Wireless MIMO Switching with Trusted and Untrusted Relays: Degrees of Freedom Perspective

Fanggang Wang*, Xiaojun Yuan†, Jemin Lee‡, and Tony Q. S. Quek§
*State Key Lab of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China
†School of Information Science and Technology, ShanghaiTech University, Shanghai, China
‡Singapore University of Technology and Design, Singapore

Abstract—We investigate the degrees of freedom (DoF) and secrecy DoF for a general framework of multiway relay networks named wireless MIMO switching, where a number of users exchange information via a common relay. Each round of data exchange consists of one uplink transmission from users to relay and one downlink transmission from relay back to users. The data exchange model is unicast, i.e., every user transmits one message and intends to receive one message from one other user. We categorize unicast patterns using the notion of orbit borrowed from abstract algebra. Roughly speaking, an orbit is a minimum subset of users such that data exchange is closed within this subset. We analyze the achievable DoF of wireless MIMO switching with various numbers of orbits. Particularly, the DoF capacity for unicast with one and two orbits are established. Furthermore, we study communication secrecy with an untrusted relay in wireless MIMO switching. We present an achievable secrecy sum rate and the corresponding achievable secrecy DoF by assuming a non-regenerative relay. Then, we focus on unicast patterns with one and two orbits, and show that this achievable lower bound is actually the secrecy DoF capacity based on a novel genie-aided technique. Our results build a bridge between the DoF and the secrecy DoF in multiway relaying. The methodology of the proof can be generally applied to analyze the secrecy DoF in other relay networks.

Index Terms—Degrees of freedom, MIMO switching, physical-layer network coding, multiway relay, secrecy sum rate.

I. INTRODUCTION

Since the advent of physical-layer network coding [1], there has been a surge of work on multiway relaying in which multiple users exchange information via the help of a relay node [2]–[9]. The transmission protocol of a multiway relay channel usually consists of two phases, namely, one uplink phase in which users transmit to the relay simultaneously, and one downlink phase in which the relay broadcasts to users. A variety of traffic patterns have been studied in multiway relay channels, such as pairwise data exchange [6], [10], in which users form pairs and exchange data within each pair, and full data exchange, in which each user broadcasts to all other users [8]. Later, the authors in [9] and [11] studied efficient communication protocols for clustered full data exchange and clustered pairwise data exchange, where the users in the network are divided into clusters and data exchange is conducted within each cluster.

Multiple-antenna (or multiple-input multiple-output (MIMO)) techniques have been introduced into multiway relaying to achieve multiplexing gain. Degrees of freedom (DoF) is an important performance measure to characterize the multiplexing gain in the high signal-to-noise regime. Interference alignment is a powerful tool to analyze the DoF of a multiway relay channel. A similar idea, termed signal space alignment, was proposed in [12] to derive the DoF capacity of a three-user multiway relay channel with pairwise data exchange. Recently, multiway relaying with clustered full data exchange was investigated in [9], and achievable DoF was derived for the configuration of an arbitrary number of user nodes and an arbitrary number of antennas at each user/relay node. However, these results generally serve as DoF lower bounds, and the DoF capacity of the multiway relay channel, especially with a general traffic pattern, is still far from being well understood.

Information secrecy poses a critical concern in wireless networks. The three-node relay channel with the relay being an eavesdropper was first proposed in [13]. In this model, the relay is forced to forward signals following a designated relaying protocol; at the same time, the relay is free to guess the source data based on the received signal. This model is relevant because in reality a user in a network is likely to face unsecure channels and routers operating with known protocols, such as in the case of Wi-Fi in public areas. This motivates people to understand the effect of an untrusted relay on cooperative communications secrecy. Interestingly, it has been shown in [14], [15] that non-zero secrecy rates can be achieved in one-way and two-way relaying with an untrusted relay. Furthermore, the authors in [16] derived the secrecy rate regions of two-way wiretap channels. However, to the best of our knowledge, little progress on multiway relaying with an untrusted relay has been reported so far.

