Experimental Analyses of RF Fingerprint Technique for Securing Keyless Entry System in Modern Cars

Kyungho Joo
Korea University
khjoo0512@gmail.com

Wonsuk Choi
Hansung University
wonsuk@hansung.ac.kr

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

Abstract—**Background: Modern vehicles equipped with a keyless entry system prove more convenient for car owners. When a driver with a key fob is in the vicinity of their vehicle, doors are automatically unlocked. Unfortunately, however, 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 for added security, these keyless entry systems remain vulnerable to a range of signal-relaying types of attacks. This is because relayed signals result in valid packets that are verified as legitimate, and this makes it is difficult to distinguish a legitimate request from a malicious signal.**

Aim: To address these cyber security issues, we published research for our RF-fingerprinting method (coined "HOld the DOoR", `HODOR`) to detect attacks on keyless entry systems in the NDSS 2020 as the first attempt to exploit the RF-fingerprint technique in the automotive domain. We designed `HODOR` to operate as a sub-authentication method that supports existing authentication systems of keyless entry systems. HODOR does not require any modification of the main system to perform.

Results: Based on a series of real-world experiments, we demonstrated that HODOR competently and reliably detects attacks on keyless entry systems. Furthermore, we evaluated `HODOR` in different environments to reflect variations in temperature, non-line-of-sight (NLoS) conditions, and battery aging. In addition to the evaluation results in previous work, in this paper, we present deatils of an additional analysis into the difficulty of individual feature impersonation and performance at low sample rates.

Conclusions: `HODOR` is designed as a sub-authentication system to prevent keyless entry system car theft. Specifically, `HODOR` is an RF fingerprinting method that differentiates between a legitimate unlock request from a malicious attempt and a legitimate request. Through the evaluation results, we show that `HODOR` is able to effectively detect signal-relay types of attacks that are defined in our attack model, minimizing the number of erroneous detections (i.e., false alarms) at the same time. The only requirement for successful implementation of the `HODOR` is to add a device to sample UHF band RF signals and analyze them.

Learning from Authoritative Security Experiment Results (LASER) 2020
23 February 2020, San Diego, CA, USA
ISBN 1-891562-65-7
https://dx.doi.org/10.14722/laser.2020.23002
www.ndss-symposium.org

I. Introduction

Keyless entry systems have been developed and installed in modern vehicles to enhance the convenience of drivers. Traditionally, a physical key must be inserted to the key hole to unlock the doors of a vehicle. This traditional way to unlock doors was not only inconvenient but also vulnerable to physical key copying which leads to 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 most PKES systems are designed to include remote lock and unlock functions provided by the RKE system. However, as keyless entry systems are becoming commonplace in modern vehicles, cyber security attacks are also on the rise. Vehicle manufacturers, therefore, have applied their own security mechanisms to verify the request from the key fobs. In particular, encryption with a pre-shared, long-term secret key and rolling codes [23], [44] are common methods used to verify a legitimate key fob.

Despite these security mechanisms, several vulnerabilities with keyless entry systems have been discovered in the past decade. In 2010, researchers demonstrated a relay attack on PKES systems, in which vehicle doors were unlocked [24]. In the relay attack, two 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 can 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 [6], [12]. 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 [13], [26], [29], [30], [42], [46], [47].

The underlying reason of the aforementioned cyber security

attacks on the keyless entry system is that radio frequency (RF) signals emitted from key fobs can be relayed regardless of active security methods like encryption or authentication. Since the keyless entry system considers any request for authentication as valid signals, extension of the communication range by relaying or forwarding a signal ultimately enables an attacker to unlock car doors. One approach to address this issue might be the use of an RF distance-bounding protocol that verifies the actual physical proximity of a request [16], [28]. 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], [36], [39], [40]. 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 [17], [19], [20], [38], [49], 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. Our 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 modifications to the current communication system. Building on our work as published in NDSS, 2020, this research presents a comprehensive analysis on the experimental results of HODOR. As an addition to the NDSS 2020 paper [31], we further present in this paper a comprehensive analysis on HODOR experimental results. We analyzed the difficulty of individual feature impersonation and performance at low sample rates. Our experimental results show that HODOR precisely and accurately detects several types of attack attempts.

II. Background

This section presents the system overview of HODOR presented in the NDSS 2020 paper [31], including how HODOR detects malicious attacks on keyless entry systems. For a clear understanding of HODOR, we define the attack model and adversaries' 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 is equipped with an RF receiver and mounted to the vehicle and integrated with the

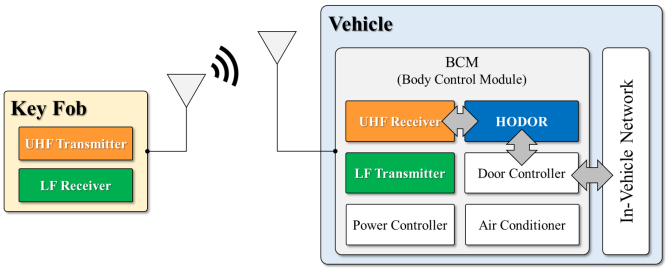


Fig. 1: System model

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. 1 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. Three types of attacks against the PKES system are described in the attack model as to how the attacker passes a valid message that the adversary can unlock the door. For a relay attack, we categorized these into **Single-band relay attack** and **Dual-band relay attack**. In this model, two adversaries must cooperate to perform either a single-band or dual-band relay attack because relayed signals are forwarded and injected in this model to extend the communication range. In a **Cryptographic attack**, however, there is a single adversary who attempts to unlock doors on the keyless entry system.

