On User Selective Eavesdropping Attacks in MU-MIMO: CSI Forgery and Countermeasure

Sulei Wang[1], Zhe Chen[2], Yuedong Xu[1], Qiben Yan[3], Chongbin Xu[1], Xin Wang[1]
[1]School of Information Science and Technology, Fudan University, Shanghai, China
[2]School of Computer Science and Engineering, Nanyang Technological University, Singapore
[3]Department of Computer Science and Engineering, University of Nebraska-Lincoln, Lincole, NE, USA
{wangsl16, zhechen13, ydxu, chbinxu, xwang11}@fudan.edu.cn, yan@unl.edu

***Abstract*—Multiuser MIMO (MU-MIMO) empowers access points (APs) with multiple antennas to transmit multiple data streams concurrently to users by exploiting spatial multiplexing. In MU-MIMO, users need to estimate channel state information (CSI) and report it to APs, thus opening a backdoor to attackers who may forge CSI to eavesdrop the content of victims. In this paper, we explore the eavesdropping attack in a novel and practical context in which CSI forgery entangles MU-MIMO user selection in a many-users regime. The attacker hopes to optimize both the eavesdropping opportunity of being selected with the victim and the corresponding decoding quality. We propose new attack and defense mechanisms: (1) *USE Attack* that enables attackers to achieve near optimal eavesdropping opportunity and high decoding quality through constructing orthogonal CSI against victims followed by stepwise refinements; (2) *AngleSec* that exploits channel reciprocity for attacker detection without any modification to legacy CSI feedback in which CSI forgery induces a mismatching of downlink and uplink angular spectra at the AP. We implement and evaluate *USE Attack* and *AngleSec* in a software defined radio platform WARPv3. Extensive experiments manifest that *USE Attack* significantly improves the overall eavesdropping quality compared with state-of-the-art counterparts and *AngleSec* is able to detect CSI forgery attackers almost for sure.**

I. Introduction

Multiple-Input-Multiple-Output (MIMO) is a key enabling technology to scale up wireless network capacity [1]. A transmitter equipped with multiple antennas can either send the same data stream to a receiver to achieve spatial diversity, or simultaneously transmit multiple independent data streams to different receivers for spatial multiplexing. The latter, termed as multi-user MIMO (MU-MIMO), has been incorporated in the latest 802.11ac standard [2][3]. In 802.11ac MU-MIMO, each user measures the *channel state information (CSI)* between every pair of transmit and receive antennas, and feeds this information to an access point (AP). The AP then sends out multiple data streams such that each user receives only the needed data stream, while the interfering streams are suppressed. This process is called beamforming, and zero-forcing beamforming (ZFBF) [4] has been widely adopted as a standard beamforming scheme. With CSI feedback, MU-MIMO leverages the beamforming technology to nullify the inter-user interference to achieve a spatial multiplexing gain.

As a crucial component of MU-MIMO systems, CSI is estimated by users and transmitted in plaintext. Endowing users such a freedom will expose system vulnerability to malicious attacks. Tung and Han *et al.* [5] presented the first study of CSI forgery attack in MU-MIMO systems. A malicious user can overhear a victim's CSI and report a carefully forged CSI to the AP in order to mislead the beamforming scheme. Then the data stream transmitted to the victim is projected to the attacker's receiving space, enabling him to extract the leaked downlink content. Wang and Liu *et al.* [6] generalized this attack by forging CSI feedback as a polynomial (actually linear) function of the CSI of victims and eavesdroppers (interchangeable with attacker), namely *Polynomial Attack*. A similar eavesdropping attack is observed in Time-Division Duplex systems with implicit CSI estimation [7] and a throughput attack is studied in massive MIMO systems that misleads power allocation with forged CSI [8]. CSI forgery attack will be disastrous for MU-MIMO systems that are usually not affordable to computationally expensive encryption/decryption schemes. This calls upon the research community to scrutinize how detrimental the CSI forgery attacks are, and how to defend against them.

Although *Polynomial Attack* achieves a satisfactory eavesdropping quality, it is conditioned on that the attacker and the victim are served concurrently, otherwise *Polynomial Attack* fails "miserably". When the user population is more than the number of antennas at the AP, it entangles the intrinsic scheduling algorithm of MU-MIMO that selects a subset of users for simultaneous transmission in a time slot. The rationale of scheduling is to group users that can effectively reduce channel correlation and cross-talk interference [9][10][11][12], while that of *Polynomial Attack* is to exploit channel correlation for information leakage. Consequently, the attacker may face a dilemma in reaching both the high *eavesdropping opportunity* and high *eavesdropping quality* simultaneously.

In this paper, we first explore the possibility of CSI forgery attack to achieve both goals in MU-MIMO systems and develop a novel forgery scheme, namely *User Selective Eavesdropping (USE) Attack*. *USE Attack* operates in two stages that construct an orthogonal CSI to guarantee eavesdropping opportunity and then search for a CSI direction with the best overhearing quality. We further generalize *USE Attack* to include the simultaneous eavesdropping of multiple victims with multiple attackers. By defining a new metric, the eaves-

This work was supported in part by the Natural Science Foundation of China under Grant 61772139, in part by the Shanghai-Hong Kong Collaborative Project under Grant 18510760900, and in part by US National Science Foundation under Grants CNS-1566388, CNS-1731833, CNS-1717898. Yuedong Xu is the corresponding author.

dropping mutual information, we present a CSI refinement algorithm for multiple attackers to optimize the effectiveness of simultaneous eavesdropping. We implement *USE Attack* on the software defined radio platform WARPv3 [13]. Our experimental studies manifest that *USE Attack* has almost the same eavesdropping opportunity as the orthogonally forged CSI and the gently degraded eavesdropping quality compared with *Polynomial Attack*, while harvesting a significant improvement on the overall eavesdropping effectiveness.

We propose *AngleSec* to protect existing MU-MIMO networks from *USE Attack*. *AngleSec* is a novel physical layer solution that does not involve any modification to legacy CSI feedback scheme and does not occupy any airtime for transmission. It exploits the characteristics of channel reciprocity in which a downlink angle-of-departure (AoD) resembles an uplink angle-of-arrival (AoA) in terms of normalized angular spectrum at the AP. The AoD and AoA spectra are computed by MUSIC algorithm [14] from the reported CSI and the preamble of CSI feedback packet, respectively. The channel reciprocity holds if the reported CSI is genuine, and is broken if the reported CSI is forged according to a broad range of methods not limited to *USE Attack*. Moreover, *AngleSec* is complementary with encryption based approaches that turn plaintext CSI into encrypted CSI [6] at the cost of certain changes to the feedback scheme. *AngleSec* is lightweight because the angle detection and matching has a small complexity order. Our experiments on WARPv3 platform manifests that the detection rate can be as high as more than 99%.

To sum up, this paper makes the following contributions:

- We discover the complicated entanglement between the CSI forgery attack and the MU-MIMO user scheduling that makes previous forgery strategies much less effective.
- We develop *USE Attack* that optimizes the eavesdropping quality with the guarantee of eavesdropping opportunity.
- We design *AngleSec* that detects the eavesdropper with extraordinarily high probability yet complies with legacy 802.11ac standard.
- We implement and evaluate *USE Attack* and *AngleSec* on software defined radio platform and conduct extensive experiments to validate the eavesdropping gain of *USE Attack* and the detection accuracy of *AngleSec*.

