TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES
Trans. Emerging Tel. Tech. 2015; **26**:482–490
Published online 17 May 2013 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/ett.2657

RESEARCH ARTICLE

On singularity attacks in MIMO channels

S. Sodagari* and T. C. Clancy

Electrical and Computer Engineering Department, Virginia Tech, Arlington 22203, VA, USA

ABSTRACT

All multiple-input multiple-output (MIMO) systems need a method to estimate and equalise their channel, whether through channel reciprocity or sounding, and most modern orthogonal frequency division multiplexing (OFDM)-based MIMO waveforms use sounding via OFDM pilot tones. Previous research has focused on jamming data transmissions. We instead focus on jamming channel sounding symbols and introduce the MIMO singularity attack, which attempts to reduce the rank of the channel gain matrix estimate by the receiver through transmission of specific jamming signals. More specifically, we introduce and analyse the MIMO singularity attack, in which a multi-antenna jammer tries to manipulate pilot tones to skew the channel state information obtained at the receiver. We prove singularity jamming can be more destructive than data jamming attacks such as barrage or pilot jamming by studying its effects on channel bit error rate and capacity. We develop the constraints associated with jamming MIMO sounding channels and further describe how these attacks specifically impact data symbol estimates for OFDM pilot-based sounding systems. Through simulation, we demonstrate efficiency gains over barrage jamming. Copyright © 2013 John Wiley & Sons, Ltd.

***Correspondence**
S. Sodagari, Electrical and Computer Engineering Department, Virginia Tech, Arlington 22203, USA.
E-mail: shabnams@vt.edu

Received 5 October 2012; Revised 27 February 2013; Accepted 2 April 2013

1. INTRODUCTION

Because of the nature of wireless channels, which involves multipath fading, multiple-input multiple-output (MIMO) technology is a strong tool towards enhancing the performance and reliability of wireless communications, in terms of throughput and spectral efficiency, by taking advantage of diversity. In long term evolution, MIMO concept is being used in both downlink and uplink. However, like any communication system, MIMO channels have their own vulnerabilities in the presence of jamming.

In the majority of previous studies linked to jamming attacks against MIMO-enabled communications systems [1–9], there is a lack of investigation of efficient attacks against the portions of the signals that enable MIMO channel estimation and equalisation. Most of the work so far on MIMO attacks has focused on data or barrage jamming. Rather, less attention is being paid to exploiting pilot signals or the channel sounding process to jam MIMO communications. It is to be noted that, as mentioned in [10], targeting the channel sounding or accuracy of channel state information (CSI) estimation requires less power while being more efficient than barrage jamming at the same time.

Clancy *et al.* [11] discussed possibility of jamming the channel estimation procedure as an efficient type of attack. Following [11], jamming of channel estimation and equalisation was studied for single-input single-output communications [12] and MIMO channels [13]. Synchronisation issues related to MIMO channel sounding attack were discussed in [14]. Miller *et al.* [15] showed this type of attack can be applied to Alamouti space time codes, which are used as a basis of many protocol standards, such as 802.11n [15]. Also, different types of attacks on the channel sounding process in MIMO channels in low and high signal-to-noise ratio (SNR) regimes and their effects on constellation manipulation have been addressed in [10]. As a result, authenticating the channel estimation procedure is an effective countermeasure against this type of attack [16]. Our scheme [13, 14] is similar to channel rank attack briefly mentioned in [10]. However, we approach the attack on CSI estimation and perception of the channel response matrix from a different angle and present a more in-depth analysis and formulations on how this can be accomplished and the effects it will have on the MIMO channel capacity and eigenmodes.

The distinction of our work lies mainly in introducing the *MIMO singularity attack*, which seeks to introduce artificial singularities in the perception of the channel gain matrix in a MIMO communication link and studies its effect on MIMO capacity and perceived singular values along with bit error rate (BER). When the channel

is estimated by the receiver's equaliser, this manipulated state will induce a significant number of bit errors in the underlying signals upon demodulation. This work builds upon previous work targeting orthogonal frequency division multiplexing (OFDM) pilot tones [12] and is fundamentally different from previous research on spatial jamming because rather than focusing on the MIMO channel itself, we target attacks against the receiver's *perception* of the channel. This allows us to achieve significant efficiency gains over directly jamming data transmissions with lower jamming power. We also benchmark the capacity degradation effects that each type of jamming technique can have on MIMO channels.

The remainder of this paper is organised as follows. Section 2 details jamming attacks specifically targeting CSI measurement. Section 3 details the specific MIMO singularity attack as applied to OFDM-enabled MIMO communications systems. Section 4 discusses the effects of singularity attack on the capacity of MIMO channels. Section 5 contains numerical results from simulations of various attacks. Section 6 concludes. Table I includes the notation for most frequently used variables in this paper.

2. ANALYSIS OF JAMMING IN MULTIPLE-INPUT MULTIPLE-OUTPUT CHANNELS

Consider a MIMO communication system as in Figure 1. We seek to *efficiently* jam it. We measure our efficiency relative to *barrage jamming*, where the attacker barrage jams all symbols by transmitting additive white Gaussian noise (AWGN) to degrade received SNR. When the adversary has no knowledge of target signal, this type of attack is proven to be the best strategy [17]. In Section 5, we use this type of attack as a benchmark in evaluating the destructive effects of pilot jamming and pilot singularity attacks on MIMO channels.

fOR OUR Analysis, we assume a narrowband MIMO channel model with flat fading, which is a reasonable assumption for OFDM-based waveforms where individual subcarriers have channel bandwidth significantly less than the coherence bandwidth of the fading channel. Although the model developed in this section is not OFDM-specific, we will employ an OFDM waveform in Section 3 for developing a more specific version of our attack.

Table I. Notation.

$\mathbf{H}$	MIMO channel between transmitter and receiver
$\mathbf{J}$	Matrix of attack signals
$\mathbf{P}$	Matrix of sounding symbols
$\mathbf{S}$	Received sounding signals
$\mathbf{G}$	MIMO channel between jammer and receiver
$\hat{\mathbf{H}}$	Receiver's estimation of $\mathbf{H}$
$\hat{\mathbf{H}}_J$	Jammer's estimation of $\mathbf{H}$
$\hat{\mathbf{G}}_J$	Jammer's estimation of $\mathbf{G}$
$\check{\mathbf{H}}$	Receiver's perception of $\mathbf{H}$ under attack

MIMO, multiple-input multiple-output.

