Identity-Based Attack Detection in Mobile Wireless Networks

Kai Zeng, Kannan Govindan, Daniel Wu, Prasant Mohapatra

Department of Computer Science, University of California, Davis, CA 95616
Email: {kzeng,gkannan,wud,prasant}@cs.ucdavis.edu

***Abstract*—Identity-based attacks (IBAs) are one of the most serious threats to wireless networks. Recently, received signal strength (RSS) based detection mechanisms were proposed to detect IBAs in static networks. Although mobility is an inherent property of wireless networks, limited work has addressed IBA detection in mobile scenarios. In this paper, we propose a novel RSS based technique, Reciprocal Channel Variation-based Identification (RCVI), to detect IBAs in mobile wireless networks. RCVI takes advantage of the location decorrelation, randomness, and reciprocity of the wireless fading channel to decide if all packets come from a single sender or more. If the packets are only coming from the genuine sender, the RSS variations reported by the sender should be correlated with the receiver's observations. Otherwise, the correlation should be degraded, then an attack can be flagged. We evaluate RCVI through theoretical analysis, and validate it through experiments using off-the-shelf 802.11 devices under different attacking patterns in real indoor and outdoor mobile scenarios. We show that RCVI can detect IBAs with a high probability even when the attacker is half a meter away from the genuine user.**

I. Introduction

Wireless networks are susceptible to various types of attacks due to the "open air" nature of the wireless medium. Identity-based attacks (IBAs) are one of the most serious threats to wireless networks, and they are easy to launch [1]. For instance, in IEEE 802.11 networks, an attacker can sniff the traffic in the network and get to know the MAC addresses of the legitimate users, and then masquerade as a legitimate user by modifying its own MAC address simply using an *ifconfig* command. IBAs are considered to be an important first step in an intruder's attempt to launch a variety of other attacks on 802.11 networks, such as session hijacking, man-in-the-middle, data modification, and authentication-based denial of service.

Certain IBAs, such as deauthentication/disassociation attacks, are feasible mainly due to the fact that management and control frames are not protected in 802.11 networks. Although IEEE 802.11w adds protection to the management frames, it fails to protect against DoS attacks that are equivalent to the deauthentication and disassociation attacks [2]. Furthermore, even with cryptographic mechanisms, the authentication key can still be compromised. If the key is broken, the cryptography-based mechanism will fail and IBAs are still possible.

This research was supported in part by the National Science Foundation through the grant CNS-0709264 and the Army Research Office through the MURI grant W911NF-07-1-0318.

Under the above circumstances, there is an increasing interest in using the physical-layer information or characteristics to detect IBAs in wireless networks [3]–[11]. Received signal strength (RSS) information has been used for IBA detection due to its location distinction property and availability in the network interface card (NIC) of the off-the-shelf devices. RSS profiles are location specific and can be used to flag IBAs in static environments. Although the existing IBA detection schemes work well in a static network, they tend to raise excessive false alarms in a mobile environment where the RSS profiles change over time due to node mobility. Although mobility is an inherent property of wireless networks, little work has addressed IBAs in mobile scenarios.

In this work, we propose a novel Reciprocal Channel Variation-based Identification (RCVI) technique to detect IBAs in mobile wireless networks. Our technique can work even when the attacker is very close to the genuine node and the attacking packets are arbitrarily interleaved with the genuine packets. In RCVI, we assume the sender and receiver can record the RSS information of the bidirectional frames (such as DATA-ACK) with short time interval. Based on the reciprocity of the wireless channel [12], the sender and receiver should observe similar temporal RSS variations of the received frames. Since the RSS variation is mainly caused by channel fading, it is random and unpredictable. Moreover, based on the location decorrelation property of the wireless channel, an attacker cannot observe the same channel variation (which induces the RSS variation) as the sender-receiver channel if it is located several wavelengths away [12].

In RCVI, the receiver asks the sender (associated with an identity) to report the RSS records during their past communication. When there is no IBA, the reported RSS variation should be correlated with the receiver's observation. In case there is an IBA, the RSS records observed by a victim node should be a mixture of the RSS induced by the genuine user and the attacker. Since the attacker cannot figure out the RSS variations observed by the genuine user, its reported records should be less correlated with the victim node's, and the attack can be detected.

RCVI can make use of the readily available RSS measurement of DATA and ACK frames, so it can be implemented

in the current 802.11 systems with minimal overhead. We evaluate RCVI through theoretical analysis, and validate it through experiments using off-the-shelf 802.11 devices under different attacking patterns in real indoor and outdoor mobile scenarios. RCVI achieves desirable detection performance in the tested scenarios. To the best of our knowledge, this is the first work on using reciprocal temporal RSS variations for detecting IBAs in mobile wireless networks. Our technique can be generally applied to any wireless networks, as long as there are bi-directional frames exchanged between the communication parties within a time interval shorter than the channel coherence time.

Our contributions are summarized as follows:

- We propose a new technique (RCVI) to detect IBAs in mobile wireless networks.
- We conduct theoretical analysis on RCVI, and identify its applicability.
- We evaluate RCVI through extensive experiments using off-the-shelf 802.11 devices under different attacking patterns in real indoor and outdoor mobile scenarios.

The rest of this paper is organized as follows. In Section II, we discuss the related work. Section III introduces the system model and attack model. We propose RCVI in Section IV, and provide theoretical analysis in Section V. Section VI covers the experimental methodology. In Section VII, we analyze the experimental results. Related issues about RCVI are discussed in Section VIII. Finally, we conclude this paper in Section IX.

II. Related Work

There is an increasing interest in exploiting physical layer characteristics for detecting IBAs in wireless networks [4], [6], [8], [10], [11], [13]–[15]. The existing non-cryptographic IBA detection mechanisms can be classified into three categories: software-based, hardware/transceiver-based, and channel/location-based fingerprinting [16].

Software-based fingerprinting techniques are essentially based on the unique characteristics and style of the software programs or protocols running on the devices. Frame sequence numbers can be used to detect presence of multiple 802.11 devices using the same MAC address [17]. The traffic patterns (such as packet sizes and destination addresses) of the wireless users have been exploited to identify different users [18]. The disadvantage of software based fingerprint is that it cannot distinguish between different physical devices running the same software.

Hardware/Transceiver-based fingerprinting is a technique to identify individual devices based on the properties of the radios. It can be classified into two categories: signal transient-based identification [19] and modulation domain-based identification [10]. Although this technique shows its effectiveness on identifying different 802.11 NICs, it is vulnerable to impersonation and replay attacks when attackers use software-defined radios (SDR) or high-end arbitrary waveform generators that can mimic the signal signatures [20].

