Guessing on Dominant Paths: Understanding the Limitation of Wireless Authentication Using Channel State Information

Zhe Qu*, Rui Duan†, Xiao Han†, Shangqing Zhao‡, Yao Liu†, and Zhuo Lu†
*Central South University, China. †University of South Florida, USA. ‡University of Oklahoma, USA.

2024 IEEE Symposium on Security and Privacy (SP) | 979-8-3503-3130-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/SP54263.2024.00042

***Abstract*—The channel state information (CSI) has been extensively studied in the literature to facilitate authentication in wireless networks. The less focused is a systematic attack model to evaluate CSI-based authentication. Existing studies generally adopt either a random attack model that existing designs are resilient to or a specific-knowledge model that assumes certain inside knowledge for the attacker. This paper proposes a new, realistic attack model against CSI-based authentication. In this model, an attacker Eve tries to actively guess a user Alice's CSI, and precode her signals to impersonate Alice to the verifier Bob who uses CSI to authenticate users. To make the CSI guessing effective and low-cost, we use theoretical analysis and CSI dataset validation to show that there is no need to guess CSI values in all signal propagation paths. Specifically, Eve can adopt a Dominant Path Construction (DomPathCon) strategy that only focuses on guessing the CSI values on the first few paths with the highest channel response amplitude (called dominant paths). Comprehensive experimental results show that DomPathCon is effective and achieves up to 61% attack success rates under different wireless network settings, which exposes new limitations of CSI-based authentication. We also propose designs to mitigate the adverse impact of DomPathCon.**

1. Introduction

Physical layer authentication has been proposed as a potential solution for resource-constrained wireless devices, such as Internet of Things (IoT) devices and Radio Frequency Identity (RFID) sensors [1]–[9] to avoid computational operations, save energy or facilitate auxiliary verification. Instead of using cryptographic primitives, physical layer authentication leverages Channel State Information (CSI) as a type of unique fingerprinting for authentication or identity verification [10]–[13]. The CSI, also known as multi-path channel response, represents the wireless signal attenuations over multiple propagation paths between two communicating parties Alice and Bob [14]–[16]. As shown in Figure 1, the CSI between Alice and Bob is unique and differs from the CSI between an attacker Eve (at a different location 1 or 2) and Bob. This creates the basis for CSI-based authentication and has enabled substantial efforts of research [10]–[13].

Despite existing research to create different ways to leverage CSI for various wireless applications, the less focused is a systematic attack model to evaluate such an authentication design. Existing studies generally adopt either (i) a random attack model or (ii) a specific-knowledge attack model. (i) The random attack model places Eve at a random location (e.g., location 1 or 2 in Figure 1) and evaluates whether Eve's CSI looks similar to Alice's CSI to pass the authentication at Bob. Existing designs are shown to be resilient against such an attack model. (ii) The specific-knowledge model is able to launch more successful attacks, but requires that Eve gains knowledge from Alice and Bob. For example, if Eve knows the CSI between Alice and Bob [4], [17], [18], she can successfully impersonate Alice to Bob. However, it is difficult for Eve to obtain such information in a practical wireless scenario.

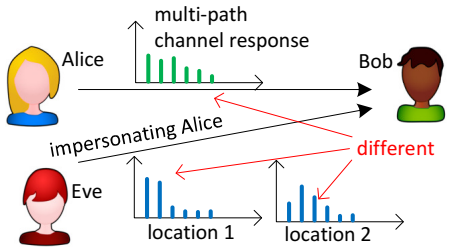


Figure 1: CSI-based authentication and a random attack.

As a result, the random attack model does not seem strong and the specific-knowledge model is strong, but imposes assumptions that may not hold in practice. In this paper, we aim to propose a new attack model filling the gap between the two previous models. In other words, we focus on creating a new attack model that is stronger than the random model and also practical to launch. The new model will not only help understand the limitation of CSI-based authentication, but also provide new design guidelines.

Our approach focuses on making Eve more proactive: As shown in Figure 1, although Eve at a different location has no knowledge of Alice's CSI at Bob, this does not prevent her from actively guessing Alice's CSI. Each time, she can guess a different value of Alice's CSI and send a packet to Bob with a manipulated wireless signal falsifying her CSI observed by Bob to be her guess value. Her signal will pass the authentication when her guess CSI is sufficiently similar to Alice's CSI at Bob.

Apparently, Eve should not randomly guess Alice's CSI and try to send a significant number of packets to Bob. The key question in this attack strategy is what strategy Eve should adopt in order to succeed with just a few tries.

To this end, we take a close look at how CSI is collected and used in wireless authentication [13], [19]–[28]. CSI can

DOI 10.1109/SP54263.2024.00042

be collected (i) inside one transmit-receive antenna pair (i.e., the multiple propagation paths of the wireless signal in a single-antenna system [19], [20], [23], [26], [27], [29]) or (ii) across antenna pairs (i.e., the paths of different transmit-receive antenna pairs in a multi-antenna system [13], [21], [24], [30]). We propose different strategies to guess the CSI on the two types of paths.

Inside a single antenna pair, the wireless signal propagates through multiple paths with varying lengths from the transmit antenna to the receive antenna. As the signal attenuates over long distance, the channel response amplitudes of first few paths with short distances are usually higher than the other paths with long distances [31], [32]. Our intuition is that although existing studies adopt statistical measures [10], [13], [33]–[36] or machine learning [23], [24], [30], [37], [38] to process all the path responses in CSI for verification, building a reliable system would inevitably be biased towards these first few paths (we call them dominant paths) as the remaining paths generally undergo deeper attenuations and are substantially affected by the noise. We find that the CSI as a feature vector has quite uneven importance levels in its elements for a CSI-based classification system. This can be exploited by an attacker to design a more efficient CSI guessing strategy called Dominant Path Construction (DomPathCon) to break the authentication (i.e., just focusing on guessing on the dominant paths). To the best of our knowledge, the dominant path phenomenon is not identified and investigated in existing studies on either CSI-based authentication or CSI-related confidentiality.

Across antenna pairs, additional signal propagation paths are created. Our observation is that multiple antennas in small-factor wireless devices are usually placed close to each other (e.g., 22.29mm on Apple Watch [39] and 43.38mm on Amazon Echo Dot [40]), which can create correlated path attenuations. The correlation has been seen in existing studies [41]–[43] and also observed in our realistic dataset analysis. As strong antenna correlation can be modeled by a linear relationship [44], [45], we are motivated to use a Linear Regression (LR) model [46] based on the guess values of DomPathCon for one transmit-receive antenna pair to compute the guess values of other pairs, which we call the LR-DomPathCon version of DomPathCon.

The LR-DomPathCon strategy can be considered as leveraging the correlation (antenna correlation in our case) in wireless systems to create attacks, which is related to some existing studies. Related work has adopted different ways to exploit the correlation in wireless systems to create attacks targeting confidentiality-based designs, including leveraging data correlation inside a packet (e.g., known-plaintext attacks [47]–[49]), leveraging CSI correlation over time (e.g., attacking wireless key establishment [50]), and leveraging CSI correlation over space (CSI inferencing attacks [51], [52]). In our method, the LR-based design as a part of attacking the MIMO authentication is mostly related to exploiting the CSI correlation over space. Compared with these studies, we do not assume the close proximity between Eve and Alice. We only assume that the CSI values across Alice-Bob's antenna pairs should be correlated (as antennas in smart/IoT devices are placed close to each other), then validate this assumption using dataset evaluation and create the prediction for the MIMO CSI guess value construction.

Under DomPathCon, Eve generates a set of different guess values of Alice's CSI at Bob, and then keeps sending the packets to Bob with the CSI to be different guess values until she successfully fools Bob. Our experiments using commodity WiFi devices based on Atheros AR5822/AR9580 chipsets and TP-Link WDR4300 AP show a wide range of the attack success rates up to 61% under various wireless network settings and conditions, including location, bandwidth, the number of users, the number of antennas, wireless channel condition, and authentication method. Based on the results, DomPathCon has a direct impact on the setups and deployment of CSI-based authentication in wireless scenarios. Our main contributions are as follows: (i) We propose a new attack model, DomPathCon, for Eve to attack CSI-based authentication. We find via theoretical analysis and dataset validation that DomPathCon can focus on the dominant paths inside a single transmit-receive antenna pair and use the LR model to guess the CSI values across different antenna pairs to significantly reduce the number of packets that Eve needs to send until she succeeds. (ii) We conduct comprehensive experiments based on commodity WiFi devices to evaluate the attack performance of DomPathCon in realistic indoor environments, and show that DomPathCon achieves a wide range of successes and has become a much stronger attack model than the random attack model commonly used in existing studies for CSI-based authentication evaluation. (iii) We find that although CSI-based authentication has been considered as a non-cryptographic, low-cost alternative for power/capability-limited IoT authentication, its resilience against DomPathCon in fact requires larger bandwidth, fewer users, more antennas and more cost. This reveals the new limitation of CSI-based authentication, which must be carefully designed to balance its cost and resilience against DomPathCon. (iv) Finally, we propose countermeasure designs that properly set up CSI-based authentication to mitigate the security threat of DomPathCon and evaluate the designs under different conditions.

2. Background and Design Motivation

In this section, we first introduce the background of authentication leveraging CSI. Then, we describe the attack model and present our design motivation.

2.1. Physical Layer Authentication using CSI

The wireless signal from a transmit antenna arrives at a receive antenna via multiple propagation paths. Each path generally leads to different signal amplitude attenuation and phase shift, creating a power-delay profile [10], [14], [16] in wireless communication. Today's MIMO wireless system, equipped with multiple antennas, also creates additional paths between different antenna pairs. The CSI, also known as multiple-path channel response, consists of the amplitudes and phase shifts on all paths [10], [14], [53], [54].

We consider a common CSI-based authentication wireless scenario where Bob uses the CSI to determine if a packet is

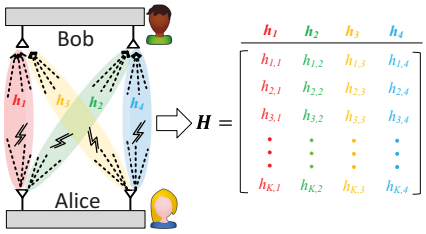


Figure 2: CSI matrix measurement.

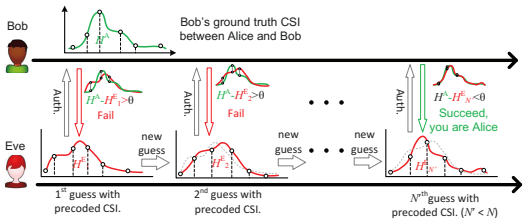


Figure 3: Basic attack process by Eve.

indeed sent by Alice (or another user). As shown in Figure 2, the CSI is represented by a matrix as

$$\boldsymbol{H} = \begin{bmatrix} h_{1,1} & h_{1,2} & \cdots & h_{1,M_T M_R} \\ h_{2,1} & h_{2,2} & \cdots & h_{2,M_T M_R} \\ \vdots & \vdots & \ddots & \vdots \\ h_{K,1} & h_{K,2} & \cdots & h_{K,M_T M_R} \end{bmatrix}, \quad (1)$$

where M_T and M_R are the numbers of transmit and receive antennas, respectively, K is the number of paths between a signal transmit-receive antenna pair, and $h_{i,m}$ denotes the channel response for the i-th ($i \in [1, K]$) path on the m-th ($m \in [1, M_T M_R]$) transmit-receive antenna pair.

Note that the CSI can be represented in either the time domain (i.e., using power delay profile) or the frequency domain (i.e., using CSI values on all subcarriers in OFDM). The representation can be easily converted from one domain to the other [14], [53]. The transformation between the two domains is linear, one-one corresponding, and information-preserving without adding or removing any information. In this paper, we focus on describing the attack strategies using the CSI in the time domain (i.e., the representation of the power delay profile) unless otherwise specified.

The CSI matrix is unique between two users and unknown to a third party at a different location, which offers a type of fingerprinting for authentication design. Many existing studies [13], [19]–[28] have already created a diversity of design portfolios to leverage CSI for low-cost authentication to help wireless and IoT devices to save energy or avoid computational complexity.

The basic procedure in CSI-based authentication is to let Bob first train Alice's CSI to build her profile at Bob (as well as for other users in the network), then verify if the CSI of an incoming packet fits Alice's profile. It is common for Bob to use hypothesis testing [13], [20], [21], [29], [33], [35], [55]–[57] or machine learning [22]–[24], [37], [58] to perform the CSI verification.

2.2. Attack Model

We consider an impersonation attacker Eve who aims to fool Bob's CSI-based authentication by making Bob believe her packets are from a different user in the network. We consider two goals for Eve: (i) targeted attack, in which Eve aims to impersonate a specific user in the network (i.e., Alice) to Bob [13], [20]–[24], and (ii) untargeted attack, in which Eve just wants to fool Bob as long as Bob recognizes her packets as a different user's [4]–[6], [59], [60].

To achieve her attack goals, Eve needs to make sure the CSI of her packets observed by Bob is sufficiently similar to Alice's CSI (or some other user's). Existing studies [10], [13], [24], [33], [56] have shown that if Eve is randomly placed at a different location, she generally cannot have CSI similar to Alice (or any other user) in the network, thereby having a very low chance to launch a successful attack. But if Eve indeed knows Alice's CSI at Bob, she can precode her signal [4], [17], [18] to make sure the CSI observed in her packets is the same as Alice's to pass Bob's verification. However, it is difficult for Eve to know Alice's CSI in a realistic network. In this paper, we adopt a realistic assumption that Eve has no knowledge of any other user's CSI (except her own CSI) observed by Bob. In addition, we assume that Eve has no knowledge of the algorithm used by Bob to verify the CSI.

