FMS-AMS: Secure Proximity-based Authentication for Wireless Access in Internet of Things

Jeongyoon Heo, Yongjae Yoo, Jihwan Suh, Woojin Park, Jeongyeup Paek, and Saewoong Bahk

Abstract: **Proximity-based authentication enables wireless access points (AP) to allow connection only to devices within a certain authentication range. This would be very convenient for allowing network access only to those within a physical boundary. However, an attacker not within the authentication range may deceive the AP into authenticating its proximity by eavesdropping with higher receiver gain and increasing its transmit power. This can be done easily using an amplifier or a directional antenna. To address this challenge, we propose '*Fixed MCS SNR* (*FMS*)' filtering scheme based on the intuition that high MCS requires high SNR, and amplifying the received signal strength does not necessarily improve SNR. We experimentally show that this is true in reality, and our real-world evaluation in various environments (14 locations) shows that *FMS* scheme prevents 'amplifier attacks' in all cases. To further counter the false positives of *FMS* against 'directional antenna attacks' (avg. 35.7%), we also propose '*Authentication Motion with Signal strength gap* (*AMS*)' filtering scheme which defends against both attacks in all cases at the cost of requiring the user to make a simple motion. *FMS* or *AMS* scheme can be selected according to the application requirement to enhance the security of proximity-based authentication in upcoming IoT.**

Index Terms: **IEEE 802.11n, proximity-based authentication, security, wireless, authentication**

I. INTRODUCTION

With the development of Internet of Things (IoT) technology, the number of wireless devices is increasing rapidly. In addition to smartphones and laptops, AR/VR HMDs, wearable devices, and many of the latest consumer electronics also use wireless to communicate with their owners. However, broadcasting nature of wireless signal not only frees users from tethers, but also brings potential threats of those devices being used by unauthorized users [1]–[3]. Thus in this multi-device environment, convenient and secure authentication is crucial to allow owners to easily manage multiple devices, prevent waste of limited resources by unauthorized users, and reduce security concerns such as privacy leakage.

Cryptographic techniques such as passwords have widely been applied to authentication, and they are still viable options. However, they impose a requirement of creating, remembering, sharing among the authorized, and entering a password whenever required. For example, one of the first things that attendees ask in a meeting/conference is the WiFi password which they may sometimes need to repeat hundreds of times. Furthermore, password is vulnerable with a single exposure, and frequent change of password decreases usability especially in a multi-device environment. In addition, for IoT devices with no screen or input interface, authentication without a password is strongly preferred.

In a scenario where we regard proximity as a measure of authority, we may achieve significantly higher convenience by using proximity instead of a password. Said differently, if a user is in a room that can be accessed physically only by authorized personnel (e.g., home with a key lock), then asking for another password to access devices within that room is only a cumbersome duplicate measure. Surely, I would like to control all devices in my home without a password, while preventing my neighbors from doing so. For this purpose, *proximity-based authentication* can be employed. A straight forward approach is to use received signal strength (RSS) to detect and filter out devices in (non-)proximity, and allow connection only to devices within a certain authentication range [4]. It can be used independently of, or in addition to, password-based authentication. This would be very convenient for allowing intranet access only to employees within a physical boundary, or providing Internet access only to customers at a store.

Specifically, proximity-based authentication can be useful in the following scenarios.

- Many restaurants, coffee shops, and shopping malls provide free WiFi. Proximity-based authentication allows this to be provided only to customers inside the stores.
- Some meetings (e.g., standardization meeting) do not distribute their materials to the public. In this case, only the committee members within the room can download the materials through the connected network.
- Wireless can be used for attendance check systems in classrooms or offices [5], [6]. Proximity-based authentication prevents users from cheating from outside.
- In home networks, proximity-based authentication can be used for authenticating family members and home visitors only, without a password, and not neighbors or outsiders.
- Proximity-based authentication can provide a smart lock that automatically unlocks a device when its user is nearby and locks it when the user is away from the device.

However, an attacker not within the authentication range may deceive the AP into authenticating its proximity by eavesdropping with higher receiver gain and increasing their transmit

Manuscript received March 31, 2020; revised April 6, 2020; approved for publication April 26, 2020. This paper is specially handled by EIC and Division Editor with the help of three anonymous reviewers in a fast manner.

This work is supported by SAMSUNG Research, Samsung Electronics Co.,Ltd.

J. Heo and W. Park are with Samsung Research, Samsung Electronics, Seoul, Republic of Korea, email: {jr.heo, woojin1.park}@samsung.com

Y. Yoo, J. Suh and S. Bahk are with the Department of Electrical Engineering, Seoul National University and INMC, Seoul, Republic of Korea, email: {yjyoo, jhsuh, sbahk}@netlab.snu.ac.kr.

J. Paek is with School of Computer Science & Engineering, Chung-Ang University, Seoul, Republic of Korea, email: jpaek@cau.ac.kr.

Saewoong Bahk is the corresponding author.

Digital Object Identifier: 10.1109/JCN.2020.000009

1229-2370/19/$10.00 © 2020 KICS

power using an amplifier ('amplifier attack') or a directional antenna ('directional antenna attack'). In these attacks, the attacker may amplify transmit/received signals to satisfy the required RSS for decoding at both the attacker and the AP, and pretend as if it were within the authentication range. Ideally, phase-based ranging [7] can defeat those attacks by providing accurate distance estimation, but it requires a customized protocol and a specialized signal that are often hard to implement in commercial off-the-shelf (COTS) devices.

To address this challenge, we propose '*Fixed MCS SNR* (*FMS*)' filtering scheme. *FMS* scheme is based on the intuition that typical amplifiers improve only the RSS but not SNR (signal-to-noise ratio) when receiving signals, and the BER (bit error rate) of MCS (modulation and coding scheme) is dependent on SNR not RSS. Said differently, an amplifier amplifies the noise component as well in addition to the intended received signal, which does not improve SNR. Since high MCS requires high SNR and SNR decreases with physical distance, an amplifier attacker not within proximity is unable to decode high MCS packets due to low SNR despite high RSS. Then, by fixing the MCS level high for authentication (temporarily disabling automatic MCS adaptation and keeping the MCS level high), the AP can infer whether the device is within proximity or not.

We evaluate our proposed schemes through real-world experiments in various environments (14 locations) to show that *FMS* scheme prevents amplifier attacks in all cases (100%) and directional antenna attacks in 64.3% of the cases. To further tackle the 35.7% of false positives against the directional antenna attacks, we also propose '*Authentication Motion with Signal strength gap* (*AMS*)' filtering scheme. *AMS* utilizes temporal change and spatial difference of RSS over time and over two antennas when a user makes a simple authentication motion that moves his/her device from one antenna to another. It is based on the idea that this motion (and resulting RSS change and difference) is difficult for an attacker to mimic from a distance. Our real-world evaluation shows that *AMS* scheme can defend against both attacks in all cases (100%) at the extra cost of requiring user's motion at a close distance.

The contributions of this work are as follows.

- We study two potential attacks in proximity-based authentication: 'amplifier attack' and 'directional antenna attack', and experimentally show that they both are feasible and plausible attacks.
- We propose two schemes, '*FMS*' and '*AMS*', which use wireless signal characteristics to defeat the attacks.
- We implement proof-of-concept prototypes of our proposals on COTS IEEE 802.11n devices, and evaluate them through extensive real-world experiments in various environments to show their effectiveness.

