SFIRE: Secret-Free In-band Trust Establishment for COTS Wireless Devices

Nirnimesh Ghose, Loukas Lazos, and Ming Li
Department of Electrical and Computer Engineering, University of Arizona, USA
Email: {nghose, llazos, lim}@email.arizona.edu

***Abstract*—We address the problem of trust establishment between wireless devices that do not share any prior secrets. This includes the mutual authentication and agreement to a common key that can be used to further bootstrap essential cryptographic mechanisms. We propose SFIRE, a secret-free trust establishment protocol that allows the secure pairing of commercial off-the-shelf (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, but can be applied to any COTS device. Moreover, 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 such as a smartphone and by using the RSS fluctuation patterns to build a robust "RSS authenticator". We perform extensive experiments using COTS devices and USRP radios and verify the validity of the proposed protocol.**

I. Introduction

The number of networked devices–smartwatches, wearable sensors, medical devices, cameras, home monitoring sensors, smart garage door openers. Internet-enabled appliances–has recently exploded. These devices often connect to a gateway/hub (e.g., a Wi-Fi access point) for delivering data or for remote actuation. Securing the communication between wireless devices and the hub is crucial because the former often collect personal sensitive data, or actuate critical functions. For instance, a remotely programmable pacemaker controls the electric pulses applied to one's heart. A smart garage door provides access to the house premises.

Fundamentally, two devices need to establish trust before they can securely communicate. Trust is established by executing a *secure pairing* protocol that achieves two-party mutual authentication and key-agreement. The first property is used to verify the device's identity (or legitimacy), whereas the second establishes a secure channel over a public medium. The prevailing methods for secure pairing either involve the manual input of the hub's secret to the device or by preloading the device with some unique secret. This secret is loaded to the hub via an out-of-band (OOB) channel, e.g., the user enters the secret manually. Alternative solutions relying on a public key infrastructure have also been proposed.

However, conventional solutions pose significant scalability, usability, and interoperability challenges. Many new wireless devices lack the necessary interfaces to enter or change passwords. Even if those passwords are entered a priori, manufacturers frequently opt for default secrets that are easily leaked. Indeed, the largest DDoS attack to date exploited default passwords preloaded to IP cameras, digital video recorders, etc. to form the Mirai botnet and attack the DNS infrastructure [1]. Finally, PKI-based solutions are difficult to widely deploy across different manufacturers.

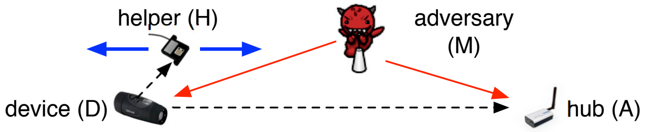


Fig. 1: Entities and system model of the basic setup.

To address these limitations, pairing methods that do not rely on pre-shared secrets have been explored [2]–[6]. Most rely on an out-of-band (OOB) human verification via, for example, a visual or an audio channel, to provide authentication and assert the protocol success. However, not all devices may be equipped with the necessary sensors for supporting OOB channels. Protocols that achieve pairing in-band via a common wireless interface have been proposed as alternatives [7], [8]. These protocols often rely on special PHY-layer mechanisms, e.g., Manchester coded ON/OFF keying, to thwart certain data integrity attacks such as a signal overshadowing. However, they still remain vulnerable to more advanced signal manipulations such as wireless signal cancellation which was demonstrated by Popper *et al.* [9] under stable channel conditions. Signal cancellation enables a man-in-the-middle (MitM) attack over wireless during the pairing process, which is difficult to counter in the absence of prior trust.

In this work, we investigate the problem of *secure in-band pairing for devices that do not share any prior secrets.* We develop the Secret-Free In-band tRust Establishment (SFIRE) primitive that draws security from hard-to-forge signal propagation laws and randomness introduced by the user. The basic operational scenario for SFIRE is shown in Fig. 1. A user initiates a pairing session between the legitimate device D and the hub A, in the presence of an active adversary M. The pairing is assisted by a helper device H. During pairing, M launches a MitM attack over the wireless channel. In SFIRE, active attacks are detected by correlating RSS fluctuations measured simultaneously at the helper and the hub, while the pairing device is active. RSS has been explored in several prior works for device authentication [8], [10], however these techniques require hardware and/or firmware modifications.

Our contributions: Our main contributions are three-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, who can perform advanced signal manipulations including wireless signal cancellation under predictable channel conditions. This presents the worst-case adversarial scenario for the pairing process. The security of SFIRE relies on a novel "RSS authenticator" that exploits limitations in signal transmission laws to thwart active attackers.
- We use SFIRE to construct a secure in-band pairing protocol based on the Diffie-Hellman (DH) key agreement. Our protocol allows a legitimate device 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 pairing device. The latter property makes SFIRE interoperable with any commercial off-the-shelf (COTS) device that has a common wireless interface with the hub.
- We carry out extensive experimentations to establish the distinct RSS-features used in the RSS authenticator. We analyze the security of SFIRE under active adversaries with increasing capabilities (in terms of antenna directionality, transmission power, etc.). We implement SFIRE on COTS equipments and USRPs to validate the offered security. Our experiments verify that SFIRE is resistant to active signal manipulations, even if the adversary enjoys favorable channel conditions to the hub and the helper.

