In-band Secret-Free Pairing for COTS Wireless Devices

Nirnimesh Ghose, *Member, IEEE,* Loukas Lazos, and Ming Li, *Senior Member, IEEE*.

Abstract—Many IoT devices lack the necessary interfaces (keyboards, screens) for entering passwords or changing default ones. For these devices, bootstrapping trust can be challenging. We address the problem of device pairing in the absence of any shared secrets. Pairing is a two-phase process that requires mutual authentication between the two parties and the agreement to a common key that can be used to further bootstrap essential cryptographic mechanisms. We propose a secret-free and in-band trust establishment protocol that achieves the secure pairing of commercial off-the-shelf (COTS) wireless devices with a hub. As compared to the state-of-the-art, our protocol does not require any hardware/firmware modification to the devices, or any out-of-band channels, but can be applied to any COTS device. Furthermore, our protocol is resistant to active signal manipulations attacks that include recently demonstrated signal nullification at an intended receiver. These security properties are achieved in-band with the assistance of a helper device such as a smartphone and by exploiting hard-to-forge signal propagation laws. We perform extensive theoretical analysis to verify the security of the proposed protocol. In addition, we validate our theoretical results with experiments using COTS devices and USRP radios.

Index Terms—Bootstrapping, Physical-layer Security, Wireless Signal Manipulation Attacks, Man-in-the-Middle Attacks, Key Establishment, Message Integrity, Internet-of-Things, Secret-free, In-band, Trust establishment, COTS wireless devices.

1 Introduction

The number of wirelessly connected devices–wearables, cameras, medical devices, smart locks, home monitoring sensors, industrial sensors and actuators, Internet-enabled appliances, etc.–has recently exploded. These devices collect a wealth of sensitive information about the user's environment, behavior, whereabouts, and health. They are also assigned to perform safety-critical tasks such as control entry to one's residence, automatically deliver drugs and regulate one's heart rate, control electric and gas appliances, and others. For example, a smart garage door provides access to the house premises. A remotely-programmable pacemaker controls the electric pulses applied to one's heart. Smart insulin pumps continuously monitor and adjust the insulin delivered to diabetic patients.

The vast majority of devices that are introduced in the market today adopt the gateway model where end devices connect to a hub/gateway for remote actuation and data reporting. To protect the device and the data it collects from unauthorized parties, each device and the hub need to build trust before they can securely communicate. The so-called device pairing consists of a mutual authentication phase followed by a common key agreement phase. The first phase is used to verify the device's identity (or legitimacy), whereas the second confirms a secure channel over a public medium. The common key is further used to bootstrap other essential cryptographic functions. Classic techniques for secure pairing either involve the manual input of the hub's secret to the device or the preloading of a unique secret. This secret is loaded to the hub via an out-of-band (OOB) channel, e.g., the user enters the secret manually [1], scans a quick-response (QR) code [2] or relies on a public key infrastructure [3]. Nevertheless, traditional solutions pose significant usability, scalability, and interoperability hurdles. Several new wireless devices lack the necessary interfaces to enter or change keys. QR codes have been shown to be vulnerable to several attacks that allow for identity misbinding [4]–[6]. These attacks either fool devices to connect to a rogue access point or allow the introduction of malicious devices to networks. Moreover, manufacturers often opt to pre-load default secrets that are easily leaked. Indeed, the largest DDoS attack to date exploited default passwords preloaded to IP cameras, network printers, smart TVs, and other IoT devices to form the Mirai botnet and attack the DNS infrastructure [7].

These limitations have led to new pairing methods that do not rely on pre-shared secrets [8]–[15]. Most utilize out-of-band (OOB) verification via, for instance, a visual or an audio channel. However, not all devices may be equipped with the required sensors for supporting OOB channels. Protocols that achieve pairing in-band via a common wireless interface have been proposed as alternatives [16], [17]. These protocols often rely on special PHY-layer mechanisms, e.g., Manchester coded ON/OFF keying, to thwart certain integrity attacks such as signal overshadowing. In-band methods still remain vulnerable to more advanced signal manipulations such as wireless signal cancellation which was demonstrated

N. Ghose is with the Department of Computer Science and Engineering, University of Nebraska–Lincoln, Lincoln, NE, 68588 USA e-mail: (nghose@unl.edu).

L. Lazos and M. Li are with Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ, 85721 USA e-mail: (llazos,lim@email.arizona.edu).

Manuscript received April 03, 2019; revised February 28, 2020.

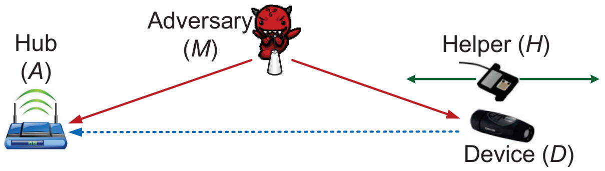


Fig. 1: The basic system model depicting all the entities.

by Pöpper *et al.* [18] under stable channel conditions. Signal manipulation enables a Man-in-the-Middle (MitM) attack over wireless during the trust establishment process. In addition, implementing ON/OFF keyed transmission requires updating the firmware on COTS devices.

In this paper, we study the problem of *secure in-band pairing for devices that do not share any prior secrets.* We focus on the gateway model where a user wants to securely introduce a new device into a network by pairing it with the hub. This scenario covers the majority of IoT devices in home networks, office networks, or even industrial settings. Some examples of devices that fit into this model are smart thermostats, smart door locks and garage door openers, wireless cameras, wearables, wireless medical devices, industrial sensors and actuators, and Internet-enabled appliances.

We develop a secret-free in-band trust establishment primitive, called SFIRE for short, that draws security from hard-to-forge signal propagation laws. The primary operational scenario for SFIRE is shown in Fig. 1. A user executes a pairing session between the legitimate device D and the hub A. During pairing, M launches an active attack over the wireless channel to establish a key with the hub and/or the device. In SFIRE, active attacks are detected by correlating RSS fluctuations measured simultaneously at A and a helper device H, while the pairing device is active. RSS has been explored in several prior works for device authentication [17], [19] however, these methods require firmware and/or hardware alterations and do not protect against advanced adversaries such as MitM attackers. The role of the helper is a relatively advanced device such as a smartphone that has already established trust with the hub.

Our contributions: Our main contributions are four-fold:

- We develop a novel PHY-layer primitive called SFIRE that prevents rogue devices from joining the network. SFIRE is resistant to a MitM attacker, capable of advanced signal manipulations. SFIRE's security relies on a novel "RSS authenticator" that exploits physical signal propagation laws to thwart attackers.
- We use SFIRE to construct a secure in-band pairing protocol based on the Diffie-Hellman (DH) key agreement [20]. Our protocol allows a legitimate device to join a hub and establish a pairwise key. One notable feature of our protocol is that it does not require any hardware/firmware modifications or special transmission modes for the device. This makes SFIRE interoperable with any commercial off-the-shelf (COTS) device that has an RF interface.
- We theoretically explore the security of the RSS authenticator under worst-case scenarios. We analyze the ability of active adversaries with increasing capabilities (antenna directionality, transmission power control, etc.) to defeat SFIRE.
- We carry out extensive experimentation to establish the distinct RSS features that can be used for message integrity verification. We analyze the security of SFIRE under active adversaries with increasing capabilities. We implement SFIRE on COTS equipment and USRPs to validate the offered security. Our experiments attest to the theoretical findings and verify the resistance to active signal manipulations, even if the adversary enjoys favorable channel conditions to the hub and the helper.
- Compared with the conference version [21], we make the following additional contributions. We formalize the steps of all four RSS authentication tests employed by SFIRE. We theoretically analyze the threshold selection for all tests and discuss practical considerations to ensure correctness for legitimate devices and security against active adversaries. We present a security analysis for each of the four RSS authentication tests against all three adversary types considered in the adversary model. The security analysis provides guarantees on the security of SFIRE beyond the validations of the experimental results. We have also updated the fourth test to more accurately reflect the correlation between the user's motion pattern and the RSS pattern recorded by the helper.

2 Related Work

In this section, we review previous works in trust establishment without secrets. Key agreement over a public channel can be achieved using cryptographic methods such as a DH key exchange [20]. However, public message exchanges over the wireless medium are vulnerable to MitM attacks. To thwart MitM attacks, additional message authentication and integrity protection mechanisms are required.

Several secure pairing techniques rely on some out-of-band (OOB) channel to defend against MitM attacks [10], [12], [14], [15], [22]. The OOB communications implement a private channel that cannot be accessed by the adversary. However, OOB channels need non-trivial human support and advanced device interfaces. For instance, if a visual channel is used, a human is required to read a string from one device's screen and input it into another [10], [12], [15], or visually compare multiple strings or LED flashing patterns [14], [23]. Other works require specific hardware such as a Faraday cage to isolate the legitimate communication channel [24], [25]. Alternatively, biometric solutions [26]–[31] create a secure wireless channel through which nodes on the same body can derive a shared secret. However, their applications are limited to wearable devices, require uniform sensing hardware, and are susceptible to remote biometrics sensing attacks [32]. Others have exploited the shared physical context for authentication and key agreement. Examples of common modalities include accelerometer measurements when two devices are shaken together [33]–[35], or light and sound for two devices located in the same room [36], [37]. These require additional hardware and are not interoperable, whereas in many cases the context source has low entropy.

Several efforts have proposed in-band message integrity protection techniques using only the ubiquitous RF modality [8], [9], [11], [13], [38], [39]. A common assumption in the state-of-the-art is that advanced signal manipulations such as signal cancellation are infeasible or occur with bounded success [38], [39]. For instance, the tamper-evident pairing proposed by Gollakota *et al.* [38] and the integrity codes proposed by Čapkun *et al.* [39] rely on the infeasibility of signal cancellation. Moreover, message authentication is achieved by assuming the presence of the legitimate device (a.k.a. authentication through presence). Nevertheless, the infeasibility of signal cancellation does not always hold. Pöpper *et al.* demonstrated an effective relay signal cancellation attack using a pair of directional antennas, which works regardless of the packet content and modulation [18]. Recently, Pan *et al.* [9] showed that it is possible to prevent signal cancellation only if the channel itself has enough randomness. A standard indoor environment may not be sufficient because the devices are static and the channel is usually stable. In this work, we assume such a worst-case scenario. We recently proposed secure pairing and group pairing protocols that detect or prevent signal cancellation attacks [8], [11]. *The key difference of SFIRE with these works is that it provides protection to cancellation attacks without relying on ON/OFF keying modulation*. This makes it universally applicable to COTS devices.

A different set of methods derive trust from *hard-to-forge* PHY-layer features unique to each device/link [16], [19], [40], [41]. Typical properties include (a) *location distinction*, (b) *device identification*, and (c) *device proximity*. Distance bounding [42], [43] was also intended to ensure proximity, but they are not so practical yet (either resort to OOB channels or special hardware). Device identification techniques [44], [45] recognize devices based on their unique PHY layer or hardware features. Unfortunately, these methods need prior training and regular retraining. Zhang *et al.* used RSS measurements from the ambient environment to verify proximity and establish trust [16]. However, this method can only authenticate devices located very close (within 5cm) assuming rapidly changing channels. Lastly, in device proximity methods, the common idea is to exploit the channel reciprocity and its rapid decorrelation with distance. Such techniques typically require advanced hardware. For example, [17], [46] require multiple antennas and [41] needs a wide-band receiver. Furthermore, these techniques do not prevent MitM attacks. In SFIRE, the pairing devices can be located far apart and no assumptions are made on the channel unpredictability.

Table 1 compares different classes of prior works and SFIRE in terms of COTS compatibility, resistance to passive attacks, resistance to active attacks such as message injection and overshadowing, and resistance to advanced active attacks that may additionally involve signal cancellation. The majority of methods are not universally applicable to all IoT devices because they either require advanced interfaces such as keyboards and screens, or they rely on special hardware and out-of-band-channels. Moreover, while all methods are resistant to passive attacks, they are not secure against all active attacks. The majority of methods are vulnerable to MitM attacks where the adversary can mount overshadowing and/or signal cancellation (advanced MitM attacks). We emphasize that the classification is shown in Table 1 is somewhat fuzzy because of all the point details of each individual method and the wide range of adversary models that are considered.

3 Model Assumptions

Table 2 summarizes the most frequently used notations.

3.1 System Model

The following entities are part of the system model.

Hub (A): The hub coordinates the secure pairing process. It is responsible for the authentication of the legitimate device and the coordination with the helper device.

Legitimate Device (D): A COTS device that attempts to pair with A in-band. Pairing results in the establishment of a secret key. D does not share secrets with A before pairing. It is assumed to be under the user's control.

Helper Device (H): The helper is a trusted device such as a smartphone that is under the user's control. It assists A with the pairing process and already shares a secure authenticated channel with A. This authenticated channel can be established using well-analyzed secure authentication methods such as WPA3 [51]. However, H does not share any secrets with D. Using this secure channel, H can apply an authenticated encryption function $\text{AE}(\cdot)$ on any transmission to guarantee the message confidentiality and integrity, and the authenticity of the source. Any such $\text{AE}(\cdot)$ can be utilized with the proposed protocol. For example, if H and A share a public/private key pair, H can encrypt–sign–encrypt (or sign–encrypt–sign), or if they share a common master symmetric key, an encrypt-then-MAC operation can be followed to implement $\text{AE}(\cdot)$, after separate symmetric keys are generated from the master key for the encryption and MAC operations. We refer the reader to [52] for more details on authenticated encryption.

