Exploring Relay Cooperation Scheme for Load-Balance Control in Two-hop Secure Communication System

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 load-balance control among the relays under the secure transmission protocol via relay cooperation in two-hop wireless networks without the information of both eavesdropper channels and locations. The available two-hop secure transmission protocols in physical layer secrecy framework cannot provide a flexible load-balance control, which may significantly limit their application scopes. This paper proposes a secure transmission protocol in case that the path-loss is identical between all pairs of nodes, in which the relay is randomly selected from the first $k$ preferable assistant relays. This protocol enables load-balance among relays to be flexibly controlled by a proper setting of the parameter $k$, and covers the available works as special cases, like ones with the optimal relay selection ($k = 1$) and ones with the random relay selection ($k = n$, i.e. the number of system nodes). The theoretic analysis is further provided to determine the maximum number of eavesdroppers one network can tolerate by applying the proposed protocol to ensure a desired performance in terms of the secrecy outage probability and transmission outage probability.

I. INTRODUCTION

The promising applications of wireless ad hoc networks in many important scenarios (like battlefield networks, emergency networks, disaster recovery networks) make a lot of attention turn to ensure security and high efficiency of wireless transmission. Two-hop wireless networks, as a building block for large multi-hop network system, have been a class of basic and important networking scenarios [1]. The analysis and design of secure transmission protocol in basic two-hop relay networks serves as the foundation for secure information exchange of general multi-hop network system. The secure transmission protocols based on traditional cryptographic approach can hardly achieve everlasting secrecy, because the adversary can record the transmitted messages and try any way to break them [2]. This motivates the signaling scheme is considered in physical layer secrecy framework to provide a strong form of security recently [4][5].

By now, a lot of research efforts have been dedicated to secure transmission through physical layer methods. A few secure transmission protocols with optimal relay selection via cooperative relays have been proposed in [6][7][8], in which the system node with best link condition to both source and destination is selected as information relay. Although these protocols are attractive in the sense that provides very effective resistance against eavesdroppers, some relay nodes with good link conditions always preferred to relay package, since the channel state is relatively constant during a fixed time period, which results in a severe load-balance problem and a quick node energy depletion. In fact, the load-balance capacity is of important property of wireless networks [9][10]. Such, these protocol is not suitable for energy-limited wireless networks (like wireless sensor networks). In order to address load-balance problem, Y. Shen et al. further proposed a random relay selection protocol [11][12], in which the relay node is randomly selected from the system nodes. However, this protocol has lower transmission efficiency, although achieving a very good load-balance and energy consumption distribution among system nodes. Such it is more suitable for large scale wireless network environment with stringent energy consumption constraint.

In summary, the available secure transmission protocols cannot provide a flexible load-balance control, which may significantly limit their application scopes. This paper focuses on this problem and consider load-balance control capacity for secure transmission protocol via relay cooperation in two-hop wireless networks without the information of both eavesdropper channels and locations. The main contributions of this paper as follows:

- This paper extends available works and proposes a secure transmission protocol via cooperative relays in two-hop relay wireless networks without the knowledge of eavesdropper channels and locations, where the relay is randomly selected from the first $k$ preferable assistant relays. With respect to the available works, this protocol provides flexible load-balance control by a proper setting of $k$ under the premise of specified secure and reliable requirements.
- The theoretic analysis of the proposed protocol is provided to determine the corresponding exact results on the maximum number of eavesdroppers one network can tolerate to satisfy a specified requirements in case that the path-loss is identical between all pairs of nodes. The analysis results also show that the proposed protocol covers all the available secure transmission protocols as special cases, like ones with the optimal relay selection ($k = 1$) [6][7][8] and ones with the random relay selection ($k = n$).
Our goal here is to design a transmission protocol to ensure the relay nodes and eavesdroppers are independent and also among the relays.

A two-hop wireless network scenario is considered 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 $E_1$, $E_2$, $\cdots$, $E_m$ without knowledge of channels and locations. The relay nodes and eavesdroppers are independent and also uniformly distributed in the network, as illustrated in Fig.1. Our goal here is to design a transmission protocol to ensure the secure and reliable information transmission from source $S$ to destination $D$ and provide flexible load-balance control among the relays.

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, $R$, are generating noises, the $i^{th}$ signal received at node $B$ from node $A$, denoted by $y_i^{(B)}$, is determined as:

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

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 $E[|h_{A,B}|^2] = 1$.

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

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

For a legitimate node and an eavesdropper, we use two separate SINR thresholds $\gamma_R$ and $\gamma_E$ 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 $\gamma_R$, whereas each eavesdropper try to achieve target SINR $\gamma_E$ to recover the transmitted message.

C. Transmission Protocol

With respect to the protocols with optimal and random relay selection as special cases, a secure transmission protocol is proposed to enable the tradeoff between the transmission efficiency and load-balance capacity among the relays to be flexibly controlled. The proposed 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 $k$ large $\min \{ |h_{S,R_j}|^2, |h_{D,R_j}|^2 \}, j = 1, 2, \cdots, n$ form the candidate relay set.