II. Related Work

Key agreement over a public channel can be achieved using a cryptographic method such as a DH key exchange [11]. However, public message exchanges over the wireless medium are vulnerable to Man-in-the-Middle (MitM) attacks, which are notoriously difficult to thwart without a message integrity protection mechanism. Many existing secure device pairing methods rely on out-of-band (OOB) channels to defend against MitM attacks [2]–[6]. The OOB channel is assumed to possess certain security properties, for example, it is only accessible by the user, which helps verify the message source. However, OOB channels usually require non-trivial human support and advanced user interfaces. For example, when a visual channel is used, a user needs to read a string from one device's screen and input it into another [5], [6], or visually compare multiple strings or LED flashing patterns [4].

Other methods exploit the shared physical context to verify device proximity and establish trust. Examples of common modalities include accelerometer measurements when two devices are shaken together [12], or light and sound for devices located in the same room [13], [14]. Again, these require additional sensing modalities that are not available to all devices. Also, in many cases, the contextual sources bear low entropy.

There have been several attempts to design in-band message integrity protection mechanisms, which assume that signal cancellation over the wireless channel is not possible [15], [16], or occurs with bounded success [17]. For example, the Tamper-Evident Pairing (TEP) protocol proposed by Gollakota *et al.* [18] and the integrity codes (I-codes) proposed by Čapkun *et al.* [15] both relied on the infeasibility of signal cancellation when signals were modulated with Manchester coded ON/OFF keying. Because ON slots could not be canceled, an active adversary could not inject its own messages.

In our work, we assume advanced signal manipulations are possible, especially when the channel conditions are predictable and relatively stable (e.g., an indoor LoS scenario with static devices). Pöpper *et al.* demonstrated an effective relay signal cancellation attack using a pair of directional antennas [9], which is agnostic to the packet content and modulation. Recently, Hou *et al.* [17] showed that signal cancellation can be prevented only in rich-scattering environments. A recent protocol that detects signal cancellation [19] still relies on ON/OFF keying to transmit key primitives. The key difference of SFIRE is that it provides protection to cancellation attacks *without the need of specific modulation (ON/OFF keying) type*.

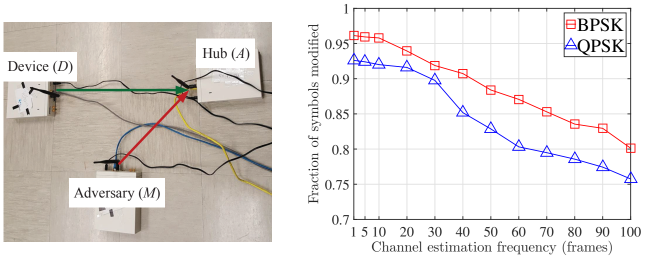
Another class of techniques derive trust from *hard-to-forge* PHY-layer properties unique to each device/link [7], [10], [20], [21]. Typical properties include (a) *device proximity*, (b) *location distinction*, and (c) *device identification*. In device proximity methods, the common idea is to exploit the channel reciprocity and its rapid decorrelation with distance. However, such techniques typically require advanced hardware. For example, [8], [10] require multiple antennas and [21] needs a wide-band receiver. Moreover, these techniques do not prevent MitM attacks. Distance bounding [22], [23] was also proposed to ensure proximity, but they are not so practical yet (either resort to OOB channels or special hardware). Finally, device identification techniques [24], [25] distinguish devices based on their unique PHY layer or hardware features. Unfortunately, device identification techniques require prior training and frequent retraining, which is not applicable to wireless devices first introduced to an environment. The technique in [7], the most recent works uses RSS measurements from the ambient environment to verify proximity and establish trust. This method, however can only authenticate devices located very close (5cm) and only under the assumption of rapidly time-varying the channels at the pairing locations. In SFIRE, the pairing devices can be located far apart and no assumptions are made on the channel unpredictability.

III. Motivation and Model Assumptions

A. MitM over Wireless

PHY-layer integrity verification mechanisms typically rely on the combination of Manchester coding with ON/OFF keying to detect message modification attacks [15], [16], [18], [26]. As annihilating ON signals is a hard problem in rich-scattering environments. To annihilate an ON-slot, the adversary has to inject the inverse of the signal at the receiver, which involves accurate channel estimation. Such signal annihilation is possible when the wireless channel is predictable and slow-varying [9]. Hence, an active adversary could hijack a key agreement session and inject his own messages to join the network.

To verify the adversary's ability in manipulating wireless signals, we performed a signal cancellation and injection experiment using three NI-USRP 2921 devices, organized in



(a) (b)

Fig. 2: (a) Experimental setup for evaluating signal cancellation and insertion for a single device pair, and (b) the fraction of symbols modified by the adversary as a function of the frequency of channel estimation.

the topology of Fig. 2(a). All devices were synchronized and transmitted at 2.4GHz. Device D transmitted random BPSK-modulated signals to the hub while the adversary M performed channel estimation using D's transmissions. The estimated channel was used to craft the signal injected by A to modify D's signal at A. The channel estimation was performed based on the location of the transmitter-receiver pair and D's preambles.

Fig. 2(b) shows the fraction of successfully modified symbols as a function of the frequency of channel estimation operation measured in symbols. When the channel is frequently and therefore, more accurately estimated, the success of symbol modification is quite high (96.14% and 92.60% for BPSK and QPSK modulation, respectively). Although the experiment was performed in a favorable setting (LoS slow varying channel and controllable locations for the adversary), the results show a *worst-case scenario under which MitM attacks over wireless are possible.* This motivates us to investigate a pairing protocol that is resistant to active signal manipulations.

