Extending Channel Comparison Based Sybil Detection to MIMO Systems

Yue Liu
University of Michigan
liuyue@umich.edu

David Bild
University of Michigan
drbild@umich.edu

Robert P. Dick
University of Michigan
dickrp@umich

ABSTRACT

Although wireless channel comparison based techniques have been shown to defeat Sybil attacks in wireless environments, most assume single-input single-output (SISO) models for the radio system. We consider extending wireless Sybil defenses to multi-input multi-output (MIMO) systems.

1. INTRODUCTION

Wireless channel comparison based Sybil defense techniques have been shown effective [1, 2, 3, 4, 5]. By comparing wireless channel conditions one may determine whether two (or more) transmissions originated from the same location and are thus likely to be part of a Sybil attack. The technique is based on the location uniqueness of wireless channels, i.e., even slightly different transmission locations experience uncorrelated wireless channel conditions [6].

Wireless channel comparison based Sybil defenses fall into the class of resource testing based Sybil defenses [7, 8]. In this case transmitter antennas are the resource. Specifically, a group of Sybil transmissions are detected because they demonstrate much less use of antennas (and thus much less wireless channel variations) than the same number of protocol-compliant transmissions.

Existing channel comparison techniques assume single input, single output (SISO) radio systems [1, 2, 3, 4, 5]. In this report we make an initial attempt to extend them to multi-input multi-output (MIMO) systems, which are becoming increasingly popular [9, 10]. Our approach also follows resource testing; we examine received signals to identify transmissions that demonstrate inadequate resource use, or more precisely, to identify numerous transmissions from the same device that claim to be coming from different identities.

Before going into technical details, we will present a mathematical model for MIMO systems and give an intuitive explanation for our technique.

1.1 Mathematical Model of MIMO Systems

Figure 1 illustrates a general MIMO system with n_T transmitters and n_R receivers. Note that the transmitters and receivers may or may not belong to the same MIMO antenna array. Assuming flat-fading or narrowband channels—which is a common

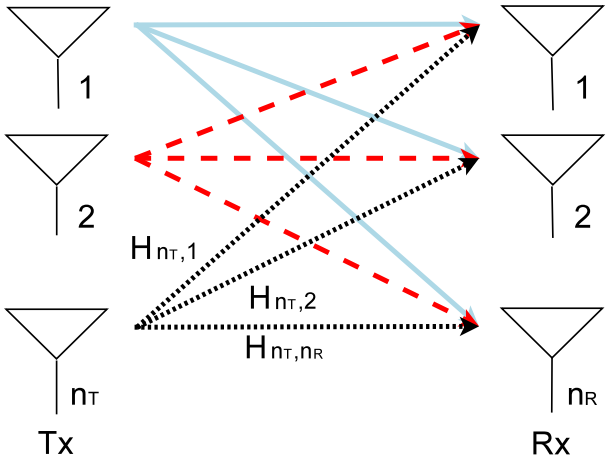

Figure 1: A MIMO system with n_T transmitters and n_R receivers.

practice, this system is modeled as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}. \quad (1)$$

All numbers here are in complex space. The n_T-dimensional vector $\mathbf{x}$ represents the transmitted signals and the n_R-dimensional vector $\mathbf{y}$ represents the received signals. $\mathbf{n}$ is the additive white noise. $\mathbf{H} \in \mathbb{C}^{n_R \times n_T}$ is the channel matrix, where $\mathbf{H}_{i,j}$ represents the channel from the jth transmitter to the ith receiver [10]. Note that $\mathbf{H}$ characterizes the wireless channels between the transceivers and is purely determined by the surrounding environment.

Equation 1 can be expanded as

$$\mathbf{y} = \sum_{j=1}^{n_T} \mathbf{h}_j x_j + \mathbf{n}, \quad (2)$$

showing that the received signals of a given MIMO system fall in the column space of its channel matrix $\mathbf{H}$. Since the channel matrix $\mathbf{H}$ is determined by the environment and a Sybil attacker can only change the transmitted signals (x_js) to create Sybil transmissions, this means all these Sybil transmissions fall into the same dimension n_T (at maximum) linear subspace of $\mathbb{C}^{n_R}$. On the other hand, transmissions originated from different MIMO devices fall into different linear subspaces because the corresponding channel matrices vary due to the spatial variations among wireless channels. We thus could decide whether a

group of transmissions are originated from the same MIMO system (and thus Sybil) by observing the linear subspace they span. This is the basic observation of our Sybil detection technique.

In the remaining parts of the paper, we first establish a basic assumption for channel matrix $\mathbf{H}$ in Section 2. We then proceed to tackle the particular Sybil detection problem. Section 3 formally sets up the problem. Section 4 then develops the observations and techniques for Sybil detection. Finally, Section 5 discusses practical considerations and future work.

