical layer security issue in a two-way untrusted relay system was also investigated with friendly jammers in [19][20]. The cooperative communication in mobile ad hoc networks was discussed in [21]. Effective criteria for relay and jamming node selection were developed to ensure nonzero secrecy rate in case of given sufficient relays in [22]. In practice, however, it is difficult to gain the information of eavesdropper channels and locations, since the eavesdroppers always try to hide their identity information as much as possible. To alleviate such a requirement on eavesdroppers information, some recent works explored the implementation of

secure and reliable information transmission in wireless networks without the information of both eavesdropper channels and locations.

For the case that the information of eavesdropper channels and locations is unknown, the works in [23][24] considered the secrecy for two-hop wireless networks, the works in [25][26][27] considered the secrecy for large wireless networks, and the further work in [28] considered the energy efficiency cooperative jamming strategies. These works considered how cooperative jamming by friendly nodes can impact the security of the network and compared it with a straightforward approach based on multi-user diversity. They also proposed some protocols to embed cooperative jamming techniques for protecting single links into a large multi-hop network and explored network scaling results on the number of eavesdroppers one network can tolerate. A. Sheikholeslami et al. explored the interference from multiple cooperative sessions to confuse the eavesdroppers in a large wireless network [29]. The cooperative relay scheme for the broadcast channel was further investigated in [30][31]. It is notable, however, that these works mainly focus on exploring the scaling law results in terms of the number of eavesdroppers one network can tolerate as the number of system nodes tends to infinity. Although the scaling law results are helpful for us to understand the general asymptotic network behavior, they tell us a little about the actual and exact number of eavesdroppers one network can tolerate. In practice, however, such exact results are of great interest for network designers.

This paper focuses on applying the relay cooperation to achieve secure and reliable information transmission in a more practical finite two-hop wireless network without the knowledge of both eavesdropper channels and locations. The main contributions of this paper are as follows.

- For achieving secure and reliable information transmission in a more practical two-hop wireless network with finite number of system nodes and equal path-loss between all pairs of nodes, we consider the application of the cooperative protocol proposed in [24] with an optimal and complex relay selection process but less load balance capacity, and also propose to use a new cooperative protocol with a simple and random relay selection process but good load balance capacity.
- Rather than exploring the asymptotic behavior and scaling law results, we provide theoretic analysis for above two cooperative protocols to determine the corresponding exact results on the number of eavesdroppers one network can tolerate to meet a specified requirement in terms of the maximum secrecy outage probability and

the maximum transmission outage probability allowed.

- We further extend our study to the more general and practical scenario where the path-loss between each pair of nodes also depends on their relative locations, for which we propose a new transmission protocol with both preferable relay selection and good load balance and also present the corresponding theoretical analysis under this new protocol.

The remainder of the paper is organized as follows. Section 2 presents system models and also introduces transmission outage and secrecy outage for the analysis of transmission protocols. Section 3 considers two transmission protocols for the scenario of equal path-loss between all pairs of nodes and provides the corresponding theoretical analysis and numerical results. Section 4 further presents a new transmission protocol and its theoretical analysis to address distance-dependent path-loss issue. Section 5 presents the analysis on load balance. The numerical results are in Section 6 and Section 7 concludes this paper.

2. System Models

2.1. Network Model

As illustrated in Fig.1 that we consider a network scenario where a source node S wishes to communicate securely with its destination node D with the help of multiple relay nodes R_1, R_2, \dots, R_n . In addition to these normal system nodes, there are also m eavesdroppers E_1, E_2, \dots, E_m that are independent and also uniformly distributed in the network. Our goal here is to ensure the secure and reliable information transmission from source S to destination D under the condition that no real time information is available about both eavesdropper channels and locations.

2.2. Transmission Model

Consider the transmission from a transmitter A to a receiver B , and denote by $x_i^{(A)}$ the i^{th} symbol transmitted by A and denote by $y_i^{(B)}$ the i^{th} signal received by B . We assume that all nodes transmit with the same power E_s , path-loss between all pairs of nodes is independent, and the frequency-nonspecific multi-path fading from A to B is a complex zero-mean Gaussian random variable. The fading is assumed constant during K message transmissions, called flat interval hereafter, and varies randomly and independently from interval to interval. Under the condition that all nodes in a group of nodes, \mathcal{R} , are generating noises, the i^{th} signal received at node B from node A is determined as:

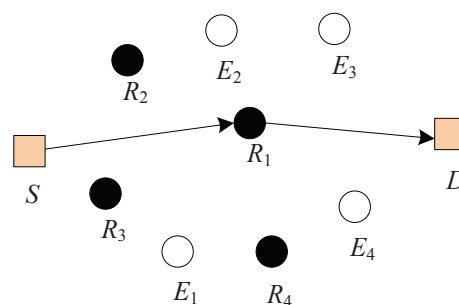


Figure 1. System scenario: Source S wishes to communicate securely with destination D with the assistance of finite relays R_1, R_2, \dots, R_n ($n=4$ in the figure) in the presence of passive eavesdroppers E_1, E_2, \dots, E_m ($m=4$ in the figure). Cooperative relay scheme is used in the two-hop transmission. A assistant node is selected randomly as relay (R_1 in the figure).

$$y_i^{(B)} = \frac{h_{A,B}}{d_{A,B}^{\alpha/2}} \sqrt{E_s} x_i^{(A)} + \sum_{A_i \in \mathcal{R}} \frac{h_{A_i,B}}{d_{A_i,B}^{\alpha/2}} \sqrt{E_s} x_i^{(A_i)} + n_i^{(B)}$$

where $d_{A,B}$ is the distance between nodes A and B , $\alpha \geq 2$ is the path-loss exponent. The noise $\{n_i^{(B)}\}$ at receiver B is assumed to be i.i.d complex Gaussian random variables with $E[|n_i^{(B)}|^2] = N_0$, and $|h_{A,B}|^2$ is exponentially distributed with mean $E[|h_{A,B}|^2]$. Without loss of generality, we assume that $E[|h_{A,B}|^2] = 1$. The SINR $C_{A,B}$ from A to B is then given by

$$C_{A,B} = \frac{E_s |h_{A,B}|^2 d_{A,B}^{-\alpha}}{\sum_{A_i \in \mathcal{R}} E_s |h_{A_i,B}|^2 d_{A_i,B}^{-\alpha} + N_0/2}$$

In the wireless transmission, the receiver can decode the message if and only if the received signal quality is better than a special threshold. In this paper, for a legitimate node and an eavesdropper, we use two separate SINR thresholds γ_R and γ_E to define the minimum SINR required to recover the transmitted messages, respectively. Therefore, a receiver (relay or destination) is able to decode a packet if and only if the SINR at receiver is greater than γ_R , while the transmitted message is secure if and only if the SINR at each eavesdropper is less than γ_E . In this paper, γ_R and γ_E depend on the sensitivity of the receiver. When the node is manufactured, the SINR threshold is determined. In the subsequent analysis on the numerical results, (γ_R, γ_E) is fixed as $(0.5, 0.5)$ for Protocol 1 and 2, and $(0.5, 15)$ for Protocol 3. If the eavesdroppers are original system nodes which are captured by the adversary, the SINR threshold γ_E can

be identical to γ_R . If the eavesdroppers are illegal nodes distributed by the adversary, γ_E is not relative to γ_R .

2.3. Transmission Outage and Secrecy Outage

For a transmission from the source S to destination D , we call transmission outage happens if D can not decode the transmitted packet, i.e., D received the packet with SINR less than the predefined threshold γ_R . The transmission outage probability, denoted as $P_{out}^{(T)}$, is then defined as the probability that transmission outage from S to D happens.

We predefined a upper bound ε_t on $P_{out}^{(T)}$, which is an extremely small quantity and if the $P_{out}^{(T)}$ is less than ε_t , the communication is regarded as reliable. ε_t is determined according to the transmission outage the application can tolerate. For the video transmission, it can be tolerated that some messages are lost, thus ε_t can take a larger value i.e. 10^{-1} . For the applications in which the messages can not be lost, ε_t can take a smaller value i.e. 10^{-2} .

We call the communication between S and D is reliable if $P_{out}^{(T)} \leq \varepsilon_t$. Notice that for the transmissions from S to the selected relay R_{j^*} and from R_{j^*} to D , the corresponding transmission outage can be defined in the similar way as that of from S to D . We use $O_{S \rightarrow R_{j^*}}^{(T)}$ and $O_{R_{j^*} \rightarrow D}^{(T)}$ to denote the events that transmission outage from source S to R_{j^*} happens and transmission outage from relay R_{j^*} to D happens, respectively. Due to the link independence assumption, we have

$$P_{out}^{(T)} = P\left(O_{S \rightarrow R_{j^*}}^{(T)}\right) + P\left(O_{R_{j^*} \rightarrow D}^{(T)}\right) - P\left(O_{S \rightarrow R_{j^*}}^{(T)}\right) \cdot P\left(O_{R_{j^*} \rightarrow D}^{(T)}\right)$$

Regarding the secrecy outage, we call secrecy outage happens for a transmission from S to D if at least one eavesdropper can recover the transmitted packets during the process of this two-hop transmission, i.e., at least one eavesdropper received the packet with SINR larger than the predefined threshold γ_E . The secrecy outage probability, denoted as $P_{out}^{(S)}$, is then defined as the probability that secrecy outage happens during the transmission from S to D .

We predefined a upper bound ε_s on $P_{out}^{(S)}$, which is an extremely small quantity and if the $P_{out}^{(S)}$ is less than ε_s , the communication is regarded as secure. ε_s is determined by the amount of messages obtained by the eavesdroppers can be tolerated which represents a level of security. If the higher secure level is required, ε_s can take a smaller value i.e. 10^{-1} . Otherwise, ε_s can take a larger value i.e. 0.2, which means it is able to tolerate 20% messages obtained by the eavesdroppers.

We call the communication between S and D is secure if $P_{out}^{(S)} \leq \varepsilon_s$. Notice that for the transmissions

from S to the selected relay R_{j^*} and from R_{j^*} to D , the corresponding secrecy outage can be defined in the similar way as that of from S to D . We use $O_{S \rightarrow R_{j^*}}^{(S)}$ and $O_{R_{j^*} \rightarrow D}^{(S)}$ to denote the events that secrecy outage from source S to R_{j^*} happens and secrecy outage from relay R_{j^*} to D happens, respectively. Again, due to the link independence assumption, we have

$$P_{out}^{(S)} = P\left(O_{S \rightarrow R_{j^*}}^{(S)}\right) + P\left(O_{R_{j^*} \rightarrow D}^{(S)}\right) - P\left(O_{S \rightarrow R_{j^*}}^{(S)}\right) \cdot P\left(O_{R_{j^*} \rightarrow D}^{(S)}\right)$$

3. Secure and Reliable Transmission under Equal Path-Loss

In this section, we consider the case where the path-loss is equal between all pairs of nodes in the system (i.e., we set $d_{A,B} = 1$ for all $A \neq B$). We first introduce two transmission protocols considered for such scenario, and then provide theoretical analysis to determine the numbers of eavesdroppers one network can tolerate under these protocols.