B. 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): The legitimate device is a COTS device who attempts to pair with A via a common wireless interface. Pairing results in the establishment of a secret key for future communications. D does not share any 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 channel is established via conventional means such as loading a common key. Using this secure channel, H can apply an authenticated encryption function AE$(\cdot)$ on any transmission to guarantee the message confidentiality and integrity, and the authenticity of the source. Any such 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 AE$(\cdot)$, after separate symmetric keys are generated from the master key for the encryption and MAC operations. We refer the reader to [27] for more details on authenticated encryption. Note that pairing H to A is a one-time effort and need not be repeated with every device join. We believe that this is an acceptable tradeoff for pairing many other heterogeneous devices. Finally, H is assumed to be time-synchronized with A, using any known method [28]. Synchronization can also be achieved on the fly via synchronization messages sent from the hub.

C. Threat Model

Adversary (M): We consider an active adversary that controls one or more adversarial devices. We assume that M is at a farther distance to the helper H than D. M's goal is to (a) pair with A as a legitimate device, or (b) spoof a rogue hub that pairs with D. To realize his goal, M launches a MitM attack during a pairing session. Because the pairing process is initiated by the user, M can only hijack on an ongoing session. The Man-in-the-Middle attack is performed by canceling D's (A's) signal at A (D) and injecting his own message. When the helper is involved, M may also perform a cancellation and injection at H. The adversary is aware of the protocol executed by the legitimate entities but does not have physical access to any of the devices. 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 [29] to inject his own message at H and A.

Type 2: A type 2 adversary is a type 1 adversary that may additionally employ coordinating devices with directional antennas to achieve a desired RSS at A and D.

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

IV. The SFIRE Protocol

In this section, we present SFIRE, an in-band pairing protocol that does not require secret preloading. SFIRE makes use of a new PHY-layer protection primitive which authenticates the legitimate device D by using an "RSS authenticator". We first describe the PHY-layer protection primitive and then use it to construct SFIRE.

A. 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, while both H and A simultaneously measure the RSS. The helper 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 authenticate 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. 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 of H:** While m_D is repeatedly transmitted, the user performs a series of sweeping motions of H over D (see Fig. 3(a)). A sweeping motion is defined as a continuous motion starting away from D, passing over D and ending away from D. While in motion, H decodes messages $m'_D(1), m'_D(2), \ldots, m'_D(k)$ and also records an RSS sequence of samples taken at a pre-specified frequency. Let $\mathbf{r}_H = \{r_H(1), r_H(2), \ldots, r_H(n)\}$ denote such a sequence, with $n \geq k$. H also timestamps the first sample as $t_H(1)$.

4) **Reception at m_D at A:** The hub decodes $m''_D(1), m''_D(2), \ldots, m''_D(k)$ while the k m_Ds are being transmitted by D. The hub also records $\mathbf{r}_A = \{r_A(1), r_A(2), \ldots, r_A(n)\}$, and the reception time $t_A(1)$ of the first sample.

5) **Authentication data at H:** H checks if $m'_D(1) \overset{?}{=} m'_D(2) \overset{?}{=} \cdots \overset{?}{=} m'_D(k)$. If not, H sends an AE(ABORT) message to A via their shared authenticated channel. If the decoded messages match, H compiles message $m_H = \{\mathbf{r}_H, m'_D(1), t_H(1)\}$. H sends AE(m_H) to A.

6) **Authentication of m_H:** The hub decrypts m_H and verifies its integrity using VD$(\cdot)$, which is the corresponding authentication/integrity verification function to AE$(\cdot)$. If verification fails, A aborts m''_D.

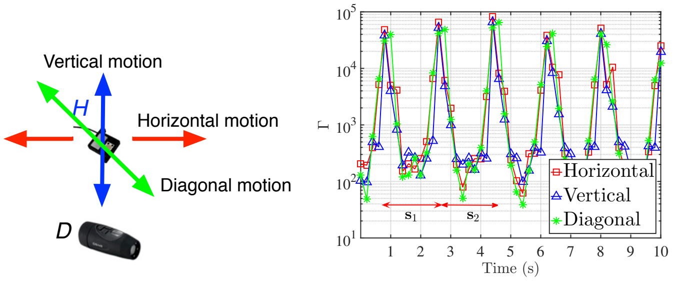
7) **Authentication of m_D:** The hub first verifies that $m''_D(1) \overset{?}{=} m''_D(2) \overset{?}{=} \cdots \overset{?}{=} m''_D(k)$. If verification fails, it aborts the pairing process. If successful, the hub verifies $m''_D(1) \overset{?}{=} m'_D(1)$. If verification fails, the hub aborts the pairing process. Otherwise, A proceeds to the RSS authentication. The hub uses the timestamp $t_H(1)$ to align $\mathbf{r}_H$ with $\mathbf{r}_A$. If $t_H(1) > t_A(1)$, sample alignment is achieved by mapping the first sample of $\mathbf{r}_A$ to the sample of $\mathbf{r}_H$ closest to $t_A(1)$. In the other case, the alignment process is reversed. The hub and computes the ratio:

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

The hub performs a set of RSS authentication tests Γ 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 test pass H displays SUCCESS. If the timer at A expires, the pairing process fails.

B. RSS Authentication Tests

We now describe the RSS authentication tests performed by A to verify m_D. For each test, the hub divides the RSS ratio samples in Γ in sweeps, by organizing the samples in a timeline. *Each sweep is determined by observing a valley-peak-valley-peak sequence*. If the user does not start away from D, the first few samples are discarded, until a valley is found. One such timeline based on our experiments (see Section V) for the three motion types of Fig. 3(a) is shown in Fig. 3(b). The first two sweeps are also marked. Let $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_\ell$ denote the sample set for each sweep, with $\mathbf{s}_i = \{s_i(1), s_i(2), \ldots, s_i(w)\}$. Each RSS authentication test is performed on a per sweep basis. For ease of presentation, we discuss the test performance and relevant test parameters in Section V.



