Are We Really Close? Verifying Proximity in Wireless Systems

Aanjhan Ranganathan, Srdjan Capkun
Institute of Information Security, ETH Zurich
{raanjhan,capkuns}@inf.ethz.ch

1 Introduction

It's Friday, late afternoon. Jane is delighted that a hectic week at work came to an end. On her way home, she stops at a nearby store. Her flying drone follows her closely, remaining within few meters distance, filming her movements and making her feel safer. In the store, Jane picks up her groceries and simply taps her credit card on the payment terminal to pay for them. A second later, there is a beep indicating that the card was sensed to be in the proximity of the terminal and that the payment transaction was successful. Jane carries the groceries and heads to her car. As she approaches the car, the door unlocks, the trunk opens allowing her to unload the goods into the car without her having to search for the keys. When she arrives home, her house door unlocks and opens, after it sensed that her keys are in close proximity. Her friends come over for dinner and as they physically enter her home, their devices automatically gain access to her WiFi connection as well as to multimedia that Jane selected for her guests. Jane doesn't worry about her data being accessed by strangers, it is only accessible by devices that are physically located in her home.

Today, we live in a physical world in which a wide variety of applications depend on location and proximity information. The above story illustrates this through a mix of existing and future applications. Contactless access tokens (e.g., contactless smart/proximity cards, key fobs) are prevalent today in a number of systems including public transport ticketing, parking and highway toll fee collection, payment systems, electronic passports, physical access control and personnel tracking. In a typical access control application, an authorized person simply taps his smart card against a card reader setup at the entrance to gain access to an infrastructure. Smart card-based physical access control and authentication are deployed even in safety- and security-critical infrastructures such as nuclear power plants and defense research organizations. Similarly, in an electronic payment scenario, the consumer places the contactless card in close *proximity* (a few centimeters) to the payment terminal for making secure payments. Furthermore, modern automobiles use passive keyless entry systems (PKES) to unlock, lock or start the vehicle when the *key fob* is in close proximity without any user interaction. PKES also enhances security in scenarios e.g., where the user forgets to manually lock the car or in the case of a jamming attack. In all the above systems, proximity between two entities is verified based on their ability to communicate with each other.

Even though the communication range for many such wireless systems is assumed to be limited, several works [1, 2] have demonstrated that these systems are vulnerable to relay attacks. In a relay attack (Figure 1 and Figure 2), the attacker uses a proxy devices to relay the communications between two legitimate entities without requiring any knowledge of the actual data being transmitted; therefore independent of any cryptographic primitives implemented. In [1] researchers were able to unlock the car and drive away even though the legitimate key was several hundred meters away from the car. In addition to relay attacks, an attacker can also modify the measured distance by manipulating or building specialized radio hardware, or by colluding with other entities. Thus, distance modification attacks have serious implications: an attacker can gain entry into a

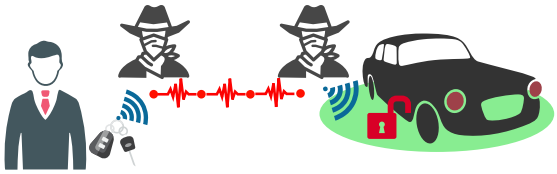

Figure 1: Relay attack on Passive Keyless Entry Systems in Automobiles

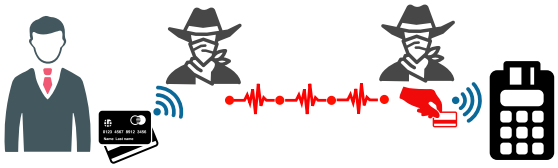

Figure 2: Relay attack on Contactless Payment Systems

restricted area, make fraudulent payments or steal a car by simply relaying the communications between the reader and the card which is several meters away without the knowledge of the card's owner.

Given the potential implications of the attacks mentioned above, there is a clear need to design and develop proximity systems that are secure against modern day cyber physical attacks. In order to prove proximity in wireless systems, it is fundamental to estimate the physical distance between two or more entities. In this article, we survey various approaches that are currently used to infer proximity. Further, we analyse their resilience to distance modification attacks which leads to a false proximity inference. Finally, based on the observations, we draw conclusions on the design requirements for proving proximity in wireless systems.

2 Establishing Proximity

Establishing proximity requires estimating the physical distance between two or more wireless entities. Typically, the distance is estimated either by observing the changes in the signal's physical properties (e.g., amplitude, phase) that occur as the signal propagates or by estimating the time taken for the signal to travel between the entities.

