Analog Physical-Layer Relay Attacks with Application to Bluetooth and Phase-Based Ranging

Paul Staat
Max Planck Institute for Security and
Privacy
Bochum, Germany
paul.staat@mpi-sp.org

Kai Jansen
PHYSEC GmbH
Bochum, Germany
kai.jansen@physec.de

Christian Zenger
PHYSEC GmbH
Bochum, Germany
christian.zenger@physec.de

Harald Elders-Boll
Technische Hochschule Köln
Cologne, Germany
harald.elders-boll@th-koeln.de

Christof Paar
Max Planck Institute for Security and
Privacy
Bochum, Germany
christof.paar@mpi-sp.org

ABSTRACT

Today, we use smartphones as multi-purpose devices that communicate with their environment to implement context-aware services, including asset tracking, indoor localization, contact tracing, or access control. As a de-facto standard, Bluetooth is available in virtually every smartphone to provide short-range wireless communication. Importantly, many Bluetooth-driven applications such as Phone as a Key (PaaK) for vehicles and buildings require proximity of legitimate devices, which must be protected against unauthorized access. In earlier access control systems, attackers were able to violate proximity-verification through relay station attacks. However, the vulnerability of Bluetooth against such attacks was yet unclear as existing relay attack strategies are not applicable or can be defeated through wireless distance measurement.

In this paper, we design and implement an analog physical-layer relay attack based on low-cost off-the-shelf radio hardware to simultaneously increase the wireless communication range and manipulate distance measurements. Using our setup, we successfully demonstrate relay attacks against Bluetooth-based access control of a car and a smart lock. Further, we show that our attack can arbitrarily manipulate Multi-Carrier Phase-based Ranging (MCPR) while relaying signals over 90 m.

1 INTRODUCTION

Today, billions of smart wireless devices, including the Internet of Things (IoT), surround us in our daily live. Increasingly, the wireless environment is used beyond mere communication to provide context-aware services: Wireless devices are integrated into the environment and applications such as asset tracking, indoor localization, contact tracing, and access control bring physical aspects into the digital world. Here, devices must be aware of their environment and distance to others.

Not surprisingly and in line with the ongoing technological convergence, the smartphone is a central aspect of many context-aware applications. Using a generic platform eliminates the need of dedicated hardware devices while further enhancing convenience. For Phone as a Key (PaaK) [32, 57], the smartphone acts as a personal token for access control systems of, e. g., vehicles and buildings. As

a prominent example, during the Covid-19 pandemic, smartphone-enabled contact tracing applications have emerged worldwide to track infection chains based on the proximity of individuals [5]. Such applications naturally have to make use of the wireless communication systems implemented in smartphones. Being available in virtually every smartphone, Bluetooth has become the technology of choice for the required ad hoc short-range networks. Within this trend, vendors now increasingly also utilize Bluetooth for security-critical proximity verification applications, e. g., access control. However, Bluetooth was originally designed for wireless communication rather than for secure proximity verification. Thus, one may suspect a vulnerability against *relay attacks*.

In the classical relay attack, an attacker makes distant victim parties being able to communicate by establishing an artificial communication channel. The distant parties thus may falsely assume to be in each other's proximity. In the past, this has been exploited to circumvent earlier-generation automotive Passive Keyless Entry (PKE) systems [26]. Thus, attackers are able to gain access to vehicles and media frequently reports car thefts due to relay attacks [10, 30]. In contrast, relay attacks on Bluetooth-based proximity verification have received only very little attention as of yet. While the attack has been identified as a threat for smart locks [32], realizations are still limited to unidirectional forwarding of contact tracing advertisement packets [5]. Other than this, full-blown bidirectional range-extending relay attacks – required for challenge-response authentication – have not been reported. Since Bluetooth uses a very different wireless physical-layer architecture than traditional automotive PKE systems, previous attack strategies [26] cannot directly be applied. Consequently, the lacking attack realization currently hampers risk assessment of Bluetooth w.r.t. practical relay attacks and leaves the exploration of threat potential as an open research problem.

To close this gap, in this work we identify technical peculiarities of relay attacks on Bluetooth and outline why previous attack strategies are not applicable. Based on our analysis, we utilize commodity Radio Frequency (RF) components to design and implement an analog attacker setup to achieve bidirectional physical-layer relaying of time-division duplex (TDD) wireless communication such as Bluetooth. Our cable-based proof-of-concept allows hands-on testing of products and enables real-world relay attacks in certain scenarios.

We use our setup to test recent Bluetooth-based PKE systems of a car and a smart lock, both of which utilize smartphone-based key replacements. Our attack allowed us to unlock the door and start the engine (in case of the car) while the legitimate smartphone was at a distance of more than 65 m. Our results confirm that Bluetooth alone is vulnerable against simple range-extending relay attacks.

As per its latest v5.3 specification [12], the only way to infer the distance between two Bluetooth devices is based on signal strength which is known to be notoriously inaccurate [27]. Therefore, vendors increasingly implement Multi-Carrier Phased-Based Ranging (MCPR) aside of Bluetooth [1, 2, 11, 21, 34, 53, 61], recently even within integrated circuits geared towards MCPR [6, 33, 54]. Since MCPR in the past has been marketed as High Accuracy Distance Measurement (HADM) [11, 13, 24], it is also interesting to note that the Bluetooth SIG lists a specification under development bearing this very name [14]. In view of these developments, we additionally study the security of MCPR against our attacker setup, showing that MCPR is a viable detection method for simple range-extension attacks. However, adding a simple phase-shifter to our setup, we demonstrate a novel distance manipulation attack against MCPR. Thus, for the first time, we achieve both range-extension (bridging a physical distance of 90 m) and distance manipulation *at the same time.* Our results confirm previous findings of Ólafsdóttir et al. [44], who first described vulnerabilities of MCPR against signal manipulation attacks. Further, we give guidelines to enhance attack difficulty, e. g., by leveraging frequency hopping or analyzing channel reciprocity.

Differentiation from previous work. The general idea for relay and distance manipulation attacks is not original to this paper. The vulnerability of access control against range-extending relay attacks was first demonstrated by Francillon et al. [26] for earlier PKE systems, using unidirectional signal amplification. However, this strategy is insufficient to achieve the bidirectional range extension of TDD wireless communication such as Bluetooth, required due to challenge-response authentication. In our work, we realize a bidirectional amplification approach using power detection to toggle signal directions. Ólafsdóttir et al. [44] presented the first security analysis of MCPR, revealing vulnerabilities against signal manipulation. The authors proposed the general idea of manipulating the phase of individual MCPR tones, although not presenting a practical attack realization. The authors gave a brief technical proposal based on mixing with locally generated RF signals. We believe that this approach is of low practicality as an attacker needs to generate a coherent RF carrier before phase manipulation can be applied. Ólafsdóttir et al. also acknowledge this challenge in their paper as they sketch a countermeasure based on randomized phase shifts which later was adopted by Abidin et al. [1]. We build on the idea of manipulating individual MCPR tones [44], albeit using an entirely different signal manipulation mechanism based on a simple phase shifter circuit, eliminating the unrealistic requirement of a coherent RF carrier. Moreover, we contribute the method to properly schedule phase shifts. Not only does this facilitate a real-world implementation (as our results show), it also bypasses the previously suggested countermeasure. To the best of our knowledge, this

is the first work to unify range extension [26, 31, 42, 48] and distance manipulation [25, 44, 46] – previously addressed separately – within a real-world implementation.

Contribution. In summary, this paper makes the following contributions:

- We design a practical physical-layer relay attack, generically applicable to standard 2.4 GHz TDD communication systems such as Bluetooth. We use a novel attack strategy which adapts to the transmit-receive timing of the legitimate parties. We present a prototypical cable-based implementation built from commodity RF components.
- We analyze the Bluetooth-based access control implementations of a car and a smart lock and demonstrate successful relay attacks against both systems. To the best of our knowledge, this is the first work to fully implement a relay attack to demonstrate the insecurity of Bluetooth-based access control.
- We investigate MCPR as a countermeasure against our attack and demonstrate a novel phase manipulation attack to simultaneously perform range extension and distance manipulation.

Responsible Disclosure. We provided this paper to the Bluetooth SIG and the affected manufacturers.

2 RELATED WORK AND BACKGROUND

In this section, we outline related works and provide background information on RF proximity verification, relay attacks, and Bluetooth communications.

2.1 Related Work

The literature describes various relay attacks against different RF proximity verification systems. Francillon et al. [26] have demonstrated signal amplification attacks to increase the range of immobilizing signals of classical automotive PKE systems. Their study revealed vulnerabilities on all tested models. Payment systems are subject to relay attacks as well and have been demonstrated for ISO 14443 [31] and NFC [42, 48]. Relay attacks against Bluetooth communications have received little attention as of yet, although Levi et al. [40] discussed the possibility of such attacks already in 2004. In a security analysis of Bluetooth-based smart locks, Ho et al. [32] identified the attack as a threat, albeit not addressing technical realization. Baumgärtner et al. [5] demonstrated Software-Defined Radio (SDR)-based unidirectional forwarding of advertisement packets to study the security of contact tracing applications. Protocol-level impersonation attacks as described by Antonioli et al. [3] and Jasek [52] are conceptually different from a relay attack but likewise allow attackers to forward Bluetooth traffic between victim parties.

