Identity-Based Attack Detection and Classification Utilizing Reciprocal RSS Variations in Mobile Wireless Networks

Jie Tang, Long Jiao, Kai Zeng, Hong Wen, Kannan Govindan, Daniel Wu, Prasant Mohapatra

Abstract—Identity-based attacks (IBAs) are one of the most serious threats to wireless networks. Recently, there is an increasing interest in using the received signal strength (RSS) to detect IBAs in wireless networks. However, current schemes tend to generate excessive false alarms in the mobile scenario. In this paper, we propose a stronger Reciprocal Channel Variation-based Identification and classification (RCVIC) scheme for the mobile wireless networks, which exploits the reciprocity of the wireless fading channel and RSS variations naturally incurred by mobility to improve the detection performance. Different from current schemes only detect IBAs, RCVIC scheme conducts a multi-stage detection processes. If the IBAs are detected, RCVIC scheme partitions the received frames into two classes. The frames in the same class should be sent from the same senders, which could benefit the further analysis, such as network forensics, attacker localizing and trajectory analysis, etc. The feasibility of RCVIC are numerically evaluated through theoretical analysis and simulations. It is further validated through experiments using off-the-shelf 802.11 devices under different attacking patterns in real indoor and outdoor mobile scenarios.

Index Terms—Identity-based attacks detection, mobile network, RSS, channel reciprocity, partition, IEEE 802.11.

1 Introduction

Among the various types of attacks in wireless networks, identity-based attacks (IBAs) are one of the most serious threats to wireless networks[1, 2]. 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. Then it could masquerade as a legitimate user by modifying its own MAC address. IBAs are considered to be an important first step in an intruder's attempt to launch a variety of other attacks [3], such as session hijacking, man-in-the-middle, data modification, and authentication-based denial of service. Although traditional cryptographic techniques can potentially prevent IBAs in wireless networks, the authentication key can still be compromised. If the key is broken, the cryptography-based mechanism will fail and IBAs are easy to lunch.

Under the above circumstances, there is an increasing interest in using the environment-dependent wireless channel features such as received signal strength (RSS) and channel state information (CSI) to detect IBAs in wireless networks [4–8]. The foundation of these schemes is that CSI and RSS are location-specific due to path loss and channel fading, and they are random and unpredictable. An attacker who is at a different location from the genuine user will incur different CSI or RSS profiles as observed by monitors/access points [9].

There are two typical solutions for current channel-based IBA detection schemes. One [10] is based on the assumptions that the previous data frame D_{n-1} has already been authenticated, then the receiver just need to determine whether current frame D_n is sent by the same sender. If the CSI or RSS of D_n is "similar" enough to D_{n-1}, it is believed to be sent by the same sender or not. Otherwise, it is sent by the attacker. However, in a mobile scenario, these schemes tend to generate excessive false alarms [11]. This is mainly because this type of scheme only works well when the interval between two consequent frames is within the channel coherence time. Furthermore, if one frame was erroneously measured by the receiver, or it was fabricated by a nearby attacker [12], the receiver could get erroneous judgement on all the subsequent frames.

The other typical solutions are based on the cluster partition analysis [4–6]. Work [4] partitioned the receive frames of RSS trace into two classes and detect IBAs if the two classes have low correlation. If there is no attack, the distance between the two cluster centres should be close. Based on the cluster partition results, the receiver can implement further countermeasures to enhance security, such as determining the number of attackers and localizing them [5, 6]. However, in a mobile environment, work [11] showed that the detection performance will decrease with excessive false alarms, when the nodes are moving with a higher speed.

In this work, we propose a novel Reciprocal Channel Variation-based Identification and classification (RCVIC) technique to improve the detection performance in mobile environments. RCVIC consists of four distinct and ordered processes as: DATA-ACK communication, RSS records feedback, IBA detection and partition. In order to improve the detection performance in mobile environments, RCVIC first

- *Jie Tang (cs.tan@uestc.edu.cn) and Hong Wen (sunlike@uestc.edu.cn) are with School of Aeronautics and Astronautics, University of Electronic Science and Technology of China (UESTC), Chengdu, China, 611731. Jiao long and Kai Zeng are with George Mason University, Fairfax, Virginia 22030, U.S.A. Kannan Govindan (g.kannan16@samsung.com) has been working with Amazon. Daniel Wu is with Google company. Prasant Mohapatra is with the Department of Computer Science at UC Davis.*

directly detects IBAs by utilizing DATA-ACK communication with RSS records feedback processes. Then, if the further detection is triggered, the well-designed RSS variation lists are constructed for further detection. Finally, if IBAs are detected, RCVIC scheme triggers the partition process to partition the received frames into two classes without prior channel information. The frames in the same class should be sent from the same senders, which are very beneficial for the system to implement the further analysis, such as network forensics [13], attacker localizing [4], etc.

In the first DATA-ACK communication, RCVIC assumes that the sender and receiver can record the RSS value of the bidirectional frames with a short time interval. In the RSS records feedback phase, the receiver asks the sender to feedback the RSS records during DATA-ACK communication. Then receiver can directly detect IBA by checking the length of feedback RSS records. If the length of feedback satisfies requirements, the receiver further detects IBAs by constructing well-designed RSS variation lists, based on its own RSS records and feedback RSS records. Based on the reciprocity of the wireless channel [9], the mobile sender and receiver should observe similar temporal RSS variation lists. Therefore, when there is no IBA, the reported RSS variation lists should be correlated with the receiver's observation. Meanwhile, for the location decorrelation property of the wireless channel, an attacker cannot observe the same channel variation as the sender-receiver channel if it is located several wavelengths away [9]. 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 variation lists observed by the genuine user, its reported RSS records should be less correlated with the victim node's, and IBAs can be detected.

One advantage of RCVIC is that it 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. It can also be generally applied to any wireless networks, as long as there are bidirectional frames exchanged between the communication parties within a time interval shorter than the channel coherence time. Our contributions are summarized as follows:

- We proposed a multi-stage detection and decision model. If an IBA is detected by RSS variation lists, RCVIC partitions the frames to two classes for further analysis.
- The closed-form expressions of false alarm rate and detection rate, regarding to attack density and channel reciprocity coefficients are derived. The optimal hypothesis threshold for RCVIC detection is analyzed. The numerical results illustrate how channel reciprocity, attacking intensity and channel correlation variations affect the RCVIC detection and false alarm rate.
- We evaluate RCVIC through extensive experiments using off-the-shelf 802.11 devices under different attacking patterns in real indoor and outdoor mobile scenarios. we show that RCVIC can detect IBAs with a high probability even when the attacker is half a meter away from the genuine user.

TABLE 1
Summary of important symbols

ΔS_{gv}	RSS variation at victim if no Attack
$\Delta\tilde{S}_{gv}$	RSS variation with measure error at victim if no attack
$\Delta\tilde{S}_{vg}$	RSS variation with measure error at genuine if no attack
$\Delta\tilde{S}_{a}$	RSS variation with measure error at attacker
$\Delta\tilde{S}_{v}$	RSS variation with measure error at victim under attack
ρ_{gv}	Reciprocity coefficient of victim and genuine nodes
ρ_{av}	Reciprocity coefficient of attacker and victim
ρ_{ag}	Reciprocity coefficient of attacker and genuine nodes
$\tilde{\rho}_{gv}$	RSS variation correlation coefficient if no attack
$\tilde{\rho}_{a}$	RSS variation correlation coefficient under attack
$\tilde{\rho}_{A}$	RSS correlation coefficient under attack of situation A
$\tilde{\rho}_{B}$	RSS correlation coefficient under attack of situation B
$\tilde{\rho}_{C}$	RSS correlation coefficient under attack of situation C
P_a	Attack intensity
r	Ratio of the number of attacking frames to the number of genuine frames

The rest of this paper is organized as follows. In Section 2, we discuss the related work. Section 3 introduces the RCVIC system model and attack model. We propose RCVIC IBA detection algorithm in Section 4. The IBA detection performance evaluation is provided in Section 5. Section 6 illustrates the RCVIC partition process. We conduct the numerical simulations to verify the performance of RCVIC in Section 7. In Section 8, we analyze the experimental results. Related issues about RCVIC are discussed in Section 9. Finally, we conclude this paper in Section 10. For ease of reference, some important notations are summarized in Table I.

2 Related Work

There is an increasing interest in using wireless channel features, such as RSS and CSI to detect IBAs in wireless networks [5, 14]. In work [4], a generalized IBAs detection model was proposed that utilized the spatial correlation of RSS inherited from static wireless nodes. The model used K-means algorithm to partition the received RSS records into two clusters. In particular, the RSS records over time from the same physical location will belong to the same cluster points in the n-dimensional signal space, while the RSS records from different locations over time should form different clusters in signal space. Based on work [4], work [5, 11, 14] proposed an integrated detection and localization system that can localize the positions of multiple attackers as well as determine the number of attackers. Since the RSS is readily available in current devices, the RSS based IBAs detections were further extended to various mobile application scenarios, such as trust ad hoc networks and vehicular networks [7, 8].