*1) **Single-band relay attacks**:* In the PKES system, a vehicle transmits a verification request (i.e. challenge message) to the corresponding key fob using the LF-band RFID communication. When the key fob receives the request, it automatically responds to the vehicle using the UHF band RFID communication. 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, adversaries force the key fob to 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 can differ by 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 in this attack scenario.

*2) **Dual-band relay attacks**:* 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 [6], [12], 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 [11]. 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 process to forward a binary information contained in LF/UHF-band signal.

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 IV, 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 forward and inject attack signals. Adversaries perform demodulation and decoding processes on LF/UHF band signals to exchange the binary information contained in legitimate signals to each other. Adversaries can deliver binary information through various wireless communication systems such as Wi-Fi or Bluetooth. After receiving the valid binary information, the adversary injects the attack signal through the encoding and modulation process, which is a reverse order of the demodulation and decoding process. The noteworthy advantage of digital relay attacks is that adversaries can achieve a much larger range of communication than single-band relay attacks or amplification attacks, which enhance the stealthiness of the attack. This is because the adversaries relay binary information through state-of-the-art wireless digital communication, not an analog UHF-band signal. However, since most PKES systems assign a maximum delay [24], 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 [11].

3) ***Cryptographic attacks****:* In cryptographic attacks, attackers exploit the weaknesses of cryptographic algorithms built into PKES systems. 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 attacker performs a cryptographic analysis to extract the long-term secret key. As a result, it is possible to inject a valid UHF band signal in response to challenge signals from vehicles at any time. 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 [46]. Researchers have uncovered that the outdated proprietary cipher DST40 has been mounted to the Telsa Model S. More recently, it was revealed that another outdated proprietary cipher DST80 was implemented on the vehicles manufactured by Hyundai and Toyota [47]. Furthermore, unrevealed PKES systems with weak cryptographic algorithms or poor key management [26] are also expected to be vulnerable to a cryptograhic attack. 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, given that the adversary extracts the binary code and injects the attack signal.

4) ***Attacks on RKE systems****:* Attacks on PKES systems are categorized into single-band relay, dual-band relay, and cryptographic attacks. In addition, previous studies have shown that an attacker can compromise a long-term secret key that is used in an RKE system through reverse engineering [13], [15], [29], [42], an exhaustive key search [30], [43], or combining both methods [26]. As a result, attackers can generate valid packets in a manner similar to cryptographic attacks. 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 simultaneously eavesdrops on valid UHF signals. When the driver (victim) presses the unlock button on the remote key fob, the vehicle remains locked because the signal has been blocked by the jamming attack, and the driver (victim) 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.

III. Our Method: HODOR

A. Overview

In this section, we demonstrate our design decisions to realize HODOR. Fig. 2 shows an overall architecture of HODOR. HODOR aims at detecting an attack signal using a one-class classifier which is created by features extracted from legitimate signals only. There are two main phases: 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 of features per RF signal are extracted and the classifier is trained. In addition, normalization parameters, which are used for output normalization in the *Attack Detection* phase, are computed. In the *Attack Detection* phase, HODOR is now able to detect any attacks defined in our attack model in Section II-B. 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, based on the normalized output of classifier and pre-defined threshold, HODOR makes a decision whether the received RF signal has been transmitted from a legitimate key fob or not. In an invalid case, when the normalized output exceeds the threshold, the corresponding

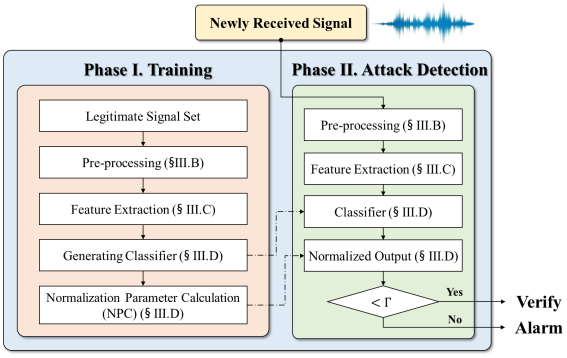


Fig. 2: Overview of HODOR architecture

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. 3. The received signal includes a carrier signal $c(t)$, baseband signal $s(t)$, and channel noise $n(t)$ which are denoted as follows.

$$r(t) = s(t) \otimes c(t) + n(t) \tag{1}$$

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 passband signal is shifted back down to the baseband by mixing the sinusoidal signal at the same carrier frequency as follows.

$$r[t] \otimes c[t] = s[t] + n[t] \otimes c[t] \tag{2}$$

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 II-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. This is because the received signal strength (RSS) is highly effected by a channel condition, it would be difficult to reliably extract the features under the same 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.

