Physical Layer Secure Information Exchange Protocol for MIMO Ad-hoc Networks Against Passive Attacks

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo
200 University Avenue West
Waterloo, ON N2L 3G1, Canada
Email: ggong@uwaterloo.ca

Abstract

In this paper, it is proposed a transmission protocol for two users in an n-hop MIMO ad-hoc network to exchange their respective information using physical layer's transmission models including one-way untrusted relay, two-way untrusted relay, and multiple access. At each time slot of the proposed n-hop information exchange protocol, a relay node, acting as a receiver, or passive eavesdroppers, only can demodulate it to a sum signal and they cannot decompose it to obtain the individual summand signal. It is shown that the total number of time slots in the proposed protocol is equal to $n+1$ which is minimized. The security of the protocol is analyzed. The secrecy capacity with no external eavesdroppers is also presented. The protocol is simulated and the simulation results demonstrate that the confidentiality of exchanged message is achieved in terms of bit-error-rate for the intended receivers and how the number of hops and the number of antennas influence the secrecy capacity.

Keywords: MIMO, ad-hoc network, physical layer security, information exchange protocol, passive attacks.

1 Introduction

The mobile ad-hoc networks (MANETs) have attracted increasing interests over the past years due to its important applications in disaster relief, temporal networking infrastructure, military usage, health care networks and so on. With the properties of self-forming, self-configuring and self-administering, the MANETs enjoys its rapid deployment in a cost efficient way. However, the absence of fixed network infrastructure and the feature of multi-hop communication make securing MANETs extremely challenging for more than a decade. The main challenges that need to be addressed when designing security solutions for MANETs are 1) the lack of infrastructure; 2) resource-constrained nodes and communication links; 3) node mobility and network dynamics; 4) likely node compromise.

At the same time, the multi-input multi-output (MIMO) has shown its significant theoretical improvement in channel capacity for wireless communication networks. Meanwhile, in 2013, the Apple company has equipped two antennas in its products: iPad Air and iPad Mini. This practice shows that the multiple antennas technique can be used in delicate mobile devices rather than giant equipments, such as base stations for cellular communications. It is foreseeable that MIMO systems will be one of the most critical techniques in future wireless systems from the point of view in theory as well as in practice.

As an integration of those two key topics in wireless communications, MIMO MANETs or MIMO ad-hoc networks, as it has been termed, has tremendously attracted increasing attentions in recent years. It has been shown that MIMO techniques can enhance MANETs' transmission efficiency. Addition to that redundancy brought by multiple antennas in physical layer becomes a useful recourse to secure MANETs without deploying cryptographic mechanisms in some situations or the cases that key distribution and management in MASETs are hardly deployed. The benefit of physical layer security approach lies exactly in its no need of key share. Thus, it is desirable to have physical layer security schemes for securing MANETs as the complement of cryptography based security solutions to MANETs, since key distribution and management in cryptography based schemes is a challenge problem for MANETs since the sight of MANETs.

The recent research on MIMO ad-hoc networks are largely laid on topics on QoS, throughput, power control and routing protocol, see [3, 7, 8, 10, 16, 17], just to list a few. On the other hand, physical layer security has been investigated for some special MIMO networks. In this direction, the authors in [11] give a joint source and relay secure beamforming design for the one-way MIMO untrusted relay model. In [18], the authors proposed a method to secure two-way relay channel (TWRC) models by transmitting jamming signals by friendly jammers. However, an direct observation is that the selection of friendly jammers will be difficult to realize in practice. The authors in [15] give an approach to achieve secrecy capacity in MIMO two-way untrusted relay channels based on the signal alignment precoding. A recent work, reported in [14], proposed a new scheme for securing MIMO two-way untrusted relay channels for multiple end-to-end user pairs with one untrusted relay.

It is evidently that MIMO cooperation with untrusted relay is largely related to MANETs with existing untrusted helper nodes, acting as relay nodes. So, the research on securing MIMO cooperation can be applied to the MIMO ad-hoc case.

In this paper, we explore physical layer transmission approaches for securing information exchange for an n-hop MIMO ad-hoc network with minimized time slots for each information exchange. We consider the problem that two users in this system would like to exchange their information securely and all the relay nodes along the path cannot get the exchanged signals. Our contributions for solving this problem are summarized as follows.

(a) We propose a novel transmission protocol for securing information exchange in an n-hop MIMO ad-hoc network using three basic transmission models, namely, one-way untrusted relay, two-way untrusted relay, and multiple access.

(b) We show that each relay node can only obtain a sum signal for which it cannot recover the individual signal. We prove that the total number of time slots used in the proposed protocol is equal to $n+1$ in the n-hop information exchange and this number is minimized at the same security level.

(c) We give the security analysis for the protocol against eavesdropping attacks from both relay nodes and external eavesdroppers, and derive the secrecy capacity. Some comparisons among the proposed protocol, crypto based approach, and naive approach. We derive the secrecy capacity of the proposed protocol for n-hop information exchange.

(d) the protocol and use simulations to demonstrate the security of the proposed protocol by a) the compar-

isons of bit-error rate between the intended receivers and relay nodes in the n-hop information exchange protocol, b) the relationship between the secrecy capacity and hop number, and c) how the number of antennas influences the secrecy capacity.

(e) To validate the performance of our protocol, we simulate the protocol and use simulations to demonstrate the security of the proposed protocol by the comparisons of bit-error rate between the intended receivers and relay nodes, the relationship between the secrecy capacity and hop number, and how the number of antennas influences the secrecy capacity.

2 System Model and Preliminaries

We consider the case that two mobile nodes in an ad-hoc network, namely user A and user B, exchange their information with the help of one or multiple relay nodes.

2.1 Some Basic Conditions and Definitions

We assume that B is in n-hop distance from A where $n > 1$. So they need $n-1$ relay nodes to help for transmission. We set $S_0 = A$, $B = S_n$ and the relay nodes between A and B denote as $S_i, i = 1, \cdots, n-1$. We write $(A, S_1, \cdots, S_{n-1}, B)$ as a path between A and B. We denote $N_A(i)$ as the i-hop neighbours of user A, so $S_i \in N_A(i)$. We assume the users are equipped with m_A and m_B antennas, and S_i is equipped with m_{S_i} antennas. So these nodes with multiple antennas form an MIMO system.

The model of n-hop information exchange system in an MIMO ad-hoc network is depicted in Figure 1. In each information exchange, which will be executed in multiple time slots, user A and B will exchange d independent signal streams where d subjects to the constraint: $d \leq \min\left(m_A, m_{S_1}, \cdots, m_{S_{n-1}}, m_B\right)$. In other words, the maximum signal streams must be no more than the least antenna number of the nodes in the path. We assume that the selection of the relay node S_i from $N_A(i)$ is done according to the routing protocols in [1, 5, 6, 12, 13].

Let $\mathbf{a}$ and $\mathbf{b}$ be signal streams from A and B respectively, which need to be exchanged. We use the symbol $TS_n(t)$ to denote the tth time slot of n-hop information exchange. The objective of this paper is to design a physical layer secure information exchange protocol for the n-hop MIMO ad-hoc network with the minimized total number of time slots at the same security level.

2.2 Security Model

Adversarial Model for Relay Nodes. We have the following assumptions and requirements about relay nodes.