The remainder of this paper is structured as follows. Section II discusses related work, and Section III describes the attack models. Then, we propose *FMS* and *AMS* schemes that counter the attacks, in Section IV. Section V presents how we implement the attacks and the proposed schemes, and evaluates both the impact of the attacks and the performance of our proposed defense measures in various environments. Finally, Section VI concludes the paper.

II. RELATED WORK

Many proximity-based authentication techniques have been studied based on the idea that the channel environments of co-located devices are similar to each other, and a device can infer which devices are physically close to it by comparing their channel characteristics.

P. Sapiezynski *et al.* propose to detect proximity of devices by comparing the lists of available routers and the routers' RSSI [8]. There are also symmetric key generation techniques, each of which establishes a key with channel characteristics such as RSSI or channel state information (CSI) [9]–[11]. These techniques reduce key exposure threats by locally generating symmetric keys without explicitly exchanging them over wireless channels. However, these techniques are applicable only when the channels between the two devices are reciprocal. This may be challenging to apply in environments with multi-path or delay [12].

More recently, SFIRE [13] tackled the problem of trust establishment between wireless devices by using the RSS fluctuation patterns to build a robust RSS authenticator. The idea of using RSSI gap (in the form of a ratio) is similar to our *AMS* approach. However, this scheme requires an extra external helper device, whereas *AMS* only requires two antennas in the AP which is quite common in today's WiFi APs. SNAP [14], on the other hand, uses single-antenna WiFi device to determine proximity. It leverages the repeating nature of WiFi's preamble and the behavior of a signal in the near-field region to detect proximity with high probability. However, the detection scope (definition of proximity) of this work is different from ours; SNAP distinguishes within 12 cm against beyond, up to 3 m, whereas the focus of our work is within a room size ($\sim$5 m) against beyond.

In Amigo [15], locally measured channel information is exchanged between devices that want to connect to each other to verify that they are co-located. However, an attacker with pre-estimated channel information at the location of interest can induce 45% and 15% false-positive rates when it is 1 m and 5 m away from the legitimate devices, respectively. Since the attacker can attack multiple times, these false-positive rates (which can be regarded as attack success rates) seem insufficient. Therefore, the authors propose to use hand waving in front of the antennas of the two co-located devices to prevent the attack, similar to our *AMS*.

Similar to Amigo, several studies have adopted user gestures to enhance the security of proximity-based authentication [16]–[18]. C. Castelluccia *et al.* use an action that shakes legitimate devices to prevent an eavesdropping attacker from analogizing the key through signal strength [17]. Y. Nishida uses a gesture that moves the user device closer to an AP [18]. When the device close to the AP moves closer, change in the intensity of the device signal received by the AP is greater than when it is farther away. Based on this idea, the AP determines whether the device is physically in its proximity. However, an attacker can adjust its signal strength to create a signal pattern similar to that generated by a legitimate device, and we have confirmed this feasibility through real experiments.

Additional devices such as sensors can be used to improve the security of authentication schemes. Move2Auth [19] uses RSSI variation and correlation between an RSSI trace and a sensor

trace when a user device moves. The false-positive rate is 8.2% against an attacker who knows the gesture used for authentication. Shake-n-Shack [20] generates a key using the accelerometer data when shaking hands among users with wearable devices. It needs 1.3 s to generate a 128-bit key, and its false-positive rate is 1.6% when false-positive and false-negative are equal. Perceptio [21] uses the fingerprint of inter-event timing measured by various devices such as accelerometers and motion detectors. It uses the similarity of the fingerprint to judge whether the devices are co-located within a boundary. Distance bounding [22] or phase-based ranging [7], [23] techniques can also be used to defeat distance reduction attacks. Although these techniques are effective, they are not applicable to COTS devices lacking additional hardware for authentication. On the contrary, we propose light-weight proximity-based authentication schemes which do not require additional hardware and much computational overhead.

III. ATTACK MODEL

In our proximity-based authentication system scenario, an AP authenticates a device in the same physical space (e.g., a room of bounded size) and identifies it as legitimate during connection establishment. Without loss of generality, we consider IEEE 802.11 WiFi in this work. However, we believe our idea can be applied to other technologies such as Bluetooth, Zigbee, LTE or 5G[1]. Then an attacker is a device that tries to deceive the AP into authenticating it while not residing in the same space with the AP. Therefore, our attack model assumes that a legitimate device is close to the AP and mostly in line-of-sight (LoS), while an attacker is distant (e.g., >5 m) and in non-LoS (NLoS) from the AP.

A simple way to provide proximity-based authentication is to use *RSSI filtering*. That is, an AP regards a device as being in close range if the device can respond to AP's requests (challenges) and if the RSSI of the packets received at the AP exceeds a predetermined threshold. However, an attacker can pretend to be a legitimate device in proximity of the AP by strengthening its transmit signals such that their received strength at the AP is similar to that sent by a legitimate device. The attacker can also improve its received signals with additional hardware. Under this general model, we classify attacks into two specific types: 'amplifier attack' and 'directional antenna attack' because the link characteristics vary depending on the equipment the attacker uses to strengthen the signals.

Amplifier attack: Using a powerful amplifier is a simple way to increase transmit and received signal strength and thus increase the transmission and reception range of wireless signals. The property of an amplifier can be represented by its transmit/receive gain (the amount of amplification) and noise figure (NF). NF is the dB scale of the signal-to-noise ratio (SNR) degradation caused by components in the signal-processing chain. Low noise amplifier (LNA) is an amplifier that has NF below 3 dB. Usually, an amplifier needs extra power supply to amplify signals.

[1]In such cases, an 'AP' is equivalent to a gateway, a coordinator, or a base station. Without loss of generality, We use the term 'AP' for all those cases for simplicity of description.

Directional antenna attack: Since SNR is attenuated even with an LNA, a directional antenna can be used as an alternative for signal enhancement. A directional antenna emits or receives a larger amount of (focused) signal power in a specific direction to enhance transmission or reception performance. To achieve this, it needs to be oriented towards the direction in which the AP is located. Since most directional antennas are larger than typical handheld/embedded wireless IoT devices, it is not easy to make a hand-gesture-like motion with a directional antenna while amplifier attackers are more capable of doing so.

IV. PROPOSED DESIGN: *FMS* & *AMS*

To defend against the attacks aforementioned in Section III, we first propose the *'Fixed MCS with SNR based filtering scheme'* (*FMS* scheme). It authenticates a user when the user is closely located within the proximity of the AP (e.g., in the same room with the AP). This scheme does not require any action from the user; it can be embedded into the connection establishment protocol at the link layer (e.g., WiFi) or at the application layer (e.g., HTTP). Therefore, it is suitable for scenarios that provide easy connectivity to many users in a room.

However, it may have some false positives in the presence of more advanced directional antenna attacks that achieves high SNR for received signals even at a distance. To eliminate this vulnerability, we further propose *'Authentication Motion with Signal strength gap based filtering scheme'* (*AMS* scheme). It prevents both the amplifier and the directional antenna attacks at an extra cost of requiring the user to make a hand gesture at a close distance from the AP. Therefore, it is suitable for a more personal space that needs high-level of security, such as home or a private office. In this section, we describe the idea, design, and operation of the two proposed schemes.