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

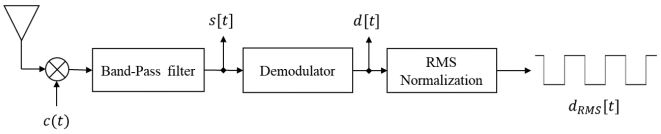
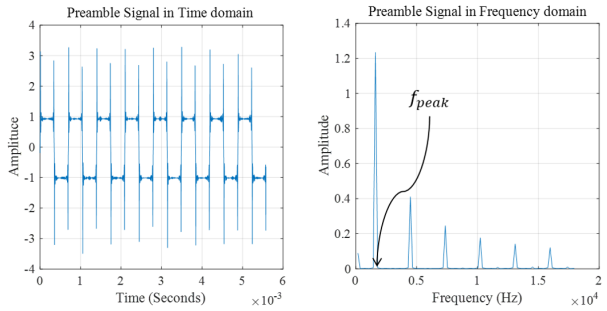


Fig. 3: Preprocessing block diagram



(a) (b)

Fig. 4: Preamble signal in time and frequency domains: (a) Preamble signal in time domain, (b) Preamble signal in frequency domain

C. Feature Extraction

After the preprocessing phase, 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) region is used to synchronize the clock between a transceiver and a receiver. Preamble region 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. We first extract the peak frequency feature from a frequency domain. Since the preamble region of a time-domain pulse signal is given, it must be transformed to the frequency-domain signal by fast fourier transform (FFT). Fig. 4 shows the preamble region 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 of the preamble signal. The peak frequency (f_{peak}) is the frequency where the highest amplitude value exists as follows.

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

where $D_{RMS}[f]$ is the FFT result of $d_{RMS}[t]$. The peak frequency feature represents the characteristic of a hardware clock source used for micro controllers. Due to the imperfection of clock sources, different peak frequency values can be extracted from different key fobs. Accordingly, this feature is used to distinguish a legitimate key fob from other RF 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 sinusoidal baseband signal s[t]. As each key fob has a non-ideal carrier frequency f_c' (i.e., deviated from 433.92MHz) due to the hardware imperfection, the RF receiver reliably receives signals from the key fob [48] in a real vehicle. This imperfection also occurs in the receiver, which leads the non-ideal frequency of f_c'' when generating $c(t)$. Consequently, on the receiver side, 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 another 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.

$$SNR_{dB} = 10\log_{10}\frac{P_{signal}}{P_{noise}} \tag{5}$$

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 a PKES system, UHF band RF signals emitted at a distance greater than the LF band communication range must be considered malicious even if the signal is transmitted from a legitimate key fob. Since the SNR are easily effected by channel conditions, it is possible to estimate the path loss or attenuation in power level of the signal propagating through the path. HODOR can analyze the SNR feature to see if a received signal is generated in a vicinity of the vehicle.

Statistical features. A set of statistical functions was also employed to support the aforementioned feature. Statistical features indicate various characteristics of the sampled signal. As a result, numerous studies in the area of signal processing and wireless communication employed statistical features to identify nodes or channels [21], [22], [37]. Statistical features were used to differentiate attack signals because the hardware characteristics and channel conditions of the attack device distort the legitimate signal characteristics. With the three crafted features and 20 statistical features used in [21], we ran a feature selection algorithm to eliminate features that are not beneficial to performance. Then, we selected the top 5 best features and decided not to use all 23 while testing HODOR, taking into account execution time during the feature extraction phase. As more features are used, more execution time is required to extract the features, and this time delay hinders user convenience. Moreover, the risk of an overfitting problem can occur when a large number of features are included, and thus, we performed an exhaustive feature selection by limiting the number to five [27]. 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 a signal sampled in the time domain. As signals propagate through the air, noise signals and multi-path signals distort the signal quality. In addition, pass-band signals and noise signals are also enhanced by analog amplifiers, so external amplification affects the signal kurtosis. Thus, single-band relay and amplification attacks have a higher kurtosis value than a legitimate signal. The kurtosis is calculated as follows:

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

where μ and σ are the mean and standard deviation of the d_{RMS}, respectively. Spectral brightness is the amount of spectral energy that exhibit in a frequency band above a given cutoff frequency. In a playback attack, the adversary records the legitimate signal and injects (playbacks) to the vehicle. During this process, the baseband RF signal is digitally sampled through an analog-to-digital converter (ADC). However, digital sampling introduces quantization errors due to the non-ideal sampling rate and vertical resolution of the ADC. When the attack is mounted, recorded samples are reconstructed into an analog baseband signal via a digital-to-analog converter (DAC). At this point, the quantization error introduced during digital sampling affects the spectral density of the reconstructed signal [45]. Spectral brightness is calculated as follows.

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

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

Algorithm 1 Attack detection for the PKES system

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

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

D. Training and Attack Detection

For the attack detection process, HODOR requires one-class classifiers. One-class classifiers are generated with a

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}

set of features extracted exclusively from a legitimate key fob. Feature extraction during training can only occur through legitimate key fob, and classifiers are generated through semi-supervised learning. Table I shows the features used for each modulation scheme. After the classifier is trained, HODOR assigns a threshold for each classifier. When considering the implementation in real vehicles, it is necessary to assign the same threshold to a specific key fob model. For this requirement, HODOR compensates for the difference in feature distribution between key fobs by performing z-normalization on the output of the classifier. Z-normalization computes 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 [35], 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 computes 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 the output of the classifier is not within the indicated threshold (Γ), the input is considered malicious. The evaluation set the appropriate threshold for each keyless entry system, as in the following chapter. Finally, HODOR rejects the request to unlock the door if the output of classifier exceeds the threshold. The algorithm 1 shows the operation HODOR during training and attack detection.

