Secure and Reliable Transmission with Cooperative Relays in Two-Hop Wireless Networks

Yulong Shen, Xiaohong Jiang, Jianfeng Ma and Weisong Shi

Abstract This work considers the secure and reliable information transmission in two-hop relay wireless networks without the information of both eavesdropper channels and locations. This papers focuses on a more practical network with finite number of system nodes and explores the corresponding exact results on the number of eavesdroppers the network can tolerant to ensure a desired secrecy and reliability. For achieving secure and reliable information transmission in a finite network, two transmission protocols are considered in this paper, 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 is further provided to determine the exact and maximum number of independent and also uniformly distributed eavesdroppers one network can tolerate to satisfy a specified secrecy and reliability requirements.

Keywords Two-hop wireless networks · Physical layer secrecy · Relay cooperation · Transmission outage · Secrecy outage

Y. Shen (✉) · J. Ma
School of Computer Science and Technology, Xidian University, Xi'an 710071, China
e-mail: ylshen@mail.xidian.edu.cn

X. Jiang
School of Systems Information Science, Future University, Hakodate 418655, Japan

W. Shi
Department of Computer Science, Wayne State University, Detroit 48202 MI, USA

J. J. (Jong Hyuk) Park et al. (eds.), *Information Technology Convergence*,
Lecture Notes in Electrical Engineering 253, DOI: 10.1007/978-94-007-6996-0_41,

1 Introduction

Two-hop ad hoc wireless networks, where each packet travels at most two hops (source-relay-destination) to reach its destination, has 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, emergency 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. This paper focuses on the issue of secure and reliable information transmission in the basic two-hop ad hoc wireless networks.

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. While the cryptography is acceptable for general applications with standard security requirement, it may not be sufficient for applications with a requirement of strong form of security (like military networks and emergency networks). That is because the cryptographic approach can hardly achieve everlasting secrecy, since the adversary can record the transmitted messages and try any way to break them [2]. 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 guarantee secure and reliable information transmission in the two-hop wireless networks.

By now, a lot of research efforts have been dedicated to providing security through physical layer methods. A power control scheme is proposed in [3] to ensure that an eavesdropper can never reach its desired signal-to-noise-plus-interference ratio (*SINR*). However, such scheme is not effective when the eavesdropper has a better channel than the receiver. The technique of artificial noise generation has also been widely explored to jam the eavesdroppers and provide secure transmission in the relay communications [4–7]. Recently, the cooperative jamming through node cooperation has been demonstrated to be efficient in ensuring physical layer security [8–10]. It is notable that these schemes generally reply on the knowledge of eavesdropper channels and locations to jam eavesdroppers. In practice, however, it is difficult to gain such information, specifically in untrusted network environment. To address this constraint, a cooperative protocol based on artificial noise generation and multi-user diversity has been proposed recently in [11] to achieve secure transmission in two-hop wireless networks without the knowledge of eavesdropper channels and locations. In particular, the asymptotic behavior of such cooperative protocol in a network has been reported there to illustrate how the number of eavesdroppers the network can tolerate scales as the number of system nodes there tends to infinite.

This paper focuses on applying the relay cooperation scheme 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 remainder of the paper is organized as follows. Section 2 introduces the system models and two cooperative transmission protocols considered in this paper. Section 3 provides theoretical analysis and also related discussions of the two protocols, and Sect. 4 concludes this paper.

2 System Models and Transmission Protocols

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 $R_1, R_2, \ldots, R_n$. In addition to these normal system nodes, there are also m eavesdroppers $E_1, E_2, \ldots, E_m$ 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 ith symbol transmitted by A and denote by $y_i^{(B)}$ the ith signal received by B. We assume that all nodes transmit with the same power E_s, path loss between all pairs of nodes is equal and independent, and the frequency-nonselective multi-path

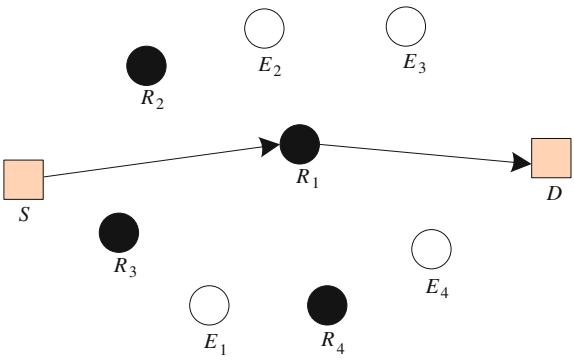

Fig. 1 System scenario

fading from A to B is a complex zero-mean Gaussian random variable. Under the condition that all nodes in a group of nodes, $\mathcal{R}$, are generating noises, the ith signal received at node B from node A is determined as:

$$y_i^{(B)} = h_{A,B}\sqrt{E_s}x_i^{(A)} + \sum_{A_j \in R} h_{A_j,B}\sqrt{E_s}x_i^{(A_i)} + n_i^{(B)} \tag{1}$$