A. Fixed MCS with SNR based Filtering (FMS)

FMS scheme defends against the amplifier attack by exploiting the characteristics of amplifiers and MCS. Specifically, it is based on the intuition that an amplifier can only improve RSS but not the SNR when receiving signals, and each MCS level in IEEE 802.11(n) has minimum requirements on RSSI and SNR for decoding the received packets [24]. That is, when a higher MCS level is used, higher RSSI and SNR are required.

Under the assumption that the noise floor is constant, SNR decreases as the distance increases or if the signal passes through obstacles. Then, even if an amplifier can amplify the received signal and increases the RSSI, it does not improve the SNR and may even make it worse because the noise component included in the incoming signal is amplified together, and the internal noise of the amplifier is also added to the signal. Therefore, SNR at a remote attacker will be lower than that at a closer legitimate device, and low SNR leads to failure of decoding packets encoded with high MCS level, helping to differentiate the attacker from a legitimate device.

Based on this idea, AP encodes and transmits messages with a high MCS level (7 in our prototype) when performing proximity-based authentication. If the target device successfully decodes and replies to those messages, the AP identifies the de-

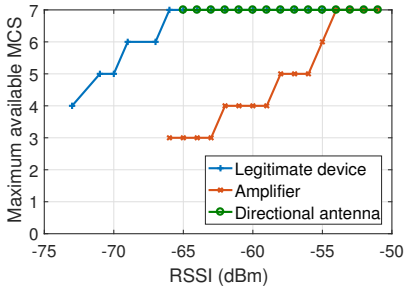


Fig. 1. Proof of the concept of *FMS* scheme.

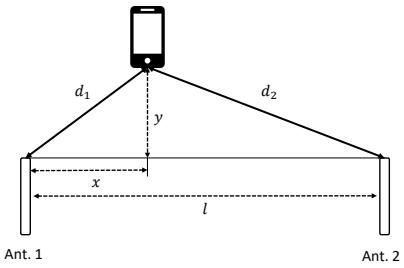


Fig. 2. Principle of *AMS* scheme.

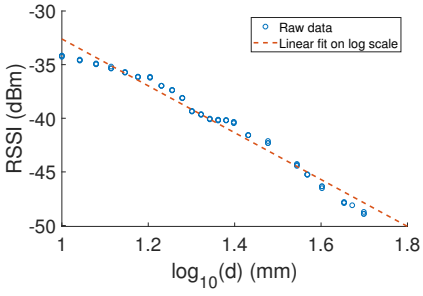


Fig. 3. RSSI measurements and its linear fitting curve on the log scale distance in the near-field.

vice as in its proximity[2]. However, if the AP always sends the same messages (challenges) for authentication, it is vulnerable to *replay attacks* even if the attacker cannot decode AP's messages [25]. Replay attack is an attack where the attacker overhears the messages sent by a legitimate device and use it for its authentication by repeating it without a need for decoding it. To address this problem in *FMS*, the AP generates and includes a random nonce in every challenge for the legitimate device to reply to.

For proof-of-concept, we performed a preliminary experiment using three devices with varying distances (Fig. 6); (1) one with a 5 dBi dipole antenna (legitimate device), (2) with a 5 dBi dipole antenna and an 11 dB receive gain amplifier (amplifier attacker), and (3) with a 24 dBi directional antenna (directional antenna attacker), respectively. In each case, we measured the maximum available MCS level with respect to RSSI measured by the device in line-of-sight with the AP with varying distances. We define the maximum available MCS as the maximum MCS level at which the device successfully decodes more than 90% of the received packets.

Fig. 1 shows that, for the device with an amplifier, the maximum available MCS is lower even at higher RSSI values than that without an amplifier. This indicates that an amplifier cannot improve the SNR since the receiver with an amplifier cannot decode the high MCS packets even though it has sufficient RSSI to do so. However, when using a directional antenna, the attacker (somewhat distant from the AP) is able to obtain the maximum available MCS similar to that of the legitimate device. This implies that the *FMS* scheme may not be sufficient to defend against the directional antenna attack, which leads us to propose the *AMS* scheme.

For *FMS* scheme to be effective, an appropriate transmit power of the AP should be identified and selected according to the surrounding physical environments. For example, if the AP is in a room with thick concrete walls, signals received by an attacker outside the room will be highly attenuated. However, a room with glass walls will attenuate signals minimally, leaving chances for the attacker. Therefore, in an environment where attenuation by proximity boundary (e.g., walls) is low, the AP should use a lower transmit power to lower the SNR at the attacker and distinguish between the user in the room and the attacker outside the room. At the same time, it should have the transmit power strong enough to provide reliable connectivity to legitimate devices. To determine the proper transmit power, we follow the WINNER-II channel model [26] which provides a path loss model suitable for office environments. According to the WINNER-II channel model, the path loss, PL is expressed as,

$$PL = A\log(d) + B + C\log(f_c/5.0), \tag{1}$$

where A is the filtering parameter that includes the path loss exponent, B is the intercept parameter, C is the parameter that describes the path loss frequency dependence, and f_c is the frequency band. As we use 2.4 GHz frequency band in the experiments, f_c is 2.4. In indoor LoS and NLoS environments, A is 18.7 and 36.8, B is 46.8 and 43.8, respectively and C in both environments is 20. By using this path loss model, we can easily calculate the RSSI at the legitimate device, P_{R_L} as,

$$P_{R_L} = P_T + G_T + G_R - PL, \tag{2}$$

where P_T is the transmit power of the transmitter (i.e., the AP in *FMS*), G_T is the transmit gain of the transmitter's antenna, and G_R is the receive gain of the receiver's antenna (i.e. a user device or an attacker in *FMS*). Then, by subtracting noise of legitimate device P_{N_L}, the SNR at the legitimate device is expressed as,

$$P_{R_L} - P_{N_L} = P_T + G_T + G_R - PL - P_{N_L}. \tag{3}$$

Since we should let the legitimate device properly decode high MCS level used in *FMS*, the SNR at the legitimate device should meet the following condition:

$$P_T + G_T + G_R - 18.7\log(d_L) - 46.8 - 20\log(2.4/5.0) - P_{N_L} \geq SNR_{MCS}, \tag{4}$$

where SNR_{MCS} is the minimum required SNR to decode the MCS level used in *FMS*, and d_L is the distance between the AP and the legitimate device. At the same time, we should ensure that the attacker is unable to decode our MCS level. To isolate the NLoS attacker by preventing it from decoding high MCS level used in *FMS*, the transmit power of the AP should be

[2]In our prototype implementation, we use 100 authentication challenge messages of 100 bytes each, and authenticate the device if 90% or more responses are valid.

adjusted to satisfy the following condition:

$$P_T + G_T + G_R - 36.8\log(d_A) - 43.8 - 20\log(2.4/5.0) - P_{N_L} - NF < \textit{SNR}_{\textit{MCS}}, \tag{5}$$

where d_A is the distance between the AP and the attacker and NF is the noise figure of the amplifier. Finally, we can derive the range of AP's transmit power that makes *FMS* effective.

$$\begin{aligned} &36.8\log(d_A) + 43.8 + 20\log(2.4/5.0) + P_{N_L} + NF \\ &+ \textit{SNR}_{\textit{MCS}} - G_T - G_R > P_T \geq 18.7\log(d_L) + 46.8 \\ &+ 20\log(2.4/5.0) + P_{N_L} + \textit{SNR}_{\textit{MCS}} - G_T - G_R. \end{aligned} \tag{6}$$

Based on this principle, we can choose an appropriate transmit power of the AP depending on the environment.