Since the RSS information is readily available in the current wireless device driver, it has been widely used to detect IBAs [4], [8], [11], [21]. Most of the work in this category assumes the users are static. In a mobile scenario, the RSS profiles change over time, and these schemes will generate excessive false alarms. Limited work has considered the mobile scenarios.

The most related work to ours is the DEMOTE system [22]. DEMOTE partitions the RSS trace of a node identity into two classes, and detect the IBA when the two classes have low correlation. However, DEMOTE cannot work when the attacker is close to the genuine node or when the attacking frames come after or before the genuine ones. With regularly interleaved attacking and genuine frames, DEMOTE needs about 150 seconds (or 1500 frames) to detect the IBA with desirable performance. Our RCVI can achieve high detection rate with low false alarm rate even when the attacker is shadowing the genuine node and the attacking frames are arbitrarily interleaved with the genuine frames. RCVI is different from all the existing RSS-based IBA detection schemes as it exploits RSS variations naturally induced by mobility and the reciprocity of the wireless fading channel.

III. System Model

We consider an 802.11-based wireless network and introduce three different parties: a genuine node, a victim, and an attacker. Any of these three parties can be mobile.

We assume there is bidirectional communication between the genuine node and victim which allows them to probe the bidirectional channel characteristics (i.e., RSS) in a synchronized way. In an 802.11 system, this bidirectional channel probing is naturally provided by the DATA-ACK pair even when there is unidirectional data traffic from the genuine node to the victim. All the three parties are assumed to have only one antenna. We will discuss how to extend RCVI to multiple antenna systems in Section VIII.

Without loss of generality, we assume in a communication period, the victim node received M *data frames* from the same MAC address. For each frame, the victim node records its RSS. Assume the victim node sends back a *pairing frame* (e.g., ACK) with a short time interval after receiving each data frame. The M frames might be all sent from a genuine node, or some of them are sent from an attacker. When a genuine node receives a pairing frame, it records the RSS value. We assume the pairing frames are reliable. Our scheme can be easily extended to the case of unreliable pairing frames, which will be discussed in Section VIII.

A. Attack Model

We assume a powerful attacker who can masquerade the genuine node by modifying its own identity into the genuine one's. The attacker can manipulate arbitrary fields in a frame, such as the source and destination IP/MAC addresses, BSSID, sequence number, frame check, and so on. It may even compromise the authentication key after sniffing the communication between the genuine node and victim nodes. That is, the victim node may not be able to use cryptography to prevent/detect IBAs. The attacker can shadow the genuine node. It can overhear all the communications between the

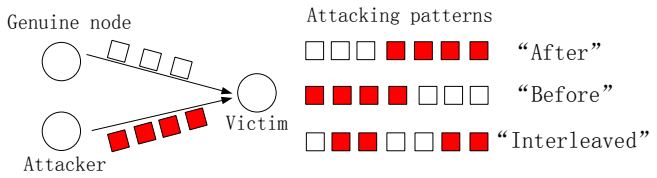


Fig. 1. IBA attack model. "After"/"Before" means the attacker's frames arrive after/before the genuine node's. "Interleaved" means the attacker's frames are interleaved with the genuine node's.

genuine and victim nodes. When the attacker overhears a pairing frame, it records the RSS. It also records the RSS of the pairing frame destined to itself when it launches the IBA. The attacker can launch the IBA at any time during the communication between the genuine and victim nodes. Therefore, the RSS traces of the genuine node and attacker can be mixed in any pattern in time at the victim node.

Fig. 1 shows the roles in the IBA attack and an example of the attacking patterns. The packet interval can be constant or time varying. The attacking patterns are shown in Fig. 1 which will be referred as "After", "Before" and "Interleaved" in the rest of this paper.

IV. RCVI Design

In RCVI, the victim node sends a verification request to the sender for the M RSS records of the pairing frames during their past communication. If there is no attack, the genuine node sends back the M RSS of the pairing frames. If there is an attack, we consider the worst case scenario that only the attacker responds. It is possible that the genuine nodes are still in the network, and may also respond, which will give more advantage for the victim to detect the attacks.

When the attacker responds, we assume it can always make the list length as M by combining the RSS of the pairing frames transmitted to itself and the genuine node.

After receiving the RSS of the M pairing frames, denoted as $\mathbf{S}_p = [S(t'_1), ..., S(t'_M)]$, the victim node constructs K pairs of variation lists using $\mathbf{S}_p$ and its own RSS records $\mathbf{S}_d = [S(t_1), ..., S(t_M)]$. We assume $\mathbf{S}_p$ and $\mathbf{S}_d$ are sorted by time and aligned. For each pair of the constructed lists, the victim node computes the sample correlation coefficient of the two lists. It then computes the mean of these correlation coefficients. If the mean is larger than some threshold, it assumes no attack. Otherwise, it raises an alarm. The flow of RCVI is summarized in Algorithm 1.

Algorithm 1 RCVI flow

Input: $\mathbf{S}_d = [S(t_1), ..., S(t_M)]$, $\mathbf{S}_p = [S(t'_1), ..., S(t'_M)]$
Construct K pairs of variation lists $(\Delta\mathbf{S}_{p_k}, \Delta\mathbf{S}_{d_k})$ $(1 \le k \le K)$
Compute sample correlation coefficient $\hat{\rho}_k$ of each pair of the lists, and $\bar{\hat{\rho}} = \frac{\sum_{k=1}^{K} \hat{\rho}_k}{K}$
if $\bar{\hat{\rho}} \le \rho_{th}$ **then**
  "attack"
else
  "no attack"
end if

The intuition behind RCVI is that if there is no attack, the RSS variations of the genuine node and the victim node should be highly correlated according to the reciprocity. While if there is an IBA, the correlation should be degraded, because the reported RSS record of the pairing frames is a mixture of the "right" and "wrong" RSS. The "right" RSS stands for the RSS of the pairing frames destined to the attacker, while the "wrong" RSS stands for the ones of the pairing frames destined to the genuine node but overheard by the attacker.

Next, we will discuss the method of constructing the RSS variation lists, and the reason we construct multiple of them.

A. Constructing RSS variation lists

Given two RSS measurements $S(t_s)$ and $S(t_e)$, we define the *temporal RSS variation* as:

$$\Delta S(t_s, t_e) = S(t_s) - S(t_e) \quad (1)$$

We call t_s and t_e as the *start time* and *end time* for this variation.