- Relay nodes can only launch passive attacks. In other words, the relay nodes would comply with the transmission protocols, however, they are curious about the messages from the users and try to recover them. This is referred to as a *honest-but-curious adversary model*.
- We also assume that there are no neighbouring nodes colluded. So all the relay nodes will only transmit their signals following the protocol without sharing their own information with other relays. The relay

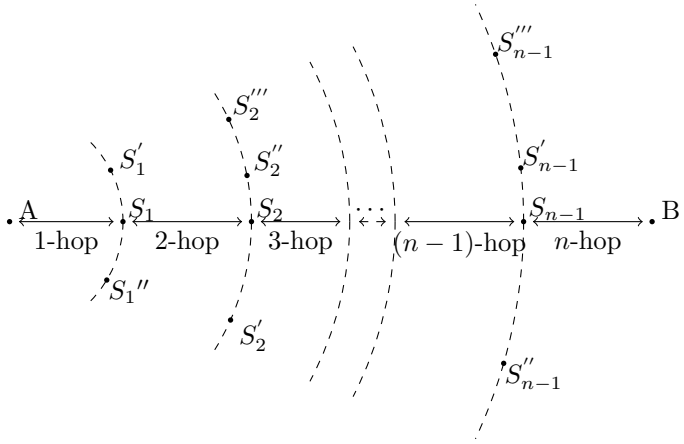

Figure 1: An n-hop Ad-hoc Network System for Information Exchange

nodes are also not colluded with external eavesdroppers, i.e., those which are not relay nodes in the system. For the selection of relay nodes, it is referring to [1, 5] for routing protocols and [9] for monitoring-based key revocation schemes for detecting colluded nodes.

- Each node in the path $(A, S_1, \cdots, S_{n-1}, B)$ employs a pseudorandom sequence generator (PRSG). For each information exchange, S_i generate a q-bit vector, which is modulated to a vector $\mathbf{r}_i, i = 0, \cdots, n$ where $\mathbf{r}_0 = \mathbf{a}$ and $\mathbf{r}_n = \mathbf{b}$ which are messages to be exchanged. For each information exchange, $\mathbf{r}_i$ is different. So, we assume that PRSG is secure in the sense that the probability that it generates identical random vectors at different exchange sessions is negligible.

Adversarial Model for External Eavesdroppers We assume that eavesdroppers are of wiretappers, i.e., they can only launch passive attacks by intercepting transmitted signals. This is the standard assumption for all physical layer security approaches. External eavesdroppers are allowed to collude together to recover the exchanged information.

In this paper, we will consider the eavesdropping attacks from both honest-but-curious relays and external eavesdroppers.

2.3 Transmission Model

We assume that each node, including user and relay nodes, only has direct communication link with its neighbours. For simplicity, we call the transmission with the direction from A side to B side as *right-link transmission*, and the opposite direction called *left-link transmission*.

We assume that the channels of all the links are flat-fading. So the entries of $\mathbf{H}_{J,K}$ and $\mathbf{H}_{K,J}$ are i.i.d symmetric complex Gaussian random variables with zero mean and unit variance. Both $\mathbf{H}_{J,K}$ and $\mathbf{H}_{K,J}$ remain constant in each round of information exchange. Finally, the channel state information (CSI) of each node is available for its neighbour nodes. Three types of transmission channel models will be used in our protocol, namely, one-way relay, two-way relay and multiple access channel models.

2.3.1 One-Way Relay Channel Model

In one-way relay channel model, only one node J or K transmit signal to its neighbour. For the right-link transmission, the node J transmit its signal with channel matrix $H_{J,K}$ to K as follow:

$$\mathbf{Y}_K = \mathbf{H}_{J,K}\mathbf{X}_J + \mathbf{Z}_K, \tag{1}$$

where $\mathbf{X}_K$ is a column vector which represents the transmitted signal vector of node J with size of $m_J \times 1$, $\mathbf{Y}_M$ denotes the received signal vector at K, which is an $m_K \times 1$ column vector, and $\mathbf{Z}_K$ is an $m_K \times 1$ zero mean circularly symmetric complex Gaussian noise vector at the node K with entries $\mathbf{Z}_K \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$.

Note. The notations $\mathbf{X}_*, \mathbf{Y}_*$ and $\mathbf{Z}_*$ will be used throughout the paper.

Similarly, we have the received signal at J by the left-link transmission as follows

$$\mathbf{Y}_J = \mathbf{H}_{K,J}\mathbf{X}_K + \mathbf{Z}_J, \tag{2}$$

where K sends its signal $\mathbf{X}_K$ to J with received signal $\mathbf{Y}_J$ and zero mean circularly symmetric complex Gaussian noise $\mathbf{Z}_J$. Also we have $\mathbf{Z}_J \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$.

We denote the covariances of the channel inputs as $\mathbf{Q}_t = \varepsilon\left(\mathbf{X}_c\mathbf{X}_c^t\right)$ for $t \in \{J, K\}$ where X^t denotes the transpose of X. Furthermore, we have the power constraint, given as

$$\mathrm{Tr}\left\{\mathbf{Q}_A + \sum_{i=1}^{n-1}\mathbf{Q}_{S_i} + \mathbf{Q}_B\right\} \leq P_{Tx} \tag{3}$$

where P_{Tx} is the total transmission power of all nodes.

2.3.2 Two-Way Relay Channel Model

Let $L \in N_K(1)$. The two-way relay channel model can guarantee that nodes J and L exchange information through the middle node K in two time slots.

In the first time slot, node J and L send their messages to K simultaneously and the received signal at K is given by

$$\mathbf{Y}_K = \mathbf{H}_{J,K}\mathbf{X}_J + \mathbf{H}_{L,K}\mathbf{X}_L + \mathbf{Z}_K. \tag{4}$$

This is also called the multiple access phase in the two-way relay channel model. In the second time slot K broadcasts its message to J and L. So the received signals at J and L are

$$\mathbf{Y}_J = \mathbf{H}_{K,J}\mathbf{X}_K + \mathbf{Z}_J, \tag{5}$$

$$\mathbf{Y}_L = \mathbf{H}_{K,L}\mathbf{X}_K + \mathbf{Z}_L. \tag{6}$$

2.3.3 Multiple Access Channel Model

In the multiple access channel model, the nodes J and L send their messages to K simultaneously. This channel model is identical to the first phase of the two-way relay channel model.

3 n-hop Information Exchange Protocol

In this section, we present a protocol for an n-hop exchange for $n > 2$. For $n = 2$, it reduces to a two-way relay channel model. However, since its operations serve as basic operations for a general n, we will first introduce it. The design principle is to guarantee that each of relay nodes or external eavesdroppers only received a sum signal from which it cannot recover each individual signal with non-negligible error probability.

3.1 *2*-hop Information Exchange Protocol

In the *2*-hop case, user A and B exchange information with a single relay S_1. This can be done as the same case as a two-way relay channel model. The approaches presented below are adopted from [14] for the two-way untrusted relay model with some modification to fit the n-hop ad-hoc case.

