Hold the Door! Fingerprinting Your Car Key to Prevent Keyless Entry Car Theft

Kyungho Joo*
Korea University
khjoo0512@gmail.com

Wonsuk Choi*
Korea University
wonsuk85.choi@gmail.com

Dong Hoon Lee
Korea University
donghlee@korea.ac.kr

Abstract—Recently, the traditional way to unlock car doors has been replaced with a keyless entry system which proves more convenient for automobile owners. When a driver with a key fob is in the vicinity of the vehicle, doors automatically unlock on user command. However, unfortunately, it has been shown that these keyless entry systems are vulnerable to signal-relaying attacks. While it is evident that automobile manufacturers incorporate preventative methods to secure these keyless entry systems, they continue to be vulnerable to a range of attacks. Relayed signals result in valid packets that are verified as legitimate, and this makes it is difficult to distinguish a legitimate door unlock request from a malicious signal. In response to this vulnerability, this paper presents an RF-fingerprinting method (coined "HOld the DOoR", HODOR) to detect attacks on keyless entry systems - the first attempt to exploit the RF-fingerprint technique in the automotive domain. HODOR is designed as a sub-authentication method that supports existing authentication systems for keyless entry systems and does not require any modification of the main system to perform. Through a series of experiments, the results demonstrate that HODOR competently and reliably detects attacks on keyless entry systems. HODOR achieves both an average false positive rate (FPR) of 0.27% with a false negative rate (FNR) of 0% for the detection of simulated attacks, corresponding to current research on keyless entry car theft. Furthermore, HODOR was also observed under environmental factors: temperature variation, non-line-of-sight (NLoS) conditions, and battery aging. HODOR yields a false positive rate of 1.32% for the identification of a legitimated key fob even under NLoS conditions. Based on the experimental results, it is expected that HODOR will provide a secure service for keyless entry systems, while remaining convenient.

I. Introduction

Recently, keyless entry systems have been developed and installed in modern vehicles for the convenience of drivers. Before the keyless entry system, it was necessary to physically insert a key into the key hole to unlock the doors of a vehicle. This traditional way to unlock doors was inconvenient as well as vulnerable to physical key copying leading to relatively easy automotive theft or break-ins. The keyless entry system enables a driver to unlock doors without inserting anything, via two distinct systems: the remote keyless entry (RKE) system and the passive keyless entry and start (PKES) system. The RKE system unlocks doors with the press of a button on a

remote key fob at a distance. In the PKES system, car doors are automatically unlocked as the user makes physical contact with a button on a door when the key fob is in the vicinity. This implies that drivers no longer need to remove their key fobs from their pockets or bags. We note that the PKES system is mostly designed to include the remote lock and unlock functions provided by the RKE system. However, as keyless entry systems are becoming commonplace on modern vehicles, cyber security attacks are also on the rise. Vehicle manufacturers, therefore, have applied their own security mechanisms to verify either the remotes or key fobs. In particular, encryption with a pre-shared, long-term secret key and rolling codes [37], [64] are common methods used to verify a legitimate key fob.

Despite these security mechanisms, several vulnerabilities with keyless entry systems have been discovered. In 2010, the authors of [38] demonstrated a relay attack on PKES systems, in which vehicle doors were unlocked. In the relay attack, two colluding adversaries would work in concert to extend the original range of RF communication between a vehicle and its key fob. One adversary must be close to the target vehicle and the other must be close to its key fob. They cooperate with each other to relay signals from the vehicle to the key fob side. As a consequence, even outside of the pre-defined communication range, the vehicle and its key fob interact with each other, which leads to the unlocking of the doors. In Germany and the United Kingdom, automotive thieves successfully carried out these types of signal-relaying attacks, which were captured on security cameras [10], [19]. In addition, an adversary could exploit a particular vulnerability of a cryptographic algorithm used in the remote keyless entry system to extract a pre-shared secret key between the vehicle and its key fob, thereby creating and transmitting a malicious message for a door unlock command [22], [40], [45], [47], [61]. Furthermore, recent studies have shown that long-term secrets can be compromised not only in the RKE system but also in the PKES system [66].

The underlying reason of the cyber security attacks on the keyless entry system is that radio frequency (RF) signals emitted from key fobs can be relayed or replayed regardless of active security methods like encryption or authentication. Since the keyless entry system accepts any request for authentication as long as valid signals are within the communication range, extension of the communication range by relaying or forwarding a signal ultimately enables an attacker to unlock car doors. One approach to resolve this issue might be the use of an RF distance-bounding protocol that verifies the actual physical proximity of a request [25], [44]. However, RF distance-

bounding protocols are highly sensitive to timing errors. This is because the distance-bounding protocol measures the distance based on the time of flight (ToF) of an RF signal which propagates at the speed of light. Recently, an ultra-wide band impulse radio (UWB-IR) ranging technique has emerged as a prominent technology to deploy a distance-bounding protocol, and numerous efforts are underway to deploy a secure UWB-IR ranging technique [4], [52], [57], [58]. However, this approach would require the keyless entry system to adopt an entirely new communication system to implement the RF distance-bounding protocol.

To detect attacks on keyless entry systems, we employ an RF fingerprinting technique that extracts fingerprints of individual RF devices from their RF signals. Due to hardware imperfections, distinct characteristics per RF device can be extracted even if they transmit the same binary message. In other areas, RF fingerprinting methods have already been proposed to identify RF devices [26], [30], [31], [55], [68], which are referred to as the ground truth of `HODOR`. These existing methods were designed to identify RF devices in line-of-sight (LoS) and indoor conditions. However, `HODOR` is herein proven to function in both non-line-of-sight (NLoS) and outdoor conditions.

In this paper, we present our evaluations of `HODOR` in detecting attacks on keyless entry systems, including RKE and PKES systems. The method has been designed as a sub-authentication system that supports an existing authentication system. As such, it can be directly applied to a keyless entry system without any modification to the current communication system. Our experimental results show that `HODOR` precisely and accurately detects several types of attack attempts. The detailed contributions of this research are as follows.

- Based on previous attack demonstrations conducted in existing research, we present a new attack model that combines all known attack methods; our attack model covers both PKES and RKE systems. This is the first attempt to formalize existing attacks on keyless entry systems.

- We present an RF fingerprinting method, `HODOR`, to identify legitimate key fobs and detect malicious attempts defined in our attack model. `HODOR` can be easily employed by adding a new device that captures and analyzes the ultra-high frequency (UHF) band RF signals emitted from a key fob, which implies that the current system would require no alterations.

- We performed a series of experiments to evaluate `HODOR`. We simulated malicious attacks that are defined in our attack model with different kinds of RF devices. The experimental results show that `HODOR` is able to correctly detect the attacks, which has an average FPR of 0.27% with an FNR of 0% for the PKES system.

- `HODOR` was also evaluated under varying environmental factors, such as temperature variations, NLoS conditions (e.g., a key fob placed in a pocket) and battery aging. We show that the features we present work properly under these environmental factors, indicating that `HODOR` can be applied in current commonly existing systems.
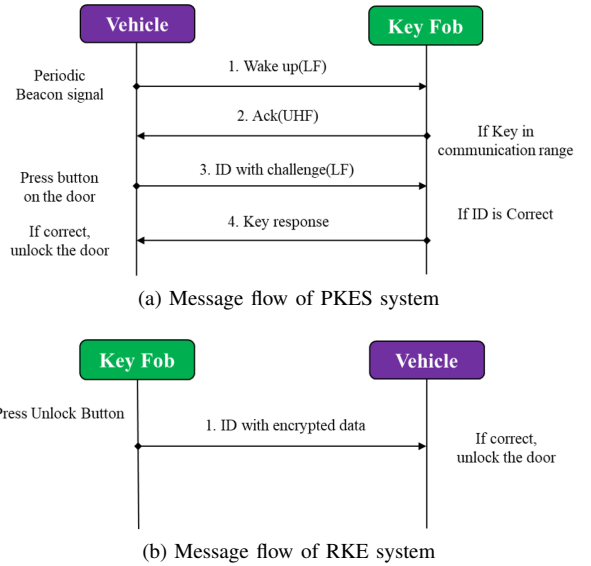

(a) Message flow of PKES system

(b) Message flow of RKE system

Fig. 1: Message flow of each keyless entry system

II. BACKGROUND

To easily understand `HODOR` and our attack model, we describe the background of keyless entry systems and digital communication.

A. Keyless Entry Systems

When a vehicle is equipped with a PKES system, a driver can unlock their doors as long as he/she is in the vicinity of their vehicle. In some cases, a driver must also press a button on the vehicle. Mutual communication between the key fob and vehicle is needed to verify whether the driver is actually nearby. The vehicle then sends a challenge to the key fob via low frequency (LF) band (125 ∼ 135kHz) communication, and the corresponding key fob responds to the request via UHF-band communication. Fig. 1a illustrates an example of the message flow for verification in the PKES system. Vehicles periodically broadcast LF signals to check if a proper key fob is in the vicinity, like beacon signals [41]. In the case that a key fob is within the communication range of an LF band (e.g., 1 ∼ 2m), it receives a periodical LF-band signal from the vehicle which enables it to transmit the response signal in a UHF band. In North America, 315MHz is assigned for the UHF-band, whereas 433.92MHz or 868MHz is assigned in Europe [40]. For security reasons, packets are encrypted with a long-term secret key that is shared between a remote key fob and its corresponding vehicle in advance. It is noted that in the PKES system, a driver is even able to start the engine without inserting a physical key into the ignition switch.

In an RKE system, UHF-band signals from the key fob are transmitted unidirectionally. Only when the driver presses the button on the key fob is the UHF-band signal transmitted. Fig. 1b illustrates an example of the messages flow for verification in the RKE system. The transmission of the same RF signals from a remote key fob is repeated multiple times to increase the reliability of communication [40].
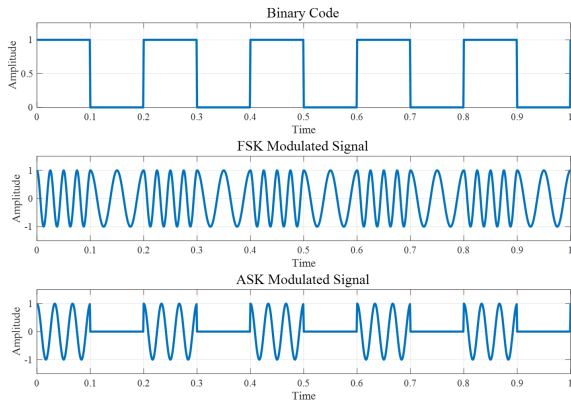
Fig. 2: An example of FSK and ASK modulation

B. Digital Communication

The information source (i.e., binary code) is encoded to be delivered via wireless communication. Next, encoded binary information is mapped into a *symbol* and conveyed to an analog RF signal (the so-called baseband signal) through various modulation schemes. Frequency shift keying (FSK) and amplitude shift keying (ASK) modulation are the most common methods for modulating RF signals in keyless entry systems. Specifically, *symbol* consists of several bits. But in the case of Binary-ASK and Binary-FSK where a *symbol* consists of a single bit, the meaning can be seen as interchangeable. Since most keyless entry systems use BFSK or BASK, for the remainder of this paper, we will use the terms interchangeably.

BFSK expresses bits 0 and 1 by shifting the frequency of the baseband signal by a specific frequency deviation based on the center frequency f_c. The center frequency f_c means the frequency of the carrier signal. A carrier signal is a sinusoidal wave with a carrier frequency. This carrier frequency is defined as standard according to its application and region. That is, f_c of a UHF-band signal is 315MHz or 433.92MHz and f_c of an LF-band signal is $125 \sim 135$Khz. Fig. 2 shows an example of one FSK and one ASK modulated signal corresponding to the binary code. In FSK modulation, if a sinusoidal wave of the frequency $f_c + f_d$, which is higher than the center frequency by f_d indicates bit 1, a sinusoidal wave having a frequency of $f_c - f_d$, which is lower than the center frequency by f_d, indicates bit 0. The f_d indicates the frequency deviation. BASK expresses 0 and 1 bits using the amplitude of sinusoidal with center frequency f_c. If a sine wave having an amplitude of A_0 indicates bit 1, a sine wave having an amplitude of 0 indicates bit 0. Finally, the baseband signal is mixed with a carrier signal and transmitted through an antenna. Since a high-frequency electric signal is emitted from the antenna, the RF signal can be physically transmitted through the air in the form of an electromagnetic wave. At the receiver side, the received signal is processed through a mixer, demodulator, and decoder - reverse order of the transmission process. We refer readers to [59] for further reading on digital communication.