In the mobile environments, the RSS or CSI measurements will change over time, thus will generate excessive false alarms. Work [11] considered channel variations due to environmental changes and terminal mobility. It numerically verified that the detection performance tends to degrade with excessive false alarms, when the nodes are moving at a higher speed. Aiming to improve the detection performance, work [15] proposed a CSI profile model, which integrated different detection strategies for static and mobile users, respectively. Works [16] utilized multiple antennas

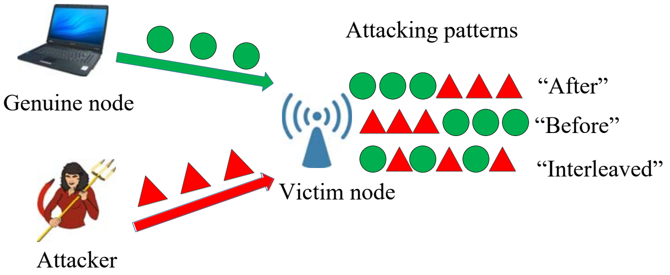


Fig. 1. IBA attack model. "After"/"Before" means the attacker's frames arrive after/before the genuine node's. "Interleaved" means the attacker's frames are interleaved with the genuine node's.

and multiple landmarks to improve the detection performance. For unknown the channel model, works [10, 16] utilized learning algorithms to enhance the spatial resolution of the channel information and thus improve the detection performance. However, utilizing learning algorithms usually requires an additional training phase, which increases the overall delay and complexity [12].

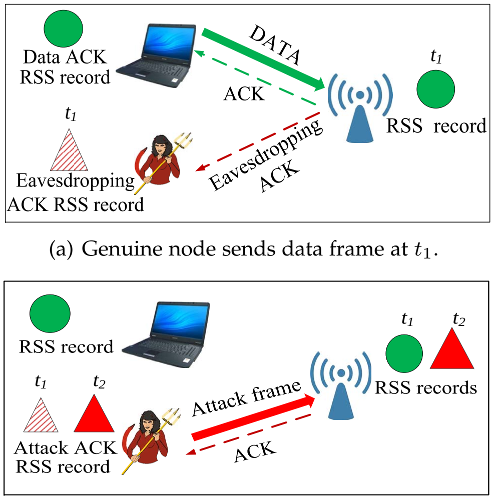
The most related work is the DEMOTE system proposed in [17]. DEMOTE partitions the RSS trace of a node identity into two classes, and detect the IBA when the two classes have low correlation. However, it cannot work well when the attacker is close to the genuine node or when the attacking frames come 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.

Difference from conference version: Preliminary results have been published in a previous conference version [18] (IEEE INFOCOM) of this journal version. Comparing to the conference version, we have made significant improvements and propose a stronger RCVIC model, which not only detect IBAs, but also partition the received frames into two classes, which are very beneficial for the system to implement the further analysis, such as network forensics, attacker localizing, and trajectory analysis, etc. In addition, we derive the tractable closed-form expressions of IBA false alarm rate and detect rate, the key factors that impact IBA false alarm rate and detect rate are fully investigated. The optimal hypothesis test threshold for RCVIC detection is also analyzed. The factors that impact the performance are fully investigated.

3 System Model and multi-stage decision

3.1 Attack model

We consider an 802.11-based wireless network and introduce three different single antenna parties: a genuine node, a victim, and an attacker. We assume a powerful attacker who could compromise the authentication key by sniffing the communication traffic between the victim and genuine node, if cryptographic authentication mechanisms are employed. After that, it masquerades the genuine node by modifying its own identity into the genuine one's, and sends fake frames to victim. The attacker can manipulate arbitrary fields in a frame, such as the source and destination IP/MAC addresses, sequence number, and so on. We assume the attacker may have compromised the authentication key of the genuine node if cryptographic authentication mechanisms are employed. The RCVIC scheme aims to detect such IBAs. If an IBA is detected, the victim could initialize a rekey process (renew/update the authentication keys) to recover from the attack and conduct further analysis.



(a) Genuine node sends data frame at t_1.

(b) Attacker inserts attack frame at t_2.

Fig. 2. DATA-ACK communication. (a) At t_1, victim received genuine node's DATA frame and feedback ACK. Genuine node recorded the corresponding RSS. Attacker eavesdropped ACK and recorded its RSS; (b)At t_2, victim received attacker's frame and feedback ACK, attacker recorded RSS from ACK of himself.

When IBAs are lunched, the attacker intends to insert fake frames to victims after/before or interleave with the genuine node's frames. Therefore, The frames of victim received might be all sent from a genuine node, or some of them are sent from an attacker. Those attacking patterns are shown in Fig. 1 which will be referred as "After", "Before" and "Interleaved" in the rest of this paper.

3.2 DATA-ACK communication and RSS feedback

RCVIC consists four distinct and ordered processes as: DATA-ACK communication, RSS feedback records, IBA detection and partition, which are described below.

DATA-ACK communication: We assume there is bidirectional communication between genuine node and victim which allows them to probe the bidirectional RSS channel characteristics in a synchronized way. For each time slot, if victim receives a frame from the same MAC address, he records its RSS and immediately sends back an *ACK frame* to the sender within a very short time interval. When a genuine node has send a data frames and then "listen" an ACK within a very short monitor time window, he also records his RSS value. Otherwise, if he does not sent a DATA, he does not monitor the feedback channel to receive ACK. It is reasonable to assume that the time interval between the data frame and its corresponding ACK frame is very small, and the channel reciprocity should hold well during the exchange of the data frame and ACK frame. In an 802.11 system, this ACK frame is naturally provided by the DATA-ACK frames [19]. For example, the time interval between

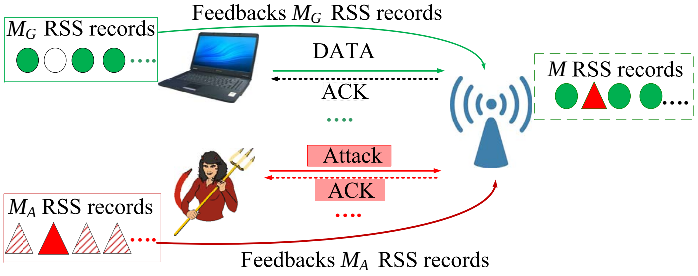


Fig. 3. DATA-ACK communication and RSS records feedback.

a DATA and its ACK frame is about 0.47ms, by assuming the DATA frame size is 512 bytes and transmission rate is 12Mbps in 802.11g networks [19, 20] (We assume ACK frames are reliable and our scheme can tackle the case of unreliable ACK frames, which is discussed in Section 9).

We assume the attacker can eavesdrop the ACK frames destined from victim to genuine node in DATA-ACK communication phase. However, for the location decorrelation property of the wireless channel, attacker can only observe "falsified" RSS records from eavesdropping ACKs, based on his specific-location. Therefore, the RSS records of ACKs corresponding to the spoofed DATA frames will be highly correlated with RSS records at victim, giving that the channel reciprocity holds well (as shown in Fig. 2 (b)). However, the correlation between the falsified RSS records from the eavesdropping ACKs and the ones at the victim node will be much lower (as shown in Fig. 2 (a)).

Fig. 2 shows an example where genuine node and attacker send frames to victim at two different time slots t_1 and t_2, respectively. In the figure, we use green circles and red triangles to denote RSS records based on different locations of genuine node and attacker, respectively. In addition, for RSS records of attacker, we use red triangles with different fill patterns to denote the highly correlated records from ACK of itself, and the lowly correlated records from eavesdropping ACK of genuine node, respectively.

RSS records feedback: In the first DATA-ACK phase, when the victim has received M *DATA frames* from the same MAC address, he requests the sender to feedback the M RSS records of ACK frames during their past DATA-ACK communication period. This value of M is only known by victim, and victim can randomly change value of M time by time without pre-informing genuine node. The process is shown in Fig. 3. The M RSS records might be all sent from genuine node, or sent from an attacker who inserted falsified/eavesdropped RSS into his RSS records. Next we describe RCVIC multi-stage detection processes.

3.3 RCVIC multi-stage detection and partition

We outline RCVIC multi-stage detection flows in Fig 4. After received M data frames, victim requests the sender to feedback the M RSS records during DATA-ACK communication period, and conducts further IBA detection process based on different situations below.

1) If victim received RSS feedback records with a length $M_F \neq M$, he directly declares an IBA attack and perform the following partition process.

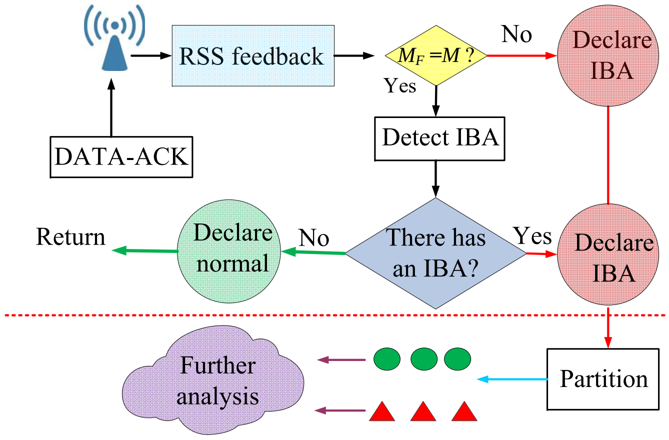


Fig. 4. RCVIC multi-stage IBA detection flow.