The goal of this paper is to study efficient communication mechanisms for a general framework of multiway relaying, termed wireless MIMO switching [17]. The traffic pattern considered in this framework is arbitrary unicast, where each user in the network transmits one message and intends to...
receive exactly one message from one other user. The model is of practical importance since any traffic demand in multiway relaying can be realized by scheduling multiple unicast traffic flows. Compared with [17], a major difference of this work is to allow multiplexing for every user, i.e., to deploy multiple antennas at each user node, instead of only at the relay. As such, signal space alignment plays an indispensable role in the system design for the considered network.

In this paper, we focus on analyzing the DoF of MIMO switching with a trusted relay and the secrecy DoF of the same network but with an untrusted relay. Specifically, we characterize a unicast pattern by borrowing the notion of *orbit* from abstract algebra [18], where an orbit consists of a minimum subset of users such that every user in the subset exchanges information with one other user still in this subset. Based on that, we establish the DoF capacity of MIMO switching with one and two orbits. Furthermore, we consider an untrusted relay and establish the secrecy DoF capacity of MIMO switching with one-orbit/two-orbit unicast. For this, we first derive an achievable lower bound of the secrecy DoF by assuming a non-regenerative relay; then, we develop a genie-aided upper bound by proposing a novel technique, in which the relay node is split into an uplink part and a downlink part, and genie signals are provided to the downlink part without affecting the secrecy requirement on the uplink part. We show that these two bounds coincide and therefore yield the secrecy DoF capacity that amounts to the DoF capacity (with a trusted relay) subtracting the DoF capacity achieved the relay. Our results build a bridge between the DoF and the secrecy DoF in multiway relaying. The methodology of the proof can be generally used to analyze the secrecy DoF in other relay networks.

**II. SYSTEM DESCRIPTION**

**A. System Model**

Consider a MIMO multiway relaying network in which $K_{\text{total}}$ users exchange information via the help of a multi-antenna relay. A symmetric MIMO setup is assumed, i.e., each user has $M$ antennas, and the relay has $N$ antennas. We assume that there is no direct link between any two users, and all information exchanges go through the relay. Half-duplex is assumed throughout this paper, i.e., every node in the network cannot transmit and receive signals simultaneously. Each round of data exchange consists of two phases: one uplink phase and one downlink phase. In the uplink, the users deliver messages, one from each user, to the relay simultaneously. In the downlink, the relay forwards a signal generated from its received signal back to the users. Following the wireless MIMO switching protocol in [17], we focus on unicast data exchange, i.e., in every round of data exchange, each of the $K_{\text{total}}$ messages is intended for exactly one user, and each user only has one of the intended messages to transmit. It is worth noting that any traffic demand in multiway relaying including unicast, multicast, broadcast, and any of their combinations, can be accomplished by scheduling multiple unicast patterns.

The data exchange for a unicast pattern is defined by a permutation matrix. To be specific, let $P$ be a permutation matrix (which is obtained by reordering the columns of an identity matrix). Each column of $P$ only contains one nonzero entry (which is “1”). Let $P_{ij}$ be the $(i, j)$th element of $P$. Then, $P_{ij} = 1$ means that the message user $j$ is intended for user $i$. Equivalently, we can also use $\pi(\cdot)$ to denote the permutation, i.e., $i = \pi(j)$. Note that the diagonal elements of such a permutation are all zeros, implying that the message sent by a user is distinct from the message desired by this user. In general, this permutation determines a natural partition of the user set $\mathcal{U}$ into subsets, where any two users, denoted by $a$ and $b$, belong to a common subset if and only if $b = \pi^n(a)$ for some $n \in \mathbb{Z}$. In abstract algebra, a subset defined in this way is referred to as an *orbit* [18]. Without loss of generality, we assume that the $K_{\text{total}}$ users are divided into $L$ orbits. Let $K_l$ be the number of users in orbit $l$, where $l \in \mathcal{I}_L = \{1, \ldots, L\}$, and $K_{\text{total}} = K_1 + \ldots + K_L$. The $k$th user in orbit $l$ is denoted by $\mathcal{U}_{lk}$, where $k \in \mathcal{I}_{K_l} \triangleq \{1, \ldots, K_l\}$. The block diagram of a general wireless MIMO switching scheme is depicted in Fig. 1. With appropriate user labeling, the permutation matrix for a unicast can be generally expressed as $P = \text{diag}\{P_1, \ldots, P_L\}$ and thus $P_l$ defines the traffic pattern of orbit $l$. This general unicast model covers both pairwise and non-pairwise data exchange. When $K_l = 2$, pairwise data exchange is performed in orbit $l$. When $K_l > 2$, the users in this orbit conduct non-pairwise data exchange with a traffic-flow circle of length $K_l$.