In this model, the transmitter transmits $\mathbf{x}$, a length-M vector of transmit symbols. They pass through channel $\mathbf{H}$, an $N \times M$ matrix of pairwise channel gains, and are affected by AWGN $\mathbf{n}$, a length-N vector. The received signal $\mathbf{y}$ is a length-N vector. Mathematically, this can be expressed as

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

where $\mathbf{n}$ is an additive white circularly symmetric complex Gaussian noise vector with N elements and in a Rayleigh fading environment, real and imaginary parts of elements of matrix $\mathbf{H}$ are independent normal Gaussian distributed. If without loss of generality, we assume the additive white circularly symmetric complex Gaussian noise vector is normalised; its covariance matrix is the identity matrix. Also, in this case, the average power constraint P across all transmitter antennas, which should satisfy $E\{\mathbf{x}\mathbf{x}^*\} \leqslant P$, will be equal to the SNR.

We denote the estimated values of $\mathbf{x}$ and $\mathbf{H}$ by $\hat{\mathbf{x}}$ and $\hat{\mathbf{H}}$, respectively.

To equalise the underlying signal, the channel gain matrix is estimated through a process called channel sounding. In channel sounding, known data is transmitted over a series of symbols in a spatially orthogonal way such that the receiver can estimate the channel response. For example, in OFDM-based systems employing MIMO, the OFDM pilot tones are typically used for this purpose; for example, certain pilot tones are used by certain antennas at certain times to estimate the channel state.

Here, we introduce the *singularity attack*, where the jammer tries to manipulate the channel matrix estimation at the receiver by turning it into a singular matrix. This way, the noise term asymptotically approaches infinity, and transmitted signal will be buried in noise at the receiver.

We consider a jammer having approximate estimates of h_{ij} or the elements of channel matrix $\mathbf{H}$ and adjust its transmitted signal $\mathbf{J}$ through channel $\mathbf{G}$ (which is the MIMO channel between jammer and receiver antennas), such that the overall channel matrix appearing to receiver antennas becomes singular with no inverse. Hence, the receiver will not be able to estimate what $\mathbf{x}$ was transmitted.

As an efficient jammer, we seek to influence the estimate of $\mathbf{H}$ and accordingly its singular values. This way the transmitter assigns wrong waterfilled power levels to channel eigenmodes, because of its miss-estimation of eigenvalues, resulting in degraded capacity.

More concretely, let $\mathbf{P}$ be an $M \times M$ matrix of sounding symbols. Each column represents values transmitted on a particular antenna, and each row represents values transmitted at a particular orthogonal spectral–temporal channel. For single-carrier modulations, these could be different symbols, and for multi-carrier modulations, they could be different subcarriers.

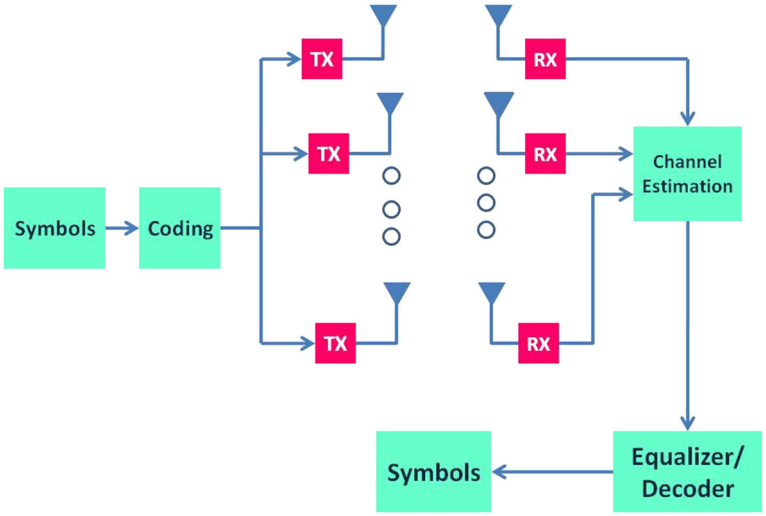

Figure 1. Block diagram of a MIMO communication system.

Next, let $\mathbf{J}$ be a $K \times M$ matrix of attack symbols using K transmit antennas over the same M orthogonal spectral–temporal channels as used by the transmitter. Let $\mathbf{G}$ be the $N \times K$ matrix of channel gains between the K-antenna jammer and the N-antenna receiver.

The received sounding signals $\mathbf{S}$ is an $N \times M$ matrix and is equal to

$$\mathbf{S} = \mathbf{HP} + \mathbf{GJ} + \mathbf{N} \tag{2}$$

where $\mathbf{N}$ is AWGN. The receiver estimates the channel gain matrix by computing

$$\begin{aligned} \hat{\mathbf{H}} &= \mathbf{SP}^{-1} \\ &= (\mathbf{HP} + \mathbf{GJ} + \mathbf{N})\mathbf{P}^{-1} \\ &= \mathbf{H} + \mathbf{GJP}^{-1} + \mathbf{NP}^{-1} \end{aligned} \tag{3}$$

Ignoring the noise term, our goal is to select $\mathbf{J}$ that minimises rank$(\mathbf{H} + \mathbf{GJP}^{-1})$. Because the rank of $\mathbf{H}$ cannot exceed its dimensionality, if $K \geqslant \min(M, N)$, we have enough degrees of freedom to arbitrarily change $\hat{\mathbf{H}}$, subject to the constraints of the AWGN term.

In the overdetermined case where $K \geqslant \min(M, N)$, then we can transmit

$$\mathbf{J} = -\mathbf{G}^{-1}\mathbf{HP} \tag{4}$$

where $\mathbf{G}^{-1}$ is the Moore–Penrose pseudoinverse of matrix $\mathbf{G}$. In the underdetermined case, our ability to affect the rank of $\hat{\mathbf{H}}$ will be limited. In general, we can reduce the rank of $\hat{\mathbf{H}}$ to $\max(0, \min(M, N) - K)$ assuming $\mathbf{G}$ and $\mathbf{H}$ are full rank.

