Flexible Relay Selection for Secure Communication in Two-hop Wireless Networks

Yulong Shen*§, Xiaohong Jiang† and Jianfeng Ma*
*School of Computer Science and Technology, Xidian University, China
†School of Systems Information Science, Future University Hakodate, Japan
§Email:ylshen@mail.xidian.edu.cn

***Abstract*—This work considers two-hop wireless networks in the presence of eavesdroppers with unknown channels and locations, and proposes a new transmission protocol with flexible relay selection to achieve secure and reliable communication in such networks. For a two-hop network with n system nodes, the new protocol first identifies the k ($1 \leq k \leq n$) relay candidate nodes with the best links to both source and destination and then randomly selects one among them for message relay, such that a flexible tradeoff between eavesdropper tolerance capability and load-balance capability can be controlled by a proper setting of parameter k. Theoretical analysis is further provided to help us understand the eavesdropper tolerance capability of the new protocol. While previous works mainly focus on exploring the asymptotic behavior and scaling law results for infinitely large networks, this paper considers a more practical network with finite number of system nodes, and provides a theoretical analysis to determine the exact results on the number of eavesdroppers one network can tolerate when the new protocol is adopted to ensure a desired performance in terms of the maximum allowed secrecy outage probability and transmission outage probability.**

I. Introduction

The flexible and self-configuring wireless ad hoc networks hold great promises for a lot critical applications, like the battlefield networks, emergency networks, disaster recovery networks, etc., while the consideration of secrecy (and also reliability) in such networks is of great importance for ensuring the high confidentiality requirements of these applications. Two-hop 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]. Since the two-hop wireless network serve as the basic building blocks for general multi-hop network system, the study of secure information transmission in such networks lays the foundation for secure information exchange in general multi-hop network system.

The secure transmission protocols based on traditional cryptography can hardly achieve everlasting secrecy, because the adversary can record the transmitted messages and try any way to break them later [2]. The physical layer secrecy framework, 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, has been regarded as a promising approach to provide everlasting and thus a strong form of security [3][4][5]. This paper focuses on the issue of applying physical layer method to guarantee secure and reliable information transmission in the basic two-hop wireless networks in the presence of eavesdroppers of unknown channels and locations.

Based on idea of optimal relay selection for information transmission and relay cooperation for artificial noise generation, some transmission protocols have been proposed recently in [6][7][8] to implement secure information transmission in a two-hop wireless network with eavesdroppers of unknown channels and locations. Although these protocols are attractive in the sense they have very good eavesdropper tolerance capability, they may suffer from severe load-balance problem. This is because that the channel state is relatively constant during a fixed time period, while these protocols always select the optimal system node with the best link condition to both source and destination as information relay, which will result in a severe load distribution problem and thus a quick node energy depletion of the selected optimal relay node. It is notable that the load-balance issue is of great importance for wireless networks [9][10], in particular for energy-constrained wireless networks (like wireless sensor networks). To address the load-balance issue, Y. Shen et al. proposed a random relay selection protocol [11][12], in which the relay node is always randomly selected from all the system nodes. Such protocol can guarantee the best load balance property and it is more suitable for large scale wireless networks with stringent energy consumption constraint, but it is not efficient enough in resisting against eavesdroppers.

To keep the advantages of available transmission protocols while avoiding their limitations, this paper explores a more flexible relay selection scheme for secure (and also reliable) information transmission such that a desired trade off between load-balance capability and eavesdropper tolerance capability can be initiated. The main contributions of this paper as are follows:

- By extending the available transmission protocols, this paper proposes a new transmission protocol for secure and reliable information transmission in two-hop relay wireless networks. For a two-hop network with n system nodes, the protocol first identifies the k ($1 \leq k \leq n$) relay candidate nodes with the best links to both source and destination and then randomly selects one among them as message relay, such that a flexible tradeoff between eavesdropper tolerance capability and load balance capability can be controlled by a proper setting of parameter k. Such protocol covers the available ones as

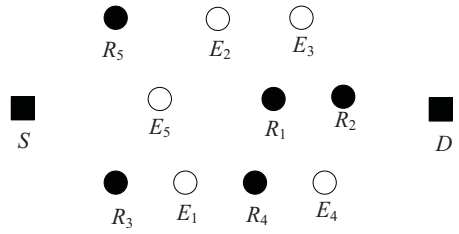

Fig. 1. System scenario: Source S wishes to communicate securely with destination D with the assistance of finite relays R_1, R_2, $\cdots$, R_n (n=5 in the figure) in the presence of passive eavesdroppers E_1, E_2, $\cdots$, E_m (m=5 in the figure). Cooperative relay scheme is used in the two-hop transmission.

special cases, like the ones with optimal relay selection ($k = 1$) [6][7][8] and the ones with random relay selection ($k = n$)[11][12].