Our proposed attack model is to make Eve more proactive, and let her keep sending packets with different CSI values observed by Bob until a value eventually passes Bob's verification. Specifically, as shown in Figure 3, Eve generates a set of guess values of CSI; each time, she precodes and sends a packet to Bob to make him observe the CSI to be one of her guess values. Eve succeeds when the guess value is similar to Alice's CSI and Bob acknowledges the reception. Then, Eve can precode all her follow-on packets with the successful guess value.

As shown in Figure 3, Eve has to keep sending guess packets to Bob. In practice, she may not be able to send packets as many as she wants. An essential question is that given a budget N (i.e., the maximum number of CSI-guessing packets Eve can send), how Eve should generate such N guess values. The attack will pose serious security threat against CSI-based authentication if Eve can succeed with a small N (e.g. $N = 10$ or even smaller).

If Eve just randomly generates N CSI values and sends them to Bob to try her luck, she will have a low success chance. We need to design a smarter strategy to generate the N values for Eve. To this end, we first take a look at how CSI is collected in wireless communication [13], [19]–[28]. Fundamentally, the CSI matrix $\boldsymbol{H}$ in (1) of a wireless signal observed at a receiver consists of two parts.

(1) Inside a transmit-receive antenna pair, the signal propagates through multiple paths with different lengths. The elements inside a column vector in (1), such as $h_{1,1}$, $h_{2,1}$, $\cdots$, and $h_{K,1}$, represent the CSI of all such paths.

(2) Across transmit-receive antenna pairs, the signal also propagates multiple paths as additional antennas create more paths, which lead to different columns in the CSI matrix (1).

In the next two sections, we will focus on creating guess

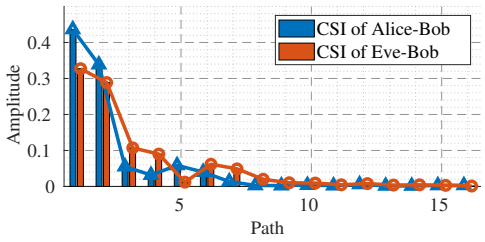


Figure 4: CSIs of Alice-Bob and Eve-Bob in the CRAWDAD Utah/CIR dataset [10].

strategies for Eve to generate the CSI values inside and across transmit-receive antenna pairs, respectively, and show that our strategies with a small budget N have substantial attack success rates against CSI-based authentication.

3. Guessing inside Single Antenna Pair

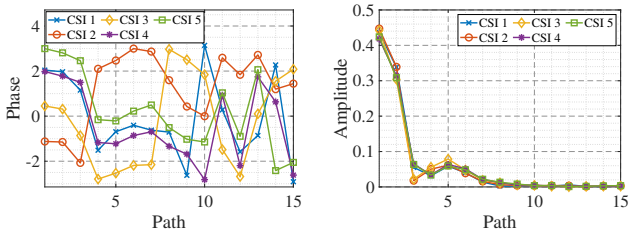
In this section, we address the challenges of guessing CSI values inside a single transmit-receive antenna pair. We first present our design intuition with dataset analysis, then provide our designed attack.

3.1. Observation and Design Intuition

To provide a better strategy for Eve to guess Alice's (for the targeted attack) or any other user's CSI (for the untargeted attack), we first look at the property of CSI samples in the CRAWDAD Utah/CIR dataset [10] under a single antenna system. The dataset includes over 9,300 real CSI samples in an indoor environment. We randomly select two nodes to be Alice and Eve, and one node to be Bob. Figure 4 shows the normalized amplitudes of Alice's and Eve's CSIs observed by Bob. It can be observed from Figure 4 is that although transmitters have distinct CSI amplitude values on different paths, the range of value variations generally decreases as the path number increases since a larger path number indicates a longer path that the signal travels through in wireless communication. This means that when the channel response is used as a key feature to verify transmitters by comparing statistical measures [10], [33]–[36] or using machine learning classifications [24], [30], [38], the verification should be biased towards the first few paths with larger ranges of value variations (which we call dominant paths) because these paths 1) provide more value diversity to differentiate features in a CSI verification mechanism; and 2) are more resilient to the noise on the wireless channel.

As a result, our intuition is that with a limited budget N, Eve only needs to guess the CSI values on these dominant paths instead of all paths because the CSI values on the remaining paths should be less weighted at Bob's verification. For example, Figure 4 shows that there are 16 paths in Alice's CSI. If Eve plans to generate two guesses of the amplitude value on each path, the total of possibilities is 2^{16}. But if Eve focuses only on the first three paths, the total is 2^3, which is feasible for the attack procedure in Figure 3. When Eve generates guess values on these paths similar to Alice's values, Eve is still likely to succeed in impersonating Alice.

Note that each path in CSI is a complex number whose amplitude and phase represent the power attenuation and



(a) Phase. (b) Amplitude.

Figure 5: CSI phase/amplitude values of Alice-Bob in the CRAWDAD Utah/CIR dataset [10].

phase shift, respectively. The phase value is either not used (e.g., many studies [61]–[63] use the amplitudes only) or nearly zero-weighted in a properly trained classifier due to random factors such as the random initial phase of a radio frequency carrier and frequency drifting at a transmitter/receiver [64], [65]. For example, we show in Figure 5a the phases of consecutive 5 CSI values between the same transmit-receive pair in the CRAWDAD Utah/CIR dataset. It can be observed that the phases are of different values distributed over $(-\pi, \pi]$ on each path. By contrast, the amplitudes of these CSI values in Figure 5b are quite similar. Accordingly, we only need to focus on guessing the amplitude values in the attack strategy design.

3.2. Dominant Path Construction

Next, we propose the Dominant Path Construction (DomPathCon) strategy for Eve to guess the CSI values on the dominant paths. We first describe the DomPathCon strategy and then discuss how to choose parameters in DomPathCon.

3.2.1. Attack Strategy Design. Since we consider a single transmit-receive antenna pair, the CSI matrix in (1) becomes a column vector. Let $\boldsymbol{h}^E = [h_1^E, h_2^E, \cdots, h_K^E]^T$ denote Eve's CSI vector observed by Bob, where h_i^E is Eve's channel response on the i-th path ($i \in [1, \cdots, K]$). Eve considers the first $K' < K$ paths as dominant paths and focuses on guessing values on these K' paths with the following DomPathCon procedure.

1) The guessing is based on Eve's CSI; namely, Eve aims to obtain different CSI guess vectors by making some changes to her own CSI vector $\boldsymbol{h}^E$. The reason is that in a wireless network, nearby nodes can experience similar channel fading effects [10], [12]: (i) when Eve is close to Alice, Eve's CSI may also be close to Alice's CSI; (ii) when Eve is far away from Alice and experiences independent fading, no other information is assumed in our attack model to help Eve go beyond random guessing (then using Eve's CSI is just a random guess). Jointly considering (i) and (ii), we see that there is still an advantage of starting from Eve's CSI to guess.

2) To generate guesses based on Eve's CSI, DomPathCon defines a value step Δ and a set of value changes $\mathcal{D} = \{\pm\Delta, \pm 2\Delta, \cdots, \pm n\Delta\}$ on the r-th dominant path, where $r \in [1, \cdots, K']$ and parameter n controls the maximum change. Then, DomPathCon computes the CSI guess $\hat{h}_r$ on the r-th dominant path as $\hat{h}_r = h_r^E + \delta_r \angle h_r^E$ where $\delta_r \in \mathcal{D}$

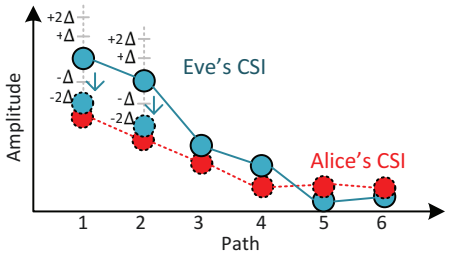


Figure 6: An example of DomPathCon by Eve.

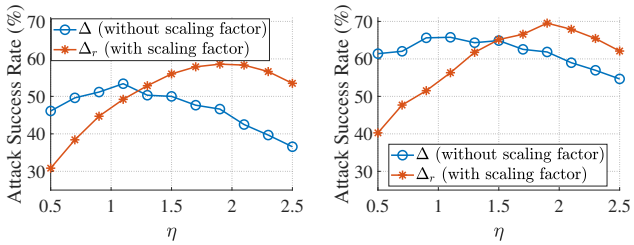
and $\angle h_r^E$ is the phase of h_r^E. For the non-dominant paths, DomPathCon just uses Eve's CSI values as the guess values. Figure 6 shows an example of $n = 2$ and $K' = 2$. It is seen from the figure that DomPathCon only changes the channel responses on the first two paths by four values Δ, $-\Delta$, 2Δ, and -2Δ. Thus, the total number of guesses is $4^2 = 16$.

3) Eve then follows the attack procedure in Figure 3 to precode her signals based on different CSI guess, and then keeps sending the signals to Bob to attack the authentication. Existing precoding techniques (e.g., [17], [18]) are directly adopted to craft intended the CSI for a packet.

3.2.2. Parameter Selection and Optimization. According to the DomPathCon procedure, it generates a total of $(2n)^{K'}$ guesses. We can see the number of dominant paths K' is quite critical if we want to ensure that the total is no more than the budget N. This means Eve may only choose K' to be a very small value (e.g., 1-3) to be practical. Once Eve selects the value of K', she obtains the value of n given the budget N by using $(2n)^{K'} = N$.

Another important value in DomPathCon is the value step Δ. Its value should not be too small otherwise the guess CSI is still quite similar to Eve's CSI. As CSI-based authentication generally involves computing a distance measure compared with a threshold θ in its decision [13], [20], [21], [33], Δ should have a comparable value to θ. In practice, Bob may not disclose his choice of θ to other users. In this case, Eve can collect other users' CSI, build her own CSI-based authentication and choose the proper value $\hat{\theta}$ to distinguish others' CSI with low false alarm. This $\hat{\theta}$ may serve as a predicted value of θ as Eve is in the same network environment with Bob. Then, Δ can be assigned to have a comparable value to $\hat{\theta}$.

In DomPathCon, the value step Δ is the same for the guesses on all dominant paths. However, the channel response amplitude generally decreases as the path number increases (a large path number indicates the signal travels with a longer distance) in wireless communication [31], [32]. This means that the equal value step on all paths may create a CSI guess that is less likely to happen in practice. For example, in Figure 6, decreasing the first path amplitude by 2Δ and increasing the second path amplitude by 2Δ will create a CSI guess with the second path amplitude substantially higher than the first one. This may happen in practice, but is less likely. Hence, a potential way to improve the guess success probability is to scale the value step by a scaling factor for each dominant path: Eve chooses $\Delta_r = b_r\Delta$ for the r-th dominant path, where b_r is called the scaling factor, defined as the ratio between the average CSI amplitude on the r-th path and the average CSI amplitude on the first path in all CSI received by Eve.



(a) Targeted attack. (b) Untargeted attack.

Figure 7: Eve's success rates of different value step $\Delta = \eta\hat{\theta}$.

3.3. Dataset Evaluations

We use a CRAWDAD Utah/CIR dataset [10] based simulations to conduct the preliminary evaluation of DomPathCon.

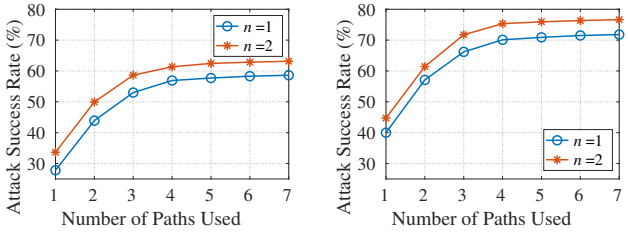
3.3.1. Setups. The dataset is a CSI dataset for single antenna systems and contains 44 locations for 44 users, leading to 13,244 location arrangements for Alice, Bob and Eve. We enumerate all these arrangements to measure the effectiveness of Eve's DomPathCon against Bob's CSI-based authentication for both targeted attack (to impersonate Alice) and untargeted attack (to impersonate any other user at a different location).

For the CSI verification method, for user u, Bob collects all his/her CSI values during training and computes the average CSI vector as $\bar{\boldsymbol{h}}^u$. For an incoming packet with CSI $\boldsymbol{h}$, he finds the shortest distance in all distances of $\boldsymbol{h}$ to each user's average CSI vector (i.e., $d(\boldsymbol{h}) = \min_{u\in\mathcal{U}} \|\boldsymbol{h} - \bar{\boldsymbol{h}}^u\|$) and the corresponding user $u^* = \arg\min_{u\in\mathcal{U}} \|\boldsymbol{h} - \bar{\boldsymbol{h}}^u\|$, where $\mathcal{U}$ is the set of all users. He then compares this distance with the threshold θ, and associates the packet with user u^* if $d(\boldsymbol{h}) \le \theta$.

Since Eve has no knowledge of Bob's CSI verification algorithm and decision threshold θ in our attack model, Eve has to compute her own threshold $\hat{\theta}$ as discussed in Section 3.2.2. In the simulations, we let Eve conduct the Generalized Likelihood Ratio Test (GLRT) [35] to decide $\hat{\theta}$ under a false alarm rate less than 0.05, and then choose her value step Δ to have a comparable value to $\hat{\theta}$, in particular, $\Delta = \eta\hat{\theta}$ with η's value varying around 1–2.

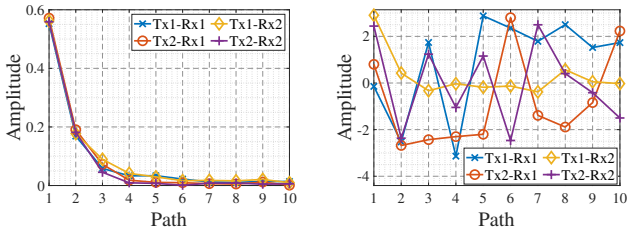
3.3.2. Evaluation Metrics. We use the attack success rate to be the metric to evaluate DomPathCon. For the targeted attack, the attack success rate is the probability that Eve successfully impersonates Alice to Bob using no more than N impersonation packets. For the untargeted attack, the attack success rate is defined as the probability that Eve successfully impersonates anyone in the network to Bob using no more than N impersonation packets.