(a) (b)

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

Test 1: Peak RSS Test: In the first test, the hub compares the peak RSS value in $\mathbf{s}_i$ with a threshold τ_{peak}. The verification passes if there is at least one sample in every $\mathbf{s}_i$ with a ratio measurement greater than τ_{peak}. This test exploits the small distance between H and D during each sweep and the physical signal propagation laws. The helper reaches within less than a wavelength from D, whereas A is at a significantly longer distance. At the closest distance, H will be within the near field of D receiving a fairly high power. As the signal attenuates at least quadratically with distance, it is expected that the peak RSS at H will be several orders of magnitude higher than A's. To mimic the same peak RSS ratio from a remote location, an adversarial device has to transmit at very high power.

Test 2: RSS Ratio Range: In the second test, the hub computes the range of the RSS ratio for sweep $\mathbf{s}_i$ as $\Delta_i = {}^{\max_{s_j}(\mathbf{s}_i)}/_{\min_{s_j}(\mathbf{s}_i)}$. The verification passes if $\Delta_i \geq \tau_{range}$, for every $\mathbf{s}_i$. This test exploits the higher roll-off rate of the signal power observed at short distances relative to longer ones. An adversary transmitting a few meters away from H will invoke a different range than that of D.

Test 3: Sweep Period: In the third test, the hub measures the period $T_s(i)$ for each sweep $\mathbf{s}_i$ and verifies that they are consistent. Consistency is verified by checking if ${}^{T_s(i)}/_{T_s(j)} \leq \tau_{period}$, $\forall i, j; i \neq j$ where the longer period is always placed at the nominator. This test exploits the fact that for a subset of motions, the peak-valley-peak sequence that defines a sweep will take twice as long if the signal originates from a remote location. This is because without passing over the remote device, a sweep will exhibit one peak and one valley. To accommodate variability in the user's motion, τ_{period} is set at a value between one and two.

Test 4: Correlation of the RSS ratio with the helper's motion: In the fourth test, the hub correlates the helper motion

D		A
Given ID_D, $(\mathbb{G}, q, g)$ Pick $X_D \in_U \mathbb{Z}_q$ $z_D \leftarrow g^{X_D}$		Given ID_A, $(\mathbb{G}, q, g)$ $X_A \in_U \mathbb{Z}_q$ $z_A \leftarrow g^{X_A}$
$m_D \leftarrow ID_D, z_D$	$\xrightarrow{[m_D]_{Up}}$	$m_A \leftarrow ID_A, z_A$
(H active)	$\xrightarrow{\text{AE}(m_{H,j}, K)}$	Verify & Extract z_D
Verify & Extract m_A at H	$\xleftarrow{\text{AE}(m_A, K)}$	
	$\xleftarrow{[m_A]_{Dw}}$	(H active)
$k_{D,A} \leftarrow (z_A)^{X_D}$		$k_{D,A} \leftarrow (z_D)^{X_A}$

Fig. 4: DH key agreement using SFIRE as a message authenticator.

with the RSS ratio fluctuation. This test requires acceleration data from H to identify the beginning and end of a sweep, independently of Γ. During the sweeping motion, H changes direction at its maximum separation from D. This change in direction causes a peak in the acceleration of H, which can be used to specify the beginning and end of a sweep. This test is successful if the Pearson correlation coefficient $\rho(t_{RSS}, t_{acc})$ exceeds a threshold τ_{corr}, where t_{RSS} is the time at which a local RSS minimum is measured and t_{acc} is the local acceleration maximum closest to t_{acc}. This test particularly targets a type 3 adversary who may defeat the previous three tests via fine-grained power control. If the power manipulation is not synchronized with the helper's motion, which is difficult to achieve in real time, the fourth test is violated.

We note that reporting acceleration values does require a helper with an embedded accelerometer. However, it does not place any additional hardware requirement on D. Smartphones, which are the most suitable helper candidates, already have accelerometer sensors embedded. Moreover, the fourth test is needed to thwart the most advanced attack that integrates signal cancellation, high power availability, antenna directionality, and precise power control.

C. SFIRE-Enabled Device Pairing

We now describe how 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. 4. The hub (or D) use 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 Figure 4), D broadcasts $m_D : ID_D, z_D$ in plaintext to the A. The hub verifies this broadcast using SFIRE. In the protocol of Fig. 4, messages protected by SFIRE are denoted by $[\cdot]_{Up}$. 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 [30]. If any of the verification steps fail, the corresponding party aborts the pairing protocol.

1) Securing the Downlink Communication: In the DH exchange of Fig. 4, 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 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 H 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 the RSS from the respective transmissions of H and A. Therefore, H and D need not share an authenticated channel. Moreover, D does not need any special hardware, as RSS measurements are readily available in-band.