3.1.1 $TS_2(1)$ - Multiple Access Phase

In the first time slot, two users and one relay node S_1 execute the operations for multiple access channel model. Namely, two user A and B transmit their respective signals, $\mathbf{a}$ and $\mathbf{b}$, to a relay node S_1 simultaneously. Prior to the transmission, the information symbols $\mathbf{a}$ and $\mathbf{b}$ are modified by a precoding matrix $\mathbf{P}_A$ and $\mathbf{P}_B$ respectively at A and B. As the condition we made before, $\mathbf{a}$ and $\mathbf{b}$ are $d \times 1$ vectors with modulated signal entries. For example, if the elements in $\mathbf{a}$ and $\mathbf{b}$ are the baseband BPSK signal values, then

$$\begin{aligned} &\mathbf{a} = (a(0), a(1), \cdots, a(d-1)), \\ &\mathbf{b} = (b(0), b(1), \cdots, b(d-1)), \\ &a(i), b(i) \in \{1, -1\}. \end{aligned} \tag{7}$$

There are two time slots needed in *2*-hop information exchange. The pre-coding matrices $\mathbf{P}_i, i \in \{A, B\}$ are of $m_i \times d$ matrices, which is given by

$$\mathbf{P}_A = \mathbf{V}_A \mathbf{\Sigma}_A^{-1} \mathbf{U}_A^t \mathbf{R}_{A,B} \mathbf{\Psi}_A \mathbf{L}_{A,B} \tag{8}$$

where $\mathbf{U}_A$ and $\mathbf{V}_A$ are unitary matrices, and $\mathbf{\Sigma}_A^{-1}$ is the pseudo-inverse of $\mathbf{\Sigma}_A$. Note that $\mathbf{U}_A$, $\mathbf{V}_A$ and $\mathbf{\Sigma}_A$ are obtained from the singular value decomposition (SVD) of $\mathbf{H}_{A,S_1}$ as follows:

$$\mathbf{H}_{A,S_1} = \mathbf{U}_A \mathbf{\Sigma}_A \mathbf{V}_A^t. \tag{9}$$

The matrix $\mathbf{R}_{A,B}$ is the unitary *direction rotation matrix* with size of $m_{S_1} \times m_{S_1}$, which is available at the middle node S_1. The matrix $\mathbf{\Psi}_A$ represents the allocated transmission power for user A. In this paper, we assume that it is identical for all users and relay nodes. The *channel allocation matrix* $\mathbf{L}_{A,B}$ is formed by collecting the first d column vectors from the $m_{S_1} \times m_{S_1}$ identity matrix. So $\mathbf{L}_{A,B}$ is an $m_{S_1} \times d$ matrix. The $\mathbf{L}_{A,B}$ is the same for both A and B.

With precoding, the transmitting signals in user A and B can be rewritten as: $\mathbf{X}_A = \mathbf{P}_A \mathbf{a}$ and $\mathbf{X}_B = \mathbf{P}_B \mathbf{b}$, respectively. Then A and B send $\mathbf{X}_A$ and $\mathbf{X}_B$ to S_1 simultaneously, and the received signal at S_1 is

given by

$$\mathbf{Y}_{S_1} = \mathbf{H}_{A,S_1}\mathbf{P}_A\mathbf{a} + \mathbf{H}_{B,S_1}\mathbf{P}_B\mathbf{b} + \mathbf{Z}_{S_1} \tag{10}$$

where $\mathbf{Z}_{S_1}$ is the noise receiving at S_1. Note that

$$\begin{aligned}\mathbf{H}_{A,S_1}\mathbf{P}_A =& \mathbf{U}_A\mathbf{\Sigma}_A\mathbf{V}_A^t\mathbf{V}_A\mathbf{\Sigma}_A^{-1}\mathbf{U}_A^t\mathbf{R}_{A,B}\mathbf{L}_{A,B}\\ =& \mathbf{R}_{A,B}\mathbf{L}_{A,B},\end{aligned} \tag{11}$$

$$\begin{aligned}\mathbf{H}_{B,S_1}\mathbf{P}_B =& \mathbf{U}_B\mathbf{\Sigma}_B\mathbf{V}_B^t\mathbf{V}_B\mathbf{\Sigma}_B^{-1}\mathbf{U}_B^t\mathbf{R}_{A,B}\mathbf{L}_{A,B}\\ =& \mathbf{R}_{A,B}\mathbf{L}_{A,B}.\end{aligned} \tag{12}$$

Substituting (11) and (12) into (10), the received signal at relay node S_1 becomes

$$\mathbf{Y}_{S_1} = \mathbf{R}_{A,B}\mathbf{L}_{A,B}\left(\mathbf{a}+\mathbf{b}\right) + \mathbf{Z}_{S_1}. \tag{13}$$

Since S_1 has the knowledge of both $\mathbf{R}_{A,B}$ and $\mathbf{L}_{A,B}$, by multiplying $\mathbf{Y}_{S_1}$ by $\mathbf{L}_{A,B}^t\mathbf{R}_{A,B}^t$, the resulting signal is given by

$$\widetilde{\mathbf{Y}}_{S_1} = \left(\mathbf{a}+\mathbf{b}\right) + \mathbf{Z}_{S_1}^{'} \tag{14}$$

where $\mathbf{Z}_{S_1}^{'}$ is the resulting noise at S_1.

From (13) or (11) we can see that the signals from the separate nodes are aligned into the same direction. This would bring some benefits in transmission efficiency as well as security. For security aspects, the alignment causes a sum signal for the middle node or any external eavesdroppers. So the middle node or eavesdroppers can only get partial information which cannot guarantee a correct decode or the error probability of decoder is non-negligible. Consequently, by regulating controllable information leakage, the system can achieve information theoretic security [15].

Before we discuss the second time slot, we summarize the above results into the following proposition for easier reference later.

Proposition 1 *With the assumption and notation above, in the first time slot, $TS_2(1)$, the 2-hop exchange protocol aligns their respective transmitting signals* $\mathbf{a}$ *and* $\mathbf{b}$ *of A and B at their relay node S_1, which causes S_1's received signal given by (14). Thus, S_1 can only obtain the sum signal* $\mathbf{a}+\mathbf{b}$.

Since the operation involved in the 2-hop case will be frequently used later, we introduce an operator Δ to present it.

Definition 1 *For three consecutive nodes, say (U,V,W) in the n-hop path, the operator $\Delta(U,V,W)$ is defined as a function of U, V and W, for which U and W transmit their respective received signals* $\mathbf{x}$ *and* $\mathbf{y}$ *which are aligned at V, as shown in the 2-hop case through (8) - (14). So after removing pre-coding, V's received signal is the sum signal* $\mathbf{x}+\mathbf{y}$. *We call $\Delta(U,V,W)$ an* alignment operator*, and write*

$$\Delta(U(\mathbf{x}),V,W(\mathbf{y})) = V(\mathbf{x}+\mathbf{y}).$$

3.1.2 $TS_2(2)$ - Broadcasting Phase

In the second time slot, the relay node S_1 generates its transmitting signal X_{S_1} and broadcast. For the *2*-hop case, the relay just forwards the received signal with power constraint. So the received signal in user A is given by

$$\begin{aligned}\mathbf{Y_A} =& \mathbf{H}_{S_1,A}\mathbf{X}_{S_1} + \mathbf{Z}_A \\ =& \mathbf{H}_{S_1,A}(\mathbf{a}+\mathbf{b}) + \mathbf{Z}_{S_1} + \mathbf{Z}_A\end{aligned} \tag{15}$$