Note that it is reasonable to assume that smartphones, which can be used as helpers, incorporate much stronger security than many computationally-limited IoT devices. The relatively few mobile operating systems that dominate the market integrate well-established security protocols. IoT devices, on the other hand, come from hundreds of different manufacturers and oftentimes implement proprietary, poorly analyzed, and highly-varied authentication methods that are repeatedly proved to be insecure [53]. Moreover, the pairing between H and A is a one-time effort and is not repeated with every device join. We believe that this is an acceptable tradeoff for pairing many COTS devices. Finally, H is assumed to be loosely synchronized to A. Synchronization can be maintained by using transmissions from the device D as a common time reference. The physical layer of wireless protocols such as the 802.xx family of standards already specifies

TABLE 1: State-of-the-art on initial trust-establishment (✓ : met, × : not met, ✓* : partially met).

Method	COTS compatibility	Passive Attacks	MitM Attacks	Advanced MitM Attacks
Password typing [1]	✓*	✓	×	×
Secret preloading [47], QR codes [2]	✓	✓	×	×
PKI [3]	✓*	✓	✓	✓
Out-of-band channels [10], [12], [14], [15], [22]	×	✓	✓	✓
In-band, special modulation [38], [39]	×	✓	✓	×
In-band, special modulation [9], [11], [48]	×	✓	✓	✓
In-band, hard-to-forge property [16], [42], [43], [49], [50]	✓	✓	×	×
In-band, special hardware [19], [40], [41], [45]	×	✓	✓	✓
SFIRE (this work)	✓	✓	✓	✓

TABLE 2: Notation

Notation	Definition
A	Hub
H	Helper device
D	Legitimate device
M	Adversary
m_X	Message transmitted by the entity X
$\mathbf{r}_X$	RSS sequence recorded by the entity X
Γ	Set of the RSS ratios $(\gamma(1), \ldots, \gamma(n))$
$\mathbf{s}_i$	RSS ratio sample set of the i^{th} sweep
Δ_i	RSS ratio range
$T(i)$	Sweeping period for i^{th} sweep
$\mathbf{t}_{acc}$	Set of times when the maximum acceleration is achieved
$\mathbf{t}_{RSS}$	Set of times when the minimum RSS is achieved
P_X	Power transmitted by an adversary to the entity X
G_X	Antenna gain of the entity X
G_{MX}	Transmitting antenna gain of adversary to the entity X
d_{XY}	Distance between the entities X and Y
L_M	Location of the adversary

synchronization mechanisms based on frame preambles that allow the transmitter and the receiver to establish a common time reference. Therefore, no special synchronization protocol is necessary. Note that possible mis-synchronization due to the difference in propagation delay from D to H and A, respectively is negligible.

3.2 Threat Model

Adversary (M)**:** We consider an active adversary that controls one or more adversarial devices. We assume that M cannot get very close to the helper and the legitimate device (e.g., within 1-2 meters) as it will become noticed by the user. M's goal is to either pair with A as a legitimate device or spoof a rogue hub that pairs with D. Because device pairing is initiated by the user, M attempts to realize his goal by launching a MitM attack during a pairing session. The MitM attack is performed by canceling/overshadowing signals at D, A, and H and injecting rogue messages. The adversary is aware of the protocol executed by the legitimate devices but does not have physical access to any of them. Denial-of-service (DoS) attacks such as jamming, are orthogonal to our studies. Moreover, as commonly assumed, M is incapable of physically blocking signals (*e.g.*, by adding a Faraday cage) around D, A, or H. We consider three adversary types with increasing capabilities.

Type 1: A type 1 adversary can perform an overshadowing attack [54] to inject his own message at H and A using omnidirectional transmissions.

Type 2: A type 2 adversary is a type 1 adversary that additionally employs coordinating devices with directional antennas that can target individual devices.

Type 3: A type 3 adversary is a type 2 adversary that additionally applies fine-grained power control to achieve any desired RSS profile.

4 The SFIRE Protocol

SFIRE is an in-band pairing protocol that does not require secret preloading. Authentication is achieved via a novel PHY-layer protection primitive which we call as an "RSS authenticator". We first describe the RSS authenticator and then use it to construct SFIRE.

4.1 Constructing an RSS Authenticator

Referring to the basic scenario of Fig. 1, consider D attempting to pair with A. Let D transmit m_D in plaintext because D and A do not share any prior security association. While m_D is transmitted, H is swept over D in an oscillating motion, with both H and A simultaneously measuring the RSS. H relays the received message, say m'_D, and the associated RSS samples to A via their shared authenticated channel. The hub compares m'_D with its own received message m''_D and also computes the RSS ratio between the samples sent from H and its own samples. The hub uses the RSS ratio fluctuation patterns to verify that m''_D indeed originated from D. Formally, the authentication steps are as follows.

1) **Initialization:** The user presses a button on D or simply switches D on to set it to pairing mode. The user then presses a button or a virtual button on H to initiate the protocol. H sends an authenticated *request-to-communicate* message to A using the AE$(\cdot)$ function, which attests that D is present. The hub starts a timer.
2) **Transmission of** m_D**:** D broadcasts m_D a total of k times in plaintext using back-to-back frames. The repetition of m_D bridges the time scales between message transmission and the user actions, as the latter are several orders of magnitude slower.
3) **Sweeping motions:** While m_D is transmitted, the user sweeps H over D (see Fig. 3(a)). A sweeping motion is defined as a continuous motion passing over D. While in motion, H decodes messages $m'_D(1), \ldots, m'_D(k)$ and samples the RSS at a fixed rate. Let $\mathbf{r}_H = \{r_H(1), \ldots, r_H(n)\}$ by the RSS sequence with $t_H(1)$ denoting the timestamp of the first sample.
4) **Reception of** m_D **at** A**:** The hub decodes $m''_D(1), \ldots, m''_D(k)$. The hub also records $\mathbf{r}_A = \{r_A(1), \ldots, r_A(n)\}$, and the reception time $t_A(1)$ of the first sample.

5) **Authentication at H:** The helper checks if $m'_D(1) \overset{?}{=} \cdots \overset{?}{=} m'_D(k)$. If not, H sends an $AE(\text{ABORT})$ message to A via their shared authenticated channel. If the decoded messages match, H compiles message $m_H = \{\mathbf{r}_H, m'_D(1), t_H(1)\}$ and sends $\text{AE}(m_H)$ to A.
6) **Authentication of m_H:** The hub decrypts m_H and verifies its integrity using $\text{VD}(\cdot)$, which is the corresponding authentication/integrity verification function to $\text{AE}(\cdot)$. If verification fails, A aborts m''_D.
7) **Authentication of m_D:** The hub first verifies that $m''_D(1) \overset{?}{=} \cdots \overset{?}{=} m''_D(k)$. If verification fails, it aborts the pairing process. If successful, the hub verifies $m''_D(1) \overset{?}{=} m'_D(1)$. If verification fails, the hub aborts the pairing process. Otherwise, A proceeds to the RSS authentication. The hub uses the timestamps $t_H(1)$ and $t_A(1)$ to align $\mathbf{r}_H$ with $\mathbf{r}_A$. The hub computes the RSS ratio (Γ) between $\mathbf{r}_H$ and $\mathbf{r}_A$:

$$\Gamma = \{\gamma(1), \gamma(2), \dots, \gamma(n)\},\ \gamma(i) = \frac{r_H(i)}{r_A(i)}.$$

The hub performs a set of RSS authentication tests to verify the authenticity of m''_D. If any of the tests fail, the pairing is aborted and the user has to restart the pairing process. If all tests pass H displays SUCCESS. If a timer at A expires, the pairing process fails.

4.2 SFIRE-Enabled Device Pairing

Parties A and D can securely establish a pairwise key by integrating SFIRE to the DH key-agreement protocol. The SFIRE-enabled DH message exchange is shown in Fig. 2. The hub (or D) uses public parameters $(\mathbb{G}, q, g)$ of the DH scheme, where ($\mathbb{G}$ is a cyclic group of order q and g is a generator of G). Device D computes $z_D = g^{X_D}$, where X_D is chosen from $\mathbb{Z}_q$ uniformly at random. After the initialization step (omitted from Fig. 2), D broadcasts $m_D : ID_D, z_D$ in plaintext to A. The hub verifies this broadcast using SFIRE. In the protocol of Fig. 2, messages protected by SFIRE are denoted by $[\cdot]$. The hub replies with $z_A = g^{X_A}$, where X_A is chosen in $\mathbb{Z}_q$ uniformly at random. Each party independently computes $k_{D,A} = g^{X_D \cdot X_A}$. Immediately following the key-agreement, D and A engage in a key confirmation phase, initiated by D. This can be done by executing a two-way challenge-response protocol [55]. If any of the parties fails verification, it sends an abort message.

4.3 Securing the Downlink Direction

In the DH exchange of Fig. 2, the authenticity of m_A is not verified at D. A MitM adversary acting as a rogue hub may attempt to pair with D by replacing m_A with its own message. However, this will result in an incomplete session at A. In this case, A can notify H of the incomplete pairing that displays a failure message. The user can then re-initiate the pairing protocol.

Message m_A can be explicitly authenticated by increasing human effort. After verifying and accepting m_D, A transmits m_A to H using $\text{AE}(\cdot)$. Then A sends m_A in plaintext to D. Device D records m'_A and the corresponding RSS values as dictated in step 4 of the SFIRE protocol. The helper repeats the transmission of m_A while it is being swiped over D several times. The device decodes m''_A and records the RSS values. To deem m_A authentic, it must hold that $m'_A \overset{?}{=} m''_A$ and the first three RSS authentication tests are passed at D. Note that the helper does not relay any RSS measurements to D, but D directly measures RSS from the respective transmissions of H and A. D does not need special hardware, as RSS measurements are readily available in-band.

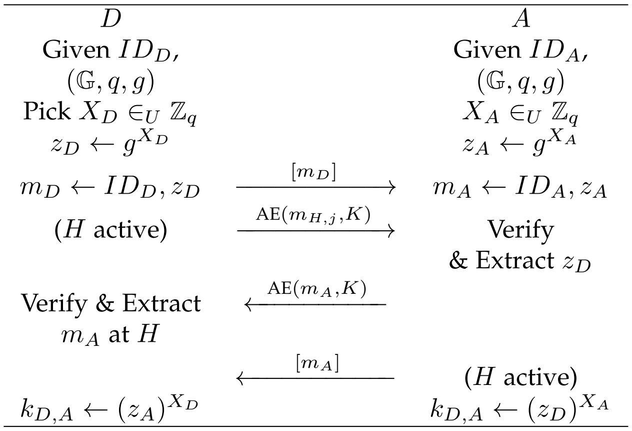


Fig. 2: DH key agreement using SFIRE as a message authenticator.

5 RSS Authentication Tests

We now describe four RSS authentication tests performed by A to verify m_D. Tests are introduced to mitigate adversaries with increasing capabilities. Three of our tests rely on identifying the samples that belong to each sweep performed by the user. The hub organizes the RSS samples Γ in sweeps as follows:

Definition 1. Sweep $\mathbf{s}_i$: *Let Γ be a set of RSS ratio samples ordered according to time. Let $\mathcal{F}$ be the fitted smooth curve on Γ. A sweep $\mathbf{s}_i$ is a set of samples $\{s(i,1), s(i,2), \dots, s(i,w_i)\}$, where $s(i,1)$ and $s(i,w_i)$ are the samples closest to the i^{th} and $i+1^{st}$ local maximum of $\mathcal{F}$, respectively.*

We use a fitted smoothed curve [56] to address the temporal RSS ratio variation. Although the RSS ratio is expected to be proportional to distance (especially in the presence of a strong LoS component), the RSS would vary with nearby movement. The fitted smooth curve allows us to uniquely define local maxima. When a point from Γ is assigned to a sweep $\mathbf{s}_i$, it is removed from Γ such that sweeps form disjoint sets. If the user does not initiate the device movement close to D where the peak ratio is achieved, the first few samples are discarded until a peak is found. One RSS ratio timeline indicating a sample set Γ based on our experiments (see Section 6 for the experimental setup description) for the three motion types of Fig. 3(a) is shown in Fig. 3(b).

5.1 Test 1: Peak RSS Ratio

In the first test, the hub compares the largest sample value in every sweep $\mathbf{s}_i$ with a threshold τ_{peak}. The verification passes if there is at least one sample in every $\mathbf{s}_i$ with a value greater than τ_{peak}. This test exploits the short distance between H

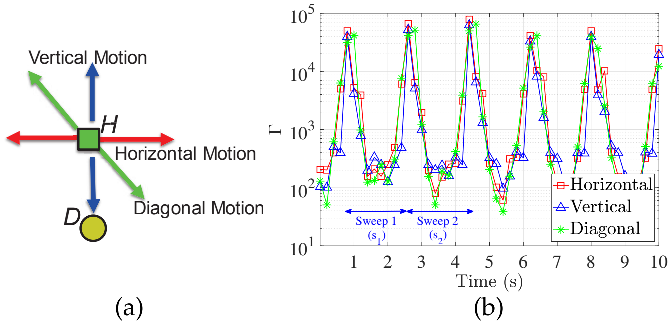


Fig. 3: (a) Various sweeping motions of H over D, (b) RSS ratio fluctuation as a function of time for various motions.

and D during each sweep and the physical signal propagation laws. When the helper is swept over D, he reaches within a few wavelengths from D, whereas A is expected to be at a significantly longer distance. The peak RSS at H becomes several orders of magnitude higher than the RSS at A. The peak RSS ratio from a remote location M relative to D cannot achieve very high values due to geometric constraints (the distance difference between the M-H and M-A paths becomes smaller as M's location becomes more remote unless the three are co-linear). Formally, the steps of Test 1 are as follows:

1) **Compile sweeps:** Compile the sweep set $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_\ell$ from sample set Γ according to Definition 1.
2) **RSS ratio test:** If

$$\max_{\mathbf{s}_i}(s(i,j)) \geq \tau_{peak},\ \forall\, i = 1, 2, \ldots, \ell$$

then D passes Test 1.