V. Security Analysis and Experimental Evaluation

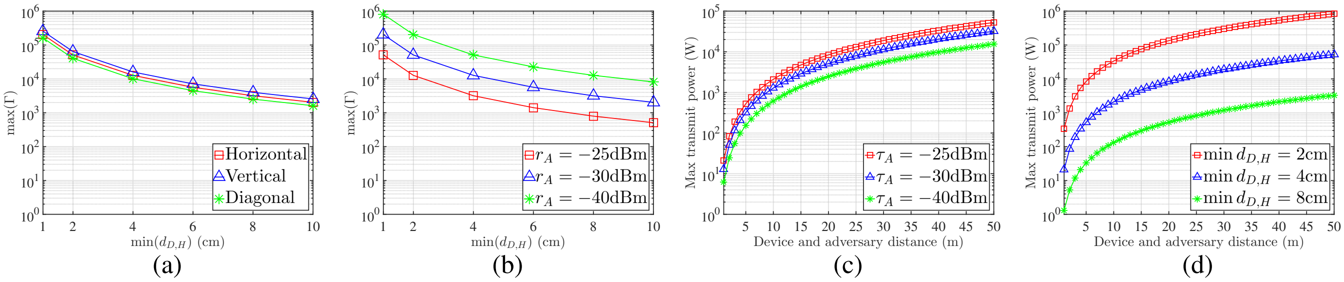
In this section, we evaluate the security of SFIRE. For the experimental evaluation, we used two setups. Setup 1 used COTS devices to obtain measurements from a legitimate device, whereas Setup 2 used USRP devices to implement various attacker models. We describe each in detail.

Setup 1: SFIRE with COTS devices: In setup 1, D and A were implemented by a Lenovo Y-480 IdeaPad laptop and a Dell XPS desktop, respectively, equipped with Intel® Centrino® Wireless N-200 wireless cards, which transmit at 20dBm. The helper was implemented on a Samsung Android-based smartphone equipped with an 802.11 a/b/g/n/ac 2.4G+5GHz compatible chipset. The helper and the hub were synchronized via an Internet server. During pairing, we performed the three sweeping motions shown in Fig. 3.

A sweeping motion was characterized by three parameters: (a) the orientation (a horizontal sweep across the D-A line, a perpendicular sweep to the D-A line and a diagonal sweep to the D-A line). (b) minimum separation $(\min d_{D,H})$ between D and H measured in cm, and (c) maximum separation $(\max d_{D,H})$ between D and H measured in cm. Minimum and maximum separations were adhered 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. Each sweeping motion was repeated 1,000 times, which took about 35min.

Setup 2: SFIRE on USRPs: In setup 2, 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 devices were synchronized via the same computer.

Test 1: Peak RSS ratio: To evaluate the peak RSS ratio $\max(\Gamma)$ achieved in a benign scenario, we performed two experiments using Setup 1. In the first experiment, D was placed at 10m from A such that the average RSS at A was -40dBm and H was swept over D. In Fig. 5(a), we show the peak RSS ratio as a function of $\min d_{D,H}$, for all the sweeping



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

Fig. 5: (a) Peak RSS ratio for various sweeping motions, (b) peak RSS ratio for various RSS at A, (b) maximum transmit power of a type 2 adversary to achieve τ_{peak} for various τ_A, and (d) maximum transmit power of a type 2 adversary to achieve τ_{peak} for various $\min d_{D,H}$.

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.

In the second experiment, we varied the distance $d_{A,D}$, such that the RSS at A also varied. In Fig. 5(b), we show the peak RSS as a function of $\min d_{D,H}$. 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 $\min d_{D,H}$. Plots in Fig. 5(a) and 5(b) can be used to select the threshold τ_{peak} for Test 1.

Security Analysis: We further analyze the security of Test 1 for a Type 1 and Type 2 adversaries. To pass the RSS authentication at A, a Type 1 adversary performs an overshadowing attack [29] at A and H simultaneously. Let the adversary perform the overshadowing attack from a particular location L_M. Assuming an omnidirectional antenna, his transmission will impact the RSS at both H and A. Figure 6 shows different possible orientations of M for a fixed distance $d_{M,H}$.

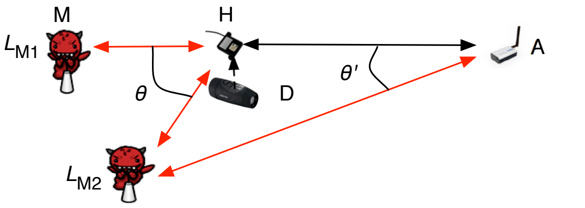


Fig. 6: L_{M1} (on the line from A to H) is the optimal direction for maximizing the RSS peak ratio.

To determine the impact of M's transmission on the peak RSS ratio, we consider a simple propagation model with an attenuation factor α.

$$P_{Rx} = P_{Tx} G_{Tx} G_{Rx} \left(\frac{\lambda}{4\pi d}\right)^{\alpha}. \tag{1}$$

The RSS ratio γ_M at A based on M's transmission is:

$$\gamma_M = \frac{r_H}{r_A} = \left(\frac{G_H}{G_A}\right)\left(\frac{d_{M,A}}{d_{M,H}}\right)^{\alpha} = \left(\frac{d_{M,A}}{d_{M,H}}\right)^{\alpha}, \tag{2}$$

assuming the same antenna gains at H and A. For a fixed distance $d_{M,H}$, it is straightforward to show that this ratio is maximized when the nominator is maximized, i.e, M is located on the H-A line at position L_{M1} Manipulating (2) yields