- While the previous theoretical performance analysis for secure transmission protocols mainly focuses on exploring the asymptotic behavior and scaling law results for infinitely large networks, this paper provides theoretical analysis for a more practical and finite network to determine the exact number of eavesdroppers the network can tolerate when the new protocol is adopted to ensure a desired performance in terms of the maximum allowed secrecy outage probability and transmission outage probability.

The remainder of this paper is organized as follows. Section II first introduces the system models and then presents the new secure transmission protocol. Section III provides the theoretical performance analysis for the new protocol, and Section IV concludes this paper.

II. System Models and Transmission Protocol

A. Network Model

The two-hop wireless network scenario considered in this paper is illustrated in Fig.1, 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, $\cdots$, R_n. Also present in the environment are m eavesdroppers E_1, E_2, $\cdots$, E_m of unknown channels and locations. The relay nodes and eavesdroppers are independent and also uniformly distributed in the network.

B. Transmission Model

Consider the transmission from a transmitter A to a receiver B, and denote the i^{th} symbol transmitted by node A by $x_i^{(A)}$. We assume that all nodes transmit with the same power E_s and path-loss between all pairs of nodes is identical and independent. We denote the frequency-nonselective multi-path fading from A to B by $h_{A,B}$. 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, denoted by $y_i^{(B)}$, is determined as:

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

The multi-path fading $h_{A,B}$ is assumed to follow a Rayleigh distribution, which remains constant during the transmission of each packet. Then, $|h_{A,B}|^2$ is exponentially distributed, and without loss of generality, we assume that $E\left[|h_{A,B}|^2\right] = 1$. The noise $n_i^{(B)}$ at receiver B is assumed to be i.i.d complex Gaussian random variables with mean N_0. The SINR $C_{A,B}$ from A to B is then given by

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

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 nodes and eavesdroppers, respectively. Therefore, a system node (the selected relay or destination) is able to decode a packet if and only if its received SINR is greater than γ_R, whereas each eavesdropper try to achieve target SINR γ_E to recover the transmitted message.

C. Transmission Protocol

For secure transmission in two-hop relay networks, available protocols adopt either optimal or random relay selection, which significantly limit their flexibility in trade-off control between eavesdropper tolerance capability and load balance capability. To address such limitation, we extend available protocols and proposal a more flexible relay selection scheme, where the k ($1 \le k \le n$) relay candidate nodes with the best links to both source and destination are first identified and one among them is then randomly selected as message relay.

The proposed new protocol works as follows.

1) ***Channel measurement*:** The source S and destination D broadcast a pilot signal to allow each relay to measure the channels from S and D to itself. The relays, which receive the pilot signal, can accurately calculate h_{S,R_j} and $h_{D,R_j}, j = 1, 2, \cdots, n$.
2) ***Candidate relay selection*:** The relays with the first k largest $\min\left(|h_{S,R_j}|^2, |h_{D,R_j}|^2\right), j = 1, 2, \cdots, n$ form the candidate relay set.
3) ***Relay selection*:** The relay, indexed by j^*, is selected randomly from candidate relay set. Using the same method as Step 1, each of the other relays $R_j, j = 1, 2, \cdots, n, j \neq j^*$ in network can determine $h_{R_j,R_{j^*}}$.
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 $|h_{R_j,R_{j^*}}|^2, j = 1, 2, \cdots, n, j \neq j^*$, 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 $|h_{R_j,D}|^2, j = 1, 2, \cdots, n, j \neq j^*$, transmit noise to generate interference at eavesdroppers.

Remark 1: In the new protocol, the larger the value of k, the better the load balance among relays at the cost of a weaker eavesdropper tolerance capability, and vice versa. Thus, a tradeoff between eavesdropper resistance capability and load-balance capability among relays can be flexibly controlled by a proper setting of k. It is also notable that the new protocol covers the available ones as special cases, like the ones with optimal relay selection ($k = 1$) [6][7][8] and the ones with random relay selection ($k = n$)[11][12].