The interference for recovering $\mathbf{a}+\mathbf{b}$, A can be cancelled using detection vector $\mathbf{D}_A$, which is based on the channel matrix $\mathbf{H}_{S_1,A}$. Note that $\mathbf{H}_{S_1,A}$ is the transpose of the channel matrix $\mathbf{H}_{A,S_1}$ where the latter is known to A. Thus A computes

$$\mathbf{D}_A = \mathbf{U}_A\left(\Sigma_A^t\right)^{-1}\mathbf{V}_A^t.$$

Applying $\mathbf{D}_A$ to the front-end signal from S_1, the received signal of A becomes

$$\begin{aligned}\widetilde{\mathbf{Y}}_A &= \mathbf{D}_A\mathbf{Y}_A = \mathbf{D}_A\left[\mathbf{H}_{S_1,A}(\mathbf{a}+\mathbf{b})\right] + \mathbf{D}_A\mathbf{Z}_{S_1} + \mathbf{D}_A\mathbf{Z}_A \\ &= \mathbf{U}_A\left(\Sigma_A^t\right)^{-1}\mathbf{V}_A^t\mathbf{V}_A\Sigma_A^t\mathbf{U}_A^t(\mathbf{a}+\mathbf{b}) + \mathbf{D}_A\mathbf{Z}_{S_1} + \mathbf{D}_A\mathbf{Z}_A \\ &= (\mathbf{a}+\mathbf{b}) + \mathbf{Z}_A^{'},\end{aligned}$$

where $\mathbf{Z}_A^{'}$ is the sum noise at A. The operation at B is the same as A. Thus B can also decode $\mathbf{a}$ with the subtraction of its self-information. One information exchange of the 2-hop case is now completed.

We summarize the above results into the following proposition.

Proposition 2 *With the above assumptions and notation, in $TS_2(2)$, after S_1 broadcasts $\mathbf{a}+\mathbf{b}$, both A and B can recover the exchanged signal $\mathbf{a}$ and $\mathbf{b}$, i.e., A can recover $\mathbf{b}$, which is transmitted from B in the first time slot, and B can recover $\mathbf{a}$, which is transmitted from A in the first time slot.*

3.2 Protocol for n-hop Exchange

For a general n-hop case, we need to distinguish the cases of n being even or odd. We define

$$k = \begin{cases} \frac{n}{2} & n \text{ is even, i.e., } n = 2k \\ \frac{n+1}{2} & n, \text{ is even, i.e., } n = 2k-1 \end{cases}$$

3.3 Protocols for n-hop Exchange

Recall that $S_0 = A$ and $S_n = B$. We present the protocol in Tables 1 and 2 for n even and odd respectively using the operation Δ with the additional operation that the middle node will subtract its self-information to get $\mathbf{a}+\mathbf{r}_{i+1}$ at S_i for $i > 1$ (when $i = 1$ and $i = n-1$ there is no subtraction) and prepare for the next time slot transmission.

Table 1: Protocol 1: n-Hop Information Exchange for $n = 2k > 3$

Time Slot	Actions
$TS_n(i)$	$\Delta(S_{i-1}, S_i, S_{i+1})$
$1 \le i \le k-2$	$\Delta(S_{n-(i-1)}, S_{n-i}, S_{n-(i+1)})$
$TS_n(k-1)$	$\Delta(S_{k-2}, S_{k-1}, S_k)$
$TS_n(k)$	$\Delta(S_k, S_{k+1}, S_{k+2})$
$TS_n(k+1)$	$\Delta(S_{k-1}, S_k, S_{k+1})$
$TS_n(k+2)$	S_k broadcasts $\mathbf{a}+\mathbf{b}$
$TS_n(k+2+i)$	S_{k+i} right-link one-way relay
$1 \le i \le k-1$	S_{k-i} left-link one-way relay

Table 2: Protocol 1: n-Hop Information Exchange for $n = 2k-1 \ge 3$

Time Slot	Actions
$TS_n(i)$	$\Delta(S_{i-1}, S_i, S_{i+1})$
$1 \le i \le k-2$	$\Delta(S_{n-(i-1)}, S_{n-i}, S_{n-(i+1)})$
$TS_n(k-1)$	$\Delta(S_{k-2}, S_{k-1}, S_k)$
$TS_n(k)$	$\Delta(S_{k-1}, S_k, S_{k+1})$
$TS_n(k+1)$	S_k broadcasts $\mathbf{a}+\mathbf{b}$
$TS_n(k+1+i)$	S_{k+i} right-link one-way relay
$1 \le i \le k-2$	S_{k-i} left-link one-way relay
$TS_n(2k)$	S_1 left-link one-way relay

The actions in Protocol 1 for n even are detailed as follows. From now on, any explanation involving different time slots, we will restrict ourselves to the even case. Since the discussions for n odd are similar, they will be omitted here.

(a) *Phase 1.* Time slots from 1 to k: For time slot 1 to $k-2$, each set of consecutive three nodes acts as a multiple access model to conduct an alignment in the middle node starting from both ends A and B. For $k-1$ and k, it executes just one alignment for left then right-link respectively. From the left-link, the aligned sum $\mathbf{a}+\mathbf{r}_2$ is propagated to $\mathbf{a}+\mathbf{r}_k$ at S_{k-1}. From the right direction, the aligned sum $\mathbf{b}+\mathbf{r}_{n-2}$ is propagated to $\mathbf{b}+\mathbf{r}_{k+1}$ at S_{k+1}.

(b) *Phase 2.* Time slots $k+1$ and $k+2$: (S_{k-1}, S_k, S_{k+1}) acts as a two-way untrusted relay model or equivalently a 2-hop exchange. Namely, they align at S_k to get $\mathbf{a}+\mathbf{b}$, then S_k broadcasts it.

(c) *Phase 3.* Time slots from $k+3$ to $2k+1 = n+1$: From S_{k-1}, it conducts right-link one-way relay model, and from S_{k+1}, left-link one-way relay transmission simultaneously until they reach both end nodes, A

and B. Then A and B can recover the exchanged secrets respectively.

Theorem 1 *With Protocol 1,*

(a) the total number of time slots for Protocol 1 is equal to $n+1$.

(b) The received signal of each relay node or external eavesdroppers is the sum signal, say $\mathbf{w} = \{w(0), \cdots, w(d-1)\}$. Relay nodes or the external eavesdroppers can only decode the ith entry of $\mathbf{w}$ in each summand for the case that all ith summands in $w(i)$ are equal. For the other cases, the decoder does not work better than a random guess.

Proof. The first assertion follows immediately from Protocol 1. For the second assertion, from Protocol 1 (n even), $\mathbf{w}$ can only be one of the following four types of sum signals.

(a) For Phase 1, the sum signal for the first time slot is

$$\begin{array}{l} \mathbf{d}+\mathbf{u}: \text{ Type 1 where} \\ \mathbf{d}+\mathbf{u} \in \{\mathbf{a}+\mathbf{r}_2, \mathbf{b}+\mathbf{r}_{n-2}\}. \end{array} \tag{16}$$

For $1 < i \leq k$, the sum signal is

$$\mathbf{a}+\mathbf{r}_i+\mathbf{r}_{i+1} \text{ and } \mathbf{b}+\mathbf{r}_{n-i}+\mathbf{r}_{n-(i+1)}: \text{ Type 2.} \tag{17}$$

(b) For Phase 2, the sum signal is given by

$$\mathbf{a}+2\mathbf{r}_k+\mathbf{b}: \text{ Type 3} \tag{18}$$

(c) For Phase 3, for each relay node, the received sum signal is

$$\mathbf{a}+\mathbf{b}: \text{ Type 4} \tag{19}$$

For simplicity, in the following, we only show that for the BPSK case.