2) If $M_F = M$, victim conducts further IBA detection by constructing the RSS variation lists from his RSS records and the feedback. If an IBA is further detected, the following partition process is triggered. Otherwise, if victim does not detect an IBA, he believes there is no IBA and return without conducting the next processes.

The specifical RCVIC detection, partition algorithms are provided in the following Sections. We provided attack analysis below.

3.4 Attack discussion

From analysis above, the primary purpose for the attacker is to conduct IBAs and try to avoid detection. If IBAs are detected, victim and genuine node will updated/renew their authentication keys, which will prevent the attacker from impersonating the genuine node further. Therefore, the attacker has no incentive to expose itself or increase the chance of being detected. In order to avoid the immediately detection described above in (1) of Section 3.3, the attacker must always feeds back RSS records with the length of $M = M_F$ to satisfy the expected length of the feedback list. Consequently, attacker must record each RSS of ACKs corresponding to himself, and eavesdrop all the ACKs sent from victim to genuine node in the DATA-ACK phase. Otherwise, he can hardly know the exact number of M, and he cannot always feedback the RSS records to satisfy the expected length of $M = M_F$.

We assume in DATA-ACK communication phase, victim received attacker's DATA frames with a density P_a, where $0 < P_a < 1$ denotes the ratio of the number of attack frames to the total number of received DATA frames. Thus attacker can averagely get P_aM ACK frames from victim and record P_aM RSS records by himself. However, in the DATA-ACK communication period, the genuine node can only received $M_G = M - P_aM$ ACK frames and record M_G corresponding RSS records by himself. This is mainly because the P_aM DATA frames received at victim were spoofed successfully by the attacker (This process is indicated in Fig. 2), and genuine node does not record any RSS of ACKs which correspond to the spoofed DATA sent by the attacker.

Because genuine node only honestly records the RSS of the ACKs corresponding to the DATA frames sent by himself, when victim asks for RSS feedback, the genuine node honestly feedback M_G RSS records to victim during their past communication period. **If victim received M_G RSS records, he can immediately detect an IBA attack because $M_G < M$.** Therefore, to avoid be detected easily, the attacker also must launch jamming [21] to interfere victim to receive $M_G < M$ RSS records feedback from genuine node. For a worst case consideration, we assume a powerful attacker that can successfully interfere victim and enforce victim receive the RSS feedback from attacker.

From discussion above, if attacker directly feeds back $M_A = P_a M$ RSS records where he has recorded, victim can easily detect IBA since $M_A < M$. Therefore, in order to avoid detection and meet the length requirement $M_A = M$, attacker must eavesdrop all $(1 - P_a)M$ ACK frames sent from victim to genuine node in DATA-ACK phases. He can record the corresponding $(1 - P_a)M$ eavesdropping RSS values or just insert $(1 - P_a)M$ random records as the falsified RSS records. After that, when victim asks for RSS feedback, by combining his $P_a M$ RSS records with the $(1 - P_a)M$ falsified RSS records, the attacker can feedback the exactly right number of $M_A = M$ RSS records to victim. We assume attacker does not disrupt the order of his feedback RSS records. Because if he disrupts the RSS records order, the correlation between his RSS feedback records and RSS records at victim becomes quite low and the IBA will be easily detected by victim. On the other hand, the attacker can work much harder than genuine node to make victim only received attack's stream, where $P_a = 1$ (as the worst case for IBA detection) to make victim only received one stream of RSS signals from attacker. However, in the practical application, this attack is very hard to realize. On one hand, the attacker should first sniff the communication traffic between genuine node and victim, e.g., to find the target of attack. Therefore, when IBAs are lunched, the genuine node usually has already communicated with the victim for a certain period of time and the corresponding RSS records have already been established at both sides. On the other hand, even if the attacker could launch the attack in the very beginning, it is hard for the attacker to fully prevent the genuine node from communicating with the victim. In order to do so, the attacker has to block/jam all the communications between the genuine node and victim, which would be easily detected by the genuine node or victim using existing jamming detection methods [21–23]. For example, as shown in Fig. 2 (b), when genuine node sends frames to victim, but he cannot receive any/few ACK from victim, he could lunch the jamming detection methods.

4 RCVIC IBA DETECTION DESIGN

In this section, we present the IBA detection algorithms. In subsection 4.1, the RCVIC detection algorithm is illustrated. In subsection 4.2, we illustrate the construction of RSS variation lists. In subsection 4.3, we discuss the appropriate parameter selection.

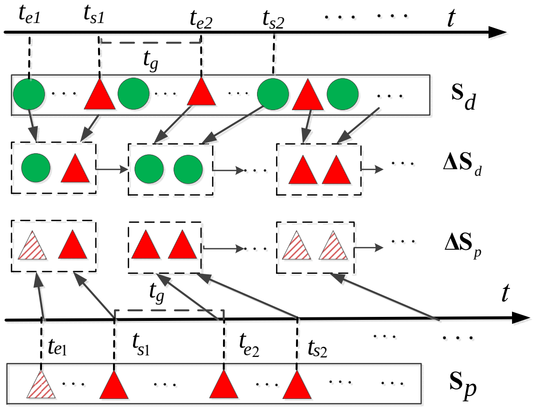


Fig. 5. Victim constructs RSS varitaion lists $\Delta\mathbf{S}_p$ and $\Delta\mathbf{S}_d$ with length N under IBA

4.1 RCVIC IBA detection

In RCVIC, the victim sends a verification request feedback to the sender for the M RSS records of the ACK frames during their past communication period. If there is an IBA attack, we consider the worst case scenario that victim received the M RSS records responded by attacker, as discussed above in Section 3.3.

After receiving the RSS records of the M ACK frames, denoted as $\mathbf{S}_p = [S(t'_1), ..., S(t'_M)]$, the victim constructs K RSS 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 variation lists, the victim computes the sample correlation coefficient of the two variation 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 IBA detection is summarized in Algorithm 1.

Algorithm 1 IBA detection flow

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

The intuition behind RCVIC is that if there is no attack, the RSS variations of the genuine node and the victim should be highly correlated according to the reciprocity. While if there is an IBA, the correlation should be degraded, because the reported RSS record is a mixture of the "right" and "wrong" RSS. This point is indicated in Fig. 2 and 3. Next, we will discuss the method of constructing the RSS variation lists, and the reason we construct multiple of them.

4.2 Constructing RSS variation lists

The process of constructing RSS variation lists $\Delta\mathbf{S}_p$ and $\Delta\mathbf{S}_d$ with length N are illustrated in Fig. 5. Given two RSS measurements $S(t_s)$ and $S(t_e)$, we define the *temporal RSS variation* as:

$$\Delta S(t_s, t_e) = S(t_s) - S(t_e) \tag{1}$$

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* ($t_l < t_s - t_e < t_u$). 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
```

Parameter selection and discussion: 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 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 8.1 that $N > 50$ and $K > 5$ are good choices in practice.

5 IBAs Detection Performance Evaluation

In this section, we theoretically analyze the RCVIC detection performance and derive the closed form expressions of detection rate and false alarm rate.

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. Thus RCVIC can be modeled as a hypothesis test:

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

where H_0 and H_1 are the null and alternative hypothesis, respectively. According to Algorithm 1, we have

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

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

where f_0 and f_1 are the PDF of the sample correlation coefficient under null and alternative hypothesis, respectively. For illustration purpose, we give the following definitions:

- forward genuine channel ($g \to v$): channel from the genuine to the victim
- backward victim to genuine response channel ($v \to g$): channel from the genuine to the victim
- attacking channel ($a \to v$): channel from the attacker to the victim
- eavesdropping and backward victim to attacker channel ($v \to a$): channel from the victim to the attacker

5.1 False alarm rate if no attack

This subsection derive RCVIC false alarm rate when there are no attacks.

5.1.1 RSS variation at victim and genuine node

According to the empirical measurement, the RSS follows a log normal shadowing fading model [9]. Suppose at time t, the victim receives a data frame sent from the genuine node, and the genuine node receives an ACK frame at time t'. The RSS of the data frame can be expressed as:

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

where d_0 is a close-in reference distance, $P_g(d_0)$ is genuine node's transmission power in dBm at the reference distance d_0, $d_{gv}(t)$ is the distance between the genuine node and the victim at time t, α_{gv} is the path loss exponent, $L_{gv}(d_0)$, 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 (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 8.1 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 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 $\mathcal{N}(0, 2\sigma_v^2)$.

RSS variation at genuine node: Similarly, the RSS variation of the corresponding ACK 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.

5.1.2 *The false alarm rate if no attack:*

Under the no attack situation, for a given threshold ρ_{th}, we can evaluate α by using expressions in *Property 1* as below.

Property 1: the false alarm rate α is denoted as

$$\alpha = \int_0^{\rho_{th}} f(\rho|\tilde{\rho} = \tilde{\rho}_{gv})\, d\rho \tag{9}$$

where

$$\boxed{\begin{aligned} f(\rho|\tilde{\rho}) =& \frac{(N-2)\Gamma(N-1)(1-\tilde{\rho}^2)^{\frac{(N-1)}{2}}(1-\rho^2)^{\frac{(N-4)}{2}}}{\sqrt{2\pi}\Gamma(N-0.5)(1-\rho\tilde{\rho})^{N-1.5}} \cdot \\ & {}_2F_1(0.5, 0.5; \frac{2N-1}{2}; \frac{\rho\tilde{\rho}+1}{2}), \quad (0 \le \rho \le 1). \end{aligned}}$$

$\Gamma(\cdot)$ is the gamma function and ${}_2F_1(\cdot)$ denotes the gaussian hypergeometric function. $\tilde{\rho}_{gv}$ is the population correlation coefficient, which is written as

$$\tilde{\rho}_{gv} = \frac{\rho_{gv}}{\sqrt{(1+\sigma_v^2/\sigma_X^2)(1+\sigma_g^2/\sigma_X^2)}}. \tag{10}$$

ρ_{gv} denotes the sample correlation coefficient between $X_{gv}(t_s)$ and $X_{vg}(t'_s)$ and that between $X_{gv}(t_e)$ and $X_{vg}(t'_e)$.

Proof. From the analysis above, the constructed RSS variation lists $\Delta\mathbf{S}_p$ and $\Delta\mathbf{S}_d$ with length N are sample sequences from two Gaussian population $\Delta\tilde{S}_{gv}(t_s, t_e)$ and $\Delta\tilde{S}_{vg}(t'_s, t'_e)$ with population correlation coefficient $\tilde{\rho}_{gv}$. For two sample sequences with length N from bivariate Gaussian variables with population correlation coefficient $\tilde{\rho}_{gv}$, the PDF of the sample correlation coefficient [24] can be presented with hypergeometric function in Property 1. From (2), we get *property 1*. For the detailed derivation of (10), please refer to Appendix A for the derivation. □

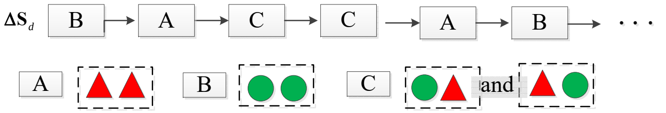


Fig. 6. $\Delta\mathbf{S}_d$ is regarded as a "package" list and each "package" contains two RSS records. There are three types of"package" corresponding to situation A, B and C, respectively.

Discussion: From Property 1, the false alarm rate is determined by the sample sequences length N and channel reciprocity coefficient ρ_{gv}. Further, ρ_{gv} is determined by the time interval between the data frame and its corresponding ACK frame, which are denoted as $t'_s - t_s$ and $t'_e - t_e$. We could shorten the time intervals to obtain a relatively high ρ_{gv}. The values of measured ρ_{gv} in the real world experiments are summarized in Table 3. Moreover, $\tilde{\rho}_{gv}$ is degraded by the estimation errors as 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}, and when the errors approach zero, $\tilde{\rho}_{gv}$ approaches ρ_{gv}.

5.2 Detection rate under attack

This subsection derives the detection rate under different attack patterns. For IBA attack situation, the M RSS record frames observed by victim are mixed of RSS of forward genuine channel $g \rightarrow v$ and attacking channel $a \rightarrow v$. In the second phase, assume the victim receives the M RSS record frames sent from the attacker, which are RSS records of eavesdropping channel $v \rightarrow a$.

5.2.1 *RSS variation at attacker and victim*

No matter what attacking pattern is, the RSS variations observed at the attacker is

$$\Delta\tilde{S}_{va}(t'_s, t'_e) = \Delta S_{va}(t'_s, t'_e) + \Delta n_a \tag{11}$$

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 ACK frame destined to the attacker/genuine node. Similar to the discussion in Section 5.1, $\Delta S_{va}(t'_s, t'_e)$ 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.

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

- 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.

Thus under IBA attack, the constructed RSS variation list $\Delta\mathbf{S}_d$ observed by the victim is mixed with three kinds of random variations, corresponding to situation A, B and C (situation D is included into situation C), respectively, which can be illustrated in Fig. 6. 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 as ΔS_v. The corresponding measured RSS variations with errors are $\Delta\tilde{S}_a$ and $\Delta\tilde{S}_v$.

5.2.2 *Population correlation coefficient*

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

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

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

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

$$\tilde{\rho}_B = \frac{\rho_{ag}}{\sqrt{(1+\sigma_v^2/\sigma_X^2)(1+\sigma_a^2/\sigma_X^2)}} \tag{13}$$

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

$$\Delta S_v \approx X_{av}(t_s) - X_{gv}(t_e) \tag{14}$$

We can derive that

$$\tilde{\rho}_C = \frac{\rho_{av}+\rho_{ag}}{2\sqrt{(1+\sigma_v^2/\sigma_X^2)(1+\sigma_a^2/\sigma_X^2)}} \tag{15}$$

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

5.2.3 ***The detection rate under different attack patterns***

The detection rate can be evaluated by using *Property 2* below.

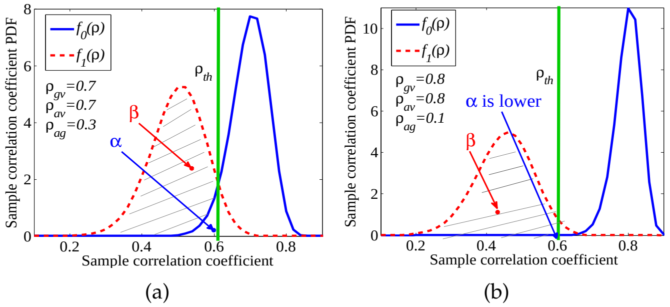
Property 2: For a given attack intensity P_a, the detection rate β under attacks is written as :

$$\beta = \int_0^{\rho_{th}} f(\rho|\tilde{\rho} = \tilde{\rho}_a)\, d\rho \tag{16}$$

where function $f(\rho|\tilde{\rho}_a)$ is the expression in the box of Property 1 by taking $\tilde{\rho} = \tilde{\rho}_a$. $\tilde{\rho}_a$ denotes the population correlation coefficient between $\Delta\tilde{S}_a$ and $\Delta\tilde{S}_v$ under "Interleaved" and "After/Before" attacks, which is written as

$$\tilde{\rho}_a = \frac{P_a\rho_{av} + (1-P_a)\rho_{ag}}{\sqrt{1+\sigma_v^2/\sigma_X^2}\sqrt{1+\sigma_a^2/\sigma_X^2}} \tag{17}$$

The derivation please refer to the Appendix B.



(a) (b)

Fig. 7. The key factors that impact false alarm rate. (a) $(\rho_{gv}, \rho_{av}, \rho_{ag}) = (0.7, 0.7, 0.3)$ in and $(\rho_{gv}, \rho_{av}; (b)\rho_{ag}) = (0.8, 0.8, 0.1)$.

5.2.4 *The key factors that impact false alarm rate*

From Property 2, the hypothesis functions in (2) and (3) are written as

$$f_0(\rho) = f(\rho|\tilde{\rho} = \tilde{\rho}_{gv}), \quad f_1(\rho) = f(\rho|\tilde{\rho} = \tilde{\rho}_a).$$

