Stemming Downlink Leakage from Training Sequences in Multi-User MIMO Networks

Yunlong Mao
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, China 210023
njucsmyl@163.com

Yuan Zhang
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, China 210023
zhangyuan05@gmail.com

Sheng Zhong[*]
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, China 210023
zhongsheng@nju.edu.cn

ABSTRACT

Multi-User MIMO has attracted much attention due to its significant advantage of increasing the utilization ratio of wireless channels. Recently a serious eavesdropping attack, which exploits the CSI feedback of the FDD system, is discovered in MU-MIMO networks. In this paper, we firstly show a similar eavesdropping attack for the TDD system is also possible by proposing a novel, feasible attack approach. Following it, a malicious user can eavesdrop on other users' downloads by transforming training sequences. To prevent this attack, we propose a secure CSI estimation scheme for instantaneous CSI. Furthermore, we extend this scheme to achieve adaptive security when CSI is relatively statistical. We have implemented our scheme for both uplink and downlink of MU-MIMO and performed a series of experiments. Results show that our secure CSI estimation scheme is highly effective in preventing downlink leakage against malicious users.

CCS Concepts

•Security and privacy → Security protocols; Mobile and wireless security; •Networks → *Mobile networks;*

Keywords

Multi-User MIMO, Channel State Information, Eavesdropping, Physical Security

1. INTRODUCTION

Multiple-Input Multiple-Output (MIMO) system has received much attention from both academia and industry. Lots of applications of MIMO technique have been developed since MIMO emerged. For example, transmitter with multiple antennas can use beamforming to transmit to receiver with multiple antennas to achieve a significant array gain [22]. This is an application of single-user MIMO scenario. On the other hand, transmitter with multiple antennas can serve multiple users in the same time-frequency slot through precoding symbols for each antenna [24]. And this is an application of Multi-User MIMO (MU-MIMO) scenario. With advantage of improving the speed and capacity of networks, MU-MIMO has been standardized in IEEE 802.11ac [25].

To ensure that MU-MIMO can fully utilize spatial potential of wireless channels, two main problems should be considered carefully when a MU-MIMO system is constructed: the multi-user detection problem in uplink and the multi-user interference cancellation problem in downlink [20]. The multi-user detection problem concerns how to demultiplex signals of multiple Mobile Stations (MSs) for the Base Station (BS). The multi-user interference cancellation problem concerns how to maximize received signal strength of each MS. Solutions for these two problems, especially the latter, greatly depend on Channel State Information (CSI) which plays an important role in MU-MIMO because CSI characterizes channel coefficients. With the help of full CSI, the BS can provide reliable services for many MSs concurrently.

There is plenty of work that studies the acquisition of CSI. According to ways in which the BS learns CSI, methods for the acquisition of CSI can be categorized into two types: explicit CSI estimation [32] and implicit CSI estimation [3]. In explicit CSI estimation, pilots or training sequences[1], which are commonly known to MSs and the BS, will be transmitted to MSs from the BS. Then MSs can use received training sequences and original sequences to estimate CSI. When the estimation is done, MSs will feed back their estimated CSI to the BS explicitly. In implicit CSI estimation, commonly known training sequences will be transmitted from MSs to the BS in the contrary. Then the BS will do CSI estimation with received training sequences implicitly. Implicit CSI estimation is usually used in Time-Division Duplex (TDD) systems. Because of the reciprocity of TDD channels, esti-

[*]This work was supported in part by the Jiangsu Province Double Innovation Talent Program and in part by the National Natural Science Foundation of China under Grant NSFC-61300235, Grant NSFC-61321491, Grant NSFC-61402223, and Grant NSFC-61425024. The corresponding author is Sheng Zhong. All authors are with the State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, P.R.China, and with the Computer Science and Technology Department, Nanjing University, Nanjing 210023, P.R. China.

CCS '16, October 24–28, 2016, Vienna, Austria.
© 2016 ACM. ISBN 978-1-4503-4139-4/16/10...$15.00
DOI: http://dx.doi.org/10.1145/2976749.2978412

[1]There is no significant difference between pilots and training sequences for estimating CSI in principle. To keep succinct, we will use training sequence to refer the material for estimating CSI.

mation of CSI at transmitting end can be done by implicit CSI estimation in a single pass of training sequences.

Recently, a serious eavesdropping attack on downlink of MU-MIMO with explicit CSI estimation is proposed [33]. In this attack, the attacker feeds back forged CSI to the BS so that the victim's downlink signal at the attacker's receiver will not be a total cancellation. The attacker's received signal will be a mixture of the attacker's download and the victim's download. With a careful selection of forged CSI, the attacker will be able to extract the victim's downlink content. This eavesdropping attack has been proved feasible in explicit CSI estimation. However, there is no evidence for the possibility of this attack in implicit CSI estimation.

In fact, this eavesdropping attack cannot be easily performed in implicit CSI estimation because the biggest difference between implicit CSI estimation and explicit CSI estimation is that there is no explicit CSI feedback in implicit CSI estimation. To our best knowledge, our work in this paper is the first attempt to launch the eavesdropping attack on the downlink of MU-MIMO with implicit CSI estimation. The gist of our approach is as follows. Same as that in [33], the attacker in our approach also keeps eavesdropping on the BS. In this way, the attacker will get every bit of information from MSs to the BS. Because training sequences are commonly known, the attacker is able to do estimation of the victim's CSI with received training sequences at the BS. Then a careful selection of forged CSI $\boldsymbol{H}_1$ is calculated. With his own CSI $\boldsymbol{H}_2$, the attacker can calculate the difference between $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$. Based on this difference, the attacker will transform his training sequence to mislead the BS. When the BS estimates the attacker's CSI, it believes that the received training sequences are commonly known ones. Then the difference coefficient hidden in transformed training sequence will be transferred to the attacker's CSI. However, the BS regards the attacker's CSI as correct and do the precoding as usual. In this way, received signal of the attacker will be a mixture of his download and the victim's download. Because of the selection of forged CSI, the attacker will be able to extract the victim's downlink content.

We note that it is quite challenging to stem this downlink leakage. First, this eavesdropping attack in implicit CSI estimation is difficult to be identified, since there is no evidence of the transforming of training sequences for the BS to tell whether his received training sequences are original ones. Second, there is a conflict in protecting CSI estimation, where CSI and training sequences should be available to the BS but should not be available to other MSs even in the situation in which the BS may be eavesdropped on. Third, when CSI has not been estimated in TDD systems, we cannot assume that a reliable uplink is available as the case in Frequency-Division Duplex (FDD) system because of the reciprocity of channel. This means, if we assume that reliable uplink is available before doing estimation, we are assuming reliable downlink at the same time. Fourth, complex cryptographic tools cannot be adapted. Construction of secure communication or secure key exchanging in unstable transmitting is too inefficient for estimation phase. Masking or confusing techniques cannot be adapted because training sequences and CSI need to be as accurate as possible.

With overcoming these challenges, we have proposed a secure CSI estimation scheme for TDD systems. We observe that it is very hard to keep MSs' historical CSI secret, so we trade outdated CSI records off for the security of current CSI estimation. Our secure CSI estimation is designed to be a two-phase scheme, in which uplink and downlink will be carefully designed. The first phase is for the BS to collect commitments of training sequences from MSs, which should happen in the previous coherence interval before expected downlink interval. A fuzzy commitment scheme [16] is employed to generate commitments of training sequences for MSs, which can help the BS ensure that when the BS does CSI estimation, MSs will use exactly the same sequences as they have committed. The first phase mainly involves uplink of MSs. This phase can be regarded as a process of multi-user detection in conventional uplink schemes. The second phase should happen in expected coherence interval. In the beginning of the second phase, MSs should reveal their training sequences to the BS. Then the BS will verify whether these training sequences can match those that have been committed before. If the training sequence of any MS is legal, the BS will recover the original training sequence from the MS's commitments and estimates this MS's CSI with the original training sequence and received training sequence.