II. Preliminary

A. Beamforming in MU-MIMO

Consider a typical MU-MIMO system where the AP is equipped with N antennas, and serves M single-antenna users contending for transmission slots. Denote $\mathbf{x} = [x_1, x_2, \cdots, x_N]^T$ as the signals transmitted by the AP's antennas. The received signals of users can be written as:

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{1}$$

where $\mathbf{y} = [y_1, y_2, \cdots, y_M]^T$, $\mathbf{H}$ is the $M \times N$ complex channel gain matrix, and $\mathbf{n}$ is the noise vector of users.

To ensure that each user can get its own data without being interfered by other data streams, zero-forcing beamforming is applied. Denote $\mathbf{m} = [m_1, m_2, \cdots, m_M]^T$ as the data symbols that users request. The data streams are precoded by the $N \times M$ precoding matrix $\mathbf{W}$, i.e., $\mathbf{x} = \mathbf{W}\mathbf{m}$. If the precoding matrix $\mathbf{W}$ is configured as the pseudo-inverse of channel matrix $\mathbf{H}$, the received signals can be written as:

$$\mathbf{y} = \mathbf{H}\mathbf{W}\mathbf{m} + \mathbf{n} = \mathbf{H}\mathbf{H}^*(\mathbf{H}\mathbf{H}^*)^{-1}\mathbf{m} + \mathbf{n} = \mathbf{m} + \mathbf{n}, \tag{2}$$

indicating that each user receives its intended data.

B. CSI Forgery Attack

The implementation of ZFBF relies on the channel state information of the users' channels. However, the CSI feedback mechanism is vulnerable to CSI forgery attack as there exists no validation scheme for CSI feedback [5]. If a malicious user reports forged CSI instead of genuine CSI, the channel matrix received by the AP will be $\mathbf{H}^f$, and the corresponding precoding matrix in ZFBF becomes $\mathbf{W}^f$. The received signals are in turn given by: $\mathbf{y} = \mathbf{H}\mathbf{W}^f\mathbf{m} + \mathbf{n}$. As illustrated in Fig. 1, under legitimate beamforming, the data stream for $U1$ is steered towards the direction orthogonal to $\mathbf{h}_2$ to nullify the inter-user interference. However, if the malicious user $U2$ reports a forged CSI $\mathbf{f}_2$, the data stream for $U1$ is precoded at the direction orthogonal to $\mathbf{f}_2$. In this case, the data stream m_1 is leaked in the direction of $\mathbf{h}_2$ and eavesdropped by the malicious user.

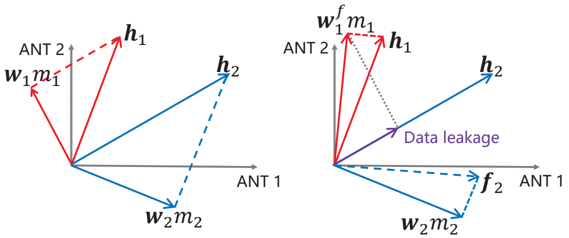


Fig. 1: CSI forgery leads to data leakage in MU-MIMO.

C. User Selection in MU-MIMO

In practical deployment, the number of single-antenna users M is much more than transmit antennas equipped on the AP N, i.e., $M \gg N$. The AP cannot serve all users at one transmission slot, hence an effective user selection scheme is implemented for MU-MIMO systems [15] [16]. The objective of user selection is to decide a subset of the users to maximize the potential aggregate throughput of MU-MIMO system. User selection is generally carried out by the AP after it collects all users' CSI feedback. Once the user selection decision is reached, only the selected users will receive intended data. In addition, the design of modern user selection scheme takes throughput fairness among users into consideration [11].

III. User Selective Eavesdropping Attacks

In this section, we first describe why state-of-the-art CSI forgery attacks can hardly achieve a satisfactory eavesdropping outcome. Then, a novel eavesdropping attack model is formulated that yields a near optimal CSI forging strategy.

A. Why are existing CSI forgery attacks inefficient?

The implementation of MU-MIMO relies on CSI feedback mechanism, which endows an attacker with the chance of misreporting his CSI to the AP and causing data leakage because of imperfect beamforming. Existing CSI forgery attacks are conditioned on simultaneous transmissions to the attacker and the victim by the AP. In practice, the APs are usually deployed with a user selection module in face of large user population. The tussle between CSI forgery and MU-MIMO scheduling may significantly degrade the effectiveness of eavesdropping.

To validate our claim, we implement an 802.11 MU-MIMO system based on WARPv3 platform with a two-antenna AP in an indoor environment. There exist four single-antenna users, one is the eavesdropper, one is the victim, and two others are irrelevant legitimate users. The eavesdropper intends to eavesdrop data symbols transmitted to the victim where we take a *Lena* grayscale image as an example. Given two antennas at the AP, the simultaneous transmission to two users is allowed in each time slot. If the victim is scheduled, a line of pixels are transmitted. Two kinds of eavesdropping attack strategies are evaluated:

- *Passive Eavesdropping*. When the AP transmits data streams to benign users, a passive eavesdropper is capable of overhearing composite data symbols [17].
- *Polynomial Attack*. An eavesdropper reports a forged CSI to the AP that is a polynomial function of CSI of all the eavesdroppers and victims [6]. The data stream steered toward the eavesdropper contains the leaked information of the victim that can be decoded by interference cancellation (IC) [18].

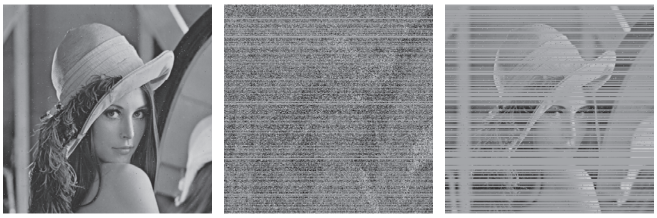

(a) Image received by the victim (b) Image received by a passive eavesdropper (c) Image received by a polynomial attacker

Fig. 2: *Lena* image received by the victim and the benchmark eavesdroppers in MU-MIMO.

As shown in Fig. 2(a), the victim always receives its intended data with few pixels contaminated by noise. The passive eavesdropper only gets a grainy black and white image (Fig. 2(b)). The reasons are two folds. On one hand, if the passive eavesdropper is grouped with the victim, the victim's data symbols are nullified in his direction by beamforming. On the other hand, if the victim is grouped with an irreverent user, the eavesdropper overhears a composition of their data streams, while none of them could be decoded. The polynomial attacker can decode the data symbols with a certain level of distortion if it is grouped with the victim. Similar to the passive eavesdropping case, it is not capable of decoding composite data symbols if scheduled with an irreverent user, resulting in grey stripes in Fig. 2(c). As a rule of thumb, the passive eavesdropping is invalid in MU-MIMO systems, and the polynomial eavesdropping lacks of consideration of multi-user scheduling. This incentives an attacker to launch more effective eavesdropping that contends for as many attacking opportunities as possible and achieves a high eavesdropping quality meanwhile.

B. Basic Eavesdropping Attack: Single Victim

Consider a MU-MIMO system where the AP is equipped with two antennas and three single-antenna users request data from the AP. Without loss of generality, we assume that $U1$ is the victim and $U2$ is the malicious attacker. $U3$ is neither an attacker nor a victim. The attacker is capable of overhearing the CSI feedback of the victim and reporting forged CSI.

