Message Integrity Protection over Wireless Channel: Countering Signal Cancellation via Channel Randomization

Yanjun Pan, Yantian Hou, Ming Li, Ryan M. Gerdes, Kai Zeng, Md. A. Towfiq, Bedri A. Cetiner

Abstract—Physical layer message integrity protection and authentication by countering signal-cancellation has been shown as a promising alternative to traditional pure cryptographic message authentication protocols, due to the non-necessity of neither pre-shared secrets nor secure channels. However, the security of such an approach remained an open problem due to the lack of systematic security modeling and quantitative analysis. In this paper, we first establish a novel signal cancellation attack framework to study the optimal signal-cancellation attacker's behavior and utility using game-theory, which precisely captures the attacker's knowledge using its correlated channel estimates in various channel environments as well as the online nature of the attack. Based on theoretical results, we propose a practical channel randomization approach to defend against signal cancellation attack, which exploits state diversity and swift reconfigurability of reconfigurable antenna to increase randomness and meanwhile reduce correlation of channel state information. We show that by proactively mimicking the attacker and placing restrictions on the attacker's location, we can bound the attacker's knowledge of channel state information, thereby achieve a guaranteed level of message integrity protection in practice. Besides, we conduct extensive experiments and simulations to show the security and performance of the proposed approach. We believe our novel threat modeling and quantitative security analysis methodology can benefit a wide range of physical layer security problems.

Index Terms—Wireless Security, Signal Cancellation, Channel Randomization, Reconfigurable Antenna.

1 Introduction

Message integrity protection and authentication are two fundamental security services in the Internet-of-Things, given the exponential growth of wireless sensors and mobile devices [2]. Traditionally, such services have assumed the existence of pre-shared secret keys or secure channels. However, in many scenarios these premises may not be satisfied, e.g. when initial security associations need to be established among two or more constrained wireless devices. Generally, secret keys need to be distributed either via an offline secure channel or using a public key infrastructure (PKI). But key pre-distribution may not be always feasible due to the lack of hardware interfaces and the absence of a global PKI. Some existing research proposed using out-of-band (OOB) secure auxiliary channels to build message authentication protocols without pre-shared keys [3]–[8]. However, an OOB channel would require special hardware and non-trivial human interaction, while its security has been revisited [9]. In addition, whenever keys are stolen or compromised, re-keying involves significant human effort as well.

Ideally, we want to provide message integrity protection and authentication without relying on pre-shared keys or secure channels. That is, to establish the veracity of a message and its source using only wireless in-band transmissions. Čapkun et. al. [10] showed that it is possible to construct such an in-band integrity protection primitive, by assuming the infeasibility of signal cancellation and combining unidirectional error detection codes and ON/OFF keying modulation. Later a few works have followed up in this direction. However, an important question remained unanswered about its security. Since the security depends on the infeasibility of signal-cancellation, work should be done to evaluate to which extent this is true, i.e. there lacks quantitative analysis of its security. Previously, Pöpper et. al. [11] demonstrated a practical relaying attack that can fully cancel the source's signal in indoor scenarios, regardless of message content and modulation. In practice, the effect of signal cancellation attack is similar to message deletion, which can lead to serious consequences and is also hard to detect. For example, in the scenarios that the attacker is capable of canceling out RTS/CTS messages, the CSMA/CA protocol would suffer from the hidden terminal problem.

In reality, the probability of adversarial signal-cancellation heavily depends on the wireless channel conditions. But again, so far only qualitative results are available,

- *Yanjun Pan and Ming Li are with the Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721. E-mail: {yanjunpan,lim}@email.arizona.edu*
- *Yantian Hou is with the Department of Computer Science, Boise State University, Boise, ID, 83725. E-mail: yantianhou@boisestate.edu*
- *Ryan M. Gerdes is with the Department of Electrical and Computer Engineering, Virginia Tech, Arlington, VA 22203. Email: rgerdes@vt.edu*
- *Kai Zeng is with the Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA 22030. Email: kzeng2@gmu.edu*
- *Md. A. Towfiq and Bedri A. Cetiner are with the Department of Electrical and Computer Engineering, Utah State University, Logan, UT 84322. E-mail: aztowfiq@aggiemail.usu.edu, bedri.cetiner@usu.edu*

This paper is an extension of our previous work in AsiaCCS 2015 [1].
This work was partly supported by NSF grants CNS-1410000, CNS-1619728, CAREER Award CNS-1564477, ONR YIP Award N00014-16-1-2650. The multifunctional reconfigurable antenna design aspect of this work performed at Utah State University is supported in part by AFOSR Grant No FA 9550-15-1-0040 DEF. We thank Giuseppe Lo Voi for his help with antenna maintenance, and Firas Almoualem for assisting with the experimental setup.

while no quantitative security guarantee can be provided by any of the previous designs. Unfortunately, in general such a security guarantee is quite challenging to establish for any wireless physical-layer security mechanism. This is primarily due to a lack of systematic modeling of attacker's behaviors in this area, unlike well-known methodologies for cryptography. To do so one needs to connect the theoretical and practical aspects of wireless security. In addition, the fact that wireless is an open medium makes it easy for common attacks to be launched, thus threat modeling needs to be comprehensive. A smart and strategic attacker who is knowledgeable about the wireless channel environment must be assumed. In fact, depending on the channel environment, the channel state information (CSI) can only be viewed as a partial secret (or non-secret) of the legitimate communicating pairs. Moreover, the attacker can possess advanced hardware and processing capabilities such as multi-antennas and directional antennas. Many other existing physical layer security schemes failed to provide any security [12], [13] when the attacker is powerful as such.

In this paper, we first present a systematic threat modeling for signal cancellation attacks. We observe that the attacker can exploit the intrinsic channel correlation existing in various domain(s) (e.g. temporal, spatial and frequency domains) to estimate the CSI of the legitimate communication pairs with help of advanced hardware (such as directional antennas or multi-antennas). However, no matter how powerful the attacker is, since the signal cancellation attack is an active attack, all the attack behaviors must be carried out in an *online* fashion. Therefore, we observe that the success of the signal cancellation attack is only depending on the channel correlations in the temporal and spatial domains. Correspondingly, we propose two types of attack models, which are more general or stronger than those adopted by existing works.

Rooted in this key observation, we then develop a signal cancellation attack and defense framework by adapting previous information-theoretic study in correlated jamming [14]. Our framework captures the attacker's knowledge about the legitimate communication pair's CSI using a correlation coefficient. We consider both indoor and outdoor environments in our system model. The signal cancellation attack and defense process are modeled as a zero-sum game, in which the attacker aims at minimizing receiver's energy detection probability, while the defender seeks to maximize this probability. Under this framework, we theoretically analyze the optimal attack/defense strategies and detection probability under signal cancellation attack, given any correlation coefficient. Then we summarize our previous simulation results that validated our theoretical analysis, and revealed the impact of attacker's correlation coefficient and the detection threshold to the system's security level.

Based on the theoretical results, we propose a practical physical-layer message integrity protection approach via channel randomization. The realization of channel randomization builds upon swift reconfigurability and state diversity characteristics of the reconfigurable antenna (RA). Our idea is to let the legitimate pair proactively make a worst case estimation of the attacker's knowledge of their CSI (mimic the attacker), and use that to derive a lower-bound of the energy detection probability under optimal cancellation attacks. As we need to consider both temporal and spatial correlations of the CSI, we need to impose some constraints on the location of the attacker (and we show that the spatial correlation decreases with attacker's distance). Interestingly, by increasing the randomness of the wireless channel over both temporal and spatial domains via RA, we can achieve an arbitrary goal of minimum signal detection probability by tuning the number of symbols in each ON slot.

In addition, we carry out real-world experiments and implement our channel randomization approach on USRP devices. We found that by actively randomizing the physical channel via RA, the indoor static channel can be turned into a dynamic channel which can effectively defend against signal cancellation attack and protect message integrity. In contrast to prior work in physical layer security, our approach neither requires nor depends on the channel advantage of the legitimate channel over the adversary channel.

Compared with our preliminary work [1], our main additional contributions are: (1) Besides the two attack models in [1], we propose a more practical attack model, i.e., the type III attacker, in order to model the attacker which exploits the channel correlation in spatial domain. With all three attack models, it is more complete and systematic to evaluate the security of wireless systems under signal cancellation attack. (2) We propose a systematic and effective channel randomization approach which exploits swift reconfigurability and state diversity characteristics of RA to protect message integrity. Extensive experiments and security analysis are carried out to show its resistance to optimal signal cancellation attack. (3) We present the method to combine our approach with existing message integrity protection schemes and evaluate its performance under normal communication scenarios using BER and link throughput. (4) We identify that the correlation coefficient and variance of CSI are two key factors affecting the detection probability and show the influence of the selection of antenna modes on these two factors. To the best of our knowledge, this is the first work that systematically employs RA to defend against signal cancellation attack in the real world.

The rest of this paper is organized as follows. Sec. 2 presents the related work and motivation to our threat modeling and message integrity protection approach, followed by the system and attack models in Sec. 3. In Sec. 4, we present the game-theoretical framework to analyze the attacker/defender's strategies and their optimal utilities. Sec. 5 gives our channel randomization approach and introduces our method to protect message integrity in practice. In Sec. 6, we present the implementation and experimental study. Sec. 7 concludes the paper and lists the insights gained.