There are several means for the jammer to estimate the $\mathbf{G}$ channel. For example, as shown in Figure 2, in full duplex mode, through the knowledge of deployed wireless protocol such as WiMAX, the jammer can synchronise to

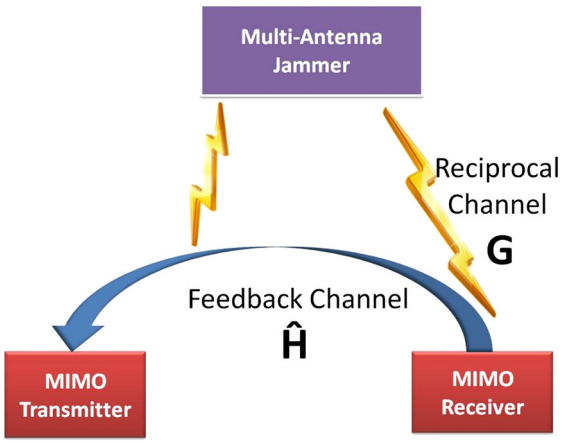

Figure 2. Jammer's estimation of **H** and **G** channels.

OFDM pilot tones. The jammer receives $\mathbf{GP}$ for pilot tones sent, and through the knowledge of $\mathbf{P}$ from the protocol standard, it can estimate channel $\mathbf{G}$. Also, the backward and forward reciprocity of $\mathbf{G}$ in time division duplex case can be used by the jammer to estimate $\mathbf{G}$ according to what is being received over this channel. This attack takes advantage of knowledge of standards for typical MIMO communication systems, such as WiMAX [18]. For the nonideal case of imperfect knowledge of the jammer, we derive performance bounds of destructive effects of this attack on MIMO communication.

Synchronisation of the adversary to pilot tones, which is important for this jamming method to be successful, is attainable with current software defined radio technologies, especially for synchronous protocols [10], such as 802.11n. We have comprehensively addressed the effects of time and frequency synchronisation misalignments on the performance of the pilot singularity attack in [14].

Trans. Emerging Tel. Tech. **26**:482–490 (2015)
DOI: 10.1002/ett

3. SINGULARITY ATTACK TO ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING BASED MULTIPLE-INPUT MULTIPLE-OUTPUT

In this section, we focus on waveforms employing OFDM and MIMO technologies, such as Mobile WiMAX (IEEE 802.16e), WiMAX2 (IEEE 802.16m) and E-UTRAN, the air interface specified for 3GPP long term evolution. In these systems, during each OFDM symbol, a fraction of the subcarriers are used as pilot tones. Pilot tones are used to calculate the frequency response of the channel across all subcarriers, and in MIMO-enabled versions of OFDM, each pilot tone is only used by a single transmit antenna. For example, in a system with two transmit antennas, even pilot tones might carry pilot data for antenna 1, whereas odd pilot tones might carry pilot data for antenna 2.

Figure 3 shows *matrix B* mode of Mobile WiMAX, which uses 2×2 MIMO with no space–time coding. The transmitter antennas 1 and 2 send pilot signals P_1 and P_2, respectively, at different times and frequencies; that is, for a specific pilot frequency, signals $(P_1, 0)$ and $(0, P_2)$ are sent from antennas in two different subcarriers and/or symbols. As such, the coefficients of 2×2 matrix $\hat{\mathbf{H}}$ are calculated at the receiver for a specific frequency. As this channel sounding procedure is repeated, we obtain different 2×2 channel coefficient matrices, each for a different pilot frequency.

$$\begin{bmatrix} \hat{h}_{11}^{P_m} & \hat{h}_{12}^{P_m} \\ \hat{h}_{21}^{P_m} & \hat{h}_{22}^{P_m} \end{bmatrix} \tag{5}$$

To obtain the values of the channel matrix at a frequency other than pilot tones P_m, we interpolate between values of $h_{ij}^{P_m}$.

$$\hat{h}_{ij}^{f} = \frac{1}{P_{m+1} - P_m}\left(\hat{h}_{ij}^{P_m}(P_{m+1} - f) + \hat{h}_{ij}^{P_{m+1}}(f - P_m)\right) \tag{6}$$

The previous interpolation introduces some error. Interpolation methods such as spline and polynomial can also be used rather than linear. However, they do not result in significant error reduction, as compared with linear interpolation [12].

In the 2×2 WiMAX MIMO case, we consider a singularity or singularity attack by a jammer sending its signal through channel $\mathbf{G}$ and having approximate estimates of channel gain matrices $\mathbf{H}$ and $\mathbf{G}$ (as shown in Figure 4).

For equalisation, and in case the distributions of channel noise and MIMO channel are not known, the channel matrix can be estimated by least square estimator (LSE) [19] as

$$\mathbf{H}_{\text{LSE}} = \mathbf{Y}\mathbf{P}^*(\mathbf{P}\mathbf{P}^*)^{-1} \tag{7}$$

where $(\cdot)^*$ denotes the conjugate transpose.

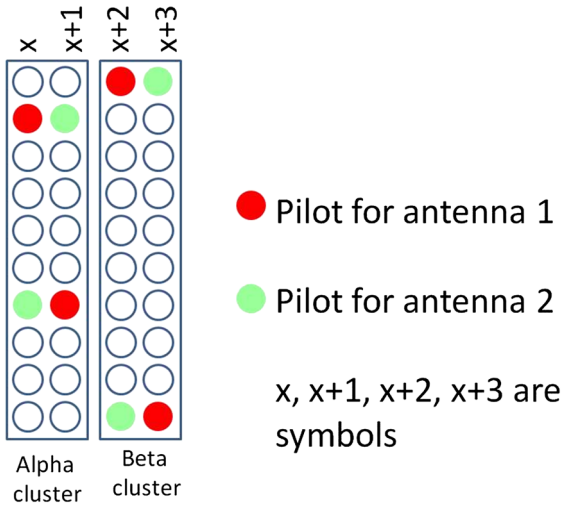

Figure 3. Pilots in a 2×2 WiMAX OFDM.