III. System Model

This section presents the system overview, including how HODOR detects malicious attacks on keyless entry systems. For
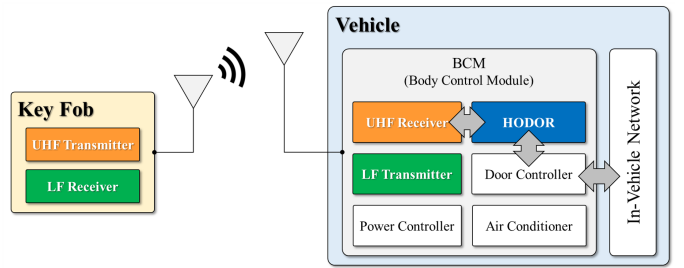

Fig. 3: System model

a clear understanding of HODOR, we define the attack model that simulates the actions of adversaries and their capabilities.

A. System Overview

In this subsection, we present the system overview of HODOR. The vehicle should verify the UHF-band signals emitted from the key fob. Therefore, HODOR should be equipped with an RF receiver and mounted to the vehicle and integrated with the Body Control Module (BCM) of a car which controls various electronic accessories in the car's body. One typical function of BCM is transmitting a lock/unlock command packet through the in-vehicle network communication such as CAN or LIN. In the case of an attack being detected, HODOR raises an attack detection alarm and BCM does not transmit the CAN packet which contains the unlock command. Fig. 3 illustrates the overall system model of HODOR.

B. Attack Models

We present a new attack model for PKES systems. Our attack model covers attacks on PKES systems, which were implemented with the LF/UHF band RFID communication. In addition, our attack model also covers existing demonstrations of attacks on RKE systems using UHF band RFID communication. In our attack model, the main objective of a hypothetical adversary is to unlock a vehicle. For the simplicity of the attack model, we excluded other functions, such as an engine start message. In addition, physical damage to a vehicle is beyond the scope of our attack model, regardless of whether doors are successfully unlocked via a malicious message. Three different types of attacks on PKES systems were outlined in our attack model in regards to how an adversary might deliver a valid message that enables the agent to unlock doors. For a relay attack, we categorized these into **Single-band relay attack** and **Dual-band relay attack**. Two adversaries must collaborate to accomplish either a single-band or dual-band relay attack because relayed signals are used in this model to extend communication range. In a **Cryptographic attack**, however, there is a single adversary who attempts to unlock doors on the keyless entry system. In addition to the attack model on the PKES system, we also considered an attack model for the RKE system. In **Attacks on RKE system**, we demonstrate that all known attacks on RKE systems can be grouped into the two categories.

1) Single-band relay attacks: In the PKES system, a vehicle transmits a verification request to the corresponding key fob using the LF-band RFID communication. When the request is received in the LF band, the key fob automatically

responds in the UHF band. The PKES system was originally intended to only operate within the LF-band communication range (e.g., $1 \sim 2$ meters). However, by relaying an LF-band request from a vehicle to its key fob, an adversary is able to make a key fob respond to a request within the UHF-band communication range (e.g., up to 200 meters) even if it is out of the LF-band communication range. It should be noted that the communication range of a key fob differs per manufacturer. In essence, a single-band relay attack aims to relay an LF-band request to the key fob, in which case the UHF-band response for the LF-band request is directly transmitted to the vehicle. In other words, the UHF-band response is not relayed and is transmitted within its communication range. This paper focuses on the UHF-band RF signals emitted from key fobs, and, as such, does not consider how the LF-band signals are relayed to the key fobs.

2) Dual-band relay attacks: Unlike a single-band relay attack, a dual-band relay attack is not only able to relay a request from the vehicle within the LF band, but also a response from a key fob within the UHF band. Accordingly, in a dual-band relay attack, the PKES system can be attacked even if the key fob is much farther away from the vehicle during a single-band relay attack. Adversaries intending to commit a dual-band attack must also possess industry-standard equipment in order to relay both the LF-band and the UHF-band RF signals. The UHF-band signals can be delivered to the vehicle by a signal-extending module [10], [19], or through two adversaries, one who would record and forward the UHF-band signal out of communication range and the other who would inject the forwarded signal into the vehicle [18]. We denote the former as an **Amplification attack** and the latter as a **Digital relay attack**. The difference between the two attack types is whether the adversaries perform digital communication to forward binary information contained in LF/UHF-band signals.

During an **Amplification attack**, adversaries simply amplify both the LF band and the UHF-band signals using the RF amplifier. There are two ways to inject UHF-band signals to the vehicle. First, the adversary at the key fob side amplifies the UHF-band signals and directly injects it into the vehicle. Second, both adversaries amplify the UHF-band signals. Although the latter case can produce a higher signal strength than the former, the RF amplifier intensifies both the pass-band signal and the noise leading to unintended feature variation. Therefore, in Section V, we have simulated an amplification attack based on the former case. In a **Digital relay attack**, adversaries perform the whole process of digital communication to inject an attack signal. Adversaries demodulate and decode the LF/UHF-band signal to forward binary information to each other. The delivery of binary information can be conducted through various wireless communication systems such as Wi-Fi or Bluetooth. After receiving the binary information, the adversary injects an attack signal through an encoding and modulation process. The advantage of a digital relay attack is that the communication range can be much larger than with a single-band relay attack or amplification attack. This is because binary information is forwarded through state-of-the-art digital communication. However, since most PKES systems assign a maximum delay [38], the attack signal should be injected within the maximum delay period. Nevertheless, researchers have shown that digital relay attacks can be successfully mounted with cheap RF devices [18].

3) Cryptographic attacks: An adversary can extend the communication range between a vehicle and its key fob, as well as mount a cryptographic attack. In a cryptographic attack, the adversary exploits the weaknesses of the cryptographic algorithm which is equipped in the PKES system. In the vicinity of the key fob, the adversary injects malicious LF-band signals (challenge) to the key fob and collects the UHF-band signals (response). Due to the lack of mutual authentication in the PKES system, the key fob accepts malicious LF-band signals and transmits corresponding responses. After collecting sufficient challenge and response pairs, the adversary performs cryptanalysis to extract a long-term secret key. Consequently, the adversary can inject valid UHF-band signals depending on a challenge signal from the vehicle. A 2018 study has shown that the PKES system of Telsa Model S is equipped with a weak cryptographic algorithm and does not require mutual authentication [66]. Researchers have uncovered that the outdated proprietary cipher DST40 has been mounted to the Telsa Model S. Furthermore, unrevealed PKES systems with weak cryptographic algorithms or key management failure [40] are also expected to be vulnerable to a cryptograhic attack, given that the adversary extracts the binary code and injects the attack signal. With regards to HODOR, this attack scenario is considered to be the same as the transmitted signal that would be analyzed in a digital relay attack.

4) Attacks on RKE systems: We categorized the attacks on PKES systems as Single-Band Relay, Dual-Band Relay, and Cryptographic Attack. In addition, previous studies have shown that where a long-term secret key is used in an RKE system, it can be compromised by an adversary through the use of cryptanalysis with reverse engineering [22], [24], [45], [61], an exhaustive key search [47], [63], or combining both methods [40]. As a result, an adversary can generate a valid packet in a similar manner to a cryptographic attack. To the best of our knowledge, our cryptographic attack model also covers all known attacks on RKE systems except a *rolljam attack*. In a *rolljam attack*, an adversary performs a jamming attack and eavesdrops on valid UHF signals. When the driver presses the unlock button on the key fob, the vehicle remains locked because the signal has been blocked by the jamming attack, and the driver will naturally attempt to unlock the door again. This creates a second signal that is also recorded and blocked, however, at this time, the adversary replays the first code to unlock the door. As a result, the driver assumes that the key fob is working normally. However, the adversary can now inject an attack signal using a second rolling code which has not been received by the vehicle.

IV. OUR METHOD: HODOR

A. Overview

In this section, we explain our design decisions to realize HODOR. Fig. 4 shows an overview of HODOR's architecture. HODOR aims at detecting an attack signal using a classifier which is generated by legitimate signals only. There are two main phases in HODOR: the *Training* phase and the *Attack Detection* phase. In the *Training* phase, HODOR creates a classifier based on a training dataset which contains only legitimate signals. Through preprocessing and feature extraction, a set
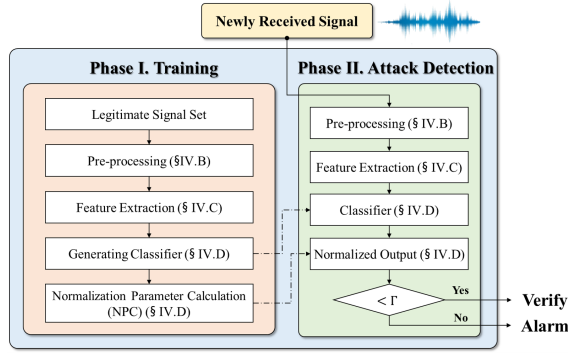
Fig. 4: Overview of HODOR architecture

Fig. 5: Preprocessing block diagram

of features per RF signal are obtained and the classifier is trained. In addition, normalization parameters, which are used for output normalization in the *Attack Detection* phase, are computed. After the classifier is trained, in the *Attack Detection* phase, HODOR is now able to detect any attacks defined in our attack model in Section III-B. In the *Attack Detection* phase, HODOR receives a new RF signal which contains a door unlock request. Then, HODOR conducts preprocessing and feature extraction on this newly received RF signal, as outlined in the *Training* phase. The extracted feature set is used as input to the trained classifier, and HODOR makes a decision whether the received RF signal has been transmitted from a legitimate key fob or not. This decision is made based on the normalized output of the classifier and a pre-defined threshold. In an invalid case, when the normalized output is larger than the threshold, the corresponding door unlock request is not validated and HODOR alerts the BCM module.

B. Preprocessing

At the outset, HODOR receives UHF-band RF signals, which become preprocessed as illustrated in Fig. 5. The received signal, including a carrier signal $c(t)$, a baseband signal $s(t)$, and channel noise $n(t)$, is denoted as follows.

$$r(t) = s(t) \otimes c(t) + n(t) \qquad (1)$$

where $\otimes$ is the operation for the mixer. The carrier signal is a sinusoidal signal at the carrier frequency (f_c) of the UHF band. To obtain meaningful information for analysis located in the baseband signal, the carrier signal must be removed. In other words, the received raw signal is shifted back down to the baseband by mixing the sinusoidal signal at the same carrier frequency as follows.

$$r[t] \otimes c[t] = s[t] + n[t] \otimes c[t] \qquad (2)$$

It should be noted that HODOR samples a continuous analog RF signal, and owing to this, we denote the sampled signal as $[t]$ which represents discrete values. To remove $n[t] \otimes c[t]$, the bandpass filter is performed on $r[t] \otimes c[t]$. As a result, we obtain the baseband signal $s[t]$ from the received signal $r[t]$.

Subsequently, HODOR demodulates the baseband signal $s[t]$ into a pulse signal $d[t]$. The pulse signal is encoded from a binary code. As mentioned in Section III-B, FSK and ASK are typical modulation schemes used in keyless entry systems, which are determined by manufacturers. After demodulation,
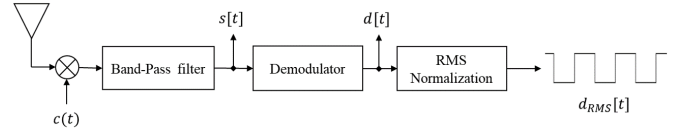
the pulse signal is normalized to scale its power to a certain value. Since the received signal strength (RSS) is determined by a channel condition, it would be difficult to reliably extract the features under noisy channel conditions. To be independent to the degree of RSS, HODOR applies root-mean-square (RMS) normalization, through which the power of a demodulated signal is scaled as 1. For example, if $d[t]$ is composed of N samples (d_1, d_2, ..., d_N), the RMS-normalized signal is calculated as follows.

$$d_{RMS}[t] = \frac{d[t]}{\sqrt{\frac{\sum_{i=1}^{N} d_i^2}{N}}} \qquad (3)$$

C. Feature Extraction

On the preprocessed signals, HODOR extracts salient features by which a legitimate request and a malicious attempt are distinct. In wireless transmissions, the radio preamble (sometimes called a header) is used to synchronize the clock between a transceiver and a receiver. Preamble has a static bit sequence independent of the data packet. HODOR extracts the features from the preamble of the pulse signal since it allows HODOR to extract features independent of the data and the key fob. We propose four types of features: i) peak frequency, ii) frequency offset, iii) SNR, and iv) a set of statistical features.

Peak frequency. Peak frequency is a feature in a frequency domain. Since the preamble part of a time-domain pulse signal is given, it must be transformed to the frequency-domain signal by fast fourier transform (FFT). Fig. 6 shows the preamble part of the UHF-band RF signal transmitted from a key fob and its FFT result. It can be seen that several dominant peaks exist in the frequency-domain preamble signal. The peak frequency (f_{peak}) is the frequency where the highest amplitude value exists as follows.

$$f_{peak} = \arg\max_{f} |D_{RMS}[f]| \qquad (4)$$

where $D_{RMS}[f]$ is the FFT result of $d_{RMS}[t]$. The peak frequency feature is affected by a clock source used for micro controllers. Because of the imperfection of clock sources, different peak frequency values can be extracted from different RF devices. Accordingly, this feature is used to distinguish a legitimate key fob from other devices used for malicious attacks.