The channel is modeled as follows. Let $H_{lk} \in \mathbb{C}^{N \times M}$ be the uplink channel matrix from user $\mathcal{U}_{lk}$ to the relay, and $G_{lk}^T \in \mathbb{C}^{M \times N}$ be the downlink channel from the relay to $\mathcal{U}_{lk}$. We assume that $H_{lk}$ and $G_{lk}$ are both full column or row rank, whichever is smaller, with probability one. We also

\[ \text{Fig. 1. Wireless MIMO switching with } L \text{ orbits.} \]
assume that all channel state information is perfectly known to every node, following the convention in [3], [17]. The received signals in the uplink and in the downlink transmission can be respectively written as

\[ Y_R = \sum_{l=1}^{L} \sum_{k=1}^{K_l} H_{lk} X_{lk} + Z_R \quad (1) \]

\[ Y_{lk} = G_{lk}^{R} X_{lk} + Z_{lk}, \quad \forall l \in \mathcal{I}_L, \forall k \in \mathcal{I}_{K_l} \quad (2) \]

where \( X_{lk} \in \mathbb{C}^{M \times n} \) and \( Y_{lk} \in \mathbb{C}^{M \times n} \) are the transmitted and received signals of user \( U_{lk} \), respectively, and \( X_R \in \mathbb{C}^{N \times n} \) and \( Y_R \in \mathbb{C}^{N \times n} \) is the transmitted and received signals at the relay, respectively. Here, \( n \) is the number of channel uses in one transmission, \( \rho \) and received signals of user \( X \), respectively, and

\[ Z \in \mathbb{C}^{M \times n} \] signals in the uplink and in the downlink transmission can be received signals of user \( U \), respectively, and \( X_R \in \mathbb{C}^{N \times n} \) and \( Y_R \in \mathbb{C}^{N \times n} \) is the transmitted and received signals at the relay, respectively. Here, \( n \) is the number of channel uses in one transmission, \( \rho \) and \( \sigma^2 \) is the relay’s noise power. The transmit powers of each user and the relay are upper-bounded by

\[ \frac{1}{n} \text{Tr}[X_{lk}^H X_{lk}] \leq P, \quad \forall l \in \mathcal{I}_L, \forall k \in \mathcal{I}_{K_l} \quad (3) \]

\[ \frac{1}{n} \text{Tr}[X_{R}^H X_{R}] \leq P_R \quad (4) \]

where \( P \) and \( P_R \) are the power budgets per channel use of each user and of the relay, respectively. \( \text{Tr}[\cdot] \) represents the trace of a matrix. Since this paper is concerned with DoF analysis, we always assume \( P = P_R \) for convenience of discussion.