To defeat relay attacks, numerous works study wireless distance measurements [7] and their security guarantees. Ranganathan and Čapkun [45] survey techniques for secure ranging and conclude with Ultra Wideband Impulse Radio (UWB-IR) as the most promising candidate. The fine time resolution of wideband waveforms promotes UWB systems to be used for Time-of-Flight (ToF)-based ranging within distance-bounding protocols. While ToF itself cannot be reduced by an attacker, the measurement procedure can still

be vulnerable: Clulow et al. [19] have introduced the Early-Detect, Late-Commit (ED/LC) attack that has later been applied to UWB-based ranging [25]. Singh et al. [51] and Leu et al. [39] recently introduced novel physical-layer security primitives to diminish the attacker's success while preserving the ability of long-range communication. Another work of Singh et al. [50] aims to detect UWB distance-enlargement attacks. Apart from UWB, previous work also investigates the security of other RF proximity verification techniques. Ólafsdóttir et al. [44] presented the first security analysis of MCPR and demonstrated a delay-based distance reduction attack. In order to counteract these attacks, Abidin et al. [1] recently combined MCPR with a coarse ToF measurement. Notably, they report a promising implementation on a standard Bluetooth transceiver. Ranganathan et al. [46] have shown ED/LC attacks on chirp-based ToF measurements.

Other than distance measurement, proposals for relay attack detection are RF fingerprinting [36], channel reciprocity [35, 37], protocol timing [47], and sensor fusion [49, 56]. In 1993, Brands and Chaum [16] introduced distance bounding protocols to cryptographically verify an upper bound on the distance of a prover. Finally, the literature reports additional vulnerabilities in access control systems. Eisenbarth et al. [23] demonstrated a side-channel based extraction of group keys from the KeeLoq system. Wouters et al. point out security weaknesses in the implementations of access control systems of luxury cars [58, 59].

2.2 Background

Relay Attacks. In a classic relay attack, an adversary establishes a communication channel between distant parties that otherwise would not be able to communicate. Wireless radio systems are particularly prone to such attacks as radio wave propagation relies on a shared medium that the attacker can access, i. e., to capture/eavesdrop legitimate signals. To forward legitimate signals, attackers employ *amplify-and-forward* or *decode-and-forward* relaying schemes [28]. The latter involves recovery of bits or symbols from analog waveforms which is attractive for long-range transfers. In contrast, amplify-and-forward omits demodulation and forwards the analog waveform with minimal processing efforts, e. g., amplification only, resulting in low delays and moderate design complexity at the cost of link budget constraints. With the advent of distance measurement techniques, the scope of relay attacks became broader: The attacker is required to alternatively or additionally perform some sort of signal manipulation to overcome the implemented proximity verification. In turn, a location-based wireless service may falsely allow access to restricted applications, potentially causing economical damage to individuals and businesses. Examples for threatened services are wireless payment systems, contact tracing, electronic door locks, and PKE systems for cars.

RF Proximity Verification. Wireless communication systems can be used for localization and ranging [7, 15, 61]. Leveraging physical-layer observations such as ToF, Received Signal Strength (RSS), or carrier phase, devices infer distances to others. Distance measurements from ToF are based on the signal propagation delay being a function of the speed of light and distance. Accurate measurement of the ToF requires nanosecond time resolution as provided, e. g., by UWB-IR [60]. RSS-based ranging leverages the propagation path loss of radio waves as a function of the distance [27]. RSS indication is available for almost every wireless receiver but suffers from inaccuracies due to multipath propagation. Carrier phase-based ranging, i. e., MCPR, uses unmodulated RF carrier signals to observe phase shifts that are proportional to the ToF [7]. The measurement procedure can conveniently be implemented with narrowband frequency hopping systems such as Bluetooth Low Energy (BLE) [61] and is capable of accuracies below 30 cm [6].

Bluetooth. Bluetooth is designed for short-range wireless communication. The specification [12] defines two wireless stacks, namely BLE and Bluetooth BR/EDR. In the following, we use the terms BLE and Bluetooth to refer to BLE devices. Still, our results also apply to BR/EDR in principle. BLE operates on a total of 40 sub channels with 2 MHz spacing within the 2.4 GHz ISM band and uses TDD to realize bidirectional communication. On the physical layer, transmissions use Gaussian Frequency Shift Keying (GFSK) with data rates of either 1 Mbps or 2 Mbps. Furthermore, BLE employs an adaptive frequency hopping scheme over 37 channels with a hopping rate of up to approx. 133 Hz. Device discovery in BLE is realized through periodic advertisement packets. In a subsequent *pairing* phase, parties can establish an authenticated and encrypted channel, i. e., cryptographic keys are exchanged. The secure channel is persistent as both nodes store long term keys, which is referred to as *bonding* of two devices in BLE. Bluetooth does not specify a dedicated measurement procedure to find the distance between two devices. Instead, RSS values can to be used to coarsely estimate distances. When multiple devices are available, an alternative approach is triangulation based on Angle-of-Arrival (AoA) or Angle-of-Departure (AoD) which was added to the Bluetooth specification v5.1. Both features leverage the Constant Tone Extension (CTE) which was already used to implement MCPR [61].

3 RELAY IMPLEMENTATION

Next, we introduce the system and attacker model and outline challenges associated with relay attacks on Bluetooth. Finally, we outline our proof-of-concept analog physical-layer relay attack.

3.1 System and Adversary Model

We consider an external relay attacker operating on the wireless physical layer with the goal of circumventing Bluetooth-based RF proximity verification between a pair of distant communication parties A and B. Considering an access control application, B is a mobile device, e. g., a smartphone, whereas A is mostly stationary, e. g., a smart lock or a car. We assume that A and B are honest and have created a bond before, i. e., the attacker is not able to break the applied cryptography, that is to read or make valid manipulations of secured payload data. The nodes employ standard-compliant BLE communication and A needs to infer proximity to B from the ability to communicate and reasonable RSS levels. The attacker is capable of transmitting and receiving RF signals to and from both parties. Also, the attacker can choose a strategic position close to A.

3.2 Previous Attack Strategies

Previous strategies for practical attacks were based on unidirectional relaying. While this is sufficient for inherently unidirectional
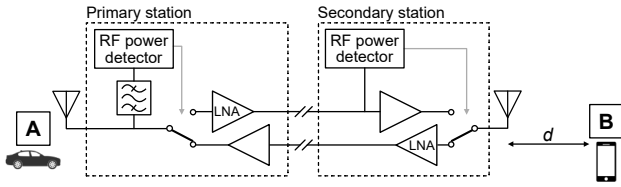
Figure 1: This block diagram illustrates the hardware setup for the analog relay attack, comprising of the two distant primary and secondary stations.

systems, e. g., advertisement-based contact tracing [5], system designers can enforce bidirectional communication using challenge-response authentication. However, even then, unidirectional attacks can be sufficient, as is the case for earlier generation automotive PKE [26]: Here, a dedicated wireless protocol is used between a car and a key fob. The car transmits Low Frequency (LF) signals at around 100 kHz to the key fob which responds on an Ultra-High Frequency (UHF) channel at 315 or 433 MHz. The LF signals only have short range and therefore *immobilize* the system. In contrast, the UHF signals from the key have a wide range. The attack outlined by Francillon et al. [26] exploits this observation, extending the LF signal range to reach the distant key. This simplifies the attack to a unidirectional amplification of the LF signals while the response from the key fob reaches the car directly. Importantly, the distinct signal frequencies allow attackers to separately manipulate each communication direction.

However, the situation is different with BLE-based communication. Here, the legitimate parties share the same frequency resource over time using TDD to establish bidirectional communication, having the same range in both directions. Thus, in order to extend the victim's effective communication range, a relay attacker faces the challenge of extending *both* directions. Now, one may suggest to use a pair of BLE receivers and transmitters at both ends to accomplish this task by forwarding only the application payload data, i. e., decode-and-forward relaying. Unfortunately, this cannot be done since resource allocation of the legitimate parties, e. g., the transmit-receive timing and frequency hopping sequence[1], is unknown to the attacker who is completely external and cannot impersonate the legitimate parties. Further, decode-and-forward relaying neglects physical-layer information and is easily detected by, e. g., MCPR or channel reciprocity (see Section 5).

Alternatively, following the style of attack of [26] for both directions, the attacker could try to amplify and forward the entire Bluetooth spectrum at both legitimate parties towards the other. However, this approach requires careful design consideration since both communication directions use the same frequency range. That is, an attacker naively following this approach could end up building a large feedback loop that amplifies itself, eventually leading to instability and self-destruction.

3.3 Relay Implementation

The attacker's goal is to (*i*) establish a bidirectional communication channel while (*ii*) applying amplification in both directions

for range-extension and to circumvent RSS-based proximity verification. However, as outlined before, the relay attacker cannot simply amplify the legitimate BLE signals in both directions independently. To resolve this issue, we propose a novel relaying strategy which adapts to the legitimate node's transmit-receive behavior. An implementation block diagram is shown in Fig. 1. The attacker positions their antenna close to A and uses an analog RF power detector to sense when A transmits. Upon detection of a transmission of A, an RF switch is used to select the upper signal path, applying amplification and forwarding signals to B. In the other case that no transmission is detected, the lower signal path is selected, applying amplification in the other direction to forward signals from B to A. This strategy allows the attacker to synchronize to the node's TDD, preventing simultaneous amplification in both directions to eliminate the aforementioned feedback loop.

The output of the power detector is a voltage proportional to the RF input power. Using a comparator, we implement a threshold-based binary power detection to sense transmissions of A. The comparator output logic signal controls an RF switch to change signal directions. Allowing the attacker to bridge relatively large distances between the two relay end-points, we apply this technique at both the primary and secondary relay stations, cf. Fig. 1. At the primary side, close to A, the power detection takes place after the antenna but before the RF switch and signals of A will reach the power detector regardless of the switch position. At the secondary side, power detection is again used to detect forwarded transmissions of A. Due to the attacker's close position to A, the signals of A reach the primary power detector rather strongly. In contrast, after over-the-air and cable losses, the signals of B arrive weaker and will not trigger the switching mechanism. Thus, the power-detection threshold should be selected below the expected high signal power from A and above the low signal power from B.