Carrier frequency offset. Carrier frequency offset is another feature in the frequency domain of a preamble signal. Different from *peak frequency*, carrier frequency offset is the feature that is extracted from the baseband signal s[t] which is shown in Fig. 2. As each key fob has a non-ideal (i.e., deviated from 433.92MHz) carrier frequency (f_c') due to the hardware imperfection, the RF receiver works on a wide band to reliably receive signals from the key fob [67] in a real vehicle. This
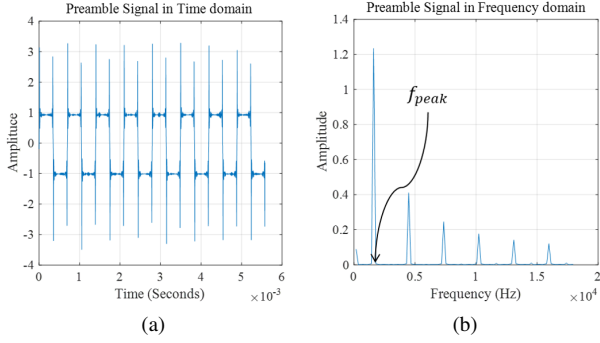
Fig. 6: Preamble signal in time and frequency domains: (a) Preamble signal in time domain, (b) Preamble signal in frequency domain

imperfection also occurs in the receiver, which leads the non-ideal frequency of f_c'' when generating $c(t)$. Consequently, when the $r(t)$ is mixed with $c(t)$, the baseband signal ($s[t]$) in Equation (2) has a different frequency offset value ($f_c' - f_c''$) according to each transmitter and receiver pair. We exploit this frequency difference as a feature to verify legitimate key fobs and denote it as f_c^{offset}.

SNR. Signal-to-noise ratio (SNR) is a measure that compares the level of a desired signal to the level of background noise. SNR is defined as the ratio of signal power to noise power. In addition, SNR is expressed in decibels (dB) as follows.

$$SNR_{dB} = 10 \log_{10} \frac{P_{signal}}{P_{noise}} \qquad (5)$$

Where P_{signal} is the power of a demodulated signal (i.e., meaningful information) and P_{noise} is the power of background noise (i.e., unwanted signal). It is noted that measures greater than 0 dB indicate more signal than noise. In the PKES system, a UHF-band RF signal emitted at a larger distance than the proximity distance should be considered malicious even if the signal is from the legitimate key fob. Since a feature of SNR is easily affected by channel conditions, path loss, or the reduction in power density of a signal as it propagates through space, can be estimated. By analyzing the features of SNR, HODOR is able to verify whether a particular signal has been generated within a specific vicinity.

Statistical features. To support the above features, a set of statistical features were also employed. Statistical features represent the various characteristics of a sampled signal. As a result, numerous studies on signal processing and wireless communication area employed statistical features for node or channel identification [33], [34], [54]. Since the hardware characteristics of an attack device and channel condition affect the signal characteristics, we employed the statistical features to differentiate an attack signal. With the three crafted features and 20 statistical features used in [33], we ran a feature selection algorithm to eliminate features that are not beneficial to performance. From there, we selected the top five highest performing features and decided to not employ all 23 while testing HODOR in consideration of execution time during the feature extraction phase. As more features are used, more time is required to compute the features, and this time delay hinders driver convenience. Moreover, the risk of

an overfitting problem can when a large number of features are included, and thus, we performed an exhaustive feature selection by limiting the number to five [42]. Interestingly, all of the crafted features were selected by the feature selection algorithm and the remaining two features were kurtosis and spectral brightness. Table I shows the features selected for HODOR according to the modulation scheme. Kurtosis is a measure of the peakedness of the sampled signal in the time domain. As the signal propagates through the air, noise signals and multipath signals affect signal quality. In addition, since the passband signal and noise signals are also intensified by an analog amplifier, and external amplification affects the kurtosis of the signal. Therefore, single-band relay and amplification attacks inhere greater kurtosis values than a legitimate signal. The kurtosis is calculated as follows.

$$Kurtosis = E\left[\left(\frac{d_{RMS} - \mu}{\sigma} \right)^4 \right] \qquad (6)$$

where μ and σ are the mean and standard deviation of the d_{RMS}, respectively. Spectral brightness is the amount of spectral energy corresponding to frequencies higher than a given cut-off threshold. In a playback attack, the adversary records the legitimate signal. In this process, the baseband RF signal goes through an analog-to-digital converter (ADC) and is digitally sampled. However, digital sampling introduces a quantization error due to the sampling rate and vertical resolution of ADC. When the attack is mounted, these samples go through a digital-to-analog converter (DAC) and are reconstructed to an analog baseband signal. At this point, the quantization error introduced during digital sampling affects the spectral density of the reconstructed signal [65]. Spectral brightness is calculated as follows.

$$SpectralBrightness = \sum_{f=f_{th}}^{0.5 \times f_s} |D_{RMS}[f]|^2 \qquad (7)$$

where f_{th} is the threshold frequency and f_s is the sampling frequency. In our evaluation, we assigned f_{th} as $0.1 \times f_s$.

TABLE I: Features used for each modulation scheme

Modulation Scheme	FSK	ASK
Selected Features	f_{peak} Kurtosis Spec. Brightness SNR_{dB}	f_{peak} Kurtosis f_c^{offset} Spec. Brightness SNR_{dB}

D. Training and Attack Detection

Before attack detection, HODOR requires a one-class classifier, which facilitates attack detection. One-class classifiers are trained with a set of features derived exclusively from a legitimate key fob. Feature extraction during training can only occur via the legitimate key fobs, and as such, the classifiers are created via semi-supervised learning. Table I shows the features used for each modulation scheme. After the classifiers are trained, HODOR assigns a threshold for each classifier. Considering implementation in a real vehicle, it is necessary

Algorithm 1 `Attack detection for the PKES system`

1: **function** SEMI-SUPERVISED LEARNING (S: A SET OF SIGNALS)
2:     **for** i=1 to $|S|$ **do**
3:         $d_{RMS} \leftarrow$ preprocessing (s_i) $(s_i \in S)$
4:         $N^i_{PKES} \leftarrow$ FeatureExtraction (d_{RMS}, F_{PKES})
5:         /* F : Selected features */
6:         /* N : Extracted feature set */
7:     **end for**
8:     $\mathbb{C}_{PKES} \leftarrow$ Training (N_{PKES})
9:     $\mu_{PKES}, \sigma_{PKES} \leftarrow$ NPC (N_{PKES})
10:     /* $\mathbb{C}$: Classifier */
11:     **return** $\mathbb{C}_{PKES}, \mu_{PKES}, \sigma_{PKES}$
12: **end function**

13: **function** PKES SYSTEM ATTACK DETECTION (s: RECEIVED SIGNAL)
14:     $d_{RMS} \leftarrow$ preprocessing (s)
15:     $N_{PKES} \leftarrow$ Feature Extraction (d_{RMS}, F_{PKES})
16:     $O_{PKES} \leftarrow \mathbb{C}_{PKES} (N_{PKES})$
17:     $O_{PKES} \leftarrow \frac{|O_{PKES} - \mu_{PKES}|}{\sigma_{PKES}}$
18:     **if** $O_{PKES} > \Gamma_{PKES}$ **then**   /* Γ : Threshold */
19:         **return** Reject   /*Attack*/
20:     **else**
21:         **return** Accept   /*No Attack*/
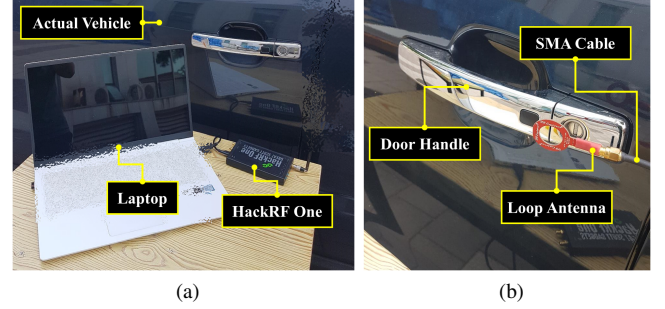22:   **end if**
23: **end function**

Fig. 7: Experimental setup for single-band relay attack simulation: (a) Signal acquisition setup on the vehicle side, (b) LF-band signal relay using a loop antenna and SMA cable
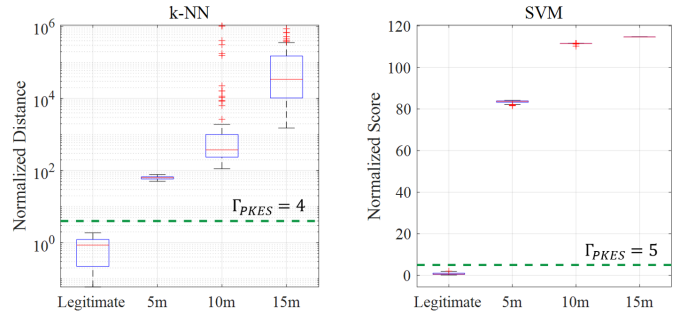

Fig. 8: Output distributions of k-NN and SVM algorithms as a function of distance in a single-band relay attack

to assign equal thresholds to a specific key fob model. For this requirement, HODOR performs z-normalization on the output of the classifier, to compensate for the difference of feature distribution between the key fobs. Z-normalization calculates a z-score which has a distribution with a mean of 0 and a standard deviation of 1. To set a normalization parameter mean and standard deviation, inspired by the k-fold cross validation [51], HODOR randomly selects 90 percent of the legitimate data set for training and 10 percent of the legitimate data for testing. After repeating 10 times to accumulate the output of the legitimate test data, HODOR calculates the mean (μ) and standard deviation (σ) of the corresponding key fob. We denote this process as *Normalization Parameter Calculation (NPC)*. In the attack detection phase, output (x) of a classifier from a newly received signal is normalized as $\frac{|x-\mu|}{\sigma}$. If any output from the classifier is not within the indicated threshold (Γ), the corresponding input is considered malicious. We set an adequate threshold for each keyless entry system through evaluation, as shown in the following chapter. Finally, HODOR rejects the door unlock request if at least one classifier is deemed malicious. Algorithm 1 illustrates HODOR operation during training and attack detection.

V. EVALUATION

In this section, we report the evaluation results for HODOR to show that the system accurately detects attacks defined in Section III-B. In addition, we performed further evaluations to demonstrate how HODOR handles environmental factors, such as temperature variations, NLoS conditions, and battery aging.

A. Experimental Setup

Keyless Entry System. We performed a series of experiments on actual vehicles, a 2014 Kia Soul and 2016 Volkswagen Tiguan. Both vehicle models are equipped with a PKES system. In the case of the Soul, an FSK modulation was employed, and a center frequency of 433.92MHz with a frequency deviation of 30kHz was assigned for UHF-band RF communication. In the Tiguan, ASK modulation with a center frequency of 433.92MHz was employed for UHF-band RF communication.