B. Authentication Motion and Signal Strength Gap based Filtering (AMS)

Although *FMS* scheme is highly effective and convenient in defending against the amplifier attack, it may not be secure enough against the directional antenna attack. To overcome this problem, we propose *AMS* scheme that requires the AP to have at least two antennas. Without loss of generality, we will call them Ant.1 and Ant.2 hereafter. *AMS* also requires a simple motion from the user for authentication; The user who wants to have his/her device authenticated needs to move the device from Ant.1 to Ant.2 at a close distance to the AP at the time of authentication (e.g., connection establishment phase). Then the gap between the RSSIs at Ant.1 and Ant.2, $\textit{GAP}_{1\to2}$ is measured as the device moves[3]. The key intuition is that, as the device moves, $\textit{GAP}_{1\to2}$ will change significantly when the device is in proximity to the AP, but will not differ much otherwise. Using this fact, the AP can authenticate the device when the difference in $\textit{GAP}_{1\to2}$ is above a certain threshold, Th_{gap}.

Fig. 2 illustrates how *AMS* scheme works. Let l be the distance between the two antennas of the AP. x ($0 \leq x \leq l$) is the moved distance of the device, y is the perpendicular distance between the AP and the device, and d_1 and d_2 are the distances from the device to Ant.1 and Ant.2, respectively. As the device moves by x from Ant.1 to Ant.2, the received power P_{R_1} at Ant.1 and the received power P_{R_2} at Ant.2 can be given by

$$\begin{aligned} P_{R_1}(x) &= P_T + G_T + G_R - PL(d_1), \\ P_{R_2}(x) &= P_T + G_T + G_R - PL(d_2). \end{aligned} \tag{7}$$

Since the user device is the transmitter and the AP is the receiver in *AMS*, P_T is the transmit power of the device, G_T is the transmit gain of the device's antenna, G_R is the receive gain of the AP's antenna, and $PL(d)$ is the path loss between the device and the AP at distance d.

From (1), the path loss $PL(d)$ can be simplified as,

$$PL(d) = D\log(d) + E, \tag{8}$$

where parameters D and E depend on the frequency and environment. However, most path loss models including WINNER-II are described for the *far-field* where the distances are much larger than the wavelength. In the *near-field* where the radius is a few wavelengths or less, those path loss models may not be generally applicable [27]. Nevertheless, Ohira et al. demonstrated that path loss can be linearly proportional to $log(d)$ also in the near-field [28]. To verify that (8) can be applied to our model in the near-field, we measured RSSI values at varying distances between the AP and a device from 10 mm to 50 mm in line-of-sight. Fig. 3 plots the RSSI at one antenna of the AP on the log scale $log(d)$. The result shows that RSSI is linearly proportional to $log(d)$, and since P_T, G_T, and G_R are constants, path loss is also linear with respect to $\log(d)$ in the near-field. This implies that (8) can be used also in the near-field, and we can determine D as approximately 21.8 from this measurement.

From (7), (8), and the Pythagorean theorem, $\textit{GAP}_{1\to2}$ after the device moves by x, $\textit{GAP}_{1\to2}(x)$, can be calculated as,

$$\begin{aligned} \textit{GAP}_{1\to2}(x) &\overset{\text{def}}{=} P_{R_1}(x) - P_{R_2}(x) \\ &= A\log\left(\frac{\sqrt{(l-x)^2 + y^2}}{\sqrt{x^2+y^2}}\right). \end{aligned} \tag{9}$$

As the device moves from Ant.1 to Ant.2 (i.e. x increases from 0 to l), d_1 increases from y to $\sqrt{l^2+y^2}$ and d_2 decreases from $\sqrt{l^2+y^2}$ to y. Therefore, d_2/d_1 and $\textit{GAP}_{1\to2}(x)$ decrease as the device moves. To this end, we use $\mathcal{GAP}_{\text{diff}}$, the difference of $\textit{GAP}_{1\to2}(x)$ as the device moves from x=0 to x=l, for authentication. Specifically, *AMS* authenticates a device as legitimate if $\mathcal{GAP}_{\text{diff}}$ is above the authentication gap threshold Th_{gap}. From (9), $\mathcal{GAP}_{\text{diff}}$ can be calculated as,

$$\begin{aligned} \mathcal{GAP}_{\text{diff}} &\overset{\text{def}}{=} \textit{GAP}_{1\to2}(0) - \textit{GAP}_{1\to2}(l) \\ &= A\log\left(1 + \frac{l^2}{y^2}\right). \end{aligned} \tag{10}$$

Thus, shorter y and longer l will exhibit greater $\mathcal{GAP}_{\text{diff}}$ for less ambiguity in authentication.

However, there is a small but non-negligible chance that even a random movement by an attacker may happen to have $\mathcal{GAP}_{\text{diff}}$ above the threshold Th_{gap} by accident. The attacker then may succeed after several attempts. Therefore, *AMS* additionally checks the trend of $\textit{GAP}_{1\to2}(x)$. Differentiating $\textit{GAP}_{1\to2}(x)$ with x, we obtain $\frac{d}{dx}\textit{GAP}_{1\to2}(x)$ as,

$$\frac{d}{dx}\textit{GAP}_{1\to2}(x) = -\frac{A}{\ln 10}\left(\frac{l-x}{(l-x)^2+y^2} + \frac{x}{x^2+y^2}\right). \tag{11}$$

We already know that A is positive and 0≤x≤l, $\frac{d}{dx}\textit{GAP}_{1\to2}(x)$ is non-positive which indicates that $\textit{GAP}_{1\to2}$ should decrease when the motion is performed. Thus, *AMS* scheme checks whether $\textit{GAP}_{1\to2}$ decreases monotonically.

To confirm that $\textit{GAP}_{1\to2}$ is monotonically decreasing, *AMS* detects and counts the number of times that the $\textit{GAP}_{1\to2}$ decreases by more than 0.2 dB consecutively (i), or increases by more than 0.3 dB (j). If $\textit{GAP}_{1\to2}$ decreases by more than 0.2 dB for Th_{dec} consecutive times (i.e. $i \geq Th_{\text{dec}}$), *AMS* regards it

[3]Extending this to work with motion from Ant.2 to Ant.1, thus with $\textit{GAP}_{2\to1}$, is trivial.