Remark 2: The parameter t involved in the proposed protocol serves as the threshold on the number of noise generating nodes. Notice that a too large t may disable legitimate transmission, while a too small t may not be sufficient for interrupting all eavesdroppers. Thus, the parameter t should be set properly to ensure both secrecy requirement and reliability requirement.

III. Theoretical Performance Analysis

The previous theoretical performance analysis on secure transmission protocols mainly focus on exploring the scaling law results as network size tends to infinite [6][7][8]. However, the actual performance in terms of the exact number of eavesdroppers one finite network can tolerate is of great interest for network designers. 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.

A. 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. We define the transmission outage probability, denoted by $P_{out}^{(T)}$, 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 $P_{out}^{(T)} \leq \varepsilon_t$.

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. We define the secrecy outage probability, denoted by $P_{out}^{(S)}$, 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 $P_{out}^{(S)} \leq \varepsilon_s$.

B. Eavesdropper Tolerance Capability Analysis

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 to 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 exist two constants τ_1 and τ_2, which satisfies $|h_{R_j,R_{j^*}}|^2 \leq \tau_1, R_j \in \mathcal{R}_1$ and $|h_{R_j,D}|^2 \leq \tau_2, R_j \in \mathcal{R}_2$.

To determine the eavesdropper tolerance capability in terms of the number of eavesdroppers one network can tolerate based on the new protocol, 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 new transmission protocol the transmission outage probability $P_{out}^{(T)}$ and secrecy outage probability $P_{out}^{(S)}$ there satisfy the following conditions:

$$P_{out}^{(T)} \leq 2\left(\frac{1}{k}\sum_{j=1}^{k}\left[\sum_{i=n-j+1}^{n}\binom{n}{i}\left[1-\Psi\right]^i\Psi^{n-i}\right]\right) - \left(\frac{1}{k}\sum_{j=1}^{k}\left[\sum_{i=n-j+1}^{n}\binom{n}{i}\left[1-\Psi\right]^i\Psi^{n-i}\right]\right)^2 \tag{1}$$

and

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

where $\Psi = e^{-2\gamma_R t\max\{\tau_1,\tau_2\}}$.

Due to space limitation here, the proof of this lemma is provided in [13].

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

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

and

$$\tau \leq \frac{-\log\left(\left[\binom{k}{\lfloor\frac{k}{2}\rfloor}\left(1+k\sqrt{1-\varepsilon_t}\right)\right]^{\frac{1}{k}}-1\right)}{2\gamma_R\max\{\tau_1,\tau_2\}}$$

$\lfloor\cdot\rfloor$ is the floor function.

Due to space limitation here, the proof of this lemma is provided in [13].

Based on the results of Lemma 2, we now can establish the following theorem regarding the eavesdropper tolerance capability of the new transmission 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 $P_{out}^{(S)} \leq \varepsilon_s$ under the new transmission

protocol, the number of eavesdroppers m the network can tolerate satisfies the following condition:

$$m \leq \left(1-\sqrt{1-\varepsilon_s}\right)\varsigma$$

here

$$\varsigma = (1+\gamma_E)^{\frac{-\log\left(\left[\binom{k}{\lfloor \frac{k}{2} \rfloor}\left(1+k\sqrt{1-\varepsilon_t}\right)\right]^{\frac{1}{k}}-1\right)}{2\gamma_R \max\{\tau_1,\tau_2\}}}$$

Proof:

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

$$t \leq \frac{-\log\left(\left[\binom{k}{\lfloor \frac{k}{2} \rfloor}\left(1+k\sqrt{1-\varepsilon_t}\right)\right]^{\frac{1}{k}}-1\right)}{2\gamma_R \max\{\tau_1,\tau_2\}} \tag{3}$$

and to ensure the secrecy requirement, we need

$$m\left(\frac{1}{1+\gamma_E}\right)^t \leq 1-\sqrt{1-\varepsilon_s} \tag{4}$$

By letting t take its maximum value, Substituting (3) into (4), we get the following bound