Combining standard and ready-to-use RF components, we implemented a prototypical cable-based attacker setup that is depicted in Fig. 9 in Appendix A. We give an outline of implementation details and example traces of power detector output signals in Appendix A. Further, the exact parts are listed in Table 2 likewise in the appendix. While we have not optimized the design for low cost, we estimate the total cost for the parts to be about € 2200. However, omitting the evaluation boards, the individual components and ICs can be purchased for under € 1200.

The maximum distance the attacker can bridge can be found by means of a link budget analysis, where the wireless loss to and from the relay antennas as well as the total amplification gain and loss of the relay hardware needs to be taken into account. Note that our attacker implementation is based on a mixed-signal design with the relay channel being completely analog. As no sampling is involved, the attacker operates with minimum latency which is desired for attacks on proximity verification. On the other hand, targeted and intelligent signal manipulation is more difficult, yet possible as we show in Section 5.2.2. Another aspect related to the analog nature is the impact of interference. In our setup, *all* signals picked up by the receiving antenna are forwarded to the other relay station, including signals from the legitimate and other parties. Thus, multiple wireless devices in reach of the relay stations won't diminish the attacker's success. Still, interference from other devices may affect the legitimate receiver, as is always the case in multi-user

---

[1]The BLE frequency hopping is randomized and synchronization is cumbersome due to the prediction of PRNG values [17].

wireless settings. However, on the primary relay side, strong interfering signals could falsely trigger the power detector. We utilize a 2.4 GHz bandpass filter on the power detector input, rejecting interference from other frequency bands. To mitigate in-band interference, the attacker should ensure that the victim signals are the strongest received signals, e. g., by means of short distances or directional antennas. In our experiments, we did not encounter performance degradation due to interference, even though operating in busy wireless environments. For instance, close-by 2.4 GHz Wi-Fi routers did not trigger the relay's power detection (cf. Fig. 11 in the appendix). Finally, in view of PaaK systems, please note that Bluetooth and Wi-Fi do not transmit simultaneously [18].

4 ATTACKS ON BLUETOOTH-BASED ACCESS CONTROL

In this section, we test our attacker setup in two case studies on Bluetooth-based access control systems that both implement smartphone-based PKE. In particular, we analyzed the behavior of a car and an electronic door lock for buildings. Both products allow the smartphone to be used as a personal entry token, not requiring any user interaction for unlocking doors or starting the engine.

4.1 Case Study 1: Car

For our first case study, we tested the Bluetooth-based PKE system of a car. The car accepts smartphones as an access tokens, allowing to unlock the doors and start the engine. The car uses Bluetooth to monitor the presence of an authorized smartphone. The user only needs to possess the phone and is not required to actively participate in the unlocking procedure.

Initially, we tested the system in a non-adversarial setting. With the authorized smartphone, we approached the locked car towards the passenger side until it unlocked. Then, we moved away from the car until it locked again. The observed distances are given in Table 1 and it is evident that different conditions apply for locking and unlocking. Since BLE is used, proximity verification is likely accomplished through analysis of RSS[2]. Thus, we suspect that the car applies different RSS thresholds for unlocking and locking. The RSS hypothesis is further backed by the distances in Table 1 varying significantly with the phone location: The distances are largest when the phone is carried in the hand (strong line-of-sight channel) and lowest when the phone is carried in a trouser pocket on the back of the body (weak non-line-of-sight channel due to human body shadowing). Further, we observed that unlocking the car does not imply the ability to start the engine. In line-of-sight conditions, we were able to start the engine with the smartphone at a distance of 2 m from the car, hinting a third RSS threshold.

Next, we tested the effectiveness of our attacker setup outlined in Section 3.3. We placed the primary relay station close (10 cm to 30 cm) to the B-pillar of the car. We placed the secondary relay station at a distance of approx. 65 m to the car. Both relay stations were equipped with a directional antenna as can be seen from Fig. 2, showing the experimental attack setup. Approaching the secondary relay station antenna with the authorized smartphone in the hand, the car unlocked at a distance of 4 m to the relay antenna. Being

---

[2]AoA and AoD methods can also be utilized to find distances, however, requiring multiple locator devices to perform triangulation.

(a)   (b)

Figure 2: Attack setup, relaying Bluetooth signals between the primary (a) and secondary (b) relay stations to establish communication between a car and a distant smartphone.

Table 1: Observed non-adversarial car unlocking and locking distances.

Phone Location	Unlock	Lock
Hand	5 m	13 m
Trouser pocket	3 m	11 m
Trouser pocket (back)	1 m	6 m
Jacket pocket	4 m	12 m

at a distance of 2 m to the relay antenna, it was possible to start the engine. Also, we observed the previously outlined behavior for unlocking which took place when the smartphone was at a distance of 13 m to the relay antenna.

Our attack clearly succeeds to substantially extend the Bluetooth communication range between the car and the smartphone. We were able to unlock and start the car with the authorized smartphone being at a distance of 69 m and 67 m, respectively. Consequently, we circumvented the Bluetooth-based RF proximity verification, highlighting yet another attack vector to compromise keyless entry systems. During our experiments, we have not perceived any indication of additional countermeasures. Several approaches may be feasible, including GPS position comparison using the car's cellular network connection or plausibility checks of RSS values across the various Bluetooth antennas of the Model 3. However, as researchers have already stressed for a long time, using RSS for proximity verification is generally considered insecure.

We carried out all tests and attacks with a Tesla Model 3 Long Range from 2019, firmware version v10.2 (2021.4.12). The smartphone was a Huawei P Smart FIG-LX1 running Android 9.1.0.

4.2 Case Study 2: Smart lock

For our second case study, we tested a smart lock which is a Bluetooth-enabled keyless entry system which retrofits traditional key-based doors. It is controlled using a smartphone app and also supports an optional PKE mode which automatically unlocks the door upon proximity of an authorized smartphone. Similarly to the previous experiments with the car, we placed the primary relay station close to the smart lock. Then, with our setup we again bridged a distance of approx. 65 m between an authorized smartphone and the smart lock. Now, with the smartphone as close as 2 m to the secondary relay station, the smart lock unlocked the door. Again, our attacker setup successfully circumvents the Bluetooth-based RF proximity verification.

Compared to the previous car entry system, a smart lock has the distinct advantage of being deployed in a fixed location. This allows the smartphone to perform a number of plausibility checks before sending an unlock command to the lock. During our relay attack attempts, we noticed that the lock's smartphone app leverages multiple such checks. To analyze the behavior in detail, we took advantage of plain-text log files provided by the app, originally intended for diagnostic purposes. Notably, the log files in some cases even provide commentary insight to the application logic. From our analysis, we identified several measures and conditions when the lock is configured to automatically unlock: (1) Low Bluetooth transmission power is used and the application obtains RSS values. (2) The user must first exit and then re-enter a pre-defined geofence area before unlock. Distance to the lock is validated using GPS data and the known fixed device location. (3) The android app leverages Google Play services [20] to monitor device activity such as walking. (4) Plausibility checks are applied, i. e., when location changes occur too fast or despite no movement being detected. Clearly, the outlined plausibility checks increase the hurdles for a successful attack. However, as GPS positions are considered insecure and may be spoofed, we conclude that attacks are still possible.

We carried out the tests and attacks with a Nuki Smart Lock 2.0, firmware version 2.9.10. As the authorized smartphone, we used a Huawei P10 VTR-L09 running Android 9.1.0 with Nuki Smart Lock app version 2.7.4.

5 ATTACKS ON PHASE-BASED RANGING

To counter attacks against Bluetooth-based proximity detection, RF-based physical distance measurement techniques can be employed. RSS-based distance estimates as per the current Bluetooth specification [12] are inaccurate and prone to manipulations, e. g., by signal amplification like demonstrated in Section 4. Therefore, Bluetooth recently is increasingly being complemented by MCPR [1, 2, 11, 21, 34, 53, 61], enabling distance measurements with high accuracy. In this section, we outline how our analog relay attack can be used to simultaneously increase the communication range while arbitrarily manipulating distances measured using MCPR.

5.1 Background on MCPR

MCPR is based on single carrier phase measurements, thus enabling accurate distance finding with narrowband radios. Notably, MCPR would be particularly attractive to implement with Bluetooth radios as the frequency hopping necessary for MCPR can be reused from or shared with the Bluetooth signaling, e. g., by using the CTE.

In order to find the distance, the radios exchange unmodulated carrier signals and observe their phase shifts [7]. In particular, node A transmits a tone to node B, which reflects the received tone back to A (see Fig. 3). Upon reception, A detects the phase of the response and can indirectly measure the ToF to calculate the distance to B. The idealized two-way tone exchange at frequency f_i, assuming a line-of-sight channel, leads to a phase delay of $\phi_i = 4\pi f_i \tau$ which is a function of twice the ToF τ (and the distance between the nodes). As the carrier phase wraps with 2π, measurements at two frequencies f_1 and f_2 resolve distance ambiguities [44] and allow A
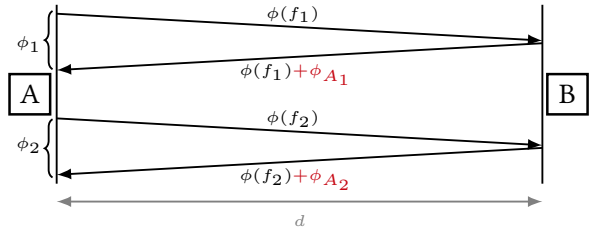

Figure 3: Illustration of the MCPR measurement procedure between nodes A **and** B **and potential phase manipulation attack using by applying adversarial phase shifts** ϕ_{A_1} **and** ϕ_{A_2}**.**

to calculate its distance to B:

$$d = \frac{c_0}{4\pi} \frac{\phi_2 - \phi_1}{f_2 - f_1} = \frac{c_0}{4\pi} \frac{\Delta\phi}{f_{\text{step}}} \quad (1)$$

In practice, the measurement is repeated for multiple frequencies in rapid succession to combat noise and multipath distortion, e. g., by sweeping over N frequencies to gather $N-1$ distance estimates for averaging.