Since the elements of $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{r}_j$ have values in $\{1,-1\}$, the elements of $\mathbf{w} = (w(0), \cdots, w(d-1))$ are given by

		Deterministic case
Type 1, Type 4	$w(i) \in \{0, \pm 2\}$	$w(i) = \pm 2 \Longrightarrow d(i) = u(i) = \pm 1$
Type 2	$w(i) \in \{\pm 1, \pm 3\}$	$w(i) = \pm 3 \Longrightarrow d(i) = u(i) = v(i) = \pm 1$
Type 3	$w(i) \in \{0, \pm 2, \pm 4\}$	$w(i) = \pm 4 \Longrightarrow d(i) = u(i) = v(i) = \pm 1$

where the column lists the deterministic case. In other words, when $w(i)$ is equal to the maximum magnitude of the possible values of $w(i)$, it can decode that each components is of equal value. For all the other cases, the decoder can only randomly guess the values of $b(i)$, $u(i)$, and $r_j(i)$. Thus, the result is true.

□

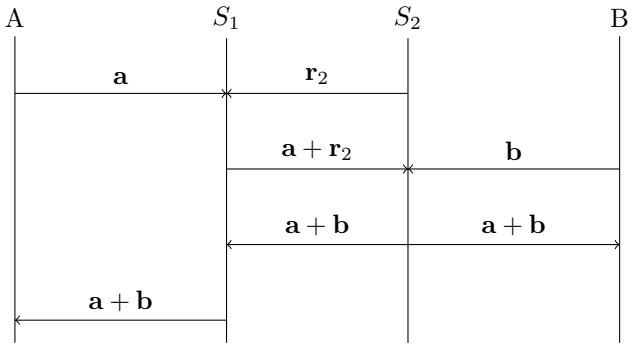

Figure 2: Information Flow in Protocol 1 for 3-hop Exchange

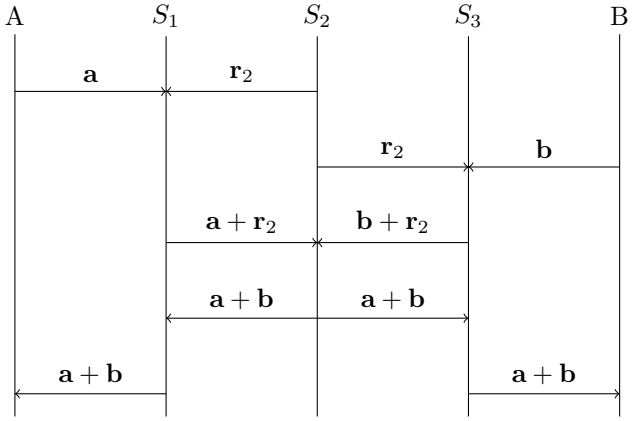

Figure 3: Protocol 1 for 4-hop Information Exchange

Remark 1 *Note that we distinguish Type 1 and Type 4, because Type 1 can be considered as the case that the information signal is masted by a pseudorandom signal* $\mathbf{r}_j$ *generated by a PRSG, but Type 4 is just the sum of two exchanging signals. This fact will be used in next section for security analysis of the protocol.*

Theorem 2 *The total number of time slots in Protocol 1 is minimized.*

Proof. Note that there are n-hops. Without the requirement for privacy, users A and B exchanging their respective signals $\mathbf{a}$ and $\mathbf{b}$ need at least $n+1$ time slots. The minimum number is $n+1$ which can be achieved by A conducting right-link one-way relay along the path from A to B and B, left-link one-way relay along the path from B to A (recall that we assumed that the crossing node can only do half duplex transmission). Thus the assertion is established. □

Example of Protocol 1 for $n = 3, 4$ *and 5.* The protocol flows of $n = 3, 4, 5$ are shown in Figures 2 , 3 and 4 respectively.

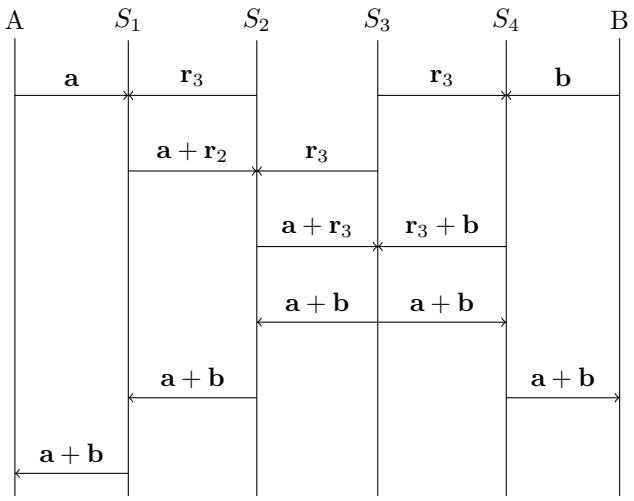

Figure 4: Protocol 1 for 5-hop Information Exchange

4 Security Analysis and Secrecy Capacity of the n-hop Exchange Protocol

In this section, we first analyze the security brought by the sum signals in transmission processes of Protocol 1, then we briefly introduce secrecy capacity of the system.

4.1 Security for Preventing Honest-but-Curious Relays

The goal of the relays is to attempt to recover the exchanged message $\mathbf{a}$ and $\mathbf{b}$. From (16) - (19), in the first $k+2$ time slots, a sum signal that a relay can obtain is the sum of one exchanged signal and the other is a vector generated by a PRNG or the linear combination of two sequences generated by PRNGs. In this case, it is analog to the cryptographic approach, i.e., the sum signal can be considered as a ciphertext from stream cipher encryption at the signal level (for the details of stream cipher encryption, the reader is referring to [2]. Thus, the relay node cannot decrypt that.

In the last $k-2$ time slot, each relay nodes receives the sum signal $\mathbf{a}+\mathbf{b}$. This is analog to the case that in a stream cipher encryption, to encrypt two messages, say $\mathbf{m}_1$ and $\mathbf{m}_2$, using an identical key stream, say K, then attacker can obtain $\mathbf{m}_1-\mathbf{m}_2$ when he gets two ciphertext $\mathbf{c}_1=\mathbf{m}_1+K$ and $\mathbf{c}_2=\mathbf{m}_2+K$. Thus, if two messages $\mathbf{a}$ and $\mathbf{b}$ are correlated, then it is possible that a relay node can recover $\mathbf{a}$ so that $\mathbf{b}$ with non negligible probability. Hence, this is a similar weakness as a stream cipher encryption. This can be prevented by increasing number of time slots, which will be discussed in a future work.

4.2 Security for Preventing External Eavesdroppers

In general, there are three different scenarios for an external eavesdropper (we allow them to collude together).

(a) *Case 1.* The eavesdroppers cannot correctly receive the signals in each transmission in Protocol 1 unless they can get the CSI of all the channels. Otherwise the eavesdroppers cannot cancel the channel influence, Nevertheless, the intended receiver will correctly receive with the help of the precoding matrix.

(b) *Case 2.* Assume that the eavesdroppers can get the CSI, which is a rather strong assumption. However, the eavesdropper still cannot get the liner filter, used in MIMO modulation. So the eavesdroppers still fail to recover the message from the users.

(c) *Case 3.* Even though the eavesdroppers can get all the signals as the relay nodes, the received signal in the eavesdroppers is still a sum signal which is the same case as in the relay nodes. So the security will be identical as the analysis for the relay nodes above. Note that the sum signal receiving at an eavesdropper will be more complexity than the relay nodes. Hence some void signal at the beginning and the ending of each time slot may be used, and the detail discussions of those cases will be in a future work.