3.1. Transmission Protocols

The first protocol we consider (hereafter called Protocol 1) is the one proposed in [24], in which the optimal relay node with the best link condition to both source and destination is always selected for information relaying. Notice that although the Protocol 1 can guarantee the optimal relay node selection, it suffers from several problems. Protocol 1 involves a complicated process of optimal relay selection, which is not very suitable for the distributed wireless networks, in particular when the number of possible relay nodes is huge. More importantly, since the channel state is relatively constant during a fixed time period, some relay nodes with good link conditions are always preferred for information relaying, resulting in a severe load balance problem and a quick node energy depletion in energy-limited wireless environment.

Based on above observations, we propose to use a simple and random relay selection rather than the optimal relay selection in Protocol 1 to achieve a better load balance among relay nodes in terms of the energy consumption. Notice that the energy consumption hereafter indicates the energy consumed by each relay for relaying message to the destination for the source. By modifying the Protocol 1, the new transmission protocol (hereafter called Protocol 2) works as follows.

- 1) **Relay selection:** A relay node, indexed by j^* , is randomly selected from all candidate relay nodes $R_j, j = 1, 2, \dots, n$.
- 2) **Channel measurement:** The selected relay R_{j^*} broadcasts a pilot signal to allow each of other

relays to measure the channel from R_{j^*} to itself. Each of the other relays $R_j, j = 1, 2, \dots, n, j \neq j^*$ then knows the corresponding value of $h_{R_j, R_{j^*}}$. Similarly, the destination D broadcasts a pilot signal to allow each of other relays to measure the channel from D to itself. Each of the other relays $R_j, j = 1, 2, \dots, n, j \neq j^*$ then knows the corresponding value of $h_{R_j, D}$.

- 3) **Two-hop transmission:** The source S transmits the messages to the selected relay R_{j^*} , and concurrently, the relay nodes with indexes in $\mathcal{R}_1 = \left\{ j \neq j^* : |h_{R_j, R_{j^*}}|^2 < \tau \right\}$ transmit noise to generate interference at eavesdroppers. The relay R_{j^*} then transmits the messages to destination D , and concurrently, the relay nodes with indexes in $\mathcal{R}_2 = \left\{ j \neq j^* : |h_{R_j, D}|^2 < \tau \right\}$ transmit noise to generate interference at eavesdroppers.

Remark 1: The parameter τ involved in the Protocol 1 and Protocol 2 serves as the threshold on fading, based on which the set of noise generating relay nodes can be identified. Notice that a too large τ may disable legitimate transmission, while a too small τ may not be sufficient for interrupting all eavesdroppers. Thus, the parameter τ should be set properly to ensure both secrecy requirement and reliability requirement.

Remark 2: The two protocols considered here have their own advantages and disadvantages and thus are suitable for different network scenarios. For the protocol 1, it can achieve a better performance in terms of the number of eavesdroppers can be tolerated (see Theorem 1). However, it involves a complex relay selection process, and more importantly, it results in an unbalanced load and energy consumption distribution among systems nodes. Thus, such protocol is suitable for small scale wireless network with sufficient energy supply rather than large and energy-limited wireless networks (like wireless sensor networks). Regarding the Protocol 2, although it can tolerate less number eavesdroppers in comparison with the Protocol 1 (see Theorem 2), it involves a very simple random relay selection process to achieve a good load and energy consumption distribution among system nodes. Thus, this protocol is more suitable for large scale wireless network environment with stringent energy consumption constraint.

3.2. Analysis of Protocol 1

We now analyze that under the Protocol 1 the number of eavesdroppers one network can tolerate subject to specified requirements on transmission outage and secrecy outage. We first establish the following two lemmas regarding some basic properties of $P_{out}^{(T)}$, $P_{out}^{(S)}$

and τ , which will help us to derive the main result in Theorem 1.

Lemma 1: Consider the network scenario of Fig.1 with equal path-loss between all pairs of nodes, under the Protocol 1 the transmission outage probability $P_{out}^{(T)}$ and secrecy outage probability $P_{out}^{(S)}$ there satisfy the following conditions.

$$P_{out}^{(T)} \leq 2 \left[1 - e^{-2\gamma_R(n-1)(1-e^{-\tau})\tau} \right]^n - \left[1 - e^{-2\gamma_R(n-1)(1-e^{-\tau})\tau} \right]^{2n}$$

$$P_{out}^{(S)} \leq 2m \cdot \left(\frac{1}{1 + \gamma_E} \right)^{(n-1)(1-e^{-\tau})} - \left[m \cdot \left(\frac{1}{1 + \gamma_E} \right)^{(n-1)(1-e^{-\tau})} \right]^2$$

The proof of Lemma 1 can be found in the Appendix A.

Lemma 2: Consider the network scenario of Fig.1 with equal path-loss between all pairs of nodes, to ensure $P_{out}^{(T)} \leq \varepsilon_t$ and $P_{out}^{(S)} \leq \varepsilon_s$ under the Protocol 1, the parameter τ must satisfy the following condition.

$$\tau \in \left[-\log \left[1 + \frac{\log \left(\frac{1 - \sqrt{1 - \varepsilon_s}}{m} \right)}{(n-1) \log(1 + \gamma_E)} \right], \sqrt{\frac{-\log \left[1 - \left(1 - \sqrt{1 - \varepsilon_t} \right)^{\frac{1}{n}} \right]}{2\gamma_R(n-1)}} \right]$$

The proof of Lemma 2 can be found in the Appendix B.

Based on the results of Lemma 2, we now can establish the following theorem regarding the performance of Protocol 1.

Theorem 1. Consider the network scenario of Fig.1 with equal path-loss between all pairs of nodes. To guarantee $P_{out}^{(T)} \leq \varepsilon_t$ and $P_{out}^{(S)} \leq \varepsilon_s$ under the Protocol 1, the number of eavesdroppers m one network can tolerate must satisfy the following condition.

$$m \leq \left(1 - \sqrt{1 - \varepsilon_s} \right) \cdot (1 + \gamma_E) \sqrt{\frac{-(n-1) \log \left[1 - \left(1 - \sqrt{1 - \varepsilon_t} \right)^{\frac{1}{n}} \right]}{2\gamma_R}}$$

The proof of Theorem 1 can be found in the Appendix C.

3.3. Analysis of Protocol 2

Similar to the analysis of Protocol 1, we first establish the following two lemmas regarding some basic properties of $P_{out}^{(T)}$, $P_{out}^{(S)}$ and τ under the Protocol 2.

Lemma 3: Consider the network scenario of Fig.1 with equal path-loss between all pairs of nodes, the transmission outage probability $P_{out}^{(T)}$ and secrecy

outage probability $P_{out}^{(S)}$ under the Protocol 2 satisfy the following conditions.

$$P_{out}^{(T)} \leq 2 \left[1 - e^{-\gamma_R(n-1)(1-e^{-\tau})} \right] - \left[1 - e^{-\gamma_R(n-1)(1-e^{-\tau})} \right]^2$$

$$P_{out}^{(S)} \leq 2m \cdot \left(\frac{1}{1 + \gamma_E} \right)^{(n-1)(1-e^{-\tau})} - \left[m \cdot \left(\frac{1}{1 + \gamma_E} \right)^{(n-1)(1-e^{-\tau})} \right]^2$$

The proof of Lemma 3 can be found in the Appendix D.

Lemma 4: Consider the network scenario of Fig.1 with equal path-loss between all pairs of nodes, to ensure $P_{out}^{(T)} \leq \epsilon_t$ and $P_{out}^{(S)} \leq \epsilon_s$ under the Protocol 2, the parameter τ must satisfy the following condition.

$$\tau \in \left[-\log \left[1 + \frac{\log \left(\frac{1-\sqrt{1-\epsilon_s}}{m} \right)}{(n-1) \log(1 + \gamma_E)} \right], \sqrt{\frac{-\log(1 - \epsilon_t)}{2\gamma_R(n-1)}} \right]$$

The proof of Lemma 4 can be found in the Appendix E.

Theorem 2. Consider the network scenario of Fig.1 with equal path-loss between all pairs of nodes. To guarantee $P_{out}^{(T)} \leq \epsilon_t$ and $P_{out}^{(S)} \leq \epsilon_s$ based on the Protocol 2, the number of eavesdroppers m the network can tolerate must satisfy the following condition.

$$m \leq \left(1 - \sqrt{1 - \epsilon_s} \right) \cdot (1 + \gamma_E) \sqrt{\frac{-(n-1) \log(1 - \epsilon_t)}{2\gamma_R}}$$

The proof of Theorem 2 can be found in the Appendix F.

Remark 3: It can be observed that the right hand side in Theorem 1 is larger than that of Theorem 2, when all the given parameters are same for Theorem 1 and 2. This means that more eavesdroppers can be tolerated in the network applying Protocol 1 than Protocol 2, given the same system settings and reliability and security requirements.

4. Secure and Reliable Transmission under Distance-Dependent Path-Loss

In this section, we consider the more general scenario where the path-loss between each pair of nodes also depends on the distance between them. We first introduce the coordinate system adopted in our discussion, and then propose a flexible transmission protocol to achieve both the preferable relay selection and good load balance under such distance-dependent path-loss scenario. The related theoretic analysis is further provided to determine the number of eavesdroppers one network can tolerate by adopting this protocol.

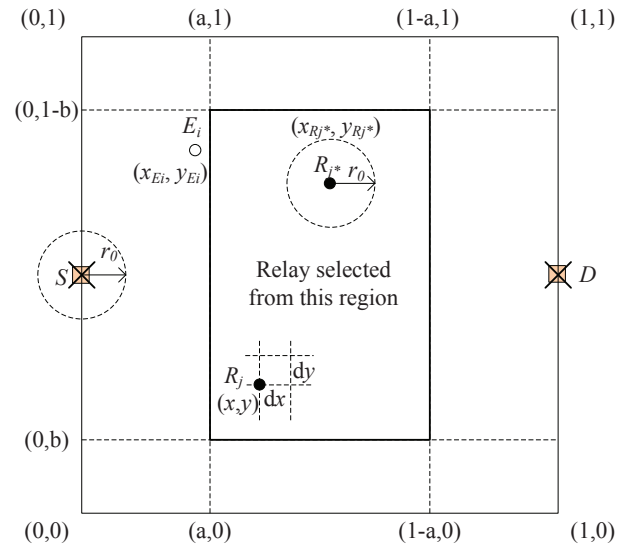


Figure 2. Coordinate system for the scenario where path-loss between pairs of nodes is based on their relative locations.