The above countermeasure is based on the observation that instantaneous CSI is changing significantly. Therefore we can make use of the timeliness of CSI to ensure that current CSI is secure against attackers. But there may be relatively statistical CSI cases which should be also taken into consideration. To this end, we extend our secure CSI estimation scheme to achieve adaptive security in relatively statistical CSI case. Adaptive security here means that varying degree of security can be achieved according to the selection of security parameter. If a security threshold is determined, then varying degree of resources will be expended according to the statistical degree of CSI.

Our major contribution in this paper can be summarized as follows:

- A feasible approach is proposed to make eavesdropping attack happen in downlink of MU-MIMO with implicit CSI estimation. To our best knowledge, this is the first study for this situation. We verify this approach in a TDD MU-MIMO network.

- We propose a secure CSI estimation scheme which takes advantage of the timeliness of instantaneous CSI. Solutions for both uplink and downlink of MU-MIMO have been given to implement our scheme.

- In case that CSI is relatively statistical, an adaptive security approach is proposed. This approach is integrated into our scheme to ensure security with varying cost according to the statistical degree of CSI.

2. RELATED WORK

MU-MIMO systems have attracted more and more attention since it emerged. A lot of work has been done during recent years. Some techniques which are essential components supporting MU-MIMO systems are growing mature. For uplink, both the multi-user detection problem and simultaneous upload problem have been carefully studied. Minimum mean square error method and maximum likelihood method have been proved efficient in multi-user detection [14, 20]. Many uplink protocols have been proposed for MU-MIMO. Some of them are designed to contend for channels without coordination [23, 30, 21]. This kind of methods is easy to establish, and flexible to use. Some other methods are designed to use uplink with coordinated access [13, 31, 19]. This kind of methods usually has higher utility of channels, but the prerequisite is that full CSI of users must be available. As for downlink of MU-MIMO, block-diagonalization and zero-forcing are two most popular methods [29]. Although dirty paper coding [9] has been proved to have optimal performance, its computing complexity is too high to be used in reality.

No matter what protocol is used to build download links, full CSI is needed if a highly reliable transmitting is to be acquired. To obtain CSI within small delay for transmitting, lots of subtle estimation schemes are proposed. Among them, a training sequence based approach [6] has gained much favor. A robust training sequence has also been proposed [27] for correlated MIMO channel. According to feedback styles, CSI estimation schemes can be classified into explicit CSI estimation and implicit CSI estimation, both of which have been well studied and widely applied. Explicit CSI estimation is usually employed in frequency-division duplex systems. Since explicit feedback of CSI is needed, an efficient feedback scheme is indispensible. Many efficient feedback schemes and training techniques have been proposed, such as [32, 28, 8]. Implicit CSI estimation has an advantage of single-pass training form. This can be used with reciprocity characteristic of time-duplex division systems to shape a complete CSI estimation scheme [3, 18] for both transmitters and receivers in TDD mode.

Although much work about CSI estimation has been done, only a small part studies the security of CSI. It is commonly agreed that CSI should be fed or learnt in plain text. But recently a serious eavesdropping attack has been proved to be practicable in MU-MIMO system even with protection of artificial noise [33]. This attack can threaten users' download if CSI is available to the attacker. The attack will be able to extract the victim's downloading message if forged CSI is reported to the BS. This attack is proposed and proved in explicit CSI estimation with FDD mode. In implicit CSI estimation, this kind of attack will be inapplicable because CSI is not explicitly reported. In this paper, we will show a feasible approach to launch the eavesdropping attack in implicit CSI estimation. Different with prior work [33], we will launch this attack by misleading the BS with the fraudulent training sequence instead of forging a CSI report. And before this our work, there has been no effective method to identify this attack in implicit CSI estimation.

3. PRELIMINARIES

We will focus on the leakage of downlink in a single-cell MU-MIMO TDD system in this paper. We note that the biggest difference between the TDD system and FDD system is that the TDD system uses the reciprocity of channels for transmitters and receivers. This is also the main factor that makes secure CSI estimation in TDD systems difficult to be achieved. In the favor of TDD systems, we use implicit CSI estimation method as the default setting. Before the introduction of our attack model and proposed scheme, we will review downlink model of MU-MIMO system and implicit CSI estimation first.

3.1 Downlink in MU-MIMO

In this MU-MIMO network, we assumt that the BS uses M antennas to communicate with K single-antenna MSs. As mentioned above, there are two elementary requirements to design MU-MIMO MAC protocols: multi-user detection scheme in uplink and multi-user interference cancellation scheme in downlink [20]. Although dirty paper coding [9] has been proved to be the most effective interference cancellation scheme theoretically, zero-forcing (ZF) is now the most popular scheme in practical use. So we use ZF scheme as the foundation of downlink. The stochastic block-fading channel of downlink between the BS and MSs can be represented by a $K \times M$ matrix:

$$\boldsymbol{H} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1M} \\ h_{21} & h_{22} & \cdots & h_{2M} \\ \vdots & & \ddots & \vdots \\ h_{K1} & h_{K2} & \cdots & h_{KM} \end{bmatrix}, \qquad (1)$$

where $h_{ij}, i \in [1:K], j \in [1:M]$ is the complex coefficient from the j-th antenna of the BS to the i-th MS. According to IEEE 802.11ac standard, download data should be modulated into multiple streams for N subcarriers based on Orthogonal Frequency-Division Multiplexing (OFDM). We should use $\boldsymbol{H}_k$ to denote the channel coefficient on the k-th subcarrier. But to be succinct, we ignore the sign k of subcarrier unless when the statement is in need of specific subcarriers. We use H_i to denote the i-th row of $\boldsymbol{H}$, which characterizes full CSI from the all M antennas of the BS to the i-th MS. In this way, the received signal of MSs in downlink can be represented as:

$$\boldsymbol{Y} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_K \end{bmatrix} = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_K \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_K \end{bmatrix} + \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_K \end{bmatrix} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{z}, \qquad (2)$$

where $\boldsymbol{x} = [x_1, x_2, \ldots, x_K]^T$ is modulated symbols from BS's M antennas, $\boldsymbol{z} = [z_1, z_2, \ldots, z_N]^T$ is the additive white Gaussian noise (AWGN), satisfying $E\{z_i\} = 0, Var\{z_i\} = \sigma^2, i \in [1, K]$. We use H^T to denote transpose of H, and $H^\dagger$ to denote Hermitian transpose of H.

3.2 Channel Estimation

According to ZF scheme, symbols $\boldsymbol{x}$ modulated by the BS should be precoded with inverse matrix of CSI. To obtain full CSI at the transmitter end, MSs should transmit commonly known training sequences on N subcarriers to the BS in the training phase. Assume that all these N subcarriers are orthogonal perfectly. We can denote training symbols of these N subcarriers as a matrix: $\boldsymbol{X} = [X_1, X_2, \ldots, X_N]^T$, where X_i is training symbol of the i-th subcarrier. Note that the length of training symbols should be larger than M. The BS will estimate MSs' CSI with known training sequences $\boldsymbol{X}$ and received training sequences $\boldsymbol{Y}$. In order to calculate the approximation of $\boldsymbol{H}$, minimum mean square error (MMSE) is commonly used. The linear MMSE estimator [5] of $\boldsymbol{H}$ is:

$$\hat{\boldsymbol{H}}_{MMSE} = \boldsymbol{Y}(\boldsymbol{X}^H \boldsymbol{R_H} \boldsymbol{X} + \sigma_0^2 K \boldsymbol{I})^{-1} \boldsymbol{X}^H \boldsymbol{R_H}, \qquad (3)$$

where $R_H = E\{\boldsymbol{H}^H \boldsymbol{H}\}$.