The authors in [5] proved that if the malicious user and the victim are grouped together, then the malicious user is capable of eavesdropping the data for victim by reporting forged CSI. If the malicious user $U2$ in a 2×2 MU-MIMO system reports forged CSI $\mathbf{f}_2 = [f_{21}\ f_{22}]$ instead of genuine CSI $\mathbf{h}_2 = [h_{21}\ h_{22}]$, its received signal is a linear combination of m_1 and m_2:

$$y_2 = \frac{h_{21}f_{22} - h_{22}f_{21}}{h_{11}f_{22} - f_{21}h_{12}} m_1 + \frac{h_{11}h_{22} - h_{12}h_{21}}{h_{11}f_{22} - f_{21}h_{12}} m_2 + n_2. \quad (3)$$

where m_1 and m_2 are the data symbols for $U1$ and $U2$, and $h_{11}, h_{12}, h_{21}, h_{22}$ are complex channel gains between the AP and users. Moreover, if the forged CSI is $\mathbf{f}_2 = w\mathbf{h}_1 - \mathbf{h}_2$, then the signal received by the malicious user is

$$y_2 = w \cdot m_1 + m_2 + n_2 \quad (4)$$

The malicious user is able to decode the data m_1 by removing its own data m_2 with interference cancellation [18].

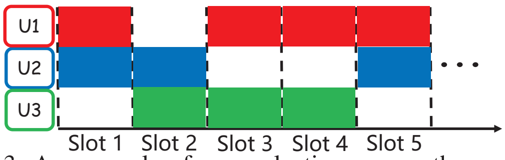


Fig. 3: An example of user selection among three users.

However, the assumption that the attacker and the victim are grouped together is not always satisfied because of the user selection module in MU-MIMO. Fig. 3 gives an example of user selection among three users where colored bars indicate the user is served in the slot. Due to the time-varying nature of wireless channel, the user selection results are different from time to time. The attacker $U2$ is grouped with $U1$ only in Slot 1 and Slot 5. In the other time slots, the CSI forgery attack does not work totally. The reason that AP selects other user combinations is that their channels pose better orthogonality and weaker correlation. For instance, the channel vector $\mathbf{h}_1$ and $\mathbf{h}_3$ in Fig. 4 are with the best orthogonality, thus the AP will select $U1$ and $U3$ to serve. In order to launch effective eavesdropping attack, the forged CSI of malicious user is supposed to be well orthogonal to the CSI of victim. If the forged CSI $\mathbf{f}_2$ has the direction as the blue dashed vector, the user selection module will be misled to select $U1$ and $U2$, making it possible for the CSI forgery attack.

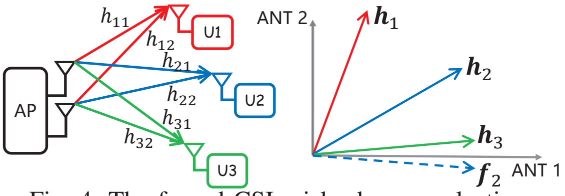


Fig. 4: The forged CSI misleads user selection.

C. Generalized Eavesdropping Attack: Multiple Victims

Suppose that the AP is equipped with N antennas, and there are K coordinated attackers and L victims among M single-antenna users ($M > N$, $L + K \leq N$). Denote $U_1, U_2, \cdots, U_L$ by the victims and $U_{L+1}, U_{L+2}, \cdots, U_{L+K}$ by the attackers. The attackers report forged CSI $\mathbf{f}_{L+1}, \mathbf{f}_{L+2}, \cdots, \mathbf{f}_{L+K}$ instead of genuine CSI $\mathbf{h}_{L+1}, \mathbf{h}_{L+2}, \cdots, \mathbf{h}_{L+K}$ to launch concurrent eavesdropping attacks.

For attacker $U_k (L + 1 \leq k \leq L + K)$, if it is grouped with the victims and report forged CSI $\mathbf{f}_k$ by a polynomial function of the genuine CSI $\mathbf{h}_1, \cdots, \mathbf{h}_{L+K}$, i.e.,

$$\mathbf{f}_k = \sum\nolimits_{i=1}^{L+K} \theta_{k,i}\mathbf{h}_i, \qquad (5)$$

then the forged channel matrix is given by $\mathbf{H}^f = \Theta \cdot \mathbf{H}$, where $\mathbf{H} = [\mathbf{h}_1^T, \cdots, \mathbf{h}_L^T, \mathbf{h}_{L+1}^T, \cdots, \mathbf{h}_{L+K}^T]^T$ is the genuine channel matrix and Θ is a coefficient matrix. The elements in the k^{th} row of matrix Θ correspond to the coefficients in the above Eq. (5), and the elements in the other rows is identical to the entries of the unit matrix with the same dimension. The mistaken beamforming weight matrix $\mathbf{W}^f$ is calculated from $\mathbf{W}^f = \mathbf{H}^{f^H}(\mathbf{H}^f\mathbf{H}^{f^H})^{-1}$, and the received signals of attackers and victims can be obtained by

$$\mathbf{y} = \mathbf{H}\mathbf{W}^f\mathbf{m} + \mathbf{n} = \Theta^{-1}\mathbf{m} + \mathbf{n}, \qquad (6)$$

It has been proved in [6] that $y_i = m_i + n_i$ always holds for $i = 1, 2, \cdots, L$, which means that the victims receive the intended data without being impacted. However, the received signals of attackers are given by $y_k = \sum_{i=1}^{L+K} \phi_{k,i}m_i + n_k$, where the coefficients $\phi_{k,i}$ are elements in the inverse of matrix Θ, which is known to the coordinated attackers. After removing the components of its own data with interference cancellation, the received signals become $y_k^{IC} = \sum_{i=1}^{L} \phi_{k,i}m_i + n_k$, where $k = L + 1, L + 2, \cdots, L + K$. Combining the equations together, we have

$$\mathbf{y}^{IC} = \Phi\mathbf{m} + \mathbf{n}, \qquad (7)$$

where $\mathbf{y}^{IC} = [y_{L+1}^{IC}, y_{L+2}^{IC}, \cdots, y_{L+K}^{IC}]^T$ and Φ is the $K \times L$ coefficient matrix. If $K \geq L$, the variables $\mathbf{m} = [m_1, m_2, \cdots, m_L]^T$ are decoded with linear least square method $\hat{\mathbf{m}} = (\Phi^H\Phi)^{-1}\Phi^H\mathbf{y}^{IC}$, which means that the L victims are eavesdropped concurrently.

The theory of concurrently eavesdropping multiple victims with coordinated users is also based on the prerequisite that the attackers and victims are in the same MU-MIMO user group. If the number of selected attackers is fewer than the number of victims, the concurrent eavesdropping will fail because there are more unknown variables than equations in Eq. (7).

D. Design of User Selective Eavesdropping Attack

With the theory of concurrently eavesdropping multiple victims with coordinated users well established, we next investigate how to design forged CSI to make sure the attackers and victims are grouped together and maximize the eavesdropping quality. Mathematically, the problem is to find a set of parameters $\theta_{k,i}, i = 1, \cdots, L+K$ in Eq. (5). Intuitively, if the forged CSI of attackers are orthogonal to the CSI of victims, and the forged CSI of attackers are orthogonal to each other, the channel correlation would be the least compared with all other possible user combinations that contain the victims.