4.1. Coordinate System

To address the distance-dependent path-loss, we consider a two-hop relay wireless network deployed in a square of unit area and defined by the coordinate system shown in Fig.2, where the source S located at coordinate $(0, 0.5)$ wishes to establish two-hop transmission with destination D located at coordinate $(1, 0.5)$. Since only one $S - D$ pair is considered in this paper, we can define a coordinate axis system with x -axis parallel to the segment $S - D$. In addition to the source S and destination D , we assume that there are n cooperative relays and m eavesdroppers of unknown channels and locations independently and uniformly distributed in the network area. This scenario is similar to ones in [23][24] [29].

4.2. Transmission Protocol

Notice that under the distance-dependent path-loss scenario, the further the distance between a transmitter and a receiver, the weaker the signal received at the receiver. Thus, the system nodes located in the middle region between source S and destination D are preferable relays. Based on such observation, we propose here a general and practical protocol (hereafter called Protocol 3) to ensure both the preferable relay selection and good load balance for distance-dependent path-loss scenario, which works as follow.

- 1) **Relay selection:** We first define a relay selection region $[a, 1 - a] \times [b, 1 - b]$ between source S and destination D , where a and b are two parameters determining the area of the selection region. Since

this region is located in the normalized network, we can scale it such that $0 \leq a \leq 0.5, 0 \leq b \leq 0.5$. A relay node, indexed by j^* , is then selected randomly from relays falling within the relay selection region.

- 2) **Channel measurement:** Each of the other relays measures the channel from the selected relay R_{j^*} and destination D by accepting the pilot signal from R_{j^*} and D for determining the noise generation nodes.
- 3) **Two-hop transmission:** The source S and the selected relay R_{j^*} transmit the messages in two-hop transmission. Concurrently, the relay nodes with indexes in $\mathcal{R}_1 = \{j \neq j^* : |h_{R_j, R_{j^*}}|^2 < \tau\}$ in the first hop and the relay nodes with indexes in $\mathcal{R}_2 = \{j \neq j^* : |h_{R_j, D}|^2 < \tau\}$ in the second hop transmit noise respectively to help transmission.

Remark 4: In the Protocol 3, a trade off between the preferable relay selection and better load balance can be controlled through the parameters a and b , which determine the relay selection region. As to be shown in Theorem 3 that by adopting a small value for both a and b (i.e., a larger relay selection region), a better load balance capacity can be achieved at the cost of a smaller number of eavesdroppers one network can tolerate.

4.3. Analysis of Protocol 3

To address the near eavesdropper problem and also to simplify the analysis for the Protocol 3, we assume that there exists a constant $r_0 > 0$ such that any eavesdropper falling within a circle area with radius r_0 and center S or R_{j^*} can eavesdrop the transmitted messages successfully with probability 1, while any eavesdropper beyond such area can only successfully eavesdrop the transmitted messages with a probability less than 1. Based on such a simplification, we can establish the following two lemmas regarding some basic properties of $P_{out}^{(T)}, P_{out}^{(S)}$ and τ under this protocol.

Lemma 5: Consider the network scenario of Fig.2, under the Protocol 3 the transmission outage probability $P_{out}^{(T)}$ and secrecy outage probability $P_{out}^{(S)}$ there satisfy the following conditions.

$$P_{out}^{(T)} \leq \left[1 - e^{-\frac{\gamma_R \tau (n-1)(1-e^{-\tau})}{\phi^{-\alpha}} (\varphi_1 + \varphi_2)} \right] (1 - \vartheta) + 1 \cdot \vartheta$$

$$P_{out}^{(S)} \leq 2m \left[\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha} \right)^{(n-1)(1-e^{-\tau})} (1 - \pi r_0^2) \right] - \left[m \left(\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha} \right)^{(n-1)(1-e^{-\tau})} (1 - \pi r_0^2) \right) \right]^2$$

here,

$$\vartheta = \left[1 - (1 - 2a)(1 - 2b) \right]^n$$

$$\varphi_1 = \int_0^1 \int_0^1 \frac{1}{[(x-0.5)^2 + (y-0.5)^2]^{\frac{\alpha}{2}}} dx dy$$

$$\varphi_2 = \int_0^1 \int_0^1 \frac{1}{[(x-1)^2 + (y-0.5)^2]^{\frac{\alpha}{2}}} dx dy$$

$$\phi = \sqrt{(1-a)^2 + (0.5-b)^2}$$

$$\psi = \int_0^1 \int_0^1 \frac{1}{(x^2 + y^2)^{\frac{\alpha}{2}}} dx dy$$

The proof of the Lemma 5 can be found in the Appendix G.

Lemma 6: Consider the network scenario of Fig.2, to ensure $P_{out}^{(T)} \leq \epsilon_t$ and $P_{out}^{(S)} \leq \epsilon_s$ by applying the Protocol 3, the parameter τ must satisfy the following condition.

$$\tau \in \left[-\log \left[1 + \frac{\log \left(\frac{1 - \sqrt{1 - \epsilon_s} - \pi r_0^2}{1 - \pi r_0^2} \right)}{(n-1) \log(1 + \gamma_E \psi r_0^\alpha)} \right], \sqrt{\frac{-\log \left(\frac{1 - \epsilon_t}{1 - \vartheta} \right) \phi^{-\alpha}}{\gamma_R (n-1) (\varphi_1 + \varphi_2)}} \right]$$

here, $\vartheta, \varphi_1, \varphi_2, \phi$ and ψ are defined in the same way as that in Lemma 5.

The proof of the Lemma 6 can be found in the Appendix H.

Based on the results of Lemma 6, we now can establish the following theorem about the performance of Protocol 3.

Theorem 3. Consider the network scenario of Fig.2. To guarantee $P_{out}^{(T)} \leq \epsilon_t$ and $P_{out}^{(S)} \leq \epsilon_s$ based on the Protocol 3, the number of eavesdroppers m the network can tolerate must satisfy the following condition.

$$m \leq \frac{1 - \sqrt{1 - \epsilon_s}}{\pi r_0^2 + (1 - \pi r_0^2) \omega}$$

here,

$$\omega = (1 + \gamma_E \psi r_0^\alpha)^{-\sqrt{\frac{-(n-1) \log \left(\frac{1 - \epsilon_t}{1 - \vartheta} \right)}{\gamma_R (\varphi_1 + \varphi_2) \phi^\alpha}}}$$

$\vartheta, \varphi_1, \varphi_2, \phi$ and ψ are defined in the same way as that in Lemma 5.

The proof of the Lemma 6 can be found in the Appendix I.

Remark 5: From the practical point of view, the two-hop transmissions are not independent as the common relay is used. In practical, the distance between source S and the selected relay R_{j^*} is correlative with the distance between the selected relay R_{j^*} and destination D . However, the independence assumption has no any affects on our results, which is described as follow. 1) In the case of equal path-loss (described in the section 3), the channel state information is exponentially distributed, which is independent of distance between transmitter and receiver. Thus, in this case, this assumption holds. 2) In the case of distance-dependent path-loss (described in this section), in each hop, the worst case about distance between source S and the selected relay R_{j^*} and between the selected relay R_{j^*} and destination D is considered, and a minimum value of maximum number of eavesdroppers one network can tolerate is obtained. Thus this assumption has no affect on our results.

5. Analysis on Load Balance

Load balance is used to characterize how the energy consumptions among n system relays are balanced. For the three protocols considered in this paper, we denote the corresponding load balance by $L^{(1)}, L^{(2)}$ and $L^{(3)}$. Recall that each of the channels stays constant during K message transmissions (i.e., flat interval). We assume that total N messages are transmitted are from the source S to the destination D and the unit energy consumption of one message transmission is I_0 for the message relay. In addition, we define the expectation of the energy consumption for each relay $R_i, i = 1, 2, \dots, n$ under protocol 1, 2 and 3 by $C_i^{(1)}, C_i^{(2)}$ and $C_i^{(3)}$ and variance by $\sigma_i^{(1)}, \sigma_i^{(2)}$ and $\sigma_i^{(3)}$, respectively. In order to analyze the load balance performance of different protocols, we simply characterize it as follows

$$L^{(A)} \propto \frac{\max_i C_i^{(A)} - \min_i C_i^{(A)}}{\sum_{i=1}^n C_i^{(A)}} \propto \frac{\sigma_i^{(A)}}{E[C_i^{(A)}]}$$

, where $A = 1, 2$ and 3 . Notice that the larger the $L^{(A)}$ is, the worse the energy consumption is balanced among n relays.

5.1. Analysis of Protocol 1

As the flat interval is K message transmissions, there are $\frac{N}{K}$ intervals in each of which all the channels stay constant. We define the number of such intervals in which relay $R_i, i = 1, 2, \dots, n$ is selected as the message relays by Y_i . Notice that a relay is always selected as

the message relay during the same interval. Hence, the energy consumption of relay R_i is $C_i^{(1)} = I_0 K Y_i$. Defining the event that relay R_i is selected as the message relay in one interval by A_i , we have

$$\begin{aligned} P(A_i) &= \int_0^\infty P(A_i | x) f(x) dx \\ &= \int_0^\infty \prod_{j=1, j \neq i}^n P(\min(|h_{S,R_j}|^2, |h_{R_j,D}|^2) \leq x) f(x) dx \\ &= \int_0^\infty 2(1 - e^{-2x})^{n-1} e^{-2x} dx \\ &= \frac{1}{n} \end{aligned}$$

where $f(x) = 2e^{-2x}$ for $x > 0$ is the pdf of $\min(|h_{S,R_i}|^2, |h_{R_i,D}|^2)$. From the above, we know that Y_i is a binomial random variable with parameters $\frac{N}{K}$ and $\frac{1}{n}$. Therefore, the expected energy consumption of each relay R_i is

$$E[C_i^{(1)}] = I_0 K E[Y_i] = \frac{I_0 N}{n}$$

and the variance is

$$\sigma_i^{(1)} = I_0^2 K^2 \sigma_{Y_i} = K \frac{I_0^2 N(n-1)}{n^2}$$

Consequently,

$$L^{(1)} \propto \frac{\sigma_i^{(1)}}{E[C_i^{(1)}]} = K \frac{I_0(n-1)}{n}$$

5.2. Analysis of Protocol 2

For each relay $R_i, i = 1, 2, \dots, n$, define the times of being selected as the message relay among N transmissions by X_i . Obviously, $C_i^{(2)} = I_0 X_i$. Since the message relay is randomly selected, the probability that relay R_i is selected as the message relay is $\frac{1}{n}$ for each transmission, resulting in X_i is a binomial random variable with parameters N and $\frac{1}{n}$. Therefore, the expected energy consumption of each relay R_i is

$$E[C_i^{(2)}] = I_0 E[X_i] = \frac{I_0 N}{n}$$

and the variance is

$$\sigma_i^{(2)} = I_0^2 \sigma_{X_i} = \frac{I_0^2 N(n-1)}{n^2}$$

At last,

$$L^{(2)} \propto \frac{\sigma_i^{(2)}}{E[C_i^{(2)}]} = \frac{I_0(n-1)}{n} = \frac{L^{(1)}}{K}$$

Following the above, we can observe that the random relay selection protocol outperforms the optimal relay selection protocol in terms of the load balance performance.