3.3 Fuzzy Commitment Scheme

Fuzzy commitment is usually applied to biometric templates, such as fingerprint authentication system. Since the readings of the same fingerprint are not always identical, biometric templates, as important as passwords, require resilience to small corruptions. Fuzzy commitment was proposed to meet this need. A fuzzy commitment scheme can allow a blob $y = F(b, x)$, where $F()$ represents fuzzy commitment function, x is confidential message, b is blurring parameter, to be opened using any witness x' that is close to x in some appropriate metric, but not necessarily identical to x. There are two main tasks for the fuzzy commitment employed in our scheme: one is to protect MSs' training sequences against malicious users, and the other one is to deal with unreliable channel when MSs reveal commitments. More detailed description and examples of fuzzy scheme can be found in [17].

4. EAVESDROPPING ATTACK BASED ON TRAINING SEQUENCE

To do channel estimation normally, every MS should transmit commonly known training sequence. However, some malicious MS is capable of misleading the BS by transmitting elaborately forged training sequence instead of the benign one. More specifically, the BS will give estimation $\hat{\boldsymbol{H}} \approx \boldsymbol{H}$ when the benign training sequence $\boldsymbol{X}$ is transmitted. If the MS transmits $\Delta\boldsymbol{H}\boldsymbol{X}$ instead, the BS will give estimation $\hat{\boldsymbol{H}} \approx \boldsymbol{H}\Delta\boldsymbol{H}$, since the BS still uses $\boldsymbol{X}$ as expected training sequence. This kind of eavesdropping attack is hard to be identified because the attacker can forge any channel state by transforming his training sequence and the BS has no ability to find out whether CSI is forged or not. The main reason is that conventional CSI estimation is based on the assumption that both the BS and MSs are trusted.

4.1 Threat Model

The BS must be trusted in any scenario, because every effort for physical security will be in vain if the BS is compromised. We do not consider attackers from outside of this MU-MIMO network because the attack that we study here can only be launched inside, because attackers from outside cannot have interactive behavior such as estimating and downloading with the BS. This means our attacker is some MS in the MU-MIMO network. Other kinds of attacks from outside or higher layers are out of our concern. We will focus on physical security of MSs' CSI and downlink.

The attacker in our work is militant, who is able to eavesdrop on the BS to grab all information which is supposed to be received by the BS. Since the training sequences are transmitted in plain text, the attacker can get BS's received training sequences easily. Generally, we assume that the victim is some MS, say MS_1, and the attacker is another MS, say MS_2. MS_1's training sequence received at the BS is also known to MS_2. Then MS_2 can do the same estimation as the BS and obtain CSI of MS_1 in the coherence interval. We assume that all transmitters are physically secure with artificial noise. Our attack will be considered under this secure assumption.

4.2 Transforming of Training Sequence

The attack we investigated is based on the observation that training sequences can be transformed without BS's awareness. For brevity, we will illustrate training sequence based attack in the context of a 2 × 2 MU-MIMO TDD system. The BS uses two antennas to transmit messages to two MSs with single antenna respectively. The setting of this system can be extended to more complicated systems with more antennas. In this 2 × 2 MU-MIMO system, received signals from downlink of two MSs can be written as:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \begin{bmatrix} \sqrt{p_1}s_1 \\ \sqrt{p_2}s_2 \end{bmatrix} + \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}, \qquad (4)$$

where $[C_1, C_2] = [H_1, H_2]^{-1}$ is the precoding matrix that the BS precodes downlink streams according to ZF, $\sqrt{p_1}, \sqrt{p_2}$ are transmitting power of signal, and s_1, s_2 are signals transmitted to MS_1 and MS_2.

Generally, we assume that MS_2 is coveting downlink message s_1 that MS_1 are downloading from the BS. To achieve his attempt, MS_2 first eavesdrops on training sequences that the BS receives from other MSs including MS_1. Then MS_2 estimates MS_1's channel coefficient $\hat{\boldsymbol{H}}_1$. Attacker MS_2 now knows both MS_1's CSI $\hat{\boldsymbol{H}}_1$ and his own CSI $\hat{\boldsymbol{H}}_2$. Then, MS_2 can calculate the difference $\Delta\boldsymbol{H}$ between his channel coefficient and MS_1's channel coefficient:

$$\hat{\boldsymbol{H}}_1 = \hat{\boldsymbol{H}}_2\Delta\boldsymbol{H}. \qquad (5)$$

Since the BS can only estimate MSs' CSI by commonly known training sequences, it is possible for attacker MS_2 to mislead the BS to learn MS_2's CSI by transforming benign training sequence. With CSI difference $\Delta\boldsymbol{H}$ learnt, if MS_2 wants his CSI to be estimated by the BS to be the same as MS_1, MS_2 should transform his training sequence into:

$$\boldsymbol{X}_2^f = \Delta\boldsymbol{H}\boldsymbol{X}_2. \qquad (6)$$

Then this transformed training sequence will be received by the BS as:

$$\boldsymbol{Y}_2^f = \boldsymbol{H}_2\Delta\boldsymbol{H}\boldsymbol{X}_2 + \boldsymbol{z}_2. \qquad (7)$$

The BS will estimate MS_2's CSI as $\hat{\boldsymbol{H}_2}^f$, which will seem like $\hat{\boldsymbol{H}}_1$. Forged CSI $\hat{\boldsymbol{H}_2}^f$ surely is different to MS_1's actual CSI $\boldsymbol{H}_1$. But we should not worry about this, because what we want is to let $\hat{\boldsymbol{H}_2}^f$ looks like $\hat{\boldsymbol{H}}_1$, not $\boldsymbol{H}_1$, in BS's observation. A bound of difference between $\hat{\boldsymbol{H}_2}^f$ and $\hat{\boldsymbol{H}}_1$ is given in Theorem.1, which directly follows a property of MMSE [12].

THEOREM 1 (DIFFERENCE OF CSI). *The difference between forged CSI $\hat{\boldsymbol{H}_2}^f$ and estimated CSI $\hat{\boldsymbol{H}}_1$ can be bounded by $(\frac{2}{X_2\Delta H})^n\sqrt{n!}$.*

PROOF. We regard channels' coefficient of both MS_2 and MS_1 as variable independently. Estimated CSI $\hat{\boldsymbol{H}}_2$ and $\hat{\boldsymbol{H}}_1$ are known to the BS. Transformed training sequence is only corresponding to $\hat{\boldsymbol{H}}_2$ and $\hat{\boldsymbol{H}}_1$. MMSE estimator of this sequence will be:

$$mmse(H_2^f, (X_2\Delta H)^2) = E(H_2^f - EH_2^f|(X_2\Delta H)H_2^f + z_2)^n$$
$$\le (\frac{2}{X_2\Delta H})^n\sqrt{n!}.$$

□

4.3 Eavesdropping Attack

In a trusted MU-MIMO scenario, after having training sequences received from MSs, the BS will estimate MSs' CSI and prepare download for MSs. Having download content precoded with inverse matrix of full CSI by the BS, MSs are supposed to receive their own downlink content. But when there is an attack who covets another MS's downlink content, received content of the attacker will be a mixture of the attacker's download and the victim's download. The attacker must use his own CSI and the victim's CSI to eliminate channel coefficient and precoding matrix. Hence, a big problem for eavesdropping attack is the elimination of interference. To solve this problem, the prerequisite for eavesdropping is acquisition of the victim's CSI, assuming that CSI is in plain text.