2 Related Work and Motivation

2.1 In-band Message Integrity Protection and Authentication

A few previous works proposed in-band message integrity protection and authentication schemes without relying on pre-shared secret keys [10], [15], [16]. The common underlying idea is to combine ON/OFF keying with unidirectional error detection code. By using this coding method, bit 1 is encoded into ON_OFF slots and bit 0 is encoded into OFF_ON slots. To provide message integrity protection, a

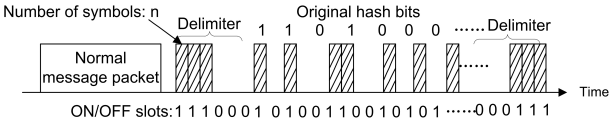


Fig. 1: The messaging structure of message integrity protection and authentication.

data packet is sent first using normal modulation, followed by a cryptographic hash calculated over the message which is encoded using the ON/OFF keying approach (the idea is also shown in Fig. 1). The security of this approach is based on the infeasibility of signal cancellation in the wireless channel, which ensures that only unidirectional bit modification is feasible, i.e. attacker could only change OFF slot into ON slot but not in the opposite direction. Besides, according to the second preimage resistance property of Hash functions, it is computationally infeasible for the attacker to compute a new message with the same Hash result. Therefore any tampering with the original message will be detected (w.h.p.). The authentication property is derived based on $authentication\ through\ presence$ [10], that is, the received message is authorized if and only if the receivers verify only one message is received from the intended transmitter and has not been modified. Anti-signal-cancellation is achieved by setting the signal to be random in each ON slot, and based on the assumption that attacker could not extract any knowledge of the source signal and the channel thus it cannot cancel the signal.

However, this assumption is too strong because practical signal cancellation attack has been demonstrated [11], which uses a pair of directional antennas to relay the source signal such that the phase differs by $k\pi$ from the direct signal at the receiver. The signal cancellation attack aims at completely canceling out the received signal at the receiver, by assuming the attacker knows the transmitted source signal x (or a correlated version of it). This is achieved in [11] by using directional antennas, such that the attacker obtains x from A in real time, and it has almost complete knowledge of the direct channel from A to B (which is a stable indoor channel). Through signal cancellation attack, the attacker has the potential to cancel/modify any signal in wireless channel. Considering that receiver in ON_OFF scheme decodes message via energy detection, when encountering signal cancellation attack, the message integrity cannot be protected. Thus, it is essential to investigate the possibility of signal cancellation in the real-world, so as to provide quantitative security guarantees.

2.2 Channel Randomization

Recent studies in wireless communication show that due to the inherent randomness of wireless channel such as multipath, even small motions of the antenna can create large variations on CSI [17], which makes channel randomization a promising technology in preventing attackers from estimating accurate CSI. Here, we briefly discuss the previous works on using channel randomization method to defend passive attacks and active attacks.

2.2.1 Countering Passive Attacks

The channel randomization approach in [18]–[20] was proposed to defend eavesdroppers for secrecy purpose. In [18], the transmitter is equipped with eight antennas that are rotated with a fan motor at a constant speed. In every transmitter's ON and OFF states, a micro-controller randomly chooses an antenna to activate. However, since the fan motor rotates at a constant speed, it is not difficult for the attacker to obtain and predict the positions of antennas. For an eavesdropper who is capable of conducting offline experiments to measure the CSI of possible paths, once the attacker gets the positions of antennas, the only unknown variable left for attacker is which antenna is activated. Since only eight antennas are used, the eavesdropper could effectively decode the message using brute force.

On the other hand, [19] and [20] also use RA to randomize wireless channel, which is similar to us. However, [19] and [20] focus on protecting the secrecy of generated key. More specifically, [19] and [20] utilize the reciprocity of radio wave to create the same received signal strength indicator (RSSI) sequence at the transmitter and receiver, then extract a common secret key from the received RSSI sequence. Thus, the main purpose of [19] and [20] to use RA is to prevent the eavesdropper from obtaining the exact CSI between legitimate pairs. While an eavesdropper can use offline methods to estimate the CSI more accurately, a signal cancellation attack must be launched in an online fashion, which fundamentally changes how we model the attacker. Actually, for our type II attacker, it is assumed to be capable of obtaining exact channel for every symbol. The main idea to defend type II attacker is to capture the online nature of signal cancellation attack process, and exploit the randomness of CSI in temporal domain to prevent the attacker from predicting future CSI. Besides, the independence of the generated key between legitimate pairs and the key obtained by the eavesdropper is crucial criterion for secret generation, however, for signal cancellation attack, the energy detection probability is the most important criterion that needs to pay attention to.

2.2.2 Countering Active Attacks

Except for defending against passive attackers like eavesdroppers, channel randomization can also be used to counter active attacks such like jamming. For example, [21] proposes a mechanical beam-forming approach and auto-configuration algorithm to track the powerful jammer and weaken its signal. In [21], the attacker emits a powerful jamming signal to interfere with the communication between legitimate pairs. By changing the angle and distance of the two antennas placed at the receiver, the optimal beam pattern which maximizes the signal-to-jamming (SJR) can be configured and cancel the jamming signal. However, signal cancellation attack is different from tradition jamming attack (where the jamming signal is not correlated with the legitimate signal). First, the goal in our work is to prevent legitimate signal from being canceled, while in jamming they aim at canceling out the external signal. Second, the strategies that are proposed to defend jammers are not suitable for our model. The key to signal cancellation attack is the energy detection probability, therefore, a more powerful

traditional jamming signal actually strengthens the received signal, which enhances the energy detection probability and helps to protect message integrity. Besides, since the signal cancellation attack can be carried out on every symbol, forming antenna beams mechanically is too slow to counter signal cancellation attack in practice.

Our previous work [1] achieves message integrity protection over signal cancellation by using an electric fan blowing the aluminum foil strips attached on the transmitter to introduce external disturbance in wireless channel. However, the disturbance introduced by a fan is tiny. Considering that two channels which are close to each other are highly correlated [22], [23], it might be the case that the attacker can cancel out most part of the received signal power via powerful devices. Besides, randomizing wireless channel via fan is not a systematic way in practice. Taken the considerations above, we propose to randomize wireless channel via RA in this paper. Many parameters in our new approach are controllable, which provides us a more systematic way to study the performance and security of the wireless system.

2.3 Quantifying Adversary's Knowledge in Signal Cancellation Attack

Previous results on the signal cancellation attack are qualitative [11], which show that a static environment leads to higher chance of cancellation. Signal cancellation attack can be seen as one of the special cases of tradition correlated jamming. In Médard's work on studying the capacity of wireless channels under correlated jamming, the channel is assumed to be constant and known by the jammer [24]. Later, Kashyap et. al. expand the study on channel capacity under correlated jamming to MIMO case and assume the CSI is totally random and the attacker only knows the statistics [14]. Some other theoretical results in correlated jamming follow similar assumption, that is, the legitimate pair's CSI h is assumed to be either perfectly known by the attacker, or not known but only statistics are available. However, in practice this is often not the case. Instead, the attacker's knowledge about the channel can lie between these two extremes. And how to quantify the attacker's capability remained as an open problem. Intuitively, the more accurate the attacker could estimate the legitimate pair's channel h, the more effective it could launch the correlated jamming attack. Therefore, we can use the correlation coefficient $r_{h\bar{g}}$ to quantize the attacker's capability, where g denotes the attacker's estimation of h.

Generally, the attacker can exploit correlations in three domains to obtain knowledge of legitimate h: spatial domain, temporal domain, and frequency domain. In the spatial dimension, previous works [22], [23] demonstrated high correlations between channels where the receivers (or transmitters) are close to each other (typically within half wavelength). He et. al. [25] even showed that the attacker can obtain a very accurate estimation of the legitimate pair's channel by placing multiple eavesdroppers around the legitimate receiver. The idea is to let all the eavesdroppers measure the channel simultaneously, and then combine them into a linear minimum mean square error (LMMSE) estimator. The estimation error can decrease to zero with increased number of eavesdroppers in some cases.

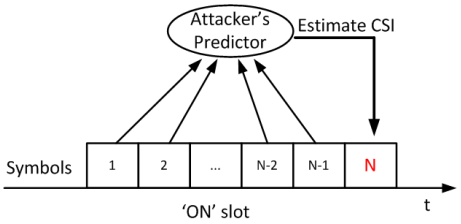


Fig. 2: Example of CSI prediction attack.

It has also been shown by previous works that channel is self-correlated in temporal domain. The correlated time scale is typically measured by the channel coherence time, which is usually several ms in dynamic environments and hundreds of ms in static environments.

Similarly, channel correlation exists in the frequency domain. The attacker can also exploit CSI measurements made in adjacent channels to derive a better estimate of the CSI in the frequency used by the legitimate pair.

In a word, the attacker could leverage channel correlation in any of the three domains and combine them. Such correlation should be considered in the threat model and design of any anti-signal-cancellation based integrity protection scheme.

In this paper, we first derive a theoretic result showing that the attacker's successful cancellation probability increases with its channel correlation with the legitimate one. However, in reality it is difficult (if not impossible) to know the attacker's capabilities in advance (e.g., location, device type, number), and it seems hopeless to upper-bound the attacker's knowledge about the legitimate channel. Fortunately, since signal cancellation is an active attack, it is only effective when attacker's signal is in the same frequency. Also, it must be timely – attacker's channel estimation needs to be done in real-time without any delay, otherwise the cancellation opportunity will be missed. Therefore, even though the attacker can accurately measure the historical legitimate CSI via spatial and frequency domain correlation, it still needs to predict the CSI in the present (and future) in order to generate its own correlated signal (illustrated in Fig. 2). Any approach to obtain the current channel knowledge through measurements takes time, and after that the optimal cancellation opportunity is already missed. That means, we can exploit the intrinsic time-domain unpredictability of the legitimate channel to prevent it from knowing the future CSI. To do so, in our scheme the legitimate TX/RX quantify the CSI's self-correlation in the time domain and use that to bound the knowledge of attacker. On the other hand, from the attacker's point of view, except for CSI prediction attack, processing and relaying the received signal which results in a correlated version of legitimate signal at the receiver, if attacker's physical channel is directly correlated with the legitimate one is also a feasible strategy. In this case, the key to defending strategy is to increase the randomness of CSI in spatial domain instead of temporal domain.