3.3.3. Results. In the dataset, each CSI contains over 15 paths. First, we choose $K' = 2$ and $n = 2$ (budget $N = 16$) for DomPathCon and show the attack success rates under different values of η in Figure 7. We also compare the impact of scaling the value step on each dominant path (i.e., reducing the value step by a scaling factor b_r for the r-th path as discussed in Section 3.2.2) with the non-scaling case.



(a) Targeted attack (b) Untargeted attack

Figure 8: Eve's success in Utah/CIR dataset [10].



(a) Amplitude (b) Phase

Figure 9: CSI examples of two transmit antennas to two receive antennas in MIMO CIR dataset [69].

From Figure 7b, we can see that DomPathCon achieves substantial attack success rates. The untargeted attack has a rate about 10-20% higher than the targeted attack. There is an optimal value of η to maximize the attack success rate, which differs in the scaling and non-scaling cases: η is near 2 for under scaling and is around 1 under non-scaling. Both at the optimal values, scaling achieves better attack success than non-scaling (i.e., 69.08% vs 65.57%). Thus, scaling shows a slight advantage and will be used by default in all following evaluations of DomPathCon.

Figure 8 shows the impact of the number of selected paths K' in DomPathCon for targeted and untargeted attacks, where we set $n = 1$ or 2 and $\eta = 1.9$. From Figure 8, we observe that even when $K' = 1$ and $n = 2$ (so the budget N is just 4), Eve has a 43.92% success rate with the untargeted attack. Eve's success rate increases with K' increasing (e.g., 60.78% with $K' = 2$), but if the number of K' is too large, the success rate does not have significant improvement (e.g., 74.41% and 74.57% with $K' = 6$ and 7). Although the success rate reduces for the targeted attack in Figure 8, she still achieves 27.79% success by only guessing the first path. Even if Eve chooses $n = 1$, her attack performance does not have large degradation compared to the $n = 2$ case (e.g., 43.03% vs 58.15% with $K' = 2$), which indicates that DomPathCon is effective even with a small budget against CSI-based authentication.

Our dataset evaluation results demonstrate that by simply focusing the guessing on the first few dominant paths, DomPathCon is able to cause a substantial security degradation to CSI-based authentication. In Appendix A, we provide theoretical analysis to understand the fundamental relationship between the attack success probability and the number of guessed dominant paths K' and show how guessing the first few paths is effective against CSI authentication.

4. Guessing across Antenna Pairs

We have shown that DomPathCon is an effective strategy to degrade CSI-based authentication within a single transmit-receive antenna pair. In this section, we describe the strategy to perform the guessing across different antenna pairs. We first present our design intuition with dataset validation. Then, we present and evaluate the attack strategy of LR-DomPathCon to guess CSI across antenna pairs.

4.1. Design Intuition

Today's wireless devices use the MIMO technology to improve the communication performance [66], [67]. DomPathCon is designed to guess the CSI on dominant paths in a single-antenna pair with a total number of guesses $(2n)^{K'}$. For a MIMO system with M_T transmit antennas and M_R receive antennas, Eve can perform DomPathCon on each antenna pair independently, which we call Independent-DomPathCon. It leads to totally $(2n)^{K' M_T M_R}$ guesses and can easily consume a small budget N. As a result, we need to design a strategy better than Independent-DomPathCon to reduce the guessing complexity for CSI in MIMO systems.

As we mentioned previously, multiple antennas create more signal propagation paths than a single antenna pair and result in different columns in the CSI matrix (1). As many wireless devices are designed in a more and more compact form, antennas are usually placed close to each other (e.g., 22.29mm on Apple Watch [39] and 43.38mm on Amazon Echo Dot [40]). The closer the antennas, the more correlated their signal attenuations. Such correlations have been seen in the literature [41]–[43]. Moreover, strong signal correlation can be modeled using a linear relationship [44], [45], [68]. As a result, if correlations exist among many transmit-receive antenna pairs, Eve can build a Linear Regression (LR) model to model the channel responses among these pairs. In this way, Eve only needs to perform the DomPathCon strategy on one antenna pair and use the LR model to predict the guesses for other antenna pairs, leading to totally $(2n)^{K'}$ guesses for the MIMO system independent of the number of antennas. We call this strategy LR-DomPathCon.

4.2. Dataset Validation of Antenna Correlations

The underlying idea of LR-DomPathCon is to leverage the correlation of channel responses in different antenna pairs. We use the 20MHz bandwidth MIMO CIR dataset [69] to measure the correlation in CSI samples between 2 transmit antennas and 2 receive antennas in an indoor environment. In the dataset, the distance between two transmit antennas is 50.8cm and the distance between two receive antennas is 30.5cm. Figure 9 shows an example of the normalized CSI amplitudes from two transmit antennas to two receive antennas. We can see that inside one antenna pair, the amplitude gradually decreases as the path number increases; while the phase is random in $(-\pi, \pi]$, which is similar to the single-antenna example in Figure 5. We also observe in Figure 9a that the different transmit-receive antenna pairs indeed have similar amplitude values on each path, which indicates the existence of the correlation.

Then, we measure the correlation in antenna pairs. We use the CSI data from 10 2×2 MIMO systems in the

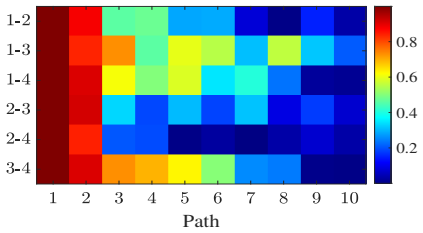


Figure 10: Correlation coefficients in MIMO dataset [69].

dataset [69]. In each 2×2 system, there are 4 transmit-receive antenna pairs, which we index them from 1 to 4. Then, we measure the Pearson correlation coefficient of the channel response amplitudes between every two pairs (i.e., pairs 1 and 2, 1 and 3, 1 and 4, 2 and 3, 2 and 4, 3 and 4) for each 2×2 system. We draw Pearson correlation coefficients between every two pairs as a temperature map in Figure 10. It can be observed that between two antenna pairs, the channel response amplitudes on the first few paths are highly correlated. For example, the coefficients of the first two paths on pairs 1-2 are larger than 0.8.

4.3. LR-DomPathCon

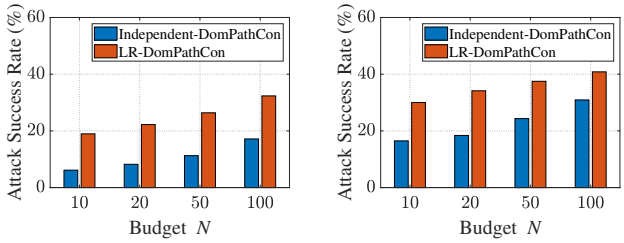
4.3.1. Strategy Design. According to our dataset correlation analysis (e.g., as observed in Figure 10), the most dominant paths are also the most correlated. This perfectly falls into the focus of DomPathCon on the first few dominant paths and further helps DomPathCon to reduce the guessing complexity by taking advantage of the high correlation. Consequently, Eve can adopt LR-DomPathCon instead of Independent-DomPathCon to (i) use DomPathCon to obtain a CSI guess on one transmit-receive antenna pair, and then (ii) use an LR model to predict other CSI guesses on other antenna pairs. We propose the LR-DomPathCon procedure as follows:

1) Eve passively collects the CSI values from Bob, and computes the correlation coefficient for each antenna pair. She then chooses the antenna pair with the highest average correlation coefficient with other pairs as the reference antenna pair, in which she will perform DomPathCon. Then, she uses the CSI values to train an LR model to predict a CSI value of each path in an antenna pair from the reference pair; i.e., $\hat{h}^E_{r,j} = w_{r,j} h_{r,j^*}$, where the j^*-th antenna pair denotes the reference antenna pair, $j \in [1, \cdots, M_T M_R]$ and $j \neq j^*$, and $w_{r,j}$ is the linear weight for the k-th path in the j-th antenna pair in the LR model.

2) After training the LR model and obtaining all weights $w_{r,j}$, given budget N, Eve uses DomPathCon to generate N CSI guesses for the reference antenna pair and then uses the LR model to generate the CSI guesses for other pairs.

3) Similar to the single antenna case, Eve keeps sending the precoded signals with different CSI guesses to Bob to attack the authentication.

4.3.2. Preliminary Evaluations. We continue to use the MIMO CIR dataset for preliminary evaluation. The dataset includes 10 users, and each user has two transmit and two receive antennas with more than 40 CSI samples. We set $K' = n = 2$ and $\eta = 1.8$ with varying budget $N = 10, 20, 50$ and 100. There are 45 combinations of Bob and Eve locations, and we compute the attack success rate averaged over all location combinations.



(a) Targeted attack. (b) Untargeted attack.

Figure 11: Comparisons between Independent-DomPathCon and LR-DomPathCon based on MIMO CIR dataset [69].

Figure 11 compares the attack success rates of Independent-DomPathCon and LR-DomPathCon. It is observed from the figure that given a fixed budget, Independent-DomPathCon always performs substantially worse than LR-DomPathCon that takes advantage of antenna correlation to predict CSI guess. For example, under budget $N = 10$, Independent-DomPathCon only obtains 7.86% success for the targeted attack and 18.15% success for the untargeted attack. By contrast, LR-DomPathCon achieves 19.73% success for the targeted attack and 30.62% success for the targeted attack. The preliminary results in Figure 11 show that LR-DomPathCon is effective to degrade the security of CSI-based authentication in MIMO systems.

5. Experimental Evaluations

In this section, we present the experimental evaluations. We first introduce the system setups, then discuss the attack effectiveness of DomPathCon against existing CSI-based authentication systems.

5.1. Experimental Setup

Experimental Settings: We collect realistic CSI on commodity WiFi routers based on Atheros AR5822/AR9580 chipsets and TP-Link WDR 4300 AP. The CSIs are collected under two different bandwidth settings: 20MHz and 40MHz. The WiFi routers are modified with Atheros CSI Tool [14], which enables fast channel switching for obtaining CSI on enlarged bandwidth WiFi signals. Specifically, we collect the CSI matrix $\boldsymbol{H}^f \in \mathbb{R}^{K, M_T M_R}$ in the frequency domain from the tool, whose rows and columns denote the transmit-receive antenna pairs and subcarriers, respectively. In our experiments, M_T and M_R are both chosen from [1, 3] (i.e., up to 3×3 MIMO) and there are $K = 52$ or 108 subcarriers for the 20MHz or 40MHz bandwidth. Then, for each column vector (i.e., the CSI vector across subcarriers for an antenna pair) $\boldsymbol{H}^f_m = [H^f_{1,m}, \ldots, H^f_{K,m}]$, we use the frequency-to-time domain transformation [14], [53] to obtain its time-domain CSI (i.e., the power delay profile) vector $\boldsymbol{H}^t_m = [H^t_{1,m}, \ldots, H^t_{L,m}]$, where $H^t_{l,m} = \sum_{k=0}^{K-1} H^f_{k,m} e^{j\frac{2\pi lk}{K}}$ for $l \in [1, L]$ with L denoting the maximum number of time-domain paths and set to be 12 (20 MHz) or 24 (40 MHz). The resultant time-domain CSI vector $H^t_{l,m}$ for each antenna

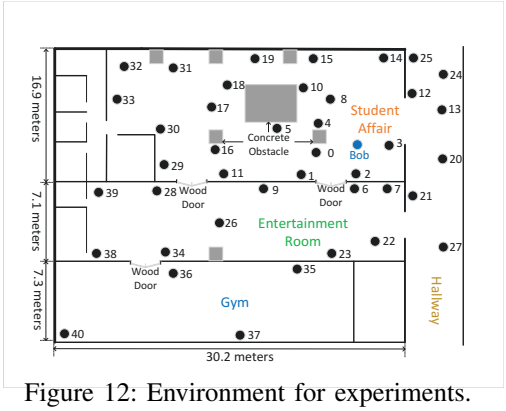


Figure 12: Environment for experiments.

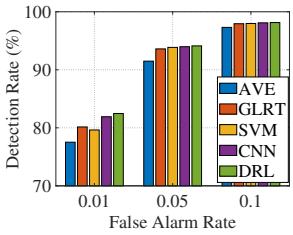


Figure 13: Detection rate of existing authentications.

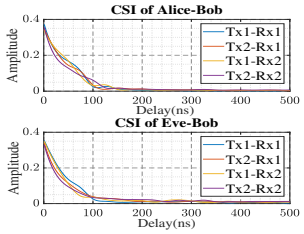
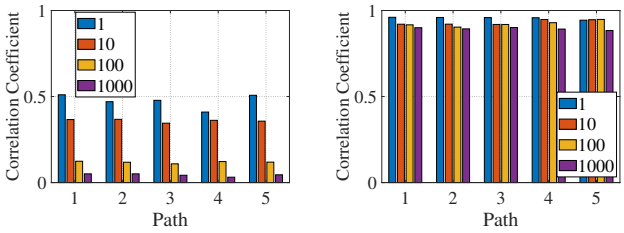


Figure 14: CSI in our experiments.



(a) Phase. (b) Amplitude.

Figure 15: Correlation coefficients of phases and amplitudes by varying sampling interval.

pair is then used in DomPathCon for constructing guess CSIs against CSI-based authentication.