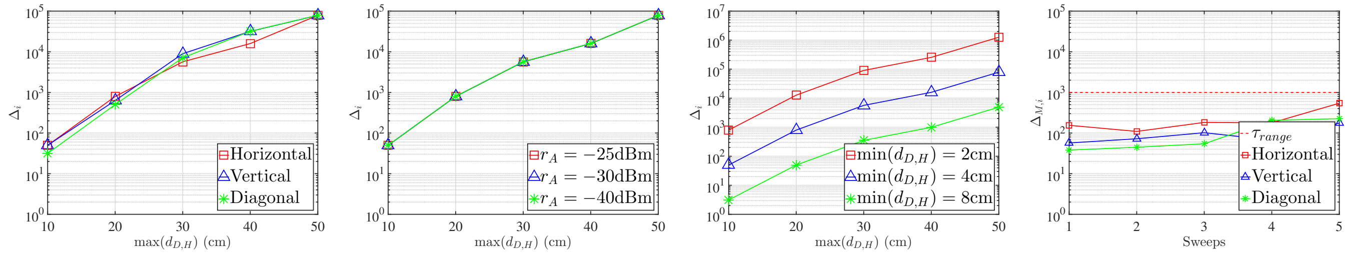
$$\begin{aligned} \gamma_M &= \left(\frac{d_{M,A}}{d_{M,H}}\right)^{\alpha} \approx \left(\frac{d_{D,M} + d_{D,A}}{d_{D,M} + d_{D,H}}\right)^{\alpha} \\ &= \left(\frac{d_{D,A}}{d_{D,H}} + \frac{d_{D,M}\left(1 - \frac{d_{D,A}}{d_{D,H}}\right)}{d_{D,M} + d_{D,H}}\right)^{\alpha} \\ &< \left(\frac{d_{D,A}}{d_{D,H}}\right)^{\alpha} = \gamma_D. \end{aligned} \tag{3}$$

In (3), we approximated $d_{M,H}$ with $d_{M,D} + d_{D,H}$ based on the close proximity of D and H during the peak RSS ratio measurement and assuming that $d_{M,D}$ is in the order of meters relative to $d_{D,H}$ which is in the order of centimeters. In (3), γ_D is the RSS ratio achieved by the legitimate device D.

Type 1: Based on (3), a Type 1 adversary that transmits from a single position will not be able to achieve the same RSS ratio as D, irrespective of its transmission power, unless it gets very close to H (in which case the approximation in (3) no longer holds). For similar channel models, the RSS ratio solely depends on the distance ratio between M and H to M and A. Intuitively, γ_M will always be less than the true value of γ_D because M is at a farther distance to H than D. Getting very close to H is easily detectable as it is under the user's control.

Type 2: A type 2 adversary deploys two devices with directional antennas such that it can independently impact the RSS at H and A. There are two ways that the peak RSS ratio can be achieved; by increasing the received power at H and decreasing the received power at A, by performing cancellation and injection at low power, but above the receiver's sensitivity. The latter attack can be prevented by requiring a minimum RSS at A during pairing. For instance, the hub may require a minimum of -50dBm of received power during pairing, which corresponds to a maximum pairing distance of up to 100m assuming a free space propagation model and 1W transmit power. In this case, the only option for the adversary is to increase the received power at H via a directional transmission.

In Fig. 5(c), we show the required transmit power for a type 2 adversary to defeat Test 1 as a function of $d_{M,H}$ and for different minimum RSS thresholds τ_A at A. For our test, we have selected $\tau_{peak} = 1995$ for $\tau_A = -25$dBm, $\tau_{peak} = 10358$ for $\tau_A = -30$dBm, and $\tau_{peak} = 30403$ for $\tau_A = -40$dBm base on the results of Fig. 5 In our calculations, we have used the free space propagation model because this presents the most favorable channel condition for M (least attenuation).



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

Fig. 7: (a) RSS ratio range of Γ for various sweeping motions, (b) RSS ratio range of Γ for various RSS at A, (c) RSS ratio range of Γ for various $\min d_{D,H}$, and (d) RSS ratio range of Γ for a type 2 adversary for $d_{D,M} = 2$m with τ_{range} selected for $\max d_{D,H} = 50$cm and $\tau_A = -40$dBm.

Figure 5(d) shows the maximum transmit power for various minimum distances between D and H during every sweep, assuming a $\tau_A = -40$dBm. From the plots, it can be observed that the required transmit power becomes quickly prohibitive with the distance from M. At 10m from H, the adversary must transmit at hundreds of watts, to achieve the required ratio. However, the adversary may still 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.

Test 2: RSS Ratio Range: We now evaluate the adversary's ability in defeating Test 2. We performed three experiments to evaluate 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 $\min d_{D,H} = 4$cm. Figure 7(a) shows the RSS ratio range as a function of the maximum separation between D and H. In the second experiment, we varied the distance between A and D, and repeated the measurements. Figure 7(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 with the motions or the RSS threshold at A. Moreover, longer sweeps significantly increase the RSS ratio range due to the near-field effect. Figure 7(c) reports the result of our third experiment where we varied $\min d_{D,H}$ and performed a horizontal sweeping motion. As the helper is passed closer to the device, the near-field effect is intensified, leading to higher RSS range. The highest value is achieved when H is passed the closest (2cm) and the range of H's motion is the longest (50cm away from D). We set the $\tau_{range} = 10^3$, which captures a any motion over 30cm with $\min d_{D,H} = 4$cm.