Thus for a given judgment threshold ρ_{th}, we can numerically calculate the detection rate β and false alarm rate α by Properties 1 and 2. From (10) and (17), it is found that the false alarm rates are mainly determined by the correlation coefficients ρ_{gv}, ρ_{av} and ρ_{ag}, attack density P_a (with the similar effect of channel fading with measurement errors). As analysis above, ρ_{av} will be relatively higher (typically close to 1) because the channel reciprocity holds well during the short time intervals of the DATA and ACK pairing frame. On the other side, ρ_{ag} will be much lower than ρ_{av} (typically close to 0), because of the location decorrelation property of the genuine and attacker [17, 25, 26]. From (17), the correlation coefficient is "smoothed out" by the lower value of ρ_{ag} multiplied with attack intensity P_a, which leads to a lower false alarm rate. When $P_a \to 0$, it has $\tilde{\rho}_a \to \tilde{\rho}_{gv}$, the correlation coefficient becomes the no IBAs stations in (10). On the other hand, when $P_a \to 1$, then $\tilde{\rho}_a \to \tilde{\rho}_A$ in (12), where the correlation coefficient is only determined by $\tilde{\rho}_{av}$.

For further illustration, Fig.7 shows the hypothesis functions $f_0(\rho)$ and $f_1(\rho)$ under $N = 100$, $P_a = 0.5$. The correlation coefficients are set as $(\rho_{gv}, \rho_{av}, \rho_{ag}) = (0.7, 0.7, 0.3)$ and $(0.8, 0.8, 0.1)$, respectively. In Fig.7 (a) and (b), the size of shaded area insides $f_1(\rho)$ (the red dotted function curve) on left side of ρ_{th} which represents the detection rate β, while the size of blank area under $f_0(\rho)$ (the blue solid function curve) on left side of ρ_{th} that measures the false alarm rate α. By comparing (a) and (b) in Fig.7, it is found that a larger gap between $f_0(\rho)$ and $f_1(\rho)$ leads to a higher detection rate β under the conditionally lower false alarm rate α. However, their gap is mainly determined by the gaps between channel reciprocity coefficients (ρ_{gv}, ρ_{av}) and ρ_{ag}. As the tie to the actual detection process, Fig.7 indicates that RCVIC constructing multiple RSS variation lists (instead of using the original RSS [5]) to detect IBAs that can decrease the false alarm rate by ruling out the following two "bad" situations: 1) smoothing out a "good luck for attacker" when attacker's variations are correlated with genuine node during his moving, and 2) smoothing out a "bad luck for genuine node" variation list when there

TABLE 2
ROC performance of Fig. 7 nearby the approximately optimal threshold.

$\rho_{th}(881)$	0.64	**0.66**	0.68
β	0.9961	0.9986	0.9996
α	0.0003	0.0012	0.0036
$\rho_{th}(773)$	0.59	**0.61**	0.63
β	0.8928	0.9393	0.9691
α	0.0284	0.0550	0.1006

is no attack but some occasional variations between genuine node and victim that are not correlated well.

5.3 RCVIC optimal decision threshold

This subsection analyzes the optimal threshold ρ_{th}^{opt}. Assume the event of existing an attacker with probability τ, then let

$$\bar{\beta} = \int_{\rho_{th}}^{1} f_1(\rho|\tilde{\rho}_a) d\,\rho = 1 - \beta \tag{18}$$

To minimize the sum of error detection rate $\bar{\beta}$ and false alarm rate α, we can formulate the problem as the optimization problem below

$$\min\ \tau\bar{\beta} + (1-\tau)\alpha \tag{19}$$

Based on (2)-(19), we can get the optimal threshold ρ_{th}^{opt} which is the solution of formula

$$(1-\tau) f_0(\rho_{th}^{opt}|\tilde{\rho}_{gv}) - \tau f_1(\rho_{th}^{opt}|\tilde{\rho}_a) = 0, 0 < \rho_{th}^{opt} < 1 \tag{20}$$

Because the complex expressions of $f_0(\rho_{th}^{opt}|\tilde{\rho}_{gv})$ and $f_1(\rho_{th}^{opt}|\tilde{\rho}_a)$, the exact solution ρ_{th}^{opt} is hard to obtain. However, based on (20), we can get the approximately optimal solution by mathematical software. Table II shows the analytical ROC performances of Fig. 7 (a), (b) nearby the approximately optimal thresholds (terms with "881" and "773"). We can see that the RCVIC can achieve good ROC performance. In Fig. 7 (b), RCVIC can achieve about $\beta = 0.9986$ with $\alpha = 0.0001$. While in Fig. 7 (a), RCVIC can achieve a performance of $\beta = 0.94$ with $\alpha = 0.05$.

6 RCVIC PARTITION PROCESS

If IBAs are detected, RCVIV conducts the next partition for further analysis. Victim first partitions the received frames into two classes. The frames in the same class should be sent from the same senders. This partition is achieved by applying the unsupervised threshold methods Otsu [17, 27, 28] without the prior channel or location information about the users. The detailed analysis and algorithms about partition are provided in Section 6.1 as below.

6.1 RCVIC partition approach

The basic principle of partition for mobile users is that for most of time slots during their movements, the RSS traces from the genuine node and attacker are correlated to the different locations in physical-time space. Thus it is reasonable to assume that genuine node and attacker are more likely to appear at different locations in most of time slots during the movements, rather than "encountering" at the same location. Thus RSS records from genuine node and attacker are not highly correlated to each other in general, which can be partitioned by victim node [17, 28].

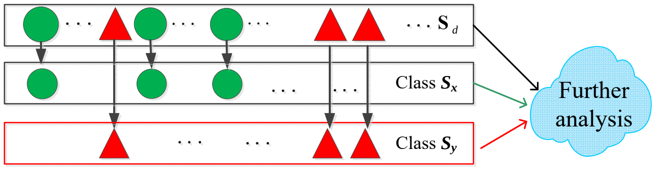


Fig. 8. RCVIC partition for further analysis

6.1.1 Partition algorithm

In RCVIC partition, where each part has M consecutive RSS records, corresponding to the M time slots. The RSS record in the ith time slot is denoted as $S_i \in \mathbf{S}_d, (i = 1, 2, 3....M)$. The victim partitions $\mathbf{S}_d$ into two classes as $\mathbf{S}_x = (S_{x,1}, S_{x,2}, ...S_{x,l})$ and $\mathbf{S}_y = (S_{y,1}, S_{y,2}, ...S_{y,h}), l + h = M$, corresponding to the RSS records sent from two different nodes. At a time slot t_i, the received S_i may be sent from the genuine node or attacker, thus the conditional probability distributions are denoted as $p(s|s \in \mathbf{S}_x) = p(s|X)$ and $p(s|s \in \mathbf{S}_y) = p(s|Y)$.

In practical applications, it is not feasible for us to know the closed form expressions of $p(s|X)$ and $p(s|Y)$ for mobile users. Without a prior knowledge about the distribution of either node's RSS, we obtain an optimal threshold by applying the unsupervised threshold methods, such as Otsu thresholding [27, 28] to partition the RSS records into two classes. Otsu thresholding obtains compact clustering by using the inter-class variance, in order to make the partition classes as tight as possible and thus minimize their overlap. Due to page limit, we do not introduce the detailed Otsu thresholding algorithm here. The more algorithm details please refer to [27]. The key steps of our partition algorithm are described below.

(1)RSS histogram estimation: the distinct RSS values are denoted as s_j with $j \in (1, 2, ..., L)$, where L is the number of distinctive values in S_i. Denote $p(s_j)$ as an estimate of the probability such that $\sum_{j=1}^{L} p(s_j) = 1$

(2)Optimal threshold ρ_t searching: victim note searches a ρ_t which leads to the maximization of the inter class variances as

$$\max_{\rho_t} \sum_{i=1}^{\rho_t - 1} p(s_i) \cdot \sum_{j=\rho_t}^{L} p(s_j) \cdot [\mu_1(\rho_t) - \mu_2(\rho_t)]^2 \tag{21}$$

where $\mu_1(\rho_t), \mu_2(\rho_t)$ are the mean values of the two partition RSS classes separated by a threshold ρ_t.

6.1.2 Factors impacts RCVIC partition

One factor impacts RCVIC partition is the average distances between genuine node and attacker: As discussed above, it is hard for the attacker to always keep closed to genuine node during their movements. Thus for most time slots during their movements, if the distances between genuine node and attacker is larger than the correlation distance, the RCVIC partition process can work well. The correlation distance is mainly determined by the prorogation environments. It is usually about 1m for indoor and 1 $\sim$ 3m for outdoor environments [9].

The other factor is the time interval between two consecutive RSS records, which is defined $dt = t_{i+1} - t_i$. The user will move a maximum distance as $\Delta d = vdt$ in the

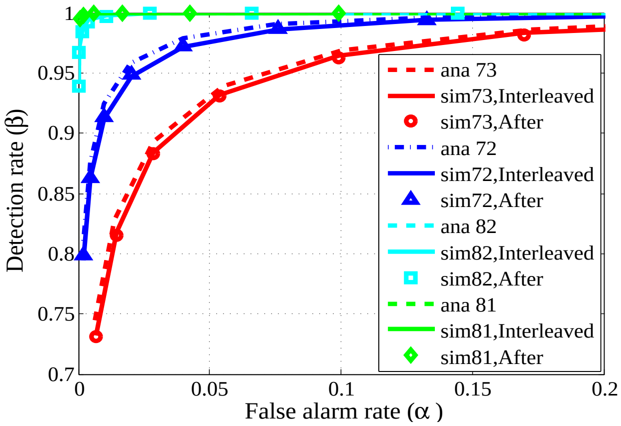


Fig. 9. Analytical and simulation results of ROC performance under different channel reciprocity coefficient and attacks

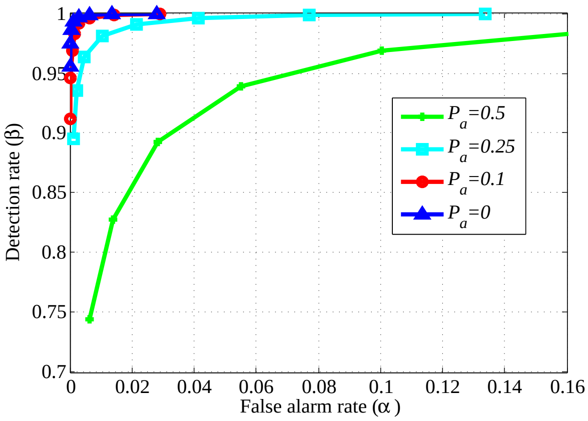
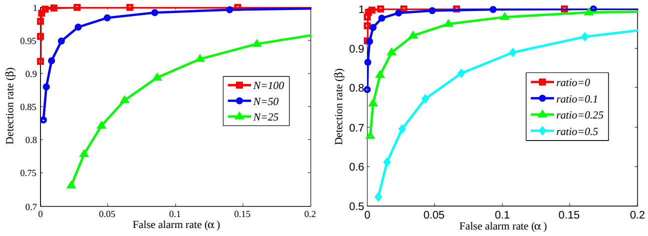


Fig. 10. ROC performance under different attack density P_a



(a) (b)

Fig. 11. (a) Impact of length N on ROC performance; (b) Impact of background noise to shadow power ratio on ROC performance.