2. CHANNEL MATRIX PROPERTIES

We have shown that the channel matrix $\mathbf{H}$ plays a critical role in the formation of received signals. Viewing each element $\mathbf{H}_{i,j}$ (i.e., the wireless channel from the jth transmitter to the ith receiver) as a random variable, Conjecture 1 establishes a basic assumption for $\mathbf{H}$.

Conjecture 1. *The channel matrix of a MIMO system has full rank if its wireless channels are all independently distributed.*

According to existing results, the probability that a square random matrix with all independent entries is singular quickly approaches zero when its size increases, and equals zero asymptotically [11, 12]. Conjecture 1 neglects this small probability and assumes a non-singular matrix for finite size random matrices, mainly for the ease of theoretical development. The rare singular cases do not invalidate our method, but do affect the performance negatively. We will leave the analysis to future experimental evaluations.

3. PROBLEM SETUP

A set of MIMO devices observe the wireless transmissions from another set of MIMO devices. The observing devices have n_R receiver antennas in total. There are two type of devices. Conforming devices only make one transmission each; we call these transmissions non-Sybil transmissions. Attacking devices make more than one transmissions each, and we call these transmissions Sybil transmissions. Our goal is to detect all the Sybil transmissions.

It is important to distinguish among two types of Sybil transmissions. If the number of Sybil transmissions an attacker makes is less than or equal to its number of transmitter antennas, then these Sybil transmissions are called *undetectable Sybil transmissions*. Otherwise, if the number of Sybil transmissions an attacker makes is greater than its number of transmitter antennas, these Sybil transmissions are called *detectable Sybil transmissions*. It will become evident in Section 4 that we are only able to identify detectable Sybil transmissions.

The following conditions are necessary for a wireless channel comparison based Sybil defense to work.

Condition 1. *An attacking device is stationary during its Sybil transmissions.*

Condition 1 is necessary because free device motion allows Sybil transmissions to experience different wireless channels. It is implicitly assumed by all previous channel comparison based Sybil defenses. We proposed a method to detect device motion in previous work, in case restricting it is impossible [**?**].

Condition 2. *The total number of receivers n_R is larger than the number of transmitters on any single attacking device.*

Condition 2 upper bounds the number of transmitters per device by n_R. N_T denotes the maximum number of transmitters per attacking device.

The following assumptions create an ideal world to simplify explanation and theoretical development.

1. All the wireless channels in the MIMO system are independent.
2. There is no noise in the system, i.e., $\mathbf{n} = \mathbf{0}$ in Equation 1 and Equation 2.

In reality both assumptions can be relaxed. For the first one, our method works as long as wireless channels from different MIMO devices are independent, which is commonly true thanks to the rich spatial variations of wireless channels [6]. For the second one, we leave it to future experiments to quantify the actual noise threshold.

4. SYBIL DETECTION

Section 1 suggested that we could detect a group of Sybil transmissions by observing that they demonstrate much less wireless channel variations and thus fewer transmitter antennas than a group of non-Sybil transmissions with equal size. In this section we detail the properties that allow us to make this distinction.

Lemma 1. *The received signals of any group of no more than $\lfloor \frac{n_R}{N_T} \rfloor$ non-Sybil transmissions are linearly independent.*

Proof. Use n to denote the total number of transmitters involved. $n \leq n_R$ because the total number of transmissions is no more than $\lfloor \frac{n_R}{N_T} \rfloor$ and each of them involves N_T transmitters at maximum.

Use $\mathbf{H}$ to represent a MIMO system with all these transmissions' transmitters and the given receivers. $\mathbf{H}$ can be written as

$$\mathbf{H} = (\ \mathbf{h}_1 \quad \mathbf{h}_2 \quad ... \quad \mathbf{h}_n\ ),$$

where $\mathbf{h}_i$ denotes the vector of wireless channels from the i-th transmitter to all the n_R receivers.

We now prove $\mathbf{h}_i$s are linearly independent. Since all the wireless channels in $\mathbf{H}$ are independent (see the first assumption in Section 3), according to Conjecture 1 $\mathbf{H}$ has full rank. Furthermore, since $\mathbf{H}$'s column size is smaller than or equal to its row size ($n \leq n_R$), the columns of $\mathbf{H}$ are linearly independent.

Finally, the received signals are linearly independent because they are linear combinations of $\mathbf{h}_i$s. □

Corollary 1. *It requires (the received signals of) at least $\lfloor \frac{n_R}{N_T} \rfloor$ non-Sybil transmissions to linearly expand (the received signal of) a non-Sybil transmission.*

Corollary 1 is just a restatement of Lemma 1. Because a group of Sybil transmissions only correspond to less (or equal) independent channel vectors than a group of non-Sybil transmissions of the same size, Corollary 1 can be generalized as follows.