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

$$C_{A,B} = \frac{E_s\left|h_{A,B}\right|^2}{\sum_{A_j \varepsilon \mathcal{R}} E_s\left|h_{A_j,B}\right|^2 + N_0/2} \tag{2}$$

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 for legitimate node and eavesdropper, respectively. Therefore, a system node (relay or destination) is able to decode a packet if and only if its *SINR* 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.

2.3 Transmission Protocols

We consider here two transmission protocols for secure and reliable information transmission in two-hop wireless networks. The first is optimal relay selection protocol, in which the optimal relay node with the best link condition to both source and destination is always selected for information relaying. The optimal relay selection protocol works as follows.

(1) *Channel measurement between source S and relays*: The source S broadcasts a pilot signal to allow each relay to measure the channel from S to itself. The relays, which receive the pilot signal, can accurately calculate $h_{S,R_j}, j = 1, 2, \ldots, n$.

(2) *Channel measurement between destination D and relays*: Analogous to the step 1, the destination D broadcasts a pilot signal to allow each relay to measure the channel from D to itself. The relays, which receive the pilot signal, can accurately calculate $h_{D,R_j}, j = 1, 2, \ldots, n$.

(3) *Relay section*: The relay with the largest $\min\left(\left|h_{S,R_j}\right|^2, \left|h_{D,R_j}\right|^2\right)$, $j = 1, 2, \ldots, n$ is selected as relay, indexed by j^*. Using the same method with step 1 and step 2, each of the other relays $R_j, j = 1, 2, \ldots, n, j \neq j^*$ exactly knows $h_{R_j,R_{j^*}}$.

(4) *Message transmission from source S to the selected relay* R_{j^*}: The source S transmits the messages to R_{j^*}. Concurrently, the relay nodes in cooperative relay node set $\mathcal{R}_1$, consists of cooperative nodes with the first t small $\left|h_{R_j,R_{j^*}}\right|^2, j = 1, 2, \ldots, n, j \neq j^*$, transmit noise to generate interference at eavesdroppers.

(5) *Message transmission from the selected relay* R_{j^*} *to destination D*: Similar to the Step 4, the relay R_{j^*} transmits the messages to destination D. Concurrently, the relay nodes in cooperative relay node set $\mathcal{R}_2$, consists of cooperative nodes with the first t small $\left|h_{R_j,D}\right|^2, j = 1, 2, \ldots, n, j \neq j^*$, transmit noise to generate interference at eavesdroppers.

The second is random relay selection protocol, in which the relay node is randomly selected. The random relay selection protocol works as follows.

(1) *Relay selection*: A relay node, indexed by j^*, is selected randomly from candidate relay nodes $R_j, j = 1, 2, \ldots, n$.

(2) *Channel measurement between the selected relay and the other relays*: The selected relay j^* broadcasts a pilot signal to allow each of other relays to measure the channel from j^* to itself. Each of the other relays $R_j, j = 1, 2, \ldots, n, j \neq j^*$ then knows the corresponding value of $h_{R_j,R_{j^*}}$.

(3) *Channel measurement between destination D and the other relays*: 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 $R_j, j = 1, 2, \ldots, n, j \neq j^*$ *the*n knows the corresponding value of $h_{R_j,D}$.

(4) and (5) These two steps are same with that of the optimal relay selection protocol.

3 Theoretical Analysis

This section first defines the transmission outage and secrecy outage adopted in this paper to depict transmission reliability and transmission secrecy, and then provides theoretical analysis to determine the numbers of eavesdroppers a network can tolerate based on the proposed protocol.

The parameter t involved in the proposed protocol determines whether the relay and destination can receive the messages successfully and whether sufficient noise is generated to suppress eavesdroppers. For the analysis of the proposed protocol, we first determine the range for the parameter t o ensure both secrecy requirement and reliability requirement, based on which we then analyze the number of eavesdroppers a network can be tolerate by applying the protocol. There are two constants τ_1 and τ_2, which satisfies $\left|h_{R_j,R_{j^*}}\right|^2 \leq \tau_1, R_j \in \mathcal{R}_1$ and $\left|h_{R_j,D}\right|^2 \leq \tau_2, R_j \in \mathcal{R}_2$.