An RSS variation list is a sequence of RSS variations:

$$[\Delta S(t_{s_1}, t_{e_1}), \ldots, \Delta S(t_{s_L}, t_{e_L})]$$

where L is the list length.

Given RSS records $\mathbf{S}_p$ and $\mathbf{S}_d$, Algorithm 2 constructs K RSS variation lists with maximum length N. It runs K rounds. In the k^{th} $(1 \le k \le K)$ round, we first select the k^{th} frame as the start frame. Then we try to find the end frame which is lagged within an interval $[t_l, t_u]$, called the *lag interval*. If we find such a frame (with end time t_j), we compute the first RSS variations ($\Delta S_d(t_i, t_j)$ and $\Delta S_p(t'_i, t'_j)$) and append them into $\Delta\mathbf{S}_{d_k}$ and $\Delta\mathbf{S}_{p_k}$, respectively. We then search for the next variation with start time lagging the end time of the previous variation by an interval of at least t_g, called *guard interval*. We try to find the following RSS variations in the same way, until we run out of the list or reach the maximum list length N. The running time of this algorithm is $O(KN)$.

Algorithm 2 RSS variation lists construction

Input: $\mathbf{S}_d = [S(t_1), ..., S(t_M)]$, $\mathbf{S}_p = [S(t'_1), ..., S(t'_M)]$, K, N, t_l, t_u, t_g
Output: $(\Delta\mathbf{S}_{p_k}, \Delta\mathbf{S}_{d_k})$ $(1 \le k \le K)$
for $k = 1$ to K **do**
  $\Delta\mathbf{S}_{p_k}$=$\Delta\mathbf{S}_{d_k}$=$\emptyset$, $n = 0$, $t_{pre} = -\infty$, $i = k$;
  while $i < M$ **do**
    for $j = i + 1$ to M **do**
      if $t_l \le t_j - t_i \le t_u$ && $t_i - t_{pre} \ge t_g$ **then**
        append $\Delta S_d(t_i, t_j)$ to $\Delta\mathbf{S}_{d_k}$, $\Delta S_p(t'_i, t'_j)$ to $\Delta\mathbf{S}_{p_k}$;
        n++, $t_{pre} = t_j$, $i = j + 1$;
        break;
      end if
    end for
    if $n == N$ **then**
      break;
    end if
  end while
end for

B. Parameter selection

The selection of the lag interval $[t_l, t_u]$ in Algorithm 2 should follow two principles. 1) t_l should be larger than the channel coherence time to ensure the variation is unpredictable

and contains reasonable entropy. Within the channel coherence time, the channel is considered stable or predictable. 2) t_u should not be too large, otherwise, the large scale path loss may dominate the variation, which may cause the variation to be predictable if the mobility pattern of the genuine or victim node is observable by the attacker.

The guard interval (t_g) is used to guarantee the independence among the variations in the list, hence it should be larger than the channel coherence time.

The list length N should be long enough to achieve a good estimation of the correlation coefficient. The K should not be too small. We will show in Section VII that $N > 50$ and $K > 5$ are good choices in practice.

C. Why using RSS variation lists

If the attacker is close to the genuine node, the RSS of the overheard pairing frames would be quantitatively close to that of the data frames received by the victim node, which will hammer the detection rate. Using RSS variation lists to compute the correlation coefficient instead of using the original RSS, we can get away with this.

D. Why constructing multiple variation lists

The purpose of constructing multiple variation lists is to improve the robustness of the detection. It has twofold: 1) smoothing out a "good luck" variation list when there is an attack, and 2) smoothing out a "bad luck" variation list when there is no attack. When the attacking pattern is "Interleaved", the frames used to compute the RSS variations may be those frames spoofed by the attacker. Under this situation, the victim node is likely to observe a high correlation if the reciprocity of the attacker-victim channel holds well, which makes it hard to detect the attack. However, if we choose different start time to construct multiple lists, we may rule out this situation in some lists. The average of the correlation coefficients are likely to be low, and the attack can be detected. When there is no attack, it could also happen that in one pair of lists, some variations are not correlated well and the computed correlation coefficient could be low. Using the average of the correlation coefficients for detection, we can compensate this "bad luck" case.

V. Theoretical Analysis

RCVI is based on the channel reciprocity and temporal variation. In this section, we theoretically analyze how these factors affect the performance of RCVI under the worst case scenario, when the attacker shadows the genuine node. For illustration purpose, we give the following definitions:

- forward genuine channel ($g \rightarrow v$): channel from the genuine to the victim node
- attacking channel ($a \rightarrow v$): channel from the attacker to the victim node
- eavesdropping channel ($v \rightarrow a$): channel from the victim node to the attacker

A. RCVI as a Hypothesis Test

The performance of a detection scheme is usually evaluated by the **receiver operating characteristic** (ROC) curve. The ROC curve plots the false alarm rate α against detection rate β. The false alarm rate is the probability of assuming an attack but there is actually no attack. The detection rate is the probability of detecting the attack when the attack happens. Our goal is to achieve high detection rate with low false alarm rate.

RCVI can be modeled as a hypothesis test:

$$H_0 : \textit{No attack}$$
$$H_1 : \textit{There is an IBA}$$

where H_0 and H_1 are the null and alternative hypothesis, respectively.

According to Algorithm 1, we have

$$\alpha = Pr(\overline{\hat{\rho}} \leq \rho_{th} | H_0) = \int_{\overline{\hat{\rho}} \leq \rho_{th}} f_0(\overline{\hat{\rho}}) d\overline{\hat{\rho}} \tag{2}$$

$$\beta = Pr(\overline{\hat{\rho}} \leq \rho_{th} | H_1) = \int_{\overline{\hat{\rho}} \leq \rho_{th}} f_1(\overline{\hat{\rho}}) d\overline{\hat{\rho}} \tag{3}$$

where f_0 and f_1 are the pdf of the mean of the sample correlation coefficient under null and alternative hypothesis, respectively.

These two pdfs are hard to obtain due to the unavailability of the close-form expression for distribution of the mean of sample correlation coefficients. Even under Gaussian assumption, there is no close form solution for the sample correlation coefficient given the population correlation coefficient [23]. Next, we will derive the population correlation coefficient under no attack and attack. Then we will numerically analyze the performance of RCVI.