5.2 Distance Manipulation

Ólafsdóttir et al. [44] have shown that MCPR has a number of vulnerabilities rooted in the feasibility to manipulate the signal phase. In turn, attackers may be able to manipulate MCPR distance measurements. One attack concept relies on individual phase manipulation of each carrier signal of a ranging procedure as illustrated in Fig. 3. Here, we follow this general idea.

We observe from Eq. 1 that the distance measured by the nodes depends on the phase *change* over frequency. Thus, an attacker attempting to manipulate the distance needs to forge a malicious phase slope by manipulating the channel phase response. By applying appropriate phase shifts ϕ_{A_i}, the legitimate parties will estimate the distance to be d_{set}:

$$d_{\text{set}} = \frac{c_0}{4\pi} \frac{\Delta\phi + (\phi_{A_2} - \phi_{A_1})}{f_{\text{step}}} = \frac{c_0}{4\pi} \frac{\Delta\phi + \Delta\phi_A}{f_{\text{step}}} \quad (2)$$

Combining Eq. 1 and Eq. 2, we arrive at the following expression which yields the phase slope the attacker needs to apply to deliberately manipulate the distance measured by the legitimate parties to be d_{set}:

$$\Delta\phi_A = \frac{4\pi f_{\text{step}}}{c_0} (d_{\text{set}} - d) \quad (3)$$

Thus, the attacker only needs to know the frequency step size f_{step} and the actual node distance d, which are either known or can be observed. Since $\Delta\phi_A$ is derived from Eq. 1, it implicitly assumes a line-of-sight channel (having linear phase) between A and B.

5.2.1 Attack Implementation. To realize the outlined attack, Ólafsdóttir et al. [44] proposed mixing of the victim signals with locally generated coherent RF carrier signals to realize the required phase shifting. However, this requires the attacker to first synchronize to the victim signals on the carrier phase level. If possible at all (note the μs timing of MCPR tones), this approach is highly complex and would be costly and cumbersome to implement. Instead, we introduce a new attack variant which only requires a coarsely aligned
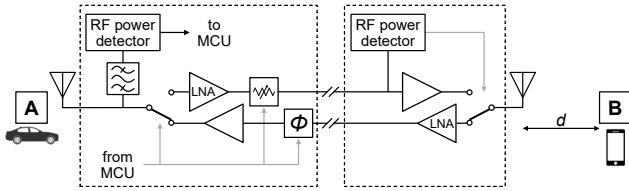
Figure 4: This block diagram illustrates the hardware setup for the analog relay attack with amplitude and phase manipulation capabilities.
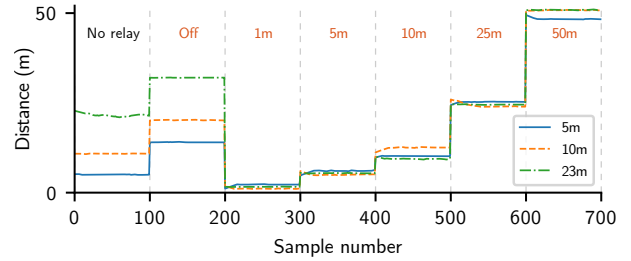

Figure 5: Demonstration of real-time distance manipulation, including reduction and enlargement for three victim node positions.
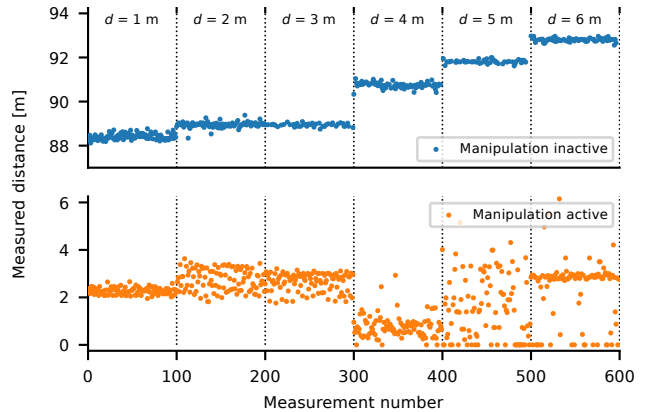

Figure 6: Combined relay and distance decreasing attack to enhance the communication range while simultaneously decreasing MCPR distance estimations of a BLE transceiver. Top: Measured distance without distance manipulation. Bottom: Measured distance with distance manipulation.

timing instead of RF carrier synchronization, therefore allowing straightforward implementation.

We start with our attacker setup from Section 3.3 to which we add signal manipulation capabilities as shown in Fig. 4. We insert a digital phase shifter [43] into one path of the relay, adding phase control to signals traveling from B to A. Please note that Fig. 4 represents our experimental realization, with the attenuator and phase shifter in separate signal directions. However, insertion into the signal paths is possible in arbitrary other combinations as well.

To achieve distance manipulation, the phase shifter needs to be adjusted dynamically for each carrier signal, according to Eq. 3 to forge a phase slope. To do so, we take advantage of the relay's power detector that we use to obtain the legitimate transmit-receive timing: As soon as A transmits, the rising power detector output indicates to the attacker that B is possibly about to respond. Thus, we can properly schedule the setting of phase shifts which need to change by $\Delta\phi_A$ (see Eq. 3) each time the victim parties proceed with the next carrier frequency. Thereby, a coarse time synchronization to the tone exchange is established. Assuming a linearly increasing carrier frequency, i.e., $f_i = f_{i-1} + f_{step}$, the phase shifter setting at time t, as dictated by the power detector output, is given by:

$$\phi_t = \phi_{t-1} + \Delta\phi_A \bmod 2\pi \qquad (4)$$

Applying this scheme in practice, the interested reader is referred to Appendix B, where we show exemplary output signals of the attacker's power detector during an MCPR procedure.

5.2.2 Attack Evaluation. We now detail the attack performance in a practical evaluation. We conduct experiments with a commercially available MCPR implementation for BLE radio transceivers [21] and demonstrate successful distance manipulation attacks while enhancing the communication range. The transceivers interleave standard BLE communication with an MCPR procedure with $N = 40$ carriers and a frequency step size $f_{step} = 1$ MHz.

In a first experiment, we study the general attack principle and focus on the effectiveness of adversarial signal manipulations. To ensure stable channel conditions and prevent direct radiation, we connect the RF port of the interrogating node A directly to the primary side of the relay. We place the reflecting node B in line-of-sight to the secondary relay antenna at distances d of 5 m, 10 m, and 23 m. For each setting, we take 100 distance measurements. We plot the results in Fig. 5 with indication of the relay settings at the top. Without the relay, the distance measured by the legitimate nodes corresponds to the correct physical distance, as shown in the leftmost portion of Fig. 5. Next, we insert the attacker hardware but

disabled any distance manipulation. The measured distances (labeled as 'Off' in the plot) are now offset by a constant distance bias of around 9 m. This offset is due to the relay's hardware time delay of around 30 ns (approx. 23 ns when excluding coaxial feed cables of 2 m length). By estimating the physical node distance d accordingly higher, the attacker can easily self-compensate this effect as we will see next. For each node distance, we then configure the relay to manipulate the measured distances d_{set} to 1 m, 5 m, 10 m, 25 m, and 50 m by adjusting the phase shifter setting based on Eqs. 3 and 4. As evident from Fig. 5, the attacker succeeds to arbitrarily increase and decrease the measured distances accurately, regardless of the actual node distance. Please note that in our experiment, the attacker only was aware of d and f_{step} but not of the actual MCPR results of A and B, i.e., we did not adjust the phase shifter setting to match the desired distances.

In the previous experiment, we investigated the attack principle and therefore granted the attacker ideal conditions, as node A was directly connected to the relay through a coaxial cable. We now test the attack under more realistic conditions for the attacker. The attacker now picks up the signals from node A wirelessly. We place the nodes A and B outside of their communication range in non-line

of sight. In between the nodes, we install our analog relay attacker setup with off-the-shelf directional antennas to span a distance of 86 m. For the experiment, we place node A at a fixed distance of 1 m to the primary relay antenna. We place node B at distances d of 1 m to 6 m to the secondary relay antenna. Hence, the total distance between the nodes adds up to 88 m to 93 m. Like in the attack demonstrations from Section 4, the nodes are only able to communicate via BLE due to the communication channel provided by the relay attacker. Next, the legitimate nodes take 100 MCPR distance measurements without adversarial distance manipulation. Fig. 6 (top) shows the results for the positions of node B (indicated by labels at the top). As expected, the measured distance corresponds to the actual (relayed) distance between the nodes and rises as the distance to the relay antenna is increased. Thus, attacks like in Section 4 would easily be detected. We now enable the distance manipulation with $d_{\text{set}} = 2$ m. The corresponding distance measurements in Fig. 6 (bottom) clearly indicate the attacker's success. This experiment highlights that our attacker implementation enables BLE communication over substantial distances while *simultaneously* manipulating the MCPR procedure in real-time.

A key observation to make is that the sweeped carrier measurement for MCPR constitutes a particular security weakness: The channel transfer function is sampled on multiple frequencies consecutively which in turn allows individual manipulation of each carrier in a divide-and-conquer manner. This weakness becomes even more severe as, to the best of our knowledge, all currently available MCPR implementations utilize a non-randomly stepped RF carrier. In turn, simple attack strategies that do not require frequency knowledge, cf. Eq. 4, can be applied. Therefore, we suggest that future MCPR deployments should use secure randomized frequency hopping sequences.