Remark 6: We notice that the expected number of messages suffering from transmission outage and secrecy outage during N transmissions are $K \cdot \frac{N}{K} P_{out}^{(T)} = NP_{out}^{(T)}$ and $K \cdot \frac{N}{K} P_{out}^{(S)} = NP_{out}^{(S)}$ for Protocol 1, and $NP_{out}^{(T)}$ and $NP_{out}^{(S)}$ for Protocol 2. Besides, the variance of the number of message suffering from outages are $KNP_{out}^{(T)}(1 - P_{out}^{(T)})$ and $KNP_{out}^{(S)}(1 - P_{out}^{(S)})$ for Protocol 1, and $NP_{out}^{(T)}(1 - P_{out}^{(T)})$ and $NP_{out}^{(S)}(1 - P_{out}^{(S)})$ for Protocol 2. Here, $P_{out}^{(T)}$ and $P_{out}^{(S)}$ are the transmission outage probability and secrecy outage probability of the corresponding protocol. The derivation is similar to that of the load balance and thus is omitted here. Therefore, it can be observed that the non-stationary channel has no impact on the reliability and security for these protocols, while the variance of the number of messages suffering from outages increase with K for Protocol 1.

5.3. Analysis of Protocol 3

Similarly, for each relay $R_i, i = 1, 2, \dots, n$, we define the times of being selected as the message relay among N message transmissions by Z_i and the energy consumption by $C_i^{(3)}$, which is a function of parameters a and b . Here, we neglect the case ($a = 0.5, b = 0.5$) where no relays will be selected as the message relay and thus the transmission could not be conducted. Again, we have $C_i^{(3)} = I_0 Z_i$. According to the relay selection protocol, each relay R_i lies in the relay selection region with probability $p = (1 - 2a)(1 - 2b)$. Furthermore, we define the event that relay R_i is selected as the message relay during one transmission by B_i . Thus, $P(B_i) = \frac{p}{U+1}$ where $U \sim B(n-1, p)$ is the number of relays in the relay selection region in addition to R_i . Applying the law of total probability,

$$\begin{aligned} P(B_i) &= E\left[\frac{p}{U+1}\right] \\ &= \sum_{k=0}^{n-1} \frac{p}{k+1} \binom{n-1}{k} p^k (1-p)^{n-1-k} \\ &= \sum_{k=0}^{n-1} \frac{1}{n} \binom{n}{k+1} p^{k+1} (1-p)^{n-1-k} \\ &= \frac{1}{n} \sum_{j=1}^n \binom{n}{j} p^j (1-p)^{n-j} \\ &= \frac{1 - (1-p)^n}{n} \end{aligned}$$

Following the above, Z_i is a binomial random variable with parameters N and $\frac{1-(1-p)^n}{n}$. Therefore, the

expectation of the energy consumption for each relay R_i is

$$E\left[C_i^{(3)}\right] = I_0 E[Z_i] = \frac{I_0 N (1 - (1-p)^n)}{n}$$

and the variance is

$$\sigma_i^{(3)} = I_0^2 \sigma_{Z_i} = \frac{I_0^2 N (1 - (1-p)^n)}{n} \left(1 - \frac{1 - (1-p)^n}{n}\right)$$

Thus, the load balance of protocol 3 is

$$L^{(3)} \propto \frac{\sigma_i^{(3)}}{E[C_i^{(3)}]} = I_0 \left(1 - \frac{1 - (1-p)^n}{n}\right)$$

Notice that p decreases as the parameters a or b (i.e., the area of the relay selection region) increases. Therefore, $L^{(3)}$ increases with increasing a and b , implying that enlarging the relay selection region can achieve better load balance performance. It is notable that each relay can be selected as the message relay with probability $1/n$ in the case ($a = 0, b = 0$), which reduces to the Protocol 2 where the message relay is randomly selected from the whole region. Therefore, the load balance of Protocol 3 in this case is identical to that of Protocol 2.

6. Numerical Results

6.1. The Number of Eavesdroppers one Networks can Tolerate

To compare the number of eavesdroppers can be tolerated by Protocol 1 with that of Protocol 2, we show in Fig.3 and Fig.4 respectively how the number of eavesdroppers can be tolerated varies with the number of system relays n when $\varepsilon_t = 0.1$, $\varepsilon_s = 0.1$, $\gamma_R = 0.5$ and $\gamma_E = 0.5$. From these two figures, we can see clearly that the number of eavesdroppers can be tolerated increases exponentially with the number of system relays n as n increases by a proper step (i.e., 10 in Protocol 1 and 100 in Protocol 2). This is because as the number of relays increase, although the threshold τ decreases in order to guarantee the reliability requirement, the expected number of noise-generating nodes increases, resulting in more interference can be generated to suppress the eavesdroppers. It can also be observed from Fig.3 and Fig.4 that Protocol 1 can tolerate significantly more eavesdroppers than Protocol 2. For instance, when the number of relays n is less than 200, Protocol 2 can hardly tolerate any eavesdroppers while Protocol 1 can tolerate relative large number of eavesdroppers. This is due to the reason that larger value of τ can be adopted in Protocol 1 than Protocol 2 under the same reliability requirement (i.e., ε_t) and number of relays n and also the number of eavesdroppers can be tolerated is relatively sensitive to the threshold τ .

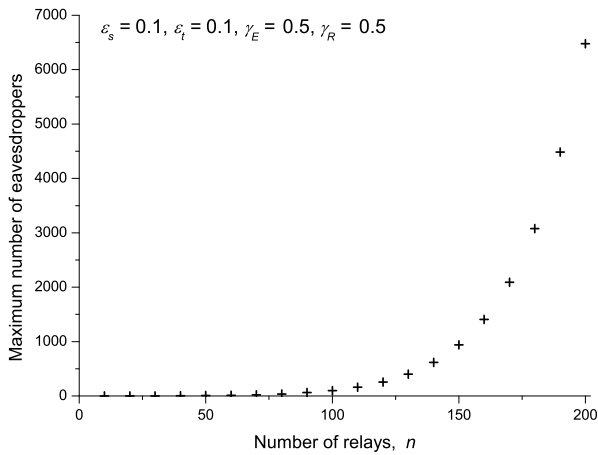


Figure 3. Maximum number of eavesdroppers for Protocol 1 vs. n , when $\varepsilon_t = 0.1$, $\varepsilon_s = 0.1$, $\gamma_R = 0.5$ and $\gamma_E = 0.5$.

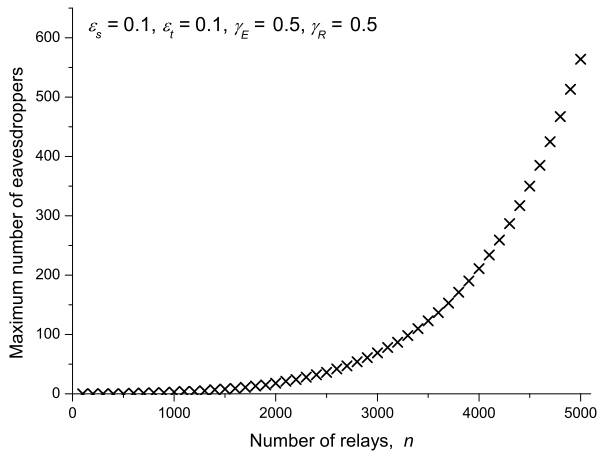


Figure 4. Maximum number of eavesdroppers for Protocol 2 vs. n , when $\varepsilon_t = 0.1$, $\varepsilon_s = 0.1$, $\gamma_R = 0.5$ and $\gamma_E = 0.5$.

Fig.5 shows the maximum number of eavesdroppers one network can tolerate for Protocol 3 with $r_0 = 0.1$, $\varepsilon_t = 0.2$, $\varepsilon_s = 0.2$ and $\gamma_E = 15$. In Fig.5, the number of eavesdroppers one network can tolerate is small than that of protocol 1 and protocol 2. There are two reasons. On the one hand, For reliable transmission, the worse case that the noise generation nodes can be very near to the receivers (the selected relay or destination) exists and is considered, thus the receivers will be disturbed seriously. On the other hand, the case that the eavesdroppers can be near to the transmitters (source or the selected relay) exists and is considered, especially any eavesdropper falling within a circle area with radius r_0 and center S or R_j can eavesdrop the

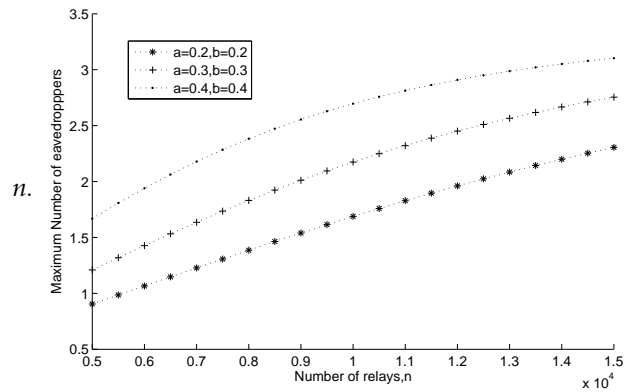


Figure 5. Maximum number of eavesdroppers for Protocol 3 vs.

transmitted messages successfully with probability 1. In the practical networks, these case dose not always happen thus more eavesdroppers can be tolerated.

6.2. Load Balance among Relays

In order to clearly illustrate the load balance performances of different transmission protocols, simulations are conducted under the settings of $n = 20$, $N = 1000$ and $I_0 = 1$. The comparison between the load balance of optimal relay selection protocol and random relay selection protocol is shown in Fig.6 and we present how the load balance of protocol 3 varies with the area of relay selection region in Fig.7. For ease of simulation, the load balance is represented by the ratio $\frac{\max_i C_i^{(A)} - \min_i C_i^{(A)}}{\sum_{i=1}^n C_i^{(A)}}$ defined above.

The Fig.6 indicates clearly that the load balance of random relay selection stays constant with varying flat interval K whereas the load balance of optimal relay selection protocol increase as the flat interval K increases, which implies that the random relay selection protocol can achieve better load balance than the optimal relay selection protocol.

It can be easily observed from Fig.7 that there is a clear threshold (about 1.0 in Fig.7) of the area of relay selection region beyond which the load balance performance cannot be improved by enlarging the area of the relay selection. However, the load balance decreases dramatically from 0.14 to 0.028 (i.e.,the load balance performance is improved) with the area of relay selection region below the threshold. This is due to the reason that the probability $P(B_i)$ increases significantly (from 0.00158 to 0.0439) with the area of the relay selection region when the latter is below the threshold and increases slowly (from 0.0439 to 0.05) when the latter is above the threshold.