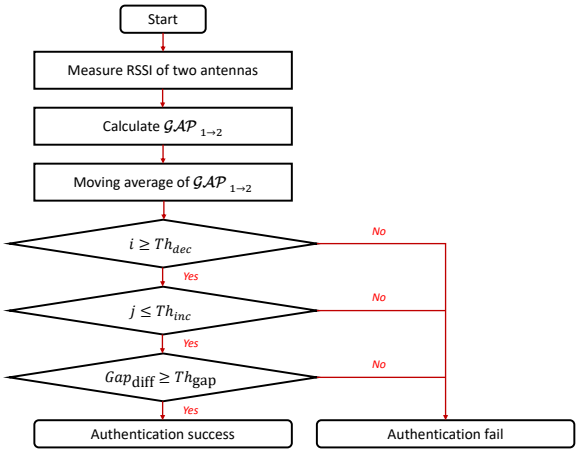


Fig. 4. Authentication procedure of *AMS* scheme at the AP.

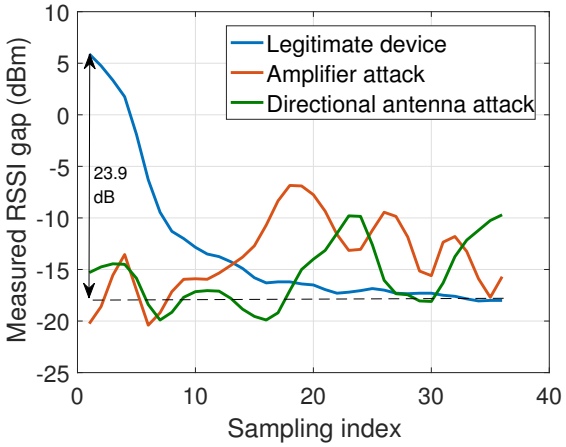
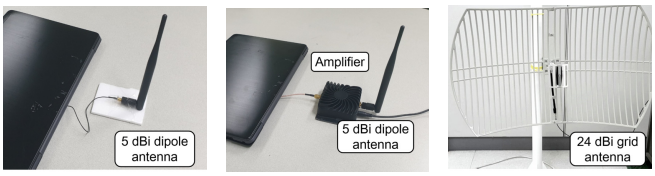


Fig. 5. Example of $GAP_{1\to2}$ variation for the legitimate device, the amplifier attacker, and the directional antenna attacker in *AMS* scheme.



(a) (b) (c)

Fig. 6. Experimental equipment of the legitimate device, the amplifier attack (amp. attack), and the directional antenna attack (dir. attack): (a) Legitimate device, (b) amp. attack, and (c) dir. attack.

Table 1. Device parameters.

Device	Parameter	Value
Common	Frequency	2.4 GHz
	Channel bandwidth	20 MHz
Legitimate device &AP	Transmit power	5 dBm
	Antenna gain	5 dBi
Amplifier attack	Transmit power	16 dBm
	Antenna gain	5 dBi
	Transmit gain	17 dB
	Receive gain	11 dB
	Noise figure	3 dB
Directional antenna attack	Transmit power	16 dBm
	Antenna gain	24 dBi

as a legitimate motion. If it increases by more than 0.3 dB for more than Th_{inc} times (i.e. $j > Th_{\text{inc}}$), *AMS* regards it as illegal or irrelevant.

Fig. 4 illustrates the protocol procedure of *AMS*. When a device to be authenticated sends an authentication request message (e.g., as part of the connection establishment phase), the AP responds to initiate authentication. Then the device sends packets continuously to the AP (until authentication timeout period, 2 seconds in our prototype) during which the user can make a motion. The AP measures the RSSI of signals received from each antenna and calculates the RSSI gap (i.e., $GAP_{1\to2}$) between the two antennas. A simple moving average technique is utilized to suppress minor RSSI fluctuation. The authentication timeout period can be adjusted based on the application requirement; increasing it provides more convenience to the user, but also more chances to the attacker at the same time.

To verify the feasibility of this approach and find appropriate parameters, Fig. 5 shows an example of how $GAP_{1\to2}$ changes for a legitimate device, an amplifier attacker, and a directional antenna attacker. The distance between the AP and the legitimate device is 5 cm, and both attackers are 5 m away from the AP and in NLoS. Two antennas of the AP are 10 cm apart. The amplifier attacker moves 1 m to make a motion and the directional antenna attacker rotates continuously at random in a hope to create a legit-mimicking motion. In the case of the legitimate device, authentication succeeds since $GAP_{1\to2}$ is continuously reduced and the total difference $\mathcal{GAP}_{\text{diff}}$ is sufficiently large (23.9 dB). On the other hand, attackers fail to authenticate because $GAP_{1\to2}$ fluctuates severely, and $\mathcal{GAP}_{\text{diff}}$ is relatively small. Based on these empirical findings (and more in Section V.D), we set Th_{dec} to 5, Th_{inc} to 3, and Th_{gap} to 10 dB by default in our prototype implementation and experiments.

In summary, *AMS* scheme authenticates a device when the spatial RSSI gap between the two antennas (i.e. $GAP_{1\to2}$) decreases monotonically as the device moves (i.e. $i \geq Th_{\text{dec}}$ && $j \leq Th_{\text{inc}}$) and the total temporal change of RSSI gap (i.e. $\mathcal{GAP}_{\text{diff}}$) is above Th_{gap}.

C. Limitations

A user employing the *FMS* scheme may need to adjust the transmit power of the AP depending on the surrounding environment, which may seem cumbersome and impractical. Furthermore, *AMS* scheme requires a user motion at a close distance from the AP, which may also seem to as inconvenience to the user. However, we show in Section V that *FMS* scheme defends against the amplifier attack well by setting the transmit power to one of three values depending on the environment. Moreover, we believe that the motion required by *AMS* is no more complicated than other authentication methods (e.g., complex password input) since it is required only once. Thus, we believe that these are only a small one-time price paid for the long-run convenience of secure proximity-based authentication it brings.

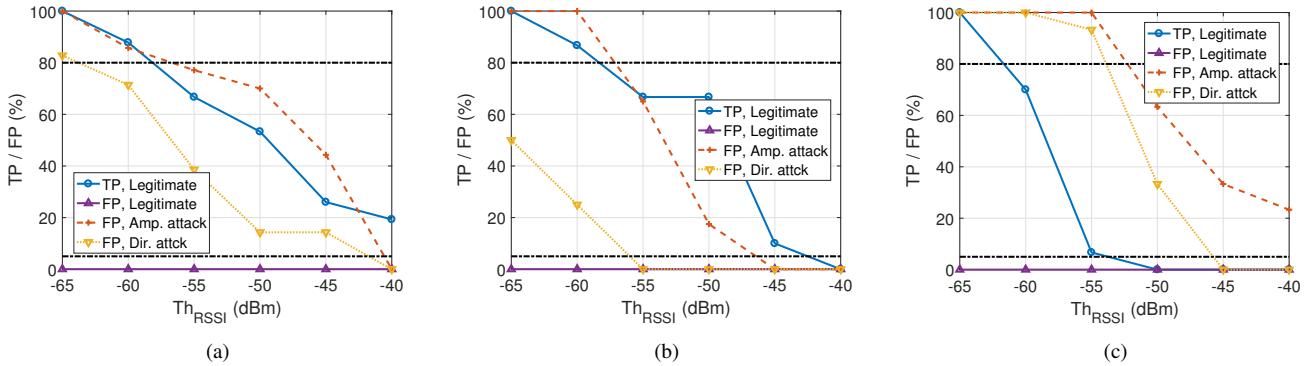


Fig. 7. True-positive (TP) and false-positive (FP) detection rates of the legitimate device, amplifier attacker (Amp. attack), and directional antenna attacker (Dir. attack) in three different cases with RSSI filtering according to Th_{RSSI}: (a) Full-blocked, (b) semi-blocked, and (c) glass-walled

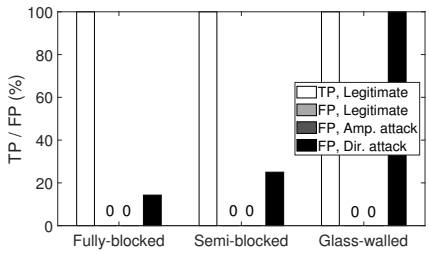


Fig. 8. True-positive (TP) and false-positive (FP) rates of *FMS* scheme with AP's transmit power of 5 dBm in fully-blocked, 0 dBm in semi-blocked, and -7 dBm in glass-walled cases.