5.3 Channel Reciprocity-based Detection

Besides carrier phase measurements, MCPR typically also provides the carrier amplitudes. While these are not necessary to infer the distance, it is still possible to evaluate them to perform a plausibility check based on *channel reciprocity*. This fundamental property of radio wave propagation states that a radio channel between two antennas is symmetric [4]. Hence, signals sent on the same frequency from A to B and vice versa from B to A experience the same random propagation effects such as loss, phase shift, and multipath propagation, e.g., represented by a frequency-dependent complex-valued transfer function $H(f)$.

Based on the claim that a relay attacker violates channel reciprocity between legitimate nodes A and B, previous works have suggested to examine the channel response to detect relay attacks [35, 37, 62]. The attack detection mechanism is constructed from an examination of channel symmetry using a dissimilarity metric d on pairs of bidirectional channel magnitude responses $|H_{\text{AB}}(f)|$ and $|H_{\text{BA}}(f)|$. These need to be exchanged by the nodes via their authenticated and encrypted communication channel. A detection threshold ϵ accounts for allowed differences in the respective channel observations made by A and B, e.g., due to noise and device-dependent hardware imperfections:

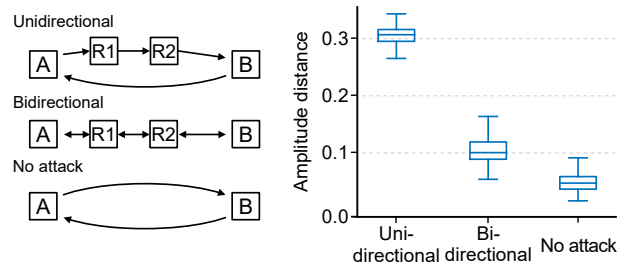$$d(|H_{\text{AB}}(f)|, |H_{\text{BA}}(f)|) > \epsilon \tag{5}$$

Figure 7: Left: Illustration of unidirectional and bidirectional relay attacks. Right: Distribution of Euclidean distances to assess channel reciprocity under unidirectional and bidirectional distance decreasing relay attacks.

Based on this condition, channel asymmetries introduced by an attacker can be detected. For instance, due to spatial decorrelation [28], this is the case in *unidirectional* attacks [44, 46]. Here, the nodes A and B are within their mutual communication range while the adversary intercepts (and manipulates) one communication direction while the other remains unchanged.

We put this claim to test in unidirectional and bidirectional (see left side of Fig. 7) distance decreasing attacks against MCPR between two BLE transceivers 15 m apart from each other in an ordinary environment. First, we use the previously outlined attacker setup for a unidirectional relay attack. The attacker here only forwards signals from A to B while applying on-the-fly phase manipulation[3] to reduce the measured distance to 2 m. Then, we repeat the attack but use bidirectional relaying where both communication directions are forwarded. Finally, we take a reference measurement without an attack with the nodes at an actual distance of 2 m. We evaluate the channel reciprocity using the Euclidean distance between $|H_{\text{AB}}(f)|$ and $|H_{\text{BA}}(f)|$. Fig. 7 (right) depicts the distributions of Euclidean distances for the three scenarios. As expected, channel reciprocity is violated most by the unidirectional attack. In contrast, the bidirectional attack exhibits increased channel reciprocity which overlaps with the results of the legitimate reference measurement.

The residual channel dissimilarity of our bidirectional attack is caused by differences between the relay's forward and reverse transmission paths, e.g., because of tolerances of the used parts. That is, in case of our attack, $|H_{\text{AB}}(f)|$ and $|H_{\text{BA}}(f)|$ now comprise of the concatenation of the reciprocal wireless channels to and from the relay antennas and the slightly non-reciprocal relay behavior. To completely circumvent attack detection, the relay hardware should be reciprocal, i.e., symmetric. This can be achieved in an additional engineering step by tuning the relay's transmission behavior to prevent Condition 5 to be fulfilled. However, again shining light on the security drawbacks of the MCPR measurement principle, an attacker can also manipulate the measurement of $|H_{\text{AB}}(f)|$ and $|H_{\text{BA}}(f)|$ to diminish the effect of the imperfect relay hardware.

We propose a relay hardware equalization scheme where the attacker individually manipulates the amplitude of the N tones exchanged by A to B (cf. Fig. 3). The approach follows a similar rationale as the previously outlined phase manipulation attack: In a divide-and-conquer manner, the attacker applies N separate

---

[3]We take the asymmetric channel into account to find the corresponding phase shifts.
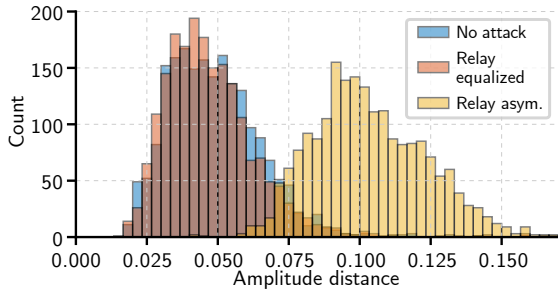
Figure 8: Distributions of Euclidean distances of channel responses, showing the effect of adversarial gain equalization in relation to non-equalized and non-adversarial settings.

amplitude manipulations to each MCPR carrier. In this way, a frequency-dependent attenuation profile $\beta(f)$ can be applied, such that $|H_{AB}(f) \cdot \beta(f)| \approx |H_{BA}(f)|$ holds. Fortunately, $\beta(f)$ does not depend on the (random) wireless channels between the relay and the legitimate parties, as those are reciprocal either way. Instead, the attacker can determine $\beta(f)$ based on the the forward and reverse transmission behavior of the relay hardware, e.g., using a vector network analyzer. We apply $\beta(f)$ using a digital step attenuator that we insert into one path of the relay (see Fig. 4).

To identify the current tone frequency, we exploit the deterministic nature of the examined MCPR implementation: (*i*) The MCPR measurement is always preceded by consistent transmit-receive patterns, allowing to identify the beginning of the tone exchange from analyzing the relay's power detector output signals. (*ii*) The MCPR tone exchange is a linear frequency sweep with step size f_{step}, i.e., $f_i = f_{i-1} + f_{step}$. Thus, the attacker can easily infer the current tone frequency from counting the number of transmissions.

We repeat the MCPR procedure with and without the outlined amplitude manipulation attack as well as in a legitimate scenario. For all three cases, we plot the histograms of Euclidean distances of channel measurements in Fig. 8. The distributions for the non-adversarial and the equalized relay settings are in complete agreement and are barely distinguishable. This demonstrates the effectiveness of the proposed equalization scheme to prevent attack detection from examining channel reciprocity. Overall, channel reciprocity can be helpful in thwarting naive attacks. However, we conclude that it only increases the attack difficulty, and thus, skilled attackers will be able to overcome this hurdle, as previously discussed and now demonstrated.

6 DISCUSSION

In this section, we discuss the real-world applicability, attacker capabilities and hardware improvements, and reason about attack detection and mitigation. Finally, we give directions for future work.

6.1 Real-World Applicability

A real-world relay attack is likely to be carried out against access control systems offering PKE operation as those do not require any user interaction other than proximity. However, manufacturers usually allow to disable this feature at will. Some products implement

geofencing, which is insufficient since GPS positions are considered to be insecure and may be spoofed. Given the availability of low-cost, credit-card sized software-defined radios [29] and ready-to-use software [22], we believe that such an attack could be carried out in parallel to relaying with little effort.

While the cable-based relay implementation certainly rules out some attack scenarios, this should pose a modest hurdle for willing and prudent attackers, e.g., when attacks take place at night times. Owing to the operation principle, our relay requires input signals strong enough for the power detector-based reactive switching. Thus, the primary relay station needs to be in proximity to one victim node. This is a realistic assumption, as proximity prior to authorization is an integral part of access control. In one of our MCPR experiments, we studied the effectiveness of our signal manipulation attack and therefore attached one node to the relay hardware through a coaxial cable. While this configuration does not represent a realistic attack scenario, it simplified evaluation and allowed systematic evaluation of the intended attack. In all of our other experiments, the attacker picked up the victim signals wirelessly in ordinary wireless environments.

6.2 Attacker Capabilities and Improvements

We assess the complexity of the attack setup to be moderate. As it is external to the legitimate parties and only uses off-the-shelf low-cost RF components, it can be realistically implemented by others. Although the setup is already capable of communication range extension and adaptive signal manipulation, further improvements can be made. Complementing the current mixed-signal processing with a digital receiver would allow to roughly track the nodes' protocol state. Eliminating signal direction finding based on power detection, RF circulators could be used to separate RF signals depending on their direction (we further discuss the use of circulators in Appendix C). Currently, the attacker relies on a cabled connection between the two relay stations. Clearly, this could be replaced with a wireless link, although requiring additional engineering efforts. A challenge would be the isolation between the receiving and re-transmitting antennas of each relay station. This could be achieved through frequency conversion [26], full-duplex radios [8], or directional antennas pointing away from each other at a distance [38]. An approach based on the latter will be part of a future publication. If bidirectional amplification is required at both relay stations, another aspect would be the wireless synchronization between the relay stations. For this, the primary power detector could trigger a radio transmitter (at another frequency) to which the secondary station listens to toggle the communication direction upon detection.