A further careful observation of Fig.6, Fig.3 and Fig.4 indicates that Protocol 1 is suitable for small

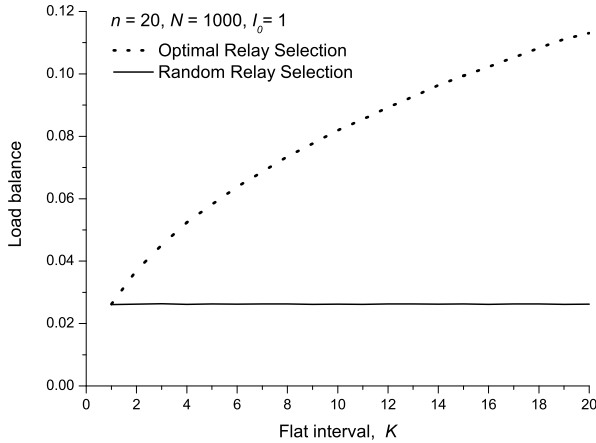


Figure 6. Comparisons between the load balance performance of protocol 1 and 2, when $n = 20, N = 1000$ and $I_0 = 1$.

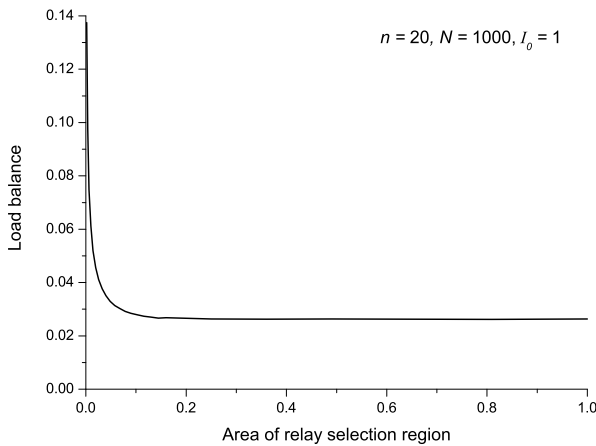


Figure 7. Load balance performance of protocol 3 vs. Area of relay selection region when $n = 20, N = 1000$ and $I_0 = 1$.

networks and Protocol 2 is suitable for large networks with both the considerations of eavesdropper tolerance capability and load balance performance, according with the Remark 2.

Remark 7: Regarding the performances of Protocol 1 and Protocol 2, both of which are proposed in the scenario with equal path loss, we notice that although Protocol 1 has a better eavesdropper-tolerance capability than Protocol 2, it has a worse load balance performance than Protocol 2. Hence, clear tradeoff exists for these two protocols. Therefore, Protocol 1 is suitable for the applications requiring strong security with acceptable load balance performance, while Protocol 2 is suitable for the applications

requiring good load balance with acceptable security requirement. Regarding the performances of Protocol 3 which is designed for the scenario with distance-dependent path loss, we notice that although it has a relatively good load balance, its eavesdropper-tolerance capability is far from acceptable, which limits its application.

7. Conclusion

To achieve reliable and secure information transmission in a two-hop relay wireless network in presence of eavesdroppers with unknown channels and locations, several transmission protocols based on relay cooperation have been considered. In particular, theoretical analysis has been conducted to understand that under each of these protocols how many eavesdroppers one network can tolerate to meet a specified requirement on the maximum allowed secrecy outage probability and transmission outage probability. Our results in this paper indicate that these protocols actually have different performance in terms of eavesdropper-tolerance capacity and load balance capacity among relays, and in general it is possible for us to select a proper transmission protocol according to network scenario such that a desired trade off between the overall eavesdropper-tolerance capacity and load balance among relay nodes can be achieved. As a possible future work, the performances study in more practical network scenarios where the source and destination are distributed within the environment instead of on the border of the network will be of great challenge. Furthermore, it is very interesting to explore the impact of the correlation of the two-hop links on the number of eavesdroppers can be tolerated which is regarded as a promising future work. Besides, conducting analysis on the performance of Protocol 1 in the scenario with distance-dependent path loss will be another interesting future direction. How to improve Protocol 3 to further enhance its eavesdropper-tolerance capability while ensuring an acceptable load balance can also be a promising future research topic.

Appendix A. Proof of Lemma 1

Proof. Notice that $P_{out}^{(T)}$ is determined as

$$P_{out}^{(T)} = P\left(O_{S \rightarrow R_j^*}^{(T)}\right) + P\left(O_{R_j^* \rightarrow D}^{(T)}\right) - P\left(O_{S \rightarrow R_j^*}^{(T)}\right) \cdot P\left(O_{R_j^* \rightarrow D}^{(T)}\right)$$

Based on the definition of transmission outage probability, we have

$$\begin{aligned} P\left(O_{S \rightarrow R_{j^*}}^{(T)}\right) &= P\left(C_{S, R_{j^*}} \leq \gamma_R\right) \\ &= P\left(\frac{E_s \cdot |h_{S, R_{j^*}}|^2}{\sum_{R_j \in \mathcal{R}_1} E_s \cdot |h_{R_j, R_{j^*}}|^2 + N_0/2} \leq \gamma_R\right) \\ &\doteq P\left(\frac{|h_{S, R_{j^*}}|^2}{\sum_{R_j \in \mathcal{R}_1} |h_{R_j, R_{j^*}}|^2} \leq \gamma_R\right) \end{aligned}$$

Compared to the noise generated by multiple system nodes, the environment noise is negligible and thus is omitted here to simplify the analysis. Notice that $\mathcal{R}_1 = \{j \neq j^* : |h_{R_j, R_{j^*}}|^2 < \tau\}$, then

$$\begin{aligned} P\left(O_{S \rightarrow R_{j^*}}^{(T)}\right) &\leq P\left(\frac{|h_{S, R_{j^*}}|^2}{|\mathcal{R}_1| \tau} \leq \gamma_R\right) \\ &= P\left(|h_{S, R_{j^*}}|^2 \leq \gamma_R |\mathcal{R}_1| \tau\right) \\ &\leq P\left(H^l \leq \gamma_R |\mathcal{R}_1| \tau\right) \end{aligned}$$

where $H^l = \min\left(|h_{S, R_{j^*}}|^2, |h_{D, R_{j^*}}|^2\right)$ is the largest random variable among the n exponential random variables $\min\left(|h_{S, R_j}|^2, |h_{D, R_j}|^2\right)$, $j = 1, 2, \dots, n$. From reference [32], we can get the distribution function of the $\min\left(|h_{S, R_j}|^2, |h_{D, R_j}|^2\right)$ for each relay R_j , $j = 1, 2, \dots, n$ as following,

$$F_{\min(|h_{S, R_j}|^2, |h_{D, R_j}|^2)}(x) = \begin{cases} 1 - e^{-2x} & x > 0 \\ 0 & x \leq 0 \end{cases}$$

From reference [32], we can also get the distribution function of random variable H^l as following,

$$F_{H^l}(x) = \begin{cases} [1 - e^{-2x}]^n & x > 0 \\ 0 & x \leq 0 \end{cases}$$

Therefore, we have

$$P\left(O_{S \rightarrow R_{j^*}}^{(T)}\right) \leq [1 - e^{-2\gamma_R |\mathcal{R}_1| \tau}]^n$$

Since there are $n - 1$ other relays except R_{j^*} , the expected number of noise-generation nodes is given by $|\mathcal{R}_1| = (n - 1) \cdot P(|h_{R_j, R_{j^*}}|^2 < \tau) = (n - 1) \cdot (1 - e^{-\tau})$. Then we have

$$P\left(O_{S \rightarrow R_{j^*}}^{(T)}\right) \leq [1 - e^{-2\gamma_R (n-1)(1-e^{-\tau})\tau}]^n$$

Employing the same method, we can get

$$P\left(O_{R_{j^*} \rightarrow D}^{(T)}\right) \leq [1 - e^{-2\gamma_R (n-1)(1-e^{-\tau})\tau}]^n$$

Thus, we have

$$P_{out}^{(T)} \leq 2 [1 - e^{-2\gamma_R (n-1)(1-e^{-\tau})\tau}]^n - [1 - e^{-2\gamma_R (n-1)(1-e^{-\tau})\tau}]^{2n}$$

Similarly, notice that $P_{out}^{(S)}$ is given by

$$P_{out}^{(S)} = P\left(O_{S \rightarrow R_{j^*}}^{(S)}\right) + P\left(O_{R_{j^*} \rightarrow D}^{(S)}\right) - P\left(O_{S \rightarrow R_{j^*}}^{(S)}\right) \cdot P\left(O_{R_{j^*} \rightarrow D}^{(S)}\right)$$

According to the definition of secrecy outage probability, we know that

$$P\left(O_{S \rightarrow R_{j^*}}^{(S)}\right) = P\left(\bigcup_{i=1}^m \{C_{S, E_i} \geq \gamma_E\}\right)$$

Thus, we have

$$P\left(O_{S \rightarrow R_{j^*}}^{(S)}\right) \leq \sum_{i=1}^m P\left(C_{S, E_i} \geq \gamma_E\right)$$

Based on the Markov inequality,

$$\begin{aligned} P\left(C_{S, E_i} \geq \gamma_E\right) &\leq P\left(\frac{E_s \cdot |h_{S, E_i}|^2}{\sum_{R_j \in \mathcal{R}_1} E_s \cdot |h_{R_j, E_i}|^2} \geq \gamma_E\right) \\ &= E_{\{h_{R_j, E_i}, j=0, 1, \dots, n+mp, j \neq j^*\}, \mathcal{R}_1} \left[P\left(|h_{S, E_i}|^2 > \gamma_E \cdot \sum_{R_j \in \mathcal{R}_1} |h_{R_j, E_i}|^2\right) \right] \\ &\leq E_{\mathcal{R}_1} \left[\prod_{R_j \in \mathcal{R}_1} E_{h_{R_j, E_i}} \left[e^{-\gamma_E |h_{R_j, E_i}|^2} \right] \right] \\ &= E_{\mathcal{R}_1} \left[\left(\frac{1}{1 + \gamma_E} \right)^{|\mathcal{R}_1|} \right] \end{aligned}$$

Therefore,

$$P\left(O_{S \rightarrow R_{j^*}}^{(S)}\right) \leq \sum_{i=1}^m \left(\frac{1}{1 + \gamma_E} \right)^{|\mathcal{R}_1|} = m \cdot \left(\frac{1}{1 + \gamma_E} \right)^{|\mathcal{R}_1|}$$

Employing the same method, we can get

$$P\left(O_{R_{j^*} \rightarrow D}^{(S)}\right) \leq m \cdot \left(\frac{1}{1 + \gamma_E} \right)^{|\mathcal{R}_2|}$$

Since the expected number of noise-generation nodes is given by $|\mathcal{R}_1| = |\mathcal{R}_2| = (n - 1) \cdot (1 - e^{-\tau})$, thus, we can get

$$P_{out}^{(S)} \leq 2m \cdot \left(\frac{1}{1 + \gamma_E} \right)^{(n-1)(1-e^{-\tau})} - \left[m \cdot \left(\frac{1}{1 + \gamma_E} \right)^{(n-1)(1-e^{-\tau})} \right]^2$$

□

Appendix B. Proof of Lemma 2

Proof. The parameter τ should be set properly to satisfy both reliability and secrecy requirements.