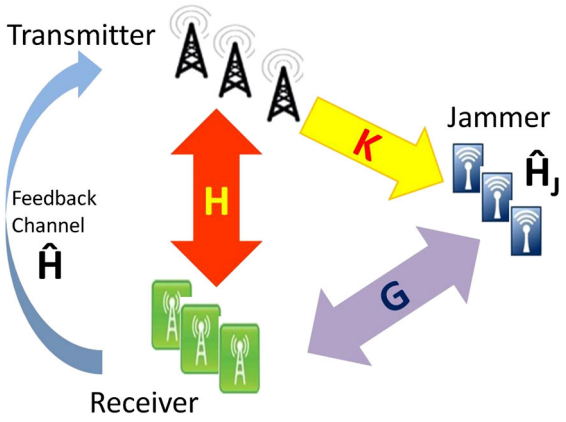

Figure 4. Multi-antenna pilot jamming attack on MIMO systems. **H**, **K** and **G** denote the channels between transmitter/receiver, transmitter/jammer and receiver/jammer, respectively. $\hat{\mathbf{H}}$ is receiver's estimated CSI of **H** fed back to the transmitter.

4. EFFECT OF PILOT JAMMING ON MULTIPLE-INPUT MULTIPLE-OUTPUT CAPACITY

The mutual information of $\mathbf{H}$ and $\hat{\mathbf{H}}$ varies as $0 \leqslant I\left(\mathbf{H}; \hat{\mathbf{H}}\right) \leqslant H(\mathbf{H})$, where $H(\mathbf{H})$ is the entropy of channel matrix $\mathbf{H}$. The jammer's estimates of $\mathbf{H}$ and $\mathbf{G}$ are denoted by $\hat{\mathbf{H}}_J$ and $\hat{\mathbf{G}}_J$, respectively. The jammer aims at increasing $I\left(\hat{\mathbf{H}}_\mathbf{J}; \mathbf{H}\right)$ and decreasing $I\left(\hat{\mathbf{H}}; \mathbf{H}\right)$ as much as possible. In fact, $I\left(\hat{\mathbf{H}}; \mathbf{H}\right) = 0$ is the ideal goal for the jammer, as in Figure 5, because this implies $\mathbf{H}$ and its estimate at the receiver $\hat{\mathbf{H}}$ does not resemble each other, whereas the receiver desires the channel estimate $\hat{\mathbf{H}}$ to be as close as possible to $\mathbf{H}$.

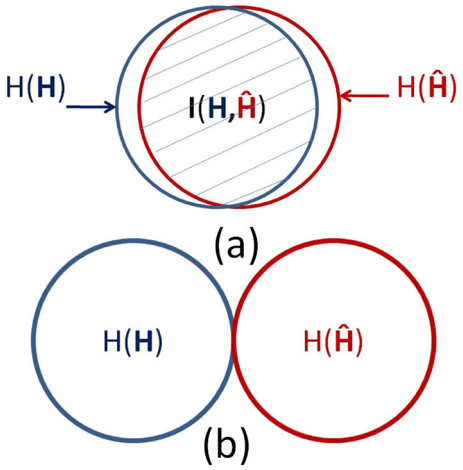

Figure 5. (a) Mutual information between MIMO channel matrix and its estimate with no jamming. (b) Jammer's ideal goal in manipulating MIMO CSI at the receiver.

Figure 4 shows a MIMO singularity attack scenario in which the multi-antenna jammer tries to estimate the full-duplex channel response from transmitter to the receiver, $\mathbf{H}$, by listening to the feedback channel that contains the receiver's estimate of $\mathbf{H}$ denoted by $\hat{\mathbf{H}}$. The jammer also tries to listen to the transmitter through channel $\mathbf{K}$ jammer. The singularity attack is then performed on the receiver through channel $\mathbf{G}$. Estimation of number of transmitter and receiver antennas by an unauthorised or cognitive terminal can be performed using the information theoretic criteria of minimum descriptor length and Akaike information criterion (AIC). For a detailed explanation, interested reader is referred to [20].

By pilot manipulation attack, the jammer changes the knowledge about true singular values σ_i, to the extent that its estimations of $\mathbf{H}$ and $\mathbf{G}$ channels are accurate. Accordingly, water-filling weights are manipulated resulting in capacity decrease proportional to α, which is the relative jammer channel estimation accuracy.

In Rayleigh fading, if the distance between the jammer J and the receiver is greater than the coherence distance of the fading environment, $\mathbf{K}$ and $\mathbf{H}$ are statistically independent.

4.1. Pilot jamming effect on capacity of single user multiple-input multiple-output channels

The constant MIMO channel capacity of single user MIMO channels with singular values of channel matrix $\mathbf{H}$ denoted by σ_i, and rank of $\mathbf{H}$ denoted by R_H can be written as

$$C = \sum_{i=1}^{R_H} (\log(\mu\sigma_i))^+ \tag{8}$$

where the function $(x)^+ = \max\{x, 0\}$ and the waterfill level μ is chosen such that $\sum_{i=1}^{R_H} P_i = P$. Here, P_i is the power allocated to each parallel non-interfering channels acquired by the singular value decomposition of channel $\mathbf{H}$, and P is the average power constraint across all transmitter antennas, as mentioned in Section 2.

Under jamming attack Equation (8) can be written as

$$\begin{aligned}
C &= \sum_{i=1}^{R_{\check{H}}} \left(\log\left(\mu\check{\sigma}_i^2\right)\right)^+ \\
&\leqslant R_{\check{H}} \log\mu + \sum_{i=1}^{R_{\check{H}}} \log\check{\sigma}_i^2 \\
&= R_{\check{H}} \log\mu + \log\prod_{i=1}^{R_{\check{H}}} \check{\sigma}_i^2 = R_{\check{H}} \log\mu + \log\left(\det\left(\check{\mathbf{H}}\check{\mathbf{H}}^*\right)\right) \\
&= R_{\check{H}} \log\mu + \log\left(\det\left(\check{\mathbf{H}}\right)\det\left(\check{\mathbf{H}}^*\right)\right) \\
&= R_{\check{H}} \log\mu + \log\left(\det\left(\check{\mathbf{H}}\right)\left(\det\left(\check{\mathbf{H}}\right)\right)^*\right) \\
&= R_{\check{H}} \log\mu + \log\left(\left|\det\left(\check{\mathbf{H}}\right)\right|^2\right) \\
&= R_{\check{H}} \log\mu + 2\log\left(\left|\det\left(\check{\mathbf{H}}\right)\right|\right)
\end{aligned} \tag{9}$$

where $\left|\det\left(\check{\mathbf{H}}\right)\right|$ denotes the magnitude of determinant of matrix $\check{\mathbf{H}}$.