IV. Evaluation

In this section, we report the evaluation results for HODOR to show that the system accurately detects attacks defined in Section II-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 conducted a series of experiments on real vehicles, the 2014 Kia Soul and the 2016 Volkswagen Tiguan. Both vehicle models are equipped with a PKES system. In the case of the Soul, FSK modulation was used and a center frequency of 433.92 MHz with a frequency deviation of 30 kHz was assigned for UHF band RF communication. For the Tiguan, ASK modulation with a center frequency of 433.92 MHz was used for UHF band RF communication.

RF Signal Receiver and Transmitter. Two types of software-defined radio (SDR) devices were used for the transmission and acquisition of UHF band RF signals for the evaluation of HODOR. SDR is a radio communication system that replaces hardware components with a software module. HackRF One [25] was used to sample the UHF-band RF signals, and the other HackRF One coupled with a universal software radio peripheral (USRP) X310 [10] was used to generate UHF-band RF signals that were to be simulated as attack signals. With GNU Radio [14], the preprocessing steps of HODOR have been implemented in the virtual hardware component. We set the sampling rate of SDR to 5M samples/sec on both vehicle models. The specifications of the communication system depend on the two vehicle models, so different parameters were assigned to receive signals from 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 33kHz. Ideally, the transition width of the filter should be zero. However, because real communication systems have an inevitable frequency offset, the receiver must be designed with a wider bandwidth than the ideal scenario. Therefore, we set the bandwidth of the bandpass filter to have a larger margin and found certain parameters heuristically. Therefore, the high and low cutoff frequencies and transition widths of the bandpass filters were set to 15kHz, 45kHz and 10kHz respectively. In addition, the LF-band RF signals were relayed by an SMA cable [8] and a loop antenna [7] 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.*

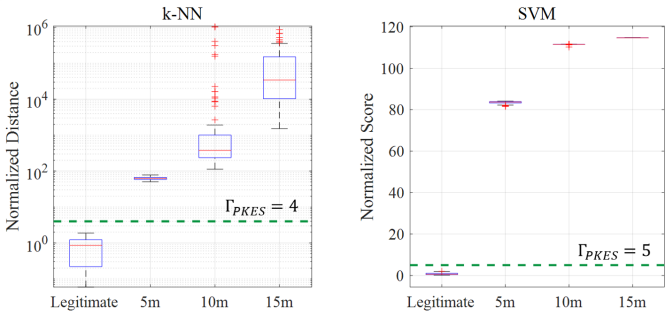


Fig. 5: Output distributions of k-NN and SVM algorithms as a function of distance in a single-band relay attack

Classification Algorithm. Classification algorithms are generally categorized as one-class or multi-class classification. Considering the practical implementation, it is impossible to train all the malicious attack signals. Therefore, the classifier must train a set of features extracted from a legitimate key fob. In other words, to deal with an unknown attack on HODOR, a semi-supervised one-class classification is required. In our evaluation, a one-class support vector machine (SVM) and a k-nearest neighbor (k-NN) algorithm were used for [32]. The SVM and k-NN algorithms provided by MatLab 2017a [9] were employed with the default parameters. More specifically, RBF (Radial Basic Function) was used for the SVM algorithm, and a standardized Euclidean distance with the parameter k of 1 was applied to the k-NN algorithm. For each classifier, we collected a set of 100 UHF-band RF signals from a

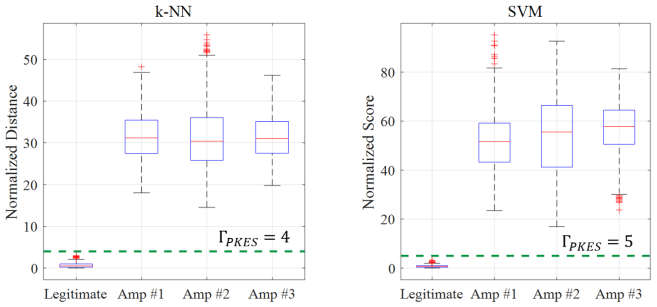


Fig. 6: Output distribution of the k-NN and SVM algorithms as a function of amplifiers in an amplification attack

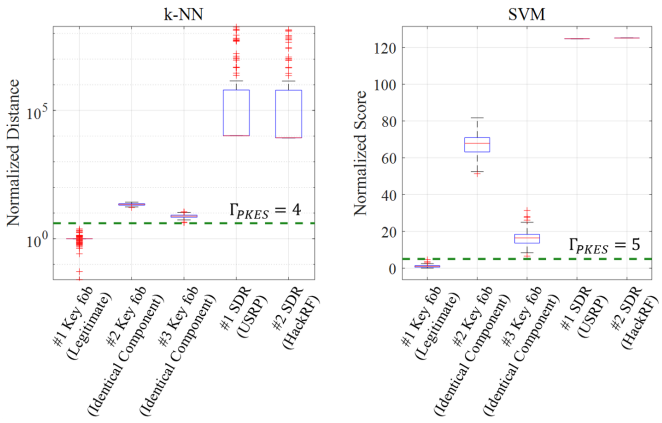


Fig. 7: Output distribution of the k-NN and SVM algorithms as a function of devices in a digital relay attack

legitimate key fob at a one-meter distance, and used them for training the classifiers. As with the training dataset, same as training dataset, 100 attack signal were collected in every attack scenario.