Determining τ_{peak}: We now show how to fix τ_{peak} for Test 1. Consider a transmission from D received by H and A simultaneously. Due to the proximity between D and H, the D-to-H channel has a strong LoS component. For this topology, the propagation loss can be modeled after the free-space channel model with a path-loss exponent $\alpha_H = 2$ [57]. The D-to-A channel, on the other hand, could adhere to different models depending on the setting. Given that no single propagation model can capture all scenarios, we consider a general pathloss model where signal attenuation is primarily captured via the attenuation factor α_A that can range from two to five. Under this general model, the RSS ratio γ at A when D transmits is given by:

$$\gamma = \frac{r_H}{r_A} = \frac{G_H}{G_A} \cdot \frac{(d_{DA})^{\alpha_A}}{(d_{DH})^2}, \tag{1}$$

where d_{DX} is the distance between D and X, G_X is the antenna gain of X, and α_A is the pathloss factor for the D-to-A channel. To ease our theoretical analysis, we assume that the path loss exponents remain constant during the brief sweeping process and focus on a single sweep. We simplify our notation by dropping the sweep index and focus on sweep $\mathbf{s}$ with samples $\{s(1), s(2), \ldots, s(w)\}$. The maximum RSS ratio in a sweep $\mathbf{s}$ is given by:

$$\begin{aligned}\max_{\mathbf{s}}\,(s(j)) &= \max_{\mathbf{r}_H}\left(\frac{r_H(j)}{r_A}\right)\\ &= \max_{\mathbf{d}_{DH}}\left(\frac{G_H \cdot (d_{DA})^{\alpha_A}}{G_A \cdot (d_{DH}(j))^2}\right)\\ &= \frac{G_H \cdot (d_{DA})^{\alpha_A}}{G_A \cdot \min\limits_{\mathbf{d}_{DH}}(d_{DH}(j))^2)}\\ &= \frac{G_H \cdot (d_{DA})^{\alpha_A}}{G_A \cdot (d_{DH}^{\min})^2},\end{aligned} \tag{2}$$

where $\mathbf{r}_H$ is the vector of all sampled RSS values at H during sweep $\mathbf{s}$, $\mathbf{d}_{DH}$ is the vector of the the corresponding distances between D and H when D's signal is sampled during the sweep $\mathbf{s}$, and $d_{DH}^{\min}$ is the minimum distance between D and H during the sweep $\mathbf{s}$ (recall that only H is moving during a sweep). When the legitimate device D is transmitting, at least one value in $\mathbf{s}$ must be greater than τ_{peak}. The benign case determines the threshold τ_{peak} that must be used for detecting a Test 1 violation.

$$\tau_{peak} \leq \max_{\mathbf{s}}\,(s(j)) = \frac{G_H \cdot d_{DA}^{\alpha_A}}{G_A \cdot (d_{DH}^{\min})^2}. \tag{3}$$

We observe that τ_{peak} depends on three parameters that vary due to the space geometry, moving objects in the environment, and relative positions of D, H, and A. To set a single τ_{peak} for any conditions, we consider the worst-case scenario. First, we fix $d_{DH}^{\min}$ to some reasonable upper bound based on the expected variability in the user's sweeping motion. Let $\delta_{low} \leq d_{DH}^{\min} \leq \delta_{high}$. Then we select $d_{DH}^{\min} = \delta_{high}$. For the distance between D and A, we assume some minimum separation $d_{DA}^{\min}$. The distance bounds set in the selection of τ_{peak} are adhered to by the user based on the guidance provided by the helper device. For instance, if the user is sweeping H too far away from D, the smartphone implementing the helper can display a message urging the user to swipe H closer to D. Similarly, if D is set to close to A, the user can be prompted to move D further away. Finally, we set the pathloss exponent in the nominator to $\alpha_A = 2$, which corresponds to a LoS channel between D and A. If the channel between D and A is worse ($\alpha_A > 2$), the device will still exceed τ_{peak}, because the nominator will increase compared to τ_{peak} with $\alpha_A = 2$. Using these conservative assumptions we, fix τ_{peak} to

$$\tau_{peak} = \left(\frac{d_{DA}^{\min}}{\delta_{high}}\right)^2.$$

Typical values for the two parameters that we have used in our experiments are $d_{DA}^{\min} = 2$m, and $\delta_{high} = 4$cm. They are over which the RSS ratio test 1 is satisfied by a legitimate device is shown in Fig. 4.

Security Analysis: In an attempt to defeat Test 1, the signal injected by M during sweep $\mathbf{s}_M$ has to achieve a maximum RSS ratio that exceeds τ_{peak}. As discussed earlier, the best case for the adversary is when τ_{peak} is minimized, which is achieved when $\alpha_A = 2$. We analyze the security of Test 1 when

$$\tau_{peak} = {}^{G_H \cdot (d_{DA})^2}\!/\!{}_{G_A \cdot (d_{DH}^{\min})^2}.$$

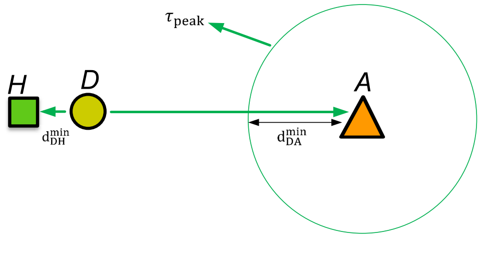


Fig. 4: The threshold for Test 1 is set by fixing the minimum allowed distance between D and A and the upper bound on the minimum distance between D and H when H is swept over D. With a fixed τ_{peak}, D will always pass the Test 1, if placed anywhere outside the circle of radius $d_{DA}^{\min}$, centered at A.

Type 1 adversary: To succeed in pairing with the hub, a Type 1 adversary launches an overshadowing attack [54] by transmitting at the desired power using an omnidirectional antenna. Let M attempt to replace D's message m_D with m_M at A from a location L_M. To succeed in injecting m_M at A, the signal from M must arrive at A with power at least higher than r_A. Given the distance between M and A, the transmit power of M must be at least,

$$P'_M \quad > \quad P_D \cdot \frac{G_D}{G_M} \cdot \left(\frac{d_{MA}}{d_{DA}}\right)^2, \tag{4}$$

where P_D is the transmit power of D and an LoS model is assumed for the channels between M and A to minimize P_M (least power requirement for the adversary). Similarly, to inject m_M at H, the transmit power of M must be at least,

$$P''_M \quad > \quad P_D \cdot \frac{G_D}{G_M} \cdot \left(\frac{d_{MH}}{d_{DH}}\right)^2. \tag{5}$$

From (4) and (5), to inject m_M simultaneously at A and H, the transmit power of M must be at least,

$$P_M \quad > \quad \max(P'_M, P''_M). \tag{6}$$

Let M perform an overshadowing attack during a sweep $\mathbf{s}$ by transmitting at power P_M. The peak RSS ratio between the received signal at H and A is,

$$\begin{aligned}\max_{\mathbf{s}_M}(s_M(j)) &= \max_{\mathbf{r}_H}\left(\frac{r_H(j)}{r_A}\right)\\ &= \frac{G_H}{G_A}\max_{\mathbf{d}_{MH}}\left(\frac{d_{MA}}{d_{MH}(j)}\right)^2\\ &= \frac{G_H}{G_A}\left(\frac{d_{MA}}{\min\limits_{\mathbf{d}_{MH}}(d_{MH}(j))}\right)^2, \end{aligned}\tag{7}$$

where $\mathbf{s}_M$ is the sweep $\mathbf{s}$ affected by M's injection.

We investigate the optimal position of M that maximizes $\max_{\mathbf{s}_M}(s_M(j))$. From (7), $\max_{\mathbf{s}_M}(s_M(j))$ is maximized when d_{MA} is maximum while d_{MD} is minimum. Let us fix the distance d_{MD} to the smallest distance that M can maintain from D without being visually detected by the user. The position of M that maximizes $\max_{\mathbf{s}_M}(s_M(j))$ is achieved when M, H, D, and A are all co-linear in this particular order. This reflected in position L_{M1} (denoted by L^*_M from now) of Fig. 5. At L^*_M the distance to A is maximized for a fixed distance to D, thus maximizing the achievable RSS ratio of M. The security analysis from here on assumes that M is at L^*_M. Fixing the position of M at L^*_M, we investigate the RSS ratio achieved at H under different helper's motions. From Fig. 6,

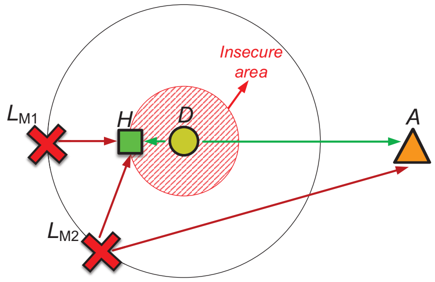


Fig. 5: The adversary placed at L_{M1} (co-linear with H-to-A line) is the optimal position is outside the insecure area with fixed M-to-D distance for maximizing the RSS peak ratio.

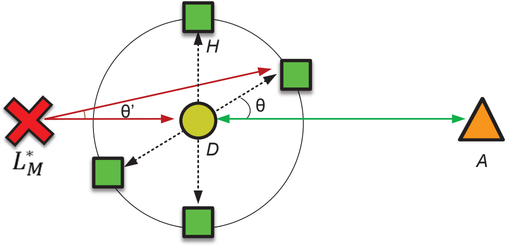


Fig. 6: Various motions for the helper.

$$d_{MA} = d_{MD} + d_{DA},\ d_{MH} = (d_{MD} + d_{DH}\cos\theta)\sec\theta',$$

where θ corresponds to the angle between the D-to-H and D-to-A lines and θ' corresponds to the angle between the M-to-H and M-to-A lines. In addition, M achieves the maximum RSS ratio when H is closest to M. This corresponds to $\theta = 180^\circ,\ \theta' = 0^\circ$. In this case, (7) can be rewritten as,

$$\begin{aligned}\max_{\mathbf{s}_M}(s_M(j)) &= \frac{G_H}{G_A}\max_{\mathbf{d}_{DH}}\left(\frac{d_{MD}+d_{DA}}{(d_{MD}+d_{DH}(j)\cos\theta)\sec\theta'}\right)^2\\ &= \frac{G_H}{G_A}\left(\frac{d_{MD}+d_{DA}}{d_{MD}-\max\limits_{\mathbf{d}_{DH}}(d_{DH}(j))}\right)^2\\ &= \frac{G_H}{G_A}\left(\frac{d_{MD}+d_{DA}}{d_{MD}-d_{DH}^{\max}}\right)^2, \end{aligned}\tag{8}$$

where $\max_{\mathbf{d}_{DH}}(d_{DH}(j)) = d_{DH}^{\max}$ which is the maximum distance between D and H during sweep $\mathbf{s}_M$. Using the value of τ_{peak} from (3) and (8), we evaluate the D-to-M distance outside which Test 1 detects a Type 1 adversary.

Proposition 1. *Test 1 detects any Type 1 adversary which is at distance d_{MD} from D, satisfying $^{(d_{MD}+d_{DA})^{\alpha_A}}/_{(d_{MD}-d_{DH}^{\max})^2} < (^{d_{DA}}/_{d_{DH}^{\min}})^2$. Parameter α_A is the attenuation factor of the M-to-A channel.*

Proof. The proof is provided in Appendix A. □

When $\alpha_A = 2$, there is only one positive solution for d_{MD} in the condition stated in Proposition 1. The adversary has to get closer to H than D to defeat Test 1. If an obstacle exists between M and A, then $\alpha_A > 2$ and a Type 1 adversary can meet τ_{peak} while being further away from D than H. For instance, consider that there is a significant blockage between M and A making $\alpha_A = 4$. By solving for d_{MD}, we find that a Type 1 adversary is successful in two regions

$$d_{MD} < {}^{d_{DA} - 2d_{DA}d_{DH}^{\min} + \sqrt{d_{DA}(d_{DA} - 4d_{DA}d_{DH}^{\min} - 4d_{DH}^{\min}d_{DH}^{\max})}}\!\Big/_{2d_{DH}^{\min}},$$

$$d_{MD} > {}^{2d_{DA}d_{DH}^{\min} - d_{DA} + \sqrt{d_{DA}(d_{DA} - 4d_{DA}d_{DH}^{\min} - 4d_{DH}^{\min}d_{DH}^{\max})}}\!\Big/_{2d_{DH}^{\min}}.$$

The first inequality is similar to the case of $\alpha_A = 2$. The adversary has to get close enough to H and D to defeat Test 1. The second inequality however, reveals the interesting case where if M moves far away from H and A, he will eventually achieve an RSS ratio higher than τ_{peak}. This is intuitive because the signal attenuates faster to A than to H due to the higher path loss exponent for the M-to-A channel. However, moving away from the legitimate devices poses a high power requirement for succeeding in the overshadowing attack. According to (6), the power required for a successful overshadowing attack grows as a function of $(d_{MA})^{\alpha_A}$. For example, for $d_{DA} = 8$m, $d_{DH}^{\min} = 4$cm, $d_{DH}^{\max} = 8$cm, $P_D = 1$mW and $G_D = G_M = 1$, the D-to-M distances $d_{MD} < 4.1$cm, or $d_{MD} > 174$m for $\alpha_A = 3$, and $d_{MD} < 4.12$cm, or $d_{MD} > 230$m for $\alpha_A = 4$. For the longer d_{MD} solutions, the transmission power to successfully launch overshadowing attacks is $P_M = 18.9$KW for $\alpha_A = 3$ and $P_M = 33$KW for $\alpha_A = 4$, which are prohibitive.