3 Model and Assumptions

3.1 System Model

In our model, Alice communicates with Bob through a wireless channel. There are two types of transmission modes. In the first one (normal mode) a message is transmitted

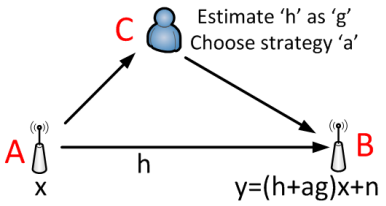


Fig. 3: The system model

using standard modulation and data rates, such as 802.11 and OFDM. The second one is called the ON/OFF keying mode, where information bits (like the hash of a normal message) are all encoded using ON/OFF keying combined with unidirectional error detection codes (e.g., Manchester coding). In each ON slot, a normal packet with random content is transmitted, while in OFF slots Alice remains silent. For this mode, Bob uses energy detection to decode the received signal. Periodically (e.g., per symbol interval), Bob obtains a received signal strength (RSS) and compares it with a threshold (α). If the RSS is larger than α for N_s samples then an ON slot is detected. We assume each transmitted signal $x \in \mathbb{C}$ is arbitrary. The channel state $h \in \mathbb{C}$ between Alice and Bob is modeled under Rayleigh fading with additive white Gaussian noise n in outdoor environments, and Rician model in indoor environments.

3.2 Threat Model

The attacker's general goal is to break integrity protection, i.e., modify the message without being detected. For the normal mode, we assume the adversary can arbitrarily eavesdrop, inject, modify, replay, and block the message (standard Dolev-Yao model). For the ON/OFF keying mode, we assume an attacker C who knows the exact transmitted signal x, and C's goal is to cancel out the signal received at Bob. To learn x in real-time, C can place a directional antenna closely to the legitimate transmitter A. To create and deliver a correlated signal at B, C will utilize x and her "knowledge" about the CSI h from A to B. Essentially, C possesses a correlated version of h denoted as g (correlation coefficient denoted as $r \in [0, 1]$), as shown in Fig. 3.

There are three types of attackers in our model depending on their attack modes. We always assume the attacker cannot replace A or B, or simply block the communication using a Faraday Cage. We do not restrict the number and type of devices the attacker may have. It can either generate its own signals or process and relay the signals from A to B.

Type I: This type of attacker relies on statistical or background information to estimate h, but makes no effort to obtain the accurate measurement of h. For example, channel propagation models can be used to derive the stable (Line-of-Sight/LoS) part of the CSI based on the distance, and large-scale fading/shadowing effects can also be predicted. However, the attacker cannot derive a correlated version for the dynamic/small-scale part. This model is adopted by [11] under a stable indoor scenario, where A-B, A-C and C-B channels are all assumed constant.

Type II: This type of attacker can obtain up-to-date and correlated estimation g about A to B's CSI using information from any of the three domains mentioned in the previous section. For example, it could place multiple receivers close to B, and measure the channel for each transmitted symbol continuously. In the worst case, it obtains the exact A-B channel for every symbol in the past and uses them to predict the future CSI. After estimating h as g, the attacker can decide the cancellation strategy a and send its own signal agx to B.

Type III: Note that type II attack model is too theoretical to be used in practice since it requires the attacker to place multiple receivers to measure the channel and combine all estimations, which is costly and computationally complex. Actually, the attacker can easily relay the correlated source signal after processing with one device. Thus, we propose type III attacker to model a more practical attacker. Instead of estimating and predicting future CSI, a type III attacker exploits the intrinsic spatial correlation between channel A-C and A-B, by multiplying the received correlated source signal from A (gx) with cancellation strategy a and relaying it to the receiver via a stable channel (or the other way around). Though in practice, the attacker cannot send its signal to the receiver without any attenuation, the attacker can use powerful directional antennas to relay processed signal to the receiver, for which the channel can be regarded as stable. Note that the type III attacker is more general than that in [11], since in our model the attacker is capable of processing received signal before relaying it, whereas in [11] the attacker only relays the signal.

In a word, the Type I attacker could only get the knowledge about the stable part of CSI, while the type II and III attacker could also get partial knowledge of the dynamic part. We note that the type II and type III attack models are stronger than previous works [10], [11], [15], [16], as the attacker can do real-time signal processing to generate a correlated cancellation signal based on source x and the correlated CSI. In addition, type III is more practical than type II attacker, since it is easier to implement in practice.

4 Optimal Strategies for Signal Cancellation Attack and Defense

4.1 Game Theoretic Framework

In this section, we theoretically analyze the signal cancellation attack for one symbol in an ON slot. We model the cancellation and anti-cancellation process as a game. The attacker's goal is to transmit a signal correlated with x such that the detection probability P_d of the combined received signal is minimized at B. Therefore we define the attacker's utility function as $U_a = -P_d$. The legitimate pair's strategy is to maximize the energy detection probability and their utility function is $U_l = P_d$. Obviously, this is a zero-sum game.

For the strategy space, let the attacker generate a linear signal [14], [26], [27] that is $agx + v$, in which a is a variable controlled by attacker, g is attacker's knowledge about h (an estimated or correlated version), and v is additive white Gaussian noise with variance σ_v. Thus the overall received signal will be:

$$y = (h + ag)x + n + v \tag{1}$$

W.l.o.g., we use the Rician model for A-B channel (Rayleigh model is a special case), note that we choose these models since they are representative and can yield closed-form solutions. In this model, the channel h is composed of two

parts: one is the deterministic LoS component h', the other is the random Gaussian distributed fading component h''. Thus the channel is denoted by $h = h' + h''$.

We assume the attacker could estimate the LoS part precisely. The estimation g is further divided into two parts $g = g' + g''$. The attacker's strategy consists of a tuple $\mathbf{a} = [a', a'', \sigma_v]$ corresponding to each component. Its transmit power can be easily derived based on $\mathbf{a}$, g, the power of x and v, and here we assume it is not bounded. To include the attacker's power in its strategy under power constraint will be our future work. On the other hand, the defender's strategy consists of A's transmit power.

Under this model, the received signal can be represented by:

$$y = (h' + a'g')x + (h'' + a''g'')x + n + v \tag{2}$$

4.2 Optimal Attack Strategy

Because the LoS and NLoS signal components are independent of each other, the attacker can cancel the two components separately.

4.2.1 LoS Component Strategy

As the LoS channel component h' is assumed to be precisely known, we have $g' = h'$. Therefore we can easily derive the optimal attack strategy for the LoS component:

Proposition 4.1. *The optimal LoS component cancellation strategy is:*

$$a' = -1 \tag{3}$$

The above indicates that the attacker will reverse the LoS signal's phase to completely cancel it out at the receiver side.

4.2.2 NLoS Component Strategy

Given that the LoS component can be completely canceled, we analyze the optimal attack strategy for NLoS part. We start from deriving the distribution of received power of this component under signal cancellation attack.

Type I attacker. For the type I attacker, the estimated channel g'' is independent from h''. Since the source signal x is randomly distributed, the power detected by receiver is $P_y = \sigma_x^2|h''|^2 + |a''g''|^2\sigma_x^2 + \sigma_n^2 + \sigma_v^2$, where $\sigma_x, \sigma_n, \sigma_v$ are the variance (power) of the source signal and noises, respectively. We can see that the variable $|h''|^2$ follows gamma distribution $\Gamma(1, 2\sigma^2)$ as $|h''|$ is Rayleigh distributed, where $\sigma^2 = \frac{1}{2}E[h''\overline{h''}]$.

Theorem 4.1. *Given detection threshold α, the probability that a symbol within an ON slot be detected under type I attacker's signal cancellation attack is:*

$$P_d(\sigma^2) = e^{-\frac{\alpha - \sigma_n^2 - \sigma_v^2 - |a''g''|^2\sigma_x^2}{2\sigma_x^2\sigma^2}} \tag{4}$$

From the detection probability, we derive the optimal NLoS attack strategy:

Theorem 4.2. *The NLoS part optimal strategy for type I attacker is:*

$$(a'' = 0, \sigma_v^2 = 0) \tag{5}$$

Due to space limitations, the proof is omitted. As shown in Theorem 4.2, the best strategy for type I attacker is to not cancel the NLoS part. This is because, the estimated channel g'' is not correlated with the real channel h''. Thus any non-zero signal will only add more energy at the receiver B, which increases the detection probability instead.

Type II and III attacker. According to the type II and III attacker model, the main difference between them is how they are implemented in practice. Thus we can use the same theory to analyze them. In the power expression $P_y = \sigma_x^2(h''+a''g'')^2+\sigma_n^2+\sigma_v^2$, the component $|h''+a''g''|^2$ follows Gamma distribution $\Gamma(1, 2\sigma^2)$ since $(h'' + a''g'')$ is a CSCG random variable, where $\sigma^2 = \frac{1}{2}E[(h'' + a''g'')\overline{(h'' + a''g'')}]$. In addition, the part $\sigma_x^2|h'' + a''g''|^2$ also follows Gamma distribution $\Gamma(1, 2\sigma_x^2\sigma^2)$, because $\sigma_x(h'' + a''g'')$ is a CSCG random variable.

Theorem 4.3. *Given detection threshold α, the probability that a symbol within an ON slot be detected under type II and III attacker's signal cancellation attack is:*

$$P_d(\sigma^2) = e^{-\frac{\alpha - \sigma_n^2 - \sigma_v^2}{2\sigma_x^2\sigma^2}} \tag{6}$$

According to equation 6, the detection probability is related to the estimated channel g''. Thus we will first analyze the effect of the parameter σ^2 on the detection probability.