RF Signal Receiver and Transmitter. For the evaluation of HODOR, two types of software-defined radio (SDR) devices were used for the transmission and acquisition of the UHF-band RF signals. SDR is a radio communication system that replaces hardware components with a software module. HackRF One [39] was used to sample the UHF-band RF signals, and the other HackRF One coupled with a universal software radio peripheral (USRP) X310 [17] was used to generate UHF-band RF signals that were to be simulated as attack signals. With GNU Radio [23], the preprocessing phase of HODOR was implemented in virtual hardware components. We set the sample rate of SDR to 5M samples/s in both vehicle models. Since specification of the communication system is different for the two vehicle models, we assigned different parameters for each vehicle. The key fob of the Kia Soul was implemented with a bit rate of 3kbps and a frequency deviation of 30kHz using FSK modulation. As a result, the frequency range of the baseband signal begins at 27kHz to
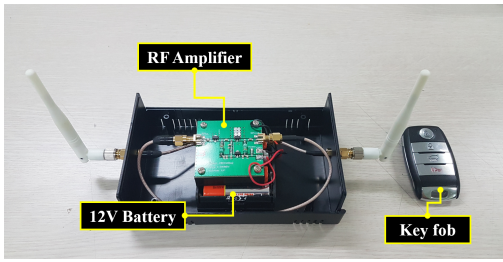
Fig. 9: Experimental setup for amplification attack simulation on the key fob side
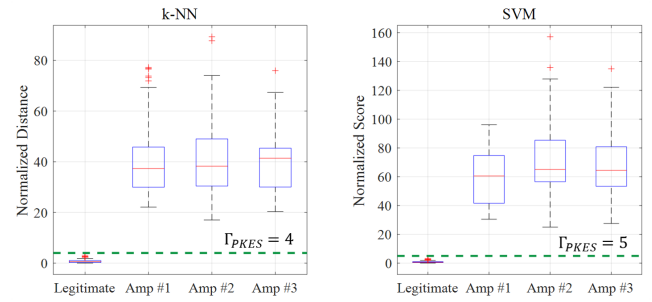

Fig. 10: Output distribution of the k-NN and SVM algorithms as a function of amplifiers in an amplification attack

Fig. 11: Experimental setup for digital relay attack simulation

33kHz. Ideally, the transition width of a filter should be zero. However, since the practical communication system has an inevitable frequency offset, the receiver must be designed with a wider bandwidth than in ideal scenarios. Accordingly, we set the bandwdith of the bandpass filter to have greater margins and found the specific parameter heuristically. Therefore, we set the high, low cut-off frequencies and transition width of the bandpass filter to 15kHz, 45kHz, and 10kHz respectively. On the other hand, the key fob of the Volkswagen Tiguan uses a MEGAMOS ID 48 transceiver [62] which utilizes ASK modulation with a bit rate of 3.5kbps. Therefore, the baseband signal of a Tiguan has a 7kHz bandwidth. As with the KIA Soul, considering the frequency offset that occurs in a practical system, we set the cut-off frequency of the lowpass filter as 20kHz. In addition, the LF-band RF signals were relayed by an SMA cable [15] and a loop antenna [14] to simulate the relay attack. Finally, three RF amplifiers were used to simulate an amplification attack, in which the communication range of a key fob was extended. In our experimental setup, *we confirmed that the vehicle verifies an attack signal as legitimate in every trial.*

Classification Algorithm. Classification algorithms are usually categorized as one-class or multi-class classification. Since it is impossible to train for all cases of malicious attacks before they occur, the classifiers should be trained with a set of features from a legitimate key fob only. In other words, a semi-supervised one-class classification is needed for HODOR to cover unknown attacks. In our evaluation, a one-class support vector machine (SVM) and k-nearest neighbors (k-NN) algorithms were used [49]. The SVM and k-NN algorithms were performed with the default parameters provided by MatLab 2017a [16]. More specifically, a residual basis function (RBF) was used for SVM algorithms, and standardized euclidean distance was applied for k-NN algorithms, whose parameter k was set to 1. For each classifier, we collected a set of 100 UHF-band RF signals from a legitimate key fob from a one-meter distance, and the classifiers were trained with them. As with the training data set, we collected a set of 100 attack signals in every attack simulation.

Performance Metric. Statistical measures of classification test performance were measured by standard metrics, such as true positive rate (TPR), true negative rate (TNR), false positive rate (FPR), and false negative rate (FNR) [42]. In our evaluation, TP refers to the case in which HODOR identified an attack signal as an attack. Alternatively, TN refers to the case in which HODOR considered a legitimate signal as legitimate. FP refers to the case in which HODOR considered a legitimate signal as an attack and FN refers to the case in which HODOR
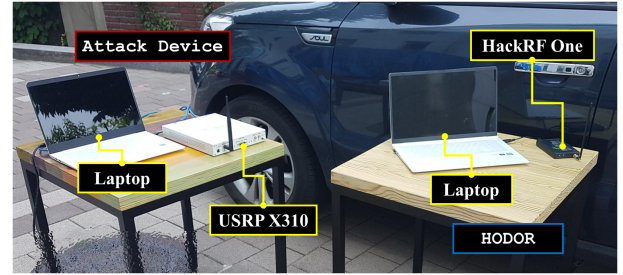
considered an attack signal as legitimate. It would only take one FN case in the keyless entry system to cause a car theft. Owing to this, we set the objective FNR as 0%, under the belief that FNR should take precedence over FPR.

B. Single-Band Relay Attack Detection

To simulate the single-band relay attack, we relayed the LF-band signals to trigger a key fob even if it is out of the LF-band communication range. An SMA cable and RF amplifier were used to minimize the path loss of the LF-band signals. We then sampled the UHF-band RF signals emitted from a key fob, varying the distance between the vehicle and the key fob (5m, 10m, and 15m). Fig. 7 shows the experimental setup for the single-band relay attack simulation. HackRF One is located on the vehicle side and controlled by a laptop. Since the signal attenuation becomes larger as the distance increases, we utilized RF amplifiers to increase LF-band signal strength to relay it to the key fob located more than 10 meters away. It should be noted that the maximum range that the UHF-band signal in the PKES system could transmit was at most 15m in our experimental setup. In addition, we set the distance between HackRF One and the key fob to one meter under LoS conditions for capturing legitimate signals. Fig. 8 shows the output distribution of the k-NN and SVM algorithms as a function of distance. Due to the nature of the PKES system, a transmission from an out-of-range key fob is considered an attack on the PKES system. For the UHF-band RF signals measured at a distance of 5m, the k-NN and SVM algorithms both output an FPR of 0%, with an FNR of 0% at thresholds (Γ_{PKES}) of 4 and 5, respectively. Furthermore, both algorithms with the same threshold output an FPR of 0%, with an FNR of 0% where the UHF-band RF signals were captured at distances of 10 or 15m. As the distance increased, it became easier to detect a single-band relay attack. Thus, we
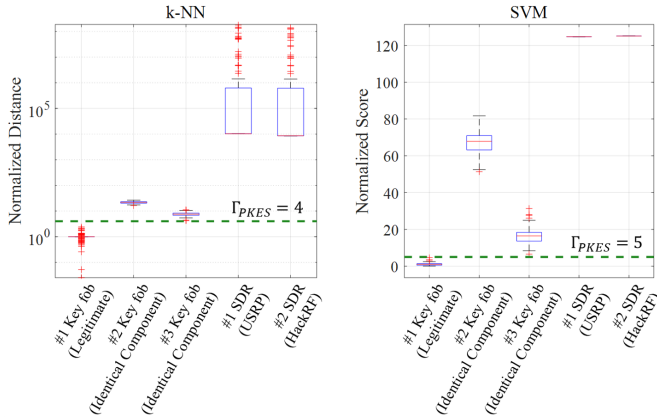
Fig. 12: Output distribution of the k-NN and SVM algorithms as a function of devices in a digital relay attack

conclude that `HODOR` is able to effectively detect single-band relay attacks.

C. Dual-Band Relay Attack Detection

We evaluate attack detection performance against two types of dual-band attacks, (i.e., amplification attack, digital relay attack) which are mentioned in Section III-B.

1) Amplification attacks: Since a single-band relay attack is only possible within the communication range of a key fob, a victim might easily become suspicious of foul play. To avoid alerting their victims, adversaries are more likely to adapt a dual-band attack strategy. A dual-band relay attack involves relaying the UHF-band signals of a key fob as well as the LF-band signals of a vehicle. Even though a key fob is placed out of the communication range, a dual-band relay attack can still successfully unlock doors. In our experiments, we first applied RF amplifiers to extend the UHF-band communication range. In an amplification attack scenario, the adversary amplifies and forwards the UHF-band signals to the vehicle. To minimize the path loss between the key fob and RF amplifier, we directly place the RF amplifier next to the key fob. Therefore, the UHF-band RF signals were transmitted much longer distances than the original communication range permitted. Fig. 9 shows the relay module for the amplification attack simulation. The 12V battery pack supplies DC voltage to the amplifier, and the experimental setup on the vehicle side is identical Fig. 7. Deviating slightly from the attack model in Section III-B, for experimental convenience, we relayed the LF-band signal using an SMA cable. Since `HODOR` only analyzes the UHF-band signal, this experimental setup is equivalent to an amplification attack model. We employed several Low Noise Amplifiers (LNA) on the UHF band in a commercial market. Each amplifier (Amp #1, Amp #2, Amp #3) used for the attack simulation had 30dB, 60dB and 64dB gains, respectively [1]–[3]. As mentioned in Section III-B, `HODOR` sampled the amplified UHF-band signals, which had been directly injected by the adversary on the key fob side. We assumed that the adversary can adjust the SNR level using a high-quality amplifier or directional antenna, and set the distance between the adversary and vehicle to the point where the SNR level is equal to that of legitimate signals. This implies that when the adversary injects the attack signal with

TABLE II: Output distribution of a digital relay attack against the PKES system of the Kia Soul

Algorithm	Legitimate Device	Output Distribution (mean / std)					FPR (%)
		#1 Key fob	#2 Key fob	#3 Key fob	#1 SDR	#2 SDR	
k-NN	#2 Key fob	22.29 /1.7	**0.97** **/0.63**	11.72 /1.76	2.32e+7 /1.15e+7	2.42e+7 /1.15e+7	0.19
	#3 Key fob	8.89 /1.49	12.31 /1.96	**0.91** **/0.49**	1.21e+7 /6.77e+6	1.61e+7 /6.06e+6	0.29
SVM	#2 Key fob	81.16 /6.47	**0.91** **/0.9**	33.32 /5.68	153.12 /2.28e-13	158.03 /1.99e-13	3.23
	#3 Key fob	15.56 /3.57	24.48 /4.92	**0.6** **/0.55**	94.91 /1.14e-13	96.73 /8.56e-14	1.17

TABLE III: Output distribution of a digital relay attack against the PKES system of the Volkswagen Tiguan

Algorithm	Legitimate Device	Output Distribution (mean / std)				FPR (%)
		#1 Key fob	#2 Key fob	#1 SDR	#2 SDR	
k-NN	#1 Key fob	**18.24** **/12.77**	123.22 /2.77	130.03 /4.34	121.8 /3.14	0
	#2 Key fob	140.74 /3.83	**11.72** **/15.72**	112.97 /13.61	112.97 /13.62	0
SVM	#1 Key fob	**21.52** **/16.62**	133.24 /0.49	134.72 /0.47	133.6 /0.58	0
	#2 Key fob	119.58 /0.02	**20.07** **/27.76**	118.74 /0.46	118.74 /0.46	0

a higher SNR than the legitimate signal, `HODOR` can easily detect an amplification attack. We found that the adversary can achieve the same SNR level as the legitimate signal at a distance of between 20 and 25 meters. Then, we sampled the forwarded signals on the vehicle side. Fig. 10 shows the output distributions of the k-NN and SVM algorithms as a function of the amplifiers. As seen in Fig. 10, even if the distance between the key fob and vehicle is larger than the maximum distance of a single-band relay attack, the normalized output distance/score is much closer to the legitimate case. Nevertheless, the k-NN and SVM algorithms both output an FPR of 0% and FNR of 0% at thresholds (Γ_{PKES}) of 4 and 5, respectively. Therefore, `HODOR` is still able to effectively detect amplification attacks.

2) Digital relay attacks: To simulate a digital relay attack, we extracted binary information from the ACK signal in Fig. 1a. Then, attack signals were injected according to the modulation scheme of the target PKES system using SDR devices. The ACK signal of each key fob contains unique, but static binary information. When the vehicle receives the ACK signal, a number of ECUs are activated to transmit the CAN packets. This *standby* function is implemented in modern vehicles for enhanced driver convenience [28]. Based on this observation, and by checking the in-vehicle network (i.e., CAN bus), we confirmed that the vehicle accepts the attack signal. In addition to the SDR devices, we further extended the capability of the digital relay adversary. The strongest adversary would, in theory, be one with access to identical electronic components as the target key fob. In practice, though, the assumption that the digital relay adversary would have the exact same electronic components might be perceived as overly cautious. However, we also evaluated `HODOR` against this well-equipped, but highly unlikely, hypothetical super adversary. For the Kia Soul, one key fob out of three used in the experiment was
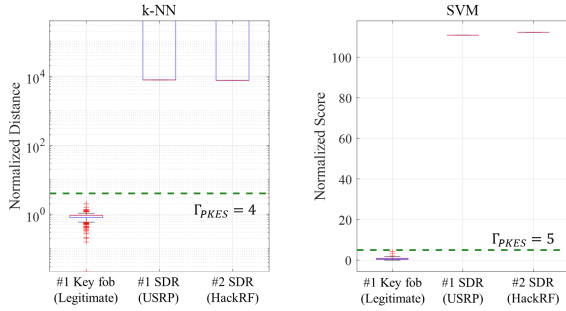
Fig. 13: Output distribution of the k-NN and SVM algorithms as a function of SDR devices in an playback attack on a PKES system

chosen as legitimate. The remaining two key fobs and two SDR devices were used to simulate malicious UHF-band RF packets. For example, if the #1 key fob were to be chosen as legitimate, features from the other key fobs would be assumed as an attack. For the Volkswagen Tiguan, one key fob out of the two was chosen as legitimate and the remaining key fob and two SDR devices were used to simulate an attack. Fig. 11 shows the experimental setup for a digital relay attack simulation. HackRF One was used for signal acquisition, and the USRP and another HackRF One was used for signal injection. All of these SDR devices were controlled by a laptop. The UHF-band RF signals corresponding to the packets were then sampled and analyzed by HODOR. Fig. 12 shows the output distributions of k-NN and SVM algorithms as a function of devices used in the simulation of digital relay attacks on the Kia Soul, when the #1 key fob was used as a training set. As shown in Fig. 12, Table II, and Table III, the output from the remaining remote key fobs is closer to that of a legitimate one than to the output from the SDR devices. Especially, features from the #3 key fob of the Soul are closer to that of the #1 key fob than to other devices. This is because the two key fobs were manufactured in the same year and month. In the case of the Soul, the k-NN and SVM algorithms output produced an average FPR of 0.65% and an average FPR of 0.27% with an FNR of 0% at thresholds (Γ_{PKES}) of 4 and 5, respectively. In the case of the Tiguan, the k-NN and SVM algorithms both output an average FPR of 0% with an FNR of 0% at a threshold (Γ_{PKES}) of 70 for both. In addition, as mentioned in Section III-B, a cryptographic attack can also be simulated in the same way. Therefore, we also verified that HODOR can effectively detect a cryptographic attack against a PKES system. As a result, HODOR successfully filtered legitimate and malicious requests from both the amplified and replayed messages. Accordingly, we conclude that HODOR is able to effectively detect dual-band relay attacks and cryptographic attacks.