In this network, user \( U_{lk} \) has two messages: a confidential message \( w_{lk} \) and a randomization message \( w_{lk}^r \), which are respectively from two sets of equally likely distributed messages \( W_{lk} = \{1, \ldots, M_{lk} \} \) and \( W_{lk}^r = \{1, \ldots, M_{lk}^r \} \). Let the overall message \( w_{lk} = (w_{lk}^c, w_{lk}^r) \), \( W_{lk} = W_{lk}^c \times W_{lk}^r \),\( M_{lk} = M_{lk}^c M_{lk}^r \), \( w_{S}^c = \{w_{lk}^c\}_{l \in \mathcal{S}} \) as \( w_{S}^r = \{w_{lk}^r\}_{l \in \mathcal{S}} \), \( S \subseteq \mathcal{K} \) where \( \mathcal{K} \) is the set of all users. The message \( w_{lk} \) is encoded by a function, i.e., \( f_{lk}(\cdot) : w_{lk} \rightarrow X_{lk} \in \mathbb{C}^{M \times n} \) for each \( w_{lk} \in W_{lk} \), where \( R_{lk}^c = \frac{1}{n} \log_2 M_{lk}^c \), \( R_{lk}^r = \frac{1}{n} \log_2 M_{lk}^r \) and \( R_{lk} = \frac{1}{n} \log_2 M_{lk} = R_{lk}^c + R_{lk}^r \). The transmit and receive signals of the relay are related as

\[ X_R = g(Y_R) \quad (5) \]

where \( g(\cdot) \) is the relay function.

Denote the decoding function \( d_{\pi_{lk}(k)}(\cdot) \) at user \( U_{\pi_{lk}(k)} \), i.e.,

\[ d_{\pi_{lk}(k)} : Y_{\pi_{lk}(k)} \rightarrow \hat{w}_{lk} = (\hat{w}_{lk}^c, \hat{w}_{lk}^r). \]

The reliability of the transmission of user \( U_{lk} \) is evaluated by the error probability, given by

\[ P_{e,\pi_{lk}(k)} = \frac{1}{\prod_{k \in \mathcal{K}} M_{lk}} \sum_{w_{\mathcal{K}} \in \mathcal{W}_{\mathcal{K}}} \Pr \{ \hat{w}_{lk} \neq w_{lk} | w_{\mathcal{K}} \text{ is sent} \}. \quad (6) \]

B. Achievable Rate and DoF

**Definition 1 (Achievable Rate):** The rate tuple \((R_{11}, \ldots, R_{LK})\) is achievable for wireless MIMO switching, if for any given \( \epsilon > 0 \), there exists a codebook \((n, M_{11}, \ldots, M_{LK})\) satisfying

\[ \frac{1}{n} \log_2 M_{lk} \geq R_{lk} - \epsilon \]

\[ \max \{ P_{e,11}, \ldots, P_{e,LK} \} \leq \epsilon, \quad U_{lk} \in \mathcal{K}. \]

Denote the signal-to-noise ratio \( \rho = \frac{P}{\sigma^2} \). The achievable rate is in general a function of \( \rho \). Then, the overall achievable DoF can be defined as

\[ d_{\text{sum}} = \lim_{\rho \to \infty} \frac{\sum_{l=1}^{L} \sum_{k=1}^{K_l} R_{lk}}{\log_2 \rho}. \quad (9) \]

The achievable DoF per user is defined for fair comparison between the cases with different number of users

\[ d = d_{\text{sum}} / K_{\text{total}}. \quad (10) \]

The maximum of all achievable DoFs is referred to as the DoF capacity, denoted by \( d \).

C. Achievable Secrecy Rate and Secure DoF

We also consider a scenario with an untrusted relay in wireless MIMO switching and analyze the secrecy rate and secrecy DoF of the network. The untrusted relay is a passive eavesdropper, which helps the transmission of the users but it also tries to wiretap the received signals.

The secrecy is defined following [19]. The equivocation at the relay is defined as

\[ \Delta_{\mathcal{K}} = H(W_{\mathcal{K}}^c | Y_R) / H(W_{\mathcal{K}}^c) \]

where \( H(\cdot) \) and \( H(\cdot | \cdot) \) are respectively the entropy and the conditional entropy functions. Then, we say that communication secrecy is guaranteed if \( \Delta_{\mathcal{K}} \) is arbitrarily close to 1 for sufficiently large \( n \). Note that such a definition of secrecy also implies secrecy of any user subset \( S \subseteq \mathcal{K} \) [16], [20].