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) [27]. In our evaluation, TP refers to a case where HODOR identified an attack signal as an attack. On the other hand, TN refers to a case where HODOR considered a legitimate signal to be a legitimate signal. FP indicates a case where HODOR considers a legitimate signal to be an attack, and FN indicates a case where HODOR considers an attack signal to be a legitimate signal. In the keyless entry system, it would only take a single FN case 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 a single band relay attack, the LF band signal was relayed to trigger the key fob even if it is out of range of the pre-defined communication. An SMA cable and RF amplifier are used to minimize path loss and amplifies the LF band signals. The UHF band RF signal emitted from the key fob was then sampled while varying the distance between the vehicle and the key fob (5m, 10m and 15m). HackRF One which records the UHF band signal and performs preprocessing process is located at the vehicle side and controlled by a laptop. More than 10 meters away from the vehicle, it was hard to reliably inject the LF band signal to the key fob due to the signal attenuation. Therefore, we used an RF amplifier to increase the signal strength of the LF band signal to relay it to the key fob from more than 10 meters away. In addition, to capture a legitimate signal used for generating the classifier, we set the distance between HackRF One and the key ring to 1 meter under LoS conditions. Fig. 5 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 as an attack on the PKES system. When the key fob is placed at a distance of 5m, both the k-NN and SVM algorithms 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 key fob placed at the distances of 10 or 15m. Intuitively, as the distance increased, we observed that it became easier to detect a single-band relay attack.

C. Dual-Band Relay Attack Detection

We evaluate attack detection performance against two types of dual-band attacks, (i.e., amplification attack and digital relay attack) which are demonstrated in Section II-B. 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 victims and enhance the stealthiness, 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. In this case, even if a key fob out of the communication range of the UHF-band signal, a dual-band relay attack could still successfully unlock doors.

1) Amplification attacks: To simulate a amplification attack, we first applied RF amplifiers to extend the UHF-band communication range. During an amplification attack, the adversary amplifies and forwards the UHF-band signals to the vehicle. To minimize path loss between the key fob and RF amplifier, we directly placed the RF amplifier next to the key fob. Therefore, the UHF-band RF signals can achieve a higher signal strength than the original communication. In addition, we assumed that 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. Among the bandpass filters for MiniCircuits, we selected one with a most similar bandwidth to the UHF-band [5]. The low and high cut-off frequencies of the bandpass filter are 400MHz and 510MHz, respectively. The pre- and post-bandpass filters were respectively connected to the input and output ports of each amplifier. Deviating slightly from the attack model in Section II-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 II-B, HODOR sampled the amplified UHF-band signals, which had been directly forwarded and injected by the adversary on the key fob side. We assumed a strong adversary who would be able to adjust the SNR level using a tunable RF amplifier or directional antenna, and as such, we set the distance between the adversary (i.e. key fob) and vehicle to the point where the SNR level is equal to that of the legitimate signal. This experimental setup implies that when the adversary injects an attack signal with a higher SNR than a legitimate signal, HODOR can easily detect the amplification attack. We found that the adversary would be able to achieve the same SNR level as a legitimate signal at a distance between 20 and 25 meters. Based on this observation, we sampled forwarded signals on the vehicle side. Fig. 6 shows the output distributions of the k-NN and SVM algorithms as a function of the amplifiers. As seen in Fig. 6, even if the distance between the key fob and vehicle is much 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. 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 noise signals within the bandwidth of the digital bandpass filter. As a result, we concluded that HODOR is able to detect an amplification attack even when pre- and post-analog filters are used.

2) Digital relay attacks: We first extracted the binary information from the ACK signal to simulate a digital relay attack. The SDR device was then used to inject the attack signal according to the modulation scheme of the target PKES system. Each key fob's ACK signal is unique but contains static binary information. When the vehicle receives the ACK signal, multiple ECUs are activated to transmit CAN packets. This *standby* function is implemented in modern vehicles for enhanced driver convenience [18]. Based on this observation, we analyzed the in-vehicle network (e.g. CAN bus) to see whether the vehicle accepts the attack signal. In addition to SDR devices, we further expanded the capability of the digital relay attacker. In theory, the most powerful adversary would be someone with access to the same electronic components as the target key fob. In practice, however, the assumption that a digital relay attacker will have exactly the same electronic components can be perceived as overly cautious. Despite the overestimated capability of an adversary, we further evaluated HODOR against this hypothetical adversary. For the Kia Soul, one key fob out of three was 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. 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 GNU Radio. Following the process of Attack Detection phase, the newly received UHF-band RF signals were sampled and analyzed by HODOR. Fig. 7 shows the output distributions of k-NN and SVM algorithms as a function of RF 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. 7, the output distribution from the remaining 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 addition, as mentioned in Section II-B, a cryptographic attack can also be simulated in the same way. Therefore, this evaluation result can be considered as the attack detection results on the 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 digital relay attacks and cryptographic attacks.