time interval, where v denotes the nodes' moving speed. The time interval should be small so that the RSS fluctuation is not too dramatically. As we have known that dt is usually less than $0.005s$ [20], and the users is usually walking or running with a speed $v < 5m/s$. As a result, $\Delta d \sim 0.02$m, which is very small.

6.1.3 System further analysis

After the partition process, victim separates $\mathbf{S}_d = [S(t_1), ..., S(t_M)]$ into two classes as $\mathbf{S}_x$ and $\mathbf{S}_y$. Accordingly, based on the time indexes of $\mathbf{S}_x$ and $\mathbf{S}_y$, victim can separate the received M data frames into two classes, and the data frames in the same class should be sent from the same senders, too. *However, the victim cannot directly identify which class of RSS records/data frames is belonged to attacker/genuie node by utilizing the feedback RSS records.* This is mainly because the feedback of RSS records may be sent by attacker. Thus the attacker may potentially fool the victim to classify the genuine stream to the attacker's by inserting false RSS records into the feedback.

However, even if victim cannot directly find which class is possibly sent by attacker/genuine node without any prior knowledge of genuine node, the partitioned classes could still benefit the further analysis, such as network forensics [13], attacker localizing [4] and trajectory analysis, etc. Besides, this partition implementation is with relatively low cost, which is desired for practical implementation.

On the other hand, in the DATA-ACK communication, the attacker could deliberately record the "falsified" RSS records from ACK of himself to hide the attack evidence, e.g., as shown in Fig. 2 (b), attacker could record the "falsified" RSS records at time slot t_2 for ACK to himself. However, this will only increase the probability of detection since the correlation between the "falsified" RSS records and the ones at the victim node will be decreased. Thus, it will only expose the attacker with a higher chance which contradicts the attacker's incentive of avoiding detection.

7 Numerical Performance Evaluation

In the subsection, we present the numerical and simulation results of ROC performance and verify our analytical approach. In the simulation, we generate 50,000 times of RSS sampling records for both of interleaved and after attack to get the average ROC performance. Fig. 9 shows the analytical and simulation results of ROC performance under "Interleaved" and "After" attack with $(\rho_{gv}, \rho_{av}, \rho_{ag}) = (0.7, 0.7, 0.3), (0.7, 0.7, 0.2), (0.8, 0.8, 0.2)$ and $(0.8, 0.8, 0.1)$, corresponding to abbreviation "73, 72, 82" and "81", respectively. In Fig. 9, we denote the analytical and simulation results by term "ana" and "sim". The attack density is set as $P_a = 0.5$, the length of RSS variation lists is set as $N = 100$ and $\sigma_X^2 = 1, \sigma_a^2 = \sigma_g^2 = \sigma_v^2 = 0$.

7.1 Impact of reciprocity

From Fig. 9, all of the analytical results are very close to simulation results. Also, the interleaved attack results are close to the after attack results, which fully validates our theoretic analysis above. From Fig. 9, under the same ρ_{gv}, ρ_{av}, a higher ρ_{ag} will obviously decrease the ROC performances. On the contrary, under the same ρ_{ag}, a higher ρ_{gv} will increase the ROC performances clearly. This phenomenon can be interpreted as a higher ρ_{gv} will increase the population PDF gap between $\tilde{\rho}_{gv}$ and $\tilde{\rho}_a$, thus will increase the ROC performance. It verifies our theoretical analysis in subsection 5. From Fig. 9, it can be found that even though ρ_{gv} decreases to 0.7 against ρ_{ag} is higher as 0.3, we can still achieve desirable performance about $\beta > 90\%$ percent against with false alarm rate $\alpha = 0.05$.

7.2 Impact of attacker density

Fig. 10 compares ROC performance with attack density $P_a = 0.5, 0.25, 0.1$ and $P_a = 0$ under the interleaved attack. The reciprocity coefficients are set as $(\rho_{gv}, \rho_{av}, \rho_{ag}) =$

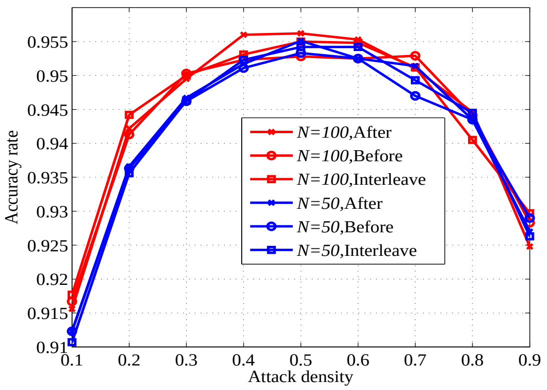


Fig. 12. Classification accuracy under different attacks and P_a

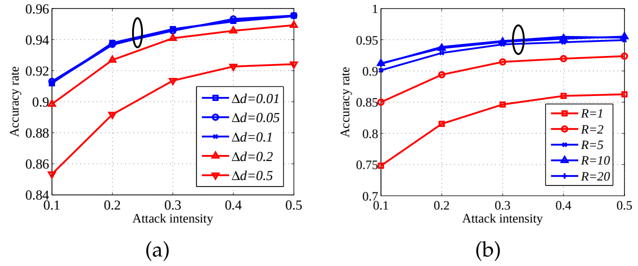
$(0.7, 0.7, 0.3)$. In Fig. 10, the RCVIC can achieve performance $\beta > 90\%$ against false alarm rate $\alpha < 0.04$ under $P_a = 0.5$. Correspondingly, the higher attack density will decrease the ROC performance. If the attacker is a passive eavesdropper with $P_a = 0$,the detect rate will closed to 1 with false alarm rate $\alpha \to 0$.

7.3 Impact of N and noise to power ratio

Fig. 11 (a) shows ROC performance under the interleaved attack with $(\rho_{gv}, \rho_{av}, \rho_{ag}) = (0.8, 0.8, 0.2)$. The lengths are set as $N = 25, 50, 100$, respectively. The other parameters are the same with Fig. 9. From Fig. 11 (a), we can find a larger N can clearly improve the ROC performance. However, too large N will cause longer delay for the RCVIC system. From Fig. 11, we find with $N = 50$, the system can achieve a relatively better performance. Fig. 11 (b) shows the impact of background noise to shadow power ratio on ROC performance. In Fig. 11 (b), we set the ratio $\sigma_a^2/\sigma_X^2 = \sigma_g^2/\sigma_X^2 = \sigma_v^2/\sigma_X^2 = 0, 0.1, 0.25$ and 0.5, respectively under $N = 100$. The other parameters are the same with Fig. 9. Intuitively from (b), a larger measurement error ratio will degrade the performance. Therefore to keep a high SNR communication is necessary.

7.4 Classification performance

Fig. 12 shows the classification accuracy performance. In Fig. 12, we let the genuine node and attacker are random located in a circular region with radius $R = 5$m and randomly moving with $\Delta d = 0.1$. Victim is located in the center of the circular. We compute numerical average accuracy performance by separating $\mathbf{S}_d$ and $\mathbf{S}_p$ into M/N segments. Each segments contains $N = 50$ and 100 RSS records, versus attacker intensity P_a varying from 0.1 to 0.9. From Fig. 12, it can be found that RCVIC model can achieve an accuracy performance higher than 90 percents for $N \geq 50$. When P_a is close to 0.5, RCVIC will achieve the highest accuracy performance. This is mainly because the numbers of attacker and genuine node's frames will be equivalent, and in this case the interval distances of consecutive frames from one node becomes the smallest in average, thus increases the correlation of the RSS records sent from the same node, which inevitably improves the classification accuracy performance.



(a)

(b)

Fig. 13. (a) Impact of Δd on classification accuracy;(b) Impact of R on classification accuracy.

Fig. 13 (a), (b) represent the scenarios the parameters Δd impacts the classification accuracy performance. From Fig. 13 (a), we can find that a higher Δd will decrease the classification accuracy. Because the higher mobile speed with larger inter-frame time interval will decrease the classification accuracy. From Fig. 13 (b), it finds that nodes moving in a smaller region will decrease the classification accuracy. This is mainly because users moving in a smaller region will have higher probability to be close to each other during their movements. The numerical results above validate our analytical results and show the prospective performance of RCVIC. The next section will investigate the RCVIC scheme in the real world tests.

8 Experimental Methodology

We carried out extensive mobile experiments in real indoor and outdoor environments and test the applicability of RCVIC 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 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 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 ACK frames in our model. Tcpdump 4.0.0 [19] 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.

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. 14. The victim 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 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.

Aligning and Matching DATA and ACK: We first align the DATA (Ping request) received by the victim with the corresponding ACK received by the genuine node. Since the ACK

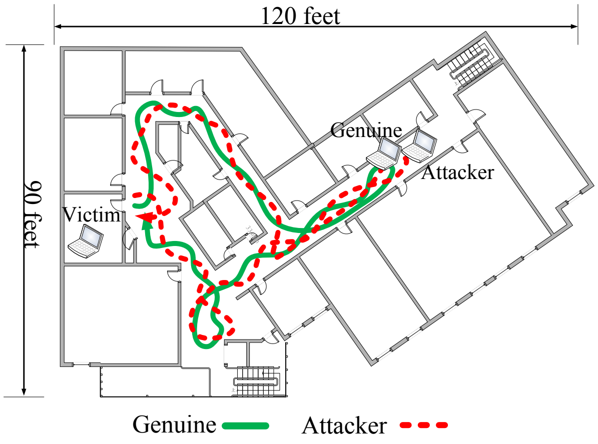


Fig. 14. Indoor experimental environment

has no sequence number, in order to match 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 victim. Using the same method, we match the DATA-ACK between the victim and the attacker. At the attacker, we also match the overheard ACK with the Ping request sent from the genuine node to the victim.

We then generate the RSS variation lists at both genuine and victims using the RSS of the matched 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'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.

8.1 Experimental analysis