Equation (9) implies that we need to have knowledge of the rank and the determinant of matrix $\check{\mathbf{H}}$ to calculate the MIMO capacity under jamming attack. The following propositions and corollary give insight into how the determinant and rank of MIMO channel matrix are affected by a singularity attack.

Proposition 1. $\left(\textit{Upper bound on rank } \check{\mathbf{H}}\right)$ $R_{\check{H}} < R_H$

Proof. Subadditivity property of rank yields $R_{\check{H}} \leqslant R_H - \text{rank}\left(\mathbf{G}\hat{\mathbf{G}}_J^{-1}\hat{\mathbf{H}}_J\right)$. On the other side, $\mathbf{G}\hat{\mathbf{G}}_J^{-1}\hat{\mathbf{H}}_J \neq \mathbf{0}$, and therefore, $\text{rank}\left(\mathbf{G}\hat{\mathbf{G}}_J^{-1}\hat{\mathbf{H}}_J\right) > 0$. □

Corollary 1. $\check{\mathbf{H}}$ *is a singular matrix.*

Proof. We showed $R_{\check{H}} < R_H$, and because $\check{\mathbf{H}}$ and $\mathbf{H}$ are of the same size, $\check{\mathbf{H}}$ cannot be full rank and is hence noninvertible. □

The previous property provides the MIMO singularity attacker with the capability of hindering channel equalisation at the receiver, even if the jammer cannot accurately estimate the $\mathbf{H}$ and $\mathbf{G}$ channels.

Proposition 2. *If both* $\mathbf{H}$ *and* $\mathbf{G}$ *are uncorrelated MIMO channels or continuous fading distribution channels, for*

Trans. Emerging Tel. Tech. **26**:482–490 (2015)
DOI: 10.1002/ett

the special case of equal number of transmitter, receiver and jammer antennas, we will have

$$\det\left(\breve{\mathbf{H}}\right) = \det\left(\mathbf{H} - \mathbf{G}\hat{\mathbf{G}}_J^{-1}\hat{\mathbf{H}}_J\right) = \left(\det\left(\hat{\mathbf{G}}_J - \hat{\mathbf{H}}_J\mathbf{H}^{-1}\mathbf{G}\right)\right)\left(\det\left(\hat{\mathbf{G}}_J^{-1}\right)\right)(\det(\mathbf{H})) \tag{10}$$

Proof. If $\mathbf{H}$ and $\mathbf{G}$ are each uncorrelated MIMO channels or channels with continuous fading distributions, then they are full rank [20], and equality of the number of antennas implies they are square matrices. Therefore, $\mathbf{H}$, $\mathbf{G}$ and accordingly $\mathbf{G^{-1}}$ are invertible, and the matrix determinant lemma [21] yields equation (10). □

Inserting Equation (10) into Equation (9), the perceived (illusional) capacity due to singularity attack at the transmitter is given by

$$\begin{aligned} C &= R_{\breve{H}} \log\mu + \\ &2\log\left(\left|\det\left(\hat{\mathbf{G}}_J - \hat{\mathbf{H}}_J\mathbf{H}^{-1}\mathbf{G}\right)\right|\left|\det\left(\hat{\mathbf{G}}_J^{-1}\right)\right||\det(\mathbf{H})|\right) \\ &= R_{\breve{H}}\log\mu + 2\log\left(\left|\det\left(\hat{\mathbf{G}}_J - \hat{\mathbf{H}}_J\mathbf{H}^{-1}\mathbf{G}\right)\right|\right) \\ &\quad + 2\log\left(\left|\det\left(\hat{\mathbf{G}}_J^{-1}\right)\right|\right) + 2\log(|\det(\mathbf{H})|) \end{aligned} \tag{11}$$

The previous property misleads the transmitter in selecting the waterfill levels for channel eigenmodes, which eventually affects the received signal in a destructive manner. This is in accordance with the system implementation of water-filling attack in [10] where in case of perfect CSI, jammer should use a matched water-filling strategy, whereas with partial CSI, the jammer should beamform in the direction of the transmit eigenvectors and perform proportional power allocation.

We note that singular values of $\mathbf{H}$ and $\breve{\mathbf{H}}$ are the square roots of the nonzero eigenvalues of $\mathbf{HH}^*$ and $\breve{\mathbf{H}}\breve{\mathbf{H}}^*$, respectively if $M \geqslant N$. Otherwise, we consider $\mathbf{H}^*\mathbf{H}$ and $\breve{\mathbf{H}}^*\breve{\mathbf{H}}$. Therefore, next we proceed with analysing the effects of pilot singularity attack on eigenvalues of $\breve{\mathbf{H}}\breve{\mathbf{H}}^*$ as compared with the original channel eigenvalues or $\mathbf{HH}^*$.