Corollary 2. *It requires (the received signals of) at least $\lfloor \frac{n_R}{N_T} \rfloor$ transmissions to linearly expand (the received signal of) a non-Sybil transmission.*

So far Corollary 2 describes the features of non-Sybil transmissions. On the other hand, the following lemma describes the features of Sybil transmissions.

Lemma 2. *For any detectable Sybil transmission, there always exists a group of transmissions with size no more than N_T, whose received signals could linearly expand (the received signal of) that transmission.*

Proof. Since all Sybil transmissions from a same device fall into a linear subspace of dimension n_T (see Equation 2 in Section 2) and there are more than n_T detectable Sybil transmissions by definition, any group of $n_T + 1$ detectable Sybil transmissions are linearly dependent. In other words, any group of n_T ($n_T < N_T$) detectable Sybil transmissions from the same device could linearly expand a detectable Sybil transmission. □

Corollary 2 and Lemma 2 indicate that the size of linearly expanding transmission groups can be a distinguishing feature of Sybil vs. no-Sybil classifications, under a stricter condition of maximum number of transmitters per device.

Condition 3. $N_T < \lfloor \frac{n_R}{N_T} \rfloor$

Lemma 3. *A transmission is detectable Sybil, if and only if there exists a group of less than $\lfloor \frac{n_R}{N_T} \rfloor$ transmissions, whose received signals could linearly expand (the received signal of) that transmission.*

Proof. It is easy to see this is true under Condition 3, according to Corollary 2 and Lemma 2. □

Note that undetectable Sybil transmissions may or may not be identified. However, from the viewpoint of resource testing, these transmissions are not disproportional to the attacking device's resources (i.e., transmitter antennas) and therefore benign.

4.1 Naive Algorithm

Lemma 3 leads to a naive Sybil detection algorithm. Produce all possible combinations of $(\lfloor \frac{n_R}{N_T} \rfloor - 1)$-tuples of transmissions and examine them one by one. For a given tuple, use it to examine all the remaining transmissions; ones that can be linearly expanded by the current tuple are marked as Sybil.

This algorithm allows us to identify all detectable Sybil transmissions because all possible combinations of $(\lfloor \frac{n_R}{N_T} \rfloor - 1)$-tuples are considered. A direction for future improvements is to intelligently reduce the possible tuples in consideration while maintaining the same level of false negative rate.

5. PRACTICAL CONSIDERATION AND FUTURE WORK

Our current solution assumes complete information about the received signals, i.e., both the power and phase of the received signal at each receiver of the MIMO antenna. In practice, we may only know the received power, not the phase. Worse, we may only know the aggregated power of all receivers if only an aggregated RSSI is exposed. A path of future work is to relax the current assumption and push the work further to deal with incomplete information.

6. REFERENCES

[1] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of Sybil attacks in wireless networks," *IEEE Trans. Information Forensics and Security*, vol. 4, no. 3, pp. 492–503, Sep. 2009.

[2] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proc. Wkshp. Wireless Security*, Sep. 2006, pp. 43–52.

[3] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in *Proc. Int. Symp. on a World of Wireless, Mobile, and Multimedia*, Jun. 2006, pp. 564–570.

[4] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proc. Wkshp. Wireless Security*, Sep. 2006, pp. 33–42.

[5] Q. Li and W. Trappe, "Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships," *IEEE Trans. Information Forensics and Security*, vol. 2, no. 4, pp. 793–803, Dec. 2007.

[6] T. S. Rappaport, *Wireless Communications: Principles & Practice*. Prentice-Hall, NJ, 2002.

[7] J. Douceur, "The Sybil attack," in *Proc. Int. Wkshp. Peer-to-Peer Systems*, Mar. 2002, pp. 251–260.

[8] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis & defenses," in *Proc. Int. Conf. Information Processing in Sensor Networks*, Apr. 2004, pp. 259–268.

[9] D. Gesbert, M. Shafi, D. Shiu, P. J. Smith, and A. Naguib, "From theory to practice: An overview of MIMO space–time coded wireless systems," *IEEE J. Selected Areas in Communications*, vol. 21, no. 3, pp. 281–302, Apr. 2003.

[10] Q. H. Spencer, J. W. Wallace, C. B. Peel, T. Svantesson, A. L. Swindlehurst, H. Lee, and A. Gumalla, "Performance of multi-user spatial multiplexing with measured channel data," in *MIMO System Technology for Wireless Communications*, G. Tsoulos, Ed. CRC Press, 2006.

[11] M. Rudelson and R. Vershynin, "The Littlewood-Offord problem and invertibility of random matrices," *Advances in Mathematics*, vol. 218, pp. 600–633, Jun. 2008.

[12] G. Pan and W. Zhou, "Circular law, extreme singular values and potential theory," May 2007, `arXiv:0705.3773 [math.PR]`.