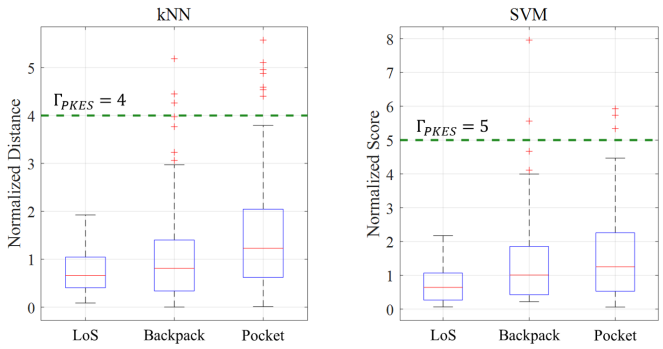


Fig. 8: Output distributions of the k-NN and SVM algorithms as a function of where a key fob is placed

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

In this experiment, the UHF band RF signals were sampled from a key fob placed in a pocket or backpack to show that the features used in the HODOR is robust under NLoS conditions. In the PKES system, car owners can open the door without physically producing a key fob at the storage location. Owning to this, we trained the classifier with UHF band RF signals sampled under LoS conditions. Then, we tested the classifier with the signals collected from the key fob which is placed in a pocket and backpack. Fig. 8 shows the output distribution 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%. Same as previous experiments, thresholds (Γ_{PKES}) were respectively assigned to 4 and 5 for each algorithm. From these results, we conclude that HODOR properly identifies a legitimate door unlock request even when in an NLoS condition. Additionally, we evaluated HODOR under various environmental conditions such as temperature variation, battery aging, and parking spaces. We would like to refer the readers to [31] for further references of our evaluation results.

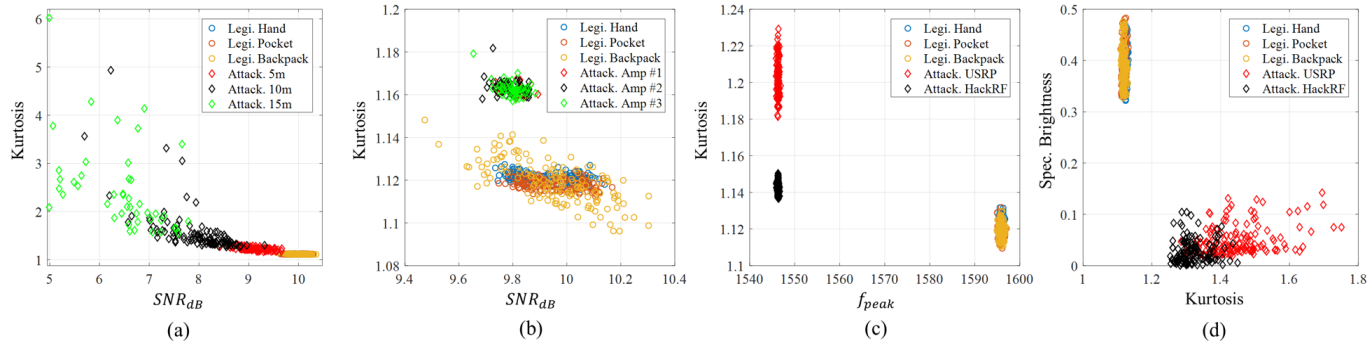


Fig. 9: Scatter plot of the top two features of the Soul as a function of an attack scenario: (a) Single-band relay attack, (b) Amplification attack, (c) Digital relay attack, (d) Playback attack

TABLE II: 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

E. Feature Importance

We minimized the feature set through the exhaustive search in Section III. 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 [33]. 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 by how they correspond to each attack detection experiment. Table II shows the rankings of the features as a function of each attack scenario. The scatter plot of the top two features in each attack scenario are represented in Fig. 9. In a single-band relay and amplification attack, SNR_{dB} and kurtosis are effective features to detect attacks. 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 legitimate key fob and the attack devices including other key fobs and SDRs (i.e., USRP and HackRF). Though not as effective as f_{peak}, kurtosis is also useful to detect the digital relay attack. In a playback attack, due to the quantization error, spectral brightness and kurtosis are both effective features to differentiate attack signals.

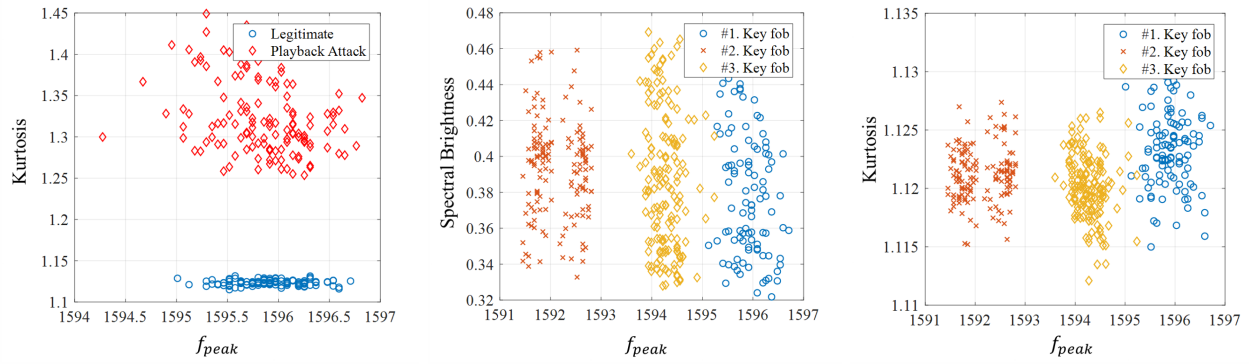
F. Difficulty of Feature Impersonation

The 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 analyzed separately.