$$\begin{aligned} \breve{\mathbf{H}}\breve{\mathbf{H}}^* &= \left(\mathbf{H} - \mathbf{G}\hat{\mathbf{G}}_J^{-1}\hat{\mathbf{H}}_J\right)\left(\mathbf{H} - \mathbf{G}\hat{\mathbf{G}}_J^{-1}\hat{\mathbf{H}}_J\right)^* \\ &= \left(\mathbf{H} - \mathbf{G}\hat{\mathbf{G}}_J^{-1}\hat{\mathbf{H}}_J\right)\left(-\hat{\mathbf{H}}_J^*\hat{\mathbf{G}}_J^{-1^*}\mathbf{G}^* + \mathbf{H}^*\right) \\ &= \mathbf{HH}^* + \mathbf{G}\hat{\mathbf{G}}_J^{-1}\hat{\mathbf{H}}_J\hat{\mathbf{H}}_J^*\hat{\mathbf{G}}_J^{-1^*}\mathbf{G}^* \\ &\quad - \left(\mathbf{GG}^{-1}\hat{\mathbf{H}}_J\mathbf{H}^* + \mathbf{H}\hat{\mathbf{H}}_J^*\hat{\mathbf{G}}_J^{-1^*}\mathbf{G}^*\right) \\ &= \mathbf{HH}^* + \mathbf{A} \end{aligned} \tag{12}$$

Because $\mathbf{HH}^*$ and $\mathbf{A}$ are each Hermitian, according to Weyl's theorem [22], if we let eigenvalues $\lambda_i(\mathbf{HH}^*)$ and $\lambda_i(\mathbf{A})$ and $\lambda_i(\mathbf{HH}^* + \mathbf{A})$ be arranged in increasing order, then for each $k = 1, 2, \ldots, n$

$$\begin{aligned} &\lambda_k(\mathbf{HH}^*) + \lambda_1(\mathbf{A}) \\ &\leqslant \lambda_k(\mathbf{HH}^* + \mathbf{A}) \\ &\leqslant \lambda_k(\mathbf{HH}^*) + \lambda_n(\mathbf{A}) \end{aligned} \tag{13}$$

Also,

$$\lambda_k(\mathbf{HH}^* + \mathbf{A}) \leqslant \min\{\lambda_i(\mathbf{HH}^*) + \lambda_j(\mathbf{A}) : i + j = k + n\} \tag{14}$$

Proposition 3. *The MIMO pilot singularity attack affects the singular values of the channel response according to the following equation*

$$\sigma_{i+j-1}\left(\breve{\mathbf{H}}\right) \leqslant \sigma_i(\mathbf{H}) - \sigma_i\left(\mathbf{G}\hat{\mathbf{G}}_J^{-1}\hat{\mathbf{H}}_\mathbf{J}\right) \tag{15}$$
$$1 \leqslant i, j \leqslant \min\{N, M\}$$
$$i + j \leqslant \min\{N, M\} + 1$$

Proof. The proof stems from Weyl's theorem and using the eigenvalues of

$$\begin{bmatrix} 0 & \breve{\mathbf{H}} \\ \breve{\mathbf{H}}^* & 0 \end{bmatrix}$$

For a rigorous proof, Cf. [23,24]. □

Equations (12)–(15) hold for arbitrary numbers of transmit, receive and jammer antennas.

The attacker's ideal goal is to have 100% accuracy in its estimations. Nevertheless, because of noise and the attacker's distance from transmitter and receiver, inaccuracies are inevitable in $\hat{\mathbf{H}}_J$. In other words,

$$\hat{\mathbf{H}}_J = \boldsymbol{\alpha}\mathbf{H} + \boldsymbol{\beta} \tag{16}$$

where β is the noise vector $\beta \sim \mathcal{CN}(0, \sigma^2)$ and α is the relative error. When $\mathbf{P} = \mathbf{I}p$, its inverse $\mathbf{P}^{-1} = \mathbf{I}/p$, and the jammer estimates the channel response by

$$\begin{aligned} \hat{\mathbf{H}} &= [(\boldsymbol{\alpha}\mathbf{H} + \boldsymbol{\beta})\mathbf{P} + \mathbf{N}]\mathbf{P}^{-1} \\ &= \boldsymbol{\alpha}\mathbf{H} + \boldsymbol{\beta} + \mathbf{N}/p \\ &= \boldsymbol{\alpha}\mathbf{H} + (\boldsymbol{\beta} + \mathbf{N}/p) \end{aligned} \tag{17}$$

$$(\boldsymbol{\beta} + \mathbf{N}/p) \sim \mathcal{CN}\left(0, \sigma^2\left(\frac{p^2+1}{p^2}\right)\right) \tag{18}$$

In the fully informed case, $\alpha = \mathbf{I}$ or identity matrix.

$$\mathbf{J} = -\mathbf{G}^{-1}(\mathbf{H} + \boldsymbol{\beta})\mathbf{P} \tag{19}$$

The received signal then becomes

$$\begin{aligned} \mathbf{S} &= \mathbf{HP} + \mathbf{GJ} + \mathbf{N} \\ &= \mathbf{HP} - \mathbf{GG}^{-1}(\mathbf{H} + \boldsymbol{\beta})\mathbf{P} + \mathbf{N} \end{aligned} \tag{20}$$

We note that in the fully informed case, the received signal becomes $\mathbf{S} = \mathbf{N}$, that is, merely noise, which neutralises the effect of pilot tones at the receiver.

In Section 5, we verify the validity of previous propositions, through simulations.

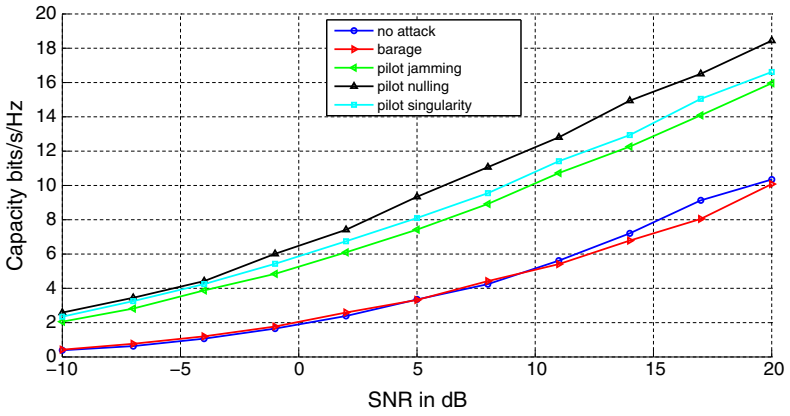

Figure 6. Comparison of perceived MIMO capacity versus SNR with and without different jamming strategies for a 2 × 2 WiMAX (with 20% error in jammer's estimation of CSI).