D. Playback Attack Detection

During an advanced attack, it is possible that an adversary might attempt to playback the sampled signals whose features most closely resemble the target key fob. This type of attack is a potential threat in PKES systems. For example, an the attack could be mounted when an adversary predicted the next challenge messages through an analysis of several previous challenge messages [21]. The adversary can inject such a

TABLE IV: Output distribution of a playback attack against the PKES system of each vehicle

Vehicle	Algorithm	Legitimate Device	Output Distribution (mean / std)			FPR (%)
			Legitimate Device	#1 SDR	#2 SDR	
Soul	k-NN	#2 Key fob	**0.99 /0.64**	1.67e+7 /5.97e+7	1.38e+7 /4.34e+7	0
		#3 Key fob	**1.08 /0.67**	1.41e+7 /3.43e+7	1.12e+7 /3.34e+7	0
	SVM	#2 Key fob	**0.66 /0.72**	86.93 /8.56e-14	85.68 /3.28e-15	0.7
		#3 Key fob	**0.7 /0.61**	97.37 /8.56e-14	98.09 /1.42e-13	0.7
Tiguan	k-NN	#1 Key fob	**16.46 /11.4**	173.37 /5.99	164.79 /5.4	0
		#2 Key fob	**12.92 /16.71**	83.27 /9.99	83.27 /9.99	0
	SVM	#1 Key fob	**25.43 /19.03**	139.66 /1e-3	139.66 /3.1e-3	0
		#2 Key fob	**18.79 /16.43**	74.6 /0.31	74.6 /0.31	0

predicted challenge into the key fob and record the response signals. Then, the adversary goes back to the vehicle and plays back the valid response signals and unlocks the door. SDR devices (i.e., HackRF One and USRP) are employed to transmit the sampled signals. Fig. 13 shows the output distributions of k-NN and SVM algorithms as a function of SDR devices used in the simulation of playback attacks on the Soul, when the #1 key fob was used as a training set. Table IV shows the mean and standard deviation of output distribution according to the vehicle and key fob. The k-NN and SVM algorithms output an average FPR of 0% and average FPR of 0.35% with an FNR of 0% at thresholds of 4 and 5, respectively, in the Soul. In the case of the Tiguan, the k-NN and SVM algorithms both output an average FPR of 0% with an FNR of 0% at the threshold of 70. For the SVM algorithm, it is clear that the average output distribution of the #1 SDR device and #2 SDR is closer to the legitimate device than to that of a digital relay attack. From these results, we understand that when the transmission is given a sampled signal (i.e., playback attack) it achieves a closer output distribution to the legitimate key fob than to when the transmission is given a binary code (i.e., digital relay attack). Nevertheless, HODOR still properly detects playback attacks.

E. Non-Line-of-Sight (NLoS) Conditions

To show that the features used for the PKES system are robust under an NLoS condition, we sampled UHF-band RF signals from the key fobs placed in a pocket or backpack. In the PKES system, a car owner is able to unlock doors without physically producing the key fob from its storage location. The classifier was trained with the UHF-band RF signals sampled under an LoS condition. Fig. 14 shows the output distributions of the k-NN and SVM algorithms as a function of where the key fob is placed. When the key fob is placed in a backpack, the k-NN and SVM algorithms output an FPR of 1.32% and 1.35% with an FNR of 0%. When the key fob is placed in a pocket, the k-NN and SVM algorithms output an FPR of 1.71% and 1.67% with an FNR of 0%. Like in previous experiments, thresholds (Γ_{PKES}) were respectively assigned to 4 and 5 for each algorithm. From these results, we conclude that HODOR
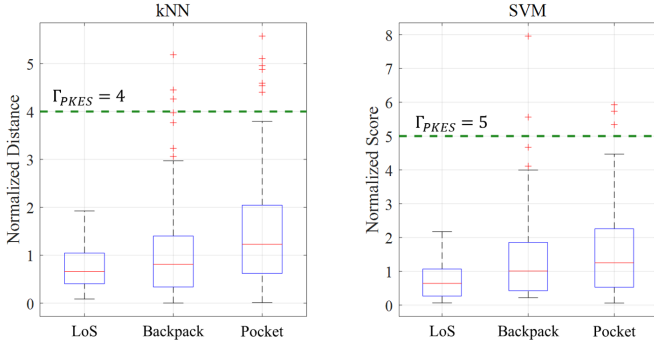
Fig. 14: Output distributions of the k-NN and SVM algorithms as a function of where a key fob is placed

properly identifies a legitimate door unlock request even when in an NLoS condition.

F. Attack Detection in RKE Systems

We further analyzed the UHF-band attack signal against the RKE system of the Soul. Cryptographic attacks on RKE systems have been extensively studied in the past decade [22], [40], [45], [47], [61]. An adversary eavesdrops on several valid packets and exploits the weaknesses of the cryptographic algorithm to extract the secret key. It is also possible for an adversary to attempt to playback the sampled UHF-band signal. One example of a playback attack on an RKE system is a roll-jam attack [11]. In this attack, the adversary interferes (i.e., jams) some frequencies and plays back valid encrypted messages.

To simulate a cryptographic attack, one remote key fob out of three used in the experiment was chosen as legitimate. The remaining two remote key fobs and two SDR devices were used to simulate malicious UHF-band RF packets. In the case of a playback attack, two SDR devices were employed to simulate attack signals. Moreover, we tested the UHF-band RF signals that were sampled at different distances from where they had been sampled during training. Even though the classifier was trained with a training set measured at a distance of one meter, the legitimate remote key fob must still be identified correctly within the communication range of the RKE system. Therefore, we measured the UHF-band signals from the legitimate key fob at a distance of 40 meters from the RF signal receiver under LoS conditions and used this for the test. Since SNR_{dB} and $Kurtosis$ are highly correlated to the distance between the key fob and receiver, they were excluded in this experiment. In other words, a classifier using a different feature set (i.e., f_{peak} and $SpectralBrightness$) was employed for the training. We denote the RKE system classifier as $\mathbb{C}_{RKE}$. As we mentioned in Section II-A, an identical packet was transmitted from a smart key multiple times for reliable communication. Accordingly, HODOR verifies a newly received signal as an attack when the number of detected preambles exceeds $\lfloor \frac{N}{2} \rfloor$ among the N received preambles. Therefore, the maximum value of N in our experiment is five. In addition, we set the threshold(Γ_{RKE}) of k-NN and SVM algorithms to 4.5 and 5, respectively. Tables V and VI show the mean and standard deviation of output distribution for both the cryptographic and playback attacks. Even though HODOR

TABLE V: Output distribution of a cryptographic attack against the RKE system of the Soul

| Algorithm	Legitimate Device	Output Distribution (mean / std)					FPR (%)
		#1 Key fob	#2 Key fob	#3 Key fob	#1 SDR	#2 SDR	
k-NN	#1 Key fob	**1.44** **/2.16**	77.97 /9.74	22.09 /5.37	5.27e+3 /511.58	5.21e+3 /220.04	2.38
	#2 Key fob	73.91 /5.4	**2.36** **/3.72**	39.17 5.09	6.56e+3 /433	4.53e+3 99.1	3.57
	#3 Key fob	23.64 /6.48	49.8 /11.83	**1.3** **/1.3**	5.76e+3 /846.02	5.04e+3 /185.41	1.79
SVM	#1 Key fob	**1.89** **/5.88**	47.26 /0.75	21.09 /4.47	47.63 /7.13e-14	43.14 /5.7e-14	0
	#2 Key fob	22.06 /1.78	**1.53** **/1.91**	9.55 /1.74	32.99 /4.98e-14	29.19 /4.28e-14	0
	#3 Key fob	18.14 /4.26	29.64 /4.63	**1.99** **/6.67**	47.26 /≈0	43.02 /7.84e-14	0.6

TABLE VI: Output distribution of a playback attack against the RKE system of the Soul

| Algorithm	Legitimate Device	Output Distribution (mean / std)			FPR (%)
		Legitimate Device	#1 SDR	#2 SDR	
k-NN	#1 Key fob	**4.96** **/32.43**	127.65 /141.48	187.96 /105.16	0
	#2 Key fob	**2.84** **/5.68**	105.21 /27.43	40.91 /14.2	3.57
	#3 Key fob	**5.15** **/28.55**	88.75 /98.71	191.29 /174.67	1.79
SVM	#1 Key fob	**1.53** **/4.87**	38.96 /2.28	45.08 /5.93	0
	#2 Key fob	**2.46** **/4.31**	42.04 /4.3	19.37 /5.32	3.57
	#3 Key fob	**1.75** **/6**	36.55 /4.88	34.48 /11.86	0

did not yield an FPR of 0% with an FNR of 0% on the RKE system during experimentation, we conclude that the achieved results are acceptable, as HODOR is designed to act as a support to an existing authentication method in a keyless entry systems.

G. Effects of Temperature Variation

Analog signals are easily affected by external factors. In particular, temperature variation is one of the most critical concerns in device fingerprinting [29], [46], [53]. In order to show that HODOR properly operates under varying temperatures, UHF-band RF signals were sampled in an ice box with dry ice to maintain a certain temperature as shown in Fig. 15a. It should be noted that this setup was only available indoors. Owing to this, evaluation on the PKES system was impossible, as it must occur within the vicinity of a vehicle (i.e., outdoors). The UHF-band RF signals for training were measured in degrees, between 20°C to -20°C in intervals of 10°C. Fig. 15b shows output distributions of the k-NN and SVM algorithms as a function of temperature. Unlike an attack detection, UHF-band RF signals measured in terms of varying temperature should be recognized as legitimate. Accordingly, this also means that the output of the RKE system classifier should remain below a given threshold. In Fig. 15b, the output distribution at 0°C and -20°C exceeds the threshold. This is
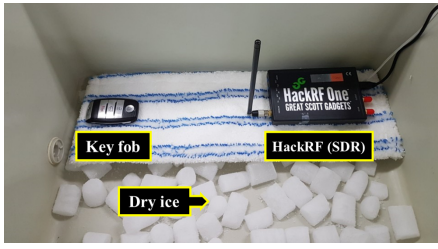
(a) Experimental setup for temperature variation
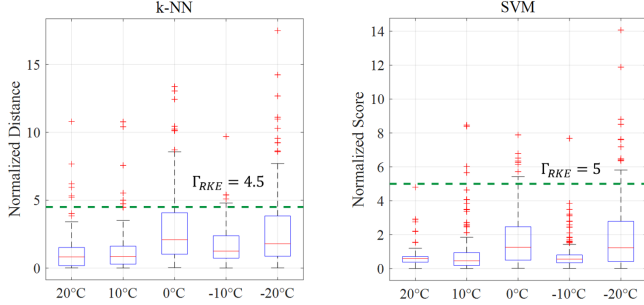
(b) Output distributions of k-NN and SVM algorithms as a function of temperature

Fig. 15: Experimental results of temperature variation

not only because of the temperature variation, but also the severe multipath environment caused by the limited space of the ice box. However, as we denoted in Section V-F, an RKE packet is considered an attack only if the number of detected preambles exceeds $\lfloor \frac{N}{2} \rfloor$ among the N received preambles. Therefore, HODOR can achieve moderate FPR under temperature variation. The k-NN and SVM algorithms output an FPR of 6.36% and 0.65% at the same threshold determined in Section V-F. Thus, we conclude that the features used in HODOR are operationally robust regardless of temperature variation.