Security Analysis: We now evaluate the capability of Type 2 adversary to pass the RSS ratio range. Intuitively, when a type 2 adversary is at a certain distance away from H, the variation between the ratios of distances to A and H will be not sufficient. As observed in (3), the numerator for the true $d_{D,H}$ varies more than $d_{D,M}$. To validate this, we performed experiments on Setup 2. We selected $\tau_{range} = 10^3$, $\max d_{D,H} = 50$cm and $\tau_A = -40$dBm. Figure 7(d) shows Δ_i achieved by the adversary for various motions when the distance between H and M is as low as 2m. The adversary's RSS ratio range is below τ_{range} for most motions and reaches the required range only for one horizontal sweep. Therefore, the type 2 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_{M1} shown in Fig. 6. However, other motions failed to achieve similar range. We further repeated our experiments for multiple sweeps and for different distances between M and D. The results in Fig. 8(a) show that even if M is very close to D (within 0.5m), it cannot achieve the required dynamic range consistently for all motions, without employing power control.

Test 3: Sweeping Period: We now evaluate the ability of Test 3 in detecting a Type 3 adversary who can vary his power during H's motion. We performed two experiments using Setup 1 to evaluate the consistency of the sweeping periods across different motion orientations. In the first experiment, we measured the ratio of the sweep periods between pairs of motions–horizontal-vertical (H-V), horizontal-diagonal (H-D) and vertical-diagonal (V-D)–when D was active. Figure 8(b) shows the period ratio for all the motion combinations as a function of $\max d_{D,H}$ 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 $\tau_{period} = 1.4$.

Security Analysis: We further 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, fixed the distance between M and D to 1m, $\max d_{D,H} = 50$cm and $\min d_{D,H} = 4$cm. M oscillated its transmitting power between 10dBm and 30dBm to meet both the τ_{peak} and τ_{range} thresholds. For the experiments, M mimicked 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. 8(c), 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 2sec, 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 8(d) shows the sweep period ratios for different $\max d_{D,H}$. 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 random motions invoked by the user have the same period, such as the horizontal and vertical motion for our setup.

Test 4: Correlation of the RSS ratio with the helper's motion: To remedy a possible failure of Test 3, we obtain

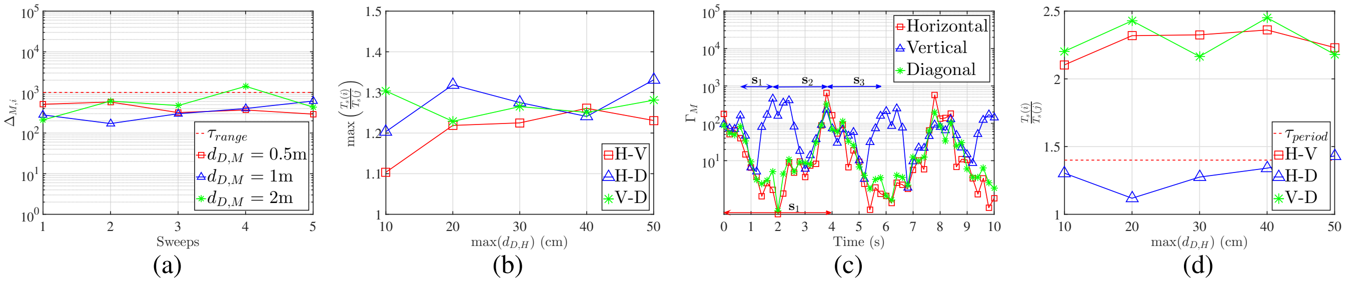


Fig. 8: (a) RSS ratio range of Γ for type 2 adversary with τ_{range} selected for $\max d_{D,H} = 50$cm and $\tau_A = -40$dBm, (b) $\max\left({}^{T_s(i)}/{}_{T_s(j)}\right)$ for each motion for various RSS at A, (c) RSS ratio fluctuation for type 2 adversary at 2m from D, and (d) ${}^{T_s(i)}/{}_{T_s(j)}$ for each motion for a type 3 adversary mimicking transmit power for vertical sweeping motion of H.

TABLE I: 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
Test 2	Fail	Fail	Pass	RSS data
Test 3	Fail	Fail	Might Pass	RSS data
Test 4	Fail	Fail	Fail	RSS, accelerometer at H

an independent measurement of the true sweep period by collecting accelerometer data from H. Based on this data, we correlate the peaks and valleys with the helper's position. We performed two experiments using Setup 1 to evaluate the correlation $\rho(t_{RSS}, t_{acc})$ between the time t_{RSS} when the minimum Γ is measured and the maximum helper acceleration t_{acc}. In the first experiment, we varied the motions of H whereas in the second experiment we varied the RSS at A by moving D closer to A. Figure 9(a) shows the Pearson correlation coefficient for various sweeping motions, whereas Fig. 9(b) shows the results for vertical sweeping motion with variable RSS at A. Significantly high correlation is present regardless of the motion type and RSS at A.

Security Analysis: We also analyzed the performance of a Type 3 adversary trying to defeat the Test 4 by employing Setup 2. In this setup, a Type 3 adversary applied power control to defeat Test 1 and Test 2. Figure 9(c) shows the achieved correlation for various sweeping motions as a function of the number of sweeps. The time when the minimum of Γ and the maximum of acceleration achieved decorrelates with the increasing number of sweeps for any motion because the mimicked power profiles have to be different for the different motions. Hence, a Type 3 adversary is unable to defeat Test 4. Table I summarizes the success of each test against each adversary type and the data requirement for each test.

VI. Evaluation of SFIRE-Enabled Device Pairing

We now analyze the security of the device pairing protocol proposed in Section IV-C. 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.

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 IV-C 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 device, the adversary cannot initiate the pairing from a remote location.