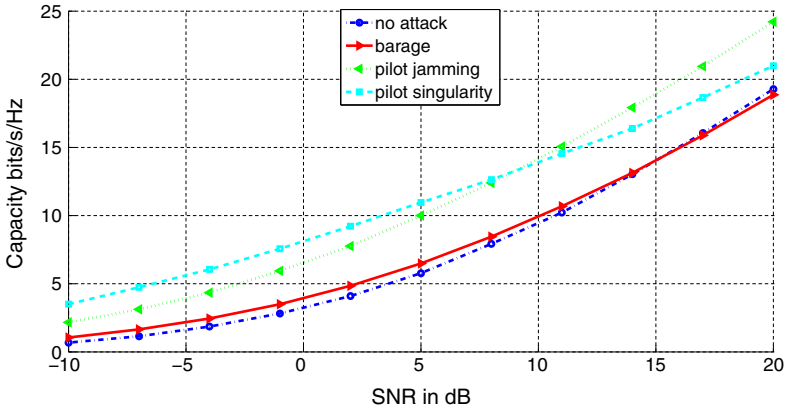

Figure 7. Comparison of perceived MIMO capacity in a 4×4 WiMAX versus SNR with and without different jamming strategies (20% error in jammer's CSI estimation).

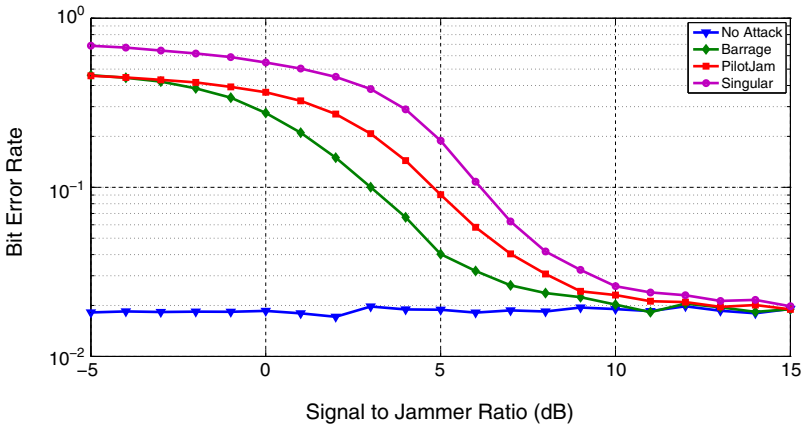

Figure 8. Performance of the three MIMO jamming methods as a function of signal to jammer ratio (SJR) at WiMAX OFDM receiver antennas for the target signal operating at 20 dB SNR with 20% error in knowledge of CSI.

Trans. Emerging Tel. Tech. **26**:482–490 (2015) © 2013 John Wiley & Sons, Ltd.
DOI: 10.1002/ett

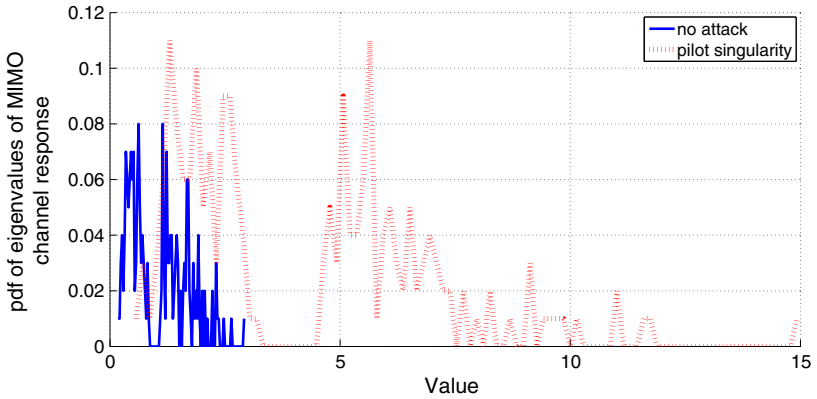

Figure 9. Effect of singularity jamming (with 20% error in CSI estimation) on manipulation of MIMO channel eigenvalues.

5. SIMULATION RESULTS

Our simulations were developed on the basis of the 2×2 WiMAX OFDM channel model of Figure 3 (and its 4×4 extension) with CSI feedback to the transmitter. Simulations were carried out for 1000 Monte Carlo iterations. The data is quadrature phase shift keyed, and data and pilot tones are passed through inverse fast Fourier transform (FFT) and then sent over an eight-tap random channel with AWGN. The FFT in OFDM modulation is 256-point with a cyclic prefix length of 1/8, and every fourth subcarrier is a pilot (half of the pilots are dedicated to antenna 1, and the other half to antenna 2). Attack signal from a two-antenna jammer is added to the received signal after being passed through a channel with different filter tap coefficients. Received signal is then passed through FFT.

Figure 6 shows the MIMO capacity for a 2×2 WiMAX system as perceived by the transmitter, through estimated channel response fed back from the receiver using water-filling. The capacity shown in Figure 6 is averaged over all pilot tones. The jammer also has two antennas, and the jammer to signal ratio is assumed to be 10 dB. Figure 7 contains same information but for a 4×4 WiMAX system and 4-antenna jammer. Pilot nulling refers to the type of attack that inverts the pilot tones by using a jamming signal that is the π-radian offset of the transmitted pilot tone value [12]. Barrage jamming is the simplest type of attack, in which noise signals are sent to degrade received SNR.

Figure 8 compares the BER performance in the presence of singularity attack, pilot jamming and barrage jamming. Results in this figure were acquired for a 2×2 WiMAX at 10 dB SNR.

There are consistencies among the BER and capacity perception graphs in that the order of attack type in term of BER degradation is the same in misleading capacity perception of the transmitter. For example, singularity jamming results in the highest perceived capacity in Figure 6 and simultaneously in the worst BER performance in Figure 8. Figure 9 shows how pilot singularity shifts the perceived eigenvalues of MIMO channel with regard to actual eigenvalues that accordingly affects the water-filling in the transmitter. As evident in this figure, the singularity attack deceptively shows the channel eigenvalues to be higher, such that the transmitter increases its rate misled by the assumption that the capacity is higher. This results in receiver saturation and worsens the BER performance.