6.3 Attack Detection and Mitigation

A physical-layer relay attack ideally does not affect the application data but only alters physical quantities. Thus, a detection mechanism should likewise be deployed on the physical layer. This alone poses a hurdle to many devices already in the field as physical-layer data typically is not reported to the application or is not measured at all. Moreover, low-level signal processing is mostly implemented in a performance-optimized but less flexible manner, e.g., in hardware, making it difficult to retrofit detection mechanisms.

MCPR. As our results show, MCPR can be used to tackle range-extension-only attacks. However, we also showed that arbitrary distance manipulation is possible with simple off-the-shelf RF components. Since linear frequency sweeping is not mandatory for MCPR, an ad hoc security improvement to the currently available implementations would be a secure random frequency hopping[4]. Although this would render attacks more difficult, it would not be a sound security measure, since frequency can easily be measured, for example by using frequency counting or a phase-frequency detector. Specific to our phase shift scheduling mechanism, the legitimate nodes could introduce agreed-upon fake transmissions to make the attacker falsely proceed to the next phase shifter setting. To impede the attacker's power detection, the victim device could transmit with very low power. However, the attacker then could utilize an improved power detector or position closer to the victim.

ToF Measurement. Another possibility would be the addition of a direct ToF measurement by means of a challenge-response based distance bounding protocol. Fortunately, proprietary implementations have been reported for various BLE transceivers [1, 27, 55]. However, due to the limited signal bandwidth of Bluetooth, it is unlikely to achieve measurement accuracy as high as with MCPR. Further, the rather slow-transient Gaussian pulse shape employed for Bluetooth could facilitate early symbol detection attacks. Still, predicting cryptographically secured challenges early certainly poses higher hurdles to attackers than manipulating MCPR measurements where the measurement signals do not carry meaningful information. Thus, we believe this could be a good starting point to impose higher attack complexities. This likewise is acknowledged by recent work of Abidin et al. [1] who proposed a ranging system that combines MCPR with ToF to implement a distance bounding protocol specifically geared towards BLE applications.

Secondary observations. Specific to PaaK-based PKE applications, smartphones should not constantly emit unlock commands to mitigate the risk of relay attacks (as we experienced for the smart lock). That is, the smartphone should first apply plausibility checks, e. g., based on sensor readings. Secondary tracking and surveillance systems of connected cars could report successful attacks. For instance, stolen cars may report location data and camera footage over a cellular connection. However, this could be bypassed, e. g., using wireless jamming.

6.4 Future Work

In this work, we presented an analog physical-layer relay attack capable of RF range extension for Bluetooth communication and adaptive signal manipulation. Based on our results, we outline possible directions for future work.

Security discussions on relay attacks are often based on vague assumptions on attacker capabilities, making it difficult to realistically assess the risk of attacks. Future work should define an attack taxonomy to properly categorize attacks and countermeasures.

While the physical layer provides the basis for proximity verification, an actual implementation lives within a possibly complex protocol. Thus, in conjunction with physical-layer analysis, proximity verification should be examined for potential weaknesses on the protocol-level.

Our current attack implementation serves as a proof-of-concept. Naturally, the hardware setup leaves room for improvements and we are currently in the process of investigating wireless relay links.

7 CONCLUSION

In this paper, we introduced a novel concept to accomplish real-world relay attacks on 2.4 GHz TDD communications such as Bluetooth. Using a setup built from off-the-shelf RF components, we carried out successful relay attacks on a car and a smart lock. Our results highlight the need for a secure proximity verification which is currently lacking for Bluetooth. Therefore and in view of our attacker setup, we investigated the security of MCPR which recently found deployment aside of Bluetooth. We demonstrated the first practical on-the-fly phase manipulation attack on MCPR while simultaneously enhancing the communication range. Based on our findings, we suggest to implement MCPR with a mandatory frequency hopping to impede attacks. Finally, we hope that our work will raise awareness for relay attacks against Bluetooth-based proximity applications to accelerate the deployment of countermeasures.

REFERENCES

[1] Aysajan Abidin, Mohieddine El Soussi, Jac Romme, Pepijn Boer, Dave Singelée, and Christian Bachmann. 2021. Secure, Accurate, and Practical Narrow-Band Ranging System. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021, 2 (2021), 106–135.

[2] Alps Alpine. 2021. Alps Alpine and Broadcom Collaborate on a Secure Distance Measurement Solution based on Bluetooth® Technology. https://www.alpsalpine.com/e/news_release/2021/0105_02.html (accessed: February 04, 2022).

[3] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. 2020. BIAS: Bluetooth Impersonation AttackS. In *2020 IEEE Symposium on Security and Privacy (SP)*. 549–562. https://doi.org/10.1109/SP40000.2020.00093

[4] Constantine A. Balanis. 2005. *Antenna Theory: Analysis and Design* (3rd ed.). John Wiley & Sons, Hoboken, NJ, USA.

[5] Lars Baumgärtner, Alexandra Dmitrienko, Bernd Freisleben, Alexander Gruler, Jonas Höchst, Joshua Kühlberg, Mira Mezini, Richard Mitev, Markus Miettinen, Anel Muhamedagic, Thien Duc Nguyen, Alvar Penning, Frederik Pustelnik, Filipp Roos, Ahmad-Reza Sadeghi, Michael Schwarz, and Christian Uhl. 2020. Mind the GAP: Security & Privacy Risks of Contact Tracing Apps. In *2020 IEEE 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, Guangzhou, China, 458–467.

[6] Elbert Bechthum, Johan Dijkhuis, Ming Ding, Yuming He, Johan Van Den Heuvel, Paul Mateman, Gert-Jan Van Schaik, Kenichi Shibata, Minyoung Song, Evgenii Tiurin, Stefano Traferro, Yao-Hong Liu, and Christian Bachmann. 2020. 30.6 A Low-Power BLE Transceiver with Support for Phase-Based Ranging, Featuring $5\mu s$ PLL Locking Time and 5.3ms Ranging Time, Enabled by Staircase-Chirp PLL with Sticky-Lock Channel-Switching. In *International Solid-State Circuits Conference (ISSCC '20)*. IEEE, San Francisco, CA, USA, 470–472.

[7] Alan Bensky. 2016. *Wireless Positioning Technologies and Applications* (2nd ed.). Artech House, Norwood, MA, USA.

[8] Dinesh Bharadia and Sachin Katti. 2014. FastForward: Fast and Constructive Full Duplex Relays. In *ACM Conference on Special Interest Group on Data Communication (SIGCOMM '14)*. ACM, Chicago, IL, USA, 199–210.

[9] Dinesh Bharadia, Emily McMilin, and Sachin Katti. 2013. Full Duplex Radios. *SIGCOMM Comput. Commun. Rev.* 43, 4 (aug 2013), 375–386. https://doi.org/10.1145/2534169.2486033

[10] Nick Bilton. 2015. Keeping Your Car Safe From Electronic Thieves. The New York Times. https://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html (accessed: February 04, 2022).

---

[4]Likely at the cost of increased measurement time due to longer PLL settling times.

[11] Blanco, Sebastian. 2020. Denso Technology Aims to Swap Out Fobs for Phones. WardsAuto. https://www.wardsauto.com/vehicles/denso-technology-aims-swap-out-fobs-phones (accessed: February 04, 2022).

[12] Bluetooth SIG. 2021. Bluetooth Core Specification Revision v5.3. https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=521059 (accessed: February 04, 2022).

[13] Bluetooth SIG. 2021. High Accuracy Distance Measurement (HADM) Demo For Keyless Entry Systems. https://www.bluetooth.com/bluetooth-resources/high-accuracy-distance-measurement-hadm-demo-for-keyless-entry-systems/ (accessed: February 04, 2022).

[14] Bluetooth SIG. 2021. Specifications in Development. https://www.bluetooth.com/specifications/in-development/ (accessed: February 04, 2022).

[15] Azzedine Boukerche, Horacio A. B. F. Oliveira, Eduardo F. Nakamura, and Antonio A. F. Loureiro. 2007. Localization Systems for Wireless Sensor Networks. *IEEE Wireless Communications* 14, 6 (2007), 6–12.

[16] Stefan Brands and David Chaum. 1993. Distance-Bounding Protocols. In *Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT '93)*. Springer, Lofthus, Norway, 344–359.

[17] Damien Cauquil. 2019. Defeating Bluetooth Low Energy 5 PRNG for fun and jamming. DEF CON 27. https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Damien-Cauquil-Defeating-Bluetooth-Low-Energy-5-PRNG-for-fun-and-jamming.PDF (accessed: February 04, 2022).

[18] J. Classen, F. Gringoli, M. Hermann, and M. Hollick. 2022. Attacks on Wireless Coexistence: Exploiting Cross-Technology Performance Features for Inter-Chip Privilege Escalation. In *2022 2022 IEEE Symposium on Security and Privacy (SP) (SP)*. IEEE Computer Society, Los Alamitos, CA, USA, 808–824. https://doi.org/10.1109/SP46214.2022.00047

[19] Jolyon Clulow, Gerhard P. Hancke, Markus G. Kuhn, and Tyler Moore. 2006. So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks. In *European Workshop on Security in Ad-hoc and Sensor Networks (ESAS '06)*. Springer, Hamburg, Germany, 83–97.

[20] Google Developers. 2021. Google Play services. https://developers.google.com/android/reference/com/google/android/gms/location/DetectedActivity (accessed: February 04, 2022).

[21] Dialog Semiconductor. 2019. SmartBond™ Wireless Ranging SDK. https://www.dialog-semiconductor.com/sites/default/files/smartbond_wireless_ranging_sdk_product_brief_hr.pdf (accessed: February 04, 2022).

[22] Takuji Ebinuma. 2018. GPS-SDR-SIM Software-Defined GPS Signal Simulator. https://github.com/osqzss/gps-sdr-sim (accessed: March 28, 2022).