4.3 Secrecy Capacity of Three Channel Models

We first present the secrecy capacity for each of three different channel models, then we show a general formulation for the entire system. For the deviation of secrecy capacity, we restrict ourselves to a simple case that there is no external eavesdroppers except for the one-way relay channel. For the other cases, it is quite involved when we consider the secrecy capacity in the presence of both honest-but-curious relays and external eavesdroppers, which will be our future work.

4.3.1 Secrecy Capacity of One-Way Relay Channel

For the one-way relaying model in Phase 3 in Protocol 1, receiver K will directly get the transmitting signal from J, which is the sum signal $\mathbf{a}+\mathbf{b}$, so the secrecy capacity of this link will be the difference of the channel capacity and external eavesdropper. We denote C_{OWt} as the secrecy capacity of t-link one-way relay channel where t is either left or right. For the left-link channel , we have:

$$C_{OWL} = I\left(\mathbf{Y}_K; \mathbf{X}_J\right) - I\left(\mathbf{Y}_E; \mathbf{X}_A, \mathbf{X}_B\right), \tag{20}$$

where $\mathbf{Y}_E$ represents the received signal at the eavesdropper, and $\mathbf{X}_A$,$\mathbf{X}_B$ are the users' transmitting signals. Similarly, we have the secrecy capacity for right-link channel as:

$$C_{OWL} = I\left(\mathbf{Y}_J; \mathbf{X}_K\right) - I\left(\mathbf{Y}_E; \mathbf{X}_A, \mathbf{X}_B\right), \tag{21}$$

4.3.2 Secrecy Capacity of Two-Way Relay Channel

In this case, the secrecy capacity of this case is similar to the two-way untrusted relay channel in [15] and [14]. Note that in order to exchange information securely, node J and L regulates their transmission rates to guarantee the successful transmission. Thus the secrecy capacity of the two-way relay channel, denoted as C_{TWR}, is given by

$$C_{TWR} = \left[C_J + C_L - R_K\right]^+, \tag{22}$$

where $[x]^+ = \max(0, x)$, C_J is the channel capacity between J and K which is the same as transmission rate of J. Thus

$$C_J = \min\left[I\left(\mathbf{Y}_K; \mathbf{X}_J\right), I\left(\mathbf{Y}_J; \mathbf{X}_K\right)\right]. \tag{23}$$

Similarly, C_L is the channel capacity between L and K which can be determined by

$$C_L = \min\left[I\left(\mathbf{Y}_K; \mathbf{X}_L\right), I\left(\mathbf{Y}_L; \mathbf{X}_K\right)\right]. \tag{24}$$

We denote R_K the achievable information rate at the untrusted relay, which is given by

$$R_K = I\left(\mathbf{Y}_K; \mathbf{X}_J, \mathbf{X}_L\right). \tag{25}$$

4.3.3 Secrecy Capacity of Multiple Access Channel Model

Since this case is equal to the first phase in a two-way relay channel model, the deviation is identical to that case. Thus, the secrecy capacity of multiple access channel model, denoted as C_{MAC}, can be derived as:

$$C_{MAC} = C_{TWR} = \left[C_J + C_L - R_K\right]^+. \tag{26}$$

However, since there is no second phase, then

$$C_J = I\left(\mathbf{Y}_K; \mathbf{X}_J\right), C_L = I\left(\mathbf{Y}_K; \mathbf{X}_L\right) \tag{27}$$

which are different from (23) and (24). The achievable information rate at the untrusted relay remains as the same as shown in (25).

4.4 Secrecy Capacity of the System

For an n-hop exchange protocol, at each time slot, the nodes conduct one of these three transmission methods. So, the question we would like to ask is: how to determine the secrecy capacity of the system.

We denote $C_n(t)$ the secrecy capacity of time slot $TS_n(t)$. Then $C_n(t)$ can be obtained by (20) and (22). Note that the secrecy capacity of each time slot of two different time slots in the two-way relay model is equal to the secrecy capacity of the two-way relay channel. Thus $C_n(t) = C_n(t+1) = C_{TWR}$.

According to the result in [4], the secrecy capacity for n-hop exchange equals the minimum supremum of the secrecy capacity of each time slot. So the secrecy capacity for n-hop exchange is given by

$$C_{nhop} = \frac{1}{T}\sup\min\left\{C_n(1), C_n(2), \cdots C_n(T)\right\}, \tag{28}$$

where T is the total time slots of an n-hop information exchange protocol. Note that the divisor T is needed because there are T time slots needed for the n-hop information exchange.

4.5 Secrecy Capacity for Protocol 1

We will first give a detailed deviation for $n = 2$ case, since it serves as a basic case for general $n > 2$. As we mentioned before, 2-hop model can be considered as the two-way untrusted relay channel. Thus the secrecy capacity of 2-hop exchange system by Protocol 1 is determined by their respective channel capacities C_A and C_B of A and B, and R_{S_1}, the rate of S_1 in transmission. The value of C_A is given by

$$C_A = \min\left[I\left(\mathbf{Y}_{S_1};\mathbf{X}_A\right), I\left(\mathbf{Y}_A;\mathbf{X}_{s_1}\right)\right] \tag{29}$$

where

$$\begin{aligned} I\left(\mathbf{Y}_{S_1};\mathbf{X}_A\right) &= \log\det\left(\mathbf{I} + \mathbf{H}_{A,S_1}\mathbf{P}_A\mathbf{P}_A^t\mathbf{H}_{A,S_1}^t\right), \\ I\left(\mathbf{Y}_A;\mathbf{X}_{s_1}\right) &= \log\det\left(\mathbf{I} + \mathbf{H}_{S_1,A}\mathbf{P}_A\mathbf{P}_A^t\mathbf{H}_{S_1,A}^t\right). \end{aligned} \tag{30}$$

Similarly, we can get C_B, given by

$$C_B = \min\left[I\left(\mathbf{Y}_{S_1};\mathbf{X}_B\right), I\left(\mathbf{Y}_B;\mathbf{X}_{S_1}\right)\right] \tag{31}$$

where

$$\begin{aligned} I\left(\mathbf{Y}_{S_1};\mathbf{X}_B\right) &= \log\det\left(\mathbf{I} + \mathbf{H}_{B,S_1}\mathbf{P}_B\mathbf{P}_B^t\mathbf{H}_{B,S_1}^t\right), \\ I\left(\mathbf{Y}_B;\mathbf{X}_{S_1}\right) &= \log\det\left(\mathbf{I} + \mathbf{H}_{S_1,B}\mathbf{P}_B\mathbf{P}_B^t\mathbf{H}_{S_1,B}^t\right). \end{aligned} \tag{32}$$

The received signal at untrusted relay S_1 is the same as in a multi-user multiple access channel (MAC). So the achievable information rate of S_1 is given by

$$\begin{aligned} R_{S_1} = \log\det\Big[\mathbf{I} + \big(&\mathbf{H}_{A,S_1}\mathbf{P}_A\mathbf{P}_A^t\mathbf{H}_{A,S_1}^t \\ &+\mathbf{H}_{B,S_1}\mathbf{P}_B\mathbf{P}_B^t\mathbf{H}_{B,S_1}^t\big)\Big]. \end{aligned} \tag{33}$$

Together with (22), (30), (32) and (33), using (28), it follows the secrecy capacity, shown below

$$C_{2hop} = \frac{1}{2}\left[C_A + C_B - R_{S_1}\right]^+. \tag{34}$$

For Protocol 1 of n even, in the case of no external eavesdroppers, we have the following analysis.