We conduct experiments in a realistic indoor environment in Figure 12 to show the attack impact of DomPathCon (and LR-DomPathCon against MIMO) on existing CSI-based authentications. Our experimental environment has 40 transmitters/users, the receiver/verifier Bob and the attacker Eve (Eve is at location 0 by default). Each user is placed at a different location for performance evaluation. We place Alice at each location, then measure the attack success rate averaged over all locations. We collect more than 100,000 CSIs from each transmitter-receiver pair and transmitter-attacker pair, and we use 100 CSIs to construct the groundtruth on each pair. Note that different transmitter-receiver pair represents different channel conditions: short-distance line of sight (S-LoS), long-distance line of sight (L-LoS), short-distance Non-LoS (S-NLoS), or long-distance Non-LoS (L-NLoS).

The default parameters in our communication systems are set as: 2×2 MIMO and 40MHz bandwidth. For DomPathCon/LR-DomPathCon, we set $K' = n = 2$, $\eta = 1.8$, $N = 50$ by default. During the experiments, we will vary these parameters and show the attack performance.

CSI-Based Authentication: In our experiments, Eve will use DomPathCon to attack the following five existing authentication designs using CSI.

Statistics based authentication: **(i) AVE [10]** and **(ii) GLRT [13], [20], [21], [33]**: Bob firstly collects the CSIs from legitimate users and calculates the corresponding averaged CSIs. For AVE, Eve uses Euclidean distance between the averaged and incoming CSIs to verify a user. For GLRT, Bob builds the likelihood ratio by (6) based on training CSI data to verify the user's CSI distribution.

Machine learning based authentication: **(iii) SVM [24]**, **(iv) CNN [23], [58]**, and **(v) DRL [4], [70]:** Bob leverages the collected CSIs from legitimate users to train a Support Vector Machine (SVM), Convolutional Neural Network (CNN), or Deep Reinforcement Learning (DRL) model, where the CSI is the input and the user index is the corresponding label. Bob uses the learning model to verify incoming CSIs for user authentication.

Figure 13 depicts the performance of each authentication method via the detection rate P_{D} (i.e., $P_{\text{D}} = \frac{\#\text{ of Bob successfully verifies the legitimate user's CSIs}}{\#\text{ of total CSIs}}$) as a function of the targeted false alarm rate P_{FA} (i.e., $P_{\text{FA}} = \frac{\#\text{ of Bob rejects the legitimate user's CSIs}}{\#\text{ of total CSIs}}$) in the presence of no attack. In general, it is observed that the value of P_{D} increases when Bob sets a larger P_{FA} for each authentication method, since a smaller P_{FA} value will reject more CSIs even from Alice. For example, $P_{\text{D}} = 77.52\%$-97.31% for AVE, when $P_{\text{FA}} = 0.01$-0.1. In our experiments, we set the default value of P_{FA} to be 0.05 such that all the methods have a good balance between the detection ratio and the false alarm, which is also widely observed in existing studies [10], [13], [24], [58].

5.2. Evaluation Results

(1) Detection performance when CSI phases are used: In Section 3, we showed that CSI phases exhibit randomness even for consecutive CSI values in the CSI dataset [10] and may not be a good feature for CSI-based authentication. Here, we use our collected CSI data to further demonstrate the impact of using the phases in CSI-based authentication. Figure 15a shows the correlation coefficients of the phases and amplitudes of two CSI samples over a fixed sample interval on the first five paths (e.g., when the sampling interval is 1, the correlation coefficient is computed based on every pair of consecutive CSI samples). It is observed that the correlation coefficient of the CSI phases decreases with increasing the sample interval. For example, when the interval increases from 1 to 1000, the correlation coefficient drops from around 0.5 (weakly correlated) to nearly zero (uncorrelated). It indicates that CSI phases are not suitable for classification. We also show the correlation coefficients of CSI amplitudes in Figure 15b and observe strong correlation (with coefficients close to 1) even over 1000 samples.

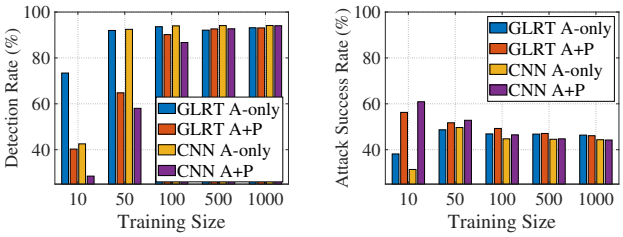
We further compare the detection performance of CSI-based authentication by using CSI amplitudes only (A-only) with the performance by using both amplitudes and phases (A+P). Figure 16a shows the detection rates achieved by two

TABLE 1: Attack success rate (%) by varying the guessing budget N under 20MHz bandwidth.

		1×1 Antenna Pair					2×2 Antenna Pairs					3×3 Antenna Pairs				
N	Attack	AVE	GLRT	SVM	CNN	DRL	AVE	GLRT	SVM	CNN	DRL	AVE	GLRT	SVM	CNN	DRL
5	Tar.	13.16	11.92	11.98	11.60	11.36	3.56	3.32	3.39	3.26	3.15	1.44	1.41	1.35	1.29	1.27
	Untar.	22.45	21.04	21.29	19.71	18.95	8.96	8.11	8.02	7.83	7.83	3.49	2.90	2.76	2.51	2.25
10	Tar.	18.74	16.69	16.77	15.86	15.52	6.89	6.41	6.55	6.27	6.13	3.19	2.81	2.70	2.62	2.58
	Untar.	31.53	28.64	28.72	27.29	26.83	23.67	20.89	20.43	19.26	18.78	14.48	12.67	12.50	11.85	11.39
20	Tar.	28.02	26.41	26.25	25.18	24.77	15.22	13.69	13.57	12.50	12.08	9.53	7.89	7.66	7.24	7.03
	Untar.	49.07	47.99	47.35	46.48	45.69	38.71	35.97	35.46	33.65	33.14	22.10	19.63	19.18	18.05	17.60
50	Tar.	37.39	34.68	34.73	33.20	32.63	23.81	22.37	22.26	20.89	20.45	10.04	9.51	8.92	8.34	8.20
	Untar.	61.31	58.66	58.24	57.45	56.73	45.19	42.84	42.02	40.53	39.82	33.27	30.23	29.76	27.33	26.69

TABLE 2: Attack success rate (%) by varying the guessing budget N under 40MHz bandwidth.

		1×1 Antenna Pair					2×2 Antenna Pairs					3×3 Antenna Pairs				
N	Attack	AVE	GLRT	SVM	CNN	DRL	AVE	GLRT	SVM	CNN	DRL	AVE	GLRT	SVM	CNN	DRL
5	Tar.	12.25	11.34	11.47	10.45	9.92	3.09	2.73	2.82	2.41	2.26	1.69	1.42	1.63	1.50	1.39
	Untar.	20.49	20.10	20.23	19.36	18.87	11.80	10.67	10.26	9.78	9.26	7.67	6.81	7.02	6.44	6.03
10	Tar.	17.66	16.25	16.04	13.87	13.15	5.38	4.60	4.37	3.86	3.71	2.20	1.85	1.81	1.79	1.62
	Untar.	27.71	26.39	25.92	25.13	24.84	20.17	17.30	16.98	15.43	14.82	12.33	10.64	10.32	8.96	8.51
20	Tar.	25.60	23.24	22.73	20.61	20.03	14.27	12.68	12.94	10.85	10.12	5.86	4.10	3.93	3.84	3.02
	Untar.	46.86	46.12	46.44	44.35	43.50	36.68	33.99	33.64	31.96	30.87	19.95	17.45	17.06	15.93	15.14
50	Tar.	35.26	32.92	33.46	31.49	30.72	21.30	20.12	20.58	18.79	18.10	8.64	7.23	6.22	5.81	5.15
	Untar.	58.91	56.16	57.39	55.20	54.37	50.12	46.89	46.06	44.74	43.92	31.98	27.82	27.05	25.11	24.30



(a) Detection. (b) Untargeted attack.

Figure 16: Detection and untargeted attack performance by varying sampling rate.

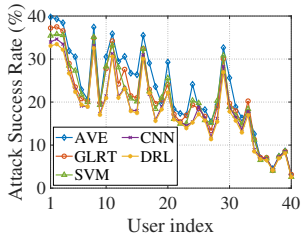


Figure 17: Impact of location of targeted attack.

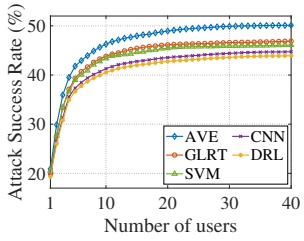


Figure 18: Impact of the number of users.

authentication methods: GLRT (statistics based) and CNN (machine learning based) with different training sizes. We can see that when the CSI training size is small, all methods have low detection performance (e.g., 76.41% for GLRT A-only with 10 CSI training). In addition, a small training size incurs severe degradation for A+P authentications (e.g., 30.49% for CNN A+P with 10 CSIs) as the random CSI phases can be considered noises instead of features for accurate authentication. When we increase the training size, the detection rate increases gradually for each method. Eventually, the A-only and A+P cases exhibit approximately the same detection performance. This is because an authentication method with sufficient training data will give the random phase in CSI nearly zero weight in its classification. As a result, we do not use the CSI phase as a feature for authentication in all follow-on experiments unless otherwise specified.

Figure 16b shows the untargeted attack success rate of DomPathCon in the A-only and A+P cases. The figure shows that when the training size is small, all authentication methods are not reliably trained and DomPathCon has a wide range of attack success rates. When we increase the training size, DomPathCon achieves relatively stable success rates, which are approximately the same for A-only and A+P.

(2) Guessing budget N and bandwidth: The guessing budget N is a critical parameter related to the attack effectiveness. If Eve is quite effective with a very small value of N (i.e., Eve only tries very few packets to fool the authentication) in a scenario, CSI authentication can be considered not secure for the scenario. In addition, because larger bandwidth can generate more paths in the time domain, it can make the authentication more secure. As a result, we thoroughly examine the impact of budget N and bandwidth on the attack effectiveness under different antenna scenarios.

Tables 1-2 show the attack success rates with different values of guessing budget N under the 20MHz and 40MHz bandwidth settings, respectively. They illustrate that the attack success rate always increases when we allow a larger guessing budget. For example, when N goes from 5 to 50, the targeted and untargeted attack success rates of GLRT increase from 4.46% to 25.89% and from 11.43% to 52.37%, respectively. For the same guessing budget N, the attack success rate under 20MHz is always higher than that under 40MHz. Even if Eve only uses 10 guesses, she also can achieve a good attack success rate (e.g., 27.71% for the untargeted attack against AVE in the 1×1 antenna system). Therefore, we consider a more challenging scenario (i.e., 40MHz) in the experiment. Furthermore, we can observe from the tables that if we increase the number of antennas (from 1×1 to 3×3) and bandwidth (from 20MHz to 40MHz), CSI-based authentication becomes indeed more resilient to DomPathCon especially when N is small.

(3) Channel conditions: We evaluate the impact of a user's channel condition on the targeted attack. Figure 17 illustrates the attack success rates for Alice at the different locations. We can see higher attack success rates against Alice at some locations than other locations (e.g., Alice at location 1 suffers an attack success rate of 39.8% on

AVE). This may be because both Alice and Eve have the S-LoS channel conditions to Bob, indicating that their CSIs are similar with more evident dominant paths. In addition, when the channel conditions of Alice and Bob are both L-NLoS, the attack performance is the worst (less than 5%). Furthermore, the experimental results show that DomPathCon can be more effective under the LoS channel conditions. For example, when Alice is at location 6 (S-NLoS), the attack success rate is only 19.38% against DRL. However, at location 29 (L-LoS), DomPathCon achieves 26.94%. The results in Figure 17 may also motivate Eve to physically move around in a network if her attack is not very successful.

(4) Number of users: Figure 18 illustrates the untargeted attack success rate as a function of the number of legitimate users in the network (from 1 to 40). It is obvious that the attack success rate increases with more users in the network. For example, the attack success rate against CNN-based authentication goes from 19.66% to 44.74%. More interestingly, when we just add very few users into the network, the attack success rate increases drastically (e.g., 20.55% to 38.98% against SVM, when the number of users goes from 1 to 5). If we continue to add more users, the attack success rate does not evidently increase and seems to gradually converge (e.g., when the number of users are 10-40, the attack success rate increases from 43.37% to 46.10%). The results from Figure 18 show that DomPathCon can still pose a security threat even when there are just a limited number of users using CSI-based authentication.

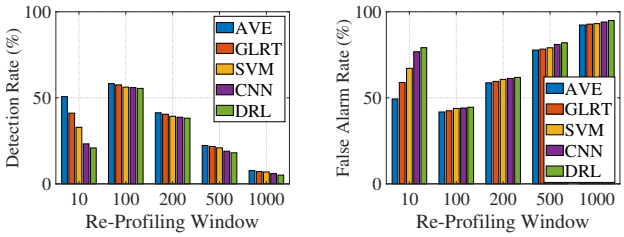
Due to the page limit, we provide additional evaluation results under different conditions in Appendix B.

5.3. Evaluations in Mobile Scenarios

Until now, we have only focused on detection and attack performance in a static network. In this subsection, we investigate CSI-based authentication and the attack performance under user mobility. Specifically, we fix Bob's location as shown in Figure 12 and consider two scenarios: (i) random movement scenario (i.e., all other users and the attacker Eve walk randomly) and (ii) intentionally mobile Eve scenario (i.e., Eve intentionally walking closer to a target). The walking speed is around 1-1.5 meters per second.

(1) Random movement scenario: In this scenario, CSI changes over time due to mobility. We have to re-profile CSI values periodically for user authentication. To this end, we define the re-profiling window, which denotes the number of the latest CSI samples received and used to re-train the CSI classifier by Bob.

Figure 19 shows the performance of CSI-based authentication (in terms of (a) detection rate and (b) false alarm) with different re-profiling window sizes. First, we can see that the performance highly depends on the re-profiling window size. Either a small (e.g., 10) or a large window size (e.g., 1000) leads to performance degradation. In Figure 19, the window size at around 100 achieves the highest detection rate as well as the lowest false alarm for each authentication method. Interestingly, the AVE method, simply computing the Euclidean distance, generally outperforms other more



(a) Detection rate. (b) False alarm rate.