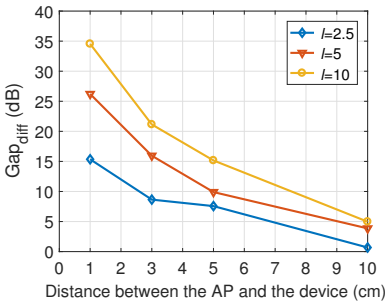


Fig. 9. $\mathcal{GAP}_{\text{diff}}$ according to the distance between the AP's two antennas and between the AP and the device.

V. EVALUATION

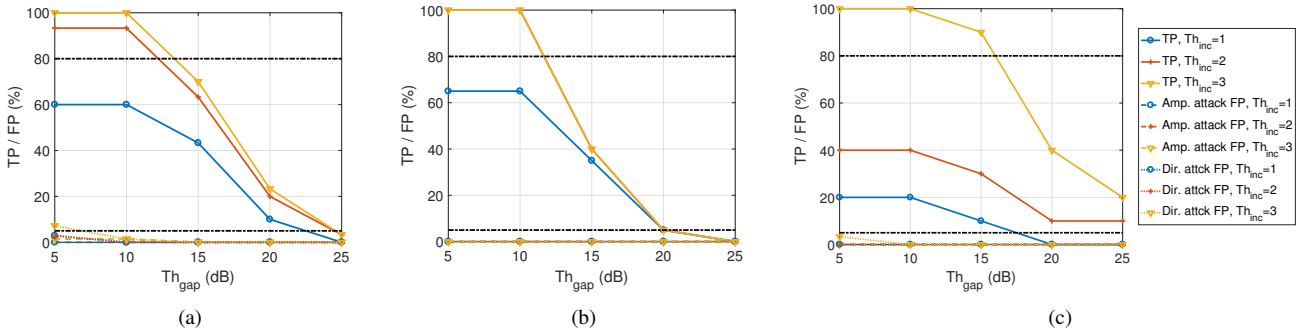
In this section, we first show the feasibility of attacks on RSSI-based authentication, and how our proposed schemes defeat the attacks in various environments.

A. Experiment Setup

We conduct experiments in five environments: an office, a stair room, a lecture room, a seminar room, and a cafe. An AP is located inside each environment and an attacker which acts as either an amplifier attacker or a directional antenna attacker attempts to be authenticated at a total of 14 different locations outside the environments. Table 2 lists 14 different locations of the attacker. At each location, the attacker is placed at least 5 m away from the AP. We categorize the attacker's location into three classes: (1) fully-blocked, (2) semi-blocked, and (3) glass-walled, according to the material of obstacles (e.g., walls, doors, and windows) between the attacker and the AP. 'Fully-blocked' is a case with concrete or metal walls and doors, 'semi-blocked' is a fully-blocked environment with glass windows, and 'glass-walled' is a case with glass walls or doors. Authentication range is internal to each environment. The goal is to achieve above 80% true-positive (TP) rate for a legitimate device inside the same room with the AP, and below 5% false-positive (FP) rates for the two attacks as well as a normal (same as legit) device outside the room. To measure TP and FP rates, a legitimate device attempts authentication 30 times in the same room with the AP, and the two attackers and a normal device attempt authentication 10 times each (30 total) at each attacker's location.

Fig. 6 shows experimental equipment of the legitimate device, the amplifier attack, and the directional antenna attack that are used in our experiments. All attackers, AP, and legitimate devices are IEEE 802.11n devices on 2.4 GHz band, implemented on laptops each with an AR9380 network interface card (NIC). The AP and legitimate devices are equipped with 5 dBi dipole antennas. To implement the amplifier attack, we use an amplifier with 17 dB transmit gain, 11 dB receive gain, and 3 dB noise figure (NF). A 5 dBi dipole antenna is connected to the amplifier. Directional antenna attack uses a 24 dBi grid antenna. Transmit power of the legitimate device is 5 dBm. That of the AP is 5 dBm by default but adaptable to the environment. Attackers can use higher transmission power than legitimate devices to attack. In our experiments, the transmit power of the attackers before the amplification is 16 dBm, and after the amplification it is 38 dBm for the amplifier attacker and 40 dBm for the directional antenna attacker. Table 1 summarizes parameters of the devices used in experiments.

It is assumed that attackers know the authentication procedure and can imitate legitimate devices. When *FMS* is used, an attacker attempts to decode the received authentication packets and respond back to the AP as if it is a legitimate device. When *AMS* is used, an amplifier attacker tries to mimic a legitimate device by making a larger motion (1 m motion in the experiments), and a directional antenna attacker uses (somewhat arbitrary) rotation to mimic a legitimate device because it has difficulty in creating a large hand-gesture-like motion due to its big size.



(a) (b) (c)

Fig. 10. True-positive (TP) and false-positive (FP) rates of the legitimate device, amplifier attack (Amp. attack), and directional antenna attack (Dir. attack) in three different cases with *AMS* scheme according to Th_{gap} and Th_{inc}: (a) Fully-blocked, (b) semi-blocked, and (c) glass-walled.

B. RSSI Filtering

First, we examine the performance of RSSI filtering as a comparison scheme. RSSI filtering authenticates a device when the averaged RSSI at the AP exceeds a certain threshold, Th_{RSSI}. Fig. 7 shows the TP and FP rates of the legitimate device, and also the FP rates of the attackers in three different cases according to Th_{RSSI}. If there is no attack, RSSI filtering successfully determines whether a device is within the authentication range or not. If we set Th_{RSSI} to -65 dBm, TP of a legitimate device is 100% and its FP is 0% in all cases.

However, when there is the amplifier attack or the directional antenna attack, RSSI filtering fails to achieve TP rate of greater than 80% and FP rate of less than 5% simultaneously. In the fully-blocked case, if we set the threshold to -40 dBm in order to keep FP rates less than 5%, the TP rate drops to 20%, greatly reducing user convenience. If we set the threshold to -60 dBm in order to have TP greater than 80%, RSSI filtering becomes vulnerable to the two attacks with FP rates of 85.7% and 71.4% under amplifier and directional antenna attacks, respectively. In the glass-walled case, the attacker's FP rates are even higher than the TP rates of the legitimate device since the attacker amplifies the signals more than the attenuation by obstacles. These results indicate not only that RSSI filtering is vulnerable to both attacks, but also finding the optimal threshold parameter is not possible.