**Definition 2 (Achievable Secrecy Rates):** The secrecy-rate tuple \((R_{11}, \ldots, R_{LK})\) is achievable for wireless MIMO switching, if for any given \( \epsilon > 0 \), there exists a codebook \((n, M_{11}, \ldots, M_{LK})\), where \( M_{lk} = M_{lk}^c M_{lk}^r \), satisfying

\[ \frac{1}{n} \log_2 M_{lk} \geq R_{lk} - \epsilon \]

\[ \frac{1}{n} \log_2 M_{lk}^r \geq R_{lk}^r - \epsilon \]

\[ \max \{ P_{e,11}, \ldots, P_{e,LK} \} \leq \epsilon, \quad U_{lk} \in \mathcal{K}. \]

\[ \Delta_{\mathcal{K}} \geq 1 - \epsilon \]

where \( P_{e,lk} \) is defined by (6).

The achievable secrecy DoF per user is defined as

\[ d_s = \frac{1}{K_{\text{total}}} \lim_{\rho \to \infty} \frac{\sum_{l=1}^{L} \sum_{k=1}^{K_l} R_{lk}^s}{\log_2 \rho}. \quad (16) \]

The maximum of all achievable secrecy DoFs is called the secrecy DoF capacity, denoted by \( d_s \).
D. Discussions

It is worth noting that some specific settings of the proposed MIMO switching framework have been studied in the literature. For unicast with two users (and a single orbit), wireless MIMO switching reduces to MIMO two-way relaying, with the DoF capacity presented in [9]. More generally, for multi-user two-way relaying (i.e., unicast with multiple two-user orbits), the DoF capacity is reported in [10] for the setup of two and three user-pairs (though without providing the proof). However, the DoF of wireless MIMO switching with an untrusted relay, and establish a closed-form relation between the DoF and the secrecy DoF. Furthermore, we will study the secrecy DoF of wireless MIMO switching with an untrusted relay, and establish a closed-form relation between the DoF and the secrecy DoF.

III. WIRELESS MIMO SWITCHING WITH A TRUSTED RELAY

Consider a trusted relay and analyze the DoF of general wireless MIMO switching. We focus on a symmetric setup that each user delivers an equal amount of messages to one other user. For ease of illustration, we assume that each orbit has an equal number of users $K$ and each orbit is defined by the same permutation $\pi(\cdot)$.\(^6\)

A. Wireless MIMO Switching with One Orbit

We consider the case of one orbit, i.e., $L=1$, with $K$ users and provide the DoF capacity for multi-antenna users setup as follows.

Theorem 1: For $M$-by-$N$ wireless MIMO switching with $L=1$, the DoF per user is given by

$$d = \min\left( M, \frac{N}{K-1} \right).$$

Remark 1: When $K=2$, i.e., two-way relaying, the DoF capacity from Theorem 1 is $d = \min(M,N)$, which is the cut-set bound of two-way relaying.

B. Wireless MIMO Switching with More Orbits

Consider a scenario with more orbits. We can also analyze the achievable DoF and the converse similarly. Due to page limit, we provide an example of two orbits, with the DoF given in Theorem 2.

Theorem 2: For $M$-by-$N$ wireless MIMO switching with $L=2$, the DoF per user is given by

$$d = \begin{cases} 
M, & \frac{M}{N} \in \left(0, \frac{1}{2K-1}\right] \\
N, & \frac{M}{N} \in \left(\frac{1}{2K-1}, 1\right] \\
\frac{2KM}{2K-1}, & \frac{M}{N} \in \left(1, \frac{2K}{K-2K^2}\right] \\
\frac{2K-1}{\frac{N}{2K-2}}, & \frac{M}{N} \in \left(\frac{2K-1}{2K^2}, \infty\right]. 
\end{cases}$$

Remark 2: When $K=2$, i.e., pairwise data exchange within each orbit, the DoF capacity has been previously derived in

\[^6\]The case that different orbits have different numbers of users can be analyzed using the same method proposed in this paper except that the determination of the $\frac{2}{N}$ thresholds is more involved and there may be more turning points in the resulting DoF curve.
which is consistent with the result in (18) by letting $K = 2$.