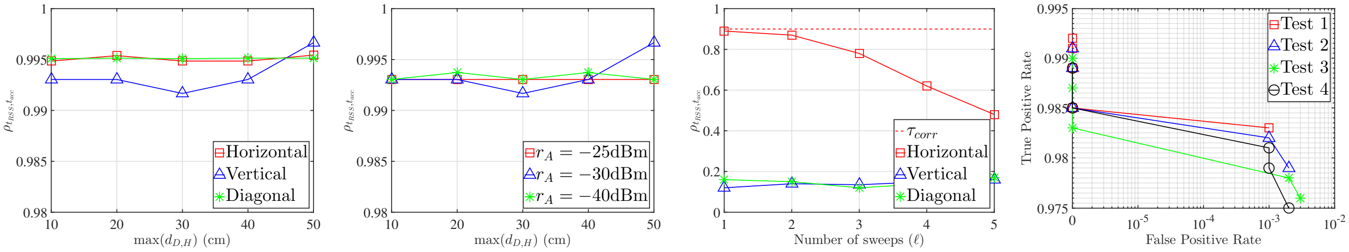
Hijacking a legitimate pairing session: Since M cannot initiate the pairing process with the A, he can only attempt to pair a rogue device with the A by hijacking a pairing session involving a legitimate device (D). To establish a secret key with the A, the adversary must modify the DH public number 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.

2) Pairing D with a Rogue Base Station: We now examine whether 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 number z'_A. The m_A is protected by downlink SFIRE primitive $[\cdot]_{Dw}$ as discussed in Section IV-C1. In the downlink SFIRE, D computes Γ, during the transmission of m_A from RSS values of frames received from A and H. The D then performs the RSS authentication that prevents pairing with A'.

3) ROC Curves: Finally, 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 1995 for $\tau_A = -25$dBm, $\tau_{range} = 78791$ for the same RSS at A, $\tau_{period} = 1.4$ and $\tau_{corr} = 0.9$. 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_{M1} as shown in Fig. 6.

Figure 9(d) 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 right most point is obtained for one sweep, whereas the left most 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



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

Fig. 9: (a) $\rho(t_{RSS}, t_{acc})$ for various sweeping motions, (b) $\rho(t_{RSS}, t_{acc})$ for various RSS at A, (c) $\rho(t_{RSS}, t_{acc})$ for a type 3 M mimicking transmit power for horizontal sweeping motion of H, and (d) ROC curve for the performance of verification tests of SFIRE against various types of adversaries.

protocols achieve both correctness and security.

4) Timing Performance: The timing performance of SFIRE is dictated by the time to complete the number of sweeps. This time dominates the computation of DH key, transmission delays, etc. From Fig. 9(d), three sweeps give zero false positive rates for all Types of M. Therefore, the time to complete the protocol requires six sweeps (three for uplink and three for downlink), translating to 6sec.

VII. Conclusions

We addressed the problem of trust establishment 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 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 and CNS-1410000. 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.

References

[1] 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

[2] A. Kumar, N. Saxena, G. Tsudik, and E. Uzun, "Caveat eptor: A comparative study of secure device pairing methods," *Proc. of Percom*, pp. 1–10, 2009.

[3] L. H. Nguyen and A. W. Roscoe, "Authentication protocols based on low-bandwidth unspoofable channels: a comparative survey," *Journal of Computer Security*, vol. 19, no. 1, pp. 139–201, 2011.

[4] T. Perković, M. Čagalj, T. Mastelić, N. Saxena, and D. Begušić, "Secure Initialization of Multiple Constrained Wireless Devices for an Unaided User," *IEEE transactions on mobile computing*, 2011.

[5] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using camera phones for human-verifiable authentication," in *Proc. of Security and Privacy Symposium*, 2005, pp. 110–124.

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

[7] J. Zhang, Z. Wang, Z. Yang, and Q. Zhang, "Proximity based iot device authentication," in *Proc. of IEEE INFOCOM–2017*, 2017.

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

[9] 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.

[10] 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.

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

[12] R. Mayrhofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices," *IEEE Transactions on Mobile Computing*, vol. 8, no. 6, pp. 792–806, 2009.

[13] 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.

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

[15] 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 Transactions on Dependable and Secure Computing*, vol. 5, no. 4, pp. 208–223, 2008.

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

[17] 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.

[18] S. Gollakota, N. Ahmed, N. Zeldovich, and D. Katabi, "Secure in-band wireless pairing," in *USENIX security symposium*, 2011, pp. 1–16.

[19] 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.

[20] 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.

[21] 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.

[22] S. Brands and D. Chaum, "Distance-bounding protocols," in *Proc. of Advances in Cryptology EUROCRYPT 93*. Springer, 1994, pp. 344–359.

[23] K. Rasmussen and S. Capkun, "Realization of rf distance bounding," in *Proc. of USENIX Security Symposium*, 2010.

[24] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. of ACM Mobicom*, 2008, pp. 116–127.

[25] B. Danev, T. Heydt-Benjamin, and S. Čapkun, "Physical-layer identification of rfid devices," in *USENIX security symposium*, 2009, pp. 199–214.

[26] R. Jin and K. Zeng, "Physical layer key agreement under signal injection attacks," in *Proc. of CNS Conference*, 2015, pp. 254–262.

[27] 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.

[28] A. Sampath and C. Tripti, "Synchronization in distributed systems," in *Advances in Computing and Information Technology*. Springer, 2012, pp. 417–424.

[29] M. Wilhelm, J. B. Schmitt, and V. Lenders, "Practical message manipulation attacks in ieee 802.15. 4 wireless networks," in *Proc. of Workshop MMB12*, 2012, pp. 29–31.

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