Note that defeating Test 1 due to an obstacle between A and M is equivalent to a Type 2 adversary that can perform two-directional transmissions targeting H and A individually. We next show that a Type 2 adversary can defeat Test 1 and then introduce additional RSS tests to detect this type of attack.

Type 2 adversary: A Type 2 adversary can independently control the received power at H and A using directional antennas. To defeat Test 1, an adversary has to achieve $\max_{\mathbf{s}_M}(s_M(j)) \geq \tau_{peak}$ when

$$\max_{\mathbf{s}_M}(s_M(j)) = \max_{\mathbf{r}_H}\left(\frac{r_H(j)}{r_A}\right) \tag{9a}$$

$$= \frac{P_H G_H G_{MH}}{P_A G_A G_{MA}}\left(\frac{d_{MA}}{d_{MD} - d_{DH}^{\max}}\right)^2, \tag{9b}$$

where P_X is the power transmitted from M to X, G_{MX} is the directional antenna gain of M transmitting to X. Without loss of generality in (9b), we assume LoS channels from M to any other device (our goal is to show some scenario for which a Type 2 adversary defeats Test 2). From (9b), an adversary achieves $\max_{\mathbf{s}_M}(s_M(j)) \geq \tau_{peak}$ when,

$$\frac{P_H}{P_A} \geq \tau_{peak}\frac{G_A G_{MA}}{G_H G_{MH}} \cdot \left(\frac{d_{MD} - d_{DH}^{\max}}{d_{MA}}\right)^2. \tag{10}$$

The condition of (10), dictates the adversary's strategy for defeating Test 1. By controlling the powers of directional transmissions P_H and P_A, he can achieve an RSS ratio that exceeds τ_{peak}. One trivial strategy is to choose a low P_A such that (10) is satisfied. However note that P_A must be sufficiently large to carry out an overshadowing attack at A, as given by (5). To detect a Type 2 adversary, we introduce Test 2 that checks the dynamic RSS ratio range.

5.2 Test 2: RSS Ratio Dynamic Range

In the second test, the hub computes the dynamic range of the RSS ratio for each sweep $\mathbf{s}_i$ as:

$$\Delta_i = \frac{\max\limits_{\mathbf{s}_i} s(i,j)}{\min\limits_{\mathbf{s}_i} s(i,j)}.$$

The device passes Test 2 if $\Delta_i \geq \tau_{range}$, for every $\mathbf{s}_i$. This test exploits the higher roll-off rate of the signal power at short distances relative to longer ones. An adversary transmitting a few meters away from H invokes a smaller dynamic range than that of D. Formally, Test 2 has the following steps:

1) **Dynamic range computation:** For a sweep set $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_\ell$, A computes Δ_i as,

$$\Delta_i = \frac{\max\limits_{\mathbf{s}_i} s(i,j)}{\min\limits_{\mathbf{s}_i} s(i,j)},\ \forall\, i = 1, 2, \ldots, \ell.$$

2) **Dynamic range test:** If $\Delta_i \geq \tau_{range},\ \forall\, i = 1, 2, \ldots, \ell$, then D passes Test 2.

Determining τ_{range}: Similar to Test 1 and without loss of generality, we focus on a single sweep $\mathbf{s}$. The RSS ratio range measured when a legitimate device D transmits is:

$$\begin{aligned}\Delta &= \frac{\max\limits_{\mathbf{s}} s(j)}{\min\limits_{\mathbf{s}} s(j)} \\ &= \frac{\max\limits_{\mathbf{r}_H}\left({}^{r_H(j)}\!/_{r_A}\right)}{\min\limits_{\mathbf{r}_H}\left({}^{r_H(j)}\!/_{r_A}\right)} = \frac{\max\limits_{\mathbf{r}_H} r_H(j)}{\min\limits_{\mathbf{r}_H} r_H(j)} \\ &= \left(\frac{\max\limits_{\mathbf{d}_{DH}}(d_{DH}(j))}{\min\limits_{\mathbf{d}_{DH}}(d_{DH}(j))}\right)^2 = \left(\frac{d_{DH}^{\max}}{d_{DH}^{\min}}\right)^2,\end{aligned} \tag{11}$$

where $d_{DH}^{\max}$ and $d_{DH}^{\min}$ are the maximum and minimum distances between D and H during sweep $\mathbf{s}$. In (11), the channel from D-to-A was assumed to be constant during the sweep $\mathbf{s}$ (and hence r_A at the nominator and the denominator is cancelled). Moreover, we assume a LoS channel for the D-to-H channel ($\alpha_H = 2$) due to the proximity between D and H (within a few cm). To fix τ_{range} so that a dynamic adjustment on a per user case is not required, we consider bounds based on the variance in the user's motion and also the guidance that is provided to the user via the helper. Let the range of motion for the user vary according to $\delta_{low} \leq d_{DH}^{\min} \leq \delta_{high}$ and $\lambda_{low} \leq d_{DH}^{\max} \leq \lambda_{high}$. We make the most conservative estimate on the threshold and set it to

$$\tau_{range} = \left(\frac{\lambda_{low}}{\delta_{high}}\right)^2. \tag{12}$$

Typical values for the two parameters that we have used in our experiments are $\lambda_{low} = 50$cm and $\delta_{high} = 4$cm. If the user's sweep range exceeds λ_{low} (i.e., it is longer sweep) then the Δ achieved exceeds τ_{range}. Note that considering a pathloss exponent of $\alpha_H = 2$ for the D-to-H channel yields the most conservative value for τ_{range}. A legitimate device with $\alpha_H > 2$, will pass Test 2 when τ_{range} is set according to $\alpha_H = 2$, as shown in (12). We experimentally evaluate τ_{range}

for various parameters and user motions in Section 6.2. We use the value of τ_{range} in (12) to evaluate the capability of Type 2 and Type 3 adversaries in defeating Test 2.

Security Analysis:

Type 2 adversary: A Type 2 adversary can control the received powers at H and A independently via directional transmissions. To defeat Test 2, the adversary has to achieve $\Delta_M \geq \tau_{range}$. The RSS ratio dynamic range depends on the motion of H given that A is static:

$$\begin{aligned}
\Delta_M &= \frac{\max\limits_{\mathbf{s}_M} s_M(j)}{\min\limits_{\mathbf{s}_M} s_M(j)} \\
&= \frac{\max\limits_{\mathbf{r}_H} \left({}^{r_H(j)}/_{r_A}\right)}{\min\limits_{\mathbf{r}_H} \left({}^{r_H(j)}/_{r_A}\right)} && \text{(13a)} \\
&= \left(\frac{\max\limits_{\mathbf{d}_{DH}}((d_{MD} + d_{DH}(j)\cos\theta)\sec\theta')}{\min\limits_{\mathbf{d}_{DH}}((d_{MD} + d_{DH}(j)\cos\theta)\sec\theta')} \right)^{\alpha_H} && \text{(13b)} \\
&= \left(\frac{d_{MD} + d_{DH}^{\max}}{d_{MD} - d_{DH}^{\max}} \right)^{\alpha_H}, && \text{(13c)}
\end{aligned}$$

where α_H is the attenuation factor of the M-to-H channel which is constant during the sweep. In (13a), the largest and smallest RSS ratio samples over all sweep samples were considered. In (13b), the min and max relative distance between M and H was considered in the general channel model with a pathloss exponent α_H, and in (13c), the maximum Δ_M was derived assumed an optimal orientation for M where $\theta = \theta' = 0^\circ$ (farthest from M) for the numerator and $\theta = 180^\circ,\ \theta' = 0^\circ$ (closest to M) for the denominator.

Although the attenuation factor α_H could vary in different settings, a directional attack targeting both H and A should have LoS to H and A, so that the adversary can aim at the two devices. In the next proposition, we compute the D-to-M distance for a Type 2 adversary when $(\alpha_H = 2)$.

Proposition 2. *A Type 2 adversary is detected by Test 2 when* $d_{MD} > {}^{d_{DH}^{\max}(d_{DH}^{\max} + d_{DH}^{\min})}/_{d_{DH}^{\max} - d_{DH}^{\min}}$.

Proof. The proof is provided in Appendix B. □

For $\alpha_H > 2$ the D-to-M distance decreases. For example, if $\alpha_H = 4$, then

$$d_{MD} \leq (d_{DH}^{\max})^2 - {}^{(d_{DH}^{\min} d_{DH}^{\max} - 2(d_{DH}^{\min})^2 \sqrt{({}^{d_{DH}^{\max}}/_{d_{DH}^{\min}})^3})}/_{(d_{DH}^{\min} + d_{DH}^{\max})}$$

or approximately $d_{MD} < (d_{DH}^{\max})^2$. However, under such a multipath environment, it is difficult to direct the power of a directional transmission to a single target. Some power is inevitably received by A thus decreasing the RSS ratio dynamic range. Moreover, a higher pathloss exponent increases by several orders of magnitude the power necessary to launch a successful overshadowing attack. Even if $d_{MD} < (d_{DH}^{\max})^2$, the D-to-M distance remains relatively large given the short distance between H and D (20 cm in our experiments).

Type 3 adversary: A Type 3 adversary can apply fine-grained power control during a sweep. To defeat Test 2, the adversary has to achieve $\Delta_M \geq \tau_{range}$. To do so, the adversary can manipulate the $\max_{\mathbf{r}_H} \left({}^{r_H(j)}/_{r_A}\right)$ and $\min_{\mathbf{r}_H} \left({}^{r_H(j)}/_{r_A}\right)$ within a sweep $\mathbf{s}_M$ by regulating the power received by A and H, respectively. The maximum RSS ratio in $\mathbf{s}_M$ is given by

$$\begin{aligned}
\max_{\mathbf{s}_M} s_M(j) &= \max_{\mathbf{r}_H} \frac{r_H(j)}{r_A} \\
&= \frac{P_H G_H G_{MH}}{P_A G_A G_{MA}} \left(\frac{d_{MA}}{\min\limits_{\mathbf{d}_{DH}} (d_{MD} + d_{DH}(j)\cos\theta)\sec\theta'} \right)^2 && \text{(14a)} \\
&= \frac{P_H G_H G_{MH}}{P_H G_A G_{MA}} \left(\frac{d_{MA}}{d_{MD} - d_{DH}^{\max}} \right)^2, && \text{(14b)}
\end{aligned}$$

where P_H, P_A are the transmission powers from M to H and from M to A respectively and G_{MH}, G_{MA} are the directional antenna gains from M to H and M to A, respectively. In (14a), we have used an LoS channel to maximize the RSS ratio assuming a fixed channel to A. In (14b), we further set the orientation of M to $\theta = 180^\circ,\ \theta' = 0^\circ$ to minimize the denominator. Using similar arguments, the minimum RSS ratio is achieved when:

$$\begin{aligned}
\min_{\mathbf{s}_M} s_M(j) &= \min_{\mathbf{r}_H} \frac{r_H(j)}{r_A} \\
&= \frac{P'_H G_H G_{MH}}{P'_A G_A G_{MA}} \left(\frac{d_{MA}}{\max\limits_{\mathbf{d}_{DH}} (d_{MD} + d_{DH}(j)\cos\theta)\sec\theta'} \right)^2 && \text{(15a)} \\
&= \frac{P'_H G_H G_{MH}}{P'_A G_A G_{MA}} \left(\frac{d_{MA}}{d_{MD} + d_{DH}^{\max}} \right)^2, && \text{(15b)}
\end{aligned}$$

where P'_H, P'_A are the transmission powers of M to H and A respectively, which can differ from the powers used when the max RSS ratio is achieved. In (15a), we have used $\alpha = 2$ for the respective channels from M to H and M to A without loss of generality, as we only need to demonstrate that under certain conditions, a Type 3 adversary can defeat Test 2. We further set the orientation of M to $\theta = \theta' = 0^\circ$ to maximize the denominator. From (14b) and (15b), the RSS ratio range for sweep $\mathbf{s}_M$ is given by:

$$\Delta_M = \frac{P_H P'_A}{P'_H P_A} \left(\frac{d_{MD} + d_{DH}^{\max}}{d_{MD} - d_{DH}^{\max}} \right)^2 \approx \frac{P_H P'_A}{P'_H P_A}, \tag{16}$$

where for sufficiently large d_{MD} we have approximated $d_{MD} - d_{DH}^{\max} \approx d_{MD} + d_{DH}^{\max} \approx d_{MD}$.