IV. WIRELESS MIMO SWITCHING WITH AN UNTRUSTED RELAY

We now consider wireless MIMO switching with an untrusted relay. We first present an achievable secrecy sum rate, based on which an achievable secrecy DoF is derived. Then, we develop a genie-aided upper bound on the secrecy DoF, and show that this upper bound can be met in the case of one and two orbits.

A. Achievable Secrecy Sum Rate

In this subsection, we present an achievable secrecy sum rate and an achievable secrecy DoF of wireless MIMO switching by assuming a non-regenerative relay. Let $x_{lk}$ (resp. $y_{lk}$ or $y_R$) be an arbitrary column of $X_{lk}$ (resp. $Y_{lk}$ or $Y_R$). For a non-regenerative relay, the relay function can be expressed in the form of per-channel use as

$$x_R = f(y_R)$$

where $f(\cdot)$ represents the relay function per channel use. Then, we have the following result.

**Theorem 3:** For $M$-by-$N$ wireless MIMO switching with an untrusted relay, the following secrecy sum rate is achievable:

$$R_{\text{sum}}^s = \left[ \sum_{\mathcal{I}_K, \mathcal{I}_K'} I(x_{lk}; y_{\pi(k)} | x_{\pi(k)}) - I(x_K; y_R) \right]^+$$

where $x_K = [x_{11}, \ldots, x_{LK}]$, and $I(x_{lk}; y_{\pi(k)} | x_{\pi(k)})$ is the information rate of user $U_{lk}$ decodable at user $U_{\pi(k)}$ with the self message $x_{\pi(k)}$.

**Remark 3:** For two-way relaying, i.e., $L = 1$ and $K = 2$, the achievable secrecy sum rate is written as

$$R_{\text{TWH}}^s = \left[ I(x_1; y_2 | x_2) + I(x_2; y_1 | x_1) - I(x_1, x_2; y_R) \right]^+.$$  

This secrecy sum rate is used as an optimization objective in two-way relaying in [15].

**Corollary 1:** An achievable secrecy DoF per user of wireless MIMO switching is given by

$$d_s = \left[ \tilde{d} - \frac{N}{LK} \right]^+$$

where $\tilde{d}$ is the achievable DoF per user for the case of a non-regenerative trusted relay, defined as

$$\tilde{d} = \frac{1}{LK} \sum_{\mathcal{I}_K} \frac{I(x_{lk}; y_{\pi(k)} | x_{\pi(k)})}{\log_2 \rho}.$$  

**Proof:** The equality in (22) follows from the fact that $\lim_{\rho \to \infty} \frac{I(x_K; y_R)}{\log_2 \rho} = N$. 

B. Secure DoF Capacity

We now present an upper bound of the secrecy DoF of wireless MIMO switching.

**Theorem 4:** For $M$-by-$N$ wireless MIMO switching, the secrecy DoF per user is upper-bounded by

$$d_s \leq \left[ d - \frac{N}{LK} \right]^+$$

where $d$ is the DoF capacity of the network.

**Proof:** We use a genie-aided approach in the proof. Since the relay is untrusted, genie messages cannot be provided directly to the relay. (Otherwise, the equivocation $\Delta_K$ cannot be made arbitrarily close to 1.) Thus, we separate the relay into two components, which is shown in Fig. 4. The first component is untrusted and can be regarded as a passive eavesdropper. The second component, i.e., the genie-aided relay, does not have the secrecy constraint and thus can be assigned with genie signals. There is a perfect link between the two components to share the knowledge of $Y_R$. Recall that the users transmit the signals $X_K$ to the untrusted relay and the untrusted relay receives $Y_R$. The genie messages $W_S$ are provided to the genie-aided relay to make sure that all messages
are decodable at the genie-aided relay with the knowledge of the genie messages. The genie messages contain one message from each orbit, such as $W_S = [W_{11}, \ldots, W_{LK}]$. For orbit $l$, $\forall n \in I_l$, all other messages can be decoded with the knowledge of $W_{1l}$ following the converse proof of Theorem 1. Therefore, the genie-aided relay has $\{Y_R, W_S\}$. We can see that $X_K \rightarrow \{Y_R, W_S\} \rightarrow Y_R$ forms a Markov chain. From data processing theorem, the Markov chain can be seen as a degraded wiretap channel. Compared to the Wyner’s degraded wiretap channel, all transmit users are presented as Alice with $X_K$, the untrusted relay as Eve with $Y_R$, and the genie-aided relay as Bob with $\{Y_R, W_S\}$. Then, we have