Peak frequency. Peak frequency represents the bit time characteristics of an individual device. In our digital relay attack and cryptographic attack, peak frequency was able to clearly differentiate the attack signals from the legitimate signals. Since every RF device has a different clock source (i.e. osciallator), it is possible to identify RF devices based on bit time characteristics. Moreover, HODOR identified RF devices even if they share identical components using peak frequency feature. Similarly, however, a playback attacker can similarly impersonate the peak frequency. Fig.10a shows the scatter plot of peak frequency and kurtosis of legitimate signals versus playback attack signals. Even though the peak frequency was successfully impersonated by the playback attacker, kurtosis feature, which are affected by the ADC and DAC process, could not be impersonated by the attacker.

SNR. Even though the SNR feature is effective to detect a single-band relay attack, an adversary can impersonate the SNR of a legitimate signal by using an tunable amplifier with a directional antenna or varying the distance from the vehicle. However, both methods also affect kurtosis. Using an RF amplifier increases noise level as well as the baseband signal level. This phenomenon is formulated by the Noise Figure term [41]. Due to this amplified noise level, it is difficult to impersonate kurtosis while simultaneously impersonating the SNR. In addition, channel conditions between the two adversaries also affect kurtosis. An ideal analog filter would perfectly amplify only the baseband signal level and not the noise level; however, it is extremely difficult to design a perfect analog filter in practice due to the complexity of analog circuits.

Spectral Brightness. Spectral brightness represents the amount of energy in the high-frequency region of signals. This feature is very helpful to detect attacks where an additional ADC and DAC process occurs, like in a playback attack. Fig.10b shows the scatter plot of peak frequency and spectral brightness for each key fob. The plot illustrates that spectral brightness for each key fob is similar in value. As a result, attacks must be carried out with identical components as the target key fob in order to accurately impersonate spectral brightness. However, devices have different bit times that are represented by peak frequency.



(a) (b) (c)

Fig. 10: Scatter plot of features from Soul: (a) Legitimate *Peak frequency* and *Kurtosis* of playback attack signals, (b) *Peak frequency* and *Spectral Brightness* of legitimate key fobs, (c) *Peak frequency* and *Kurtosis* of legitimate key fobs

Kurtosis. Kurtosis was the most salient feature across our series of evaluations. Although it was not helpful to detect digital relay attacks using identical components (i.e., other key fobs), it outperforms in detecting signal-band relay attacks and amplification attacks. As shown in Fig.10c, values for kurtosis are similarly distributed to that of spectral brightness. This implies that an attack device with identical components as a target key fob would be necessary to impersonate the corresponding kurtosis. Even if two devices were designed with identical components, as mentioned above, they would have different bit times represented by peak frequency. Accordingly, assuming that kurtosis was successfully impersonated by using a device with identical components, the attack would still be detected by the incongruent peak frequency of the attack signal.

G. Low sample rate

A sample rate is the average number of samples obtained in one second (samples per second). A high sample rate reconstructs the original signal accurately which leads to precise feature extraction. However, it requires a big memory size to store samples and long execution time for feature extraction. While environmental changes and channel conditions, which have been considered in previous experiments that focused on usability, the sample rate is another factor that is related to the expense of HODOR. To simulate the different sample rate conditions, we selected the #1 key fob of Soul and downsampled to 2.5MS/s, 1MS/s, 500kS/s and 250kS/s, respectively. In addition, we set the same threshold of k-NN and SVM algorithm as previous experiments, which are 4 and 5, respectively. Then, we computed FPR under different channel conditions. On the other hand, to evaluate the attack detection performance in low sample rate, we computed the FNR under dual-band relay attack scenarios. It should be noted that the goal of HODOR is to minimize the FPR at the 0 % of FNR. As seen in the Table III, the overall FPR was increased as the sample rate was decreased. In the case of attack detection, HODOR output 0% of FNR in most cases. Even in the sample rate of 250kS/s, which is 20 times lower than the original sample rate, HODOR effectively differentiates the amplification attack signal with an analog band-pass filter and #2 key fob. However, there was a FNR of non-zero percentage when differentiating the signals from the #3 key fob. This is because the low sample rate is insufficient to differentiate the feature (i.e. *peak frequency*) from the #3 key fob which was manufactured in the same year and month as #1 key fob. Therefore, to achieve the 0 % of FNR in low sample rate, a threshold of lower value is required. However, since the threshold is a trade-off parameter between the security and the usability, it leads to a higher FPR which hinders the driver's convenience. Based on the experimental results, we conclude that the minimum sample rate of 2.5MS/s is required for a practical deployment.

V. Discussion

A. HODOR and Security

A threshold is a trade-off parameter in HODOR's mechanism. If the output score of the classifier is greater than the threshold, HODOR determines that the signal is not transmitted from a legitimate key fob. Also, HODOR is designed with a sufficiently large threshold to minimize a false alarm. For example, high noise levels and multi-path fading occur in NLoS channels and high temperature fluctuating environments, and HODOR must tolerate feature distortion that occur under these conditions. On the other hand, due to this large threshold, HODOR might accept UHF band signals even if the feature is not perfectly impersonated. Therefore, it is essential to properly define the threshold to balance between security and usability.