From (12) and (16) we derive the condition under which the adversary defeats Test 2 from any location as

$$\frac{P_H P'_A}{P'_H P_A} \geq \tau_{range}. \tag{17}$$

The condition in (17), dictates the adversary's strategy for defeating Test 2. By controlling the ratios ${}^{P_H}/_{P'_H}$ and ${}^{P'_A}/_{P_A}$, he can achieve a desirable dynamic range that exceeds τ_{range}. The latter is defined by the distance ratio $({}^{d_{DH}^{\max}}/_{d_{DH}^{\min}})^2$. For an effective attack, it is expected that $P_H > P'_H$ whereas $P'_A > P_A$ such that the product of the ratios becomes large. One may trivially assume that choosing very low values for P'_H and P_A is sufficient to exceed τ_{range}. However, the powers selected by M for each directional transmission are lower-bounded by the minimum power required to carry out overshadowing attack at A and H, as dictated by (5) and (4), respectively. To detect a Type 3 adversary, we introduce Test 3 that checks the time period of every sweep.

5.3 Test 3: Sweep Period

In the third test, the hub measures the period $T(i)$ of each sweep $\mathbf{s}_i$ to verify the sweep consistency. The main idea here is that the user takes approximately the same time to complete a sweep. We first define the sweep period $T(i)$.

Definition 2. Sweep period $T(i)$: *The sweep period $T(i)$ of sweep $\mathbf{s}_i$ is defined as the time difference between the occurring times of the first and last sweep sample.*

Sweep Consistency is verified by checking if the ratio ${}^{T(i)}/_{T(j)} \leq \tau_{period}, \ \forall\ i, j; i \neq j$ where the longer period is always placed at the nominator. Formally, Test 3 has the following steps:

1) **Sweep period computation:** For a sweep set $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_\ell$, the sweep period $T(i)$ corresponding to the sweep $\mathbf{s}_i$ is computed according to Definition 2.
2) **Sweep period test:** If

$$ {}^{T(i)}/_{T(j)} \leq \tau_{period}\ \forall\ i, j;\ i \neq j $$

then D passes Test 3.

Figure 7(a) shows the helper's locations where RSS ratio peaks and valleys are observed during a sweep $\mathbf{s}_i$ for two motions when D is transmitting. It is expected that these periods would be fairly consistent given that H passes over D with every motion and the speed of motion is relatively constant. On the other hand, the sweep periods when a transmission originates from a remote location do not present the same consistency. For a subset of helper's motions, the sweep period takes twice as long because the helper does not pass over the remote device. This is demonstrated in Fig. 7(b) where a Type 3 adversary is performing an overshadowing attack at H from a remote location L_M^*. We have divided the area where the helper moves into two areas X and Y. These areas are defined by the intersection of two circles. The circle C_1 is centered at D and has a radius $d_{DH}^{\max}$. The circle C_2 is centered at L_M^* and has a radius d_{MD}. Assuming a straight-line movement, when the helper's motion ends in the boundaries of Y (e.g., horizontal motion), the distance between two helper locations where two consecutive peaks occur is two times the disk diameter (when the helper reaches the disk boundary closest to L_M^*). For a motion that ends in the boundaries of X (e.g., vertical motion), two consecutive peaks occur after a distance of at most one diameter. The third test exploits this irregularity in the sweep periods to detect a remote attack.

Determining τ_{period}: For a legitimate device D, the time to complete sweep $\mathbf{s}_i$ is given by,

$$ T(i) = \frac{2d_{DH}^{\max}(i)}{v}, \tag{18} $$

where v is the average sweep speed and $d_{DH}^{\max}(i)$ is the maximum distance between D and H in the i^{th} sweep. The ratio of the sweep periods ($\mathbf{s}_i$ and $\mathbf{s}_j$) when D is transmitting is given by,

$$ \frac{T(i)}{T(j)} = \left(\frac{2d_{DH}^{\max}(i)}{v}\right)\left(\frac{v}{2d_{DH}^{\max}(j)}\right) = \frac{d_{DH}^{\max}(i)}{d_{DH}^{\max}(j)}, \tag{19} $$

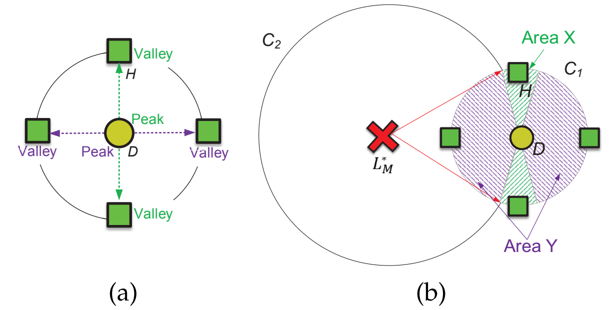


Fig. 7: (a) Peaks and valleys of Γ for various movement of H when D is transmitting, and (b) a sweep in area Y takes at least twice as much as a sweep in area X when M is transmitting from a remote location.

where the average sweep speed is assumed to be relatively the same between sweeps. To pass the Test 3, we can select

$$ \tau_{period} \leq {}^{T(i)}/_{T(j)} = {}^{d_{DH}^{\max}(i)}/_{d_{DH}^{\max}(j)}. \tag{20} $$

The threshold for the sweep period (Test 3) is determined by the expected range of motion for the user. Following the same rationale with Test 2, we fix it to

$$ \tau_{period} = \frac{\lambda_{low}}{\lambda_{high}} $$

where $\lambda_{low} \approx 4$cm and $\lambda_{high} = 50$cm. The user is given instructions to perform consistent sweeps in range and speed so that ${}^{T(i)}/_{T(j)} \approx 1$. However, to allow for a margin of error in the user's motions the threshold τ_{period} can be set to a value between 1 and 2. In Section 6.3, we experimentally show that a selection of $\tau_{period} = 1.4$ provides a sufficient error margin for motion variation.

Security Analysis: We now analyze the ability of a Type 3 adversary in defeating Test 3. Note that a Type 3 adversary incorporates the Type 1 and Type 2 capabilities and therefore a successful test will defend against all three adversaries. To defeat Test 2, a Type 3 adversary applies power control to achieve the desired RSS ratio dynamic range τ_{range}. This is achieved by injecting a maximum power P_H when H is the closest to M and a minimum power P'_H when H is farthest from M thus maximizing the range achieved measured by H. The sweep period recorded by H when M is active depends on the trajectory of H relative to M's location L_M^*. This period is defined as the time between two successive RSS ratio peaks, which are achieved when the M-to-H distance $d_{MH}(i)$ becomes minimum. Analyzing the geometry of Fig. 7(b), minimum of $d_{MH}(i)$ is achieved either on the perimeter of area Y (when H's motion terminates in Y) or inside the area of Y closest to L_M^*. In the first case, the sweep period is the time required to traverse a distance equal to twice the range of H's motion, whereas in the latter case, the sweep period is the time required to traverse a distance at most one time H's range of motion. Using τ_{period} from (20) and the adversary's sweep period, the success of Test 3 is expressed in the following proposition.

Proposition 3. *A Type 3 adversary is always detected by Test 3 if (a) the user performs at least two sweeps $\mathbf{s}_1$ and $\mathbf{s}_2$, (b) sweep $\mathbf{s}_1$ starts and ends in area X, whereas sweep $\mathbf{s}_2$ starts and ends in area Y, and (c) $d_{MD} > \min_i(d_{DH}^{\max}(i))\ \forall\ i = 1, \ldots, \ell$.*

Proof. The proof is provided in Appendix C. □

In the proposition, we perform the evaluation for D-to-M distance as assumed in the other tests. For the secure region, the sweep period achieved by the adversary is ${}^{T_M(i)}/_{T_M(j)} \geq$ 2. However, for outside the secure region $d_{DH}^{\max} \leq d_{MD} < 0$, the sweep period ratio is $2 < {}^{T_M(i)}/_{T_M(j)} < 1$, which can give ambiguous detection as the sweep period of the device varies between 1.4 and 1.

Test 3 relies on the user to perform specific motions, which may not always be performed. To disassociate the security of the RSS authenticator from the sweep motion orientation, we introduce Test 4.

5.4 Test 4: RSS Ratio and Motion Correlation

In the fourth test, the hub correlates the helper's motion with the RSS ratio fluctuation. This test requires acceleration data from H to identify the beginning and end of a sweep, independent of Γ. During the sweeping motion over the legitimate device D, the helper changes direction at its maximum separation from D. This change in direction causes a peak in the acceleration of H and a valley in Γ. Test 4 is designed to defeat a Type 3 adversary because it does not depend solely on the received power at A and H, but on the synchronization of the RSS pattern with the motion pattern of the helper. When correlating the RSS with the motion, a peak in acceleration must coincide with a low in RSS. To achieve this correlation, M must apply fine-grained power control and synchronize the RSS fluctuations with the helper's motion in real-time. This synchronization requires a line-of-site visual path to the helper, along with a precise method for estimating the helper's relative position to D. For this test, we define the minimum RSS ratio instances as:

Definition 3. Minimum RSS ratio instances $\mathbf{t}_{RSS}$: *Let $\mathcal{F}$ be the fitted smooth curve on the RSS ratio sample set Γ. The set of minimum RSS ratio instances $\mathbf{t}_{RSS} = \{t_{RSS}(1), t_{RSS}(2), \ldots, t_{RSS}(\ell)\}$ is a set of times corresponding to the local RSS ratio minima in $\mathcal{F}$.*

In addition, we define the motion change instances as:

Definition 4. Motion change instances $\mathbf{t}_{acc}$: *Let $\mathbf{a}$ be the set of acceleration values of H during the sweeping motion ordered according to time. Let $\mathcal{F}_{\mathbf{a}}$ be the fitted smooth curve on $\mathbf{a}$. The motion change instances $\mathbf{t}_{acc} = \{t_{acc}(1), t_{acc}(2), \ldots, t_{acc}(\ell)\}$ is the set of times corresponding to the local minima in $\mathcal{F}_{\mathbf{a}}$.*

A device passes Test 4 if the root mean square error (RMSE) between $\mathbf{t}_{RSS}$ and $\mathbf{t}_{acc}$ is below a threshold τ_{corr}. This test particularly targets a Type 3 adversary who may defeat Tests 1 and 2 via fine-grained power control or if Test 3 does not include the necessary helper's motions that yield different motion periods. If the adversary cannot synchronize the power fluctuation with the helper's motion, which is difficult to achieve in real-time, the fourth test is violated. Formally, Test 4 has the following steps:

1) **Acceleration data transmission:** The helper sends the minimum RSS ratio and motion change instances $\mathbf{t}_{RSS}$, $\mathbf{t}_{acc}$ to the hub, using AE($\cdot$) (authenticated encryption),
2) **RMSE calculation** The hub A computes the root mean square error (RMSE) between $\mathbf{t}_{RSS}$ and $\mathbf{t}_{acc}$ as

$$RMSE = \sqrt{\frac{\sum_{i=1}^{\ell}(t_{RSS}(i) - t_{acc}(i))^2}{\ell}}$$

3) **RSS ratio–motion correlation test:** If $RMSE \leq \tau_{corr}$, D passes Test 4.

Determining τ_{corr}: Because the helper has an LoS channel to D and the distance between D and A is fixed, the RSS ratio is proportional to the distance between H and D. Therefore, the minimum RSS ratio is achieved at the largest separation between H and D, which is also the point of maximum acceleration as the legitimate device is changing direction. However, variation in RSS and the perturbations introduced by the user motion can lead to a time misalignment between $\mathbf{t}_{acc}$ and $\mathbf{t}_{RSS}$. Let the mean time misalignment between any two samples $t_{acc}(i)$ and $t_{RSS}(i)$ be bounded by $|t_{acc}(i) - t_{RSS}(i)| \leq \epsilon$. The RMSE can then be bounded to

$$RMSE = \sqrt{\frac{\sum_{i=1}^{\ell}(t_{RSS}(i) - t_{acc}(i))^2}{\ell}} \leq \sqrt{\frac{\ell\epsilon^2}{\ell}} = \epsilon. \quad (21)$$

We set τ_{corr} for passing Test 4 to a value slightly larger than ϵ, where ϵ is the expected misalignment error between the RSS valley and the acceleration peak of the helper device. This misalignment does not depend on the user's range of motion and its variance, but it depends on the graceful change of the recorded RSS with the distance from D. Given the very short communication range and the dominance of the LoS channel when the helper is swept on top of D, the correlation threshold remains fairly constant and ϵ takes small values. We have experimentally evaluated the mean time misalignment error ϵ in Section 6.4 and set $\tau_{corr} = 10^{-5}$.

Security Analysis: To defeat Test 4, a Type 3 adversary has to achieve $RMSE \leq \tau_{corr}$, for all the sweeps. This can be done by applying power control and synchronizing the power variation with the motion of H in real-time. That is, M must predict the acceleration peaks (at the edges of the user's motion) and force RSS valleys at those locations. One can consider that this condition can be satisfied without power control if the adversary selects his location such that the M-D line is perpendicular to the helper's motion. However, the helper is moved over D in more than one orientations so there is no one location (other than$D$'s location) that satisfies this criterion. Therefore, the adversary has to apply power control in real-time to match the RSS valleys with the acceleration peaks.