Although MS_2 can transform his training sequence to $\boldsymbol{X}_2^f = \Delta \boldsymbol{H} \boldsymbol{X}_2$ to imitate CSI of MS_1, this is not the best choice to eavesdrop on MS_1. When MS_2 fakes his CSI as $\boldsymbol{F}_2 = [F_{21}, F_{22}]$ by the transforming of training sequence $\boldsymbol{X}_2^f$, the download messages of MS_1 and MS_2 from the BS with ZF precoding will be:

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix} \begin{bmatrix} C_1 \\ F_2 \end{bmatrix} \begin{bmatrix} \sqrt{p_1} s_1 \\ \sqrt{p_2} s_2 \end{bmatrix} + \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}. \quad (8)$$

When MS_2 does eavesdropping and downloading at the same time, the downlink content of MS_1 in MS_2's observation will be:

$$\begin{aligned} s_1^{MS_2} &= \frac{(h_{11}f_{22} - f_{21}h_{12})}{\sqrt{p_1}(h_{21}f_{22} - h_{22}f_{21})}(y_2 - \frac{(h_{11}h_{22} - h_{12}h_{21})}{(h_{11}f_{22} - f_{21}h_{12})}\sqrt{p_2}s_2) \\ &= m_1 + \frac{(h_{11}f_{22} - f_{21}h_{12})}{\sqrt{p_1}(h_{21}f_{22} - h_{22}f_{21})} z_2. \end{aligned} \quad (9)$$

As shown in expression of $s_1^{MS_2}$, in order to maximize the attacker's eavesdropping and minimize the interference of his own downloading message, the key is to forge the attacker's CSI. A weighted sum of genuine CSI has been proved to be the best choice [33]. $F_2 = [wh_{11} - h_{12}, wh_{21} - h_{22}]$, where w is a adjustable coefficient. This is the approach proposed by prior work [33] in a FDD system with explicit CSI estimation. We in this paper, make this eavesdropping approach also feasible in a TDD system with implicit CSI estimation by transforming training sequences. To ensure that the BS can learn F_2 as MS_2's CSI, the training sequence of MS_2 should be transformed in the way shown in Equation.6. The received signal at attacker MS_2 contains a mixture of s_1 and s_2. In order to decode m_1 of MS_1, MS_2 should download known message m_2 from a colluded or spurious server [33]. Thus, MS_2 can remove m_2 and his own interference from the received signal. In this way, we can launch this kind of eavesdropping attack in TDD systems, but no existing scheme can prevent it effectively.

5. SECURE ESTIMATION OF INSTANTANEOUS CSI

There are generally two types of CSI: statistical CSI and instantaneous CSI. Statistical CSI usually has strong correlation in space, time and frequency, and can be described by statistical characteristics of the channel. This type of CSI usually has no need to be estimated over time. Thus, we will focus on instantaneous CSI first which needs to be estimated continually. Our secure CSI estimation procedure of MSs is designed to have two phases. The first phase is MSs' generating commitments, which should happen in the previous coherence interval before MS's expected downlink interval. The second phase is revealing commitments, which should happen in the same coherence interval with expected download. As for the BS, commitments of training sequences should be collected in the first phase, and CSI estimation will be done in the second phase. In order to show the difference of CSI in different intervals, we have performed experiments to measure how big the difference can be. The result is shown in Figure.1. It can be seen that difference of CSI is greater when SNR is relatively low. When SNR is high, this difference is still significant.

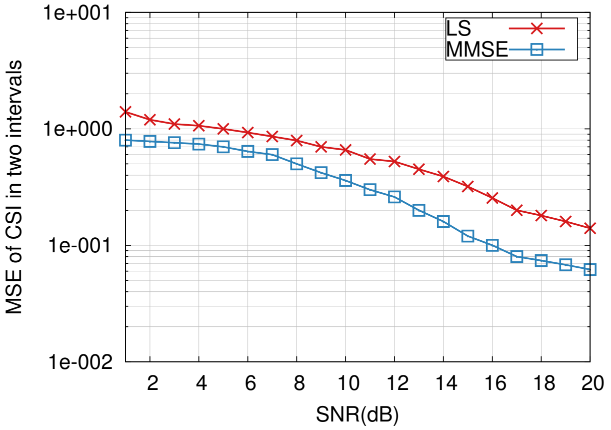

Figure 1: Difference of CSI in two intervals. The difference is measured in MSE.

Specifically, each MS generates a random training sequence in the previous coherence interval just ahead of his expected download. Then each MS makes a commitment of this random training sequence to the BS. The BS will put these MSs, whose commitments have been collected in the first phase, into the scheduling of next interval. When the second phase begins, each MS reveals his commitment of training sequence to the BS. The BS then can do correct estimation of each MS's CSI. An illustration of the two phases is given in Figure.2.

5.1 First Phase: Generating Commitments

Different from FDD systems, when CSI of downlink is unknown in TDD systems, a reliable uplink cannot be assumed because of the reciprocity of TDD channels. Thus, any secure CSI estimation scheme for TDD systems must be constructed from the very beginning of communication, including uplink and downlink. Because of lacking CSI, coordinated uplink access or synchronous uplink transmissions [20] cannot be achieved directly. To be realistic and efficient in establishing communication, we use a spatial multiple access scheme similar with SAM [30]. Then, we will construct our secure downlink scheme based on this uplink scheme to achieve an effective and secure TDD MU-MIMO system.

It is commonly agreed that training sequences should be inserted in data stream of uplink to avoid frequent interruption of continuous download in TDD systems [15, 4]. We do the same in our scheme. But what's different is that we insert the commitment of training sequence for the next co-

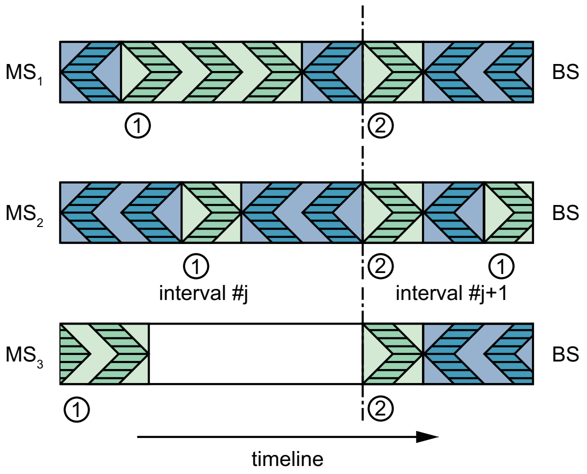

Figure 2: Examples of the relation between two phases. ① represents locations of commitments. ② represents locations of revealing messages.

herence interval in current uplink. This means MSs always commit their training sequences that will be used in the next coherence interval beforehand. MSs will reveal their training sequences in the second phase which is in the next coherence interval. MSs who newly join this MU-MIMO network should wait for an guard interval. Then these new MSs will be able to use their training sequences for CSI estimation at the BS, and start their download process. Different situations have been illustrated in Figure.2.