3.1 Transmission Outage and Secrecy Outage

For a transmission from the source S to destination D, we call transmission outage happens if D cannot 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. For a predefined upper bound ε_t on $P_{out}^{(T)}$, 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 $\mathrm{O}_{S\to R_{j^*}}^{(T)}$ and $\mathrm{O}_{R_{j^*}\to D}^{(T)}$ 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

$$P_{out}^{(T)} = P\left(O_{S\to R_{j^*}}^{(T)}\right) + P\left(O_{R_{j^*}\to D}^{(T)}\right) - P\left(O_{S\to R_{j^*}}^{(T)}\right) \cdot P\left(O_{R_{j^*}\to D}^{(T)}\right) \tag{3}$$

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. For a predefined upper bound ε_s on $P_{out}^{(S)}$, 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 $\mathrm{O}_{S\to R_{j^*}}^{(S)}$ and $\mathrm{O}_{R_{j^*}\to D}^{(S)}$ 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

$$P_{out}^{(S)} = P\left(\mathrm{O}_{S\to R_{j^*}}^{(S)}\right) + P\left(\mathrm{O}_{R_{j^*}\to D}^{(S)}\right) - P\left(\mathrm{O}_{S\to R_{j^*}}^{(S)}\right) \cdot P\left(\mathrm{O}_{R_{j^*}\to D}^{(S)}\right) \tag{4}$$

3.2 Analysis of the Optimal Relay Selection Protocol

We first establish the following two lemmas regarding some basic properties of $P_{out}^{(T)}$, $P_{out}^{(S)}$ and t, 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 optimal relay selection protocol the transmission*

outage probability $P_{out}^{(T)}$ *and secrecy outage probability* $P_{out}^{(S)}$ *there satisfy the following conditions.*

$$P_{out}^{(T)} \leq 2\left[1 - e^{-2\gamma_R t max(\tau_1,\tau_2)}\right]^n - \left[1 - e^{-2\gamma_R t max(\tau_1,\tau_2)}\right]^{2n} \tag{5}$$

$$P_{out}^{(S)} \leq 2m \cdot \left(\frac{1}{1+\gamma_E}\right)^t - m^2 \cdot \left(\frac{1}{1+\gamma_E}\right)^{2t} \tag{6}$$

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* $P_{out}^{(S)} \leq \varepsilon_s$ *by applying the proposed protocol, the parameter t must satisfy the following condition.*

$$t \in \left[\frac{\log\left(\frac{m}{1-\sqrt{1-\varepsilon_s}}\right)}{\log(1+\gamma_E)}, \frac{\log\left[1-\left(1-\sqrt{1-\varepsilon_t}\right)^{\frac{1}{n}}\right]}{-2\gamma_R \max(\tau_1,\tau_2)}\right] \tag{7}$$

The proof of Lemma 1 and Lemma 2 can be found in [12].

Based on the results of Lemma 2, we now can establish the following theorem about the performance of the proposed protocol.

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* $P_{out}^{(S)} \leq \varepsilon_s$ *based on the optimal relay selection protocol, the number of eavesdroppers m the network can tolerate must satisfy the following condition.*

$$m \leq \left(1 - \sqrt{1-\varepsilon_s}\right) \cdot (1+\gamma_E)^{\frac{\log\left[1-\left(1-\sqrt{1-\varepsilon_t}\right)^{\frac{1}{n}}\right]}{2\gamma_R \max(\tau_1,\tau_2)}} \tag{8}$$

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

$$t \leq \frac{\log\left[1-\left(1-\sqrt{1-\varepsilon_t}\right)^{\frac{1}{n}}\right]}{-2\gamma_R \max(\tau_1,\tau_2)} \tag{9}$$

To ensure the secrecy requirement, from Lemma 2 we know

$$m \leq \left(1 - \sqrt{1-\varepsilon_s}\right) \cdot (1+\gamma_E)^t \tag{10}$$

By letting t take its maximum value. Substituting (9) into (10), we get (8).

3.3 Analysis of the Random Relay Selection Protocol

We first establish the following two lemmas regarding some basic properties of $P_{out}^{(T)}$, $P_{out}^{(S)}$ and t, which will help us to derive the main result in Theorem 1.