Figure 19: Detection and false alarm rates by varying the re-profiling window size in the random movement scenario.

sophisticated methods under the mobile scenario, and has the best detection rate of 58.24% and false alarm of 41.76%.

Figure 20 shows the targeted attack success rates of DomPathCon in the random movement scenario. It is observed that the success rates are all below 20% under different re-profiling window sizes. These low rates are not surprising as DomPathCon cannot reliably target Alice with the time-varying CSI due to mobility. Despite the low attack performance, the results in Figure 19 demonstrate that CSI-based authentication cannot provide reliable results in mobile scenarios even without the presence of an adversary.

(2) Intentionally mobile Eve scenario: When two users are physically close, their CSIs are more likely to look similar, this may motivate Eve to move closer to her target Alice to launch DomPathCon. In our experiments, we let Eve move closer gradually to Alice using four different moving paths and measure the attack success rate averaged over four paths.

Figure 21 shows the attack success rate as a function of the distance from Eve to Alice. It can be observed that DomPathCon has similar attack success rates against all the five authentications methods. Moreover, we observe that decreasing the distance can gradually increase the attack success rate. For example, when the distance between Eve and Alice changes from 9m to 4m, the targeted attack success rate against SVM-based authentication increases from 23.59% to 35.81%. When Eve is physically close enough to Alice (e.g., 0.5m), the attack success rate reaches around 55% for both targeted and untargeted attacks. The results in Figure 21 further demonstrate that DomPathCon is more effective against CSI-based authentication if an attacker is able to move physically close to a target.

6. Mitigating the Impact of DomPathCon

In this section, we discuss lessons learned and propose our defense strategy to mitigate the impact of DomPathCon.

6.1. Limitations of CSI-based Authentication

Based on the theoretical analysis, dataset validation and experimental evaluations, DomPathCon can incur a serious security issue in CSI-based authentication. As CSI-based authentication has been mainly advocated for low-cost, secure wireless communications (e.g., IoT [4]–[6], [9] and RFID [7], [8]), we find that enhancing its resilience against the DomPathCon attack actually imposes requirements in contradiction with the goals for low-cost, small-factor devices.

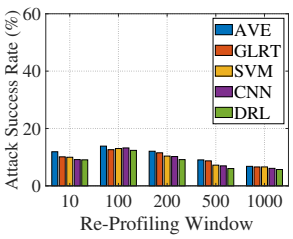


Figure 20: Attack success with random movement.

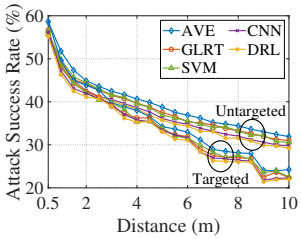


Figure 21: The intentionally mobile Eve scenario.

Specifically, (i) increasing the communication bandwidth can improve the attack resilience (e.g., in Tables 1-2); however, IoT/RFID devices/sensors usually operates at a lower bandwidth; (ii) adding more antennas to a device enhances the resilience (e.g., in Figure 31), but brings more cost and size concerns to these devices/sensors; (iii) reducing the number of users that use CSI authentication also improves the resilience (e.g., in Figure 18), but IoT is usually aimed to support many users.

As a result, it should not take it as granted that CSI-based authentication is always a good candidate for wireless security in IoT, RFID or sensor network scenarios. CSI-based authentication has its limitations when facing DomPathCon. We must carefully evaluate its performance under DomPathCon to balance the achieved security in terms of reducing the attack success rate and the cost associated with demands for more bandwidth, more antennas, more processing capability, and less supported users.

6.2. Mitigation Designs

Although DomPathCon reveals the limitations of CSI-based authentication, we still aim to create designs to mitigate the impact of DomPathCon. Our experiments show that Bob should not verify any mobile user using CSI because mobility causes unreliable authentication results. Bob only needs to consider authenticating static users. However, Eve, as the attacker, is not limited to being static and can try to move around to cause more damages (as shown in Figure 21). Hence, we adopt a two-step approach: first, we provide countermeasures against static Eve; second, based upon the static Eve solution, we further consider the mobile Eve case.

6.2.1. Mitigation designs against static Eve. To mitigate the impact of static Eve who is a malicious user in the network, our basic idea is that Bob can be proactive and launch DomPathCon against himself to select which users should adopt CSI-based authentication to meet a given security requirement, in particular,

1) Bob collects CSIs from the set of all users $\mathcal{U}$ via traditional cryptography based authentication in the network before switching to CSI-based authentication.

2) Given the user set $\mathcal{U}$, he adopts an existing method to build a CSI classifier to authenticate users.

3) Bob assumes that there is an attacker with a guess budget N. In practice, it is difficult for Bob to know the value of N. Therefore, Bob sets his own version of N denoted by N_{Bob} as his allowed budget for any potential attacker, and launches DomPathCon against his own CSI classifier to calculate the untargeted success rate $P_{\text{Untar}}(N_{\text{Bob}},\hat{\mathcal{U}})$. If $P_{\text{Untar}}(N_{\text{Bob}},\hat{\mathcal{U}})$ is greater than Bob's tolerant attack success rate P (which should be sufficiently small to meet Bob's security goal), Bob must shrink the size of $\mathcal{U}$ (i.e., supporting less users for CSI-based authentication) to obtain a subset of users $\hat{\mathcal{U}} \subseteq \mathcal{U}$ such that $P_{\text{Untar}}(N,\hat{\mathcal{U}}) \leq P$, i.e.,

$$\max \quad |\hat{\mathcal{U}}|, \tag{2a}$$

$$\text{s.t.} \quad P_{\text{Untar}}(N_{\text{Bob}},\hat{\mathcal{U}}) \leq P, \tag{2b}$$

Under the formulation of (2), Bob can find the maximum number of users in the network that adopt the CSI-based authentication given the guess budget N_{Bob} and the tolerant level P. When Bob cannot verify a user's CSI N_{Bob} consecutive times, Bob disables CSI-based authentication for the user, i.e., removing the user from the user selection set $\hat{\mathcal{U}}$. After the removal, there will be fewer users using CSI-based authentication. Bob can try to add another user previously not in $\hat{\mathcal{U}}$ into $\hat{\mathcal{U}}$ as long as (2b) is still met. This process is called user switching. The user selection and switching design enables CSI-based authentication to operate under the security tolerant level P when facing DomPathCon. Note that if Eve has her value of N greater than Bob's N_{Bob} and keeps sending packets going beyond N_{Bob}, Bob will switch off the CSI-based authentication after the number of failed authentications exceeds his own setup N_{Bob}, making Eve's further attempts ineffective.

Optimized and balanced solutions: To solve (2) in an optimized way for user selection, Bob first chooses and assumes each user as a potential attacker to launch DomPathCon against himself, and finds the user with the highest untargeted attack success probability. If the probability is larger than the tolerant level P, Bob removes this user for CSI-based authentication. Then, for the rest of the users, Bob uses their CSIs to re-train his classifier and repeats the same removing process until (2b) is met. We call it the optimized approach. Because it has to retrain the classifier after removing each user, the optimized approach requires $|\mathcal{U}| - \max|\hat{\mathcal{U}}|$ re-trainings according to (2), which entails high computational overhead, especially for sophisticated authentication methods (e.g., CNN and DRL).

To reduce the computational overhead of the optimized approach, we design another approach, called label muting, in which Bob always uses the initially-built CSI classifier. Specifically, Bob first builds the CSI classifier based on all users' CSI data. Then, Bob starts to launch DomPathCon against himself and remove users to meet the requirement (2b). When Bob removes a user, he does not change the original classifier but mutes the label of the user (i.e., the set of all possible outputs of the CSI classifier will no longer include the user). This can be achieved by intentionally skipping the comparison to the user's label in an algorithm (e.g., not estimating the probability for the user's label at the soft-max layer in CNN). Algorithm 1 in Appendix C details the procedure of label muting. Label muting only requires one round of training CSIs for all users, which is always needed for building the initial CSI classifier. After a user

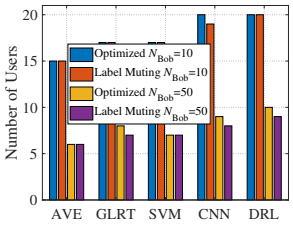


Figure 22: Number of selected users by (2).

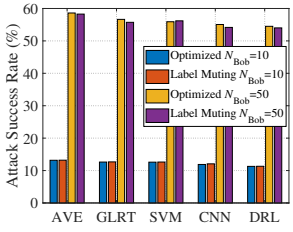


Figure 23: Untargeted success rate of mobile Eve.

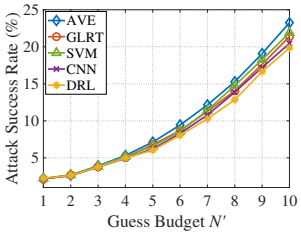


Figure 24: Untargeted success rates by varying N'.

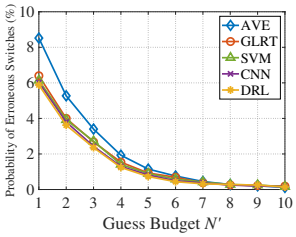


Figure 25: Probability of erroneous switching.

is removed or replaced by a new one (if adding a new one still meets (2b)), the optimized approach needs to retrain the CSI classifier while label muting will simply mute the user's label and activate the new user's label in the classifier.

Evaluations: Figure 22 shows the numbers of supported users solved by the optimized and label muting approaches with the tolerant level $P = 10\%$ and the allowed budget $N_{\text{Bob}} = 10$ or 50 (vs Eve's actual $N = 50$) in the same CSI-based authentication scenario in Figure 18 (40 users with 2×2 MIMO using different CSI classification methods). We can see from Figure 22 that given $P = 10\%$, CSI-based authentication can support a limited number of users out of all 40 users under DomPathCon. Label muting can support almost the same number of users as the optimized approach, which makes it a balanced approach between the performance and computational overhead. In addition, using sophisticated methods can help accommodate slightly more users (e.g., 20 (DRL) vs 15 (AVE)).

Figure 22 further shows that a larger budget N_{Bob} means a higher attack success rate, and thereby fewer users can be supported for CSI-based authentication. As a result, Bob cannot allow Eve to have a large guess budget N_{Bob} in practice. In other words, when Bob cannot verify a user's CSI N_{Bob} consecutive times and N_{Bob} must be small (e.g., 10), Bob should disable CSI-based authentication for the user.

6.2.2. Mitigating intentionally mobile Eve. The optimized and the label muting approaches are able to help Bob select a subset of users to participate in CSI-based authentication to combat static Eve. It is also possible that Eve, with the knowledge of her target Alice's location, aims to move physically closer to Alice and then launch DomPathCon. Indeed, our results in Figure 21 show that Eve's intentional movement can be even more damaging.

In this scenario, Bob needs to be aware that although all users are currently static and their CSIs have been trained, there may exist one malicious Eve that will later move physically closer to another user and launch DomPathCon. This is a challenging scenario that has not been fully explored in existing studies, as most of them [13], [20], [21], [23], [24], [29], [35], [37], [55] assume that Eve is static and placed at a different (random) location.

In the following, we create such an attacker, mobile Eve, who always moves physically closer (around 0.5–2m) to her target Alice and then launches DomPathCon in the same scenario used in Figure 22 (where a subset of users is selected). We measure mobile Eve's success rates in Figure 23: mobile Eve is able to have success rates greater than the tolerant level $P = 10\%$ set in both optimized and label-muting mitigations, in particular, when $N_{\text{Bob}} = 50$. This is because both mitigations select users based on their past CSI training and cannot predict the CSI when users move. Moreover, mobile Eve is assumed to know Alice's location and always move closer to Alice to benefit DomPathCon. Consequently, mobile Eve can exceed the tolerant level P set in the mitigations.

Based on the results in Figure 23, if we cannot increase the hardware capabilities in the network (e.g., increasing bandwidth or antennas), reducing the allowed budget from the originally set N_{Bob} to an even smaller value N' becomes a feasible way to reduce mobile Eve's success rate (e.g., the attack success rate decreases from 54.52% to 10.37% when N_{Bob} changes from 50 down to 10 against DRL-based authentication in Figure 23). However, further reducing the allowed budget for Bob means that he will become less patient with authentication failures and more likely to switch a user out due to random variations of CSI. We call this case erroneous switching. For example, setting $N' = 1$ means that Bob replaces a user as long as he cannot verify the CSI of just one packet from the user.

Thus, we set different values of N' and measure the resulting attack success rates of mobile Eve in Figure 24 (we adopt the same settings used in Figure 23, where we use label muting to select users with $N = 10$ and $P = 10\%$). We can see from Figure 24 that in order to meet the tolerant level $P = 10\%$ against mobile Eve, we need to set $N' = 6$ (so mobile Eve's success rate becomes around $9\% < 10\%$). Figure 25 shows the probability of erroneous switching (i.e., the probability of N' consecutive legitimate packets failing the CSI-based authentication) for different values of N'. We note that the probability gradually decreases with increasing N'. When $N' = 6$, the probability of erroneous switching is around 0.8%. A smaller N' helps further reduce the attack success rate but increases the probability of erroneous switching.

Overall, Eve can be either static or mobile in practice. To provide an effective mitigation, Bob first needs to select a subset of users based on (2) given target budget N_{Bob} and tolerant level P for the static scenario. Then, he has to further reduce the target budget to a new value $N' < N_{\text{Bob}}$ to make sure that mobile Eve's attack success rate is lower than P while maintaining a low erroneous switching probability.

TABLE 3: $(|\hat{\mathcal{U}}|, N')$ to achieve the target erroneous switching probability (1%) and the tolerant level (5% or 10%) with $N = 10$ for AVE- and CNN-based authentication.