All MSs that want to transmit to the BS should follow our spatial multiple uplink access scheme. But different from SAM [30], we use a fixed-format package to contain commitments of MSs' training sequences as uplink payload. And we employ a relatively loose time window of uplink channels for MSs. This is due to two reasons: ensuring interval to be larger than safe threshold and guaranteeing the demultiplex of potential transmitters. Without loss of generality, for any user $MS_i, i \in [1, K]$, a random training sequence r_i is generated. Then a linear error correcting code $ECC(n_e, t_e, Enc(), Dec())$ is used to encode r_i, where n_e is the length of codeword, t_e is the error-correcting capability, and $Enc()$ and $Dec()$ are encoding operation and decoding operation respectively. $Enc(r_i)$ will yield corresponding codeword $c_i \in 0, 1^{n_e}$. Without loss of generality, we use Hamming distance to depict difference between r_i and c_i, which will be $\delta_i = r_i \oplus c_i$, where $\oplus$ is XOR operation. But in order to keep readable, we still use numeric plus and minus hereafter. Then the construction of commitment function F is:

$$F(c_i, r_i) = (h(c_i), \delta_i), \tag{10}$$

where $h : \{0, 1\}^{n_e} \to \{0, 1\}^l$ is a secure hash function. This construction follows [16], so our commitment function F meets both binding condition and concealing condition. According to carrier sense multiple access with collision avoidance (CSMA/CA), MS_i will send commitment $(h(c_i), \delta_i)$ to the BS when the backoff timer of MS_i is up. The BS will keep collecting commitments generated by different MSs during time window of the first phase. Algorithm.1 shows summarized construction of commitments in the first phase.

Algorithm 1 Commitment of training sequence

```
for all $MS_i, i \in [1, k]$ do
    generates random training sequence $r_i$,
    chooses codeword $c_i \in C$,
    computes $F(c_i, r_i) = (\alpha_i, \delta_i) = (h(c_i), r_i - c_i)$.
    sends $F(c_i, r_i)$ to the BS.
end for
```

5.2 Second Phase: Revealing Commitments

When the first phase ends, those MSs whose commitments of training sequences have not been collected will not be available candidates in the next coherence interval. These MSs whose commitments have been collected will enter the second phase as soon as the BS broadcasts a *end of first phase* message which is similar to CTS package in RTS/CTS protocol. To leverage fresh CSI as soon as possible, we set time window of the second phase to be compact. So MSs are required to send the revealing message simultaneously once the BS's broadcasting is detected. Synchronous revealing messages are demultiplexed with help of short orthogonal preambles which are allocated to each MS. These revealing messages are the real training sequences that will be used to gain full CSI.

To prevent attackers who replay commitment and revealing message of a target MS to disturb MU-MIMO system, we will do cheating detection after revealing commitments. If replicate training sequences are detected, only the first MS using this sequence will be allowed to the next step according to the timestamp when the BS received these sequences in the second phase. When the BS obtains a revealing message r'_i for any MS MS_i, the BS should check whether the commitment (α_i, δ_i) can be revealed by r'_i. If the revealing message transmitted by MS_i is the same as the training sequence which has been committed, then the following equation will hold:

$$\alpha_i = h(f(r'_i - \delta_i)), \tag{11}$$

where $\alpha_i = h(c_i)$, $\delta_i = r_i - c_i$. If MS_i's commitment can be revealed correctly, then the BS will estimate the CSI using r_i and (r'_i) which are known training sequence and actually received training sequence respectively. Now, the BS can run the same MMSE as usual to calculate approximate CSI. The revealing procedure is shown in Algorithm.2.

Algorithm 2 Revealing commitment

```
for all $MS_i, i \in [1, k]$ do
    if $\alpha_i = h(f(r'_i - \delta_i))$ then
        the BS recovers $r_i = f(r'_i - \delta_i) + \delta_i$,
    end if
end for
for all $r_i, i \in [1, k]$ do
    replicate cheating detection by the BS,
    the BS: $\hat{\boldsymbol{H}} \leftarrow \hat{\boldsymbol{H}}_{MMSE}(r_i, r'_i)$.
end for
```

5.3 Security Analysis

This commitment scheme can protect instantaneous CSI of all MSs perfectly. But every CSI will still be available to the attacker in the end of each interval, because this attacker keeps eavesdropping all information that the BS has.

Although the attacker cannot use this CSI immediately, he can use this as an outdated CSI in the next coherence interval. To guarantee that any message of any MS will be safe, we need a bound of changing of CSI so that attackers can reveal nothing by outdated CSI. To this end, the SNR of received signal should be kept under threshold δ_{snr} when the attacker tries to reveal messages with outdated CSI. Assume that both the BS and attackers can learn perfect CSI $\boldsymbol{H}$ between the BS and MSs so that maximal ratio transmission (MRT) can be achieved. Then the output SNR of MRT with perfect CSI can be given by [10]:

$$\gamma_{MRT} = \lambda_{max}\frac{E_s}{\sigma^2}, \tag{12}$$

where λ_{max} is the largest eigenvalue of $\boldsymbol{H}^{\dagger}\boldsymbol{H}$. If outdated CSI is denoted by $\tilde{\boldsymbol{H}}$ then the changing of CSI is $\delta_{\boldsymbol{H}} = \boldsymbol{H} - \tilde{\boldsymbol{H}}$. Since CSI of every moment can be regarded to follow independent Gaussian distribution, $\delta_{\boldsymbol{H}}$ can be seen as an independent difference following Gaussian distribution with zero-mean and variance σ_d^2. If the attacker uses outdated CSI to reveal other MSs' messages from received signal, the SNR will be associated with $\delta_{\boldsymbol{H}}$ by Theorem.2 which is derived from a existing theorem [7].

Theorem 2 (SNR with outdated CSI). *The SNR of received signal with outdated CSI can be given by:*

$$\gamma_{MRT} = \frac{\tilde{\lambda}_{max}}{(1+\sigma_d^2)(\sigma_d^2 + \frac{(1+\sigma_d^2)\sigma^2}{E_s})}, \tag{13}$$

where $\tilde{\lambda}_{max}$ is the largest eigenvalue of $\tilde{\boldsymbol{H}}^{\dagger}\tilde{\boldsymbol{H}}$, E_s is transmitting energy of data symbol.

If a fixed SNR threshold δ_{snr} is given, then output message with SNR $\gamma_{MRT} \leq \delta_{snr}$ will be regarded as useless, i.e. no information leakage.

Except outdated CSI, preambles which are inserted to cancel frequency offset and to demultiplex MSs' signals may be leveraged by the attacker too. But everything that the attacker can get in the first phase will be outdated in the next coherence interval except for commitments. And the attacker can get nothing from these commitments. As for the second phase, it is too late for the attacker to leverage CSI which is obtained from revealing messages or short orthogonal preambles, because the BS will do zero-forcing with the CSI that the attacker has committed in the first phase.

6. ADAPTIVE SECURITY WITH STATISTICAL CSI

Generally, CSI estimation is used for instantaneous CSI because this kind of CSI keeps varying rapidly. As for statistical CSI scenario, fixed CSI is usually used instead of periodic estimation. But there is always a blurred area where instantaneous CSI may vary not that fast sometimes. Or sometimes instantaneous CSI may also change slowly. Hence, we have also considered the situation where CSI is relatively statistical. Strictly speaking, we will achieve adaptive security for slow-varying CSI when SNR with changing CSI is higher than δ_{snr}. By adaptive security, we mean that varying degree of security can be achieved according to the selection of security parameter. If a security threshold is determined, then varying degree of resources will be expended according to statistical degree of CSI.

Since $\sigma_d^2 \propto (\frac{E_p}{N_0})^{-1}$ [34], where E_p is the pilot symbol energy, according to Theorem.2, it is possible to weaken the energy of training sequences to achieve a lower SNR. But the quality of downlink of MU-MIMO will be disappointing in this way because of inaccurate CSI. The hint of lower SNR can lead to another possible solution: higher Bit Error Rate (BER). This solution sounds like irrational, but we do find out that the attacker's eavesdropping can be thwarted effectively with higher BER of download content. And this BER can be bounded in a reasonable range. In other words, a little higher BER can be traded for more secure downlink. To avoid unnecessary loss of bandwidth, we propose an adaptive security scheme to control BER of downlink to prevent eavesdropping.