B. RSS Variation Correlation under No Attack

1) RSS variation at victim node: According to the empirical measurement, the RSS follows a log normal shadowing fading model [12]. Suppose at time t, the victim node receives a data frame sent from the genuine node, and the genuine node receives a pairing frame at time t'. The RSS of the data frame can be expressed as:

$$S_{gv}(t) = S_g - L_{gv}(d_0) - 10\alpha_{gv} \log\Big(\frac{d_{gv}(t)}{d_0}\Big) + X_{gv}(t) \tag{4}$$

where S_g is genuine node's transmission power in dBm, $d_{gv}(t)$ is the distance between the genuine node and the victim node at time t, α_{gv} is the path loss exponent, d_0 is a close-in reference distance, $L_{gv}(d_0)$ is the path loss at a distance d_0, and $X_{gv}(t)$ is a stationary Gaussian random process of zero mean and standard deviation σ_X.

Assume the distance between the two nodes is not significantly changed during $[t_s, t_e]$ when we construct the variation $\Delta S_{gv}(t_s, t_e)$. According to Eq. (4), we have

$$\Delta S_{gv}(t_s, t_e) \approx X_{gv}(t_s) - X_{gv}(t_e) \tag{5}$$

This is a reasonable assumption when $t_e - t_s$ is small (e.g. tens of milliseconds). We validate it in Section VII that setting this interval as 60ms in an indoor walking scenario is enough to make $X_{gv}(t_s)$ and $X_{gv}(t_e)$ uncorrelated. Therefore, we can consider $X_{gv}(t_s)$ and $X_{gv}(t_e)$ as i.i.d. Gaussian. Then $\Delta S_{gv}(t_s, t_e)$ should follow $\mathcal{N}(0, 2\sigma_X^2)$.

In practice, there will always be unavoidable measurement errors of the RSS. The errors may be caused by interference, ambient noise, or device impairment. We model the measured

$S_{gv}(t)$ with errors as

$$\tilde{S}_{gv}(t) = S_{gv}(t) + n_v(t) \tag{6}$$

where $n_v(t)$ is the measurement error on the victim node following $\mathcal{N}(0, \sigma_v^2)$.

Therefore, the measured RSS variation becomes

$$\Delta\tilde{S}_{gv}(t_s, t_e) = \Delta S_{gv}(t_s, t_e) + \Delta n_v \tag{7}$$

where $\Delta n_v = n_v(t_s) - n_v(t_e)$. Under the assumption of the independence between the measurement errors, Δn_v should follow $\mathcal{N}(0, 2\sigma_v^2)$.

2) RSS variation at genuine node: Similarly, the RSS variation of the corresponding pairing frames received by the genuine node can be represented as

$$\Delta\tilde{S}_{vg}(t'_s, t'_e) = \Delta S_{vg}(t'_s, t'_e) + \Delta n_g \tag{8}$$

where $\Delta S_{vg}(t'_s, t'_e) \approx X_{vg}(t'_s) - X_{vg}(t'_e)$ and Δn_g (following $\mathcal{N}(0, 2\sigma_g^2)$) is the difference of measurement errors at the genuine node.

3) Correlation coefficient: Assume the time interval between the data frame and its corresponding pairing frame is small. For example, the time interval between a DATA and its ACK frame is about 0.47ms assuming the DATA frame size is 512 bytes and transmission rate is 12Mbps in 802.11g networks. That is, $t'_s - t_s$ and $t'_e - t_e$ should be very small, and the channel reciprocity should hold well during the exchange of the data frame and pairing frame. Assuming the correlation coefficient between $X_{gv}(t_s)$ and $X_{vg}(t'_s)$ and that between $X_{gv}(t_e)$ and $X_{vg}(t'_e)$ are both ρ_{gv}, we can derive that the correlation coefficient between $\Delta\tilde{S}_{gv}(t_s, t_e)$ and $\Delta\tilde{S}_{vg}(t'_s, t'_e)$ is

$$\tilde{\rho}_{gv} = \frac{\rho_{gv}}{\sqrt{(1 + \sigma_v^2/\sigma_X^2)(1 + \sigma_g^2/\sigma_X^2)}} \tag{9}$$

Please refer to Appendix A for the derivation.

Eq. (9) basically indicates that the correlation coefficient between the measured RSS variations at victim and genuine nodes is degraded by the errors. If the error σ_v^2 or σ_g^2 increases, $\tilde{\rho}_{gv}$ decreases. The degradation degree depends on the ratios of σ_v^2/σ_X^2 and σ_g^2/σ_X^2. When the ratio is larger, $\tilde{\rho}_{gv}$ deviates more from ρ_{gv}. $\tilde{\rho}_{gv}$ approaches ρ_{gv} when the errors approach zero.

C. RSS Variation Correlation under Attack

1) RSS variation at attacker: Assuming the attacker eavesdrops all the frames, no matter what attacking pattern is, the RSS variations observed at the attacker is

$$\Delta\tilde{S}_{va}(t'_s, t'_e) = \Delta S_{va}(t'_s, t'_e) + \Delta n_a \tag{10}$$

where $\Delta S_{va}(t'_s, t'_e) = S_{va}(t'_s) - S_{va}(t'_e)$ and Δn_a (following $\mathcal{N}(0, 2\sigma_v^2)$) is the measurement error difference at the attacker.

The frame received/overheard by the attacker at time t'_s and t'_e can be the pairing frame destined to the attacker/genuine node. Similar to the discussion in Section V-B, $\Delta S_{va}(t'_s, t'_e)$ should follow $\mathcal{N}(0, 2\sigma_X^2)$ assuming the shadowing fading of the eavesdropping channel has the same statistics as the genuine channel.

2) RSS variation at victim: There are four situations when computing the RSS variations at the victim node:

- Situation A: $S_{av}(t_s) - S_{av}(t_e)$, both frames come from the attacker.
- Situation B: $S_{gv}(t_s) - S_{gv}(t_e)$, both frames come from the genuine node.
- Situation C: $S_{av}(t_s) - S_{gv}(t_e)$, former frame comes from the attacker, and the latter frame comes from the genuine node.
- Situation D: $S_{gv}(t_s) - S_{av}(t_e)$, former frame comes from the genuine node, and the latter frame comes from the attacker.

In the following discussion, for simplicity, we will denote $\Delta S_{va}(t'_s, t'_e)$ as ΔS_a, and the RSS variation observed at the victim node as ΔS_v. The corresponding measured RSS variations with errors are $\Delta\tilde{S}_a$ and $\Delta\tilde{S}_v$.