The perfectly orthogonal CSI design is obtained by successive channel vector projection. Firstly, we construct a series of orthogonal bases in the subspace of the CSI of victims and attackers. The CSI of the first user is the first basis, i.e., $\mathbf{b}_1 = \mathbf{h}_1$. In the following steps, the basis $\mathbf{b}_i$ is obtained by removing the projection on constructed orthogonal bases from $\mathbf{h}_i$ successively:

$$\mathbf{b}_i = \mathbf{h}_i - \sum\nolimits_{j=1}^{i-1} proj(\mathbf{h}_i, \mathbf{b}_j), \qquad (8)$$

where $proj(\mathbf{h}_i, \mathbf{b}_j) = \frac{\mathbf{b}_j \cdot \mathbf{h}_i}{||\mathbf{b}_j||^2}\mathbf{b}_j$ is the projection of $\mathbf{h}_i$ on the direction of the j^{th} basis $\mathbf{b}_j$. The forged CSI of attackers $\mathbf{f}_k$ is obtained by scaling the magnitude of the k^{th} orthogonal basis $\mathbf{b}_k$ up to the magnitude of original CSI $\mathbf{h}_k$, i.e., $\mathbf{f}_k = ||\mathbf{h}_k|| \cdot \frac{\mathbf{b}_k}{||\mathbf{b}_k||}$. The magnitude scaling makes the forged CSI pose the same channel quality to the genuine CSI, because we intend to misreport the channel direction rather than the channel quality. Now we obtain forged CSI $\mathbf{f}_{L+1}, \cdots, \mathbf{f}_{L+K}$ that satisfy the perfectly orthogonal requirement:

$$\begin{aligned} \mathbf{h}_i \cdot \mathbf{f}_k = 0, &\qquad \forall 1 \leq i \leq L \text{ and } L+1 \leq k \leq L+K \\ \mathbf{f}_{k_1} \cdot \mathbf{f}_{k_2} = 0, &\qquad \forall L+1 \leq k_1, k_2 \leq L+K \end{aligned}$$

Meanwhile, the design complies with Eq. (5), in which the parameters $\theta_{k,i}$ is obtained during the successive channel vector projection and scaling procedure. The design is named as *Orthogonal Attack* for further evaluation.

However, the design of *Orthogonal Attack* is overqualified for the attackers and victims being selected into the same MU-MIMO user group. Chances are that a series of forged CSI, which are not perfectly orthogonal to the victims' CSI subspace, will also make the attackers and victims grouped together and achieve better eavesdropping quality. Therefore, we balance the trade-off between eavesdropping opportunity and eavesdropping quality with a heuristic algorithm.

Albeit the perfectly orthogonal forged CSI is hardly the optimal solution, it provides a rough result that will make the attackers and victims being grouped together with largest possibility. We then refine the rough design of forge CSI iteratively. Eq. (7) describes how received signals by attackers after interference cancellation are related to the data for victims. Similar to the inference of MIMO channel capacity, the mutual information between transmitted data $\mathbf{m}$ and received data after interference cancellation $\mathbf{y}^{IC}$ could be utilized as the metric for evaluating the quality of eavesdropping. The mutual information $I(\mathbf{m}; \mathbf{y}^{IC})$ is given by

$$I(\mathbf{m}; \mathbf{y}^{IC}) = H(\mathbf{y}^{IC}) - H(\mathbf{y}^{IC}|\mathbf{m}) = H(\mathbf{y}^{IC}) - H(\mathbf{n}),$$

where $H(\mathbf{y}^{IC})$ is the differential entropy of vector $\mathbf{y}^{IC}$. The covariance matrix of $\mathbf{y}^{IC}$ is given by

$$\mathbf{R_{yy}} = \phi\mathbf{R_{mm}}\phi^H + \mathbf{R_{nn}},$$

where $\mathbf{R_{mm}}$ and $\mathbf{R_{nn}}$ are the covariance matrix of victims' signals and noise respectively. If that the signals are independent, then we get $\mathbf{R_{mm}} = diag(p_1, p_2, \cdots, p_L)$, where $p_i = \mathbf{E}[m_i^2]$ is the average signal power of victim U_i. Assume that the noise is additive white Gaussian noise (AWGN) with unit power, then the signal power is computed according to the average SNR data field in the compressed feedback packets [11]. Therefore, the mutual information is given by

$$I(\mathbf{m};\mathbf{y}^{IC}) = \log\det(I + \phi\mathbf{R}_{\mathbf{mm}}\phi^{H}). \tag{9}$$

Maximizing the mutual information is equivalent to optimizing the eavesdropping quality. This is consistent with the basic attack model, where increasing w in Eq. (4) is equivalent to optimizing the eavesdropping signal-to-noise ratio (SNR).

Algorithm 1: CSI Forgery Algorithm of *USE Attack*

```
Input: CSI of $L$ victims: $\mathbf{h}_1, \cdots, \mathbf{h}_L$
       CSI of $K$ attackers: $\mathbf{h}_{L+1}, \cdots, \mathbf{h}_{L+K}$
Output: Forged CSI of attackers: $\mathbf{f}_{L+1}, \cdots, \mathbf{f}_{L+K}$
// Construct the orthogonal bases
$\mathbf{b}_1 = \mathbf{h}_1$;
for $i = 2; i \leq L+K; i++$ do
    $\mathbf{b}_i = \mathbf{h}_i - \sum_{j=1}^{i-1} proj(\mathbf{h}_i, \mathbf{b}_j)$;
// Initialize the forged CSI
for $k = L+1; k \leq L+K; k++$ do
    $\mathbf{f}_k = ||\mathbf{h}_k|| \cdot \frac{\mathbf{b}_k}{||\mathbf{b}_k||}$;
    $\mathbf{h}_k^{res} = \mathbf{h}_k - \mathbf{b}_k$;
// Refine the forged CSI iteratively
while true do
    for $k = L+1; k \leq L+K; k++$ do
        $\mathbf{f}_k^{new} = \mathbf{f}_k + \delta \cdot \mathbf{h}_k^{res}$;
        $\mathbf{f}_k^{new} = ||\mathbf{h}_k|| \cdot \mathbf{f}_k^{new} / ||\mathbf{f}_k^{new}||$;
        if $\Omega^{new} = \Omega$ && $I^{new} > I$ then
            $\mathbf{f}_k = \mathbf{f}_k^{new}$;
    if $\sum_{k=L+1}^{L+K} ||\Delta\mathbf{f}_k|| < Threshold$ then
        break;
return $\mathbf{f}_{L+1}, \cdots, \mathbf{f}_{L+K}$
```

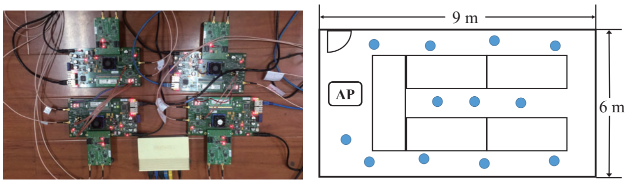
To achieve the balance between eavesdropping opportunity and eavesdropping quality, we iteratively refine the forged CSI as described in Algorithm 1. For each attacker, after extracting the orthogonal CSI $\mathbf{f}_k$ from raw CSI $\mathbf{h}_k$, there exists a residual channel vector $\mathbf{h}_k^{res} = \mathbf{h}_k - \mathbf{f}_k$ containing the non-orthogonal components. In each following iteration, a small proportion of the residual channel vector $\delta \cdot \mathbf{h}_k^{res}$ is added to the forged CSI. The reason of choosing the refinement vector is that it is for sure that the forged CSI after refinement is still a polynomial function of the CSI of victims and attackers, resulting in the received signal without being interfered by signal in the null space. If the user selection result Ω remains unchanged but mutual information is improved, the refinement is kept for next iteration. The iterative refinement automatically terminates when the forged CSI of all attackers becomes stable.