Tolerant	2×2, 20MHz	2×2, 40MHz	3×3, 20MHz	3×3, 40MHz
AVE 5%	(5, 4)	(6, 4)	(8, 4)	(10, 5)
AVE 10%	(13, 5)	(15, 6)	(17, 7)	(20, 9)
CNN 5%	(7, 4)	(9, 5)	(11, 5)	(12, 6)
CNN 10%	(17, 6)	(19, 6)	(22, 7)	(24, 10)

In Table 3, we measure the values of pair $(|\hat{\mathcal{U}}|, N')$ to achieve the target erroneous switching probability of 1% and the attack tolerant level of 5% or 10% with $N = 10$ for AVE- and CNN-based classification methods under different wireless system setups. It is easy to see that more hardware capability can support more users and allow for a large value of N' (e.g., Bob can support 24 out of a total of 40 users with $N' = 10$ for CSI-based authentication under the 40MHz 3×3 MIMO system). Table 3 shows that when facing a mobile Eve model, if Bob targets a low attack tolerant level (e.g., 5%), he has to enable a very limited number of users for CSI-based authentication (e.g., 7 out of 40 users for CNN-based authentication) and at the same time be impatient with authentication failures (e.g., 4 failures warrants the switching off). Enhancing the hardware capability (e.g., increasing bandwidth or antennas) can accommodate more users and authentication failures, but also incurs more cost, which can negatively impact IoT device design.

6.2.3. Discussions. DomPathCon is a new attack model targeting CSI-based authentication, which has not yet been studied in the literature. Through investigating DomPathCon, we show that CSI-based authentication, primarily created for IoT applications, should not be considered always secure and has to be carefully revisited. The DomPathCon model does not consider other physical layer information (e.g. radio frequency fingerprints [71], [72]) that may be combined with CSI to improve the security. As a result, using a combination of physical-layer information may improve the security against the DomPathCon model. In addition, our MIMO attack leverages the fact that many IoT devices have compact antenna designs with strong antenna correlations. If a device can sufficiently separate antennas (e.g., in a vehicle network scenario where a base station communicates with a car with multiple antennas), LR-DomPathCon may not be efficient for CSI prediction across antennas.

7. Related Work

Location or identity/user authentication: Prior studies have designed location or identity verification methods [10]–[13], [20], [21], [24], [29], [37], [73] based on the CSI properties from different users at different locations. Some studies also extended the CSI-based authentication to more complicated scenarios, such as relay networking [74]–[76] and continuous wireless authentication [23], [77], [78]. As we discussed previously, these studies adopted a random attack model, which cannot substantially degrade any CSI-based authentication design. Our work shows that the proposed DomPathCon is a stronger attack model than the random one to evaluate the security of CSI-based designs and exposes their limitations in realistic wireless network scenarios. Furthermore, several attack strategies [4], [17], [18] have also been proposed against CSI-based authentication. However, the effectiveness of these attackers requires the precondition that the attacker Eve has already known the CSI between the two communicators Alice and Bob, which is usually not practical for Eve to obtain unless some additional assumption is imposed (e.g., assuming that Eve is quite physically close to Alice or Bob such that she can know or predict the CSI). Compared with these attacks, DomPathCon is a very practical attack to launch in a wireless network. It adopts a search strategy only focusing on the dominant paths to guess the CSI. Our results have shown that DomPathCon can substantially degrade the performance of CSI-based authentication methods and expose their limitations in different practical wireless scenarios.

Behavior or activity based authentication: Leveraging WiFi signals to capture unique human behaviors inherited from their daily activities has been widely investigated for authentication [79]–[82]. Some studies attempted to authenticate users by exploring users' behavioral characteristics such as key-press durations [79] and angle preferences when operating a mouse [80]. Later, some papers [81], [82] proposed to authenticate users through sensing human gaits due to the unique variations in the CSI at the WiFi receiver. Follow-up studies have also investigated authentication based on fine-grained users' gestures (e.g., finger gestures [83], [84]). These designs that rely on a series of CSI data for accurate behavior or user recognition will also be adversely affected by the proposed DomPathCon attack strategy.

Other Physical-layer Authentication Methods: In addition to CSI-based methods, fingerprinting or authentication designs have been proposed to leverage other physical layer properties, including carrier frequency offsets (CFOs) [85]–[87], hardware impairments [88], [89], in-phase and quadrature-phase imbalances [90], and clock skews [91]. Many designs still face practical issues that affect the accuracy of the authentication. For example, it was observed in [87] that low-cost ZigBee devices have severe CFO variations even within 15 minutes and varying over time probably due to temperature changes. This research direction is complementary to our research focusing on CSI.

8. Conclusion

The CSI-based authentication has been extensively studied in the literature to facilitate authentication in wireless networks. In this paper, we proposed a new, realistic attack model against CSI-based authentication, in which an attacker Eve tries to actively guess a user Alice's CSI and precode her signals to impersonate Alice to the verifier Bob who uses CSI to authenticate users. We have shown that there is no need to guess CSI values for all signal propagation paths and a DomPathCon strategy can be adopted to focus on guessing the CSI values on dominant paths. Experiment evaluations based on commodity WiFi devices have shown that DomPathCon is a stronger adversarial model against CSI-based authentication and exposes its limitation. Finally, we provided designs to mitigate the impact of DomPathCon on CSI-based authentication.

References

[1] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, pp. 8169–8181, 2019.

[2] A. Soni, R. Upadhyay, and A. Jain, "Internet of Things and wireless physical layer security: A survey," in *Computer communication, networking and internet security*. Springer, 2017, pp. 115–123.

[3] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2018.

[4] N. Gao, Q. Ni, D. Feng, X. Jing, and Y. Cao, "Physical layer authentication under intelligent spoofing in wireless sensor networks," *Signal Processing*, vol. 166, p. 107272, 2020.

[5] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, 2009.

[6] H. K. Kalita and A. Kar, "Wireless sensor network security analysis," *International Journal of Next-Generation Networks*, vol. 1, 2009.

[7] J. Han, C. Qian, Y. Yang, G. Wang, H. Ding, X. Li, and K. Ren, "Butterfly: Environment-independent physical-layer authentication for passive RFID," *ACM IMWUT*, vol. 2, no. 4, pp. 1–21, 2018.

[8] G. Wang, H. Cai, C. Qian, J. Han, X. Li, H. Ding, and J. Zhao, "Towards replay-resilient RFID authentication," in *ACM MobiCom*, 2018, pp. 385–399.

[9] Y. Zheng, S. S. Dhabu, and C.-H. Chang, "Securing IoT monitoring device using PUF and physical layer authentication," in *IEEE ISCAS*, 2018, pp. 1–5.

[10] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *ACM MobiCom*, 2007, pp. 111–122.

[11] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in *ACM MobiCom*, 2008, pp. 26–37.

[12] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *IEEE S&P*, 2010, pp. 286–301.

[13] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564–2573, 2012.

[14] Y. Xie, Z. Li, and M. Li, "Precise power delay profiling with commodity Wi-Fi," *IEEE Trans. Mobile Comput.*, vol. 18, no. 6, pp. 1342–1355, 2018.

[15] T. Cui and C. Tellambura, "Power delay profile and noise variance estimation for OFDM," *IEEE Commun. Lett.*, vol. 10, 2006.

[16] S. Tan, L. Zhang, Z. Wang, and J. Yang, "Multitrack: Multi-user tracking and activity recognition using commodity WiFi," in *ACM CHI*, 2019, pp. 1–12.

[17] S. Fang, Y. Liu, W. Shen, and H. Zhu, "Where are you from? confusing location distinction using virtual multipath camouflage," in *ACM MobiCom*, 2014, pp. 225–236.

[18] S. Fang, Y. Liu, W. Shen, H. Zhu, and T. Wang, "Virtual multipath attack and defense for location distinction in wireless networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 2, pp. 566–580, 2016.

[19] C. Ayyildiz, R. Cetin, Z. Khodzhaev, T. Kocak, E. G. Soyak, V. C. Gungor, and G. K. Kurt, "Physical layer authentication for extending battery life," *Ad Hoc Networks*, vol. 123, 2021.

[20] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective Rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5948–5956, 2009.

[21] H. Forssell, R. Thobaben, H. Al-Zubaidy, and J. Gross, "Physical layer authentication in mission-critical MTC networks: A security and delay performance analysis," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 4, pp. 795–808, 2019.

[22] H. Fang, X. Wang, and L. Xu, "Fuzzy learning for multi-dimensional adaptive physical layer authentication: a compact and robust approach," *IEEE Trans. Wireless Commun.*, vol. 19, no. 8, pp. 5420–5432, 2020.

[23] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, 2018.

[24] H. Liu, Y. Wang, J. Liu, J. Yang, and Y. Chen, "Practical user authentication leveraging channel state information (CSI)," in *ACM ASIACCS*, 2014, pp. 389–400.

[25] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56–62, 2010.

[26] H. Rahbari and M. Krunz, "Exploiting frame preamble waveforms to support new physical-layer functions in OFDM-based 802.11 systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3775–3786, 2017.

[27] S. H. Hwang, J. S. Um, M. S. Song, C. J. Kim, H. R. Park, and Y. H. Kim, "Design and verification of IEEE 802.22 WRAN physical layer," in *IEEE CrownCom*, 2008, pp. 1–6.

[28] W. Wang, Y. Chen, and Q. Zhang, "Privacy-preserving location authentication in Wi-Fi networks using fine-grained physical layer signatures," *IEEE Trans. Wireless Commun.*, vol. 15, 2015.

[29] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *IEEE MILCOM*, 2011, pp. 538–542.

[30] H. Kong, L. Lu, J. Yu, Y. Chen, X. Xu, F. Tang, and Y.-C. Chen, "MultiAuth: Enable multi-user authentication with single commodity WiFi device," in *ACM Mobihoc*, 2021, pp. 31–40.

[31] S. S. Ghassemzadeh, L. J. Greenstein, T. Sveinsson, A. Kavcic, and V. Tarokh, "UWB delay profile models for residential and commercial indoor environments," *IEEE Trans. Veh. Technol.*, vol. 54, no. 4, pp. 1235–1244, 2005.

[32] V. Erceg, D. G. Michelson, S. S. Ghassemzadeh, L. J. Greenstein, A. Rustako, P. B. Guerlain, M. K. Dennison, R. Roman, D. J. Barnickel, S. C. Wang *et al.*, "A model for the multipath delay profile of fixed wireless channels," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 3, pp. 399–410, 1999.

[33] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *IEEE ICC*, 2008, pp. 1520–1524.

[34] J. K. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," in *IEEE COMSNETS*, 2010, pp. 1–9.

[35] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1791–1802, 2013.

[36] J. B. Perazzone, L. Y. Paul, B. M. Sadler, and R. S. Blum, "Artificial noise-aided MIMO physical layer authentication with imperfect CSI," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2173–2185, 2021.

[37] L. Senigagliesi, M. Baldi, and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1506–1521, 2020.

[38] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1676–1687, 2017.

[39] "Apple watch," https://appleinsider.com/articles/20/08/11/apple-watch-antennas-could-improve-by-being-moved-to-the-rear, 2022, accessed: 2022-03-24.

[40] "Amazon echo dot," https://predictabledesigns.com/product-development-teardown-of-an-amazon-echo-dot/, 2022, accessed: 2022-03-24.

[41] B. Nosrat-Makouei, J. G. Andrews, and R. W. Heath, "MIMO interference alignment over correlated channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 6, pp. 2783–2794, 2011.

[42] S. Silva, G. A. A. Baduge, M. Ardakani, and C. Tellambura, "Performance analysis of massive MIMO two-way relay networks with pilot contamination, imperfect CSI, and antenna correlation," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 4831–4842, 2018.

[43] X. Mei and K.-L. Wu, "Envelope correlation coefficient for multiple MIMO antennas of mobile terminals," in *IEEE IEEE AP-S/URSI*, 2020, pp. 1597–1598.

[44] J. M. Bland and D. G. Altman, "Statistics notes: Calculating correlation coefficients with repeated observations: Part 1—correlation within subjects," *Bmj*, vol. 310, no. 6977, p. 446, 1995.

[45] B. Ratner, "The correlation coefficient: Its values range between+ 1/-1, or do they?" *Journal of targeting, measurement and analysis for marketing*, vol. 17, no. 2, pp. 139–142, 2009.

[46] K. H. Zou, K. Tuncali, and S. G. Silverman, "Correlation and simple linear regression," *Radiology*, vol. 227, no. 3, pp. 617–628, 2003.

[47] M. Schulz, A. Loch, and M. Hollick, "Practical known-plaintext attacks against physical layer security in wireless MIMO systems." in *NDSS*, 2014.

[48] Y. Zheng, M. Schulz, W. Lou, Y. T. Hou, and M. Hollick, "Profiling the strength of physical-layer security: A study in orthogonal blinding," in *ACM WISEC*, 2016, pp. 21–30.

[49] ——, "Highly efficient known-plaintext attacks against orthogonal blinding based physical layer security," *IEEE Commun. Lett.*, vol. 4, no. 1, pp. 34–37, 2014.

[50] Z. Qu, S. Zhao, J. Xu, Z. Lu, and Y. Liu, "How to test the randomness from the wireless channel for security?" *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3753–3766, 2021.

[51] F. Rottenberg, T.-H. Nguyen, J.-M. Dricot, F. Horlin, and J. Louveaux, "CSI-based versus RSS-based secret-key generation under correlated eavesdropping," *IEEE Trans. on Commun.*, vol. 69, 2020.

[52] R. Zhu, T. Shu, and H. Fu, "Statistical inference attack against PHY-layer key extraction and countermeasures," *Wireless networks*, vol. 27, no. 7, pp. 4853–4873, 2021.