Table 3 summarizes the measured correlation coefficient between the forward ($g \rightarrow v$) and backward ($v \rightarrow g$) genuine channels (ρ_{gv}), between the forward ($a \rightarrow v$) and backward ($v \rightarrow a$) attacking channels (ρ_{av}), and eavesdropping ($v \rightarrow a$) and forward genuine ($g \rightarrow v$) 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 $g \rightarrow v$ and $v \rightarrow g$, and that between $a \rightarrow v$ and $v \rightarrow a$ 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. We also verify that all the RSS variations follow Gaussian distributions. Due to the page limitation, we do not show all the detailed experiments results here. The readers can refer to Fig. 4 in the conference paper.

TABLE 3
Correlation coefficient and standard deviation of the RSS variations.

		ρ_{gv}	ρ_{av}	ρ_{ag}	$\sigma_{\Delta gv}$	$\sigma_{\Delta vg}$	$\sigma_{\Delta ag}$
Indoor	shadow	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	shadow	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

8.1.1 Impact of list lengths

In this subsection, we analyze the performance of RCVIC under different lengths of variation list, number of constructions, frame intervals, and attacking intensities. Fig. 15 shows the empirical ROC varying different parameters under the indoor shadowing scenario. 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. The attacking intensity $P_a = 0.5$.

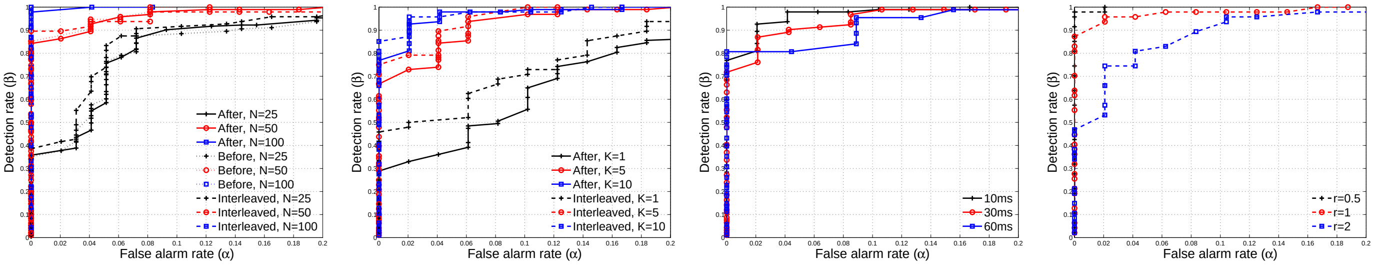
Fig. 15(a) shows the empirical ROC. We can see that with list lengths increased, the detection performance improves. Even when we only use a very short list length ($N = 25$), we can still achieve around 90% detection rate with 10% false alarm rate. When the list length is 100, we can most surely detect the attack without false alarm. It also shows that RCVIC 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.

8.1.2 Impact of number of constructions

Fig. 15(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).

8.1.3 Impact of frame intervals

Fig. 15(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 K

(c) Impact of frame intervals

(d) Impact of r

Fig. 15. Empirical performance of RCVIC under different parameters in the indoor shadowing scenario

8.1.4 Impact of attacking intensities

For easy understanding, let r denotes the ratio of the attacking frames to the genuine frames that victims received, thus $r = 1/(1 - P_a)$. Fig. 15(d) shows the ROC under different attacking intensities under attacking pattern "Interleaved" in the real world expriments. The frame interval is $10ms$, $N = 50$, and $K = 10$. It shows that the performance degrades when the attacking intensity increases. However, even with $r = 2$, RCVIC 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.

9 Discussion

Unprotected ACK Frames: If the ACK frame is used at the genuine user, he should make sure that it is sent from the victim. 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 receives the DATA, it will instantly send back an ACK to the genuine node. The attacker's ACK may collide with the victim's ACK, so the genuine node will not record the corresponding RSS but considers the ACK is lost.

Unprotected Feedback Channel: For the case of unprotected feedback channel, the attacker could eavesdrop on the RSS records of the genuine node's feedback to victim and combine with its own observations, then feedback them to the victim. However, this attack is hard to be successful. As analyzed in Section 3.3, when the victim asks for the RSS records feedback, the genuine node immediately responses with $M_G = (1 - P_a)M$ RSS records. If the victim received the M_G RSS records, he can immediately detect the IBAs because the number of RSS records in the feedback is less than M. However, because attacker has to construct M records that may pass the check, the attacker must first monitor and eavesdrop RSS records feedback from genuine node, then combine them with its own observations. After that he can feedback them to victim. Thus the attacker will inevitably suffer a larger processing delay (potentially doubling the delay of genuine node's response) than the genuine node. So the victim node can set a delay threshold for the response to significantly thwart this kind of attack.

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 match the DATA and ACK frames properly. If the victim 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.

Due to the page limitation, we do not show all the detailed discussion here. The readers can refer to Section VIII in the conference paper.

10 Conclusion

This paper proposed a RCVIC scheme for IBA detection in mobile wireless networks. We evaluated RCVIC performance through detailed theoretical analysis. We validated its feasibility through numerical simulations and real world experiments by using off-the-shelf 802.11 devices under different attacking patterns in indoor and outdoor mobile scenarios. Experimental results show that RCVIC can achieve desirable performance under the tested scenarios. RCVIC 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 (10)

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}.

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

Appendix B
Derivation of (17)

Proof. First we prove the "Interleave" attack. From the analysis above, $\Delta\mathbf{S}_d$ with length N is a mixture of three types of variations corresponding to situation A, B and C, respectively. From (12), (13) and (15), the three cases correspond to three independent gaussian variables and their population correlation coefficients with $\Delta\tilde{S}_a$ are $\tilde{\rho}_A, \tilde{\rho}_B$ and $\tilde{\rho}_C$, corresponding to situation A, B and C, respectively. Thus $\Delta\mathbf{S}_d$ can be regarded as samples coming from a mixture gaussian variable $\Delta\tilde{S}_v$ [26], where $\Delta\tilde{S}_v$ follows a mixture gaussian distribution $\mathcal{N}(0, 2\sigma_X^2 + 2\sigma_v^2)$. Let (P_A, P_B, P_C) denotes the probability of situation A, B and C occurred in $\Delta\mathbf{S}_d$ and $\lambda_A, \lambda_B, \lambda_C$ denote the gaussian variables when $\Delta\tilde{S}_v$ corresponding to situation A, B and C, respectively. The population correlation coefficient $\tilde{\rho}_a$ between $\Delta\tilde{S}_v$ and $\Delta\tilde{S}_a$ is derived as:

$$\begin{aligned}\tilde{\rho}_a &= \frac{P_A E(\lambda_A \Delta\tilde{S}_a) + P_B E(\lambda_B \Delta\tilde{S}_a) + P_C E(\lambda_C \Delta\tilde{S}_a)}{\sqrt{2\sigma_X^2 + 2\sigma_v^2}\sqrt{2\sigma_X^2 + 2\sigma_a^2}} \\ &= \frac{2\sigma_X^2 P_A \rho_{av} + 2\sigma_X^2 P_B \rho_{ag} + \sigma_X^2 P_C(\rho_{av} + \rho_{ag})}{\sqrt{2\sigma_X^2 + 2\sigma_v^2}\sqrt{2\sigma_X^2 + 2\sigma_a^2}} \\ &= \frac{P_A \rho_{av} + P_B \rho_{ag} + 0.5 P_C(\rho_{av} + \rho_{ag})}{\sqrt{1 + \sigma_v^2/\sigma_X^2}\sqrt{1 + \sigma_a^2/\sigma_X^2}}\end{aligned}$$

Victim will sample $2N$ RSS records from M RSS feedback records to build $\Delta\mathbf{S}_d$. For a large N, the probability of sampling k RSS records from attacker is $C_{2N}^k P_a^k (1 - P_a)^{2N-k}$. The probability of sampling a RSS record from attacker node is $(2NP_a)/(2N) = P_a$ and probability of a sampling a RSS record is from genuine node is $(1-P_a)$. After that the victim will construct $\Delta\mathbf{S}_d$ with length N by the $2N$ sampling RSS records. The process can be regarded as victim generates N independent "packages" from $2N$ RSS sampling records, and each "package" contains two RSS records, which is shown in Fig. 6. The probability of a "packages" corresponding to situation A, B, C can be written as $P_A = P_a^2, P_B = (1 - P_a)^2, P_C = 2P_a(1 - P_a)$, Taking them into the equality above, we obtain *property 2*. Similarly, for "before/after" attacks, when N becomes large, the victim node averagely get NP_a "packages" A, $N - NP_a$ "packages" B and zero "packages" C . Thus the density of situation A, B and C in S_B are $P_A = P_a,\ \ P_B = 1 - P_a,\ \ P_C = 0$. Taking them into the equality above, we obtain *property 2*

□

Acknowledgments

This work is supported by the NSFC (No. 61901089) and the National major R & D program (No. 2018YFB0904900, 2018YFB0904905). It was also supported in part by the Commonwealth Cyber Initiative (CCI) and its Northern Virginia (NOVA) Node, an investment in the advancement of cyber R&D, innovation and workforce development.

References

[1] P. Suhasaria, A. Garg, A. Agarwal, and K. Selvakumar, "Distributed denial of service attacks: A survey," *Imperial Journal of Interdisciplinary Research*, vol. 3, no. 3, 2017.