IV. Implementation and Evaluation

We implement *USE Attack* on WARPv3 software defined radio platform. The system consists of three modules.

- **802.11ac MIMO PHY**. The full-fledged MIMO-OFDM components including scrambler, convolution encoder, interleaver, mapper and ZFBF are realized.
- **MU-MIMO User Selection**. The standard throughput maximization scheme [9] and a most recently user selection algorithm namely *MUSE* [11] are implemented.
- **CSI Forgery**. Passive, Polynomial, Orthogonal and USE attacks are implemented for comparison.

The WARPv3 platform is shown in Fig. 5(a) where one board acts as the AP supporting four antennas and other three boards act as users. All the experiments are conducted in a multipath rich, typically sized meeting room (Fig. 5(b)). The AP is placed in the front while the users are placed randomly in this room with both line-of-sight (LoS) and non-LoS situations. Our system operates at 5GHz channel with 20MHz bandwidth, and the OFDM PHY subdivides the channel into 64 subcarriers. The 802.11 preambles in the CSI feedback are also implemented.



(a) WARP platform (b) Meeting Room

Fig. 5: Evaluation platform and environment

A. User Selective Eavesdropping: Single Victim

We start from evaluating the basic yet the most important scenario that has one eavesdropper, one victim and two legitimate users (neither eavesdroppers nor victims). The users are distributed randomly in the meeting room and the AP is equipped with two antennas that can serve two downlink users simultaneously. The maximum throughput scheduler is implemented as the AP. Each experiment is repeated five times where the transmission lasts for one hundred slots in each experiment.

To quantify how effective *USE Attack* enhances the chance of eavesdropping, we define a metric namely *Group Hit Ratio (GHR)*. GHR is the ratio of the number of slots that the attacker and the victim are scheduled together to the number of slots that the victim is scheduled with an arbitrary user. A larger GHR means a higher possibility of the victim being eavesdropped. Fig. 6 measures GHR in five different experiments. For the case of "no attack", GHR reflects the intrinsic channel correlation between the attacker and the victim, and it is usually not high. *Polynomial Attack* forges CSI toward the direction that the attacker's and victim's CSI are largely correlated. This does not comply with rationale that the AP tends to schedule users with less co-channel interference. As a result, *Polynomial Attack* has a much smaller GHR, preventing it from satisfactory eavesdropping. *Orthogonal Attack*, aiming to optimize GHR, is a special case of *USE Attack*. Due to channel variability, the victim would be grouped with a legitimate user even in *Orthogonal Attack* such that GHR cannot reach 1. The most striking feature is that *USE Attack* performs as good as *Orthogonal Attack* in terms of GHR, implying that seeking a better overhearing quality may not sacrifice eavesdropping chances.

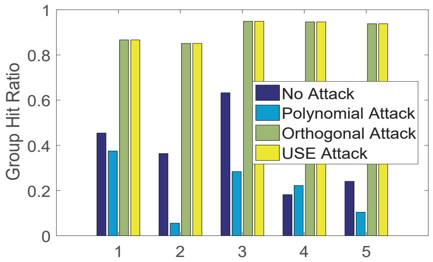


Fig. 6: GHR w/ and w/o attacks.

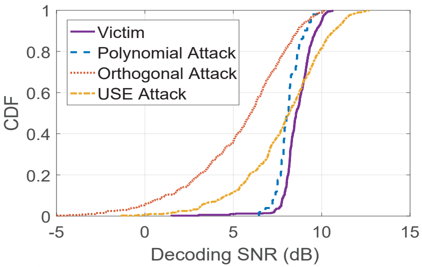


Fig. 7: Decoding SNR under attack.

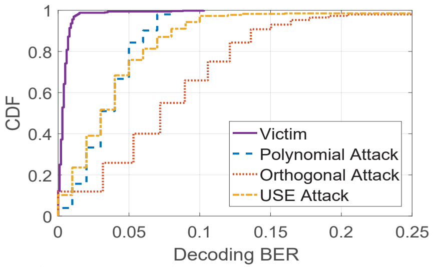


Fig. 8: Decoding BER under attack.

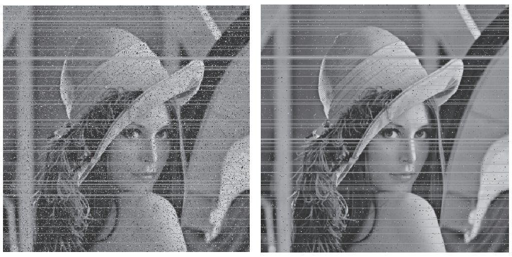


Fig. 9: *Orthogonal Attack* and *USE Attack* of *Lena* image.

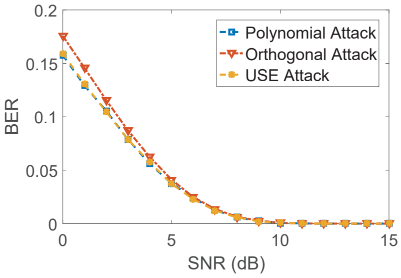


Fig. 10: Decoding BER under different received SNR levels.

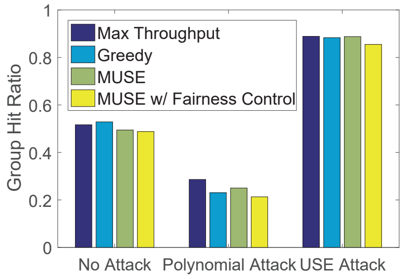


Fig. 11: GHR under different user selection algorithms.

We next evaluate to what extent *USE Attack* trades overhearing quality for eavesdropping chances. Fig. 7 and 8 show the cumulative distribution function (CDF) of decoding SNRs and BERs at the victim and the attacker conditioned on they are scheduled at the *same* time slot. The SNR of *Polynomial Attack* is close to that of the victim (consistent with [5]). However, the decoding BER of *Polynomial Attack* is obviously worse than the victim after QPSK modulation because of the noise and the residue error of interference cancellation (this observation is also in line with [5]). *Orthogonal Attack* exhibits the worst decoding performance because the perfectly orthogonal CSI causes the projection of victim's data stream toward the attacker's direction very weak. In contrast, the SNR of *USE Attack* is moderately lower than that of *Polynomial Attack* while their decoding BERs and hence eavesdropping qualities are comparable. With the same CSI trace, we visualize the effect of *Orthogonal Attack* and *USE Attack* in Fig. 9. Compared with the polynomial attacker and the orthogonal attacker, the image received by the *USE Attack* attains both the fewer noisy pixels and the fewer grey stripes. Therefore, *USE Attack* strikes a delicate balance on the eavesdropping quality and the eavesdropping opportunity, thus achieving a much better overall performance than its counterparts.