3) Relay selection: The relay, indexed by $j^*$, is selected randomly from candidate relay set. Using the same method with Step 1, each of the other relays $R_j, j = 1, 2, \cdots, n, j \neq j^*$ in network exactly knows $h_{R_j,R_{j^*}}$.

4) Two-Hop transmission: The source $S$ transmits the messages to $R_{j^*}$, and concurrently, the relay nodes with indexes in $R_1 = \{ j \neq j^*: |h_{R_j,R_{j^*}}|^2 < \tau \}$ 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 $R_2 = \{ j \neq j^*: |h_{R_{j^*},R_j}|^2 < \tau \}$ transmit noise to generate interference at eavesdroppers.

Remark 1: The proposed protocol can flexibly control load-balance capacity among the relays in terms of networks requirements by a proper setting of candidate relay set size $k$. The larger $k$, more system nodes in candidate relay set, means the better load-balance capacity among the relays and the lower transmission efficiency, and vice versa.

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

III. Theoretical Analysis

The transmission outage and secrecy outage are first defined to depict transmission reliability and secrecy, and theoretical
analysis on the maximum numbers of eavesdroppers one network can tolerate is presented by applying the proposed protocol.

A. Transmission Outage and Secrecy Outage

For a Two-hop relay transmission from the source $S$ to destination $D$, we call transmission outage happens if $D$ can not receive the transmitted packet. We define the transmission outage probability, denoted by $P_{\text{out}}^{(T)}$, as the probability that transmission outage from $S$ to $D$ happens. For a predefined upper bound $\varepsilon_t$ on $P_{\text{out}}^{(T)}$, we call the communication between $S$ and $D$ is reliable if $P_{\text{out}}^{(T)} \leq \varepsilon_t$.

Regarding the secrecy outage, we call secrecy outage happens for a transmitted from $S$ to $D$ if at least one eavesdropper can recover the transmitted packets during the process of this two-hop transmission. We define the secrecy outage probability, denoted by $P_{\text{out}}^{(S)}$, as the probability that secrecy outage happens during the transmission from $S$ to $D$. For a predefined upper bound $\varepsilon_s$ on $P_{\text{out}}^{(S)}$, we call the communication between $S$ and $D$ is secure if $P_{\text{out}}^{(S)} \leq \varepsilon_s$.

B. Analysis of the Proposed Protocol

We now analyze that under the proposed protocol the number of eavesdroppers one network can tolerate to ensure the desired performance in terms of transmission outage probability and secrecy outage probability. The following two lemmas regarding some basic properties of $P_{\text{out}}^{(T)}$, $P_{\text{out}}^{(S)}$ and $\tau$ are first presented, 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 proposed protocol the transmission outage probability $P_{\text{out}}^{(T)}$ and secrecy outage probability $P_{\text{out}}^{(S)}$ there satisfy the following conditions.

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

\[
- \left( \frac{1}{k} \sum_{j=1}^{k} \left[ \sum_{i=n-j+1}^{n} \binom{n}{i} \left(1 - \Psi^i \Psi^{n-i}\right) \right]^2 \right)
\]

(1)

Here, $\Psi = e^{-2\gamma_R(n-1)(1-e^{-\tau})}$ and

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

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

(2)

Due to space limitation, the proof of this lemma is omitted, which can be found in the reference [13].

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

\[
\tau \leq \sqrt{-\log \left( \left( \binom{k}{j} \right) \left(1 + k \sqrt{1 - \varepsilon_t} \right) \right) \frac{\delta}{2\gamma R(n-1)}}
\]

and

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

Proof:
The parameter $\tau$ should be set properly to satisfy both reliability and secrecy requirements.

- Reliability Guarantee

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

\[
2 \left( \frac{1}{k} \sum_{j=1}^{k} \left[ \sum_{i=n-j+1}^{n} \binom{n}{i} \left(1 - \Psi^i \Psi^{n-i}\right) \right] \right)
\]

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

Thus,

\[
\frac{1}{k} \sum_{j=1}^{k} \left[ \sum_{i=n-j+1}^{n} \binom{n}{i} \left(1 - \Psi^i \Psi^{n-i}\right) \right] \leq 1 - \sqrt{1 - \varepsilon_t}
\]

(3)

Notice that

\[
\frac{1}{k} \sum_{j=1}^{k} \left[ \sum_{i=n-j+1}^{n} \binom{n}{i} \left(1 - \Psi^i \Psi^{n-i}\right) \right] = \frac{1}{k} \sum_{j=1}^{k} \left[ 1 - \sum_{i=0}^{n-j} \binom{n}{i} \left(1 - \Psi^i \Psi^{n-i}\right) \right]
\]

(4)