C. FMS *Scheme*

Unlike RSSI filtering which uses solely the signal strength measured by the AP for authentication, SNR of the signal received by the device is important in *FMS* scheme. Since the attackers cannot control the transmit power of the AP, *FMS* scheme is less vulnerable to attacks than RSSI filtering.

By adjusting the transmit power and MCS of the AP, *FMS* scheme can adjust the authentication range according to the environment such as the material of walls or the size of a room. For example, in the glass-walled case, signals are less attenuated by the wall than in the fully-blocked case. Therefore, in order to confine the authentication range to the room, the AP should use lower transmit power in the glass-walled case than the fully-blocked case.

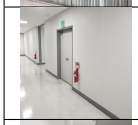
Fig. 8 plots the TP and FP rates of a legitimate device, and also the FP rates of the two attacks in three cases. Transmit power of the AP is set to 5 dBm in the fully-blocked case, 0 dBm in the semi-blocked case, and -7 dBm in the glass-walled case. In all cases, the TP rate of a legitimate device is 100% and the FP is 0%. This shows that *FMS* scheme successfully authenticates devices within and only within proximity when there is no attack. Furthermore, *FMS* scheme defends perfectly against the amplifier attack with FP rates of 0% in all cases. However, it opens doors to the directional antenna attack at some locations (35.7%). The FP rate of the directional antenna attack is higher in the order of glass-walled, semi-blocked and fully-blocked. This is because the directional antenna should be pointed to the AP correctly for a successful attack, which is easier in the glass-walled case. Moreover, signal amplification is not performed properly depending on the material of the wall.

D. AMS *Scheme*

For *AMS* scheme to be effective, proper values for Th_{gap} and Th_i parameters should be determined. For this purpose, we first examine $\mathcal{GAP}_{\text{diff}}$ according to the distance between the AP and the device. We measure the total RSSI gap (i.e., $\mathcal{GAP}_{\text{diff}}$) at distances between the AP's antennas (i.e., l) of 2.5 cm, 5 cm and 10 cm, and distances between the AP and the device (i.e., y) of 1 cm, 3 cm, 5 cm, and 10 cm. Fig. 9 confirms that $\mathcal{GAP}_{\text{diff}}$ increases as y decreases and l increases, as conjectured. That is, $\mathcal{GAP}_{\text{diff}}$ becomes larger as the distance between the AP's antennas increases and/or the distance between the AP and the device becomes shorter, which is consistent with the analysis in Section IV.B. Based on this finding, we set l to 10 cm and y to 5 cm in the following experiments.

Fig. 10 shows the performance of *AMS* scheme according to varying Th_{gap} and Th_i in three different cases. Stricter thresholds lower the authentication success rates for both legitimate devices and attackers. As Th_i becomes smaller and Th_{gap} becomes larger, FP rates of the attackers and TP rate of the legitimate device become smaller. This means that smaller Th_i and larger Th_{gap} help to defeat the attacks more (improved security), but lead to lowered authentication success rate of legitimate devices (worse user convenience). We can satisfy TP rates of more than 80% and FP rates of less than 5% in all cases by setting Th_i to 3 and Th_{gap} to 10 dB. Using these parameter selection, the results show that *AMS* scheme can effectively and successfully defend against both attacks in all 14 attacker location cases.

Table 2. Experimental environments.

Attacker's location	Environment	Material of obstacles	Category
	Office	Metal	Fully-blocked
	Office	Metal	Fully-blocked
	Office	Metal	Fully-blocked
	Cafe	Concrete	Fully-blocked
	Cafe	Glass and concrete	Semi-blocked
	Lecture room	Metal, concrete and glass	Semi-blocked
	Lecture room	Metal, concrete and glass	Semi-blocked
	Lecture room	Metal, concrete and glass	Semi-blocked
	Seminar room	Glass	Glass-walled
	Seminar room	Glass	Glass-walled
	Seminar room	Glass	Glass-walled
	Stair room	Metal and concrete	Fully-blocked
	Stair room	Metal and concrete	Fully-blocked
	Stair room	Metal and concrete	Fully-blocked

VI. CONCLUSION

We investigated attack models to a proximity-based authentication system in which adversary devices strengthen their signals to mimic a legitimate device. We have shown that amplifier attack and directional antenna attack exhibit different link characteristics, and this can be exploited to design countermeasures. To defend against these attacks, we proposed two lightweight proximity-based authentication schemes, *FMS* and *AMS*, that can be used during connection establishment phase of wireless network access. We implemented both schemes in COTS IEEE 802.11n devices and evaluated their performance in various environments through real-world experiments. Our results show that the proposed schemes successfully defend against the attacks while maintaining 100% true-positive rate. *FMS* defends against the amplifier attack in all cases and *AMS* defeats both attacks in all cases with the help of a simple user gesture. *FMS* or *AMS* scheme can be selected according to the application requirement to enhance the security of proximity-based authentication in upcoming IoT.

As future work, we plan to explore utilizing CSI information for more accurate ranging and gesture recognition to enhance the security and convenience of our schemes even further. We also plan to add human differentiation that provide authentication by distinguishing different users.

REFERENCES

[1] S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in Internet of Things," *J. Commun. Netw.*, vol. 20, no. 3, pp. 291–298, June 2018.

[2] E. L. C. Macedo, E. A. R. de Oliveira, F. H. Silva, R. R. Mello, F. M. G. França, F. C. Delicato, J. F. de Rezende, and L. F. M. de Moraes, "On the security aspects of Internet of Things: A systematic literature review," *J. Commun. Netw.*, vol. 21, no. 5, pp. 444–457, Oct. 2019.

[3] J. Heo, J. Kim, J. Paek, and S. Bahk, "Mitigating stealthy jamming attacks in low-power and lossy wireless networks," *J. Commun. Netw.*, vol. 20, no. 2, pp. 219–230, Apr. 2018.

[4] H. Alipour and R. P. Marreel, "System, apparatus, and method for received signal strength indicator (RSSI) based authentication," May 25 2017, US Patent App. 15/354,738.

[5] M. Kim, J. Lee, and J. Paek, "Neutralizing BLE Beacon-based Electronic Attendance System using Signal Imitation Attack," *IEEE Access*, vol. 6, pp. 77 921–77 930, Dec. 2018.

[6] M. Zhou, M. Ma, Y. Zhang, K. SuiA, D. Pei, and T. Moscibroda, "EDUM: Classroom Education Measurements via Large-scale WiFi Networks," in *Proc. ACM UbiComp*, 2016, pp. 316–327.

[7] P. Zand, J. Romme, J. Govers, F. Pasveer, and G. Dolmans, "A high-accuracy phase-based ranging solution with Bluetooth Low Energy (BLE)," in *Proc. IEEE WCNC*, 2019.

[8] P. Sapiezynski, A. Stopczynski, D. K. Wind, J. Leskovec, and S. Lehmann, "Inferring person-to-person proximity using WiFi signals," in *Proc. ACM IMWUT*, vol. 1, no. 2, pp. 1–20, 2017.

[9] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. ACM MobiCom*, 2008.

[10] C. Sahin, B. Katz, and K. R. Dandekar, "Secure and robust symmetric key generation using physical layer techniques under various wireless environments," in *Proc. IEEE RWS*, 2016.