We hereby evaluate the eavesdropping performance of *USE Attack* under different signal qualities by emulating the decoding procedure with the above CSI trace. Artificial noise at different levels is added to produce signal with different SNR. The emulation is repeated 100 times and the average decoding BER is shown on Fig. 10. One can see that when the SNR is below 10dB, all the attacks suffer from decoding errors. The average decoding BER of *USE Attack* stays almost the same as *Polynomial Attack*, while *Orthogonal Attack* produces more decoding errors. When the SNR of received signal exceeds 10dB, all the attackers could decode the eavesdropped data with almost no error.

Moreover, we investigate how user selection algorithms will affect the performance of *USE Attack*. The user selection procedure is repeated with the genuine and forged CSI traces under the implemented user selection algorithms respectively, and Fig. 11 shows the average GHR. One can see that different user selection algorithms cause minor influence on GHR with the same CSI feedback trace. Because all the algorithms seek to maximize the sum throughput, they will make the same user selection decision in plenty of time slots. *MUSE* with fairness control does not obviously degrades GHR performance, because the fairness control scheme prevents all users from being served continuously for fairness guarantee and has similar impact on both the attacker and victim. This demonstrates that *USE Attack* is capable of launching attack without being affected by specific user selection schemes.

B. *User Selective Eavesdropping: Multiple Victims*

The generalized *USE Attack* is evaluated with an AP equipped with four antennas and six users including two eavesdroppers, two victims and two irrelevant users. The AP transmits four data streams to four users concurrently at each time slot. Note that in this scenario, the prerequisite of performing *USE Attack* is to let all the attackers and all the victims grouped together. Each of our experiment is repeated for tens of rounds, and in each round the transmission and eavesdropping is conducted for 100 slots with users displaced in different locations.

Here, *Group Hit Ratio (GHR)* is redefined as the ratio between two slot numbers. One is the number of slots that two attackers and two victims are grouped together, the other is that of two victims being served at the same time. Our purpose is to validate the possibility of launching eavesdropping attack on multiple targets simultaneously. The CDFs of GHR with different kinds of eavesdropping attacks are shown in Fig. 12. It is clear to observe that *Polynomial Attack* suffers from low GHR (i.e. around 15% on average), implying that the attackers

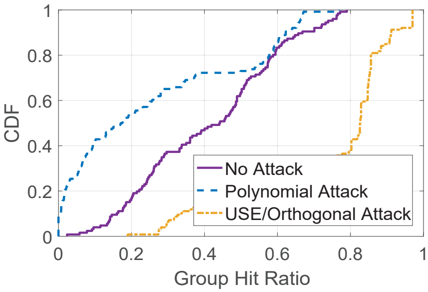


Fig. 12: GHR w/ and w/o attacks.

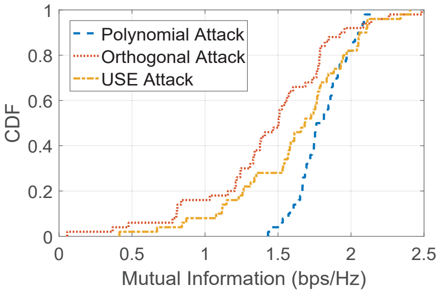


Fig. 13: Mutual Information under attacks.

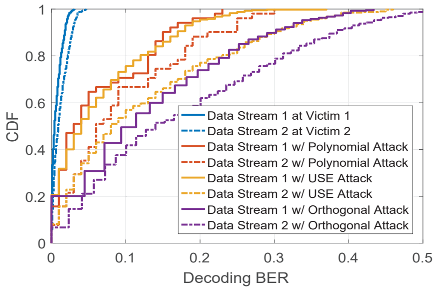


Fig. 14: Decoding BER under attacks.

miss a lot of slots of being grouped with all the victims. One can imagine that if the attackers want to eavesdrop the *Lena* image, a large part of the received image is covered by grey stripes. By forging CSI perfectly orthogonal to the victims' channels, *Orthogonal Attack* has a median GHR over 80%. The GHR of *USE Attack* is very close to that of *Orthogonal Attack* because the former tunes the forged CSI to improve overhearing SNR with almost negligible changes to the user selection results.

Fig. 13 plots the eavesdropping mutual information of two data streams under different attacks and Fig. 14 illustrates their decoding BERs respectively. Although *Polynomial Attack* has a larger value of eavesdropping mutual information than *USE Attack*, their decoding BERs do not differ greatly because of the noise and the imperfect interference cancellation. Compared with *Polynomial Attack*, *USE Attack* earns much more grouping slots to launch effective eavesdropping attacks and acquires an acceptable overhearing quality meanwhile. *USE Attack* also outperforms *Orthogonal Attack* with an obvious gain in the mutual information and the decoding BER, demonstrating the necessity of amending forged CSI for better overhearing quality.

V. Countermeasures

In this section, we propose a lightweight signal processing mechanism to detect eavesdroppers by exploiting the directional reciprocality of downlink and uplink signals.

A. Basic Idea

As the prerequisite of forgery, malicious users should know their own and other users' CSI. In existing MU-MIMO systems, CSI is estimated by users using a known training sequence and is fed back to the AP in plaintext at the basic rate. Hence, an intuitive approach of neutralizing this attack is to encrypt CSI in the feedback mechanism. *CSIsec* [5] enables the AP to transmit an unknown sequence instead of the standard one to users and the estimated CSI at each user is not genuine so that the forgery of CSI by the attacker may be prevented. However, authors in [6] proves that *CSIsec* can be bypassed. They designed *AntiPoly* in which the AP generates a list of keys for users and each user holds another secret key to encrypt CSI feedback. The potential limitations of *AntiPoly* lie in the requirement of modifying the feedback mechanism at both sides as well as the incurred overhead of generating keys and encrypting CSI.

We pursue a lightweight defense strategy from a different perspective. Instead of preventing malicious users sniffing CSI, we aim at detecting them and restraining them from being served. To achieve this goal, we take advantage of channel reciprocity in MU-MIMO systems [19]. Ideally, the CSI of downlink and uplink is ought to match because CSI reflects channel response of pairwise antenna. If a feedback CSI is forged, the channel reciprocity is likely to be destroyed. The AP can evaluate the similarity between the reported downlink CSI and the estimated uplink CSI so as to identify malicious users. However, this straightforward approach does not work due to unknown amplitude attenuations and phase rotations in CSI introduced by circuit modules of the AP and users.

An interesting property of channel reciprocity is that the angle of departure (AoD) to the user at the downlink is equivalent to the angle of arrival (AoA) at the uplink along a propagation path. Inspired by this observation, we propose a novel approach, namely *AngleSec* that compares AoA and AoD spectra for detecting the existence of malicious users. Our proposal is feasible in MU-MIMO systems because the AP equipped with multiple antennas is able to compute the AoA and AoD spectra.

B. Theory of AoA/AoD Estimation

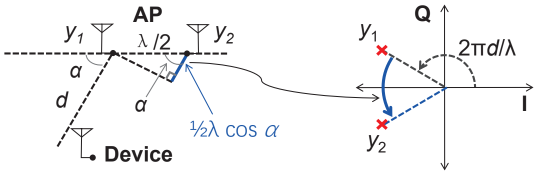


Fig. 15: Basic principle of AoA.