Lemma 3 *Consider the network scenario of Fig. 1 with equal path-loss between all pairs of nodes, under the random relay selection protocol the transmission outage probability $P_{out}^{(T)}$ and secrecy outage probability $P_{out}^{(S)}$ there satisfy the following conditions.*

$$P_{out}^{(T)} \leq 1 - e^{-\gamma_R t(\tau_1+\tau_2)} \tag{11}$$

$$P_{out}^{(S)} \leq 2m \cdot \left(\frac{1}{1+\gamma_E}\right)^t - m^2 \cdot \left(\frac{1}{1+\gamma_E}\right)^{2t} \tag{12}$$

The proof of Lemma 3 can be found in [12].

Lemma 4 *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 $P_{out}^{(S)} \leq \varepsilon_s$ by applying the random relay selection protocol, the parameter t must satisfy the following condition.*

$$t \in \left[\frac{\log\left(\frac{m}{1-\sqrt{1-\varepsilon_s}}\right)}{\log(1+\gamma_E)}, \frac{\log\left(\frac{1}{1-\varepsilon_t}\right)}{\gamma_R t(\tau_1+\tau_2)}\right] \tag{13}$$

The proof of Lemma 4 can be found in [12].

Based on the results of Lemma 4, we now can establish the following theorem about the performance of the proposed protocol.

Theorem 2 *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 $P_{out}^{(S)} \leq \varepsilon_s$ based on the proposed protocol, the number of eavesdroppers m the network can tolerate must satisfy the following condition.*

$$m \leq \left(1 - \sqrt{1-\varepsilon_s}\right) \cdot (1+\gamma_E)^{\frac{\log\log\left(\frac{1}{1-\varepsilon_t}\right)}{\gamma_R t(\tau_1+\tau_2)}} \tag{14}$$

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

$$t \leq \frac{\log\left(\frac{1}{1-\varepsilon_t}\right)}{\gamma_R t(\tau_1+\tau_2)} \tag{15}$$

To ensure the secrecy requirement, from Lemma 3 we know

$$m \leq \left(1 - \sqrt{1 - \varepsilon_s}\right) \cdot (1 + \gamma_E)^t \tag{16}$$

By letting t take its maximum value, Substituting (15) into (16), we get (14)

4 Conclusion

This paper explores reliable and secure information transmission through multiple cooperative systems nodes in two-hop relay wireless network with passive eavesdroppers of unknown channels and locations, for which two transmission protocols are considered. For each protocol, theoretical analysis has been provided to show the number of eavesdroppers the network can tolerate subject to constraints on transmission outage probability and secrecy outage probability. These two protocols, each has different performance in terms of eavesdropper tolerance, load and energy consumption distribution among nodes, and also relay selection complexity, are suitable for different network scenarios depending on network scale and also energy consumption constraint there.

References

1. Narayanan S (2006) Two-hop forwarding in wireless networks. Dissertation for the degree of Doctor of philosophy, Polytechnic University
2. Talbot J, Welsh D (2006) Complexity and crytography: an introduction. Cambridge University Press, Cambridge
3. Morrison K, Goeckel D (2011) Power allocation to noise-generating nodes for cooperative secrecy in the wireless environment. In: 45th Asilomar conference on signals, systems and computers (ASILOMAR), pp 275–279
4. Goel S, Negi R (2008) Guaranteeing secrecy using artificial noise. IEEE Trans Wireless Commun 7(6):2180–2189
5. Lai L, El Gamal H (2008) The relay-eavesdropper channel: cooperation for secrecy. IEEE Trans Inform Theory 54(9):4005–4019
6. Yuksel M, Erkip E (2007) Secure communication with a relay helping the wiretapper. In: Proceedings of 2007 IEEE information theory workshop, Lake Tahoe, CA
7. Negi R, Goelm S (2005) Secret communication using artificial noise. In: Proceedings of the IEEE Vehicular Tech. Conf, vol 3, Dallas TX, pp 1906–1910
8. Vasudevan S, Adams S, Geockel D, Ding Z, Towsley D, Leung K (2009) Multi-user diversity for secrecy in wireless networks. In: Information theorem and applications workshop
9. He X, Yener A (2008) Two-hop secure communication using an untrusted relay: a case for cooperative jamming. In: Proceedings of 2008 IEEE global telecommunications conference, New Orleans, LA
10. Dong L, Han Z, Petropulu A, Poor HV (2010) Improving wireless physical layer security via cooperating relays. IEEE Trans Signal Proc 58(3):1875–1888

11. Goeckel, Vasudevan S, Towsley D, Adams S, Ding Z, Leung K (2011) Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks. IEEE J Sel Areas Commun 29(10):2067–2076
12. Shen Y, Jiang X, Ma J (2013) Generalized secure transmission protocol for flexible load-balance control with cooperative relays in two-hop wireless networks. CoRR abs/1301.1746