[11] J. Choi, "Secret key transmission for OFDM based machine type communications," *J. Commun. Netw.*, vol. 19, no. 4, pp. 363–370, Aug. 2017.

[12] Y. Wang and Z. Shi, "Channel reciprocity and capacity analysis with outdoor MIMO measurements," in *Proc. IEEE SPAWC*, 2017, pp. 1–5.

[13] N. Ghose, L. Lazos, and M. Li, "Sfire: Secret-free-in-band trust establishment for cots wireless devices," in *Proc. IEEE INFOCOM*, 2018, pp. 1529–1537.

[14] T. J. Pierson, T. Peters, R. Peterson, and D. Kotz, "Proximity detection with single-antenna IoT devices," in *Proc. ACM MobiCom*, 2019, pp. 1–15.

[15] A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara, "Amigo: Proximity-based authentication of mobile devices," in *Proc. ACM UbiComp*, Berlin, Heidelberg, 2007, pp. 253–270.

[16] L. Cheng and J. Wang, "How can i guard my AP?: Non-intrusive user identification for mobile devices using wifi signals," in *Proc. ACM MobiHoc*, 2016, pp. 91–100.

[17] C. Castelluccia and P. Mutaf, "Shake them up!: A movement-based pairing protocol for CPU-constrained devices," in *Proc. ACM MobiSys*, 2005.
[18] Y. Nishida, "Proximity motion detection using 802.11 for mobile devices," in *Proc. IEEE PORTABLE*, 2007, pp. 1–5.
[19] J. Zhang, Z. Wang, Z. Yang, and Q. Zhang, "Proximity based IoT device authentication," in *Proc. IEEE INFOCOM*, 2017, pp. 1–9.
[20] Y. Shen, F. Yang, B. Du, W. Xu, C. Luo, and H. Wen, "Shake-n-shack: Enabling secure data exchange between smart wearables via handshakes," in *Proc. IEEE PerCom*, 2018, pp. 1–10.
[21] J. Han, A. J. Chung, M. K. Sinha, M. Harishankar, S. Pan, H. Y. Noh, P. Zhang, and P. Tague, "Do you feel what i hear? enabling autonomous IoT device pairing using different sensor types," in *Proc. IEEE SP*, 2018, pp. 836–852.
[22] C. Dimitrakakis and A. Mitrokotsa, "Distance-bounding protocols: Are you close enough?" *IEEE Security Privacy*, vol. 13, no. 4, pp. 47–51, July 2015.
[23] C. Wu, Z. Yang, Z. Zhou, K. Qian, Y. Liu, and M. Liu, "PhaseU: Real-time LOS identification with WiFi," in *Proc. IEEE INFOCOM*, 2015, pp. 2038–2046.
[24] "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput," pp. 1–565, Oct. 2009.
[25] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. Allerton*, 2009, pp. 911–918.
[26] J. Meinilä, P. Kyösti, T. Jämsä, and L. Hentilä, *WINNER II Channel Models*. John Wiley & Sons, Ltd, 2009, ch. 3, pp. 39–92.
[27] H. G. Schantz, "Near field propagation law amp; a novel fundamental limit to antenna gain versus size," in *Proc. IEEE APS*, 2005, pp. 237–240.
[28] M. Ohira, T. Umaba, S. Kitazawa, H. Ban, and M. Ueba, "Experimental characterization of microwave radio propagation in ICT equipment for wireless harness communications," *IEEE Trans. Antennas Propag.*, vol. 59, no. 12, pp. 4757–4765, Dec. 2011.

Jeongyoon Heo received the B.S. degree in Electrical Engineering from Korea University, Seoul, South Korea, in 2013 and the Ph.D. degree at the School of Computer Science and Electrical Engineering, Seoul National University, Seoul, South Korea, in 2019. She is currently a Staff Engineer at SAMSUNG Research, Samsung Electronics Co.,Ltd., Republic of Korea, where she has worked since 2019. Her research interests include the area of network security, wireless networks, Internet of Things, localization, authentication, vehicle-to-everything (V2X) and 5G.

Yongjae Yoo is currently a master course student at the School of Electrical and Computer Engineering, Seoul National University, Seoul, Republic of Korea. He received B.S. degree in Electrical and Computer Engineering from Seoul National University in 2019. His research interests are in the area of security and machine learning in wireless networks, Internet of Things and 5G networks.

Jihwan Suh is currently a Ph.D. student at the School of Electrical and Computer Engineering, Seoul National University, Seoul, Republic of Korea. He received his B.E. degree in the field of Informatics and Mathematical Science from Kyoto University in 2013. His research interests are in the area of security, localization, and 5G with AI.

Woojin Park received the B.E., M.S., and Ph.D. degrees from Korea University, Seoul, Republic of Korea, in 2000, 2002, and 2007, respectively. He is currently a Principal Engineer at SAMSUNG Research, Samsung Electronics Co.,Ltd., Republic of Korea, where he has worked since 2007. His research interests are focused on cellular networks, computer network, and network security. The current target scenarios include network traffic-driven anomaly detection and security protocols between smart devices and 5G RAN products.

Jeongyeup Paek received his B.S. degree from Seoul National University, Seoul, Republic of Korea, in 2003 and the M.S. degree from the University of Southern California, Los Angeles, CA, USA, in 2005, both in electrical engineering. He then received the Ph.D. degree in Computer Science from the University of Southern California in 2010. He joined Cisco Systems, Inc. in 2011, where he was a Technical Leader in the Internet of Things Group, Connected Energy Networks Business Unit (formerly the Smart Grid Business Unit). In 2014, he was with the Hongik University, Department of Computer Information Communication as an Assistant Professor. He is currently an Associate Professor at Chung-Ang University, School of Computer Science and Engineering, Seoul, South Korea.

Saewoong Bahk received the B.S. and M.S. degrees in Electrical Engineering from Seoul National University (SNU), in 1984 and 1986, respectively, and the Ph.D. degree from the University of Pennsylvania, in 1991. He was with AT&T Bell Laboratories as a Member of Technical Staff, from 1991 to 1994, where he had worked on network management. From 2009 to 2011, he served as the Director of the Institute of New Media and Communications. He is currently a Professor at SNU. He has been leading many industrial projects on 3G/4G/5G and the IoT connectivity supported by Korean industry. He has published more than 200 technical articles and holds more than 100 patents. He is a member of the National Academy of Engineering of Korea (NAEK) and of Whos Who Professional in Science and Engineering. He was a recipient of the KICS Haedong Scholar Award, in 2012. He is President of the Korean Institute of Communications and Information Sciences (KICS). He has been serving as Chief Information Officer (CIO) of SNU and General Chair of the IEEE WCNC 2020 (Wireless Communication and Networking Conference). He was General Chair of the IEEE DySPAN 2018 (Dynamic Spectrum Access and Networks) and Director of the Asia-Pacific Region of the IEEE ComSoc. He is an Editor of the IEEE Network Magazine. He was TPC Chair of the IEEE VTC-Spring 2014, and General Chair of JCCI 2015, Co-Editor-in-Chief of the Journal of Communications and Networks (JCN), and on the Editorial Board of Computer Networks Journal (COMNET) and the IEEE Tran. on Wireless Communications (TWireless).