$$\begin{aligned} m &\leq \frac{1-\sqrt{1-\varepsilon_s}}{\left(\frac{1}{1+\gamma_E}\right)^t} \\ &\leq \frac{1-\sqrt{1-\varepsilon_s}}{\left(\frac{1}{1+\gamma_E}\right)^{\frac{-\log\left(\left[\binom{k}{\lfloor \frac{k}{2} \rfloor}\left(1+k\sqrt{1-\varepsilon_t}\right)\right]^{\frac{1}{k}}-1\right)}{2\gamma_R \max\{\tau_1,\tau_2\}}}} \end{aligned}$$

that is

$$m \leq \left(1-\sqrt{1-\varepsilon_s}\right)\varsigma$$

here

$$\varsigma = (1+\gamma_E)^{\frac{-\log\left(\left[\binom{k}{\lfloor \frac{k}{2} \rfloor}\left(1+k\sqrt{1-\varepsilon_t}\right)\right]^{\frac{1}{k}}-1\right)}{2\gamma_R \max\{\tau_1,\tau_2\}}}$$

■

Remark 3: By setting $k = n$, the result of Theorem 1 is reduced to that of the protocol with random relay selection [11][12]. The result in Theorem 1 indicates that smaller the value of parameter k (and thus a worse load-balance), the more eavesdroppers the network can tolerate, and vice versa. Thus, a flexible tradeoff between load-balance capability and eavesdropper tolerance can be controlled by a proper setting of relay candidate set size k.

IV. Conclusion

This paper extended the available secure transmission protocols for two-hop relay wireless networks and proposed a new one with more flexible relay selection, which enables a tradeoff between eavesdropper tolerance capability and load balance capability to be made for different wireless network scenarios and applications. For a practical network that has finite number of system nodes and adopts the new protocol for secure and reliable information transmission, theoretical analysis was also provided to show the relationship between the eavesdropper tolerance capability in terms of the maximum number of eavesdroppers the network can tolerate and other important network parameters, like the maximum allowed secrecy outage probability and transmission outage probability, the number of system nodes, the size of relay candidate set, and the minimum SINR required to recover the transmitted messages for legitimate nodes and eavesdroppers, respectively. We envision that the work in this paper will be helpful for the study of secure information transmission in general multi-hop wireless networks.

References

[1] N. Sathya, *"Two-hop forwarding in wireless networks,"* Dissertation for the degree of Doctor of philosophy, Polytechnic University, 2006.

[2] J. Talbot and D. Welsh, *"Complexity and Crytography : An Introduction,"*, Cambridge University Press, 2006.

[3] A. D. Wyner, *"The wire-tap channel,"* The Bell System Technical Journal, vol.54, no.8, pp.1355-1387, 1975.

[4] S. Vasudevan, D. Goeckel and D. F. Towsley, *"Security-capacity trade-off in large wireless networks using keyless secrecy,"* In the eleventh ACM international symposium on Mobile ad hoc networking and computing (MobiHoc 2010), pp.21-30, 2010.

[5] O.O. Koyluoglu, C.E. Koksal and H.E. Gamal, *"On Secrecy Capacity Scaling in Wireless Networks,"* IEEE Transactions on Information Theory, vol. 58, no. 5, pp.3000-3015, 2012.

[6] 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.

[7] 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.

[8] 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.

[9] P.H. Hsiao, A. Hwang, H.T. Kung and D. Vlah, *"Load-Balancing Routing for Wireless Access Networks,"* In Proceeding of IEEE INFOCOM 2001, pp.986-995, 2001.

[10] J. Gao and L. Zhang, *"Load Balanced Short Path Routing in Wireless Networks,"* In Proceeding of IEEE INFOCOM 2004, pp.1099-1108, 2004.

[11] Y. Shen, X. Jiang, J. Ma and W. Shi, *"Secure and Reliable Transmission with Cooperative Relays in Two-Hop Wireless Networks,"* http://arxiv.org/pdf/1211.7075v1.pdf, 2012.

[12] Y. Shen, X.Jiang and J. Ma, *"Exploring Relay Cooperation for Secure and Reliable Transmission in Two-Hop Wireless Networks,"* http://arxiv.org/pdf/1212.0287v1.pdf, 2012.

[13] Y. Shen, X.Jiang and J. Ma, *"Generalized Secure Transmission Protocol for Flexible Load-Balance Control with Cooperative Relays in Two-Hop Wireless Networks,"* http://arxiv.org/pdf/1301.1746v1.pdf, 2013.