3) Correlation coefficient under different situations:
Situation A: Same as the analysis in the genuine channel, the correlation coefficient of $\Delta\tilde{S}_v$ and $\Delta\tilde{S}_a$ under situation A is

$$\tilde{\rho}_A = \frac{\rho_{av}}{\sqrt{(1 + \sigma_v^2/\sigma_X^2)(1 + \sigma_a^2/\sigma_X^2)}} \tag{11}$$

where ρ_{av} is the correlation coefficient between the attacking channel and eavesdropping channel.

Situation B: The victim node measured RSS variation can be expressed by Eq. (7), the reported RSS variation from the attacker is the overheard one, then

$$\tilde{\rho}_B = \frac{\rho_{ag}}{\sqrt{(1 + \sigma_v^2/\sigma_X^2)(1 + \sigma_a^2/\sigma_X^2)}} \tag{12}$$

where ρ_{ag} is the correlation coefficient between the eavesdropping channel and forward genuine channel. Generally, ρ_{ag} should be around zero according to the location decorrelation property of the wireless fading channel.

Situation C: In situation C, since the attacker and the genuine node is physically close, we have

$$\Delta S_v \approx X_{av}(t_s) - X_{gv}(t_e) \tag{13}$$

We can derive that

$$\tilde{\rho}_C = \frac{\rho_{av} + \rho_{ag}}{2\sqrt{(1 + \sigma_v^2/\sigma_X^2)(1 + \sigma_a^2/\sigma_X^2)}} \tag{14}$$

Situation D: Situation D is symmetric to situation C, so $\tilde{\rho}_D = \tilde{\rho}_C$.

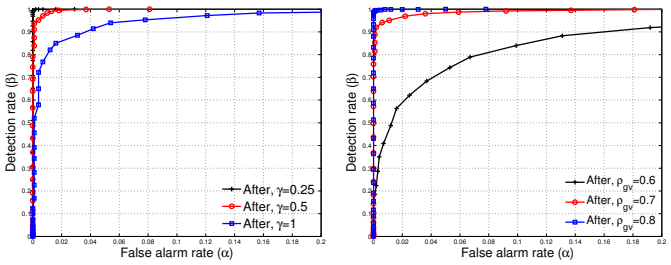
Similar to Eq. (9), Eqs. (11), (12) and Eq. (14) indicate the effect of channel fading (σ_X) and measurement errors (σ_v and σ_a) on the correlation coefficient.

D. Performance Evaluation

From the above analysis, we know that when there is no attack, the correlation coefficient between each pair of RSS variations should follow Eq. (9). While when there is an attack, the correlation coefficient between a pair of RSS variations should follow either Eq. (11), Eq. (12), or Eq. (14).

Under attacking pattern "After"/"Before", the RSS variations observed by the victim node should be either situation A or B. There might be one RSS variation of situation C or D. If the number of attacking frames is larger than the genuine frames, in one variation list, the variations of situation A should be more than that of situation B, and vice versa. Intuitively, the sampled correlation coefficient would be close to Eq. (11) or Eq. (12) depending on the ratio of the attacking frames to the genuine frames (*attacking intensity*). When the ratio is higher, it would be harder to detect the attack.

Under "Interleaved" attacking pattern, in one constructed variation list, an RSS variation observed by the victim node



(a) Impact of measurement error ratio (b) Impact of correlation in the genuine channel

Fig. 2. Theoretical performance of RCVI

can be any of the four situations.

Next, we will show the impact of measurement error and reciprocity on the performance of RCVI. We will discuss the impact of other factors, such as attack intensity, variation list length N, number of constructions K in Section VII.

In the simulation, we assume 1,000 pairs of RSS lists with length $(N+1)K$. According to the distributions and correlations between the variations under attack and no attack, we generate K variation lists with length N for each pair of list. We then compute the mean correlation coefficients and compute the false alarm rate and detection rate. Since we have found that the performance of RCVI are nearly the same under different attacking patterns, we will only show the "After" case.

1) Impact of measurement error ratio: From Eqs. (9), (11), (12), and (14), we know that the measurement error would degrade the correlation coefficient, which in turn would affect the detection performance. Assume $\sigma_a = \sigma_g = \sigma_v$, and denote them as σ_n. We call $\gamma = \sigma_n^2/\sigma_X^2$ as the *measurement error ratio*. Intuitively, larger measurement error ratio would degrade the performance. Fig. 2(a) confirms this intuition. The settings are $N = 50$, $K = 5$, $\sigma_X = 3$, $\rho_{gv} = \rho_{av} = 0.8$, and $\rho_{ag} = 0.1$. The number of attacking frames is equal to the genuine frames. We can see that even when the measurement error ratio is one, we can still achieve good performance (90% detection rate with 5% false alarm rate). We find that, when N or K increases, we can improve the performance. We will show this relationship with empirical analysis in Section VII.

2) Impact of Reciprocity: RCVI is based on the assumption of the reciprocity, which is indicated by the correlation coefficient. When the correlation coefficient in the genuine channel decreases, the performance will be degraded, and vice versa. The simulation settings are the same as the above evaluation, except that we fix $\gamma = 0.5$ and vary ρ_{gv}. Fig. 2(b) shows that when ρ_{gv} increases the detection performance improves. Under our simulation settings, when ρ_{gv} is larger than 0.7, we can achieve desirable performance.

VI. Experimental Methodology

In order to verify the effectiveness of the RCVI scheme, we carried out extensive mobile experiments in real indoor and outdoor environments. We test the applicability of RCVI under different mobile scenarios and attacking patterns. The three parties are Dell E5400 laptops, which use Intel iwl5300 chipset and iwlwifi driver. All experiments run 802.11g and

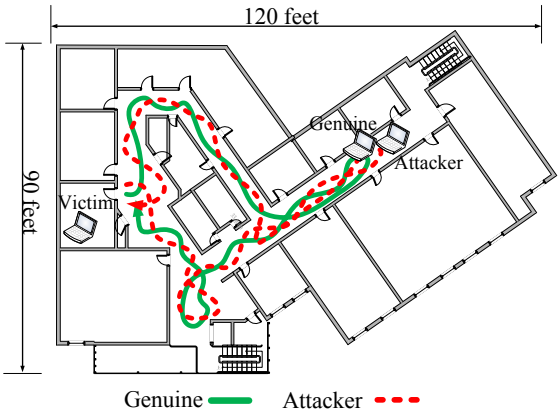


Fig. 3. Indoor experimental environment

operate on channel one in the 2.4GHz frequency. We fix the transmission rate at 12Mbps and transmission power at 15dbm. The genuine node and the attacker generate CBR UDP traffic to the victim node using Ping. The Ping packet size is set as 512 bytes and the Ping request interval is set as 10ms. We use the Ping request and ACK frames to emulate the data and pairing frames in our model. We turn off the antenna diversity function in the driver, so that the DATA and ACK can be transmitted between the same antenna pair. All three parties have one virtual interface configured as monitor mode to overhear all the packets in the channel one and log all the overheard traffic. Tcpdump 4.0.0 [24] are used to log the frame RSS. Each experiment runs for 5 minutes. Interference exists in the experiments due to nearby campus 802.11 access points and clients operating on the same channel. The RSS output by the driver are integers in the range [-92, -20]dbm.