[53] A. Goldsmith, *Wireless communications*. Cambridge univ. press, 2005.

[54] T. S. Rappaport *et al.*, *Wireless communications: principles and practice*. prentice hall PTR New Jersey, 1996, vol. 2.

[55] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171–4182, 2016.

[56] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 44–58, 2012.

[57] S. M. Kay, *Fundamentals of statistical signal processing: estimation theory*. Prentice-Hall, Inc., 1993.

[58] Q. Wang, H. Li, D. Zhao, Z. Chen, S. Ye, and J. Cai, "Deep neural networks for csi-based authentication," *IEEE Access*, vol. 7, pp. 123 026–123 034, 2019.

[59] S. Karunaratne, E. Krijestorac, and D. Cabric, "Penetrating RF fingerprinting-based authentication with a generative adversarial attack," in *IEEE ICC*, 2021, pp. 1–6.

[60] J. Liu, Y. He, C. Xiao, J. Han, L. Cheng, and K. Ren, "Physical-world attack towards WiFi-based behavior recognition," in *IEEE INFOCOM*, 2022, pp. 400–409.

[61] J. Wang, J. Xiong, H. Jiang, K. Jamieson, X. Chen, D. Fang, and C. Wang, "Low human-effort, device-free localization with fine-grained subcarrier information," *IEEE Trans. Mobile Comput.*, vol. 17, no. 11, pp. 2550–2563, 2018.

[62] Y. Lin, Y. Gao, B. Li, and W. Dong, "Revisiting indoor intrusion detection with WiFi signals: do not panic over a pet!" *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10 437–10 449, 2020.

[63] Y. Cao, Z. Zhou, C. Zhu, P. Duan, X. Chen, and J. Li, "A lightweight deep learning algorithm for WiFi-based identity recognition," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17 449–17 459, 2021.

[64] D. Vasisht, S. Kumar, and D. Katabi, "{Decimeter-Level} localization with a single WiFi access point," in *USENIX NSDI*, 2016, pp. 165–178.

[65] Y. Zhuo, H. Zhu, H. Xue, and S. Chang, "Perceiving accurate CSI phases with commodity WiFi devices," in *IEEE INFOCOM*, 2017, pp. 1–9.

[66] K. R. Jha, B. Bukhari, C. Singh, G. Mishra, and S. K. Sharma, "Compact planar multistandard MIMO antenna for IoT applications," *IEEE Trans. Antennas Propag.*, vol. 66, no. 7, pp. 3327–3336, 2018.

[67] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (iot) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23 022–23 040, 2020.

[68] A. G. Barnston, "Correspondence among the correlation, RMSE, and Heidke forecast verification measures; refinement of the Heidke score," *Weather and Forecasting*, vol. 7, no. 4, pp. 699–709, 1992.

[69] D. Maas, N. Patwari, S. K. Kasera, D. Wasden, and M. A. Jensen, "Experimental performance evaluation of location distinction for MIMO links," in *IEEE COMSNETS*, 2012, pp. 1–10.

[70] L. Xiao, G. Sheng, S. Liu, H. Dai, M. Peng, and J. Song, "Deep reinforcement learning-enabled secure visible light communication against eavesdropping," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 6994–7005, 2019.

[71] H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving zigbee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting," *IEEE Trans. Rel.*, vol. 64, no. 1, pp. 221–233, 2014.

[72] S. Rajendran, Z. Sun, F. Lin, and K. Ren, "Injecting reliable radio frequency fingerprints using metasurface for the internet of things," *IEEE Trans. on Inf. Forensics Security*, vol. 16, pp. 1896–1911, 2020.

[73] P. Zhang, Y. Shen, X. Jiang, and B. Wu, "Physical layer authentication jointly utilizing channel and phase noise in MIMO systems," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2446–2458, 2020.

[74] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, 2013.

[75] X. Du, D. Shan, K. Zeng, and L. Huie, "Physical layer challenge-response authentication in wireless networks with relay," in *IEEE INFOCOM*, 2014, pp. 1276–1284.

[76] J. Choi, "A coding approach with key-channel randomization for physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 175–185, 2018.

[77] X. Wang, F. J. Liu, D. Fan, H. Tang, and P. C. Mason, "Continuous physical layer authentication using a novel adaptive OFDM system," in *IEEE ICC*, 2011, pp. 1–5.

[78] Y. Chen, H. Wen, J. Wu, H. Song, A. Xu, Y. Jiang, T. Zhang, and Z. Wang, "Clustering based physical-layer authentication in edge computing systems with asymmetric resources," *Sensors*, vol. 19, no. 8, p. 1926, 2019.

[79] K. Revett, "A bioinformatics based approach to user authentication via keystroke dynamics," *International Journal of Control, Automation and Systems*, vol. 7, no. 1, pp. 7–15, 2009.

[80] N. Zheng, A. Paloski, and H. Wang, "An efficient user verification system via mouse movements," in *ACM CCS*, 2011, pp. 139–150.

[81] W. Wang, A. X. Liu, and M. Shahzad, "Gait recognition using WiFi signals," in *ACM UbiComp*, 2016, pp. 363–373.

[82] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT," in *ACM Mobihoc*, 2017, pp. 1–10.

[83] H. Kong, L. Lu, J. Yu, Y. Chen, L. Kong, and M. Li, "Fingerpass: Finger gesture-based continuous user authentication for smart homes using commodity WiFi," in *ACM Mobihoc*, 2019, pp. 201–210.

[84] C. Li, M. Liu, and Z. Cao, "WiHF: Enable user identified gesture recognition with WiFi," in *IEEE INFOCOM*, 2020, pp. 586–595.

[85] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, "Accurate and efficient wireless device fingerprinting using channel state information," in *IEEE INFOCOM*, 2018, pp. 1700–1708.

[86] P. Liu, P. Yang, W.-Z. Song, Y. Yan, and X.-Y. Li, "Real-time identification of rogue WiFi connections using environment-independent physical features," in *IEEE INFOCOM*, 2019, pp. 190–198.

[87] G. Shen, J. Zhang, A. Marshall, L. Peng, and X. Wang, "Radio frequency fingerprint identification for LoRa using spectrogram and CNN," in *IEEE INFOCOM*, 2021, pp. 1–10.

[88] P. Zhang, T. Taleb, X. Jiang, and B. Wu, "Physical layer authentication for massive MIMO systems with hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 1563–1576, 2019.

[89] A. Papazafeiropoulos, C. Pan, P. Kourtessis, S. Chatzinotas, and J. M. Senior, "Intelligent reflecting surface-assisted MU-MISO systems with imperfect hardware: Channel estimation and beamforming design," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 2077–2092, 2021.

[90] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "ORACLE: Optimized radio classification through convolutional neural networks," in *IEEE INFOCOM*, 2019.

[91] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," *IEEE Trans. Mobile Comput.*, vol. 9, no. 3, pp. 449–462, 2009.

[92] Y. Sun, Á. Baricz, and S. Zhou, "On the monotonicity, log-concavity, and tight bounds of the generalized Marcum and Nuttall Q-functions," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1166–1186, 2010.

[93] A. Annamalai and C. Tellambura, "Cauchy–Schwarz bound on the generalized Marcum Q-function with applications," *Wireless Communications and Mobile Computing*, vol. 1, no. 2, pp. 243–253, 2001.

[94] Á. Baricz and Y. Sun, "New bounds for the generalized Marcum Q-function," *IEEE Trans. Inf. Theory*, vol. 55, pp. 3091–3100, 2009.

[95] G. Louppe, L. Wehenkel, A. Sutera, and P. Geurts, "Understanding variable importances in forests of randomized trees," *Advances in neural information processing systems*, vol. 26, 2013.

Acknowledgement: The work at USF was supported in part by NSF CNS-2044516.

Appendix A.
Theoretical Analysis

A large number of methods [13], [20], [21], [23], [24], [29], [33], [35], [37], [38], [55]–[57] have been proposed to train and verify CSI. It is not feasible to perform analysis for each method. As the primary design objective in existing methods is always to improve the detection rate while reducing the false alarm rate. In our theoretical modeling, we assume that Bob knows the distribution of Alice's CSI vectors $\bar{\boldsymbol{h}}^A = \boldsymbol{h}^A + \boldsymbol{w}_{\rm I}$, where $\boldsymbol{w}_{\rm I}$ is a complex Gaussian noise vector from the wireless channel $\boldsymbol{w} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_{\rm I}^2 \boldsymbol{I})$. Then, Bob uses the optimal hypothesis test [13], [20], [21], [33] to verify whether CSI $\boldsymbol{h}$ of the incoming signal is transmitted by Alice or Eve. Under the hypothesis $\mathcal{H}_0$, the transmitter is Alice and Bob accepts this packet when a test statistic $d(\boldsymbol{h})$ is less than a given threshold θ. Under the hypothesis $\mathcal{H}_1$, the transmitter is Eve and Bob refuses this packet if $d(\boldsymbol{h}) > \theta$. Mathematically,

$$\mathcal{H}_0 : \boldsymbol{h} = \boldsymbol{h}^A + \boldsymbol{w}_{\rm II} \tag{3}$$

$$\mathcal{H}_1 : \boldsymbol{h} = \boldsymbol{h}^E + \boldsymbol{w}_{\rm II}, \tag{4}$$

where $\boldsymbol{w}_{\rm II} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_{\rm II}^2 \boldsymbol{I})$ and $\boldsymbol{h}^E$ is the equivalent CSI between Eve and Bob. The optimal test in CSI-based authentication is GLRT [13], [20], [21], [57]. Following the GLRT strategy in [13], [20], we write the logarithm of the likelihood ratio of the incoming CSI $\boldsymbol{h}$ as

$$d(\boldsymbol{h}) = \frac{\max f(\boldsymbol{h}|\mathcal{H}_1)}{f(\boldsymbol{h}|\mathcal{H}_0)}. \tag{5}$$

The GLRT is to compare the likelihood ratio with a given threshold $\theta > 0$ (i.e., when $d(\boldsymbol{h}) \leq \theta$, accept $\mathcal{H}_0$; otherwise, accept $\mathcal{H}_1$). By taking the logarithm of $d(\boldsymbol{h})$ and after a normalization [13], [20], we can obtain the following test statistic of $d(\boldsymbol{h})$ as:

$$d(\boldsymbol{h}) = \frac{2}{\sigma^2} \sum\nolimits_{i=1}^{K} |h_i - \bar{h}_i^A|^2, \tag{6}$$

where $\sigma^2 = \sigma_{\rm I}^2 + \sigma_{\rm II}^2$. Under the hypothesis $\mathcal{H}_0$, $d(\boldsymbol{h})$ results in a central chi-square random variable with $2K$ degrees of freedom, which is defined as:

$$d_{\mathcal{H}_0} = \frac{2}{\sigma^2} \sum\nolimits_{i=1}^{K} |w_{\rm I}^i - w_{\rm II}^i|^2 \sim \chi_{2K}^2, \tag{7}$$

where $w_{\rm I}^2$ and $w_{\rm II}^2$ are the i-th path's noise of $\boldsymbol{w}_{\rm I}$ and $\boldsymbol{w}_{\rm II}$. Under the hypothesis $\mathcal{H}_1$, $d(\boldsymbol{h})$ is a noncentral chi-square random variable with $2K$ degrees of freedom:

$$d_{\mathcal{H}_1} = \frac{2}{\sigma^2} \sum\nolimits_{i=1}^{K} |h_i^E + w_{\rm II}^i - (h_i^A + w_{\rm I}^i)|^2 \sim \chi_{2K,\beta}^2, \tag{8}$$

where β is the noncentrality parameter. Since the mean values of $w_{\rm I}^i$ and $w_{\rm II}^i$ are both zero, β can be calculated by:

$$\beta = \frac{2}{\sigma^2} \sum\nolimits_{i=1}^{K} |h_i^E - h_i^A|^2. \tag{9}$$

In the hypothesis testing: a false alarm (FA) happens when $d_{\mathcal{H}_0} > \theta$ (i.e., when Bob refuses a packet coming from Alice), and a missed detection (MD) occurs when $d_{\mathcal{H}_1} < \theta$ (i.e., when Bob accepts a packet coming from Eve). For given a threshold θ, the probabilities of FA $P_{\rm FA}$ and MD $P_{\rm MD}$ are:

$$P_{\rm FA} = P[d_{\mathcal{H}_0} > \theta] = 1 - F_{\chi_{2K}^2}(\theta), \tag{10}$$

$$P_{\rm MD} = P[d_{\mathcal{H}_1} < \theta] = F_{\chi_{2K}^2}(\beta, \theta), \tag{11}$$

where $F_{\chi^2}(\theta)$ is the Cumulative Distribution Function (CDF) of a central chi-square random variable with $2K$ degrees of freedom, and $F_{\chi_{2K}^2}(\beta, \theta)$ is the non-central chi-square CDF with noncentrality parameter β. For a target $P_{\rm FA}$, the given threshold is set from (10) as:

$$\theta = F_{\chi_{2K}^2}^{-1}(1 - P_{\rm FA}). \tag{12}$$

In this case, the MD probability $P_{\rm MD}$ is calculated as:

$$\begin{aligned} P_{\rm MD} &= F_{\chi_{2K}^2}(\beta, F_{\chi^2}^{-1}(1 - P_{\rm FA})) \\ &= 1 - Q_K(\sqrt{\beta}, \sqrt{\alpha}), \end{aligned} \tag{13}$$

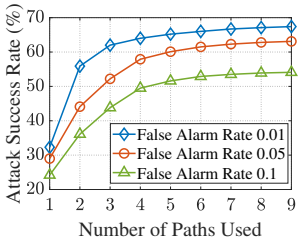


Figure 26: Theoretical success rate of false alarm rate P_{FA}.