Assume that the SNR of current downlink is t_{snr} with CSI $\boldsymbol{H}_t$ of current coherence interval. The attacker's eavesdropping is based on previous CSI $\boldsymbol{H}_p$, so the BS can always use current CSI to calculate how much BER should be added for the next coherence interval. The BER function of QPSK modulation with AWGN can be given by:

$$BER = 1/2erfc(\sqrt{\frac{E_b}{N_0}}), \tag{14}$$

where $\frac{E_b}{N_0}$ is energy per bit to noise power spectral density ratio, $erfc()$ is complementary error function:

$$erfc(x) = 1 - \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt. \tag{15}$$

As for our MU-MIMO system,

$$\begin{aligned}\frac{E_s}{N_0}(dB) &= \frac{E_b}{N_0}(dB) + \log_2(2\log_2(M)),\\ \frac{E_s}{N_0}(dB) &= 10\log_{10}(\frac{T_{symbol}}{T_{sampling}}) + SNR(dB).\end{aligned} \tag{16}$$

Then we can calculate the compensation of SNR that is needed to achieve δ_{snr}:

$$10\log_{10}\frac{\delta_{snr}}{t_{snr}} = (\frac{E_b}{N_0})_{\delta}(dB) - (\frac{E_b}{N_0})_t(dB), \tag{17}$$

where $(\frac{E_b}{N_0})_{\delta}$ is corresponding to δ_{snr}, so $(\frac{E_b}{N_0})_t$ can be calculated in Equation.17. Then Equation.14 and 15 are used to calculate necessary BER δ_{ber} which should be added to downlink of each MS.

A more intuitive explanation for our adaptive security scheme is here. Recall that a mixture of s_1 and s_2 is received when attacker MS_2 is eavesdropping on MS_1. The extraction of s_1 is based on not only full CSI but also the known content of s_2. When additional BER is introduced to downlink of each MS, both s_1 and s_2 will be less precise. When MS_2 tries to extract s_1 as shown in Equation.9, introduced BER will be cumulated. In this way, a low SNR will be achieved. If the BS calculates the compensation of SNR in each interval, then only necessary BER should be added to downlink of each MS. We can integrate this adaptive security scheme into our secure estimation scheme easily, because when SNR is higher than δ_{snr}, no additional BER is needed, which means no loss of bandwidth in instantaneous CSI situation. Algorithm.3 shows the detailed procedure after the integration of two schemes.

Algorithm 3 Secure estimation for arbitrary CSI

```
for all $MS_i, i \in [1, k]$ do
    $MS_i$ generates random training sequence $r_i$,
    $MS_i$ chooses codeword $c_i \in C$,
    $MS_i$ computes $F(c_i, r_i) = (\alpha_i, \delta_i) = (h(c_i), r_i - c_i)$.
    $MS_i$ sends $F(c_i, r_i)$ to the BS.
end for
for all $MS_i, i \in [1, k]$ do
    if $\alpha_i = h(f(r'_i - \delta_i))$ then
        the BS recover $r_i = f(r'_i - \delta_i) + \delta_i$,
    end if
end for
for all $r_i, i \in [1, k]$ do
    the BS does replicate cheating detection,
    the BS: $\hat{\boldsymbol{H}} \leftarrow \hat{\boldsymbol{H}}_{MMSE}(r_i, r'_i)$.
end for
the BS calculates the compensation of SNR with previous $t_{snr}$.
if $\delta_{snr} < t_{snr}$ then
    the BS calculates necessary BER $\delta_{ber}$ which should be introduced to downlink of each MS.
    introduce $\delta_{ber}$ by flipping bits or decreasing $E_b$.
end if
```

7. IMPLEMENTATION AND EXPERIMENTS

We have introduced our scheme in abstract construction theoretically. In this part, we will give one kind of implementation with state-of-the-art techniques. Some part which has been introduced in previous sections will also be reviewed for the completeness of reference. Then we will introduce our experimental implementation with GNU Radio and Universal Software Radio Peripheral (USRP). In the final subsection, numerical results of our scheme will be discussed.

When we construct uplink of MU-MIMO, we use a spatial multiple access scheme similar with SAM [30]. The core idea is to monitor any other MSs' upload frame and ensure that preambles of any two MSs are not overlapping. In the payload of uplink, a customized packet is employed to convey commitment of training sequences. This customized packet is easy to parse. There are two elements within this packet, one is the hash of codeword, and the other one is distance between codeword and training sequence. Both elements are within fixed length. Except for extra payload length, this packet will cause no interference to original content. We choose SHA-256 as secure hash function $h()$, and a low-density parity-check code [11, 26] (LDPC) is used as $ECC()$ for commitment scheme. Downlink construction is straightforward. After MSs' commitments are revealed, CSI will be estimated by MMSE method. Then the BS can do ZF precoding with full CSI in the same way as other normal MU-MIMO downlink [29].

7.1 Experiments

We have implemented secure CSI estimation in the MU-MIMO TDD system with the help of Gnu Radio [1] and USRP [2]. We use 8 USRP N210 to construct the BS with 8 antennas. And each MS is functioned with single USRP N210. An OctoClock-G is used to feed synchronized 10MHz clock and 1 PPS reference to the BS. Data of each USRP N210 is transmitted through Gigabyte cable to a computer for analysis. Figure.3 shows a demo of the BS and MSs.

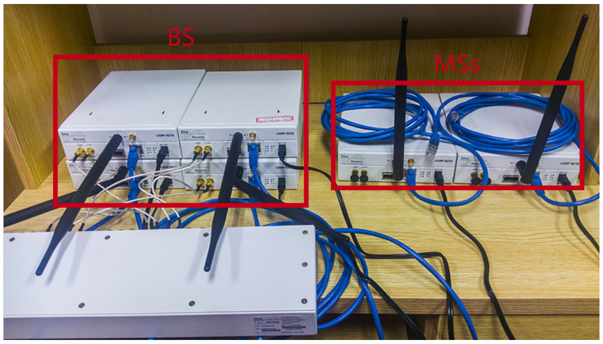

Figure 3: Demo of the BS and MSs. This BS is constructed with 4 USRP N210. Two MSs are ready to be deployed in other place with laptop connected respectively.

Gnu Radio v-3.7.9 is used to build up our MU-MIMO scheme. Original OFDM modules of Gnu Radio will be modified. Some new modules are added to run proposed secure CSI estimation. Primary modules which are needed for BS's transmitter are shown in Figure.4, including modules that have been modified or added.

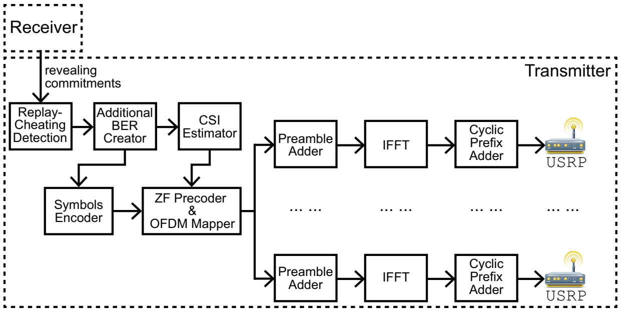

Figure 4: Primary modules for BS's transmitters.

7.2 Numerical Results

In order to verify the feasibility of our secure CSI estimation, we compare the information leakage of downlink with secure estimation and downlink without it. We use the BER of eavesdropping download to measure the information leakage of the victim. Our eavesdropping attack uses a heuristic selection of forged CSI [33] as reference, where attacker MS_2's CSI should be forged to be $w\boldsymbol{H}_1 - \boldsymbol{H}_2$. As for our attack model, we use this forged CSI to calculate corresponding ΔH. Hence, the result of eavesdropping will depend on the selection of weighting parameter w. Results of eavesdropping are shown in Figure.5. An appreciable eavesdropping can be achieved in unprotected downlink when w is about 1.1. Downlink with secure CSI estimation can avoid this low BER eavesdropping by disturbing the attacker's selection of forged training sequence. In secure CSI estimation scenario, we use previous CSI to extract the victim's download. The BER is so high that the attacker cannot extract precise downloading content of the victim.