We conducted the experiment in both indoor and outdoor environments. The indoor experiment is carried out on the second floor in a campus building illustrated in Fig. 3. The victim node is fixed in a room, and the genuine node and attacker are walking in the hallway. The outdoor environment is an open lawn. The mobile nodes walk around the victim node within 150 feet. We consider two mobile scenarios: *random* and *shadowing*. In random mobile scenario, the genuine node and the attacker randomly walk around. In the shadowing scenario, the attacker shadows the genuine node within 0.5m, which allows us to work with the worst case where the attacker has the most similar location (and received signal strength) as the genuine node.

Pairing DATA and ACK: We first pair the DATA (Ping request) received by the victim node with the corresponding ACK received by the genuine node. Since the ACK has no sequence number, in order to pair a Ping request with its corresponding ACK, we mixed the records of the sent Ping request, received ACK, and received Ping reply at the genuine node. Then we sorted these records according to time. If there is a Ping request successfully delivered, we will see three consecutive records representing Ping request, ACK, and Ping reply in the sorted records with the Ping request and reply having the same sequence number. Then we match the ACK with the corresponding Ping request received at the

		ρ_{gv}	ρ_{av}	ρ_{ag}	$\sigma_{\Delta gv}$	$\sigma_{\Delta vg}$	$\sigma_{\Delta ag}$
Indoor	shadowing	0.69	0.72	0.15	3.55	3.00	3.66
	random	0.67	0.69	0.15	3.49	2.83	3.53
Outdoor	shadowing	0.81	0.63	-0.07	3.28	2.91	5.24
	random	0.74	0.67	0.02	3.01	2.78	4.70

TABLE I
CORRELATION COEFFICIENT AND STANDARD DEVIATION OF THE RSS VARIATIONS IN DIFFERENT ENVIRONMENTS AND SCENARIOS.

victim node. Using the same method, we pair the DATA-ACK between the victim node and the attacker. At the attacker, we also pair the overheard ACK with the Ping request sent from the genuine node to the victim node.

We then generate the RSS variation lists at both genuine and victim nodes using the RSS of the paired DATA-ACK, which serves as the genuine data. For attacks, we mix the RSS of the received and overheard ACK as the attacker's report, and use the RSS of the corresponding mixed DATA as the victim node's records.

We tried different t_l and t_g for different scenarios and environment. We found that setting $t_l = t_g$ as 60ms and 160ms makes each RSS variation independent for the indoor and outdoor environments, respectively. We fix these parameters in the evaluation.

VII. EXPERIMENTAL ANALYSIS

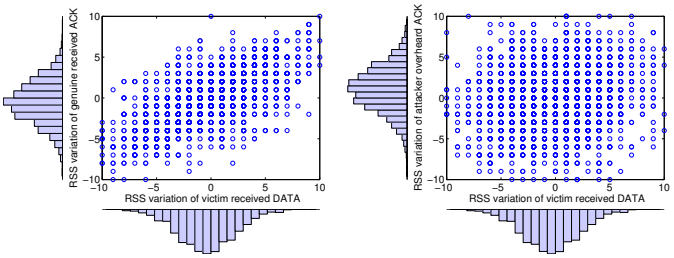
Table I summarizes the measured correlation coefficient between the forward ($g \to v$) and backward ($v \to g$) genuine channels (ρ_{gv}), between the forward ($a \to v$) and backward ($v \to a$) attacking channels (ρ_{av}), and eavesdropping ($v \to a$) and forward genuine ($g \to v$) channels. The standard deviations of ΔS_{gv}, ΔS_{vg} and the attacker overheard RSS variation ΔS_{ag} are also summarized. We found that the reciprocity between $g \to v$ and $v \to g$, and that between $a \to v$ and $v \to a$ hold well with correlation around 0.7 or above. While the eavesdropping channel has very low correlation with the forward genuine channel. The overheard RSS variations by the attacker are nearly uncorrelated with that observed by the victim node.

We also verify that all the RSS variations follow Gaussian distributions. Fig. 4 shows the distribution and scatter graph of the RSS variations in the genuine channel and eavesdropping channels under indoor shadowing scenario. We can clearly see the correlation of the bi-directional genuine channels (Fig. 4(a)), and the un-correlation between the genuine channel and the eavesdropping channel (Fig. 4(b)).

We analyze the performance of RCVI under different lengths of variation list, number of constructions, frame intervals, and attacking intensities. Fig. 5 shows the empirical ROC varying different parameters under the indoor shadowing scenario.

A. Impact of list lengths

We divide the RSS traces into consecutive blocks with equal durations of 3s, 6s, and 12s, which yield different lengths of variation list such as 25, 50, and 100, respectively. For each block, we generate 10 variation lists according to Algorithm 2.



(a) Distribution and scatter graph of RSS variations in the genuine channel node

(b) Distribution and scatter graph of victim node's RSS variations and attacker overheard ones

Fig. 4. Distribution and scatter graph of RSS variations in the genuine and eavesdropping channels under indoor shadowing scenario

The attacking intensity r is 1, that is, the number of attacking frames is equal to the genuine frames in each tested block.

Fig. 5(a) shows the empirical ROC. We can see that with list lengths increased, the detection performance improves. Even when we only use a very short list length ($N = 25$), we can still achieve around 90% detection rate with 10% false alarm rate. When the list length is 100, we can most surely detect the attack without false alarm. It also shows that RCVI can detect the IBA under different attacking patterns, and achieve similar performance. Note that it only cost 12s to achieve a desirable detection performance, where the existing solution DEMOTE need about 150 seconds to achieve a comparable performance.