$$n \sum_{l=1}^{L} \sum_{k=1}^{K} R_{lk}^* \leq I(X_K; Y_R, W_S | Y_R)$$

$$= I(X_K; W_S | Y_R)$$

$$= H(X_K | Y_R) - H(X_K | W_S, Y_R)$$

$$= H(X_K | Y_R)$$

$$= H(X_K) - I(X_K; Y_R)$$

where (25) is obtained from (3.25) in [21]. Eq. (28) is due to $H(X_K | W_S, Y_R) = 0$, which is from the Fano’s inequality and the definition of the genie messages $W_S$.

We now consider the DoF. First, by assumption of converse, the messages in $X_K$ are all decodable at their intended receivers. Therefore, $\frac{1}{2} H(X_K)$ gives the sum rate capacity of the network (with a trusted relay), which further implies $\lim_{n, \rho \to \infty} \frac{H(X_K)}{n \log_2 \rho} = L K \bar{d}$. Second, the DoF achieved by the relay is given by $\lim_{n, \rho \to \infty} \frac{I(X_K; Y_R)}{n \log_2 \rho} = \min(LKM, N)$. Therefore,

$$d_s = \lim_{n, \rho \to \infty} \frac{\sum_{l=1}^{L} \sum_{k=1}^{K} R_{lk}^*}{LK \log_2 \rho}$$

$$\leq \left[ \bar{d} - \frac{N}{LK} \right]^\top.$$  

Note that $\bar{d}$ in Corollary 1 is different from $\bar{d}$ in Theorem 4: $\bar{d}$ is an achievable DoF for non-regenerative relay setup; $\bar{d}$ is the DoF capacity of the network with a trusted relay.

**Corollary 2:** For $L = 1$ and $L = 2$, the upper bound given in Theorem 4 is also achievable. That is, the secrecy DoF capacity is $[\bar{d} - \frac{N}{LK}]^\top$ when $L = 1$ and $L = 2$.

Compared to the DoF capacity in Fig. 2 (resp. Fig. 3), we see that the secrecy DoF in Fig. 5 (resp. Fig. 6) is obtained by that in Fig. 2 (resp. Fig. 3) subtracting $\frac{N}{k}$ (resp. $\frac{N}{2K}$). Furthermore, we see that secrecy can be guaranteed only if the antennas of all users are more than that of the relay from Fig. 5 (resp. Fig. 6), i.e., $d_s = 0$ when $\frac{N}{k} \leq \frac{1}{1 - \frac{1}{2K}}$.

**V. CONCLUSIONS**

In this paper, we analyzed DoF and secrecy DoF of wireless MIMO switching with multi-antenna users and a multi-antenna relay. It was revealed that the DoF of the network varies with the uncquit pattern. This result also has the ramification that, when both can be scheduled based on the traffic demand, pairwise data exchange is preferable to non-pairwise data exchange since the former achieves a higher DoF. Further, we derived an achievable secrecy DoF and an upper bound of secrecy DoF for wireless MIMO switching with and untrusted relay. The secrecy DoF capacity for unicast with one and two orbits was established. However, in general, the DoF capacity and the secrecy capacity of wireless MIMO switching remain as a challenging open problem worthy of future endeavor.

**REFERENCES**