Theorem 4.4. *The detection probability $P_d(\sigma^2)$ is a non-decreasing function with respect to σ^2.*

The proof is in Supplementary Material. According to Theorem 4.3, the minimum detection probability is achieved when σ^2 is infinitely close to 0:

$$\lim_{\sigma^2 \to 0} P_d(\sigma^2) = 0 \tag{7}$$

The above result shows, the perfect attack precisely estimates channel h'' such that the attacker's signal is exactly the opposite of the received signal from A to B, thus the original signal will be completely attenuated. However, this is an extreme case in which perfect CSI is assumed known by the attacker. Some previous works are based on this extreme case [14], [24], under which the link from A to B has zero capacity. In this paper we consider a more realistic general case in which the real CSI h'' and the attacker's estimated CSI g'' is correlated with arbitrary $r_{h''\overline{g''}}$.

Theorem 4.5. *The NLoS part's optimal signal cancellation attack strategy is:*

$$(a'' = -\frac{E[h''\bar{g''}]}{\sigma_g^2}, \sigma_v^2 = 0) \tag{8}$$

The proof is in Supplementary Material. Given the optimal strategy of attacker, we can use Eq. (4) in Supplementary Material to derive the minimum variance $\sigma_{min}^2 = \frac{1}{2}\sigma_h^2(1 - |r_{h\bar{g}}|^2)$, where $|r_{h''\overline{g''}}|$ is the correlation coefficient. Substitute it into Eq. (6), we get the minimum detection probability:

$$P_d(\sigma_{min}^2) = e^{-\frac{\alpha - \sigma_n^2 - \sigma_v^2}{\sigma_x^2\sigma_h^2(1-|r_{h''\overline{g''}}|^2)}} \tag{9}$$

From the analysis above, we can see that the minimum detection probability decreases with the increase of attacker's correlation coefficient $|r_{h''\overline{g''}}|$. Also, previous works that either assumed a 0 or 1 correlation coefficient are two extreme cases of our result.

4.3 Optimal Defender Strategy

Next, we analyze the legitimate pair's optimal strategy. From the above, the type I attacker is only a special case of type II and III attacker when $r_{h''\overline{g''}} = 0$. In our model, the signal x is independent of h''. The only transmitter parameter that has influence on the final detection probability is the power σ_x^2. From Eq. (9), we can easily see that the detection probability increases when σ_x^2 increases. In reality, the transmitter's power is limited, thus it indicates that the transmitter should always choose its largest power level to defend against signal cancellation attacks.

4.4 Simulation Results

To show the correctness of our proposed optimal attack strategy, we used Matlab to simulate above theoretical analysis in our previous work [1]. We mainly studied the received signal power in the presence of signal cancellation attack. More specifically, in the NLoS Rayleigh fading channels, we generated two CSI sequences with a given correlation coefficient $r_{h\bar{g}}$ to simulate the legitimate channel and attacker's estimation. The transmitting power was $0dB$ and the channel gain was normalized to 1. The signal was modulated using QPSK and the SNR at the receiver side was set to be $25dB$. The attacker was assumed to know $r_{h\bar{g}}$ and σ_g^2 so as to calculate the optimal attack strategy a. The simulation results we got are: (1) The power of received signal achieves the minimum when the attacker applies the proposed optimal attack strategy, which confirms the correctness of our theoretical analysis. (2) There are three factors that could lead to a higher detection probability in optimal cancellation attack: a lower correlation coefficient, a higher detection threshold and a higher transmitting power.

5 Channel Randomization Approach

In this section, we show the crucial criteria in designing channel randomization approach. Our basic idea is to randomly switch among different radiation modes of a reconfigurable antenna (RA) to change the legitimate CSI.

5.1 Characteristics of Reconfigurable Antenna

An RA is an antenna capable of dynamically rearranging its antenna currents or radiating edges in a controlled and reversible manner [28]. For a p-i-n diode based RA, by changing its structure electronically, it can swiftly reconfigure itself in terms of radiation pattern, polarization and frequency, or combinations of them. In terms of randomizing CSI, we need to prevent the attacker from predicting future CSI from historical CSI sequences (for type II attack), as well as reduce the spatial correlation of CSI (for type III attack). Thus, ideally an RA is expected to have the following two properties for security: 1) the RA should have a large and diverse set of antenna patterns, which have different gains among different spatial directions (resulting in small spatial correlation); 2) for a given spatial direction, the antenna gains across different antenna modes should have high variations (yielding small temporal correlation).

5.2 Antenna Mode Switching Period

For the directional antenna model [29], the CSI is represented as: $h = \sum_{l \in L} f_t(\phi_l, \theta_l) \cdot L_l \cdot f_r(\phi_l^{'}, \theta_l^{'})$, where L_l is the path gain of the lth path and $f(.)$ is the antenna-specific characterization function which models the transmitter and receiver gain of the direction from which the signal is transmitted and received. Since the antenna gain of RA is different for a given direction under different antenna modes, we can randomize the wireless channel via randomly switching the modes of RA. Besides, according to a recent study in MIMO [17], the motion of beam steering can change both the LoS and NLoS components of wireless channel, which also indicates that using RA can create high CSI variations.

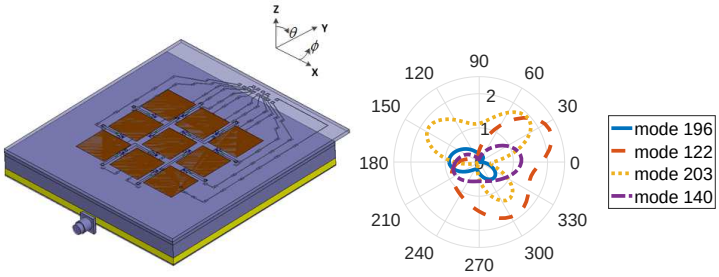
Except for increasing the randomness of CSI, to achieve message integrity protection, it is also important to prevent the attacker from predicting future CSI. Consider the scenario that CSI is changing too slowly (that is, one antenna mode lasts for several symbol periods), once obtaining one exact CSI, the attacker is able to cancel out the following symbols that use the same antenna mode. In practice, the attacker is assumed to take at least one symbol period to estimate CSI [30]. To prevent the attacker from accurately predicting future CSI through historical CSI values, the antenna mode of RA should change at least once in a symbol period. As it is not necessary to change antenna mode too frequently, we let the switching period of antenna mode equal to OFDM symbol duration time in our design.

5.3 Antenna Mode Subset Selection

From Eq. (9), we can see that the correlation and the variance of CSI are two factors that influence the detection probability under attack. The variance of CSI, which ultimately creates a big difference in the RSS is mainly caused by diversity in the antenna gains of different antenna modes. Although there are many states available for RA, the antenna gains of some modes can be very small, which can result in low detection probability even before cancellation affecting the decoding performance. Intuitively, there is a tradeoff between security and performance: with the increase of the number of candidate antenna modes, the randomness and variance of CSI will increase due to higher variety of antenna radiation patterns, however, the detection probability without cancellation will decrease since there are more antenna modes with small gains. Thus, we need to find a subset of antenna modes to optimize the balance between security and performance goals. The optimal antenna mode subset selection problem can be formulated as follows:

$$\begin{aligned} \max \ & P_d = e^{-\frac{\alpha-\sigma_n^2-\sigma_v^2}{\sigma_x^2\sigma_h^2(1-|r_{h''\overline{g''}}|^2)}} \\ s.t. \quad & P_{d_0} \geq P_s \\ & d_k \in \{0,1\}, \ \forall k \in K, \end{aligned} \tag{10}$$

where Eq. (10) means that without signal cancellation attack the detection probability P_{d_0} should be greater than a minimum threshold P_s, and $d_k = 1$ indicates that the antenna mode k is in the current subset K. As shown in Eq. (12) and (13), σ_h^2 and $|r_{h''\overline{g''}}|^2$ are non-linear functions of the CSI sequence h. Besides, [31] shows that P_{d_0} is also a non-linear function of h. Specifically, assume that the CSI under



(a) (b)

Fig. 4: Subfigure (a) shows 3D View of RA. (b) shows antenna gain in the plane of $\phi = 90°$.

antenna mode k is h_k, then the CSI sequence is randomly sampled from the set of variables $\{h_k | \forall k \in K,\ s.t.\ d_k = 1\}$, whose distributions can be obtained from channel modeling or experimentation. Thus, the formulation above is a mixed integer non-linear programming problem and in general NP-hard. We will present a heuristic method to solve this problem and show our simulation results in Sec. 6.5.

5.4 Multiple Symbols for Message Integrity Protection

We can combine our channel randomization approach with existing message integrity protection schemes. For a general message integrity protection scheme shown in Fig. 1, we only need to activate our channel randomization approach during ON slots and synchronization phase, since only those messages need to be protected against cancellation. Considering that the ON slot detection probability grows if there are multiple symbols [16], we can guarantee the energy detection probability of an ON slot by incorporating multiple symbols in it. To do so, we first upper-bound the attacker's knowledge (correlation) under type II and III attack. For the type II attack, the idea is to extract the A-B's CSI by the legitimate receiver B through channel probing, and mimic the attacker's strategy to quantify the intrinsic time-domain correlation in the channel itself, assuming perfect estimation of historical CSI by the attacker. For type III attack, we assume that the attackers can only be located at a certain distance away from the legitimate receiver (and transmitter), which can be implemented by creating a guard zone in practice, otherwise, the attacker can be easily detected. Since the correlation coefficient decreases with the increase of the distance from the attacker to the receiver (this relationship is shown in Table 1, Sec. 5.5), B can estimate the correlation of the channel that is closest to itself (which has most related CSI) to mimic the attacker.

Based on the obtained correlation, we calculate the minimum energy detection probability for each symbol under signal cancellation attack using our theoretical framework. Given a target security requirement (signal cancellation probability for each ON slot is no larger than some threshold), the number of symbols needed in each ON slot can be derived. Then the transmitter applies this parameter during its ON/OFF keying to protect message integrity, while the receiver uses energy detection to recover the source information bits. To enhance efficiency, the transmitter sends a normal message packet followed by Manchester coding and ON/OFF keying of the Hash of the message.