(a) Phase 1: In time slot $i : 1 \le i \le k-2$, $C_n(i)$ is the minimum of the secrecy capacities of two multiple access channels, and for $i = k-1$ and $i = k$, each is equal to the secrecy capacity of a multiple access channel. The secrecy capacity of the multiple access channel, C_{MAC}, is given by (22).

(b) Phase 2. In time slot $k+1$ and $k+2$, this is a two-way relay channel, so $C_n(k+1) = C_n(k+2) = C_{TWR}$ given by (22).

(c) In Phase 3, there are $k-1$ respective right-link and left-link one-way relay channel. So $C_n(k+2+i), i = 1, \cdots, k-1$ is equal to the minimum of the secrecy capacities of those two links, C_{OWL} and C_{OWR}, given by (20) and (21) where the second term in each of those equations is zero (because we assume that there is no external eavesdropper).

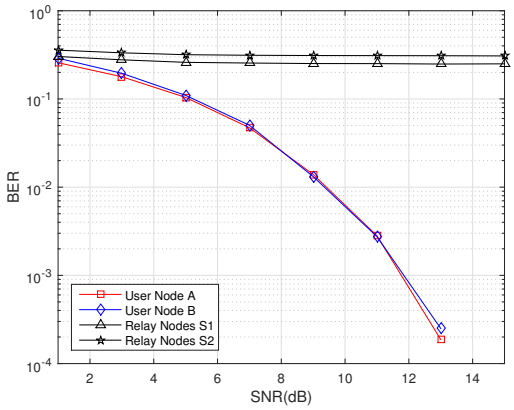

Figure 5: BER Performance Comparison between Different Nodes in 3-hop Information Exchange Protocol

According to (28), we have the following proposition.

Proposition 3 *The secrecy capacity of n-hop exchange by Protocol 1 is given by*

$$C_{nhop} = \frac{1}{n+1} \sup \min \left\{ C_n(1), C_n(2), \cdots C_n(n) \right\}, \tag{35}$$

where $C_n(j)$'s are determined by C_{OWL}, C_{OWR}, C_{TWR} and C_{MAC}, discussed above.

5 Simulations and Some Comparisons

5.1 Simulation Results

In this subsection we show three simulations to demonstrate the performance of our protocol. In the first simulation, we compare the bit error ratio (BER) between intended receivers and relay nodes in the 3-hop information exchange protocol. In the second simulation, we explore the relationship between the secrecy capacity and hop number. Last, we show how the number of antennas influences the secrecy capacity.

In the first simulation, we compare the BER of different nodes in the 3-hop information exchange protocol, shown in Figure 5. Each node is equipped with four antennas in the simulation. Also, we assume a stronger adversarial model where the relay node can obtain the direction rotation matrix. From Figure 5 we can see that the BER at each node will decrease largely when SNR increases. However, the BER at the relay nodes will remain. It is worth to point out that the BER at S_1 is slightly smaller than S_2. This phenomenon seems to suggests that S_1 may get slightly more secret information either on $\mathbf{a}$ or on $\mathbf{b}$ than S_2 from the sum signal. Indeed, S_1 receives $\mathbf{a} + \mathbf{r}_2$ and S_2 receives $\mathbf{a} + \mathbf{r}_2 + \mathbf{b}$, but it can get $\mathbf{a} + \mathbf{b}$ by subtracting itself signal $\mathbf{r}_2$. However, such increasing partial information still cannot guarantee its correct decoding. This experiment demonstrates that our proposed scheme can resist the relay's or eavesdropping attack effectively.

In Figure 6 we show the relationship between the secrecy capacity and hop number. We set the antenna number of each node is two in this simulation. By comparing secrecy capacity of *2*-hop, *3*-hop and *4*-hop,

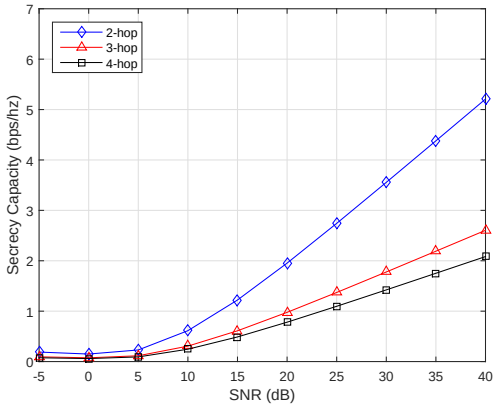

Figure 6: Secrecy Capacity Comparison among *2*-hop, *3*-hop and *4*-hop Information Exchange

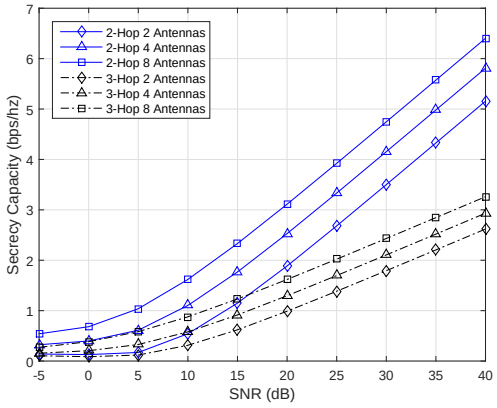

Figure 7: Secrecy Capacity Comparison between *2*-hop and *3*-hop under 2, 4 and 8 Antennas Equipment

we can see that the secrecy capacity will suffer a decline with an increased hop number. Such a decline is mainly caused by the increased total time slots. So the number of time slots optimization will be of great value. In Section 3, we have shown our proposed protocol costs the minimum time slots for each secure information exchange.

In the last simulation, we present the impact of the antenna number to the secrecy capacity. The result is plotted in Figures 7 and 8. We test the secrecy capacity under nine cases: *2*-hop case with 2, 4 and 8 antennas, *3*-hop case with 2, 4 and 8 antennas, and *4*-hop case with 2, 4 and 8 antennas. By the simulating results, as shown in Figures 7 and 8, we can conclude that the secrecy will enjoy a linear increase when the antenna number fits the accepted theoretical analysis and SNR larger than 25 dB. This simulation also shows that increasing antenna number in larger hop information exchange can increase the secrecy capacity of the system when the system is operated under some extreme serious conditions,, i.e., small SNR. This results provides a trade-off among the number of antennas, hop numbers, and SNR in the system.

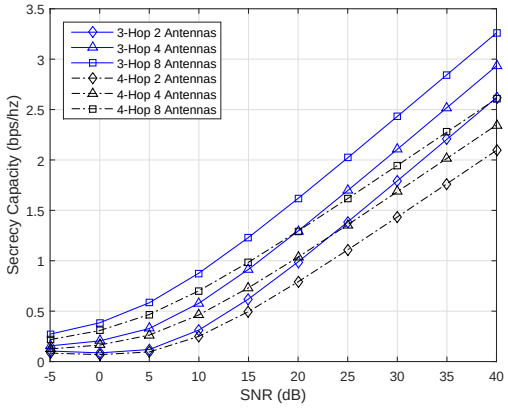

Figure 8: Secrecy Capacity Comparison between 3-hop and 4-hop under 2, 4 and 8 Antennas Equipment

5.2 Benefits and Comparisons with Known Approaches

For the performance of Protocol 1, since our proposed scheme is the first secure information protocol in MIMO ad-hoc systems with physical layer approach, we may compare it with an approach by crypto. In other words, this problem can be solved using a cryptographic approach described as follows.