• Reliability Guarantee

To ensure the reliability requirement $P_{out}^{(T)} \leq \varepsilon_t$, we know from the Lemma 1 that we just need

$$2 \left[1 - e^{-2\gamma_R(n-1)(1-e^{-\tau})} \right]^n - \left[1 - e^{-2\gamma_R(n-1)(1-e^{-\tau})} \right]^{2n} \leq \varepsilon_t$$

Thus,

$$\left[1 - e^{-2\gamma_R(n-1)(1-e^{-\tau})} \right]^n \leq 1 - \sqrt{1 - \varepsilon_t}$$

That is,

$$-2\gamma_R(n-1)(1-e^{-\tau}) \tau \geq \log \left[1 - \left(1 - \sqrt{1 - \varepsilon_t} \right)^{\frac{1}{n}} \right]$$

By using Taylor formula, we have

$$\tau \leq \sqrt{\frac{-\log \left[1 - \left(1 - \sqrt{1 - \varepsilon_t} \right)^{\frac{1}{n}} \right]}{2\gamma_R(n-1)}}$$

The above result indicates the maximum value the parameter τ we can take to ensure the reliability requirement.

• Secrecy Guarantee

To ensure the secrecy requirement $P_{out}^{(S)} \leq \varepsilon_s$, we know from the Lemma 1 that we just need

$$2m \cdot \left(\frac{1}{1 + \gamma_E} \right)^{(n-1)(1-e^{-\tau})} - \left[m \cdot \left(\frac{1}{1 + \gamma_E} \right)^{(n-1)(1-e^{-\tau})} \right]^2 \leq \varepsilon_s$$

Thus,

$$m \cdot \left(\frac{1}{1 + \gamma_E} \right)^{(n-1)(1-e^{-\tau})} \leq 1 - \sqrt{1 - \varepsilon_s}$$

That is,

$$\tau \geq -\log \left[1 + \frac{\log \left(\frac{1 - \sqrt{1 - \varepsilon_s}}{m} \right)}{(n-1) \log(1 + \gamma_E)} \right]$$

The above result implies the minimum value parameter τ we can take to guarantee the secrecy requirement.

□

Appendix C. Proof of Theorem 1

Proof. From Lemma 2, we know that to ensure the reliability requirement, we have

$$\tau \leq \sqrt{\frac{-\log \left[1 - \left(1 - \sqrt{1 - \varepsilon_t} \right)^{\frac{1}{n}} \right]}{2\gamma_R(n-1)}}$$

and

$$(n-1)(1-e^{-\tau}) \leq \frac{-\log \left[1 - \left(1 - \sqrt{1 - \varepsilon_t} \right)^{\frac{1}{n}} \right]}{2\gamma_R \tau}$$

To ensure the secrecy requirement, we need

$$\left(\frac{1}{1 + \gamma_E} \right)^{(n-1)(1-e^{-\tau})} \leq \frac{1 - \sqrt{1 - \varepsilon_s}}{m}$$

Thus,

$$m \leq \frac{1 - \sqrt{1 - \varepsilon_s}}{\left(\frac{1}{1 + \gamma_E} \right)^{(n-1)(1-e^{-\tau})}} \leq \frac{1 - \sqrt{1 - \varepsilon_s}}{\left(\frac{1}{1 + \gamma_E} \right)^{\frac{-\log \left[1 - \left(1 - \sqrt{1 - \varepsilon_t} \right)^{\frac{1}{n}} \right]}{2\gamma_R \tau}}}$$

By letting τ to take its maximum value for maximum interference at eavesdroppers, we get the following bound

$$m \leq \left(1 - \sqrt{1 - \varepsilon_s} \right) \cdot (1 + \gamma_E) \sqrt{\frac{-\log \left[1 - \left(1 - \sqrt{1 - \varepsilon_t} \right)^{\frac{1}{n}} \right]}{2\gamma_R}}$$

□

Appendix D. Proof of Lemma 3

Proof. Similar to the proof of Lemma 1, we notice that $P_{out}^{(T)}$ is determined as

$$P_{out}^{(T)} = P \left(O_{S \rightarrow R_{j^*}}^{(T)} \right) + P \left(O_{R_{j^*} \rightarrow D}^{(T)} \right) - P \left(O_{S \rightarrow R_{j^*}}^{(T)} \right) \cdot P \left(O_{R_{j^*} \rightarrow D}^{(T)} \right)$$

Based on the definition of transmission outage probability, we have

$$\begin{aligned} P \left(O_{S \rightarrow R_{j^*}}^{(T)} \right) &= P \left(C_{S, R_{j^*}} \leq \gamma_R \right) \\ &\leq P \left(\frac{|h_{S, R_{j^*}}|^2}{|\mathcal{R}_1| \tau} \leq \gamma_R \right) \\ &= P \left(|h_{S, R_{j^*}}|^2 \leq \gamma_R |\mathcal{R}_1| \tau \right) \\ &= 1 - e^{-\gamma_R |\mathcal{R}_1| \tau} \end{aligned}$$

Here $\mathcal{R}_1 = \{j \neq j^* : |h_{R_j, R_{j^*}}|^2 < \tau\}$. Since the expected number of noise-generation nodes is given by $|\mathcal{R}_1| = (n-1) \cdot (1 - e^{-\tau})$. Then we have

$$P\left(O_{S \rightarrow R_{j^*}}^{(T)}\right) \leq 1 - e^{-\gamma_R(n-1)(1-e^{-\tau})\tau}$$

Employing the same method, we can get

$$P\left(O_{R_{j^*} \rightarrow D}^{(T)}\right) \leq 1 - e^{-\gamma_R(n-1)(1-e^{-\tau})\tau}$$

Thus, we have

$$P_{out}^{(T)} \leq 2\left[1 - e^{-\gamma_R(n-1)(1-e^{-\tau})\tau}\right] - \left[1 - e^{-\gamma_R(n-1)(1-e^{-\tau})\tau}\right]^2$$

Notice that the eavesdropper model of Protocol 1 is the same as that of Protocol 2, the method for ensuring secrecy is identical to that of in Lemma 1. Thus, we can see that the secrecy outage probability of Protocol 1 and Protocol 2 is the same, that is,

$$P_{out}^{(S)} \leq 2m \cdot \left(\frac{1}{1 + \gamma_E}\right)^{(n-1)(1-e^{-\tau})} - \left[m \cdot \left(\frac{1}{1 + \gamma_E}\right)^{(n-1)(1-e^{-\tau})}\right]^2$$

□

Appendix E. Proof of Lemma 4

Proof. The parameter τ should be set properly to satisfy both reliability and secrecy requirements.

• Reliability Guarantee

To ensure the reliability requirement $P_{out}^{(T)} \leq \varepsilon_t$, we know from Lemma 4 that we just need

$$2\left[1 - e^{-\gamma_R(n-1)(1-e^{-\tau})\tau}\right] - \left[1 - e^{-\gamma_R(n-1)(1-e^{-\tau})\tau}\right]^2 \leq \varepsilon_t$$

That is,

$$1 - e^{-\gamma_R(n-1)(1-e^{-\tau})\tau} \leq 1 - \sqrt{1 - \varepsilon_t}$$

By using Taylor formula, we have

$$\tau \leq \sqrt{\frac{-\log(1 - \varepsilon_t)}{2\gamma_R(n-1)}}$$

• Secrecy Guarantee

Notice that the secrecy outage probability of Protocol 1 and Protocol 2 is same. Thus, to ensure the secrecy requirement, we need

$$\left(\frac{1}{1 + \gamma_E}\right)^{(n-1)(1-e^{-\tau})} \leq \frac{1 - \sqrt{1 - \varepsilon_s}}{m}$$

Thus,

$$\tau \geq -\log\left[1 + \frac{\log\left(\frac{1 - \sqrt{1 - \varepsilon_s}}{m}\right)}{(n-1)\log(1 + \gamma_E)}\right]$$

The above result implies the minimum value parameter τ can take to guarantee the secrecy requirement. □

Appendix F. Proof of Theorem 2

Proof. From Lemma 4, we know that to ensure the reliability requirement, we have

$$\tau \leq \sqrt{\frac{-\log(1 - \varepsilon_t)}{2\gamma_R(n-1)}}$$

and

$$(n-1)(1 - e^{-\tau}) \leq \frac{-\log(1 - \varepsilon_t)}{2\gamma_R\tau}$$

To ensure the secrecy requirement, we need

$$\left(\frac{1}{1 + \gamma_E}\right)^{(n-1)(1-e^{-\tau})} \leq \frac{1 - \sqrt{1 - \varepsilon_s}}{m}$$

Thus,

$$m \leq \frac{1 - \sqrt{1 - \varepsilon_s}}{\left(\frac{1}{1 + \gamma_E}\right)^{(n-1)(1-e^{-\tau})}} \leq \frac{1 - \sqrt{1 - \varepsilon_s}}{\left(\frac{1}{1 + \gamma_E}\right)^{\frac{-\log(1 - \varepsilon_t)}{2\gamma_R\tau}}}$$

By letting τ to take its maximum value for maximum interference at eavesdroppers, we get the following bound

$$m \leq (1 - \sqrt{1 - \varepsilon_s}) \cdot (1 + \gamma_E)^{\sqrt{\frac{-(n-1)\log(1 - \varepsilon_t)}{2\gamma_R}}}$$

□

Appendix G. Proof of Lemma 5

Proof. Notice that two ways leading to transmission outage are: 1) there are no candidate relays in the relay selection region; 2) the SINR at the selected relay or the destination is less than γ_R . Let A_1 be the event that there is at least one relay in the relay selection region, and A_2 be the event that there are no relays in the relay selection region. We have

$$P_{out}^{(T)} = P_{out|A_1}^{(T)} P(A_1) + P_{out|A_2}^{(T)} P(A_2)$$

Since the relay is uniformly distributed, the number of candidate relays is a binomial distribution $\binom{n}{n, (1-2a)(1-2b)}$. We have

$$P(A_1) = 1 - \vartheta$$

and

$$P(A_2) = \vartheta$$

where $\vartheta = \left[1 - (1-2a)(1-2b)\right]^n$. When event A_2 happens, no relay is available. Then

$$P_{out|A_2}^{(T)} = 1$$

Thus, we have

$$P_{out}^{(T)} = P_{out|A_1}^{(T)} (1 - \vartheta) + 1 \cdot \vartheta$$

Notice that $P_{out|A_1}^{(T)}$ is determined as

$$\begin{aligned} P_{out|A_1}^{(T)} &= P\left(O_{S \rightarrow R_{j^*}}^{(T)} \middle| A_1\right) + P\left(O_{R_{j^*} \rightarrow D}^{(T)} \middle| A_1\right) \\ &\quad - P\left(O_{S \rightarrow R_{j^*}}^{(T)} \middle| A_1\right) \cdot P\left(O_{R_{j^*} \rightarrow D}^{(T)} \middle| A_1\right) \end{aligned}$$