B. Concern for Practicality

We evaluated HODOR under various environmental conditions, but some results are still insufficient for actual use of HODOR. HODOR has been shown to have a relatively high FPR under dynamic conditions and temperature changes. In addition to the conditions under which HODOR is evaluated, there are more extreme environments that adversely affect accuracy. For this reason, it is necessary to further study HODOR to develop additional functions and algorithms that work correctly even in extreme environments. After that, another process is performed with HODOR to unlock the door. HODOR should also be improved to shorten execution time with respect to the total

TABLE III: Experimental results of FPR and FNR as a function of channel conditions and attack scenarios

Algorithm	Sample Rate	Channel Condition (FPR, %)				Attack Scenario (FNR, %)		
		Bag	Pocket	Underground	Roadside	Amplification attack w/ analog band-pass filter	Digital relay attack (#2 Key fob)	Digital relay attack (#3 Key fob)
k-NN	2.5MS/s	2	0	4.35	2.17	0	0	0
	1MS/s	2	6.5	2.17	5.25	0	0	1.8
	500kS/s	5.33	8.7	8.7	5.19	0	0	5.06
	250kS/s	6.52	10.57	13.04	10.39	0	0	38.75
SVM	2.5MS/s	1.3	0	4.35	5.75	0	0	0.63
	1MS/s	2	0	6.52	6	0	0	2.5
	500kS/s	2	1.7	10.87	5.5	0	0	5.93
	250kS/s	10.8	2	21.74	5	0	0	8.75

execution time of the unlock door command. Otherwise, the driver may feel frustrated when trying to unlock the door. As a result, to solve these practical problems, HODOR must be further studied. We expect that in future studies HODOR will improve and achieve the requirements for practical usage.

VI. Lessons Learned

We provide several of our observations during evaluations that would be useful to the community performing further research on RF fingerprint technique.

Experimental setup. To evaluate HODOR in real-world conditions, we employed an actual vehicle and collected the UHF band signals under various channel conditions. More specifically, we located the key fob in a backpack, pocket, and both an underground parking lot, and outdoor parking space. In addition, we simulated the series of relay attacks using the loop antenna and SMA cable, RF amplifier, and SDR devices. Through the evaluation results, we observed that the channel condition induces much more feature variation rather than environmental changes. Therefore, in future work, it is required to extract a feature set which is robust against various channel conditions in real-world scenarios.

Evaluation Metrics. There are various performance metrics used to evaluate the attack detection/prevention system. For example, F-1 Score which calculates the harmonic of Precision and Recall is a well-known metric to evaluate the accuracy of a system. In our work, HODOR, we used the FPR under the 0 % of FNR. FP refers to the case in which HODOR considered a legitimate signal as an attack. On the other hand, and FN refers to the case in which HODOR considered an attack signal as legitimate. This is because it would only take a single FN case in the keyless entry system to result in a car theft. For this reason, we set the objective FNR as 0%, under the belief that FNR should take precedence over FPR. However, through our evaluations, we observed that there are non-zero false positive cases which hinders the driver's convenience. Considering the practical implementation, it is essential to minimize the false alarm cases. To cope with these potential issues, it is possible to employ an attack counter method to alleviate the sensitivity of the HODOR. In this method, HODOR raises an alarm only if the attack counter exceeds a pre-defined threshold [34].

Feature Impersonation Attack. A feature impersonation attack is the most threatening attack type on a fingerprint-based identification system. To evaluate the security of HODOR, we discussed the difficulty of impersonating the feature set at the same time. However, an attacker equipped with a high-performance signal generator might successfully impersonate the feature set. In future work, it is required to employ a high-performance signal generator and evaluate the attack success probability on fingerprint-based identification system.

VII. Conclusion

In this paper, we presented the experimental details and lessons learned during the evaluation of HODOR presented in the NDSS 2020. HODOR is designed as a sub-authentication system to prevent car theft of the keyless entry systems. HODOR is an RF fingerprinting method that distinguishes legitimate door unlock requests from malicious attempts. Through our evaluation, we showed that HODOR can effectively reduce the number of false detections (i.e., false alarms) while effectively detecting attacks defined in our attack model. In addition, we found a suitable set of features to make HODOR work properly in real-world environments such as temperature change, battery aging, and NLoS condition. Finally, the noteworthy advantage of HODOR is its design. It is designed to be applied to existing systems without hardware modification. For a successful implementation, it is required to add a device to sample and analyze the UHF band RF signal. This novel characteristic of our method means that HODOR improves security without creating additional cumbersome or inconvenient processes for the user.

Acknowledgments

The authors would like to thank the shepherd, David Balenson, for constructive suggestions. This work was supported by Samsung Research Funding & Incubation Center for Future Technology under Project Number SRFC-TB1403-51.

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

[6] "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).

[7] "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).

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

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

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

[11] "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).

[12] "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).

[13] 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.

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

[15] 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.

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

[17] 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.

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

[19] 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.

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

[21] 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.

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

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

[24] 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.

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

[26] 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.

[27] 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.

[28] 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.

[29] 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.

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

[31] K. Joo, W. Choi, and D. H. Lee, "Hold the door! fingerprinting your car key to prevent keyless entry car theft," *arXiv preprint arXiv:2003.13251*, 2020.

[32] 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.

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

[34] M. Kneib and C. Huth, "Scission: Signal characteristic-based sender identification and intrusion detection in automotive networks," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 787–800.

[35] 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.

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

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] B. Sklar *et al.*, *Digital communications: fundamentals and applications*, 2001.

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

[43] 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.

[44] 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.

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

[46] 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.

[47] L. Wouters, J. Van den Herrewegen, F. D Garcia, D. Oswald, B. Gierlichs, and B. Preneel, "Dismantling dst80-based immobiliser systems," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2020, no. 2, pp. 99–127, 2020.

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

[49] 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.