H. Battery Aging

A coin cell battery supplies stable DC voltage to the key fob. However, as the driver uses the key fob, the supplied voltage decreases and may lead to feature variation. For this reason, we further evaluated feature robustness against battery aging. In the case of the Panasonic CR2032 lithium battery, which we selected for our evaluation, the initial voltage was 3V, but decreased to 2.5V over time [5]. This voltage interval occupies around 97.34% of the battery duration time. If the voltage drops under 2.5V, the key fob does not operate properly due to insufficient voltage supply. Therefore, using the classifier which had been trained in advance, we tested the UHF-band signals at a specific voltage level between 2.5V and 3V. Fig. 16 shows the output distribution of the k-NN and SVM algorithms as a function of voltage level. Similar to the temperature variation experiment, output of the classifier for the RKE system should be below a given threshold. The k-NN and SVM algorithms both output an FPR of 0% at the same threshold determined in Section V-F. Thus, we conclude that the features used in HODOR are operationally regardless of battery aging.
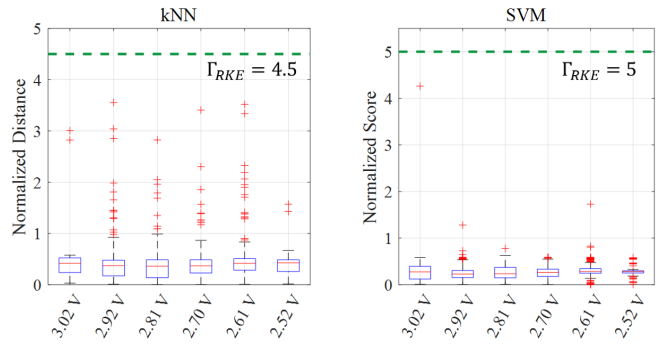

Fig. 16: Output distribution of k-NN and SVM algorithms as a function of battery level

TABLE VII: Execution time of HODOR

Phase		Algorithm	
		k-NN	SVM
Feature Extraction (FSK / ASK)	f_{peak}	4ms / 3.85ms	
	f_c^{offset}	4ms / 3.55ms	
	SNR_{dB}	130ms / 94ms	
	$Kurtosis$	20ms / 16.2ms	
	$Spec.Brightness$	5ms / 3.73ms	
NPC (FSK / ASK)	$\mathbb{C}_{PKES}$	55ms / 60ms	43ms / 45.5ms
	$\mathbb{C}_{RKE}$	50ms / 52ms	32ms / 34ms
Attack Detection (FSK / ASK)	$\mathbb{C}_{PKES}$	4.8ms / 4.94ms	.038ms / .04ms
	$\mathbb{C}_{RKE}$	3.8ms / 4ms	.04ms / .07ms

I. Execution Time

We implemented the functions that principally contribute to the total execution time of HODOR. We selected the Raspberry-pi 3B single-board computer [56] as a reference hardware platform. This platform is based on a quad core 1.4GHz Cortex-A53 (ARMv8) with 1GB RAM. Table VII shows the execution time for each basic function used in HODOR, which were implemented via Python programming. The classifiers should be trained and cross-validated in advance. Owing to this, the time for these two processes can be disregarded when it comes to the operation time for verifying a door unlock request. The results show that the k-NN algorithm takes longer to detect attacks. As a result, the total operation time for the verification of the PKES system using FSK modulation is 163.8ms and 159.038ms in the k-NN and SVM algorithms, respectively. These are the sum of feature extraction and attack detection processes. In addition, the RKE system using FSK modulation requires 12.8ms and 9.04ms in the k-NN and SVM algorithms, respectively. In ASK modulation, the total amount of operation time for the verification of the PKES system using ASK modulation is 126.27ms and 121.37ms in the k-NN and SVM algorithms, respectively. In addition, the RKE system using ASK modulation requires 15.13ms and 11.2ms in the k-NN and SVM algorithms, respectively. For the feature extraction phase, similar execution times were obtained because the numbers of samples for both ASK & FSK modulations were similar to each other. In other words, the duration of the preamble region from which the features are extracted is similar regardless of the modulation schemes. Regarding the *NPC* and *Attack Detection* phases, HODOR has
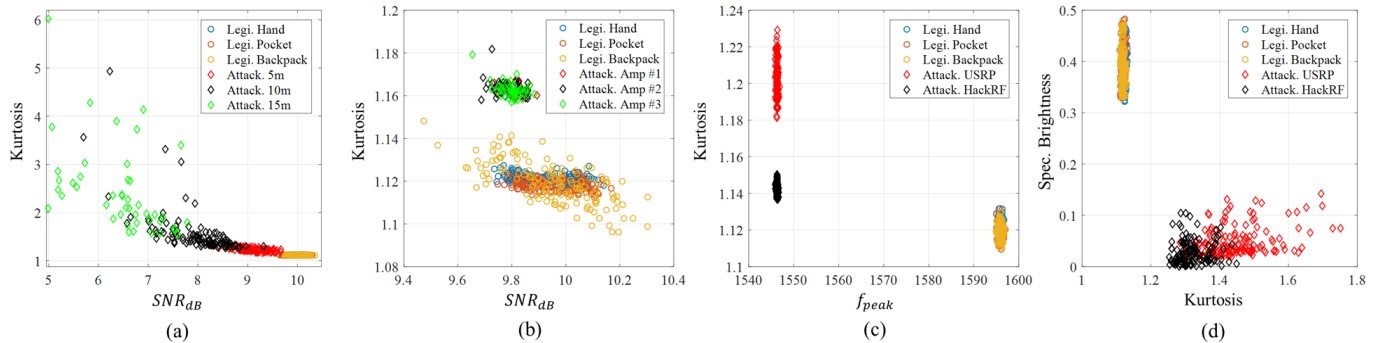
Fig. 17: Scatter plot of the top two features of the Soul as a function of an attack scenario: (a) Single-band relay attack, (b) Amplification attack, (c) Digital relay attack, (d) Playback attack

different execution times that correspond to the modulation schemes. In HODOR, the number of used features are different depending on modulation schemes. Because HODOR uses one additional feature, f_c^{offset}, for ASK-modulated signals, attack detection time for ASK modulation is longer than FSK modulation. However, since the ASK-modulated signal has a much shorter execution time for feature extraction, the total execution time of the ASK-modulated signal is shorter than the FKS-modulated signal. According to [7], humans cannot easily recognize a delay of less than $500ms$. Thus, it is expected that HODOR would be effective as a support mechanism to existing keyless entry systems without creating a noticeable delay on the user end.

J. Feature Importance

We minimized the feature set through the exhaustive search in Section IV. In this subsection, we further evaluated the feature importance as a function of each attack scenario. We employed the Relief algorithm, which is a unique family of filter-style feature-selection algorithms [50]. A key idea of the Relief algorithm is to estimate the quality of features according to how well their values distinguish between instances near to each other. Based on the MATLAB implementation of the relieff function, we ranked the features in each attack detection experiment. Table VIII shows the rankings of the features as a function of each attack scenario. The distribution of the top two features in each attack scenario are represented in Fig. 17. In a single-band relay and amplification attack, SNR_{dB} and kurtosis are effective features to detect an attack. In an amplification attack, even when the adversaries adjust the SNR level to the legitimate signal, HODOR can effectively differentiate the attack signals using the kurtosis feature. In a digital relay attack, f_{peak} has a major role. This is because of the clock difference between the key fob and the SDRs (i.e., USRP and HackRF). Though not as effective as f_{peak}, kurtosis is also useful to detect a digital relay attack. In a playback attack, due to the quantization error, spectral brightness and kurtosis are both effective features to differentiate attack signals.

K. Advanced Dual-Band Relay Attacks

In this subsection, we assumed the presence of an advanced dual-band relay attack adversary, extending the

TABLE VIII: Feature importance as a function of attack scenario

Attack Scenario		Single-band Relay Attack	Amplification Attack	Digital Relay Attack	Playback Attack
Rank	1	**SNR**	**Kurtosis**	f_{peak}	**Spec. Brightness**
	2	Kurtosis	SNR	Kurtosis	Kurtosis
	3	Spec. Brightness	Spec. Brightness	Spec. Brightness	f_{peak}
	4	f_{peak}	f_{peak}	SNR	SNR

previous experimental setup in Section V-C. Advanced adversaries are equipped with analog filters or an SDR device with a high sample rate.

1) Amplification attacks using analog filters: Advanced dual-band relay adversaries can attempt to make a low value for kurtosis by using an amplifier with a pre- and post-analog bandpass filter (BPF). In this attack scenario, adversaries use pre- and post- analog filters to reduce unwanted noise. An analog filter is a circuit made of analog components such as resistors, capacitors, inductors, and op amps. Digital filters are often embedded in a chip that operates on digital signals, such as an MCU or DSP. Analog filters are fairly simple but increase in complexity for narrow bandwidth and precise roll-off. In contrast, digital filters, which are employed in HODOR can be more precise in filtering, but the signal must be digitally sampled. Among the bandpass filters of MiniCircuits, we used the one with the bandwidth most relevant to the UHF band [9]. The low and high cut-off frequencies of the bandpass filter are 400MHz and 510MHz, respectively. Fig. 18 shows the amplifier used with the BPF in our evaluation. The pre-/post-bandpass filters were connected to the input/output port of each amplifier. We conducted the same experiment as the one used in the amplification attack. Fig. 19 shows the output distributions of the k-NN and SVM algorithms as a function of the amplifiers. As seen in the figure, compared to the amplification attack without analog filters (Fig. 10), the normalized output distance/score is slightly closer to the legitimate case. Nevertheless, the k-NN and SVM algorithms
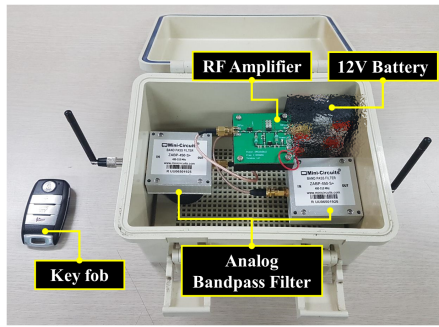
Fig. 18: Experimental setup for amplification attack simulation using pre/post-analog filter on the key fob side
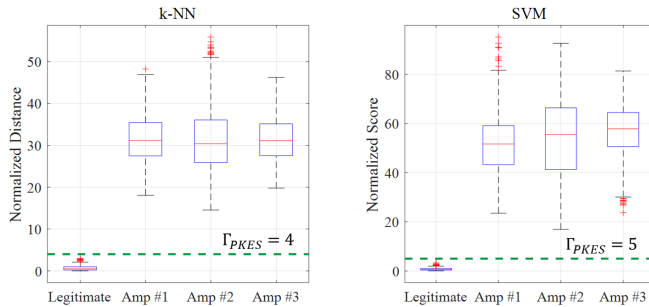

Fig. 19: Output distribution of the k-NN and SVM algorithms as a function of an amplifier under the advanced amplification attack scenario

Fig. 20: Output distribution of k-NN and SVM algorithms as a function of sample rate

both output an FPR of 0% and FNR of 0% at thresholds (Γ_{PKES}) of 4 and 5, respectively. Since the bandpass filter has a larger bandwidth (110MHz) than HODOR (30kHz), filtered noise has a negligible effect on the performance of HODOR. This is because the analog bandpass filter has a larger bandwidth than the digital bandpass filter of HODOR, which still amplifies the noise signals within the bandwidth of the digital bandpass filter and corrupts the value of kurtosis. In addition, if adversaries use the digital bandpass filter with a narrower bandwidth than that of HODOR, it accompanies both the ADC and DAC processes which corrupt the kurtosis and spectral brightness. This corruption can be observed in the evaluation results of the *playback attack* detection. As a result, we concluded that HODOR is able to detect an amplification attack even with pre-/post-analog filters.

2) Playback attack with high sample rate: We also assumed the presence of an adversary with strong PHY-layer sampling capabilities in addition to the amplification adversaries using the analog filter. To evaluate HODOR with a high sample capability, we used the maximum sampling rate of the USRP X310 used in our evaluation. Because the Ethernet interface did not support the maximum sample rate, we employed a new PCIe x4 interface that can tolerate 200M samples/s on baseband signals [6]. Through the PCIe X4 interface, the USRP X310 was connected with a desktop where an Intel i7-7700 3.6GHz processor CPU with 16G RAM and a 512GB SSD were installed.