Given the bound of attacker's correlation coefficient, we substitute it along with others parameters (including $\sigma_{h''}$, σ_x, α) into Eq. (9). Then we can derive the detection probability P_d for a single symbol, and the minimum necessary number of symbols n in each ON slot:

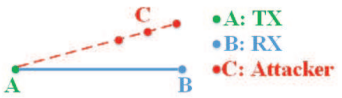


Fig. 5: Preliminary experiment on studying impact of attacker's positions on channel correlation coefficient.

TABLE 1: Impact of attacker's positions on correlation coefficient

Distance(cm)	Correlation coefficient		Variance(dB)	
C-B	RA	OA	RA	OA
10.5	0.5615	0.9890	-35.2791	-53.1417
22.2	0.2421	0.9842	-34.0399	-53.4983
40.9	0.0826	0.9938	-32.7614	-53.7439

Theorem 5.1. *Given the required minimum detection probability in each ON slot P_s, the minimal number of symbols is:*

$$n = \lfloor log_{1-P_d}^{1-P_s} \rfloor \tag{11}$$

The proof is in Supplementary Material.

5.5 Security Analysis

5.5.1 Metrics Affecting Detection Probability

As mentioned before, the correlation coefficient and the variance of CSI are crucial for detection probability. We first present their definitions in Eq. (12) and (13).

The variance of CSI h is defined as:

$$\sigma_h^2 = \frac{1}{N}\sum_{i=1}^{N} h_i^2 \tag{12}$$

where h_i represents a value of CSI sequence h.

The correlation coefficient of CSI sequences h and g is:

$$r_{h\bar{g}} = \frac{\sum_{i=1}^{N} h_i \bar{g}_i}{\sigma_h \sigma_g} \tag{13}$$

Since in our approach, the message integrity protection is achieved by increasing the randomness of CSI, we quantify the average randomness of CSI with entropy.

The entropy of CSI h is defined as:

$$H(h) = -\sum_{i=1}^{N} P(h_i) log_2 P(h_i) \tag{14}$$

where $P(.)$ is the probability mass function of CSI sequence h. Note that for simplicity, the entropy calculated in this way is an upper bound to the real entropy because the autocorrelation in the CSI sequence has not been considered. If it is considered, the entropy rate should be used.

5.5.2 Integrity Protection

For the basic message format in Fig. 1 (which is common to previous works), due to the collision resistance of cryptographic Hash functions, it is infeasible for the attacker to find another $m' \neq m$ such that $H(m') = H(m)$. In addition, if the attacker modifies any one or more bits in the original message, approximately half of the hash bits will flip. For

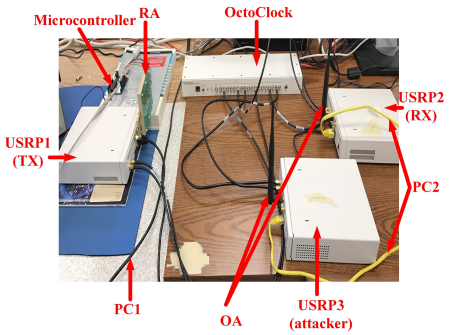


Fig. 6: Experiment setup (the devices here are placed closely to facilitate taking a picture, this is not the actual placement of experiments).

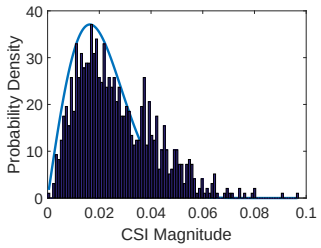


Fig. 7: Frequency histogram of CSI sequences and probability density curve of corresponding Rayleigh distribution of scenario 2 in experiment 1.

TABLE 2: Experiment parameters

frequency	bandwidth	antenna modes	switching time
$2.45GHz$	100MHz	4096	$256\mu s$
E1		E2	
TX-RX	TX-Attacker	TX-RX	TX-Attacker
$120cm$	$96cm$	$360cm$	$340cm$

each flipped bit, one ON slot needs to be converted into an OFF slot. So the probability that the attacker successfully passes verification is approximately $(1-P_s)^{L/2}$ (negligible). Thus, message integrity can be guaranteed under our attack model since we choose n to satisfy a minimum per-ON slot detection probability P_s, such that any tampering with the message m will be detected w.h.p.

6 Experiment

6.1 RA Structure

Fig. 4 (a) presents the 3D view of RA we use in this paper. The reconfigurable parasitic surface consists of 3×3 square-shaped metallic pixels that are connected by 12 p-i-n diode switches [32]. Each switch has ON and OFF status, which brings 4096 possible modes of operation to RA. To show the state diversity of RA, antenna gain in the plane of $\phi = 90°$ for four typical modes is depicted in Fig. 4 (b).

Note that although traditional smart antennas such as switched beam directional antennas can also change their radiation patterns [33], their beam shapes remain in the same direction and their switching is slow. For a typical smart antenna, its switching time is in the order of $100\mu s$ [34]. In contrast, for the RA used in this paper, the switching time is about $0.5\mu s$ [35], which is an extremely short period.

6.2 Channel Randomness and Correlation

To study the impact of attacker's positions on channel correlation coefficient when the transmitter is equipped with RA and OA (omnidirectional antenna) respectively, we conduct a preliminary experiment under 246 typical antenna modes that match our reflection coefficient constraint. Fig. 5 shows the placement of all the devices. In the aspects of parameters, the distance from the transmitter to the receiver (A-B) is always the same, which is $120cm$, while the distance from the attacker to the receiver (C-B) is changing. The results of preliminary experiments are shown in Table 1.

From the Table. 1, we can see that no matter where the attacker is, the correlation coefficient between A-B and A-C is always quite high (which is about 0.98) in OA scenarios, which indicates the high correlation between those two channels. Thus, the attacker could cancel out most of the transmitted message by just simply relaying its received signal. In contrast, when RA is used, A-B and A-C are much more independent (correlation coefficients are below 0.5 in most cases), which shows that the utilization of RA can increase the randomness between two wireless channels.

To quantify the randomness increment introduced by antenna modes and multipath, we calculate the entropy in terms of antenna gain and CSI. The entropy of antenna gain in the direction of $\phi = 90°$, $\theta = 0°$ under 246 typical antenna modes is 6.9. For the entropy of real-world CSI data, we first limit the values of real and imaginary parts of CSI for RA and OA scenarios to the same range. The range is divided into 100 bins and the probability of each CSI value is the joint probability of its real and imaginary parts, thus the largest entropy value is $log_2 10000 \approx 13.3$. In fact, the entropy of the legitimate CSI sequence is about 8.9 and 4.8 in RA and OA scenarios respectively. We can observe that: 1) when RA is used, CSI has greater entropy, which corresponds to more randomness of wireless channel in time-domain; 2) the multipath, noise and other dynamic factors in physical wireless channel lead the entropy of CSI greater than that of antenna gain (6.9) and antenna mode ($log_2 246 \approx 7.9$); 3) due to the online nature of signal cancellation attack, to achieve good cancellation performance, the attacker has to estimate the real and imaginary parts of CSI with high accuracy in every symbol period, which is hard to achieve. Thus, even if the CSI distribution has low entropy (e.g., 9 bits), the attacker's average estimation error can still be high.

6.3 Attack Effectiveness Evaluation

6.3.1 *System Layout and Parameter Selection*

We set up three USRP N210 devices with SBX daughter boards using LabVIEW on a table in an indoor lab, the experiment's setup is shown in Fig. 6. We conduct two experiments, since the distance between transmitter and receiver (TX-RX) is $120cm$ in experiment 1 (E1), which is slightly short. To make our study more systematic and practical, we conduct experiment 2 (E2) and increase the distance of TX-RX to $360cm$. Considering that for the attacker in practice, it always wants to get close to the legitimate receiver to obtain more exact CSI and signal data, however, it can be easily detected if it is too close. Therefore, we put the attacker $25.8cm$ away from the receiver in both experiments.

We implement an OFDM transmitter, receiver and attacker on the USRP devices using LabVIEW. The transmitter sends packets with known symbols in the $2.45GHz$ band with bandwidth set to $100MHz$. In order to obtain the true physical channel state, we connect the three USRPs with an OctoClock to synchronize their clocks to eliminate the impact of frequency and phase offset. Especially, the type II (signal injection) attacker needs to synchronize its clock with original signal at symbol level. This can be done by first synchronizing at the packet level (e.g., using the techniques for reactive jamming [36]), and as long as the attacker's clock does not differ much from the legitimate device's, they will be synchronized for the duration of a short packet. For type III attacker, since it only relays the signal, the synchronization at symbol level is easy. In reality, if the devices are far apart and no cable is available, we can use accurate external clocks such as GPS clocks to synchronize TX/RX. The receiver extracts the frequency domain CSI for each symbol in one OFDM subcarrier from baseband before equalization, and we analyze the CSI sequence on the computer using Matlab. The QPSK is used and each OFDM symbol contains 320 QPSK symbols. Though our OFDM system has 256 sub-channels, for simplicity, we only estimate the CSI for one of them. As mentioned in Sec. 5.2, the switching time for RA should set to be one OFDM symbol duration at most. Therefore, we connect RA with an Arduino Uno Rev 3 programmable microcontroller [37] to randomly switch antenna mode within 4096 available modes. Each mode lasts for $256\mu s$, which equals to OFDM symbol period. All parameters are shown in Table 2.