We hereby describe the procedure of obtaining AoA and AoD estimations with MUSIC algorithm [14]. Consider a simple example in Fig. 15 where wireless signal propagates from a single transmit antenna to two receive antennas along a path. Let λ be the wavelength and α be the angle of arrival. The received signal y_2 traverses an additional distance $\frac{\lambda}{2}\cos\alpha$ compared with y_1, and such a distance results in an extra phase shift in the received signals shown in Fig. 15. Thus, the angle of arrival α can be calculated by

$$\alpha = \arccos\frac{Phase(y_2) - Phase(y_1)}{\pi}. \tag{10}$$

The AoD can be estimated by the similar way where the only difference is the direction of signal propagation.

In practice, the calculation in Eq. (10) does not yield an accurate AoA estimate with merely two antennas due to multi-

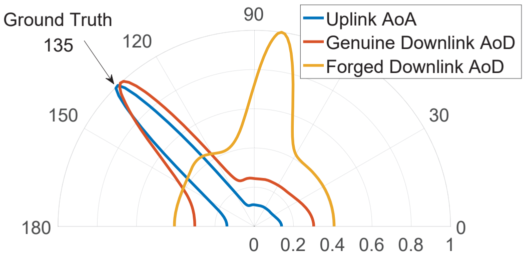


Fig. 16: Spectra of uplink AoA, genuine downlink AoD and forged downlink AoD.

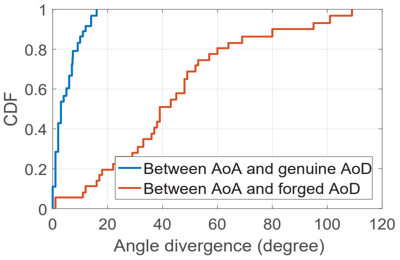


Fig. 17: Angle divergence of users in LoS environments.

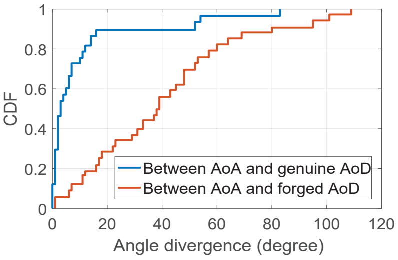


Fig. 18: Angle divergence of users in non-LoS environments.

path reflection of signals. The received signals at multiple antennas of the AP can be used jointly to separate propagation on multiple paths. Suppose that the AP is equipped with a uniform linear antenna array (ULA) [20] of N antennas and each pair of adjacent antennas is spaced by half of a wavelength. Denote by α_p the AoA of the p^{th} path. Let c be the velocity of light and f be the carrier frequency. The phase shifts across all the antenna elements are expressed as a *steering vector*:

$$\mathbf{v}(\alpha_p) = [1, e^{-j2\pi f \frac{\lambda}{2} \frac{\cos(\alpha_p)}{c}}, \cdots, e^{-j2\pi f \frac{(N-1)\lambda}{2} \frac{\cos(\alpha_p)}{c}}]^T$$

if the first element of the array is taken as the reference antenna. Denote by $s_p(t)$ the signal received by the reference antenna on path p. The vector of the received signals on path p are given by $\mathbf{y}_p(t) = \mathbf{v}(\alpha_p)s_p(t) + \mathbf{n}(t)$ where $\mathbf{n}(t)$ denotes Gaussian noise. Given P paths in total (including line-of-sight and non-line-of-sight), the composite received signal is

$$\mathbf{y}(t) = \sum\nolimits_{p=1}^{P} \mathbf{v}(\alpha_p)s_p(t) + \mathbf{n}(t). \tag{11}$$

The MUSIC algorithm is adopted to estimate AoA spectrum for the sake of low complexity and sufficient accuracy that serves our goal. The principle of MUSIC is out of the scope of this work so that we only present its operations: i) calculating the correlation matrix of received signal by $R_{\mathbf{yy}} = \mathbf{E}[\mathbf{y}\mathbf{y}^T]$; ii) computing the eigenvectors of $R_{\mathbf{yy}}$ and sorting them as $[\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_N]$ in descending order of corresponding eigenvalues; iii) solving AoA spectrum by

$$S_{AoA}(\alpha) = \frac{1}{\mathbf{v}^H(\alpha)\mathbf{E}_n\mathbf{E}_n^H\mathbf{v}(\alpha)} \tag{12}$$

where $\mathbf{E}_n$ is the subspace spanned by the last $(N - P)$ eigenvectors. The AoA spectrum captures the belief of angles that signals of a user arrive to the AP.

C. Malicious User Detection Algorithm

Two practical challenges hinder the way of detecting malicious users, one is whether *AngleSec* is backward compatible with legacy 802.11 standard, the other is how the similarity of AoA and AoD spectrum are quantified [21]. In existing 802.11 MU-MIMO systems, the users calculate downlink CSI from received training sequence and report it to the AP so that the AoD can be estimated from these feedbacks. Meanwhile, the AP can compute the uplink AoA using the 802.11 preambles in the feedback packets. One can see that *AngleSec* does not require any change on 802.11 protocols at all layers.

Before diving in the detection algorithm, we demonstrate how the forged CSI may damage the channel reciprocity. Fig. 16 shows the spectra of uplink AoA, downlink AoD of genuine CSI and downlink AoD of forged CSI in a realistic indoor environment. As an interesting observation, the uplink AoA resembles the genuine downlink AoD and their peaks point to directions close to the ground truth (no more than 5 degrees), while the peak of downlink AoD spectrum of forged CSI is steered at another direction.

The extraordinary difference in the spectra between genuine and forged CSI fosters an intuitive approach to detect forged CSI, that is, computing the correlation of spectra of uplink AoA and downlink AoD. However, a direct adoption of this approach is not robust because a slight divergence of two spectra may cause a remarkable drop of the correlation. Though not common, it does happen when the SNR of wireless signals is weak so that a genuine CSI is mistaken as a forged one. To cope with unfavourable estimation error in the low SNR regime, we propose a new correlation metric by introducing a variable angle offset. Denote by $\Delta\alpha$ the angle offset, then the corresponding correlation is given by

$$Corr(\Delta\alpha) = \sum\nolimits_{\alpha=0}^{180^\circ} S_{AoA}(\alpha)S_{AoD}(\alpha + \Delta\alpha). \tag{13}$$

The angle divergence d between AoA and AoD spectra is obtained by searching for the $\Delta\alpha$ that leads to the maximum correlation:

$$d = \arg\max_{\Delta\alpha} \sum\nolimits_{\alpha=0}^{180^\circ} S_{AoA}(\alpha)S_{AoD}(\alpha + \Delta\alpha) \tag{14}$$

The AoA and AoD spectra match best with the angle divergence d. If the angle divergence is within a small range, for instance, $|d| \leq 10^\circ$, the divergence will be thought as caused by estimation error, and the user is judged as a benign one. In contrast, the user with an obviously large angle divergence is adjudicated as that generated a malicious one.

AngleSec is effective because the attacker can hardly achieve two conflicting goals, the good eavesdropping ability and the high correlation with genuine AoD spectrum. If the forged CSI and genuine CSI have similar AoD spectra, their signal subspace and noise subspace are equivalent respectively. Although the noise subspace of forged CSI could be duplicated from genuine CSI, the signal subspace of forged CSI is decided by Algorithm 1. Recall that the forged CSI of a certain attacker is ought to be a linear combination of CSI of victims and attackers, then the signal subspace of forged CSI is hardly possible to be close to the signal subspace of genuine CSI.