Assuming that the helper's motion cannot be directly observed and analyzed in real-time (via a camera system), the adversary can attempt to synchronize the power control by guessing the average motion period T and the motion start time. Consider the series $\mathbf{t}_{acc}$ recorded by the helper as a time reference. Let the adversary vary the RSS power at H using a period $\mathcal{T}$. The error between any two samples $t_{acc}(i)$ and $t_{RSS}^{(M)}(i)$ can be bounded by $|t_{acc}(i) - t_{RSS}^{(M)}(i)| \leq i\boldsymbol{\Delta} + \mathbf{E}_M$, where $\boldsymbol{\Delta}$ is a random variable (RV) denoting the sweep

TABLE 3: Summary of abilities of various adversaries against various RSS authenticator Tests of SFIRE.

Adversary	Type 1	Type 2	Type 3	Requirement
Test 1	Fail	Pass	Pass	RSS data at H & A
Test 2	Fail	Fail	Pass	RSS data at H & A
Test 3	Fail	Fail	Might Pass	RSS data at H & A
Test 4	Fail	Fail	Fail	RSS data at H & A, accelerometer at H

period estimation error and $\mathbf{E}_M$ is an RV denoting the error due to the unknown motion start time. Note that $\mathbf{\Delta}$ does not affect the RMSE for D because the acceleration peaks and RSS ratio valleys are recorded at the edge of the motion, even if the motion period changes. For an adversary varying the RSS with a fixed period, on the other hand, the error caused by $\mathbf{\Delta}$ accumulates with the number of sweeps. In the next proposition, we explore the number of minimum sweeps ℓ^* required to detect a Type 3 adversary using Test 4.

Proposition 4. *Test 4 detects a Type 3 adversary with probability no smaller than p_0, when the user performs at least*

$$\ell^* \geq \max\left[1, \left\lceil \frac{\sqrt{1 + {}^{48\epsilon^2}/_{\delta^2(1-p_0)^2}} - 3}{4} \right\rceil\right]$$

sweeps, the sweep period estimation error is uniformly distributed in $[-\delta, \delta]$,, and the threshold for passing Test 4 is set to ϵ.

Proof. The proof is included in Appendix D. □

The proposition allows us to set the required number of sweeps such that the adversary fails Test 4 with overwhelming probability, even if he correctly guesses the start time of the motion. Table 3 summarizes the success of each test against each adversary type.

6 Experimental Evaluation

In this section, we experimentally evaluate the security of the RSS authenticator and validate our theoretical analysis. We used two setups in our evaluation. In setup 1, we implemented the RSS authenticator in COTS devices to verify correctness, whereas in setup 2 we used USRP devices to implement the different attacker types and verify soundness. We describe each in detail.

Setup 1–SFIRE with COTS devices: In Setup 1, a Lenovo Y-480 IdeaPad laptop and a Dell XPS desktop, equipped with Intel® Centrino® Wireless N-200 wireless cards were used to implement D and A, respectively. Both cards transmit at 20dBm. The helper H was implemented on a Samsung Galaxy S6 edge+ running Android 7.0 smartphone equipped with an 802.11 a/b/g/n/ac 2.4G+5GHz compatible chipset. The clocks of A and H were synchronized via an Internet server. During the pairing of D with A, we manually performed the three sweeping motions shown in Fig. 3. A sweeping motion was characterized by three parameters: (a) the minimum distance ($d_{DH}^{\min}$) from D to H, (b) the sweep orientation, and (c) the maximum distance $d_{DH}^{\max}$ from D to H. Minimum and maximum separations were adhered to by placing markers on top of D and at the two ends of the motion, although such markers are not necessary for a real protocol execution. During the sweeping motions, We sampled the RSS at a rate of 10 samples/sec at both H and A and repeated each sweeping motion 1,000 times (35 min approximately).

Setup 2–SFIRE on USRPs: Setup 2 was used to implement the attacks carried out by M on the RSS authenticator tests. The roles of D, A, and M were implemented by three NI-USRP 2921 radios operating at 2.4GHz. The helper radio had a smartphone attached to the top to collect accelerometer data for Test 4. The clocks of all the entities were synchronized via the same computer.

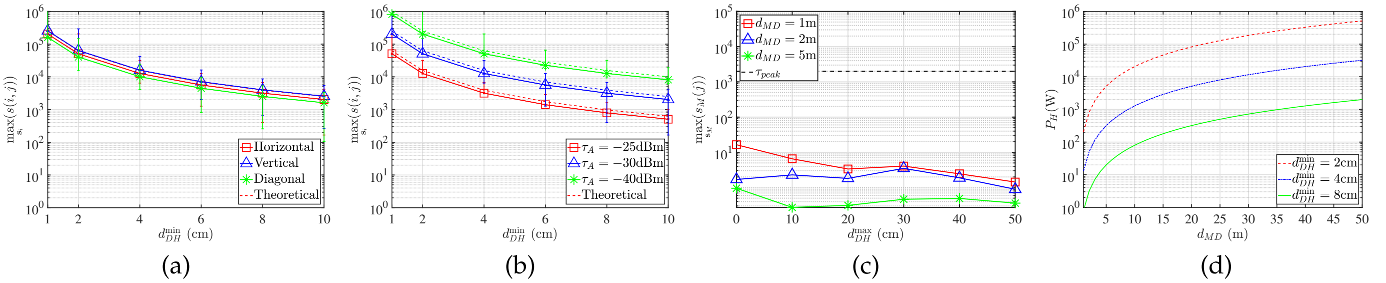
6.1 Test 1: Peak RSS Ratio

To evaluate the peak RSS ratio $\max_{\mathbf{s}_i} s(i,j)$ achieved during a benign scenario, two experiments were performed using Setup 1. In the first experiment, D was placed at 5m from A such that the average RSS at A was -40dBm, and H was swept over D. In Fig. 8(a), we show the peak RSS ratio as a function of $d_{DH}^{\min}$ for all the sweeping motions. We observe that the peak RSS obtains very similar values, irrespective of the motion orientation. These values exceed 10^3 for all minimum separations. The theoretical values computed from eq. (2) are also shown and match the experimental ones.

In the second experiment, we varied the distance d_{DA}, such that the RSS at A also varied. In Fig. 8(b), we show the peak RSS as a function of $d_{DH}^{\min}$. The theoretical values computed from eq. (8) are also shown. As expected, the peak RSS decreases as D gets closer to A (higher RSS at A), but still maintains large values. This is because the RSS is primarily dominated by $d_{DH}^{\min}$. The plots in Fig. 8(a) and 8(b) can be used to select the threshold τ_{peak} for Test 1.

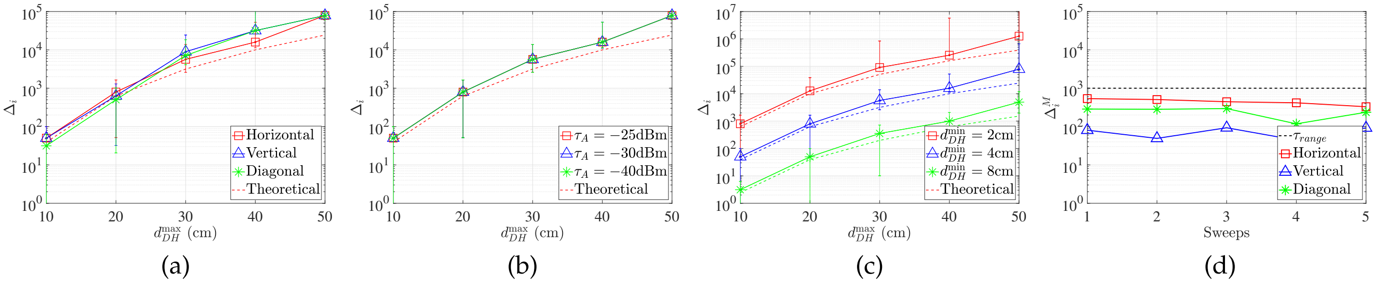
Detecting a Type 1 adversary: To demonstrate the detection of a Type 1 adversary, we performed an experiment using Setup 2. We fixed the D-to-A distance to 5m and chose the corresponding threshold as τ_{peak} = 2,000, based on Fig. 8(b). We measured the peak RSS ratio when the adversary M was placed at d_{MD} = 1m, 2m, and 5m from D and H, respectively. The adversary was set to transmit at 1W. Figure 8(c) shows the peak RSS ratio achieved by the Type 1 adversary for different values of the maximum distance between D and H for the horizontal motion. We observe that the peak RSS ratio achieved by the transmission of M is significantly lower than the threshold τ_{peak}. This is because a Type 1 adversary transmitted using an omnidirectional antenna affecting the received power both at H and A thus maintaining a relatively low ratio.

Defeating Test 1 with a Type 2 adversary: We further evaluated the transmit power required by a Type 2 adversary to defeat Test 1 under an idealized scenario. We set the threshold for Test 1 to τ_{peak} = 2,000, the antenna gains to one, and the signal strength required to perform an overshadowing attack at A to -50dBm. The transmissions to A and H were assumed to be individually controlled via directional antennas. In Fig. 8(d), we show the required transmit power to defeat Test 1 as a function of the device-to-adversary distance (d_{MD} in meters), as calculated by (10). We observe that the required transmit power that satisfies the peak RSS ratio and achieves an overshadowing attack becomes prohibitive with an increase of d_{MD}. At 10m from



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

Fig. 8: (a) Peak RSS ratio as a function of the minimum D-to-H distances in each sweep for various sweeping motions, (b) peak RSS ratio as a function of the minimum D-to-H distances in each sweep for various RSS at A, (c) peak RSS ratio as a function of the maximum D-to-H distances in each sweep for various d_{MD} for a Type 1 adversary, and (d) maximum transmit power of a Type 2 adversary to achieve τ_{peak} as a function of d_{MD} for various $d_{DH}^{\min}$.



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

Fig. 9: (a) RSS ratio range of $\mathbf{s}_i$ as a function of the maximum D-to-H distances in each sweep for various sweeping motions, (b) RSS ratio range of $\mathbf{s}_i$ as a function of the maximum D-to-H distances in each sweep for various RSS at A, (c) RSS ratio range of $\mathbf{s}_i$ as a function of the maximum D-to-H distances in each sweep for various $d_{DH}^{\min}$, and (d) RSS ratio range as a function of the sweeps for a Type 2 adversary for $d_{MD} = 2$m with τ_{range} selected for $d_{DH}^{\max} = 50$cm and $P_A = 0.1$W.

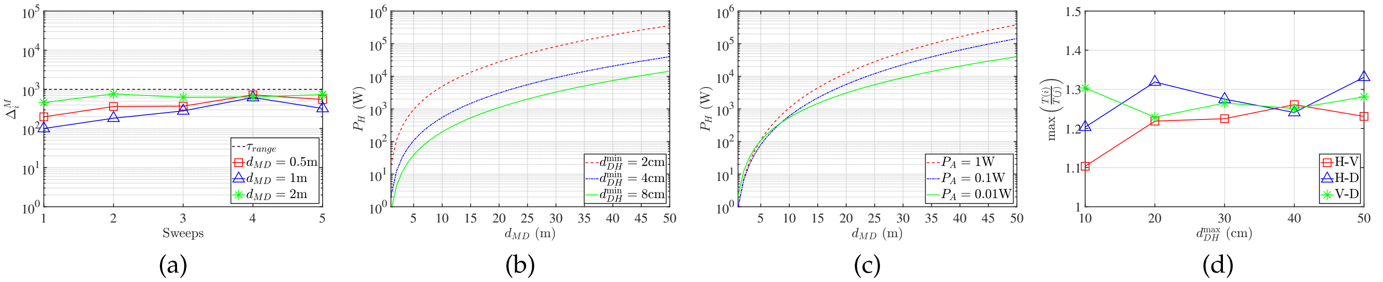
D, the adversary must transmit at hundreds of watts to the helper for achieving the required ratio due to the required power needed to achieve an overshadowing attack at A.

6.2 Test 2: RSS Ratio Dynamic Range

We performed three experiments to evaluate the dynamic range Δ_i for all sweeping motions using Setup 1. In the first experiment, we placed A at 10m from D so that the average received RSS at A was -40dBm, Moreover, we fixed $d_{DH}^{\min} = 4$cm and performed horizontal, vertical, and diagonal sweeping motions. For each motion, we recorded the dynamic RSS ratio range. Figure 9(a) shows the RSS ratio range as a function of the maximum separation between D and H. The theoretical values computed using eq. (11) are also shown. In the second experiment, we varied the distance between A and D and repeated the measurements. Figure 9(b) shows the RSS ratio range for the different RSS thresholds at A. For both experiments, it can be observed that the range does not vary significantly with the motion orientation. Moreover, the theoretical values match to track the measured values. The recorded differences are due to the free-space model considered in the theoretical calculation, however, they can serve as a lower bound on the expected Δ. Longer sweeps significantly increase the RSS ratio range. Figure 9(c) shows the results of our third experiment where we varied $d_{DH}^{\min}$ for a horizontal sweeping motion. As expected, the maximum range is achieved when H is swept at 2cm from D and the range of H's motion is maximized (50cm). Based on these results, we set $\tau_{range} = 10^3$ which captures any motion over 30cm with $d_{DH}^{\min} = 4$cm.