6.3.2 Experimental Strategies

We tested two scenarios for both type II and III attackers: the transmitter is equipped with OA and RA in scenario 1 and 2 respectively; In both scenarios, the receiver and attacker are equipped with OA. For type II attacker, to generate the attacker's estimated CSI sequence g, we assume the attacker uses a simple autoregression technique to estimate h. That is, the attacker takes the CSI of h at time t_n as the CSI of g at time t_{n+1}.

For the much more practical type III attacker, we implement two cancellation attack strategies: **strategy 1:** the attacker only relays the received signal; **strategy 2:** the attacker processes the received signal with optimal attack strategy proposed in Sec. 4.2.2 and then relays it. It is worth noting that when the transmitter is equipped with RA, the CSI is randomly changing according to antenna mode. Thus, in the second scenario, the LoS and NLoS components of CSI are both unknown to the attacker. Considering the little knowledge of the LoS component to the attacker, the optimal strategy for the attacker in scenario 2 is to regard the whole CSI as its NLoS component, and directly apply NLoS component strategy proposed in Sec. 4.2.2 to implement cancellation. In contrast, the attacker in scenario 1 adopts both LoS and NLoS component strategies due to the feasibility and optimality considerations. Besides, since antenna modes are randomly changed in scenario 2, the CSI h is not exactly the same as Rayleigh distribution, but it is somewhat close to Rayleigh. This is because in the direction of the legitimate channel, the LoS part of CSI may not exist under some antenna modes. In this case, the

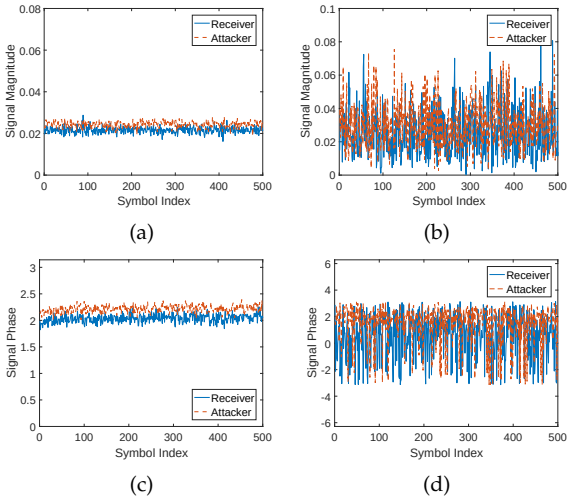


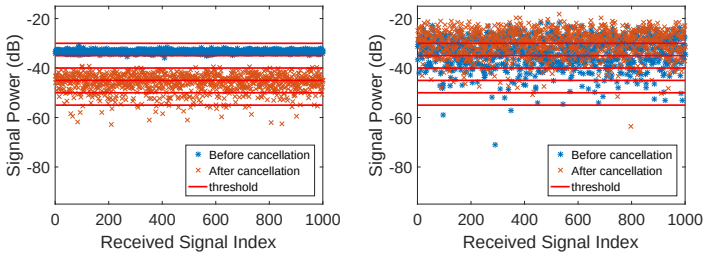
Fig. 8: Magnitude and phase of received signal at the receiver and attacker in experiment 1. Left: OA. Right: RA

CSI is mainly composed of its NLoS part which is caused by multipath effects (of which the distribution is Rayleigh distribution for indoor environment). To verify this, the frequency histogram of CSI sequences and the probability density curve of corresponding Rayleigh distribution in scenario 2 for experiment 1 are illustrated in Fig. 7. The factors mentioned above make the strategy in Sec. 4.2.2 may no longer be optimal for RA, but we will show in Sec. 6.3.3 that it is still a better strategy when comparing with strategy 1 (which is similar to the attack model in [11]).

6.3.3 Evaluation of Cancellation Results

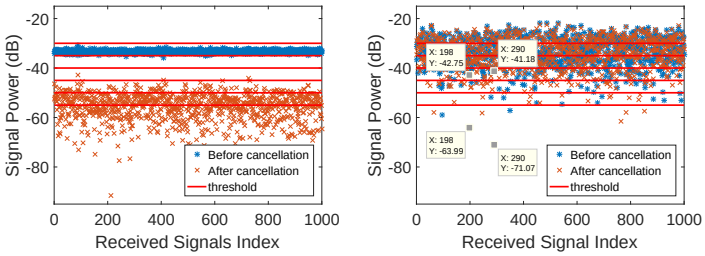
In this part, we first implement cancellation with type III attacker via the two strategies in Sec. 6.3.2, more specifically, the attacker utilizes the spatial correlation between A-B and A-C to get gx, then we process and relay gx in Matlab to simulate the online attack in the stable C-B channel.

A. Experiment 1: Fig. 9 and Fig. 10 show received signal power encountering type III attacker in scenario 1 and 2 respectively. From Fig. 9 (a) and Fig. 10 (a), we can see that strategy 2 performs better, which verifies the effectiveness of our optimal attack strategy. However, though strategy 2 achieves better cancellation performance in a traditional wireless communication system, it does not benefit the attacker in experiment 1 even if RA is used. In Fig. 12 (b), when the transmitter is equipped with RA, the detection probability after cancellation almost stay the same as before. This is because the LoS component of CSI is changing according to RA's antenna state but not every antenna mode (also the dynamic factors) in the direction of A-B and A-C follows the relationship defined by the calculated average correlation coefficient. For example, in Fig. 10 (b), for $198th$ symbol, its power is $-42.75dB$ and $-63.99dB$ before and after cancellation respectively, which indicates good cancellation result. However, for $290th$ symbol, instead of reducing its power, the attacker's cancellation strategy makes its power increases from $-71.07dB$ to $-41.18dB$. In this case, the attacker weakens its own cancellation performance due to the random change of antenna mode. In general, half of the legitimate CSI follows the linear relationship defined by attacker's strategy, however, the remaining CSI changes in



(a) (b)

Fig. 9: Type III attacker: received signal power under strategy 1 in experiment 1. Left: transmitter equipped with OA. Right: transmitter equipped with RA



(a) (b)

Fig. 10: Type III attacker: received signal power under strategy 2 in experiment 1. Left: transmitter equipped with OA. Right: transmitter equipped with RA

the opposite trend. Therefore, the overall detection probability does not change much.

Besides, from Fig. 12 (a), note that the type III attacker who adopts strategy 1 (which is similar to the attacker in [11]) even increases the detection probability in RA scenarios. This is because different multipath caused by diverse antenna patterns leads to phase changes of CSI, and makes the position attacker chose no longer optimal. To illustrate this, let $A_h e^{j\theta_h}$ and $A_g e^{j\theta_g}$ denote the received signal at the receiver and the attacker respectively. Thus, the received signal after cancellation is: $A_h e^{j\theta_h} - A_g e^{j\theta_g} = (A_h cos(\theta_h) - A_g cos(\theta_g)) + j(A_h sin(\theta_h) - A_g sin(\theta_g))$. Therefore, the power of received signal changes from A_h^2 to $A_h^2 + A_g^2 - 2A_h^2 A_g^2 cos(\theta_h - \theta g)$. For an attacker, an effective strategy must satisfy: $A_h^2 + A_g^2 - 2A_h^2 A_g^2 cos(\theta_h - \theta g) < A_h^2$, which is equivalent to $2cos(\theta_h - \theta_g) > A_g/A_h$. In OA scenario, since $A_g \approx A_h$ and $\theta_g \approx \theta_h$, strategy 1 is effective. However, in RA scenario, $A_g, A_h, \theta_g, \theta_h$ are all changing according to antenna mode, the above condition is not always satisfied. In fact, experiment 1 is opposite to this condition for the most of time, thus, strategy 1 weakens attacker itself under the RA scenario.

For type II attack, we first analyze the channel randomness and correlation. The magnitude and phase of the first 500 symbols received by receiver and attacker in scenarios 1 and 2 are depicted in Fig. 8. Since the messages transmitted in both scenarios are the same, the randomness of CSI is equivalent to the randomness of received signal. As we can see, the CSI in scenario 2 has a much higher randomness than that in scenario 1. To verify this, we calculate the auto-correlation coefficient of legitimate CSI sequence and show the result in Fig. 11 (a). We can observe that: 1) the low auto-correlation coefficient of CSI under RA (which is about 0.15) indicates that except for reducing the correlation between two spatial correlated channels, the utilization of RA can also decrease the correlation within CSI sequence in temporal domain; 2) due to the stable indoor environment, the CSI sequence are highly correlated in both temporal and spatial domains when OA is used.

Then we implement strategy 2 for type II attacker and show its cancellation performance in Fig. 11 (b). Comparing Fig. 11 (b) with Fig. 12 (b), we can see that the cancellation performance for type II attacker and type III attacker is similar. However, type III attack is much more practical.

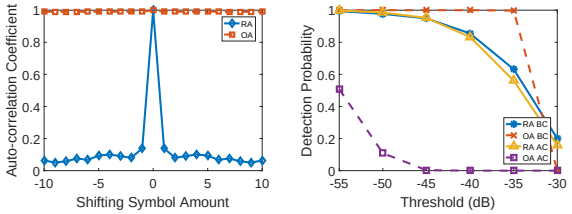
Note that for Fig. 11 (b) and Fig. 12 (b), the detection probability of type II attacker and type III attacker is almost the same, however, the correlation coefficient between h and g for them is 0.0544 and 0.0262 respectively. When threshold=$-45dB$ and the transmitter is equipped with RA, the detection probability under type II attack and type III attack is 0.9399 and 0.9380 respectively. The result seems to be counter-intuitive. In fact, this is because the correlation coefficient is too small so that the variance of CSI becomes the main factor that affects the detection probability.