AngleSec is robust when facing practical factors including multipath propagation, LoS blockage and user movement. The first two factors have negligible impact on the detection because of channel reciprocity, i.e. uplink AoA and downlink

AoD being influenced in the same way. User movement may influence CSI considerably while the angle patterns of CSI remain unaltered at the millisecond magnitude of scheduling rounds. Moreover, *AngleSec* is intrinsically tolerant to angle shift within a small range.

D. Performance Evaluation

We deploy *AngleSec* at the AP side with four antennas assembled as a uniform linear antenna array. The AP collects genuine CSI and forged CSI to compute the AoD spectrum and estimate the AoA spectrum from preambles. The AoA/AoD angle divergence is obtained according to Eq. (14). Fig. 17 shows the angle divergence of genuine users and attackers in LoS scenarios. One can see that the angle divergences of honest users are below $10°$ for over 90% percent of users. However, the angle divergences of CSI forgery attackers are much larger, ranging from $10°$ to $100°$.

When LoS path between users and the AP is blocked, the AoA and AoD estimates become less accurate because of the relatively lower receiving SNR (Fig. 18). However, the majority of AoA/AoD angular divergences remain to be small due to the intrinsic channel reciprocity. More than 90% of genuine users do not suffer from severe estimation errors, and are easily distinguished from forgery users in a *single* round.

If the angle threshold in the defense scheme is set as $10°$, the overall accuracy of malicious user detection algorithm in LoS and non-LoS environments is 91.9% and 84.7% respectively. Thus, the malicious user detection algorithm demonstrates good performance. Moreover, the threshold can be adjusted for specific purposes. A lower threshold will strictly exclude malicious users at the price of judging several legitimate users by mistake. On the contrary, increasing the threshold to $16°$ will make all legitimate users with LoS judged correctly but 15% of malicious users will be missed.

We further improve the detection performance of the defense algorithm by jointly analyzing the angle divergences in multiple continuous slots. A user will be judged as malicious user only if its angle divergences in several continuous slots are all beyond the threshold. The experiment results in Table I shows the missing alarm and false alarm rate with different number of slots combined. It is obvious that increasing the analyzed time slot improves the detection accuracy. By joint analysis on angle divergences in three slots, the probability of judging a legitimate user by mistake is only 1%, while only 0.2% of malicious users will remain undetected. The joint detection scheme is also easy to deploy in AP via modifying firmware.

Number of slots	1	2	3	4	5
False Alarm Rate	0.195	0.039	0.010	0.001	0.000
Missing Alarm Rate	0.069	0.012	0.002	0.000	0.000

TABLE I: Detection error rate in multiple slots.

VI. Conclusion

In this paper, we bridge the gap between theoretic eavesdropping model and practical user selection in MU-MIMO networks by proposing *User Selective Eavesdropping Attack*. By forging CSI, the coordinated malicious users are capable of misleading various user selection schemes and decoding the data symbols from the victims. Extensive experiments demonstrate the effectiveness of *USE Attack*. In defense, we propose *AngleSec* to detect malicious users that reports forged CSI. By exploiting the channel reciprocity, *AngleSec* evaluates the similarity between propagation patterns of uplink and downlink signal and judge the legitimacy accordingly. The defense algorithm has high detection accuracy in both LoS and non-LoS environments.

References

[1] A.J. Paulraj, D.A. Gore, R.U. Nabar, and H. Bolcskei, “An overview of MIMO communications - a key to gigabit wireless”, in *Proc. IEEE*, vol. 92, no. 2, pp. 198-218, Feb. 2004.

[2] “*IEEE Draft Standard for IT - Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications - Amd 4: Enhancements for Very High Throughput for operation in bands below 6GHz*,” IEEE P802.11ac/D3.0, June 2012.

[3] O. Bejarano, E. W. Knightly, and Minyoung Park, “IEEE 802.11ac: from channelization to multi-user MIMO”, *IEEE Comm. Mag.*, vol. 51, no. 10, pp. 84-90, Oct. 2013.

[4] N. Anand, S. Lee, and E. W. Knightly, “STROBE: Actively Securing Wireless Communications using Zero-Forcing Beamforming”, in *Proc. IEEE INFOCOM*, 2012.

[5] Y. Tung, S. Han, D. Chen, and K. G. Shin, “Vulnerability and Protection of Channel State Information in Multiuser MIMO Networks”, in *Proc. ACM CCS*, 2014.

[6] X. Wang, Y. Liu, X, Lu, S. Lv, Z. Shi, and L. Sun, “On Eavesdropping Attacks and Countermeasures for MU-MIMO Systems”, in *Proc. IEEE MILCOM*, 2017.

[7] Y. Mao, Y. Zhang, and S. Zhong, “Stemming Downlink Leakage from Training Sequences in Multi-User MIMO Networks”, in *Proc. ACM CCS*, 2016.

[8] Z. Zhang, Y. Sun, A. Sabharwal, and Z. Chen, “Impact of Channel State Misreporting on Multi-user Massive MIMO Scheduling Performance”, in *Proc. IEEE INFOCOM*, 2018.

[9] T. Yoo and G. Smith, “On the Optimality of Multiantenna Broadcast Scheduling Using Zero-Forcing Beamforming”, *IEEE J. Select. Areas Commun.*, vol. 24, no. 3, pp. 528-541, Mar. 2006.

[10] G. Dimic and N.D. Sidiropoulos, “On downlink beamforming with greedy user selection: performance analysis and a simple new algorithm”, *IEEE Trans. Signal Processing*, vol. 53, no. 10, pp. 3857-3868, Oct. 2005.

[11] S. Sur, I. Pefkianakis, X. Zhang, and K. Kim, “Practical MU-MIMO User Selection on 802.11ac Commodity Networks,” in *Proc. ACM MobiCom*, 2016.

[12] Z. Chen, X. Zhang, S. Wang, Y. Xu, J. Xiong and X. Wang, “BUSH: Empowering Large-scale MU-MIMO in WLANs with Hybrid Beamforming,” in *Proc. IEEE INFOCOM*, 2017.

[13] WARP Project, http://warpproject.org

[14] R. Schmidt, “Multiple emitter location and signal parameter estimation”, *IEEE Trans. Antennas Propagat.*, vol. 34, no. 3, pp. 276-280, Mar. 1986.

[15] X. Xie and X. Zhang, “Scalable User Selection for MU-MIMO Networks,” in *Proc. IEEE INFOCOM*, 2015.

[16] W. Shen, K. Lin, M. Shen, and K. Tan, “SIEVE: Scalable User Grouping for Large MU-MIMO Systems,” in *Proc. IEEE INFOCOM*, 2015.

[17] A. Mukherjee and A. L. Swindlehurst, “Detecting passive eavesdroppers in the MIMO wiretap channel”, in *Proc. IEEE ICASSP*, 2012.

[18] S. Gollakota, S. David Perli, and D. Katabi, “Interference Alignment and Cancellation”, in *Proc. ACM SIGCOMM*, 2009.

[19] J. Guey and L.D. Larsson, “Modeling and evaluation of MIMO systems exploiting channel reciprocity in TDD mode”, in *Proc. of IEEE VTC*, 2004.

[20] J. Tsai, R. M. Buehrer, and B. D. Woerner, “The impact of AOA energy distribution on the spatial fading correlation of linear antenna array”, in *Proc. IEEE VTC*, 2002.

[21] J. Xiong, and K. Jamieson. “SecureArray: Improving wifi security with fine-grained physical-layer information”, in *Proc. ACM MobiCom*, 2013.