We also notice $i$ can take from 0 to $n - j$, then we have

\[
1 \leq \frac{\binom{n}{i}}{(n - j)! i!} \leq \frac{n!}{(n-j)! j!}
\]
Substituting into formula (4), we have

\[
\frac{1}{k} \sum_{j=1}^{k} \left[ 1 - \frac{1}{k} \sum_{i=0}^{n-j} \binom{n-j}{i} \left(1 - \Psi \right)^i \Psi^{n-j-i} \right]
\]

or equally,

\[
= 1 - \frac{1}{k} \sum_{j=0}^{k} \frac{1}{k} \binom{k}{j} \Psi^{j - 1}
\]

\[
\leq 1 - \frac{1}{k} \left( \frac{1}{\left( \frac{k}{2} \right)} \sum_{j=0}^{k} \binom{k}{j} \Psi^{j - 1} \right)
\]

\[
= 1 - \frac{1}{k} \left( \frac{1}{\left( \frac{k}{2} \right)} (1 + \Psi)^{-1} \right)
\]

(5)

According to formula (3), (4) and (5), in order to ensure the reliability, we need

\[
1 - \frac{1}{k} \left[ \frac{1}{\left( \frac{k}{2} \right)} (1 + \Psi)^{-1} \right] \leq 1 - \sqrt{1 - \varepsilon_t}
\]

or equally,

\[
\Psi \geq \left[ \left( \frac{k}{\left( \frac{k}{2} \right)} \right) (1 + k\sqrt{1 - \varepsilon_t}) \right]^+ - 1
\]

that is,

\[
e^{-2\gamma(1-n)\left(1-e^{-\tau}\right)} \geq \left[ \left( \frac{k}{\left( \frac{k}{2} \right)} \right) (1 + k\sqrt{1 - \varepsilon_t}) \right]^+ - 1
\]

Therefore

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

By using Taylor formula, we have

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

(6)

\[
\bullet \textbf{Secrecy Guarantee}
\]

To ensure the secrecy requirement \( P_{\text{out}}^{(S)} \leq \varepsilon_s \), we know from formula (2) in Lemma 1, that we just need

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

Thus,

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

That is,

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

Based on the results of Lemma 2, we now can establish the following theorem regarding the performance of the proposed protocol in case of equal path-loss between all node pairs.

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

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

\[
\cdot \text{[\cdot]} \text{ is the floor function.}
\]

\textbf{Proof:}

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

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

and

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

To ensure the secrecy requirement, we need

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

(7)
From formula (7) and (8), we can get

\[
m \leq \frac{1 - \sqrt{1 - \varepsilon_s}}{\left(\frac{1}{1 + \gamma E}\right)^{(n-1)(1-e^{-\tau})}} \leq \frac{1 - \sqrt{1 - \varepsilon_s}}{\left(\frac{1}{1 + \gamma E}\right)^{-\log\left(\left(\frac{k}{s}\right)\left(1+k\sqrt{1-\varepsilon}\right)^{\frac{s}{k}}\right)}} \tag{9}
\]

By letting \(\tau\) take its maximum value for maximum interference at eavesdroppers, from formula (6) and (9), we get the following bound

\[
m \leq \frac{1 - \sqrt{1 - \varepsilon_s}}{\left(\frac{1}{1 + \gamma E}\right)^{-\log\left(\left(\frac{k}{s}\right)\left(1+k\sqrt{1-\varepsilon}\right)^{\frac{s}{k}}\right)}}
\]

Based on the above analysis, by simple derivation, we can get the follow corollary to show our proposal is a general protocol.

**Corollary 1.** Consider the network scenario of Fig 1 with equal path-loss between all pairs of nodes, the analysis results of the proposed protocol is identical to that of protocols with the optimal relay selection presented in [6][7] by setting of \(k = 1\), and is identical to that of protocols with the random relay selection presented in [11][12] by setting of \(k = n\). More general, the proposed protocol can flexibly control load-balance capacity among the relays in terms of networks requirements by a proper setting of candidate relay set size \(k\) in case that the path-loss is equal between all pairs of nodes.

**IV. Conclusion**

This paper extended the available protocol with considering load-balance capacity and proposed a general protocol to ensure secure and reliable information transmission through multiple cooperative system nodes for two-hop relay wireless networks without the knowledge of eavesdropper channels and locations. We proved that the proposed protocol has the ability of flexible load-balance control by a proper setting of the size \(k\) of candidate relay set. Such, in general it is possible for us to set proper value of parameters according to network scenario to support various wireless applications.

**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 Cryptography: 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](http://arxiv.org/pdf/1211.7075v1.pdf) 2012.

[12] Y. Shen, X.Jiang, J. ma, "Exploring Relay Cooperation for Secure and Reliable Transmission in Two-Hop Wireless Networks," [http://arxiv.org/pdf/1212.0267v1.pdf](http://arxiv.org/pdf/1212.0267v1.pdf) 2012.

[13] Y. Shen, X.Jiang, J. ma, "Generalized Secure Transmission Protocol for Flexible Load-Balance Control with Cooperative Relays in Two-Hop Wireless Networks," [http://arxiv.org/pdf/v1.pdf](http://arxiv.org/pdf/v1.pdf) 2012.