[2] R. Banakh, A. Piskozub, and I. Opirskyy, "Detection of mac spoofing attacks in ieee 802.11 networks using signal strength from attackers devices," in *International Conference on Theory and Applications of Fuzzy Systems and Soft Computing*. Springer, 2018, pp. 468–477.

[3] R. U. Rahman and D. S. Tomar, "Security attacks on wireless networks and their detection techniques," in *Emerging Wireless Communication and Network Technologies*. Springer, 2018, pp. 241–270.

[4] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2418–2434, Jun 2010.

[5] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 44–58, Jan 2013.

[6] M. Subhash and A. R. Babu, "Identification of spoofing attackers and determining the number of adversaries by using received signal strength in wireless networks," vol. 4, no. 6, pp. 930–933, Feb 2017.

[7] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, "Multi-channel based sybil attack detection in vehicular ad hoc networks using rssi," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2018.

[8] M. Faisal, S. Abbas, and H. U. Rahman, "Identity attack detection system for 802.11-based ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 128, 2018.

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

[10] F. Pan, H. Wen, R. Liao, Y. Jiang, A. Xu, K. Ouyang, and X. Zhu, "Physical layer authentication based on channel information and machine learning," in *2017 IEEE Conference on Communications and Network Security (CNS)*, Oct 2017, pp. 364–365.

[11] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective rayleigh channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5948–5956, December 2009.

[12] Y.-C. Tung, K. G. Shin, and K.-H. Kim, "Analog man-in-the-middle attack against link-based packet source identification," in *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM, 2016, pp. 331–340.

[13] Y. Teing, A. Dehghantanha, K. R. Choo, Z. Muda, and M. T. Abdullah, "Greening cloud-enabled big data storage forensics: Syncany as a case study," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 2, pp. 204–216, 2019.

[14] R. Niu, A. Vempaty, and P. K. Varshney, "Received-signal-strength-based localization in wireless sensor networks," *Proceedings of the IEEE*, vol. 106, no. 7, pp. 1166–1182, July 2018.

[15] H. Liu, Y. Wang, J. Liu, J. Yang, Y. Chen, and H. V. Poor, "Authenticating users through fine-grained channel information," *IEEE Transactions on Mobile Computing*, vol. 17, no. 2, pp. 251–264, Feb 2018.

[16] L. Xiao, X. Wan, and Z. Han, "Phy-layer authentication with multiple landmarks with reduced overhead," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1676–1687, March 2018.

[17] 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.

[18] K. Zeng, K. Govindan, D. Wu, and P. Mohapatra, "Identity-based attack detection in mobile wireless networks," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 1880–1888.

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

[20] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai, "Ieee 802.11 wireless local area networks," *IEEE Communications Magazine*, vol. 35, no. 9, pp. 116–126, Sep. 1997.

[21] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1746–1759, 2014.

[22] N. Sufyan, N. A. Saqib, and M. Zia, "Detection of jamming attacks in 802.11b wireless networks," *Eurasip Journal on Wireless Communications and Networking*, vol. 2013, no. 1, p. 208, 2013.

[23] A. Hamieh and J. Benothman, "Detection of jamming attacks in wireless ad hoc networks using error distribution," pp. 4831–4836, 2009.

[24] E. WEISSTEIN, "Correlation coefficient–bivariate normal distribution [online]. mathworld–a wolfram web resource," 2014.

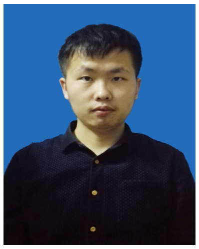
[25] Sheng, Yong and Tan, K. and Chen, Guanling and Kotz, D. and Campbell, A, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," in *The 27th Conference on Computer Communications INFOCOM*, 2008, pp. 1768–1776.

[26] 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.

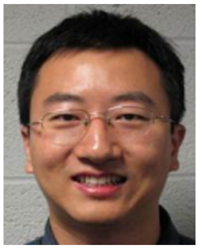
[27] N. Otsu, "A threshold selection method from gray-level histograms," *IEEE transactions on systems, man, and cybernetics*, vol. 9, no. 1, pp. 62–66, 1979.

[28] P. K. Sahoo, S. Soltani, and A. K. Wong, "A survey of thresholding techniques," *Computer vision, graphics, and image processing*, vol. 41, no. 2, pp. 233–260, 1988.

Jie Tang (cs.tan@uestc.edu.cn) is currently a lecturer in School of Aeronautics and Astronautics, University of Electronic Science and Technology of China (UESTC), Chengdu 611731. He achieved Ph.D. degree at UESTC, in 2018. From 2016-2019, He was also a visiting scholar in George Mason University, Fairfax, U.S.A. His current main interests lie in wireless communications, IoT and UAV networks.



Long Jiao (ljiao@gmu.edu) received his B.Sc. degree in information security from Xidian University, Xian, China, in 2016. Now he is currently pursuing his Ph.D. degree at George Mason University, Fairfax, Virginia. His current fields of interest include 5G physical layer security, mmWave communications and deep learning.



Kai Zeng (kzeng2@gmu.edu) received his Ph.D. degree in electrical and computer engineering from the Worcester Polytechnic Institute (WPI) in 2008. He was a postdoctoral scholar with the Department of Computer Science, University of California at Davis (UCD) from 2008 to 2011. He was with the Department of Computer and Information Science, University of Michigan-Dearborn as an assistant professor from 2011 to 2014. He is currently an associate professor with the Department of Electrical and Computer Engineering, Cyber Security Engineering, and the Department of Computer Science at George Mason University. His current research interests are in cyber-physical system security and privacy, 5G physical layer security, network forensics, and spectrum sharing networks. He was a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) Award in 2012. He received the Excellence in Postdoctoral Research Award from UCD in 2011 and the Sigma Xi Outstanding Ph.D. Dissertation Award from WPI in 2008. He is an Editor of IEEE Transactions on Information Forensics and Security, IEEE Transactions on Wireless Communications, and IEEE Transactions on Cognitive Communications and Networking.

Hong Wen (sunlike@uestc.edu.cn) received the Ph.D. degree from Southwest Jiaotong University, China, and University of Waterloo, Canada, in 2004 and 2018, respectively. She was a Visiting Scholar and a Postdoctoral Fellow with the ECE Department, University of Waterloo, Waterloo, ON, Canada. She is a professor with University of Electronic Science and Technology of China now and worked there over 15 years. Her current main interests lie in wireless communication systems and system security.

Kannan Govindan (g.kannan16@samsung.com) has been working with Amazon, heading the NLU (natural language understanding) initiatives for Alexa Local Search world wide. Earlier he was working for Walmart Labs, Target Technology Center, Samsung Research and University of California Davis. He completed PhD from Indian Institute of Technology Bombay with Microsoft Research India PhD Fellowship. He is a senior member of IEEE, and served as Associate Editor for IEEE Communications Magazine, Guest Editor of IEEE Communications Magazine, Editor of IETE Technical Review. Presently he is serving as associate editor for IEEE Access. He was also TPC member of numerous IEEE conferences including Globecom, ICC, SECON.

Daniel Wu (dyqith@gmail.com) was a postdoctoral scholar with the Department of Computer Science, University of California at Davis (UCD). He is a software engineer at Google company.

Prasant Mohapatra (prasant@cs.ucdavis.edu) is serving as the Vice Chancellor for Research at University of California, Davis.He is also a Distinguished Professor in the Department of Computer Science. He was the Department Chair of Computer Science during 2007-13. Dr. Mohapatra received his doctoral degree from Penn State University in 1993, and received an Outstanding Engineering Alumni Award in 2008. Dr. Mohapatra received an Outstanding Research Faculty Award from the College of Engineering at the University of California, Davis. He received the HP Labs Innovation awards in 2011, 2012, and 2013. He is a Fellow of the IEEE and a Fellow of AAAS. Dr. Mohapatra's research interests are in the areas of wireless networks, mobile communications, cybersecurity, and Internet protocols. He has published more than 350 papers in reputed conferences and journals on these topics. Dr. Mohapatra's research has been funded through grants from the National Science Foundation, US Department of Defense, US Army Research Labs, Intel Corporation, Siemens, Panasonic Technologies, Hewlett Packard, Raytheon, and EMC Corporation.