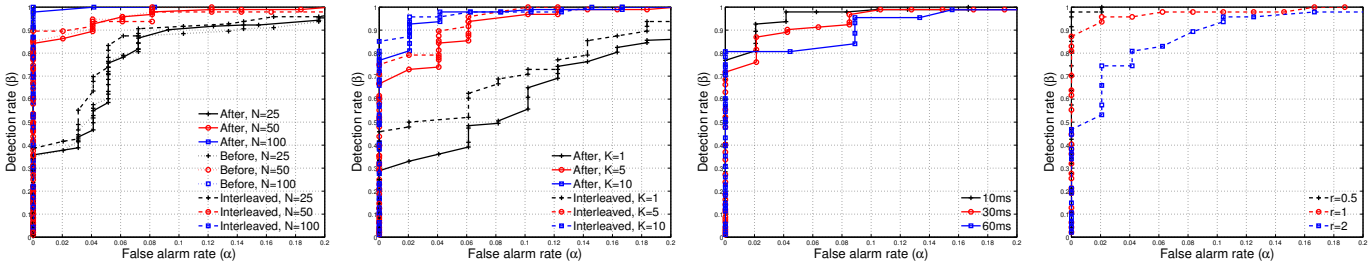
B. Impact of number of constructions

Fig. 5(b) shows that when the construction number increases, the detection performance improves. The performance gain decreases when we increase the construction number. When K reaches 10, we can get desirable detection performance (about 98% detection rate with 5% false alarm rate).

C. Impact of frame intervals

Fig. 5(c) shows the performance under frame intervals of 10ms, 30ms, and 60ms. The list length N is fixed at 50, and the construction number $K = 10$. Since the performance shows similar trend under the three attacking patterns, we only show the performance for the attacking pattern "After".

We can see that when the frame interval becomes larger, the performance degrades. The intuition behind this observation is that under the same list length and t_l and t_g, the constructed variation list would be more similar for larger frame interval. For example, when the frame interval is 60ms, which is equal to t_l and t_g, after shifting the start index at 3, we will get a variation list which repeats $N - 1$ elements of the first constructed one. So the sample correlation coefficients might be very similar under these two constructions. In this case the newly constructed variation list might not contribute much for the strength of the detection. While when the frame interval is smaller, it is more likely to construct uncorrelated variation lists, although there would be unavoidable correlation between the variation in each construction due to temporal correlation of the RSS.



(a) Impact of list lengths (b) Impact of construction numbers (c) Impact of frame intervals (d) Impact of attacking intensities

Fig. 5. Empirical performance of RCVI under different parameters in the indoor shadowing scenario

	Indoor		Outdoor	
	shadowing	random	shadowing	random
β	99%	92%	88%	79%
ρ_{th}	0.52	0.49	0.43	0.44

TABLE II
ρ_{th} AND β WITH 5% FALSE ALARM RATES, $N = 50$, $K = 10$, $r = 1$, "AFTER"

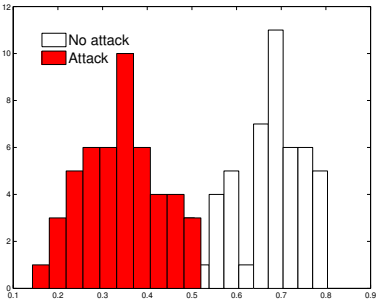


Fig. 6. Histogram of $\overline{\hat{\rho}}$ under indoor shadowing, $N = 50$, $K = 10$, $r = 1$

D. Impact of attacking intensities

Attacking intensity is an important factor that affects the detection performance. Intuitively, when the intensity is higher, it is harder to detect the attack, since the majority of the RSS reported by the attacker would be highly correlated with the victim node's.

Fig. 5(d) shows the ROC under different attacking intensities under attacking pattern "Interleaved". The frame interval is $10ms$, $N = 50$, and $K = 10$. It shows that the performance degrades when the attacking intensity increases. However, even with $r = 2$, RCVI can still detect the attack with good performance (e.g. about 85% detection rate with false alarm rate of 5% and 90% detection rate with false alarm rate of 10%.) We observe similar trend for the other two attacking patterns. Note that, given an attacking intensity (r), we can always use more data to improve the detection performance as indicated in Fig. 5(a). But more data implies higher detection delay, which is a common trade-off in the existing detection schemes [22].

E. ρ_{th} and detection rate

We summarize the detection rate and the corresponding threshold (ρ_{th}) when achieving 5% false alarm rate under the "After" attacking pattern in Tabel II. We have similar results under other attacking patterns. We can see that the detection rate of outdoor scenario is lower than the indoor scenario using the same parameters. The reason is that the outdoor channel has lower variations and longer channel coherence time than the indoor channel. So we need longer variation lists to achieve comparable performance as the indoor case. The histogram of $\overline{\hat{\rho}}$ of indoor shadowing case under attack and no attack is shown in Fig. 6. We can see that $\overline{\hat{\rho}}$ is centered around 0.7 under no attack and 0.3 under attack. There are little overlaps between the two distribution, which indicates the feasibility of RCVI.

VIII. Discussion

Overheads: RCVI requires the sender to send the RSS information, which is considered as an overhead. However, this overheard is very small. For example, if the frame interval is 10ms, in the tested indoor scenario, in order to construct an RSS variation list of length 50, we need 600 bytes assuming each RSS valued is represented by a byte. This 600-byte RSS records can be included in one packet. Even when we need longer RSS records (e.g. 1600 bytes in the tested outdoor case when $N = 50, K = 10$), one or two packets are enough to carry all of them to achieve a desirable detection performance.

MAC Retransmissions and Reliability: An unacknowledged DATA frame (due to loss or corruption of DATA or ACK) will cause retransmission. By using the frame sequence number of the 802.11 frame as a marker, we can always pair the DATA and ACK frames properly (which, in turn, will generate a proper variation list at both genuine and victim nodes). If the victim node receives multiple retransmitted DATA frames (having the same sequence number), it can use the RSS of the latest one. So our scheme can be extended to unreliable DATA or ACK cases in 802.11 networks. Actually, the ACK frame has very high reliability above 99.5% as we computed from our empirical data.

Multiple Antenna Diversity: Off-the-shelf 802.11 devices are usually equipped with multiple antennas to exploit spatial diversity. The device will switch its transmit or receive antenna according to the received signal quality. Diversity needs to be taken into account when creating the variation list so the transmitter-receiver antenna pairs are not mixed together to produce inconsistent results. At each genuine and victim node side, the two RSS records used to generate a variation list should be measured from the same channel (i.e. same transmitter-receiver antenna pair). We can easily extend RCVI

in multiple antenna systems as long as we can measure the pair of RSS variations on the channel between each antenna pairs. The multiple antenna diversity will improve the detection performance since more uncorrelated RSS variations can be obtained during the same time than single antenna systems.