Based on the definition of transmission outage probability, we have

$$\begin{aligned} P\left(O_{S \rightarrow R_{j^*}}^{(T)} \middle| A_1\right) &= P\left(C_{S, R_{j^*}} \leq \gamma_R \middle| A_1\right) \\ &= P\left(\frac{E_s \cdot \frac{|h_{S, R_{j^*}}|^2}{d_{S, R_{j^*}}^\alpha}}{\sum_{R_j \in \mathcal{R}_1} E_s \cdot \frac{|h_{R_j, R_{j^*}}|^2}{d_{R_j, R_{j^*}}^\alpha} + \frac{N_0}{2}} \leq \gamma_R \middle| A_1\right) \\ &\doteq P\left(\frac{\frac{|h_{S, R_{j^*}}|^2}{d_{S, R_{j^*}}^\alpha}}{\sum_{R_j \in \mathcal{R}_1} \frac{|h_{R_j, R_{j^*}}|^2}{d_{R_j, R_{j^*}}^\alpha}} \leq \gamma_R \middle| A_1\right) \end{aligned}$$

Compared to the noise generated by multiple system nodes, the environment noise is negligible and thus is omitted here to simplify the analysis. Notice that $\mathcal{R}_1 = \{j \neq j^* : |h_{R_j, R_{j^*}}|^2 < \tau\}$, then

$$P\left(O_{S \rightarrow R_{j^*}}^{(T)} \middle| A_1\right) \leq P\left(\frac{|h_{S, R_{j^*}}|^2 d_{S, R_{j^*}}^{-\alpha}}{\sum_{R_j \in \mathcal{R}_1} \tau d_{R_j, R_{j^*}}^{-\alpha}} \leq \gamma_R \middle| A_1\right)$$

As shown in Fig.2 that by assuming the coordinate of R_j as (x, y) , we can see that the number of noise generating nodes in square $[x, x + dx] \times [y, y + dy]$ will be $(n-1)(1-e^{-\tau}) dx dy$. Then, we have

$$\sum_{R_j \in \mathcal{R}_1} \frac{\tau}{d_{R_j, R_{j^*}}^\alpha} = \int_0^1 \int_0^1 \frac{\tau (n-1) (1-e^{-\tau})}{\left[(x-x_{R_{j^*}})^2 + (y-y_{R_{j^*}})^2\right]^{\frac{\alpha}{2}}} dx dy$$

where $(x_{R_{j^*}}, y_{R_{j^*}})$ is the coordinate of the selected relay R_{j^*} , $x_{R_{j^*}} \in [a, 1-a]$, $y_{R_{j^*}} \in [b, 1-b]$ and $a \in [0, 0.5]$, $b \in [0, 0.5]$.

Notice that within the network area, where relays are uniformly distributed, the worst case location for the selected relay R_{j^*} is the point $(0.5, 0.5)$, at which the interference from the noise generating nodes is the largest; whereas, the best case location for the selected relay R_{j^*} is the four corner points (a, b) , $(a, 1-b)$, $(1-a, b)$ and $(1-a, 1-b)$ of the relay selection, where the interference from the noise generating nodes is the smallest. By considering the worst case location for the selected relay R_{j^*} , we have

$$P\left(O_{S \rightarrow R_{j^*}}^{(T)} \middle| A_1\right) \leq P\left(\frac{|h_{S, R_{j^*}}|^2 d_{S, R_{j^*}}^{-\alpha}}{\tau (n-1) (1-e^{-\tau}) \varphi_1} \leq \gamma_R \middle| A_1\right)$$

Here

$$\varphi_1 = \int_0^1 \int_0^1 \frac{1}{\left[(x-0.5)^2 + (y-0.5)^2\right]^{\frac{\alpha}{2}}} dx dy$$

Due to $a \leq d_{S, R_{j^*}} \leq \sqrt{(1-a)^2 + (0.5-b)^2}$, we consider the worst case and let $\phi = \sqrt{(1-a)^2 + (0.5-b)^2}$, then

$$\begin{aligned} P\left(O_{S \rightarrow R_{j^*}}^{(T)} \middle| A_1\right) &\leq P\left(\frac{|h_{S, R_{j^*}}|^2 \phi^{-\alpha}}{\tau (n-1) (1-e^{-\tau}) \varphi_1} \leq \gamma_R \middle| A_1\right) \\ &= P\left(|h_{S, R_{j^*}}|^2 \leq \frac{\gamma_R \tau (n-1) (1-e^{-\tau}) \varphi_1}{\phi^{-\alpha}} \middle| A_1\right) \\ &= 1 - e^{-\frac{\gamma_R \tau (n-1) (1-e^{-\tau}) \varphi_1}{\phi^{-\alpha}}} \end{aligned}$$

Employing the same method, we can get

$$P\left(O_{R_{j^*} \rightarrow D}^{(T)} \middle| A_1\right) \leq 1 - e^{-\frac{\gamma_R \tau (n-1)(1-e^{-\tau}) \varphi_2}{\phi^{-\alpha}}}$$

here,

$$\varphi_2 = \int_0^1 \int_0^1 \frac{1}{\left[(x-1)^2 + (y-0.5)^2\right]^{\frac{\alpha}{2}}} dx dy$$

Then, we have

$$P_{out|A_1}^{(T)} \leq 1 - e^{-\frac{\gamma_R \tau (n-1)(1-e^{-\tau})}{\phi^{-\alpha}} (\varphi_1 + \varphi_2)}$$

Thus, we have

$$P_{out}^{(T)} \leq \left[1 - e^{-\frac{\gamma_R \tau (n-1)(1-e^{-\tau})}{\phi^{-\alpha}} (\varphi_1 + \varphi_2)}\right] (1 - \vartheta) + 1 \cdot \vartheta$$

Notice that $P_{out}^{(S)}$ is given by

$$P_{out}^{(S)} = P\left(O_{S \rightarrow R_{j^*}}^{(S)}\right) + P\left(O_{R_{j^*} \rightarrow D}^{(S)}\right) - P\left(O_{S \rightarrow R_{j^*}}^{(S)}\right) \cdot P\left(O_{R_{j^*} \rightarrow D}^{(S)}\right)$$

According to the definition of secrecy outage probability, we know that

$$P\left(O_{S \rightarrow R_{j^*}}^{(S)}\right) = P\left(\bigcup_{i=1}^m \{C_{S,E_i} \geq \gamma_E\}\right)$$

Thus, we have

$$P\left(O_{S \rightarrow R_{j^*}}^{(S)}\right) \leq \sum_{i=1}^m P\left(C_{S,E_i} \geq \gamma_E\right)$$

Based on the definition of r_0 , we denote by $G_1^{(i)}$ the event that the distance between E_i and the source is less than r_0 , and denote by $G_2^{(i)}$ the event that distance between E_i and the source is larger than or equal to r_0 . We have

$$\begin{aligned} & P\left(C_{S,E_i} \geq \gamma_E\right) \\ &= P\left(C_{S,E_i} \geq \gamma_E \middle| G_1^{(i)}\right) P\left(G_1^{(i)}\right) + P\left(C_{S,E_i} \geq \gamma_E \middle| G_2^{(i)}\right) P\left(G_2^{(i)}\right) \\ &\leq 1 \cdot \frac{1}{2} \pi r_0^2 + P\left(C_{S,E_i} \geq \gamma_E \middle| G_2^{(i)}\right) \left(1 - \frac{1}{2} \pi r_0^2\right) \end{aligned}$$

of which

$$\begin{aligned} & P\left(C_{S,E_i} \geq \gamma_E \middle| G_2^{(i)}\right) \leq \\ & P\left(\frac{|h_{S,E_i}|^2 r_0^{-\alpha}}{\Gamma \int_0^1 \int_0^1 \frac{1}{\left[(x-x_{E_i})^2 + (y-y_{E_i})^2\right]^{\frac{\alpha}{2}}} dx dy} \geq \gamma_E \middle| G_2^{(i)}\right) \end{aligned}$$

where (x_{E_i}, y_{E_i}) is the coordinate of the eavesdropper E_i . Γ is the sum of $(n-1)(1-e^{-\tau})$ independent exponential random variables.

From Fig.2 we know that the largest interference at eavesdropper E_i happens when E_i is located at the point (0.5, 0.5), while the smallest interference at E_i happens when it is located at the four corners of the network region. By considering the smallest interference at eavesdroppers, we then have

$$\begin{aligned} P\left(C_{S,E_i} \geq \gamma_E \middle| G_2^{(i)}\right) &\leq P\left(\frac{|h_{S,E_i}|^2 r_0^{-\alpha}}{\Gamma \psi} \geq \gamma_E\right) \\ &= P\left(|h_{S,E_i}|^2 \geq \Gamma \gamma_E \cdot \psi \cdot r_0^\alpha\right) \end{aligned}$$

here

$$\psi = \int_0^1 \int_0^1 \frac{1}{(x^2 + y^2)^{\frac{\alpha}{2}}} dx dy$$

Based on the Markov inequality,

$$\begin{aligned} P\left(C_{S,E_i} \geq \gamma_E \middle| G_2^{(i)}\right) &\leq E_\Gamma \left[e^{-\Gamma \gamma_E \psi r_0^\alpha}\right] \\ &= \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \end{aligned}$$

Then, we have

$$\begin{aligned} & P\left(C_{S,E_i} \geq \gamma_E\right) \leq \\ & \frac{1}{2} \pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \frac{1}{2} \pi r_0^2\right) \end{aligned}$$

Employing the same method, we have

$$\begin{aligned} & P\left(C_{R_{j^*},E_i} \geq \gamma_E\right) \leq \\ & \pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \pi r_0^2\right) \end{aligned}$$

Notice that

$$\begin{aligned}
 & \frac{1}{2}\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \frac{1}{2}\pi r_0^2\right) \\
 &= \pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \pi r_0^2\right) \\
 & \quad - \frac{1}{2}\pi r_0^2 \left[1 - \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})}\right] \\
 &\leq \pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \pi r_0^2\right)
 \end{aligned}$$

Therefore

$$\begin{aligned}
 P(O_{S \rightarrow R_j^*}^{(S)}) &\leq P(O_{R_j^* \rightarrow D}^{(S)}) \\
 &\leq m \left[\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \pi r_0^2\right) \right]
 \end{aligned}$$

Then, we have

$$\begin{aligned}
 P_{out}^{(S)} &\leq 2m \left[\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \pi r_0^2\right) \right] \\
 & \quad - \left[m \left(\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \pi r_0^2\right) \right) \right]^2
 \end{aligned}$$

□

Appendix H. Proof of Lemma 6

Proof. The parameter τ should be set properly to satisfy both reliability and secrecy requirements.