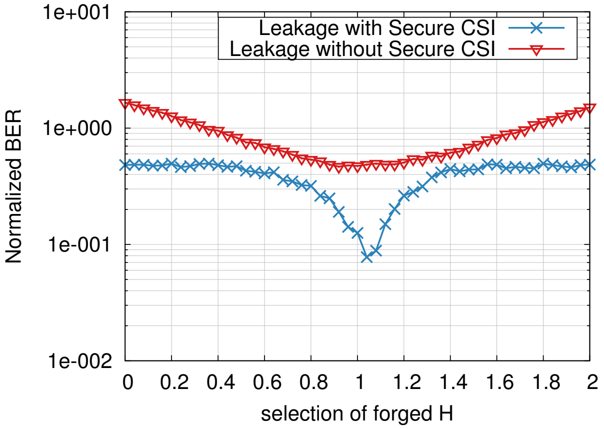

Figure 5: Eavesdropping results of downlink with secure CSI estimation and downlink without secure CSI estimation.

When the changing of instantaneous CSI is relatively slow, our adaptive security scheme will do its job. When the adaptive security is working, additional bit errors will be introduced. Definitely, additional bit errors will effect valid bandwidth, but results in Figure.6 show that loss ratio of bandwidth will decrease significantly when SNR threshold δ_{snr} is low. If we choose $\delta_{snr} = 2$ which is small enough for protection, loss of bandwidth will be lower than 10% even in the condition where CSI MSE equals 10^{-3}. When CSI MSE of two adjacent intervals keeps lower than 10^{-3} with MMSE method, we think this situation can be regarded as a statistical CSI case where statistical characterization should be used instead of CSI estimation.

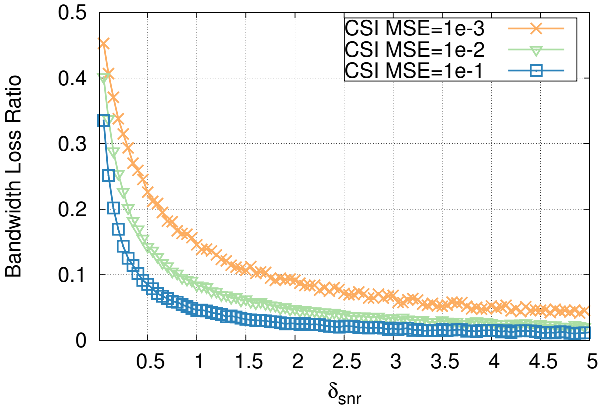

Figure 6: Loss ratio of bandwidth, which is calculated by (loss of bandwidth)/(total bandwidth), decreases significantly when δ_{snr} is low. Results are calculated for single MS.

Recall that we have modified the uplink in the first phase. Transmission of commitments of training sequences cannot be negligible. Since commitments are always transmitted with users' payload of uplink, capacity ratio of uplink can be effected by the occupancy of commitments. In our implementation, we use short training sequence which is randomly generated and the commitment of training sequence is always put in the first symbol of of frames for every subcarrier. We have measured the capacity ratio of uplinks between all MSs and the BS. As shown in Figure.7, the capacity ratio of net payload will reach a nearly saturation if net payload of each MS keeps increasing. It is reasonable that the more MSs there are, the more quickly the capacity ratio will approach to 1.0. But even there is only one MS in the network, the capacity ratio can still approach to 60% with 1Kbits net payload.

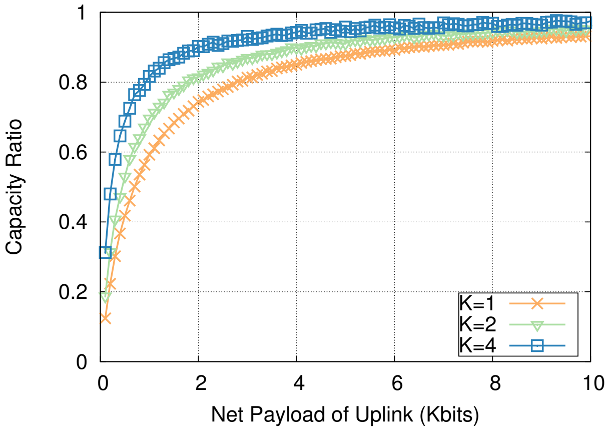

Figure 7: Capacity ratio is calculated by (capacity of commitments)/(total capacity) for all MSs.

With secure CSI estimation and adaptive security employed, results of the experiments can prove the feasibility of our scheme. Besides, downlink rate of MU-MIMO is an important evaluation. To find out how much downlink rate can be achieved with our secure CSI estimation and adaptive security employed, we have measured downlink rates with conditions of different SNR threshold δ_{snr}. Results are shown in Figure.8. SNR threshold δ_{snr} has significant effect on downlink rate, because of the loss of bandwidth which is introduced by adaptive security. Results are following a similar pattern in scenarios of different amounts of MSs. If δ_{snr} is set to be 2 as recommended in the discussion of bandwidth loss, a downlink rate of 10bits per symbol per Hz can be achieved even there is only one MS in the network.

Last but not least, we have measured the overhead of computation in CPU cycles. In the first phase, almost all work is done by MSs in the previous interval, which means MSs can do commitments' computation while downloading or waiting. Thus we will focus on the overhead of BS's computation. Figure.9 shows results of the overhead of computation for two main procedures of second phase: revealing commitments and applying adaptive security. Revealing commitments of training sequences takes most of the overhead. Although the overhead of revealing commitments increases in a nearly linear tendency, the order of magnitude of CPU cycles will keep in 10^3 unless there are about 10^3 MSs, computation can be done in microseconds by a CPU clocked in GHz. This means the overhead introduced by our scheme is acceptable.

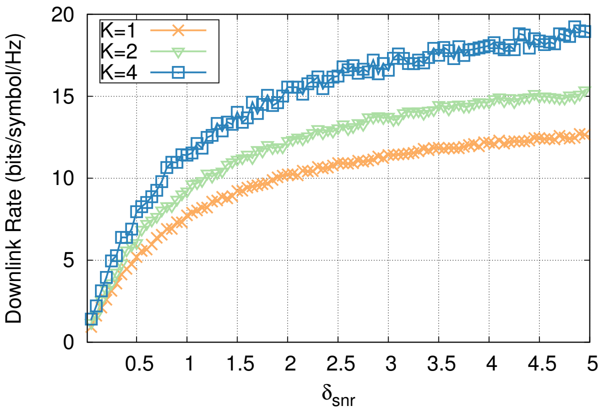

Figure 8: Download Rates of different SNR threshold δ_{snr} are measured for total download links between all MSs and the BS.

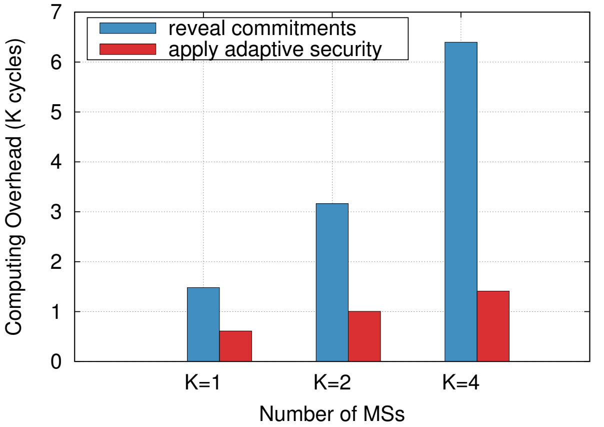

Figure 9: Overhead of computation for two main procedures of second phase are measured for different K.