Two users wish to exchange their respective information should first share the key before they start to communicate or employ a public-key system to share a key before transmitting exchanging information. After the key is established, two users will use the end-to-end encryption model to exchange information (for the end-to-end encryption, see Section 8.4.2 in [2]). In this way, no relay nodes can do decryption. Note it also requests $n+1$ time slots for an n-hop ad-hoc system where the transmission schedule will be the same as the naive scheme without privacy as described in the proof of Theorem 2. However, a key generation, distribution and management centre (KGC) is needed for generating keys, distributing keys, revoking the old key if it is compromised and issuing a new key at the same time, or update keys regularly for security results. KGCs for the ad-hoc networks constitute a challenge for implementing them.

However, our proposed scheme does not need the key, which eliminates this problem. Furthermore, the physical layer security can reduce the overhead of the upper layer security protocols. Finally, our proposed scheme can be easily to equip for the users, since it only requests only a precoding matrix. We summarize the above discussions in Table 3.

6 Concluding Remarks and Discussions

In this paper, we consider the case that two mobile users in a mobile ad hoc network (MANET) exchanges their information with the help of one or multiple relay nodes for which users and relay nodes are equipped with multiple antennas. Therefore, they form an MIMO system. We call this the n-hop information exchange. We proposed a transmission protocol for the n-hop information exchange using physical layer's three basic transmission models: one-way untrusted relay, two-way untrusted relay and multiple access. Any relay node only received a summed signal and cannot decompose it to obtain the individual summand signal. The total

Table 3: Comparisons of Three Schemes

Scheme	Resistant to EA*	Need of KGC	O
Protocol 1	Yes	No	3
Naive approach	No	No	2
Crypto approach	Yes	Yes	2

* EA represents eavesdropping attack, and O represents the number of operations in each relay.

number of time slots used in the proposed protocol is equal $n+1$, which is minimized at the same security level. The secrecy capacity is derived and formalized.

We have simulated our n-hop information exchange protocol. The simulation demonstrated the confidentiality of exchanged message is achieved in terms of bit-error-rate for the intended receivers and relayers. The simulation showed that the secrecy capacity will be declined with an increased hop number. This decline is mainly due to the total number of the time slots used in the protocol. However, we have shown that the total number of the time slots in the protocol is $n+1$ for an n-hop exchange. This simulation provided some insights for this phenomena, which will effect the way to compute the secrecy capacity for a multi-hop transmission system. Furthermore, increasing the number of antennas for each node will increase the secrecy capacity. However, under a certain threshold of SNR, increasing number of antennas can be served as compensation for the secrecy capacity loss from increased hop numbers, or equivalently, increasing the distance between two uses for exchanging secret information. The phenomena from the simulations deserve further research.

Mobile ad hoc networks (MANETs) found many applications in many extreme situations for government, business and civilian for which key distribution and management constitute a challenge problem in practice. When the devices in MANETs equipped with multiple antennas, they form an MIMO transmission system in MANETs. MIMO ad hoc networks provide an additional redundancy for physical layer security. The proposed protocol for n-hop information exchange can be served as a key exchange protocol in the system. In this case, all relay nodes should be faithfully process the protocol, but try to obtain the exchanged keys. For the outside attackers, we assume that they can only launch passive attacks, like passive eavesdropping. In cryptographic approaches, authenticated key exchange protocols using the Diffie-Hellman approach need to use public-key infrastructure to issue public-key certificates for providing authenticity of exchanged keys. Thus another interesting future work lies in investigating the possibility of designing a transmission protocol for n-hop information/secret exchange against active man-in-the-middle attacks.

Acknowledgment

The author would like to thank Qiao Liu for providing simulations and many valuable discussions for this work.

References

[1] Sonali Bhargava and Dharma P Agrawal. Security enhancements in aodv protocol for wireless ad hoc networks. In *Vehicular Technology Conference, 2001. VTC 2001 Fall. IEEE VTS 54th*, volume 4, pages 2143–2147. IEEE, 2001.

[2] Lidong Chen and Guang Gong. *Communication System Security*, pages 358–359. CRC Press Taylor & Francis Group, 2012.

[3] Shan Chu, Xin Wang, and Yuanyuan Yang. Exploiting cooperative relay for high performance communications in MIMO ad hoc networks. *IEEE Trans. Computers*, 62(4):716–729, 2013.

[4] Thomas M Cover and Joy A Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[5] Samir R Das, Elizabeth M Belding-Royer, and Charles E Perkins. Ad hoc on-demand distance vector (aodv) routing. 2003.

[6] Djamel Djenouri and Nadjib Badache. On eliminating packet droppers in MANET: A modular solution. *Ad Hoc Networks*, 7(6):1243–1258, 2009.

[7] Bechir Hamdaoui and Parameswaran Ramanathan. A cross-layer admission control framework for wireless ad-hoc networks using multiple antennas. *IEEE Transactions on Wireless Communications*, 6(11):4014–4024, 2007.

[8] Duong A. Hoang and Ronald A. Iltis. Noncooperative eigencoding for MIMO ad hoc networks. *IEEE Transactions on Signal Processing*, 56(2):865–869, 2008.

[9] Katrin Hoeper and Guang Gong. Monitoring-based key revocation schemes for mobile ad hoc networks: Design and security analysis. Technical report, Citeseer, 2009.

[10] Kaibin Huang, Jeffrey G. Andrews, Dongning Guo, Robert W. Heath Jr., and Randall A. Berry. Spatial interference cancellation for multiantenna mobile ad hoc networks. *IEEE Transactions on Information Theory*, 58(3):1660–1676, 2012.

[11] Cheol Jeong, Il-Min Kim, and Dong In Kim. Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system. *IEEE Transactions on Signal Processing*, 60(1):310–325, 2012.

[12] D Johnson, Y Hu, D Maltz, et al. The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4. Technical report, RFC 4728, February, 2007.

[13] David B Johnson and David A Maltz. Dynamic source routing in ad hoc wireless networks. In *Mobile computing*, pages 153–181. Springer, 1996.

[14] Qiao Liu, Guang Gong, Yong Wang, and Hui Li. A novel physical layer security scheme for MIMO Two-Way relay channels. *CACR 2015-05 Technical Report, University of Waterloo*, 2015.

[15] Jianhua Mo, Meixia Tao, Yuan Liu, and Rui Wang. Secure beamforming for MIMO two-way communications with an untrusted relay. *IEEE Transactions on Signal Processing*, 62(9):2185–2199, 2014.

[16] Ayfer Özgür, Olivier Lévêque, and David Tse. Spatial degrees of freedom of large distributed MIMO systems and wireless ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 31(2):202–214, 2013.

[17] Karthikeyan Sundaresan and Raghupathy Sivakumar. Routing in ad-hoc networks with MIMO links: Optimization considerations and protocols. *Computer Networks*, 52(14):2623–2644, 2008.

[18] Rongqing Zhang, Lingyang Song, Zhu Han, and Bingli Jiao. Physical layer security for two-way untrusted relaying with friendly jammers. *IEEE Transactions on Vehicular Technology*, 61(8):3693–3704, 2012.