• Reliability Guarantee

To ensure the reliability requirement $P_{out}^{(T)} \leq \varepsilon_t$, we know from Lemma 5 that we just need

$$\left[1 - e^{-\frac{\gamma_R \tau (n-1)(1-e^{-\tau})}{\phi^{-\alpha}} (\varphi_1 + \varphi_2)} \right] (1 - \vartheta) + 1 \cdot \vartheta \leq \varepsilon_t$$

that is,

$$-\frac{\gamma_R \tau (n-1)(1-e^{-\tau})}{\phi^{-\alpha}} (\varphi_1 + \varphi_2) \geq \log \left(\frac{1 - \varepsilon_t}{1 - \vartheta} \right)$$

By using Taylor formula, we have

$$\tau \leq \sqrt{\frac{-\log \left(\frac{1 - \varepsilon_t}{1 - \vartheta} \right) \phi^{-\alpha}}{\gamma_R (n-1) (\varphi_1 + \varphi_2)}}$$

• Secrecy Guarantee

To ensure the secrecy requirement $P_{out}^{(S)} \leq \varepsilon_s$, we know from Lemma 5 that we just need

$$\begin{aligned}
 & 2m \left[\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \pi r_0^2\right) \right] - \\
 & \left[m \left(\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \pi r_0^2\right) \right) \right]^2 \leq \varepsilon_s
 \end{aligned}$$

Thus,

$$\begin{aligned}
 m \cdot \left[\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \pi r_0^2\right) \right] &\leq \\
 1 - \sqrt{1 - \varepsilon_s} &
 \end{aligned}$$

That is,

$$\tau \geq -\log \left[1 + \frac{\log \left(\frac{1 - \sqrt{1 - \varepsilon_s} - \pi r_0^2}{1 - \pi r_0^2} \right)}{(n-1) \log(1 + \gamma_E \psi r_0^\alpha)} \right]$$

□

Appendix I. Proof of Theorem 3

Proof. From Lemma 6, we know that to ensure the reliability requirement, we have

$$\tau \leq \sqrt{\frac{-\log \left(\frac{1 - \varepsilon_t}{1 - \vartheta} \right) \phi^{-\alpha}}{\gamma_R (n-1) (\varphi_1 + \varphi_2)}}$$

and

$$(n-1)(1-e^{-\tau}) \leq \frac{-\log \left(\frac{1 - \varepsilon_t}{1 - \vartheta} \right)}{\gamma_R \tau \phi^\alpha (\varphi_1 + \varphi_2)}$$

To ensure the secrecy requirement, we need

$$\begin{aligned}
 m \cdot \left[\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \pi r_0^2\right) \right] &\leq \\
 1 - \sqrt{1 - \varepsilon_s} &
 \end{aligned}$$

Thus,

$$\begin{aligned}
 m &\leq \frac{1 - \sqrt{1 - \varepsilon_s}}{\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{(n-1)(1-e^{-\tau})} \left(1 - \pi r_0^2\right)} \\
 &\leq \frac{1 - \sqrt{1 - \varepsilon_s}}{\pi r_0^2 + \left(\frac{1}{1 + \gamma_E \psi r_0^\alpha}\right)^{\frac{-\log \left(\frac{1 - \varepsilon_t}{1 - \vartheta} \right)}{\gamma_R \tau \phi^\alpha (\varphi_1 + \varphi_2)}} \left(1 - \pi r_0^2\right)}
 \end{aligned}$$

By letting τ to take its maximum value for maximum interference at eavesdroppers, we get the following bound

$$m \leq \frac{1 - \sqrt{1 - \varepsilon_s}}{\pi r_0^2 + (1 - \pi r_0^2) \omega}$$

Here,

$$\omega = (1 + \gamma_E \psi r_0^\alpha)^{-\sqrt{\frac{-(n-1) \log\left(\frac{1-\varepsilon_t}{1-\varepsilon_s}\right)}{\gamma_R(\varphi_1 + \varphi_2) \phi^\alpha}}}$$

□

Acknowledgement. This work was Supported by The National Natural science foundation of china(61100153, 61373173, U1135002), the Fundamental Research Funds for the Central Universities(JY10000903005, JY10000903001).

References

- [1] N. Sathya, Two-hop forwarding in wireless networks, Dissertation for the degree of Doctor of philosophy, Polytechnic University, 2006.
- [2] H. Wang, Y. Zhang, J. Cao, Effective collaboration with information sharing in virtual universities, IEEE Transactions on Knowledge and Data Engineering, Vol. 21, No. 6, pp.840-853, 2009.
- [3] Xiaoxun Sun, Hua Wang, Jiuyong Li, and Yanchun Zhang, Satisfying Privacy Requirements Before Data Anonymization. Comput. J. Vol.55, No.4, pp.422-437, 2012.
- [4] Min Li, Xiaoxun Sun, Hua Wang, Yanchun Zhang, and Ji Zhang, Privacy-aware access control with trust management in web service, World Wide Web, Vol.14, No.4, pp.407-430, 2011.
- [5] J. Talbot and D. Welsh, Complexity and Cryptography : An Introduction,, Cambridge University Press, 2006.
- [6] J. Zhang and M. C. Gursoy, Collaborative relay beam forming for secrecy, in Proceeding of 2010 IEEE International Conference on Communications (ICC), pp.1-5, 2010.
- [7] I. Krikidis, J. S. Thompson and S. McLaughlin, Relay selection for secure cooperative networks with jamming, IEEE Transactions on Wireless Communications, vol. 8, no.10, pp.5003-5011, 2009.
- [8] J. Li, A. Petropulu and S. Weber, On Cooperative Relaying Schemes for Wireless Physical Layer Security, IEEE Transactions on Signal Processing, vol. 59, no. 10, pp. 4985-4997, 2011.
- [9] L. Dong, H. Yousefzadeh and H. Jafarkhani, Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper IEEE International Conference on Communications (ICC 2011), pp.1-5, 2011.
- [10] J. Huang and A.L. Swindlehurst, Secure Communications via Cooperative Jamming in Two-hop Relay Systems, In 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010), pp.1-5, 2010.
- [11] L. Dong, Z. Han, A.P. Petropulu, and H.V. Poor, Secure wireless communications via cooperation, in Proc. 46th Annual Allerton Conference on Communication, Control, and Computing, pp. 1132-1138, 2008.
- [12] L. Dong, Z. Han, A.P. Petropulu, and H.V. Poor, Improving wireless physical layer security via cooperating relays, IEEE Transactions on Signal Processing, vol. 58, no. 3, pp.1875-1888, 2010.
- [13] S. Luo, J. Li, and A. Petropulu, Physical Layer Security with Uncoordinated Helpers Implementing Cooperative Jamming, in Proceeding of the seventh IEEE Sensor Array and Multichannel Signal Processing Workshop, pp.97-100, 2012.
- [14] G. Zheng, L.C. Choo, and K. K. Wong, Optimal cooperative jamming to enhance physical layer security using relays, IEEE Transactions on Signal Processing, vol. 59, no. 3, pp. 1317-1322, 2011.
- [15] K. Morrison, and D. Goeckel, Power allocation to noise-generating nodes for cooperative secrecy in the wireless environment, In the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), pp.275-279, 2011.
- [16] S. Goel, and R. Negi, Guaranteeing secrecy using artificial noise, IEEE transactions on wireless communications, vol.7, no.6, pp.2180-2189, 2008.
- [17] L. Lai and H.E. Gamal, The relay-eavesdropper channel: Cooperation for secrecy, IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005 - 4019, 2008.
- [18] R. Negi and S. Goelm, Secret communication using artificial noise, In 62nd IEEE conference on Vehicular Technology Conference (VTC 2005), pp.1906-1910, 2005.
- [19] R. Zhang, L. Song, Z. Han and B. Jiao. Physical Layer Security for Two-Way Untrusted Relaying With Friendly Jammers, IEEE Transactions on vehicular technology, vol. 61, no. 8, pp. 3693-3704, 2012.
- [20] X. He and A. Yener, Two-hop secure communication using an untrusted relay: A case for cooperative jamming. in Proceeding of 2008 IEEE Global Telecommunications Conference, pp.1-5, 2008.
- [21] Q. Guan, F. R. Yu, S. Jiang, and C. M. Leung. Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications, IEEE Transactions on vehicular technology, vol.61, no.6, pp.2674-2685, 2012
- [22] Z. Ding, M. Xu, J. Lu, and F. Liu, Improving Wireless Security for Bidirectional Communication Scenarios, IEEE Transactions on vehicular technology, vol.61, no.6, pp.2842-2848, 2012.
- [23] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding and K. Leung, Everlasting Secrecy in Two-Hop Wireless Networks Using Artificial Noise Generation from Relays, In proceeding of International Technology Alliance Collaboration System (ACITA 2011), 2011.
- [24] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding and K. Leung, Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks, IEEE Journal on Selected Areas in Communications, vol.29, no.10 pp.2067-2076, 2011.
- [25] S. Vasudevan, S. Adams, D. Goeckel, Z. Ding, D. Towsley and K. Leung, Multi-User Diversity for Secrecy in Wireless Networks, In proceeding of Information Theory

- and Applications Workshop (ITA 2010), pp.1-9, 2010.
- [26] C. Capar, D. Goeckel, B. Liu and D. Towsley, Secret Communication in Large Wireless Networks without Eavesdropper Location Information, In Proceeding of IEEE INFOCOM 2012, pp.1152-1160, 2012.
- [27] Z. Ding, K. Leung, D. Goeckel and D. Towsley, Opportunistic Relaying for Secrecy Communications: Cooperative Jamming vs Relay Chatting, IEEE Transactions on Wireless Communications, vol.10, no.6, pp.1725-1729, 2011.
- [28] M. Dehghan, D. Goeckel, M. Ghaderi and Z. Ding, Energy Efficiency of Cooperative Jamming Strategies in Secure Wireless Networks, IEEE Transactions on Wireless Communications, vol.11, no.9, pp.3025-3029, 2012.
- [29] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik and D. Towsley, Physical Layer Security from Inter-Session Interference in Large Wireless Networks, In Proceeding of IEEE INFOCOM 2012, pp.1179-1187, 2012.
- [30] C. Leow, C. Capar, D. Goeckel, and K. Leung, A Two-Way Secrecy Scheme for the Scalar Broadcast Channel with Internal Eavesdroppers, In the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR 2011), pp.1840-1844, 2011.
- [31] C. Capar and D. Goeckel, Network Coding for Facilitating Secrecy in Large Wireless Networks, In 46th Annual Conference on Information Sciences and Systems (CISS 2012), pp.1-6, 2012.
- [32] H. David, Order Statistics, Wiley, New York, 1980.