Detecting a Type 2 adversary: We now evaluate the ability of a Type 2 adversary in defeating Test 2 using Setup 2. We equipped two USRP devices with directional antennas pointing to H and A, respectively. The antenna pointed at A transmitted at $P_A = 0.01$W, the minimum required value to successfully perform an overshadowing attack. The antenna pointed at H transmitted at $P_H = 1$W to achieve an overshadow attack, but also achieve the maximum RSS ratio threshold required in Test 1. Figure 9(d) shows Δ_i^M achieved by the adversary for various motions when the distance between H and M is varied. The adversary's RSS ratio range is below τ_{range} for most motions and reaches the required range only for one horizontal sweep. The adversary failed Test 2, as it needed to pass the test for all sweeps. The horizontal motion exhibited the highest RSS ratio range because we positioned M at the optimal position L_M^* shown in Fig. 5. However, other motions failed to achieve a similar range. We further repeated our experiments for multiple sweeps and different distances between M and D. The results in Fig. 10(a) show that even if M is very close to D (within 0.5m), it cannot achieve the required dynamic range consistently, without employing power control.

Defeating Test 2 with a Type 3 adversary: We further calculated the required transmit powers of M to defeat Test 2 according to the conditions of (17). A Type 3 adversary varies the transmission power to the helper between P_H' and P_H, and to the hub between P_A and P_A'. The strategy of M is to maximize the ratios ${P_A'}/{P_A}$ and ${P_H}/{P_H'}$. The minimum transmission powers P_H' and P_A are governed by (6), which expresses the power required for overshadowing. We set these to $P_H' = 0.1$W and $P_A = 0.1$W. According to (16),



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

Fig. 10: (a) RSS ratio range as a function of the sweeps for Type 2 adversary with τ_{range} selected for $d_{DH}^{\max} = 50$cm and $P_A = 0.1$W, (b) maximum transmit power of a Type 3 adversary to H as a function of d_{MD} when transmitting with $P'_A = 10$W for achieving τ_{range} for various $d_{DH}^{\min}$, (c) maximum transmit power of a Type 3 adversary to H as a function of d_{MD} when transmitting with $P'_A = 10$W for achieving τ_{range} for various τ_A, and (d) max $(T(i)/T(j))$ as a function of the maximum D-to-H distances for each motion for various RSS at A.

P'_A and P_H have the same effect on Δ_M. To see the trend of P_H, we fix the value of $P'_A = 10$W. In Fig. 10(b), we plot the maximum transmit power to H as a function of the D-to-M distances for different minimum D-to-H distances 2cm, 4cm, and 8cm.

We also varied the minimum transmit power to A to values $P_A = 1$W, $P_A = 0.1$W, and $P_A = 0.01$W, while keeping $P'_H = 0.1$W constant (varying P'_H has the same effect on Δ_M). Figure 10(c) shows the required maximum transmit power for a Type 3 adversary as a function of d_{MD} for defeating Test 2. From Fig. 10(b) and Fig. 10(c) we observe that the required transmit power becomes quickly prohibitive as the adversary moves further away. At 10m from D, the adversary must transmit at hundreds of watts to achieve the required dynamic range. It should be noted here, if the adversary fixes P_H, the variation of P'_A follows similar patterns. The adversary may be able to achieve the required peak ratio if he employs highly directional antennas and manages to be in close distance to H during the pairing.

6.3 Test 3: Sweep Period

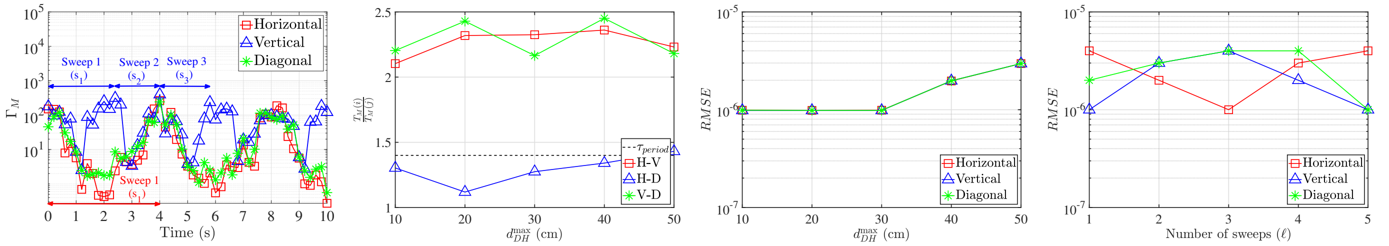
For Test 3, we performed two experiments using Setup 1 to evaluate the consistency of the sweeping periods across different motion orientations. In the first experiment, we moved the helper on top of the device D and measured the ratio of the sweep periods between pairs of motions; horizontal-vertical (H-V), horizontal-diagonal (H-D) and vertical-diagonal (V-D). Figure 10(d) shows the period ratio for all the motion combinations as a function of $d_{DH}^{\max}$. We observe that the sweep period is relatively constant with period ratios not exceeding 1.32. Moreover, the periods did not vary much with the motion range. Based on these experiments, we set $\tau_{period} = 1.4$.

Detecting a Type 3 adversary: Since a Type 3 adversary is the only model that can defeats Tests 1 and 2, we evaluated if a Type 3 adversary can defeat Test 3. We considered that M is aware of the average period of H's sweeps and regulated its power control accordingly. We employed Setup 2 to allow for power control and antenna directionality, fixed the distance between $d_{MD} = 1$m, $d_{DH}^{\max} = 50$cm, and $d_{DH}^{\min} = 4$cm. M oscillated its transmitting power between 0.01W and 1W to meet both the τ_{peak} and τ_{range} thresholds and defeat Tests 1 and 2. For the experiments, M attempted to synchronize with D's transmission for the vertical motion, with an average period of 2sec, corresponding to an average hand moving speed of 0.5m/s. The user randomized the motion direction. In Fig. 11(a), we show the RSS ratio fluctuation achieved by the power-controlled transmission of M over time. It can be observed that the sweep period of the vertical sweep is around 2 sec, but the periods of other sweeps are twice as long because only one peak occurs on every sweep (when H is closest to M). Figure 11(b) shows the sweep period ratios for different $d_{DH}^{\max}$. When the vertical motion is compared to other motions, the sweep period ratio is over 2. The adversary can pass this test only when the user restricts the helper's motion to one orientation.

6.4 Test 4: RSS Ratio and Motion Correlation

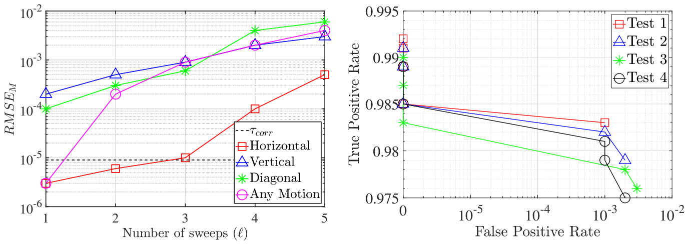
To remedy a possible failure of Test 3 due to using just one orientation, we further considered the correlation of the accelerometer data with the RSS ratio data as dictated by Test 4. We used Setup 1 to evaluate the root mean square error ($RMSE$) between the set of time instances $\mathbf{t}_{RSS}$ when the RSS ratio minimum is measured and the time instances $\mathbf{t}_{acc}$ when an acceleration peak is achieved. The acceleration values were recorded by accessing the accelerometer data on the mobile phone (helper). Figure 11(c) shows the average $RMSE$ as a function of the maximum D-to-H distance for various sweeping motions. We observe that the RMSE is quite small indicating the RSS ratio valleys and acceleration peaks remain synchronized throughout the different motions. Figure 11(d) shows the $RMSE$ as a function of number of sweeps (ℓ) for various sweeping motions. We observe no particular correlation between the number of sweeps and the $RMSE$. This is consistent with our intuition for a benign scenario where the $RMSE$ is not cumulative with the number of sweeps, but it rather varies in a random fashion. Based on the results of this experiment, we set $\tau_{corr} = 10^{-5}$.

Detecting a Type 3 adversary: We considered a Type 3 adversary attempting to defeat Test 4 by employing Setup 2. In this experiment, the adversary applied power control and attempted to synchronize to the user motion. We evaluated the best-case scenario for the adversary where he had knowledge of motion start time ($\mathbf{E}_M = 0$) and of the average sweep period, which was $T = 2$sec. The synchronization of the adversary's power control with the helper's motion was performed offline by offsetting the first RSS ratio minima to match the first acceleration maxima. Figure 12(a) shows



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

Fig. 11: (a) RSS ratio fluctuation for a Type 2 adversary as a function of the time at 2m from D, (b) $T_M(i)/T_M(j)$ as a function of the maximum D-to-H distances for a Type 3 adversary mimicking transmit power for the vertical sweeping motion of H, (c) $RMSE$ as a function of the maximum D-to-H distances for various sweeping motions, and (d) $RMSE$ as a function of the number of sweeps (ℓ) for various sweeping motions.



(a) (b)

Fig. 12: (a) $RMSE_M$ as a function of the number of sweeps for a Type 3 adversary, mimicking a horizontal sweeping motion, and (b) ROC curve for the performance of verification tests of SFIRE against various types of adversaries.

the achieved $RMSE_M$ for various sweeping motions of H as a function of the number of sweeps when the adversary mimicked the horizontal sweep motion. We observe that the error induced in the sweep period when the user moves M accumulates with ℓ leading to the eventual failure of Test 4. Moreover, when the motion mimicked by the adversary is different than that performed by H, even one sweep is sufficient to lead to high RMSE values.

7 Evaluation of SFIRE-Enabled Device Pairing

We now analyze the security of the device pairing protocol proposed in Section 4.2. We first examine if the adversary can pair a rogue device with A. We then examine if D can be deceived to pair with a rogue hub.

7.1 Pairing a Rogue Device with A

The pairing of a rogue device D' with A can occur under two different scenarios:

Pairing in the absence of a legitimate device: The pairing protocol described in Section 4.2 is initiated with the press of a button on H and D. The button pressing sends a pairing initialization message to the A which is authenticated using the secure AE$(\cdot)$ function. Without access to the helper, the adversary cannot initiate the pairing from a remote location.

Hijacking a legitimate pairing session: Since M cannot initiate the pairing process with the A, he can only attempt to pair a rogue device with the A by hijacking a pairing session involving a legitimate device (D). To establish a secret key with the A, the adversary must modify the DH public number z_D of D into its own DH public number z'_D, where z_D is contained in the first message m_D sent from D to the A (similar to a typical MitM attack against a DH key exchange). However, m_D is protected by our integrity verification primitive of SFIRE.

As discussed in this Section earlier, the adversaries with different capabilities are not able to pass the RSS authentication to forge m_D. Therefore, the adversary will be unable to pair D' with the legitimate A.

7.2 Pairing D with a Rogue Base Station

We now examine if M acting as a rogue A can pair with D. To do so, M can perform a similar MitM attack as in the uplink direction, by replacing the A's DH public parameter z_A with its own z'_A. The m_A is protected by downlink SFIRE primitive $[\cdot]_{Dw}$ as discussed in Section 4.3. In the downlink SFIRE, D computes Γ, during the transmission of m_A from RSS values of frames received from A and H. D performs the RSS authentication that prevents pairing with A'.

7.3 ROC Curves

We evaluated the receiver operating characteristic (ROC) curve for the SFIRE-enabled pairing protocol. We evaluated the performance of each adversary types against the four tests on Setup 2. The distance between M and D was set to 1m. The value for τ_{peak} was chosen as 2,000 for $P_A = 0.1$W, $\tau_{range} = 10^3$ for the same transmit power to A, $\tau_{period} = 1.4$ and $\tau_{corr} = 9 \times 10^{-6}$. The sweeping motions for each experiment were repeated $1,000$ times. The D to A and D to M distance were fixed to 1m and 0.5m respectively, with M positioned at L^*_M as shown in Fig. 5.

Figure 12(b) shows the ROC curve for all the tests in the RSS authenticator. Test 1 is evaluated against a Type 1 adversary, Test 2 is evaluated against a Type 2 adversary, and Tests 3 and 4 are evaluated against a Type 3 adversary. The various points of the ROC curve are obtained for a different number of sweeps to complete the protocol. The rightmost point is obtained for one sweep, whereas the leftmost point is obtained for five sweeps. We observe that as the number of sweeps increases, the TPR increases whereas the FPR decreases indicating that the SFIRE protocols achieve both correctness and security.

8 Conclusions

We addressed the problem of secure device pairing without prior associations. We proposed SFIRE, a secret-free protocol that achieves the secure pairing of COTS wireless devices with a hub. Compared to the state-of-the-art, SFIRE does not require any out-of-band channels, special hardware, or firmware modification, thus it is applicable to any COTS device. We showed that SFIRE is resistant to the most advanced active signal manipulations that include recently demonstrated signal nullification at an intended receiver. These security properties are achieved in-band with the assistance of a helper device and by using the RSS fluctuation patterns to build a robust RSS authenticator. We performed extensive theoretical analysis and attested the finding with experiments using COTS devices and USRP radios and validated the security and performance of the proposed protocol.