8. CONCLUSIONS

In this paper, we have proposed a feasible approach to launch a serious eavesdropping attack, which is recently proposed for explicit CSI estimation, in MU-MIMO network with implicit CSI estimation method. Based on the transforming of training sequences, we successfully make eavesdropping attack possible in implicit CSI estimation. Our countermeasure is two-fold. First, we design our secure CSI estimation scheme for instantaneous CSI, which will change significantly along with time being. With the help of fuzzy commitment scheme, our countermeasure can effectively stop the attacker from eavesdropping.

Then, considering the situation where CSI may change slowly, we integrate an adaptive security approach to our scheme. This approach can guarantee users' security in different CSI changing scenarios. Additional bits error will be calculated and introduced dynamically according to current condition of CSI. Our scheme will cause extra overhead and bandwidth loss to MU-MIMO network, which, however, are shown to be acceptable even in some undesirable conditions.

9. REFERENCES

[1] Gnu radio. http://gnuradio.org/redmine/projects/gnuradio/wiki, 2016.

[2] Usrp. https://www.ettus.com/, 2016.

[3] R. Abu-alhiga and H. Haas. Implicit pilot-borne interference feedback for multiuser mimo tdd systems. In *2008 IEEE 10th International Symposium on Spread Spectrum Techniques and Applications*, pages 334–338, Aug 2008.

[4] K. Appaiah, A. Ashikhmin, and T. L. Marzetta. Pilot contamination reduction in multi-user tdd systems. In *Communications (ICC), 2010 IEEE International Conference on*, pages 1–5, May 2010.

[5] M. Biguesh and A. Gershman. Training-based mimo channel estimation: a study of estimator tradeoffs and optimal training signals. *Signal Processing, IEEE Transactions on*, 54(3):884–893, March 2006.

[6] M. Biguesh and A. B. Gershman. Training-based mimo channel estimation: a study of estimator tradeoffs and optimal training signals. *IEEE Transactions on Signal Processing*, 54(3):884–893, March 2006.

[7] Y. Chen and C. Tellambura. Performance analysis of maximum ratio transmission with imperfect channel estimation. *IEEE Communications Letters*, 9(4):322–324, April 2005.

[8] J. Choi, D. J. Love, and P. Bidigare. Downlink training techniques for fdd massive mimo systems: Open-loop and closed-loop training with memory. *IEEE Journal of Selected Topics in Signal Processing*, 8(5):802–814, Oct 2014.

[9] M. Costa. Writing on dirty paper (corresp.). *IEEE Transactions on Information Theory*, 29(3):439–441, May 1983.

[10] P. A. Dighe, R. K. Mallik, and S. S. Jamuar. Analysis of transmit-receive diversity in rayleigh fading. *IEEE Transactions on Communications*, 51(4):694–703, April 2003.

[11] R. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, 8(1):21–28, January 1962.

[12] D. Guo, Y. Wu, S. S. Shitz, and S. Verdu. Estimation in gaussian noise: Properties of the minimum mean-square error. *IEEE Transactions on Information Theory*, 57(4):2371–2385, April 2011.

[13] W. L. Huang, K. B. Letaief, and Y. J. Zhang. Joint channel state based random access and adaptive modulation in wireless lans with multi-packet reception. *IEEE Transactions on Wireless Communications*, 7(11):4185–4197, November 2008.

[14] M. Jiang and L. Hanzo. Multiuser mimo-ofdm for next-generation wireless systems. *Proceedings of the IEEE*, 95(7):1430–1469, July 2007.

[15] J. Jose, A. Ashikhmin, P. Whiting, and S. Vishwanath. Scheduling and pre-conditioning in multi-user mimo tdd systems. In *2008 IEEE International Conference on Communications*, pages 4100–4105, May 2008.

[16] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, CCS '99, pages 28–36. ACM, 1999.

[17] E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, and R. N. J. Veldhuis. Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *IEEE Transactions on Information Forensics and Security*, 6(1):107–121, March 2011.

[18] M. Kobayashi, N. Jindal, and G. Caire. Training and feedback optimization for multiuser mimo downlink. *IEEE Transactions on Communications*, 59(8):2228–2240, August 2011.

[19] H. Li, K. Wu, Q. Zhang, and L. M. Ni. Cuts: Improving channel utilization in both time and spatial domain in wlans. *IEEE Transactions on Parallel and Distributed Systems*, 25(6):1413–1423, June 2014.

[20] R. Liao, B. Bellalta, M. Oliver, and Z. Niu. Mu-mimo mac protocols for wireless local area networks: A survey. *IEEE Communications Surveys Tutorials*, 18(1):162–183, 2016.

[21] T. H. Lin and H. T. Kung. Concurrent channel access and estimation for scalable multiuser mimo networking. In *INFOCOM, 2013 Proceedings IEEE*, pages 140–144, April 2013.

[22] B. Mondal and R. W. H. Jr. Performance analysis of quantized beamforming mimo systems. *IEEE Transactions on Signal Processing*, 54(12):4753–4766, Dec 2006.

[23] A. Mukhopadhyay, N. B. Mehta, and V. Srinivasan. Acknowledgement-aware mpr mac protocol for distributed wlans: Design and analysis. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 5087–5092, Dec 2012.

[24] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta. Massive mu-mimo downlink tdd systems with linear precoding and downlink pilots. In *Communication, Control, and Computing (Allerton), 2013 51st Annual Allerton Conference on*, pages 293–298, Oct 2013.

[25] E. H. Ong, J. Kneckt, O. Alanen, Z. Chang, T. Huovinen, and T. NihtilÃd'. Ieee 802.11ac: Enhancements for very high throughput wlans. In *2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 849–853, Sept 2011.

[26] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke. Design of capacity-approaching irregular low-density parity-check codes. *IEEE Transactions on Information Theory*, 47(2):619–637, Feb 2001.

[27] N. Shariati, J. Wang, and M. Bengtsson. Robust training sequence design for correlated mimo channel estimation. *IEEE Transactions on Signal Processing*, 62(1):107–120, Jan 2014.

[28] H. Shirani-Mehr, D. N. Liu, and G. Caire. Channel state prediction, feedback and scheduling for a multiuser mimo-ofdm downlink. In *2008 42nd Asilomar Conference on Signals, Systems and Computers*, pages 136–140, Oct 2008.

[29] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt. Zero-forcing methods for downlink spatial multiplexing in multiuser mimo channels. *IEEE Transactions on Signal Processing*, 52(2):461–471, Feb 2004.

[30] K. Tan, H. Liu, J. Fang, W. Wang, J. Zhang, M. Chen, and G. M. Voelker. Sam: Enabling practical spatial multiple access in wireless lan. In *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, MobiCom '09, pages 49–60. ACM, 2009.

[31] T. Tandai, H. Mori, K. Toshimitsu, and T. Kobayashi. An efficient uplink multiuser mimo protocol in ieee 802.11 wlans. In *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1153–1157, Sept 2009.

[32] P. Ting, C. K. Wen, and J. T. Chen. An efficient csi feedback scheme for mimo-ofdm wireless systems. *IEEE Transactions on Wireless Communications*, 6(6):2012–2015, June 2007.

[33] Y.-C. Tung, S. Han, D. Chen, and K. G. Shin. Vulnerability and protection of channel state information in multiuser mimo networks. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 775–786, 2014.

[34] H. Viswanathan and J. Balakrishnan. Space-time signaling for high data rates in edge. *IEEE Transactions on Vehicular Technology*, 51(6):1522–1533, Nov 2002.