TABLE 3: Detection Probability of the first case in Table 1

Threshold(dB)	type II attack $r_{h\bar{g}} = 0.0606$	type III attack $r_{h\bar{g}} = 0.5615$
-55	0.9930	0.9880
-50	0.9780	0.9680
-45	0.9129	0.8770
-40	0.7157	0.6650

To show the influence of correlation coefficient to energy detection probability, we calculate the detection probability for the first case in Table 1 under strategy 2. We choose this case because the correlation coefficient between A-B and A-C is 0.5615, which is relatively large compared with other cases. In addition, since the auto-correlation of legitimate CSI is 0.0606 in this case, the spatial correlation coefficient becomes the main factor that dominates the detection probability. The results are listed in Table 3. As we can see, the higher the correlation coefficient is, the lower the detection probability we get, which corresponds to our previous simulation results in [1].

B. Experiment 2: Next, we implement type III attacker for experiment 2 and show our results in Fig. 12 (c) and (d). Comparing (a) with (c) and (b) with (d), we can see that the cancellation results for OA are similar. However, when RA is used, the attacker performs better in experiment 2, which indicates the limitation of RA on randomizing wireless channel. Note that the distance of Attacker-RX is the same for both experiments, thus the angle between A-C and A-B in experiment 2 is much smaller than that in experiment 1 due to the increase of the distance between TX and RX. In this case, the antenna gains in the direction of RX and attacker are almost the same, which means the attacker can obtain a highly correlated CSI sequence. More specifically, for experiment 1, $r_{h\bar{g}} = 0.0262$ and $\sigma_h^2 = -30.9447dB$, but $r_{h\bar{g}} = 0.6723$ and $\sigma_h^2 = -37.1340dB$ in experiment 2. Thus, we can conclude that when the distance between TX and RX increases, the guard zone at the receiver should increase proportionally to guarantee the effectiveness of the channel randomization approach.



(a) (b)

Fig. 11: Subfigure (a) shows auto-correlation coefficient of legitimate CSI sequence under OA and RA in experiment 1; (b) illustrates detection probability encountering type II attacker with strategy 2 in experiment 1

6.4 Performance

Considering that CSI value under some antenna modes of RA can be low, to ensure normal communications after adopting RA, in this part we use the data of experiment 1 to analyze the performance of the message integrity scheme we mentioned in Sec. 5.4. More specifically, we first calculate the number of symbols needed in an ON slot from Theorem 5.1. Then we calculate the bit error rate (BER) and link throughput of legitimate pairs under normal communication scenarios with RA and OA respectively. Before presenting the results, we first show the definition of BER and the calculation of link throughput.

6.4.1 BER

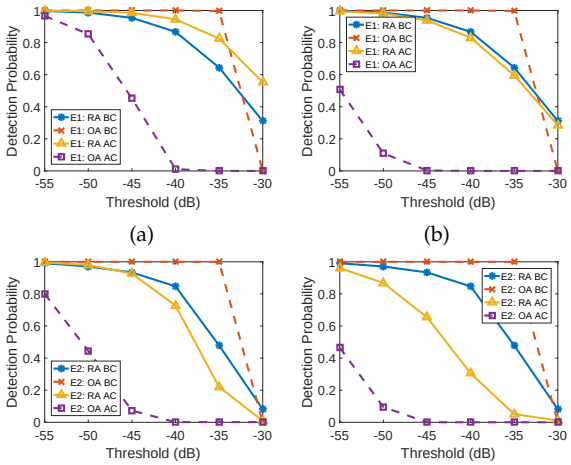
To clarify, the BER we mentioned here is referred as the error that receiver cannot decode the message (that is, the ON slot in message is canceled to the OFF slot), changing OFF to ON does not happen because the noise is very small in our experiments. So only OFF_OFF slots are undecodable, which is an error.

6.4.2 Link Throughput

If we only consider using the ON/OFF keying mode to carry data, given the number of symbols n, the security requirement P_s and the BER p, we can derive the maximum link throughput between A and B: $c = \frac{1-p}{2\lfloor log^{1-P_s}_{1-P_d} \rfloor \cdot \Delta t}$. If we consider both normal mode and the hash ON/OFF encoding, the maximum throughput will be $c' = \frac{(1-p)\cdot L_{data}}{T_{data}+2L\cdot\lfloor log^{1-P_s}_{1-P_d} \rfloor \cdot \Delta t}$, where L_{data} and T_{data} are the bit length and transmission time of a normal data packet respectively, while L is hash length. We can see that the higher the per-symbol detection probability P_d, the lower the BER and the higher the throughput.

6.4.3 Result

For simplicity, we evaluate the ON/OFF keying mode only. As shown in Table 2, the symbol duration Δt is $256\mu s$. We set the security requirement for successfully detecting each ON slot to be $P_s = 0.9999$. Since the transmitter cannot tell whether there exists the signal cancellation attack or not, to guarantee detection probability, the transmitter always use the detection probability of a single symbol under optimal attack P_d (the same as detection probability in Fig. 10 with cancellation) to calculate the number of symbols needed. Then we calculate the BER and link throughput in normal communications (without cancellation attack).



(a) (b) (c) (d)

Fig. 12: Type III attack, the detection Probability at the receiver. (a)(c): under strategy 1; (b)(d): under strategy 2 (BC: before cancellation; AC: after cancellation)

The results of the number of symbols, BER and link throughput under RA and OA scenarios are shown in Table 4. We can have several observations: 1) As the threshold α increases, the energy detection probability in each ON slot decreases, which leads to an increasing number of needed symbols and a decreasing link throughput, but the system is more tolerant to noise/interference; 2) The BER is lower when number of symbols is larger. Note that 1) since the detection threshold is set based on the noise level. The higher the noise level, the higher the threshold should we use, which can decrease the false positive rate for OFF slots. But the tradeoff is that this will decrease the true positive probability (for ON slots) and also the link throughput eventually; 2) the BER for OA scenarios is not exact, because the large number of symbols needed in an ON slot leads to enlarged length of CSI sequences, however, the CSI sequence length in our experiment is 1000, which is not long enough. The value of BER can be remedied by measuring longer CSI sequences in the experiment.

6.5 Impact of Antenna Mode Selection

Here we use the data obtained in experiment 1 to simulate the problem in Sec. 5.3. Since the channel is quite stable in indoor environments, we assume the CSI under a specific antenna mode stays the same in every measurement. Due to the experimental limitations, we tested 2166 antenna modes and corresponding CSI sequences. Based on the CSI we obtained, we first set some thresholds (β) for CSI magnitude to get a CSI subset that has higher magnitudes (which is equivalent to select antenna modes that lead to high CSI magnitude). 1000 QPSK symbols are generated with Matlab to simulate detection probability under the chosen antenna modes with type III attack. To compare the influence of antenna mode diversity and the threshold of CSI magnitude, we simulate in two ways: a) M1: we cancel the whole CSI directly; b) M2: we take the average CSI as LoS part and implement cancellation after removing average CSI. Note that the M2 here is used to evaluate the randomness of LoS part. In practice, since the type III attacker makes no effort

TABLE 4: Results of symbol number, BER and link throughput under RA and OA scenarios

Threshold (dB)	RA			OA		
	number of symbols	BER	throughput (kbps)	number of symbols	BER	throughput (kbps)
-55	1	0.0060	3.9063	12	0	0.3255
-50	2	0.0020	1.9531	79	0	0.0494
-45	3	0	1.3021	3065	—	—

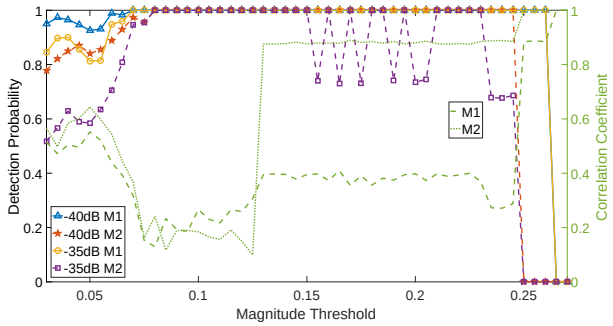


Fig. 13: Detection probability under multiple CSI magnitude threshold, the attack model here is type III attacker with strategy 2 in experiment 1

to estimate h, it cannot implement M2, when evaluating the performance of the attacker, only M1 should be considered. The simulation results are shown in Fig. 13. We can see that: 1) when β is small, the detection probability under M2 is smaller than that under M1, which means the CSI variation becomes smaller after subtracting the average value. Thus, for the subset of antenna modes, the radiation patterns are somewhat similar and the LoS part can be approximated with the average CSI. However, the difference between M1 and M2 reduces with the increase of β, that is, for the left small number of antenna modes, the radiation patterns becomes distinct and the average CSI cannot be regarded as the LoS part; 2) when $\beta = 0.05$, $r_{h\bar{g}}$ reaches the local maximum and becomes the main factor that leads to the local minimum detection probability; 3) when $0.08 \leq \beta \leq 0.26$, no matter what $r_{h\bar{g}}$ is, for M1 the detection probability stays at the optimal value, which implies that the variance of CSI dominates the detection probability and the attacker cannot cancel any message; 4) when $\beta \geq 0.265$, only one antenna mode left, the RA regresses to DA, which results in stable CSI, and in the ideal case, the attacker is able to cancel out the message completely.

7 Conclusion

In this work, we studied the security of physical layer message integrity protection scheme. We established a signal cancellation attack framework to model the attacker's behavior. Based on the analysis results of our strategy, we proposed a physical layer message integrity protection approach with reconfigurable antenna. Comprehensive experiments were implemented to evaluate the security of our proposed channel randomization approach under different attack scenarios and extensive insights were observed from our experimental results: (1) RA can randomize both LoS component and NLoS component of CSI. The LoS part is changed according to the antenna pattern switching and directional gain of antenna mode, and the variation of NLoS part is caused by both multipath and antenna pattern switching; Also, the difference between RA antenna modes can reduce both the temporal correlation within a CSI sequence and the spatial correlation between two CSI sequences; (2) Due to the ability of our channel randomization approach to reduce both temporal and spatial correlation, it is effective in defending against signal cancellation attacks. Besides, due to the online nature of the signal cancellation attack, different from previous works in protecting message secrecy, the entropy of CSI in our approach does not need to be very high; (3) Except for the correlation of wireless channel, the variance of CSI is also a key factor that could affect the detection probability. More specifically, when the correlation coefficient is small, the variance of CSI dominates the detection probability under signal cancellation attack, and the other way around when the correlation coefficient is big. Therefore, for mode selection, there is a tradeoff between mode diversity (which affects the randomness or correlation of CSI sequences) and received signal strength (which is determined by the magnitude of CSI); (4) By restricting the attacker's locations to bound its knowledge of the CSI, multiple symbols can be calculated to guarantee a desired integrity protection goal.