We generated UHF-band signals with high samples by using the USRP X310. HODOR captured the generated signals with a sample rate of 5MS/s by using HackRF One. After
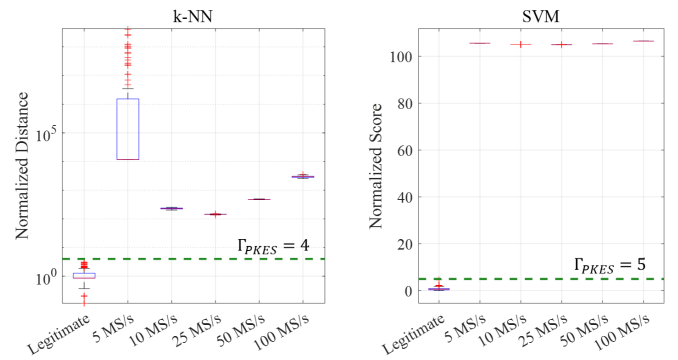
that, HODOR analyzed the features of the captured signals to compare the differences with those from a legitimate key fob. Considering the 200MHz of master clock rates (MCR) supported on the USRP X310, its sample rates must be an integer decimation rate of the MCR [8]. Accordingly, we performed experiments with sample rates of 10MS/s, 25MS/s, 50MS/s, and 100MS/s. Theoretically, 200MS/s is also possible on the USRP X310, but the signals with a sample rate of 200MS/s cannot be properly generated by our experimental setup. It seems that higher performing hardware is required. Fig. 20 shows the output distribution of the *attack with a high sample rate*. As shown in the Fig. 20, the attacks with a higher sample rate up to 25MS/s have a much closer output distance to those with legitimate signals. Rather, the output distance increases as the sample rate exceeds 50MS/s. We conclude that a higher sample rate is not helpful to impersonate a legitimate signal. However, it should be noted that this result is from an experiment done with a software-defined radio (SDR) device. For further research on high sample rate attacks, more state-of-the-art equipment is required, such as a pair of arbitrary function generators and a tunable mixer.

L. Dynamic Channel Conditions

A dynamic condition may decrease the performance of HODOR in identifying a legitimate key fob. We further evaluated HODOR under additional conditions, such as an underground parking lot and a roadside parking space as shown in Fig. 21. The underground parking lot had enough spaces for approximately 700 cars, and many cars were frequently entering and leaving the facility. Compared with an outdoor parking lot, it is expected that a greater number of multipath components are present because of the ceiling and thick concrete pillars, which can affect the performance of HODOR. In addition, we evaluated HODOR when the vehicle was parked on the road. This place was very crowded with pedestrians and moving vehicles. Furthermore, our evaluation was conducted during the most crowded hours of the day. For both environments, we placed the key fob in a backpack. Fig. 22 shows the output distribution of the k-NN and SVM algorithms as a function of place where the vehicle was parked. When the vehicle is parked in the underground parking lot, the k-NN and SVM algorithms output an FPR of 5% and 4% with an FNR of 0%. When the vehicle is parked in a roadside parking space, the k-NN and SVM algorithms output an FPR of 2% and 3% with an FNR of 0%. We should note
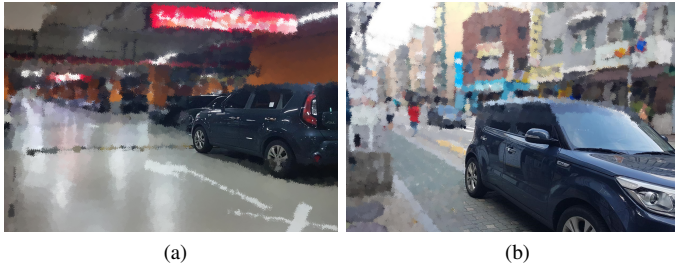
(a)   (b)

Fig. 21: Dynamic environment: (a) The vehicle parked in an underground parking lot, (b) The vehicle parked in a street parking space
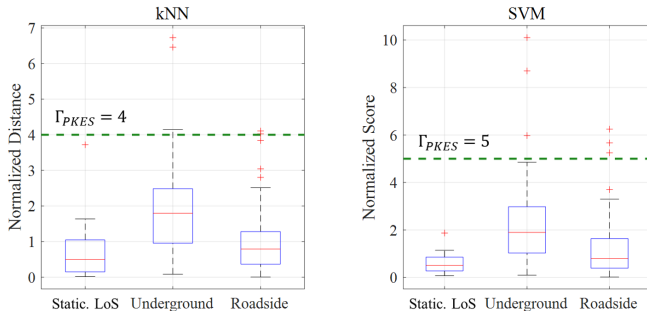

Fig. 22: Output distribution of k-NN and SVM algorithms as a function of parking space

that we used the same values for the threshold, Γ_{PKES}, as used in other evaluations. As can be seen in Fig. 14, HODOR displays weaker performance in dynamic environments than in static environments. It seems that interference due to multipath components affects the features that are analyzed in HODOR even though their RF signals originate from a legitimated key fob. However, we believe that this result is significantly meaningful, as it demonstrates that HODOR is able to identify a legitimate key fob even within a dynamic environment. Finally, we further evaluated feature importance under NLoS channel conditions, including dynamic environments. In the results, the *peak frequency* is the most salient feature followed by *kurtosis*, *SNR*, and *spectral brightness*, in that order.

VI. Related Works

In this section, we introduce existing demonstrations of attacks on keyless entry systems and device fingerprint techniques that have been proposed in previous studies.

A. Attacks on Keyless Entry Systems

Early keyless entry systems were designed without security considerations. More specifically, RKE systems deployed in Mercedes-Benz vehicles manufactured in the early 2000s still used fixed codes [40]. This means that these vehicles were vulnerable to replay attacks. To prevent replay attacks, a rolling code system using cryptography and a counter was installed in the RKE system. Although the rolling code provides an adequate level of security, several studies [35], [48] demonstrated the cryptographic weakness of the KEELOQ system via a cryptographic analysis. For example, Garcia et al.

[40] performed a comprehensive survey and security analysis of the RKE system implemented in vehicles manufactured by Volkswagen. The authors describe various types of RKE systems used in Volkswagen vehicles, and revealed that they were using a single worldwide secret key. Moreover, Benadjila et al. [22] demonstrate attacks on RKE systems using the Hitag-2 cryptographic algorithm. The authors demonstrate that it is possible to extract the rogue key (a.k.a. not the true secret key), while, in turn, exploiting a weakness of the Hitag-2 cryptographic algorithm. More recent studies further reveal a weakness of the AUT64 automotive cryptographic algorithm. In [45], the authors demonstrate the full details of AUT64 including a complete specification and analysis of a block cipher. The authors propose two key-recovery attacks based on cryptographic weakness. In addition to studies based on the weaknesses of cryptographic algorithms, roll jam attacks on RKE systems have also been studied [67]. In this type of attack, an adversary avoids being discovered by the victim while jamming and eavesdropping, and at the same time, obtains a valid rolling code. In this scenario, the car owner would not suspect an attack despite having pressed the button on their key fob twice to unlock the doors.

Alrabady et al. [20] also analyze potential attacks on PKES systems. The authors demonstrate several potential attacks on passive entry systems and propose solutions to protect vehicles from such attacks. However, to deploy these proposed solutions, the frequency band of the key fob and the vehicle would have to be altered, which forces the previous PKES system to be re-designed. The same authors also analyzed various types of security attacks against keyless entry systems and compared the attacks in terms of the vulnerability of the security mechanism deployed on the system, level of difficulty to mount the attacks, and equipment needed for the attacks [21]. Francillon et al. [38] pragmatically show a different type of attack on PKES systems, the so-called relay attack. The authors performed a comprehensive experiment and proposed two types of attack scenarios: wired and wireless relay attacks. In addition, [18] showed a similar but still different type of relay attack on PKES systems. In this work, adversaries were presumed to be extracting binary codes from RF signals and relaying these to another location. Although there is a maximum receiving time delay allowance in the PKES system, the authors showed that it was possible to overcome this constraint using cheap devices. Finally, in real car theft cases [10], [13], it was revealed that the adversaries amplified both the LF-band and UHF-band signals to mount a relay attack known as an amplification attack.

B. RF Device Fingerprinting

Depending on the signal region used to extract fingerprints, approaches can be categorized as transient-based, modulation-based, or other approaches [32]. Transient-based approaches use the turn-on/off transient of an RF signal for device identification. This approach has been applied to the identification of VHF FM transceivers or intrusion detection in a WLAN environment [36], [43]. However, transient signals have been reportedly acquired at distances close to the front-end antenna ($10 \sim 20$cm), and this is unfeasible in keyless entry systems. Modulation-based approaches extract features from the base band signal. In this study, the classifier achieves a classification error rate of 3% and 0.34% for the k-NN and SVM classifiers, respectively. However, to achieve this error rate, a high-end

vector signal analyzer [12] is necessary for signal acquisition.

Other approaches considered other regions of the RF signals to extract the fingerprints, such as the preamble of the packet. As such, Suski et al. [60] proposed a power spectrum density of the packet preamble to extract fingerprints. Jun et al. [46] also presented BlueID, which fingerprints the clock of a Bluetooth device. BlueID estimates the clock skew of a Bluetooth device applying the Generalized Hough Transform (GHT). In this work, 200 received preambles are required even though the time-stamp value is not required to calculate a clock skew. In a keyless entry system, however, the maximum five preambles can be received for attack detection. Recently, the authors of [27] proposed an RF-PUF which exploits the unique hardware characteristics of an RF device to an authenticated device. The main concept of HODOR is similar to that of an RF-PUF, given that both analyze RF signals to develop a security method, such as authentication or identification. However, in contrast to HODOR, multiple wireless devices used in an RF-PUF were simulated based on software implementation. HODOR was evaluated using physical hardware rather than simulations in environments while considering possible scenarios in the PKES system.

VII. Discussion

A. HODOR and Security

A threshold is a trade-off parameter in HODOR. If the output score of a UHF-band signal and its features is larger than the threshold, HODOR would determine that the signal is not from a legitimate key fob. In addition, HODOR is designed with a sufficiently large threshold so that it can tolerate some degree of error. For example, the environments under an NLoS channel and high-temperature variation cause a high noise level, and HODOR should tolerate a feature variation that occurs under these conditions. Because of this large threshold, on the other hand, HODOR might accept a UHF-band signal even if its features are not perfectly impersonated. We analyzed the difficulties of feature impersonation to additionally discuss HODOR's security in the following subsection.

B. Feature Impersonation

Difficulty of feature impersonation is another crucial factor in evaluating the security level of HODOR. Since HODOR employs multiple features for attack detection, the degree of feature impersonation difficulty should be discussed separately.

Peak frequency. The peak frequency represents the bit time characteristics of an individual device. In a digital relay attack and cryptographic attack, the peak frequency was clearly different between attack signals and legitimate signals. Because every RF device has a different bit time, it is possible to identify RF devices based on their bit time. Moreover, the peak frequency enables HODOR to identify RF devices even if they have identical components with each other. On the other hand, the playback attack that records and playbacks UHF-band signals from a legitimate key fob is able to similarly impersonate the peak frequency. However, even though the peak frequency was successfully impersonated by the playback attack, it fails to impersonate the spectral brightness and kurtosis which are affected by the ADC and DAC process.

SNR. Even though the SNR feature is effective in detecting single-band relay attacks, an adversary can impersonate the SNR of a legitimate signal by using an amplifier or by varying the distance from the vehicle. However, the both methods also affect kurtosis similar to the ways to impersonate the peak frequency feature. Using an amplifier especially increases noise level as well as the baseband signal level. Due to this amplified noise level, it is difficult to impersonate kurtosis while also impersonating SNR. In addition, channel condition between the two adversaries affect the kurtosis feature. An ideal analog filter would perfectly amplify only the baseband signal level, and not noise level. However, it is very difficult to design the ideal analog filter in practice because of the analog circuit complexity.

Spectral Brightness. The spectral brightness feature represents the amount of energy in a high-frequency region of signals. This feature is very helpful to detect attacks where new ADC and DAC processes occurs, such as in a playback attack. However, the spectral brightness of each key fob has a similar value. As a result, the attacks must be executed with identical components as the target key fob in order to impersonate the spectral brightness feature. However, different devices have different bit times that are represented by the peak frequency feature.

Kurtosis. The kurtosis feature was the most salient feature across the series of evaluations. Although the kurtosis feature is not helpful to detect the digital relay attack using identical components (i.e., other key fobs), it outperforms when the single-band relay attack and amplification attack are detected. However, the kurtosis feature of each key fob is similarly distributed as spectral brightness. This implies that an attack device with identical components as a target key fob is required to impersonate its kurtosis feature. Even if two devices are designed with identical components, as mentioned above, they have different bit times with each other, which are represented by peak frequency. Accordingly, if the kurtosis feature is successfully impersonated by using a device with identical components, its attack would be detected based on the different peak frequency of an attack signal.

C. Concern for Practicality

Although we evaluated HODOR under various environmental conditions, some results seem still insufficient for the practical usage of HODOR. It has been shown that HODOR has a relatively high FPR under dynamic conditions and temperature variation. Other than the conditions where we evaluated HODOR, more extreme environments certainly do exist that adversely affect accuracy. For this reason, HODOR should be further studied to develop additional features and algorithms that properly operate even in extreme environments. Subsequently, other processes will be performed together with HODOR to unlock doors. Regarding the total execution time for a door unlock command, HODOR should also be improved to shorten execution time. Otherwise, a driver may sense a lag when he/she attempts to unlock the doors. As a result, HODOR should be further studied to resolve these practical issues. Through our future research, it is expected that HODOR will improve and achieve the requirements for practical usage.