[23] Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani. 2008. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In *In CRYPTO 2008, volume 5157 of LNCS*. Springer, Santa Barbara, California, USA, 203–220.

[24] everythingRF. 2018. A BLE Based Secure Passive Keyless Entry Solution for Cars. https://www.everythingrf.com/news/details/7210-A-BLE-Based-Secure-Passive-Keyless-Entry-Solution-for-Cars (accessed: February 04, 2022).

[25] Manuel Flury, Marcin Poturalski, Panos Papadimitratos, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. 2010. Effectiveness of Distance-Decreasing Attacks against Impulse Radio Ranging. In *Proceedings of the Third ACM Conference on Wireless Network Security* (Hoboken, New Jersey, USA) *(WiSec '10)*. Association for Computing Machinery, New York, NY, USA, 117–128. https://doi.org/10.1145/1741866.1741887

[26] Aurélien Francillon, Boris Danev, and Srdjan Capkun. 2011. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Internet Society, San Diego, CA, USA.

[27] Davide Giovanelli and Elisabetta Farella. 2018. RSSI or Time-of-Flight for Bluetooth Low Energy Based Localization? An Experimental Evaluation. In *2018 11th IFIP Wireless and Mobile Networking Conference (WMNC)* (Prague). IEEE, 1–8.

[28] Andrea Goldsmith. 2005. *Wireless Communications*. Cambridge University Press, USA.

[29] Great Scott Gadgets. 2021. HackRF One. https://greatscottgadgets.com/hackrf/one/ (accessed: March 28, 2022).

[30] Andy Greenberg. 2016. Radio Attack Lets Hackers Steal 24 Different Car Models. Wired. https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/ (accessed: February 04, 2022).

[31] Gerhard Hancke. 2005. *A Practical Relay Attack on ISO 14443 Proximity Cards*. Technical Report.

[32] Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. 2016. Smart Locks: Lessons for Securing Commodity Internet of Things Devices. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security* (Xi'an, China) *(ASIA CCS '16)*. Association for Computing Machinery, New York, NY, USA, 461–472.

[33] imec. [n. d.]. Next-Gen high-accuracy fast ranging Bluetooth 5.1 0.8V ULP radio in TSMC 40nm. https://www.imec-int.com/sites/default/files/2021-03/NEXT-GEN%20HIGH-ACCURACY%20FAST%20RANGING.pdf (accessed: February 05, 2022).

[34] imec. [n. d.]. Secure High Accuracy Ranging on Bluetooth. https://www.imec-int.com/drupal/sites/default/files/2020-02/Secure-Prox-V02.pdf (accessed: February 04, 2022).

[35] Shalabh Jain, Tuan Ta, and John S. Baras. 2012. Wormhole detection using channel characteristics. In *2012 IEEE International Conference on Communications (ICC)*. IEEE, Ottawa, Canada, 6699–6704.

[36] Kyungho Joo, Wonsuk Choi, and Dong Hoon Lee. 2020. Hold the Door! Fingerprinting Your Car Key to Prevent Keyless Entry Car Theft. In *Proceedings 2020 Network and Distributed System Security Symposium*, Dongyan Xu and Ahmad-Reza Sadeghi (Eds.). Internet Society, Reston, VA.

[37] Konrad-Felix Krentz and Gerhard Wunder. 2014. 6LoWPAN Security: Avoiding Hidden Wormholes Using Channel Reciprocity. In *Proceedings of the 4th International Workshop on Trustworthy Embedded Devices* (Scottsdale, Arizona, USA) *(TrustED '14)*. Association for Computing Machinery, New York, NY, USA, 13–22.

[38] Jae-Yeong Lee, Byeongkwan Kim, Myun joo Park, and Byungje Lee. 2012. Isolation Enhancement between Indoor Repeater Antennas with Chip Resistor Embedded FSS. *International Journal of Antennas and Propagation* 2012 (2012), 1–7.

[39] P. Leu, M. Singh, M. Roeschlin, K. G. Paterson, and S. Čapkun. 2020. Message Time of Arrival Codes: A Fundamental Primitive for Secure Distance Measurement. In *2020 IEEE Symposium on Security and Privacy (SP)*. 500–516.

[40] Albert Levi, Erhan Çetintaş, Murat Aydos, Çetin Kaya Koç, and M. Ufuk Çağlayan. 2004. Relay Attacks on Bluetooth Authentication and Solutions. In *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 278–288.

[41] Linear Technology Corporation. 2008. LT5538 - 40MHz to 3.8GHz RF Power Detector with 75dB Dynamic Range. https://www.analog.com/media/en/technical-documentation/data-sheets/5538f.pdf (accessed: February 04, 2022).

[42] Lishoy Francis and Gerhard Hancke and Keith Mayes and Konstantinos Markantonakis. 2012. Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones. In *The 2012 Workshop on RFID and IoT Security (RFIDsec 2012 Asia) (Cryptology and Information Security Series, Vol. 8)*. IOS Press, 21–32.

[43] M/A-COM Technology Solutions Inc. [n. d.]. MAPS-010164: Digital Phase Shifter. https://cdn.macom.com/datasheets/MAPS-010164.pdf (accessed: February 04, 2022).

[44] Hildur Ólafsdóttir, Aanjhan Ranganathan, and Srdjan Capkun. 2017. On the Security of Carrier Phase-Based Ranging. In *Cryptographic Hardware and Embedded Systems – CHES 2017 (Lecture Notes in Computer Science, Vol. 10529)*. Springer, Taipei, Taiwan, 490–509.

[45] Aanjhan Ranganathan and Srdjan Capkun. 2017. Are We Really Close? Verifying Proximity in Wireless Systems. *IEEE Security & Privacy* 15, 3 (2017), 52–58.

[46] Aanjhan Ranganathan, Boris Danev, Aurélien Francillon, and Srdjan Capkun. 2012. Physical-Layer Attacks on Chirp-Based Ranging Systems. In *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Tucson, Arizona, USA) *(WiSec '12)*. Association for Computing Machinery, New York, NY, USA, 15–26.

[47] Jason Reid, Juan M. Gonzalez Nieto, Tee Tang, and Bouchra Senadji. 2007. Detecting Relay Attacks with Timing-Based Protocols. In *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security* (Singapore) *(ASIACCS '07)*. Association for Computing Machinery, New York, NY, USA, 204–213.

[48] Michael Roland, Josef Langer, and Josef Scharinger. 2013. Applying relay attacks to Google Wallet. In *2013 5th International Workshop on Near Field Communication (NFC)*. IEEE, Zurich, Switzerland, 1–6.

[49] Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, and N Asokan. 2014. Drone to the rescue: Relay-resilient authentication using ambient multi-sensing. In *International Conference on Financial Cryptography and Data Security*. Springer, 349–364.

[50] Mridula Singh, Patrick Leu, AbdelRahman Abdou, and Srdjan Capkun. 2019. UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 73–88.

[51] Mridula Singh, Patrick Leu, and Srdjan Capkun. 2019. UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks. In *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS)*. Internet Society, San Diego, California, USA.

[52] Sławomir, Jasek. [n. d.]. GATTacking Bluetooth Smart Devices. SecuRing. https://github.com/securing/docs/raw/master/whitepaper.pdf (accessed: February 04, 2022).

[53] Raymond Michael Stitt. 2020. Passive entry/passive start systems implementing carrier phase based ranging with music style eigenvalue decomposition for distance determinations. Patent No. US20200219344A1, Filed March 19th., 2020.

[54] synaptics. [n. d.]. Synaptics Launches Industry's First Matter-Compliant Triple Combo™ SoC with Integrated Wi-Fi 6/6E, Bluetooth 5.2, and 802.15.4/Thread for Seamless IoT Connectivity. https://www.synaptics.com/company/news/synaptics-launches-industrys-first-matter-compliant-triple-combo (accessed: February 05, 2022).

Table 2: Relay hardware components. The lower part lists components required to conduct the outlined signal manipulation attacks.

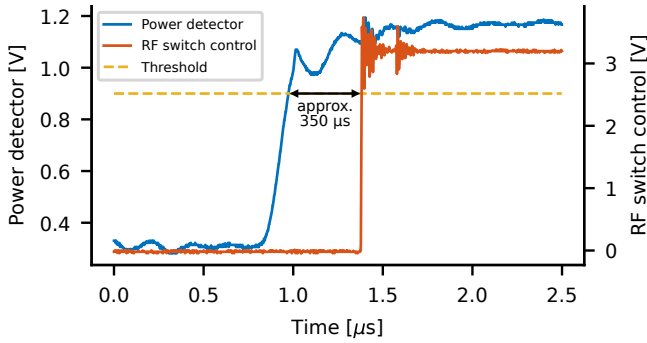| Hardware Component	Quantity	Purpose
Mini-Circuits ZX60-272LN-S+	2	Low-Noise Amplifier (LNA), first amplifier stage
Mini-Circuits ZX60-2534MA+	2	Amplifier
Mini-Circuits ZX60-2522MA+	2	Amplifier
Renesas F2932	2	SPDT RF switch, signal direction selection
Renesas F2910	2	SP1T RF switch, isolation enhancement
Mini-Circuits ZFSC-2-10G+	2	RF power splitter, tap signal for power detector
Analog Devices LT5538	2	RF power detector, signal detection of A
Crystek CBPFS-2441	1	Bandpass filter, reject noise and outband interference
Siretta LLC200A 15m	8	Coaxial cable, connect relay stations
Interline PANEL 17	2	Directional antenna, pick up victim signals
ST STM32G474RE	1	Microcontroller, comparator and relay control
M/A-COM MAPS-010164	1	Phase shifter, MCPR distance manipulation
Analog Devices HMC624A	1	Step attenuator, reciprocity manipulation

Figure 10: Output voltage of the power detector at the primary relay station, detection threshold voltage ($0.9\,\mathrm{V}$, corresponding to an RF input power of approx. $-40\,\mathrm{dBm}$ [41]), and RF switch control signal during the start of a Bluetooth transmission, indicating a reaction time of approx. $350\,\mu\mathrm{s}$ after threshold crossing.
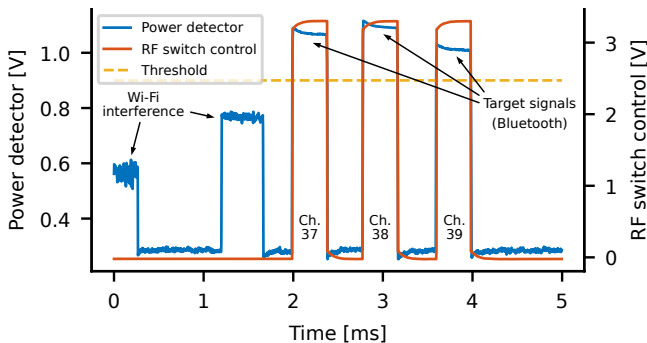

Figure 11: Power detector output voltage and RF switch control signal while receiving Bluetooth advertisement packets (consecutively on channels 37, 38, 39) of the smart lock. Nearby Wi-Fi interference is received weaker and does not trigger detection.