Acknowledgments

We thank the anonymous reviewers for their insightful comments. This research was supported in part by the NSF under grants CNS-1409172, CNS-1731164, CNS-1410000 and ARO grant W911NF1910050. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the NSF and ARO.

References

[1] J. Zhang and V. Varadharajan, “Wireless sensor network key management survey and taxonomy,” *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 63–75, 2010.

[2] K.-C. Liao and W.-H. Lee, “A novel user authentication scheme based on qr-code,” *Journal of networks*, vol. 5, no. 8, p. 937, 2010.

[3] J. Y. Hwang, S. Eom, K.-Y. Chang, P. J. Lee, and D. Nyang, “Anonymity-based authenticated key agreement with full binding property,” *IEEE Journal of Communications and Networks*, vol. 18, no. 2, pp. 190–200, 2016.

[4] M. Sethi, A. Peltonen, and T. Aura, “Misbinding attacks on secure device pairing and bootstrapping,” in *Proc. of the 2019 ACM Asia Conference on Computer and Communications Security*, 2019, pp. 453–464.

[5] D. M. Junior, L. Melo, H. Lu, M. d’Amorim, and A. Prakash, “A study of vulnerability analysis of popular smart devices through their companion apps,” in *Proc. of 2019 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2019, pp. 181–186.

[6] K. W. Ching and M. M. Singh, “Wearable technology devices security and privacy vulnerability analysis,” *International Journal of Network Security & Its Applications*, vol. 8, no. 3, pp. 19–30, 2016.

[7] The Guardian. (2016) DDoS attack that disrupted internet was largest of its kind in history, experts say. [Online]. Available: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[8] N. Ghose, L. Lazos, and M. Li, “Secure device bootstrapping without secrets resistant to signal manipulation attacks,” in *Proc of 39th IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 819–835.

[9] Y. Pan, Y. Hou, M. Li, R. M. Gerdes, K. Zeng, M. A. Towfiq, and B. A. Cetiner, “Message integrity protection over wireless channel: Countering signal cancellation via channel randomization,” *IEEE Transactions on Dependable and Secure Computing*, 2017.

[10] X. Liang, T. Yun, R. Peterson, and D. Kotz, “Lighttouch: Securely connecting wearables to ambient displays with user intent,” in *Proc. of INFOCOM*. IEEE, 2017, pp. 1–9.

[11] N. Ghose, L. Lazos, and M. Li, “Help: Helper-enabled in-band device pairing resistant against signal cancellation,” in *Proc. of 26th USENIX Security Symposium*, 2017, pp. 433–450.

[12] W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila, and Y. Cheng, “Secure key establishment for device-to-device communications,” in *Proc. of 2014 IEEE Global Communications Conference*. IEEE, 2014, pp. 336–340.

[13] Y. Hou, M. Li, and J. D. Guttman, “Chorus: Scalable in-band trust establishment for multiple constrained devices over the insecure wireless channel,” in *Proc. of the WiSec Conference*, 2013, pp. 167–178.

[14] T. Perkovic, M. Cagalj, T. Mastelic, N. Saxena, and D. Begusic, “Secure initialization of multiple constrained wireless devices for an unaided user,” *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 337–351, 2012.

[15] D. Nyang, A. Mohaisen, and J. Kang, “Keylogging-resistant visual authentication protocols,” *IEEE Transactions on Mobile Computing*, vol. 13, no. 11, pp. 2566–2579, 2014.

[16] J. Zhang, Z. Wang, Z. Yang, and Q. Zhang, “Proximity based iot device authentication,” in *Proc. of INFOCOM*, 2017.

[17] T. J. Pierson, X. Liang, R. Peterson, and D. Kotz, “Wanda: Securely introducing mobile devices,” in *Proc. of INFOCOM*, 2016, pp. 1–9.

[18] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun, “Investigation of signal and message manipulations on the wireless channel,” in *Proc. of 16th ESORICS*, 2011, pp. 40–59.

[19] L. Cai, K. Zeng, H. Chen, and P. Mohapatra, “Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas,” in *Proc. of Network and Distributed System Security Symposium*, 2011.

[20] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[21] N. Ghose, L. Lazos, and M. Li, “SFIRE: Secret-free in-band trust establishment for COTS wireless devices,” in *Proc. of 37th IEEE International Conference on Computer Communication (INFOCOM)*, 2018, pp. 1529–1537.

[22] B. Berg, T. Kaczmarek, A. Kobsa, and G. Tsudik, “Lights, camera, action! exploring effects of visual distractions on completion of security tasks,” in *Proc. of International Conference on Applied Cryptography and Network Security*. Springer, 2017, pp. 124–144.

[23] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, “Secure ad hoc trust initialization and key management in wireless body area networks,” *ACM Trans. Sen. Netw.*, vol. 9, no. 2, pp. 18:1–18:35, Apr. 2013.

[24] C. Kuo, M. Luk, R. Negi, and A. Perrig, “Message-in-a-bottle: user-friendly and secure key deployment for sensor nodes,” in *Proc. of SenSys’07*, 2007, pp. 233–246.

[25] Y. W. Law, G. Moniava, Z. Gong, P. Hartel, and M. Palaniswami, “Kalwen: A new practical and interoperable key management scheme for body sensor networks,” *Security and communication networks*, vol. 4, no. 11, pp. 1309–1329, 2011.

[26] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, “Anonymous authentication for wireless body area networks with provable security,” *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, 2017.

[27] G. Zheng, G. Fang, R. Shankaran, M. A. Orgun, J. Zhou, L. Qiao, and K. Saleem, “Multiple ecg fiducial points-based random binary sequence generation for securing wireless body area networks,” *IEEE Journal of biomedical and health informatics*, vol. 21, no. 3, pp. 655–663, 2017.

[28] T. Belkhouja, X. Du, A. Mohamed, A. K. Al-Ali, and M. Guizani, “New plain-text authentication secure scheme for implantable medical devices with remote control,” in *Proc. of IEEE Global Communications Conference*. IEEE, 2017, pp. 1–5.

[29] W. Xu, C. Javali, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, “Gait-key: A gait-based shared secret key generation protocol for wearable devices,” *ACM Transactions on Sensor Networks (TOSN)*, vol. 13, no. 1, p. 6, 2017.

[30] C. Fu, X. Du, L. Wu, and X. Fu, “Poks based low energy authentication scheme for implantable medical devices,” *arXiv preprint arXiv:1803.09890*, 2018.

[31] N. Karimian, P. A. Wortman, and F. Tehranipoor, “Evolving authentication design considerations for the internet of biometric things (iobt),” in *Proc. of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*. ACM, 2016, p. 10.

[32] X. Hei and X. Du, “Biometric-based two-level secure access control for implantable medical devices during emergencies,” in *Proc. of 30th IEEE International Conference on Computer Communications*, Shanghai, P.R.China, April 2011, pp. 346 – 350.

[33] C. T. Zenger, J. Zimmer, M. Pietersz, J.-F. Posielek, and C. Paar, “Exploiting the physical environment for securing the internet of things,” in *Proc. of the 2015 New Security Paradigms Workshop*. ACM, 2015, pp. 44–58.

[34] M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani, “Context-based zero-interaction pairing and key evolution for advanced personal devices,” in *Proc. of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 880–891.

[35] E. Hayashi, S. Das, S. Amini, J. Hong, and I. Oakley, “CASA: context-aware scalable authentication,” in *Proc. of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013, p. 3.

[36] M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani, "Context-based zero-interaction pairing and key evolution for advanced personal devices," in *Proc. of the CCS Conference*, 2014, pp. 880–891.

[37] D. Schürmann and S. Sigg, "Secure communication based on ambient audio," *IEEE Transactions on mobile computing*, vol. 12, no. 2, pp. 358–370, 2013.

[38] S. Gollakota, N. Ahmed, N. Zeldovich, and D. Katabi, "Secure inband wireless pairing," in *Proc. of USENIX security symposium*, 2011, pp. 1–16.

[39] S. Capkun, M. Cagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava, "Integrity codes: Message integrity protection and authentication over insecure channels," *IEEE TDSC*, vol. 5, no. 4, pp. 208–223, 2008.

[40] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: cooperative proximity-based authentication," in *Proc. of MobiSys*, 2010, pp. 331–344.

[41] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: proximity-based secure pairing using ambient wireless signals," in *Proc. of MobiSys*, 2011, pp. 211–224.

[42] J. Brody, S. Dziembowski, S. Faust, and K. Pietrzak, "Position-based cryptography and multiparty communication complexity," in *Theory of Cryptography Conference*. Springer, 2017, pp. 56–81.

[43] E. Pagnin, A. Yang, Q. Hu, G. Hancke, and A. Mitrokotsa, "HB+ DB: Distance bounding meets human based authentication," *Future Generation Computer Systems*, vol. 80, pp. 627–639, 2018.

[44] T. D. Nguyen, S. Marchal, M. Miettinen, M. H. Dang, N. Asokan, and A.-R. Sadeghi, "DÏot: A crowdsourced self-learning approach for detecting compromised iot devices," *arXiv preprint arXiv:1804.07474*, 2018.

[45] P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singelée, and B. Preneel, "Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning," in *Proc. of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2017.

[46] W. Cheng, K. Tan, V. Omwando, J. Zhu, and P. Mohapatra, "Rss-ratio for enhancing performance of rss-based applications," in *Proc. of 2013 INFOCOM*. IEEE, 2013, pp. 3075–3083.

[47] Y.-H. Lin, A. Studer, Y.-H. Chen, H.-C. Hsiao, L.-H. Kuo, J. M. McCune, K.-H. Wang, M. Krohn, A. Perrig, B.-Y. Yang *et al.*, "Spate: small-group pki-less authenticated trust establishment," *IEEE Transactions on Mobile Computing*, vol. 9, no. 12, pp. 1666–1681, 2010.

[48] Y. Hou, M. Li, R. Chauhan, R. M. Gerdes, and K. Zeng, "Message integrity protection over wireless channel by countering signal cancellation: Theory and practice," in *Proc. of the AsiaCCS*, 2015, pp. 261–272.

[49] X. Li, F. Yan, F. Zuo, Q. Zeng, and L. Luo, "Touch well before use: Intuitive and secure authentication for iot devices," in *Proc. of The 25th Annual International Conference on Mobile Computing and Networking*, 2019, pp. 1–17.

[50] T. J. Pierson, T. Peters, R. Peterson, and D. Kotz, "Proximity detection with single-antenna iot devices," in *Proc. of The 25th Annual International Conference on Mobile Computing and Networking*, 2019, pp. 1–15.

[51] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the dragonfly handshake of wpa3 and eap-pwd," in *Proc. of the 2020 IEEE Symposium on Security and Privacy- (S&P 2020)*. IEEE, 2020.

[52] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," in *Proc. of CRYPTO*. Springer, 2000, pp. 531–545.

[53] Symantec, "Insecurity in the internet of things," https://www.symantec.com/content/en/us/enterprise/iot/b-insecurity-in-the-internet-of-things_21349619.pdf, 2019.

[54] M. Wilhelm, J. B. Schmitt, and V. Lenders, "Practical message manipulation attacks in ieee 802.15. 4 wireless networks," in *Proc. of Workshop MMB*, 2012, pp. 29–31.

[55] V. Boyko, P. MacKenzie, and S. Patel, "Provably secure password-authenticated key exchange using diffie-hellman," in *Proc. of Eurocrypt*, 2000, pp. 156–171.

[56] H. Akima, "A new method of interpolation and smooth curve fitting based on local procedures," *Journal of the ACM (JACM)*, vol. 17, no. 4, pp. 589–602, 1970.

[57] T. S. Rappaport *et al.*, *Wireless communications: principles and practice*. Prentice Hall PTR New Jersey, 1996, vol. 2.

Nirnimesh Ghose received the Ph.D. in the Electrical and Computer Engineering department from the University of Arizona, Tucson in 2019. He is an Assistant Professor of Computer Science and Engineering with the University of Nebraska-Lincoln. He received his MS degree in Electrical and Computer Engineering from the Illinois Institute of Technology, Chicago in 2012, and his B.Tech. degree in Electronics and Communication Engineering from the Uttar Pradesh Technical University (now Dr. A.P.J. Abdul Kalam Technical University), Lucknow, India in 2010. His research focuses on network security and privacy with applications to emerging wireless networks, cyber-physical systems, Internet of Things, aviation and transportation networks, and the interaction between cybersecurity and social networks. He has served as a web chair for IEEE CNS 2018 and as a reviewer for numerous conferences and journals.

Loukas Lazos received the Ph.D. degree in electrical engineering from the University of Washington in 2006. He is a Professor of Electrical and Computer Engineering with the University of Arizona. His research interests are in the areas of security and privacy, networking, and wireless communications; detection, mitigation, and visualization of security threats; secure secret-free pairing and key management for wireless networks; secure and fair resource allocation for heterogeneous coexisting systems; privacy in dynamic spectrum access. He was a recipient of the U.S. National Science Foundation Faculty Early CAREER Development Award in 2009 for his research in the security of multi-channel wireless networks. He has served as the Technical Program Chair for the IEEE CNS Conference, the IEEE GLOBECOM Symposium on Communications and Information Systems Security, and the IEEE DSPAN Workshop. He is a Senior Associate Editor of the IEEE Transactions on Information and Forensics Security and the IEEE Transactions on Mobile Computing.

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