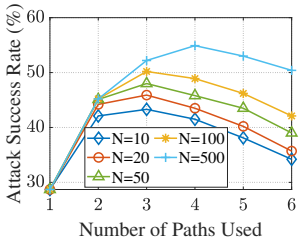


Figure 27: Theoretical success rate of guessing budget N.

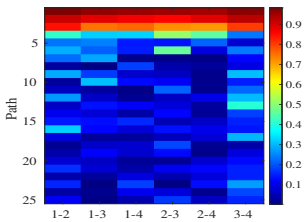


Figure 28: Correlation coefficient of Eve-Bob's CSI.

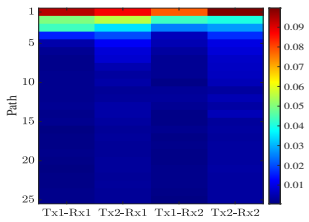


Figure 29: Feature importance score.

where $Q_K(\sqrt{\beta},\sqrt{\alpha})$ is Marcum Q-function, and $\alpha = F^{-1}_{\chi^2_{2K}}(1-P_{\text{FA}})$. The Marcum Q-function is strictly increasing in K and β for all $\beta \geq 0$ and $\alpha, K > 0$ [92]. Based on [93], [94], the Marcum Q-function $Q_K(\sqrt{\beta},\sqrt{\alpha})$ can be bounded from above as:

$$\begin{aligned} Q_K(\sqrt{\beta},\sqrt{\alpha}) \leq & e^{(-\frac{1}{2}(\sqrt{\beta}-\sqrt{\alpha})^2)} \\ & \times \sqrt{\frac{2K-1}{2} + \frac{(\beta/\alpha)^{1-K}}{2(1-\beta/\alpha)}} \\ \leq & e^{(-\frac{1}{2}(\sqrt{\beta}-\sqrt{\alpha})^2)} \sqrt{(2K+1)/2}, \end{aligned} \tag{14}$$

where the last inequality holds because $K \geq 1$ and the minimum value of β is 0 (i.e., $\boldsymbol{h}^E = \boldsymbol{h}^A$). Because K and α are both constants, under the modeling, if Eve aims to increase the MD probability P_{MD}, the most important point is to reduce the parameter β in (14), which depends on the difference between $\boldsymbol{h}^E$ and $\boldsymbol{h}^A$ (i.e., $\beta(\boldsymbol{h}^E, \boldsymbol{h}^A)$). Since DomPathCon only tries to guess the amplitude, we re-define the parameter β by CSI amplitudes and provide a lower bound $\hat{\beta}$ by the triangle inequality as:

$$\beta \geq \hat{\beta} = \frac{2}{\sigma^2} \sum\nolimits_{i=1}^{K} ||h|_i^E - |h|_i^A|^2. \tag{15}$$

Therefore, $Q_K(\sqrt{\beta},\sqrt{\alpha}) \leq Q_K(\sqrt{\hat{\beta}},\sqrt{\alpha})$. Because DomPathCon focuses on the first K' paths, we can write $\hat{\beta} = \beta(K')$ as a function of K' under the assumption that Eve can accurately guess the CSI values of the first K' paths in Alice's CSI. As such, the lower bound of P_{MD} is:

$$P_{\text{MD}} \geq 1 - e^{\left(-\frac{1}{2}(\sqrt{\hat{\beta}(K')}-\sqrt{\alpha})^2\right)} \sqrt{(2K+1)/2}. \tag{16}$$

Due to the constant values of K and α, (16) can be simplified to $P_{\text{MD}} = 1 - e^{\mathcal{O}(K')}$. It indicates that when the number of K' increases, the MD probability exhibits at least sub-linear increasing with a faster rate when K' is small. Hence, this theoretically implies the effectiveness of DomPathCon by only focusing on the first K' paths with K' being small.

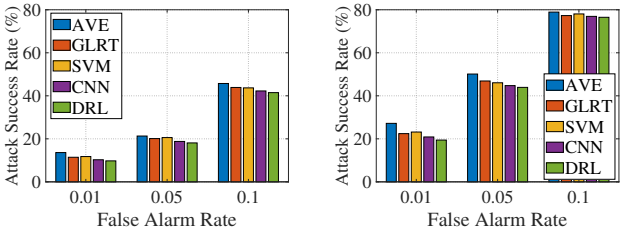
According to the simplified path decay model [53], the amplitudes of Alice's and Eve's CSI can be modeled as $|h|_i^A = |h|_1^A \gamma^A(i)$ and $|h|_i^E = |h|_1^E \gamma^E(i)$, where $\gamma^A(i)$ and $\gamma^E(i)$ are decay functions of Alice and Eve. In order to further validate our theoretical result, we conduct a numerical simulation, in which $h_1^A = 50$dB, $h_1^E = 48$dB, the SNRs of Alice and Eve are both 20dB. We set the decay function $\gamma^A(i) = 2.1^{-(i-1)}$ and $\gamma^E(i) = 2.05^{-(i-1)}$. Figure 26 shows the theoretical result in (16) as a function of the number of paths used in DomPathCon K' based on the numerical simulation. We can see that Eve can achieve sufficiently high success rates for small K' values. For example, when Bob's verification is set to have $P_{\text{FA}} = 0.05$ and Eve only modifies three dominant paths, her success rate is 50.86%. Figure 27 shows the attack rate increases if Eve has more guesses budget N. The results indicate that even when the value of N is small (i.e., $N = 10$), Eve can still use the first path to successfully pass the authentication with 27.42% success. More specifically, if Eve increases the number of paths to guess, the success rate firstly increases and then decreases. For example, when $N = 100$, the attack success rate is 50.38% with $K' = 3$ but 47.16% with $K' = 6$. This is because under a fixed budget, we have to reduce the number of guesses on each path if we consider more paths. As a result, Figure 27 also reveals that we should focus the guessing on the first few paths given a budget limit.

Appendix B. Additional Experimental Results

(1) Visualization and analysis of our collected CSIs: We randomly select two CSIs (Alice-Bob and Eve-Bob) and show the CSI amplitude on each path in Figure 14. It can be observed that the first 2-3 paths on each antenna pair have much higher amplitudes than other paths, and accordingly they can be considered dominant paths. This matches our previous observations in CIR datasets [10], [69]. In addition, Figure 28 presents the correlation coefficients across different antenna pairs. We can see that between two antenna pairs, correlation coefficients of the first two paths are larger than 0.84, which indicates the high correlation of dominant paths across different antennas and offers the proposed LR-DomPathCon a good opportunity of attack success against MIMO.

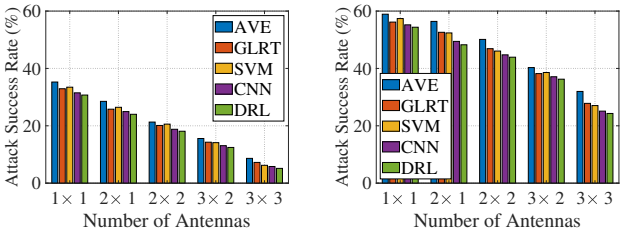
In addition, we use the importance score in a classic tree-based feature selection method [95] for machine learning to quantify the importance of CSI on a dominant path, shown in Figure 29. We can see from the figure that the first two paths across all antenna pairs have much higher importance factors (0.04-0.1) than the rest (less than 0.03). Therefore, only reconstructing the CSI via dominant paths to impersonate Alice is an effective attack.

(2) Impact of P_{FA}: Figure 30 shows the attack success rate under the commonly used $P_{\text{FA}} = 0.01, 0.05$ and 0.1 in [13], [20], [21], [29]. It is noted that even if Bob uses $P_{\text{FA}} = 0.01$, DomPathCon can still achieve a high attack



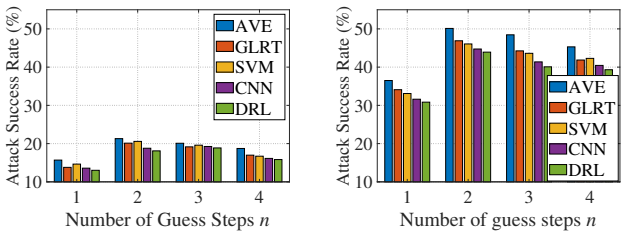
(a) Targeted attack. (b) Untargeted attack.

Figure 30: Impact of P_{FA}.



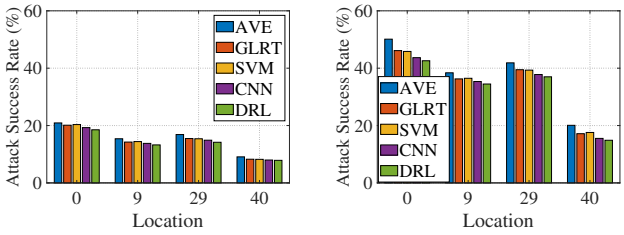
(a) Targeted attack. (b) Untargeted attack.

Figure 31: Impact of the number of antennas.



(a) Targeted attack. (b) Untargeted attack.

Figure 32: Impact of the number of guess steps n.



(a) Targeted attack. (b) Untargeted attack.

Figure 33: Impact of Eve's location.

rate (i.e., higher than 9.75% for the targeted attack and 19.42% for the untargeted attack). In addition, the untargeted attack success rate against each of the five authentications is higher than 76.50% with $P_{\text{FA}} = 0.1$, which incurs a much more serious security issue. A smaller P_{FA} reduces the attack success rate, but degrades the usability of CSI-based authentication because a lower false alarm design leads to a lower detection rate, meaning that Alice's own CSI will be more likely rejected by Bob (as observed in Figure 13).

(3) The number of antennas: We evaluate the impacts of different numbers of antennas on the effectiveness of DomPathCon. Figure 31 shows that as the number of antennas increases from 1×1 to 3×3, the attack success rate decreases for both targeted (e.g., 33.46%-6.22% for SVM) and untargeted attacks (e.g., 54.37%-24.30% for DRL). The reason is that when we increase the number of antennas, the possible guess space of Eve will increase exponentially. Although increasing the number of antennas makes CSI authentication more resilient against the attack, most of existing IoT devices may only equip one or two antennas [39], [40]. More attack resilience from adding more antennas unfortunately results in more device complexity and cost.

(4) Guess steps n: How to choose the guess step n on each dominant path is also important for DomPathCon. In Figure 32, we can see that the optimal value of n is equal to 2 on all the five authentications. For example, the targeted and untargeted success rates of AVE are 21.30% and 50.12%, respectively. We also observe that the attack success rate does not differ greatly under $n = 2$ and $n = 3$, and has minor degradation when $n = 4$. The results show that we can choose an appropriately small value of n to achieve a notable attack success rate.

(5) Eve's locations: Note that in the previous experiments, we fixed Eve's location at 0, which has an S-LoS channel to Bob. In the following, we aim to show the impact of the attacker-receiver channel condition by varying Eve's location at 9, 29, and 40, which represent the L-NLoS, N-LoS, and L-NLoS channels, respectively. In Figure 33, we can see that Eve performs the best at location 0 than other locations. This is due to the fact that more users are physically near location 0, and hence Eve's CSIs are similar to those users (e.g., user 1 or 2). The other reason is that when Eve is near Bob, the noise of Eve-Bob's wireless channel is comparably low, which does not have significant influence on the guessed CSIs. By contrast, Eve at location 40 has the worst attack success rate (e.g., 15.57% against CNN in the untargeted attack), since less legitimate users' CSIs are similar to Eve's, making Eve guess the CSI with more difficulty. In addition, if Eve is at location 29, she can achieve a higher attack success rate than being at location 9. For example, Eve can achieve 36.18% and 39.43% against GLRT at locations 9 and 29, respectively.

Appendix C.
The Label Muting Algorithm

Algorithm 1 The label muting approach to solve (2).

$\hat{\mathcal{U}} = \mathcal{U}$ and $P_{\text{Untar}}(\hat{\mathcal{U}}) = 1$;
Train the classifier W and collected CSI data $\mathcal{D}_u$ for each user $u \in \hat{\mathcal{U}}$;
while $P_{\text{Untar}}(\hat{\mathcal{U}}) > P$ **do**
  for $u \in \hat{\mathcal{U}}$ **do**
    DomPathCon generates CSI guesses from $\mathcal{D}_u$;
    Count the number of attack successes C_u on W;
    $P_u = C_u/|\mathcal{D}_u|$;
  end for
  $P_{\text{Untar}}(\hat{\mathcal{U}}) = \sum_{u\in\hat{\mathcal{U}}} C_u/(\sum_{u\in\hat{\mathcal{U}}} |\mathcal{D}_u|)$;
  Mute the label of the user label with the highest P_u value in W;
end while

Appendix D.
Meta-Review

D.1. Summary

The paper emphasizes on the lack of systematic attacker model to evaluate CSI-based authentication and proposes a realistic attack model that uses a proactive strategy named Dominant Path Construction (DomPathCon) to impersonate a user. Specifically, in contrast to cryptographic authentication, physical layer authentication (typically based on channel state information CSI) is a potential solution for identity verification for resource-constrained IoT and RFID devices. DomPathCon works by actively guessing a user's CSI on the dominant paths (first few paths with the highest channel response amplitude) and precoding their signals.

D.2. Scientific Contributions

- Independent Confirmation of Important Results with Limited Prior Research
- Addresses a Long-Known Issue
- Identifies an Impactful Vulnerability
- Provides a Valuable Step Forward in an Established Field

D.3. Reasons for Acceptance

1) The paper emphasizes an important issue of physical layer authentication in resource constrained devices and re-iterates the limitation of CSI-based authentication scheme.
2) The paper has an extensive evaluation of the attack strategy using commodity Wi-Fi and with respect to different parameters like different locations, bandwidth, the number of users, the number of antennas, wireless channel condition, etc. This evaluation is supported with theoretical analysis and dataset validation to show the DomPathCon attack success rate.
3) This paper forces the community to reconsider and re-evaluate CSI as a future authentication approach.