6. CONCLUSION

We introduced a new type of attack on MIMO channels, which we called the *singularity attack*. In this attack, the adversary tries to manipulate the perception of CSI at the receiver and accordingly at the transmitter (when the feedback channel exists from receiver to transmitter). The jammer performs this by sending signals synchronous with pilot tones and adjusting them in a way that they cancel out the received pilot tones. As such, the receiver is misled in estimating the MIMO channel response resulting in higher BER. When this misestimated CSI is fed back to the transmitter, the MIMO channel capacity perception of the transmitter is also skewed, which results in water-filling with falsified eigenvalue information. This in turn, worsens the overall throughput. We showed singularity attack can be more effective than barrage jamming, pilot jamming and pilot singularity attacks in terms of BER degradation and deceptive channel capacity perception.

As was shown in our analysis, the more accurate the jammer's estimation of the responses of the two MIMO channels, that is, transmitter/receiver and jammer/receiver, the worse the effects of the attack. Therefore, to mitigate the singularity attack, the transmitter–receiver pair should make it difficult for a third party to have access to their CSI. In other words, the communications between the transmitter and the receiver should appear to have an unlearnable structure from outside.

REFERENCES

1. Wang J, Swindlehurst AL. Cooperative jamming in MIMO ad-hoc networks, In *Forty-Third Asilomar Conference on Signals, Systems and Computers*, California, November 2009; 1719–1723.
2. Mukherjee A, Swindlehurst AL. Equilibrium outcomes of dynamic games in MIMO channels with active eavesdroppers, In *IEEE International Conference on Communications (ICC)*, Cape Town, May 2010; 1–5.
3. Asadullah G, Stüber GL. Joint iterative channel estimation and soft-chip combining for a MIMO MC-CDMA anti-jam system. *IEEE Transactions on Communications* 2009; **57**(4): 1068–1087.
4. Mehdi H, Teh KC, Li KH. Analysis of MIMO band-limited DS-CDMA systems in the presence of multi-tone jamming over generalized-K fading channels. *IEEE Transactions on Vehicular Technology* 2009; **58**(7): 3825–3829.
5. Chi DW, Das P. Effects of jammer and nonlinear amplifiers in MIMO-OFDM with application to 802.11n WLAN, In *IEEE Military Communications Conference*, San Diego, November 2008; 1–8.
6. Farahmand S, Cano A, Giannakis GB. Anti-jam distributed MIMO decoding using wireless sensor networks, In *IEEE International Conference on Acoustics, Speech and Signal Processing*, Nevada, November 2008; 2257–2260.
7. Yang L-L. Joint transmitter-receiver design in TDD multiuser MIMO systems: an egocentric/altruistic optimization approach, In *IEEE 65th Vehicular Technology Conference*, Dublin, 2007; 2094–2098.
8. Brady MH, Mohseni M, Cioffi JM. Spatially-correlated jamming in Gaussian multiple access and broadcast channels, In *40th Annual Conference on Information Sciences and Systems*, Princeton, 2006; 1635–1639.
9. Jorswieck EA, Boche H. Optimal transmitter and jamming strategies in Gaussian MIMO channels, In *IEEE 61st Vehicular Technology Conference*, Vol. 2, Stockholm, 2005; 978–982.
10. Miller R, Trappe W. On the vulnerabilities of CSI in MIMO wireless communication systems. *IEEE Transactions on Mobile Computing* 2012; **11**(8): 1386–1398.
11. Clancy TC, Georgen N. Security in cognitive; 852–856, radio networks: threats and mitigations, In *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, Singapore, May 2008; 1–8.
12. Clancy TC. Efficient OFDM denial: pilot jamming and pilot nulling, In *IEEE International Conference on Communications (ICC)*, Kyoto, June 2011; 1–5.
13. Sodagari S, Clancy TC. Efficient jamming attacks on MIMO channels, In *IEEE International Conference on Communications (ICC)*, Ottawa, June 2012.
14. Shahriar C, Sodagari S, Clancy TC. Performance of pilot jamming on MIMO channels with imperfect synchronization, In *IEEE International Conference on Communications*, Ottawa, June 2012; 898–902.
15. Miller R, Trappe W. Subverting MIMO wireless systems by jamming the channel estimation procedure, In *Proceedings of the Third ACM Conference on Wireless Network Security*, Hoboken, March 2010; 19–24.
16. Miller R, Trappe W. Short paper: ACE - authenticating the channel estimation process in wireless communication systems, In *Proceedings of the Fourth ACM Conference on Wireless Network Security (WiSec)*, Hamburg, June 2011; 91–96.
17. Basar T. The Gaussian test channel with an intelligent jammer. *IEEE Transactions on Information Theory* 1983; **29**(1): 152–157.
18. 802.16 Working Group. IEEE Std 806-16e-2005: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, 2006.
19. Biguesh M, Gershman A. Training-based MIMO channel estimation: a study of estimator tradeoffs and optimal training signals. *IEEE Transactions on Signal Processing* 2006; **54**(3): 884–893.
20. Somekh O, Simeone O, Bar-Ness Y, Su W. Detecting the number of transmit antennas with unauthorized or cognitive receivers in MIMO systems, In *IEEE Military Communications Conference (MILCOM)*, Orlando, October 2007; 1–5.
21. Harville DA. *Matrix Algebra from a Statistician's Perspective*. Springer-Verlag: New York, USA, 1997.
22. Weyl H. Das asymptotische Verteilungsgesetz der Eigenwerte linearer partieller Differentialgleichungen (mit einer Anwendung auf die Theorie der Hohlraumstrahlung). *Mathematische Annalen* 1912; **71**: 441–479.
23. Fan K. Maximum properties and inequalities for the eigenvalues of completely continuous operators. *Proceedings of the National Academy of Science* 1951; **37**(11): 760–766.
24. Gohberg IC, Krein MG. *Introduction to the Theory of Linear Nonselfadjoint Operators in Hilbert Space (Translations Of Mathematical Monographs)*. American Mathematical Society: Providence, RI, 1969.

DOI: 10.1002/ett