In the future, we will apply the design methodology in this paper to defend against other types of attacks or enhance existing protection mechanisms in wireless systems, such as friendly jamming. Also, we plan to extend our defense framework to the case of MIMO.

References

[1] Y. Hou, M. Li, R. Chauhan, R. M. Gerdes, and K. Zeng, "Message integrity protection over wireless channel by countering signal cancellation: Theory and practice," in *ACM ASIACCS*, 2015.

[2] "Top 50 internet of things applications - ranking," http://www.libelium.com/top_50_iot_sensor_applications_ranking/.

[3] S. T. Ali, V. Sivaraman, and D. Ostry, "Secret key generation rate vs. reconciliation cost using wireless channel characteristics in body area networks," in *IEEE/IFIP EUC*, 2010.

[4] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks." in *NDSS*, 2002.

[5] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun, "Loud and clear: Human-verifiable authentication based on audio," in *IEEE ICDCS*, 2006.

[6] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Key agreement in peer-to-peer wireless networks," *Proceedings of the IEEE*, vol. 94, no. 2, 2006.

[7] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using camera phones for human-verifiable authentication," in *Security and privacy, 2005 IEEE symposium on*, 2005.

[8] L. H. Nguyen and A. W. Roscoe, "Authentication protocols based on low-bandwidth unspoofable channels: a comparative survey," *JCS*, vol. 19, no. 1, 2011.

[9] T. Perkovic, M. Cagalj, T. Mastelic, N. Saxena, and D. Begusic, "Secure initialization of multiple constrained wireless devices for an unaided user," *IEEE Trans. Mobile Comput.*, vol. 11, no. 2, 2012.

[10] S. Čapkun, M. Čagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava, "Integrity codes: Message integrity protection and authentication over insecure channels," *IEEE Trans. Dependable Secure Comput.*, vol. 5, no. 4, 2008.

[11] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun, "Investigation of signal and message manipulations on the wireless channel," in *ESORICS*, 2011.
[12] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *Security and Privacy (SP), 2013 IEEE Symposium on*, 2013.
[13] M. Schulz, A. Loch, and M. Hollick, "Practical known-plaintext attacks against physical layer security in wireless mimo systems." in *NDSS*, 2014.
[14] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on mimo gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, 2004.
[15] S. Gollakota, N. Ahmed, N. Zeldovich, and D. Katabi, "Secure in-band wireless pairing." in *USENIX security symposium*, 2011.
[16] Y. Hou, M. Li, and J. D. Guttman, "Chorus: scalable in-band trust establishment for multiple constrained devices over the insecure wireless channel," in *ACM WiSec*, 2013.
[17] F. Adib, S. Kumar, O. Aryan, S. Gollakota, and D. Katabi, "Interference alignment by motion," in *ACM MobiCom*, 2013.
[18] H. Hassanieh, J. Wang, D. Katabi, and T. Kohno, "Securing rfids by randomizing the modulation and channel." in *NSDI*, 2015.
[19] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, 2005.
[20] R. Mehmood, "A study of reconfigurable antennas as a solution for efficiency, robustness, and security of wireless systems," 2015.
[21] T. D. Vo-Huu, E.-O. Blass, and G. Noubir, "Counter-jamming using mixed mechanical and software interference cancellation," in *ACM WiSec*, 2013.
[22] P. Kyritsi, D. C. Cox, R. A. Valenzuela, and P. W. Wolniansky, "Correlation analysis based on mimo channel measurements in an indoor environment," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 5, 2003.
[23] P. L. Kafle, A. Intarapanich, A. B. Sesay, J. McRory, and R. J. Davies, "Spatial correlation and capacity measurements for wideband mimo channels in indoor office environment," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, 2008.
[24] A. G. M. Médard, "Capacity of correlated jamming channels," in *Allerton Conference on Communications, Computing and Control*, 1997.
[25] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?" in *IEEE INFOCOM*, 2013.
[26] S. Shafiee and S. Ulukus, "Capacity of multiple access channels with correlated jamming," in *IEEE MILCOM*, 2005.
[27] ——, "Mutual information games in multiuser channels with correlated jamming," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, 2009.
[28] J. T. Bernhard, "Reconfigurable antennas," *Synthesis lectures on antennas*, vol. 2, no. 1, 2007.
[29] E. Anderson, G. Yee, C. Phillips, D. Sicker, and D. Grunwald, "The impact of directional antenna models on simulation accuracy," in *IEEE WiOPT*, 2009.
[30] S. Ahmadi, *LTE-Advanced: a practical systems approach to understanding 3GPP LTE releases 10 and 11 radio access technologies*. Academic Press, 2013.
[31] R. Ujjinimatad and S. R. Patil, "Mathematical analysis for detection probability in cognitive radio networks over wireless communication channels," *The Journal of Engineering*, vol. 1, no. 1, 2014.
[32] Z. Li, E. Ahmed, A. M. Eltawil, and B. A. Cetiner, "A beam-steering reconfigurable antenna for wlan applications," *IEEE Trans. Antennas Propag.*, vol. 63, no. 1, 2015.
[33] R. Ramanathan, "On the performance of ad hoc networks with beamforming antennas," in *ACM MobiHoc*, 2001.
[34] V. Navda, A. P. Subramanian, K. Dhanasekaran, A. Timm-Giel, and S. Das, "Mobisteer: using steerable beam directional antenna for vehicular network access," in *ACM MobiSys*, 2007.
[35] E. Ahmed, A. M. Eltawil, Z. Li, and B. A. Cetiner, "Full-duplex systems using multireconfigurable antennas," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, 2015.
[36] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: reactive jamming in wireless networks: how realistic is the threat?" in *ACM WiSec*, 2011.
[37] A. Inc., "Arduino uno," https://store-usa.arduino.cc/products/.

Yanjun Pan is a Ph.D. student at The University of Arizona. She received her B.S. degree from Nanjing University of Aeronautics and Astronautics in 2016. Her research interests include wireless networks and security.

Yantian Hou received his B.S. and M.S. degree in Electrical Engineering Department from Beijing University of Aeronautics and Astronautics in 2009 and 2012 respectively. He received his Ph.D. degree in Computer Science Department at Utah State University in 2016. He joined the Department of Computer Science, Boise State University as an Assistant Professor in 2016. His research interests include wireless network and security, and applied cryptography.

Ming Li (M'11) is an Associate Professor in the Department of Electrical and Computer Engineering of University of Arizona. He was an Assistant Professor in the Computer Science Department at Utah State University from 2011 to 2015. He received his Ph.D. in ECE from Worcester Polytechnic Institute in 2011. His main research interests are wireless networks and security, with current emphases on wireless network optimization, wireless security and privacy, and cyber-physical system security. He received the NSF Early Faculty Development (CAREER) Award in 2014, and the ONR Young Investigator Program (YIP) Award in 2016. He is a member of both IEEE and ACM.

Ryan M. Gerdes is an Assistant Professor in the Department of Electrical and Computer Engineering at Virginia Tech. He received his PhD. in electrical engineering from Iowa State University for his work on device fingerprinting in August 2011. From 20112016 he was an Assistant Professor at Utah State University. His research interests include cyber-physical systems security, with an emphasis on the operation of autonomous systems in unknown, uncertain, and adversarial environments, device fingerprinting, embedded systems security, sensor security, controls security, and cybersecurity.

Kai Zeng received the Ph.D. degree in electrical and computer engineering from Worcester Polytechnic Institute (WPI), Worcester, MA, USA, in 2008. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, the Department of Computer Science, and the Center for Secure Information Systems, George Mason University, Fairfax, VA, USA. His current research interests include cyberphysical system security and privacy, physical layer security, network forensics, and cognitive radio networks. Dr. Zeng currently serves as an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He received the Sigma Xi Outstanding Ph.D. Dissertation Award from WPI in 2008, the Excellence in Postdoctoral Research Award from UCD in 2011, and the U.S. National Science Foundation Faculty Early Career Development (CAREER) Award in 2012.

Md. A. Towfiq received the B.S degree from Bangladesh University of Engineering and Technology, Dhaka, Bangladesh, in 2013 and currently a Ph.D. Candidate at Utah State University, Logan, UT, USA. His research interests include multi-functional reconfigurable antenna, phased array, mm-wave antenna and microwave circuits.

Bedri A. Cetiner is a Professor in the department of electrical engineering of Utah State University. From November 1999 to June 2000, he was with the University of California, Los Angeles, as a NATO Science Fellow. From June 2000 to June 2004, he worked as a research scientist at the ECE department of University of California, Irvine. From July 2004 until July of 2007, he worked as an Assistant Professor in the Department of Space Science and Engineering, Morehead State University, Kentucky. In August 2007, he joined Utah State University. He is also Founder, President and CEO of i5 Technologies Inc., Logan, UT. His research focuses on the applications of micro-nano technologies to a new class of micro-/millimeter-wave circuits and systems, and intelligent wireless communications systems with an emphasis on multifunctional reconfigurable antenna equipped MIMO systems. He is the Principal Inventor of nine patented technologies in the area of wireless communications.