D. Scalability

The concept that analyzes RF signals can be applied to other modulations for secure proximity and distance measure-

ment. However, such analysis is beyond the scope of this paper and further research on the characteristics of baseband signals generated by other modulations is required. We suspect that HODOR may be applicable in other modulations for secure proximity and distance measurement since the hardware characteristics of an attack device and channel conditions affect the features.

VIII. Conclusion

In this paper, we presented HODOR as a sub-authentication system that supports manufacturer-installed support systems to prevent keyless entry system car theft. HODOR is an RF-fingerprinting method that distinguishes a legitimate door unlock request from a malicious attempt. Through our evaluation, we showed that HODOR is able to effectively detect simulated attacks that are defined in our attack model, while reducing the number of erroneous detection occurrences (i.e., false alarms). Furthermore, we found a set of suitable features in a number of environmental conditions, such as temperature variation, battery aging, and NLoS conditions, that make it possible for HODOR to properly operate in real-life environments. Finally, one especially noteworthy merit of HODOR is its design. It is designed such that it can be applied into an existing system without any hardware modifications. The only requirement for successful implementation is to add a device to sample UHF-band RF signals and analyze them. This novel characteristic of our method means that HODOR improves security without creating additional cumbersome or inconvenient processes for the user.

References

[1] "0.1-2ghz 64db gain rf broadband amplifier board low noise amplifier lna," https://www.banggood.com/0_1-2GHz-64dB-Gain-RF-Broadband-Amplifier-Board-Low-Noise-Amplifier-LNA-p-1237028.html?cur_warehouse=CN, (Accessed on 11/03/2018).

[2] "1-930mhz 2w rf broadband power amplifier module for radio transmission," https://www.banggood.com/1-930MHz-2W-RF-Broadband-Power-Amplifier-Module-For-Radio-Transmission-FM-HF-VHF-p-1095730.html?rmmds=buy&stayold=1&cur_warehouse=CN, (Accessed on 11/04/2018).

[3] "Hiletgo 0.1-2000mhz rf wideband amplifier 30db high gain low noise lna amplifier," https://www.amazon.com/HiLetgo-0-1-2000MHz-WideBand-Amplifier-Noise/dp/B01N2NJSGV/ref=sr_1_3?ie=UTF8&qid=1532962546&sr=8-3&keywords=low+noise+amplifier, (Accessed on 10/30/2018).

[4] "Ieee 802.15.4z task group," http://www.ieee802.org/15/pub/TG4z.html, (Accessed on 08/30/2019).

[5] "Panasonic cr2032 datasheet," http://www.cr2032.co/cms/prodimages/panasonic_cr2032_datasheet.pdf, (Accessed on 05/28/2019).

[6] "Pci-express connectivity kit (pcie desktop) — ettus research, a national instruments brand — the leader in software defined radio (sdr)," https://www.ettus.com/all-products/pcie-kit/, (Accessed on 09/07/2019).

[7] "Why perceived performance matters, part 1: The perception of time smashing magazine," https://www.smashingmagazine.com/2015/09/why-performance-matters-the-perception-of-time/, (Accessed on 05/12/2019).

[8] "X300/x310 - ettus knowledge base," https://kb.ettus.com/X300/X310, (Accessed on 10/09/2019).

[9] "Zabp-450-s+.pdf," https://ww3.minicircuits.com/pdfs/ZABP-450-S+.pdf, (Accessed on 10/06/2019).

[10] "Keyless system cars easy to steal, german car club finds - the local," https://www.thelocal.de/20160317/keyless-go-cars-easy-to-steal-german-car-club-shows, (Accessed on 07/29/2018).

[11] "This hacker's tiny device unlocks cars and opens garages — wired," https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/, (Accessed on 07/29/2018).

[12] "Agilent 89600s series vxi-based vector signal analyzers," http://literature.cdn.keysight.com/litweb/pdf/5968-9350E.pdf, (Accessed on 07/30/2018).

[13] "How to stop your car being stolen in 'relay crime' theft - bbc news," https://www.bbc.co.uk/news/av/uk-england-birmingham-42142023/how-to-stop-your-car-being-stolen-in-relay-crime-theft, (Accessed on 07/30/2018).

[14] "Rf explorer near field antenna kit - rf explorer - seeed studio," https://www.seeedstudio.com/RF-Explorer-Near-Field-Antenna-Kit-p-2784.html, (Accessed on 07/30/2018).

[15] "Sma cables," https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_ID=2888, (Accessed on 07/30/2018).

[16] "Train binary support vector machine (svm) classifier - matlab fitcsvm - mathworks deutschland," https://de.mathworks.com/help/stats/fitcsvm.html, (Accessed on 07/30/2018).

[17] "Usrp software defined radio (sdr) online catalog - ettus research," https://www.ettus.com/product, (Accessed on 07/30/2018).

[18] "Chasing cars: Keyless entry system attacks hitbsecconf2017 amsterdam," https://conference.hitb.org/hitbsecconf2017ams/sessions/chasing-cars-keyless-entry-system-attacks/, (Accessed on 08/01/2018).

[19] "Stolen cars - millions at risk of relay car hack: here's what it is and how to avoid it — express.co.uk," https://www.express.co.uk/life-style/cars/889437/stolen-car-theft-relay-hack-what-is-it-how-to-avoid-it, (Accessed on 11/19/2018).

[20] A. I. Alrabady and S. M. Mahmud, "Some attacks against vehicles' passive entry security systems and their solutions," *IEEE transactions on vehicular technology*, vol. 52, no. 2, pp. 431–439, 2003.

[21] ——, "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs," *IEEE transactions on vehicular technology*, vol. 54, no. 1, pp. 41–50, 2005.

[22] R. Benadjila, M. Renard, J. Lopes-Esteves, and C. Kasmi, "One car, two frames: attacks on hitag-2 remote keyless entry systems revisited," in *Proceedings of the 11th USENIX Conference on Offensive Technologies*. USENIX Association, 2017, pp. 19–19.

[23] E. Blossom, "Gnu radio: tools for exploring the radio frequency spectrum," *Linux journal*, vol. 2004, no. 122, p. 4, 2004.

[24] A. Bogdanov, "Linear slide attacks on the keeloq block cipher," in *Information Security and Cryptology*, D. Pei, M. Yung, D. Lin, and C. Wu, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 66–80.

[25] S. Brands and D. Chaum, "Distance-bounding protocols," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1993, pp. 344–359.

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

[27] B. Chatterjee, D. Das, S. Maity, and S. Sen, "Rf-puf: Enhancing iot security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388–398, 2018.

[28] K.-T. Cho, Y. Kim, and K. G. Shin, "Who killed my parked car?" *arXiv preprint arXiv:1801.07741*, 2018.

[29] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "Voltageids: Low-level communication characteristics for automotive intrusion detection system," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2114–2129, 2018.

[30] B. Danev and S. Capkun, "Transient-based identification of wireless sensor nodes," in *Proceedings of the 2009 International Conference on Information Processing in Sensor Networks*. IEEE Computer Society, 2009, pp. 25–36.

[31] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of rfid devices." in *Usenix Security Symposium*, 2009, pp. 199–214.

[32] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, p. 6, 2012.

[33] A. Das, N. Borisov, and M. Caesar, "Do you hear what i hear?: Fingerprinting smart devices through embedded acoustic components," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 441–452.

[34] S. Dey, N. Roy, W. Xu, R. R. Choudhury, and S. Nelakuditi, "Accelprint: Imperfections of accelerometers make smartphones trackable." in *NDSS*, 2014.

[35] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani, "On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme," in *Annual International Cryptology Conference*. Springer, 2008, pp. 203–220.

[36] K. Ellis and N. Serinken, "Characteristics of radio transmitter fingerprints," *Radio Science*, vol. 36, no. 4, pp. 585–597, 2001.

[37] B. L. Farris and J. J. Fitzgibbon, "Rolling code security system," Nov. 28 2000, uS Patent 6,154,544.

[38] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Eidgenössische Technische Hochschule Zürich, Department of Computer Science, 2011.

[39] G. S. Gadgets, "Hackrf one," 2017.

[40] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock it and still lose it-on the (in) security of automotive remote keyless entry systems." in *USENIX Security Symposium*, 2016.

[41] S. Gerasenko, A. Joshi, S. Rayaprolu, K. Ponnavaikko, and D. P. Agrawal, "Beacon signals: what, why, how, and where?" *Computer*, vol. 34, no. 10, pp. 108–110, 2001.

[42] I. Guyon and A. Elisseeff, "An introduction to variable and feature selection," *Journal of machine learning research*, vol. 3, no. Mar, pp. 1157–1182, 2003.

[43] J. Hall, M. Barbeau, and E. Kranakis, "Radio frequency fingerprinting for intrusion detection in wireless networks," *IEEE Transactions on Defendable and Secure Computing*, vol. 12, pp. 1–35, 2005.

[44] G. P. Hancke and M. G. Kuhn, "An rfid distance bounding protocol," in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*. IEEE, 2005, pp. 67–73.

[45] C. Hicks, F. D. Garcia, and D. Oswald, "Dismantling the aut64 automotive cipher," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 2, pp. 46–69, 2018.

[46] J. Huang, W. Albazrqaoe, and G. Xing, "Blueid: A practical system for bluetooth device identification," in *INFOCOM, 2014 Proceedings IEEE*. IEEE, 2014, pp. 2849–2857.

[47] V. Immler, "Breaking hitag 2 revisited," in *Security, Privacy, and Applied Cryptography Engineering*. Springer, 2012, pp. 126–143.

[48] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel, "A practical attack on keeloq," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2008, pp. 1–18.

[49] S. S. Khan and M. G. Madden, "One-class classification: taxonomy of study and review of techniques," *The Knowledge Engineering Review*, vol. 29, no. 3, pp. 345–374, 2014.

[50] K. Kira and L. A. Rendell, "The feature selection problem: Traditional methods and a new algorithm," in *Aaai*, vol. 2, 1992, pp. 129–134.

[51] R. Kohavi *et al.*, "A study of cross-validation and bootstrap for accuracy estimation and model selection," in *Ijcai*, vol. 14, no. 2. Montreal, Canada, 1995, pp. 1137–1145.

[52] P. Leu, M. Singh, and S. Capkun, "Message time of arrival codes: A fundamental primitive for secure distance measurement," 2019.

[53] S. J. Murdoch, "Hot or not: Revealing hidden services by their clock skew," in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 27–36.

[54] P.-S. Murvay and B. Groza, "Source identification using signal characteristics in controller area networks," *IEEE Signal Processing Letters*, vol. 21, no. 4, pp. 395–399, 2014.

[55] P. Padilla, J. Padilla, and J. Valenzuela-Valdes, "Radiofrequency identification of wireless devices based on rf fingerprinting," *Electronics Letters*, vol. 49, no. 22, p. 1409, 2013.

[56] R. Pi, "Raspberry pi model b," 2015.

[57] M. Singh, P. Leu, A. Abdou, and S. Capkun, "Uwb-ed: distance enlargement attack detection in ultra-wideband," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 73–88.

[58] M. Singh, P. Leu, and S. Capkun, "Uwb with pulse reordering: Securing ranging against relay and physical layer attacks." *IACR Cryptology ePrint Archive*, vol. 2017, p. 1240, 2017.

[59] B. Sklar and F. J. Harris, *Digital communications: fundamentals and applications*. Prentice-hall Englewood Cliffs, NJ, 1988, vol. 2001.

[60] W. C. Suski II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Using spectral fingerprints to improve wireless network security," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*. IEEE, 2008, pp. 1–5.

[61] R. Verdult, F. D. Garcia, and J. Balasch, "Gone in 360 seconds: Hijacking with hitag2," 2012.

[62] R. Verdult, F. D. Garcia, and B. Ege, "Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer." in *USENIX Security Symposium*, 2013, pp. 703–718.

[63] A. Verstegen, R. Verdult, and W. Bokslag, "Hitag 2 hell–brutally optimizing guess-and-determine attacks," in *12th USENIX Workshop on Offensive Technologies (WOOT 18)*, 2018.

[64] T. J. Waraksa, P. A. Michaels, S. A. Slaughter, J. A. Poirier, and I. B. Rea, "Rolling code for a keyless entry system," May 2 1995, uS Patent 5,412,379.

[65] B. Widrow and I. Kollár, "Quantization noise," *Cambridge University Press*, vol. 2, p. 5, 2008.

[66] L. Wouters, E. Marin, T. Ashur, B. Gierlichs, and B. Preneel, "Fast, furious and insecure: Passive keyless entry and start systems in modern supercars," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 66–85, 2019.

[67] Q. Yang and L. Huang, *Inside Radio: An Attack and Defense Guide*. Springer, 2018.

[68] D. Zanetti, B. Danev *et al.*, "Physical-layer identification of uhf rfid tags," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*. ACM, 2010, pp. 353–364.