Unprotected ACK Frames: If the ACK frame is used as the pairing frame, the genuine user should make sure that it is sent from the victim node. An attacker can try to generate ACKs for any DATA frames it overhears to confuse the genuine user in recording the wrong channel variation, which raises the false alarms. However, this attack is not easy to be successful because when the victim node receives the DATA, it will instantly send back an ACK to the genuine node. The attacker's ACK may collide with the victim node's ACK, so the genuine node will not record the corresponding RSS but considers the ACK is lost.

IX. Conclusion

We proposed RCVI, an identity-based attack detection technique for mobile wireless networks. RCVI exploits the reciprocity of the wireless fading channel and RSS variations naturally incurred by mobility. We evaluated RCVI through theoretical analysis considering measurement errors, and validated its feasibility through experiments using off-the-shelf 802.11 devices under different attacking patterns and indoor and outdoor mobile scenarios. Experimental results show that RCVI can achieve desirable performance under the tested scenarios. RCVI allows the user to tune the parameters to achieve strong security strengths (nearly 100% detection rate without false alarm) but introducing negligible overhead.

Appendix A
Derivation of Eq. (9)

For simplicity, we use X_1 and X_2 to represent $X_{gv}(t_s)$ and $X_{gv}(t_e)$, X_1' and X_2' to represent $X_{vg}(t_s')$ and $X_{vg}(t_e')$, and X_3 and X_4 to represent Δn_v and Δn_g, respectively. According to the assumption, X_1/X_1', X_2/X_2', X_3 and X_4 are all independent to each other. They all follow Gaussian distributions with zero means. Therefore, $X_1 - X_2 + X_3$ and $X_1' - X_2' + X_4$ should follow $\mathcal{N}(0, 2(\sigma_X^2 + \sigma_v^2))$ and $\mathcal{N}(0, 2(\sigma_X^2 + \sigma_g^2))$, respectively. According to the reciprocity, the correlation coefficients between X_1 and X_1' as well as X_2 and X_2' are both ρ_{gv}.

$$\tilde{\rho}_{gv} = \frac{E[(X_1 - X_2 + X_3)(X_1' - X_2' + X_4)]}{\sqrt{2(\sigma_X^2+\sigma_v^2)}\sqrt{2(\sigma_X^2+\sigma_g^2)}} = \frac{E[X_1X_1'] + E[X_2X_2']}{\sqrt{2(\sigma_X^2+\sigma_v^2)}\sqrt{2(\sigma_X^2+\sigma_g^2)}}$$
$$= \frac{\rho_{gv}\sigma_X^2 + \rho_{gv}\sigma_X^2}{\sqrt{2(\sigma_X^2+\sigma_v^2)}\sqrt{2(\sigma_X^2+\sigma_g^2)}} = \frac{\rho_{gv}}{\sqrt{(1+\sigma_v^2/\sigma_X^2)(1+\sigma_g^2/\sigma_X^2)}}$$

References

[1] J. Bellardo and S. Savage, "802.11 Denial-of-service attacks: real vulnerabilities and practical solutions," in *Proceedings of the 12th conference on USENIX Security Symposium SSYM*, 2003, pp. 2–2.

[2] M. Eian, "Fragility of the robust security network: 802.11 denial of service," in *Proceedings of the 7th International Conference on Applied Cryptography and Network Security, ACNS '09*. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 400–416.

[3] M. Demirbas and Y. Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," in *Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks WOWMOM*, 2006, pp. 564–570.

[4] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proceedings of the 5th ACM workshop on Wireless security WiSe*, 2006, pp. 43–52.

[5] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the physical layer for wireless authentication," in *IEEE International Conference on Communications, ICC*, 2007, pp. 4646–4651.

[6] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A Physical-Layer Technique to Enhance Authentication for Mobile Terminals," in *IEEE International Conference on Communications, ICC*, May 2008, pp. 1520–1524.

[7] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "MIMO-assisted channel-based authentication in wireless networks," in *42nd Annual Conference on Information Sciences and Systems, CISS*, 2008, pp. 642–646.

[8] Sheng, Yong and Tan, K. and Chen, Guanling and Kotz, D. and Campbell, A, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," in *The 27th Conference on Computer Communications INFOCOM*, 2008, pp. 1768–1776.

[9] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, July 2008.

[10] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking MobiCom '08*, 2008, pp. 116–127.

[11] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Determining the number of attackers and localizing multiple adversaries in wireless spoofing attacks," in *The 28th Conference on Computer Communications INFOCOM*, 2009, pp. 666–674.

[12] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall PTR, 2002.

[13] Zhang, Junxing and Firooz, Mohammad H. and Patwari, Neal and Kasera, Sneha K. , "Advancing wireless link signatures for location distinction," in *Proceedings of the 14th ACM international conference on Mobile computing and networking MobiCom*, 2008, pp. 26–37.

[14] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking MobiCom 2008*, 2008, pp. 128–139.

[15] Q. Li and W. Trappe, "Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships," *IEEE Transactions on Information Foresics and Security*, vol. 2, no. 4, pp. 793–808, December 2007.

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

[17] F. Guo and T.-c. Chiueh, "Sequence number-based MAC address spoof detection," in *Proceedings of 8th International Symposium on Recent Advances in Intrusion Detection, RAID'05*, 2005, pp. 309–329.

[18] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 user fingerprinting," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking MobiCom '07*, 2007, pp. 99–110.

[19] M. Barbeau, J. Hall, and E. Kranakis, "Detecting impersonation attacks in future wireless and mobile networks," in *Proceedings of MADNES'05 - Workshop on Secure Mobile Ad-hoc Networks and Sensors*, 2005, pp. 80–95.

[20] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proceedings of the third ACM conference on Wireless network security, WiSec '10*, 2010, pp. 89–98.

[21] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *The 13th annual ACM international conference on mobile computing and networking, MOBICOM*, 2007, pp. 111–122.

[22] J. Yang, Y. Chen, and W. Trappe, "Detecting spoofing attacks in mobile wireless environments," in *Proceedings of the 6th Annual IEEE communications society conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON'09*, 2009, pp. 189–197.

[23] Kenney, J. F. and Keeping, E. S., *Mathematics of Statistics, Pt. 2, 2nd ed.* Van Nostrand, 1951.

[24] "TCPDUMP/LIBPCAP Public repository." [Online]. Available: http://www.tcpdump.org/