[55] Texas Instruments. 2019. SimpleLink™ CC2640R2 SDK User's Guide for BLE-Stack 3.03.01.00 (RTLS Toolbox, Time of Flight). http://software-dl.ti.com/simplelink/esd/simplelink_cc2640r2_sdk/3.30.00.20/exports/docs/blestack/ble_user_guide/html/ble-stack-3.x-guide/localization-index.html (accessed: February 04, 2022).

[56] Hien Thi Thu Truong, Xiang Gao, Babins Shrestha, Nitesh Saxena, N Asokan, and Petteri Nurmi. 2014. Comparing and fusing different sensor modalities for relay attack resistance in Zero-Interaction Authentication. In *2014 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, Budapest, Hungary, 163–171.

[57] Lawrence Ulrich. 2019. Smartphones Replace Fobs for Keyless Vehicle Entry. IEEE Spectrum. https://spectrum.ieee.org/cars-that-think/transportation/advanced-cars/smartphones-replace-fobs-for-keyless-vehicle-entry (accessed: February 04, 2022).

[58] Lennert Wouters, Benedikt Gierlichs, and Bart Preneel. 2021. My other car is your car: compromising the Tesla Model X keyless entry system. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021, 4 (2021), 149–172.

[59] Lennert Wouters, Eduard Marin, Tomer Ashur, Benedikt Gierlichs, and Bart Preneel. 2019. Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2019, 3 (2019), 66–85.

[60] Ali Yassin, Youssef Nasser, Mariette Awad, Ahmed Al-Dubai, Ran Liu, Chau Yuen, and Ronald Raulefs. 2017. Recent Advances in Indoor Localization: A Survey on Theoretical Approaches and Applications. *IEEE Communications Surveys Tutorials* 19, 2 (2017), 1327–1346.

[61] Pouria Zand, Jac Romme, Jochem Govers, Frank Pasveer, and Guido Dolmans. 2019. A high-accuracy phase-based ranging solution with Bluetooth Low Energy (BLE). In *2019 IEEE Wireless Communications and Networking Conference, WCNC 2019*. IEEE, Marrakech, Morocco.

[62] Christian Zenger, Mario Pietersz, and Christof Paar. 2016. Preventing relay attacks and providing perfect forward secrecy using PHYSEC on 8-bit μC. In *2016 IEEE International Conference on Communications Workshops (ICC)*. IEEE, Kuala Lumpur, Malaysia, 110–115.

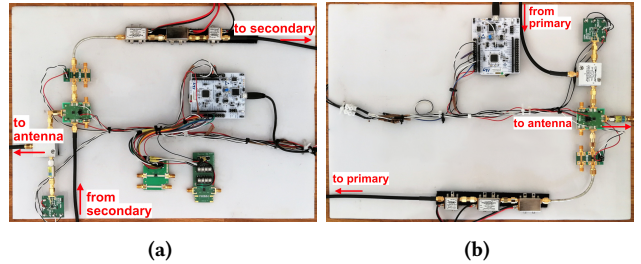## A RELAY HARDWARE DETAILS

Figure 9: Our experimental relay setup consists of the (a) primary and (b) secondary relay stations. At the primary station, a phase shifter and a step attenuator used in Section 5 can be seen.

In the following, we provide additional details on our proof-of-concept attacker implementation. Figure 9 depicts our experimental realization of the primary and secondary relay stations, assembled using off-the-shelf RF building blocks. An architectural block diagram of the implemented setup is shown in Fig. 1. For simplicity, we only show two amplifiers per direction in the block diagram. In fact, we used a cascade of three RF amplifiers, delivering a total gain of 75 dB for each direction. A detailed list of all parts and their
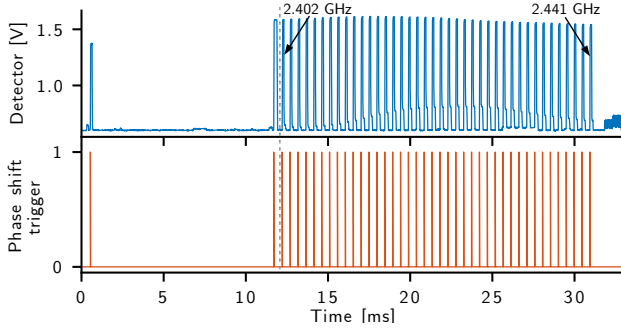
Figure 12: Top: Raw power detector output signals, indicating when node A **transmits. Bottom: Detection times of the attacker to proceed to the next phase shift setting. From** 12 ms **on (dashed line), the MCPR tone exchange comprising of** 40 **sweeped carriers is clearly visible.**

purpose to implement our attacker setup can be found in Table 2. The upper part of the table lists the parts used for the relay configuration used in Section 4. For the experiments in Section 5, we additionally added the parts listed in the lower part of the table as shown in Fig. 4.

We selected the components listed in Table 2 primarily for their operating frequency to match the 2.4 GHz frequency band. A fast response time is desired for the reactive switching of the relay to avoid cutting off initial parts of a transmission from A. Therefore, we specifically chose components having rather fast response times being much shorter than the 1 μs and 0.5 μs symbol duration of transmissions of BLE at 1 Mbps and 2 Mbps. The RF response time is governed by the power detector, the comparator which converts the power detector output into a logic signal, and the RF switches. The relay's response upon a beginning transmission of A can be seen in Fig. 10. Reactive switching is accomplished within approx. 0.35 μs after signals from A cross the power detection threshold at the primary relay station. Please note that this is approx. 0.795% and 0.016% of the shortest (44 μs) and longest (2128 μs) possible BLE packets, respectively [12]. The relay directions are flipped back after A stops to transmit, without any limitation of the maximum transmission duration. The power detector is capable of detecting signals from −75 dBm to 10 dBm. Considering interference from other radio traffic, in a typical office environment, we found input powers of −45 dBm to be sufficient to distinguish between targeted and other signals. Fig. 11 shows an example trace captured from the relay's primary power detector while the relay receives BLE advertisement packets from the smart lock (at 1 m distance). It can be seen that the high received signal power triggers the detection. In contrast, interfering signals from a nearby Wi-Fi access point (0

to 2 ms in the plot) are not as strong as the target signals and do not trigger the detection.

For adaptive signal manipulation, e. g., MCPR distance manipulation, we used a microcontroller to process and react to the comparator output signals. The microcontroller accordingly controlled a phase shifter with 6 bit phase resolution over 360° [43].

Another important aspect of the implementation is the isolation between the relay's transmission paths. Isolation is critical since a portion of the amplifier output will reach the input of the other direction's amplifiers. When the overall amplification is too large in regard of the finite path isolation, this again creates a feedback loop, causing instability of the overall system. In our relay implementation, the isolation between the paths is dominated by the electronically controlled solid state RF switches. Here, we initially were facing the RF amplifiers to slightly oscillate. We tackled the issue by adding a pair of F2910 SP1T switches in front of the LNA inputs to increase the total isolation. For the sake of simplicity, we do not indicate these switches in Fig. 1 as these are always controlled in conjunction with the main SPDT switches.

B MCPR POWER DETECTOR OUTPUT

Fig. 12 (top) shows the power detector output before and during a proprietary MCPR procedure between two BLE transceivers [21]. We clearly observe the effect of the sweeped carrier measurement comprising of $N = 40$ successive tone transmissions. The rising edges of the power detector output (bottom) correspond to the times t at which we apply the phase shift ϕ_t.

C USING CIRCULATORS

The TDD operation of the legitimate nodes is an important aspect for the implementation of our attacker setup. Although the attacker cannot predict when each node will transmit, the TDD implies that transmissions do not occur simultaneously. Importantly, this allows us to separately handle signal directions by means of adaptive switching based on power detection. As an alternative, it would be possible to replace the switches through circulators. A circulator is a passive three-port RF circuit, designed to separate signal directions. It is often used to transmit and receive over the same antenna simultaneously, which is desired for, e. g., radar or full-duplex radios. In particular, the circulator isolates the receiver from the transmitter and thereby mitigates interference. In the context of our attack, circulators would allow us to omit the power detection while applying bidirectional amplification. However, as we have outlined in Section 5, the power detector is essential to apply targeted signal manipulation. In comparison to RF switches, circulators typically are rather limited in terms of isolation [9]. This, however, limits the relay's amplification gain (and thus the maximum relaying distance) that can be applied without running into instability issues.