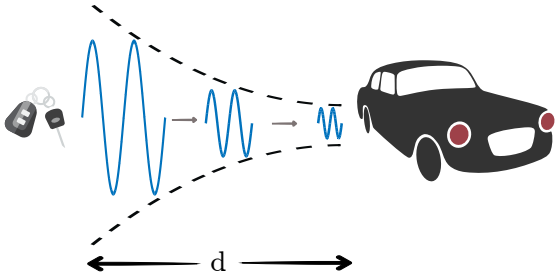

Figure 3: RSS-based distance estimation

RSS-based Distance Estimation. Radio signals experience a loss in its signal strength as it travels through the medium such as free space or air. The amount of loss or attenuation in the signal's strength is proportional to the square of the distance travelled. Mathematically, the exact distance d between the transmitter and the receiver can be calculated based on the free space path loss equation. In reality, the signal experiences additional losses due to its interaction with the objects in the environment which are difficult to account for accurately. This directly affects the accuracy of the computed distance and therefore advanced models such as the Rayleigh fading and log-distance path loss models are typically used to improve the distance estimation accuracy. Bluetooth-based proximity sensing tags (e.g., Apple iBeacon `https://developer.apple.com/ibeacon/`) that are prevalent today use the strength of the received bluetooth signal also referred to as the Received Signal Strength Indicator (RSSI) value as a measure of proximity. For example, an alarm may be sounded if the key or the item that is tagged exceeds a set threshold for RSSI values indicating that the item might be further way than necessary. Furthermore, current PKES systems used in automobiles also use RSS distance estimation to infer proximity.

Phase-based Distance Estimation. An alternative way to measure distance is to use the phase of the radio frequency signal. Two devices can measure the distance between them by estimating the phase difference between a received continuous wave signal and a local reference signal. In the scenario of the car

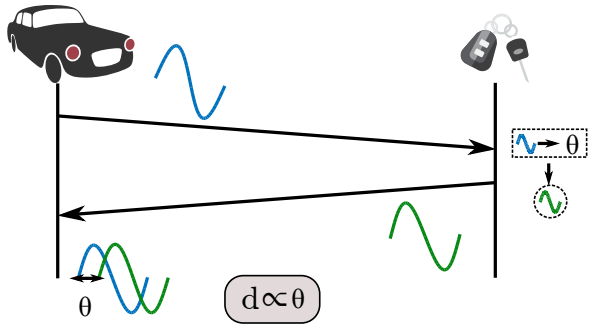

Figure 4: Phase-based distance estimation

trying to estimate its proximity to the keyfob, the car begins ranging by transmitting a continuous wave sinusoid signal. The keyfob locks its local oscillator to this incoming signal and transmits it back to the car. The car measures the distance based on the difference in the phase of the received signal and its own reference signal as shown in Figure 4. The need for keeping track of the number of whole cycles elapsed is eliminated by using signals of different frequencies typically referred to as *multicarrier phase-based ranging*.

Due to their low-complexity and low power requirement, multicarrier phase ranging (e.g., Atmel AVR2152 `www.atmel.com`) is a cost-optimized solution for a wide variety of applications including positioning of ultra-high frequency RFID systems. Further more, leveraging the proliferation of 802.11 WiFi networks and the availability of carrier phase information directly from the network cards, several indoor localization schemes [3, 4] have been proposed and implemented recently using commodity WiFi cards achieving centimeter-level precision. It is worth noting that a majority of radar systems today use techniques similar to phase-based to determine the distance and speed of a target object.

Time-of-flight based Distance Estimation. As an alternative to using the radio signal's amplitude, phase or frequency, the *time* taken for the radio waves to travel from one point to an other can be used to measure the distance. In Time-of-flight (ToF) based distance estimation, knowing the propagation speed of the signal (e.g., radio signals travel approximately at the speed of light), the distance d between two entities is given by $d = (t_{rx} - t_{tx}) \cdot c$, where c is the speed of light, t_{tx} and t_{rx} represent the time of transmission and reception respectively. The measured time-of-flight can either be one way time-of-flight or a round-trip time-of-flight. One way time-of-flight measurement requires the clocks of the measuring entities to be tightly synchronized. The errors due to mismatched clocks is compensated in a round-trip time-of-flight measurement.

The round-trip time is the time elapsed between transmitting a ranging data packet and receiving an acknowledgment back. For example, as shown in the Figure 5, the distance between the car and the keyfob is given by $d = \frac{c.(t_{tof} - t_p)}{2}$, where t_{tof} is the measured round-trip time and t_p is the processing delay i.e., the time taken by the keyfob to receive, process and transmit the acknowledgment back to the automobile. The precise distance measurement largely depends on the system's ability to estimate the time-of-arrival and the physical characteristics of the radio frequency signal itself. As a general rule of thumb, the ranging precision is directly proportional to the bandwidth of the ranging signal. Depending on the required level of accuracy, time-of-flight based distance measurement systems use either impulse-radio ultra wideband (IR-UWB) or chirp spread spectrum (CSS) signals. IR-UWB systems provide centimeter-level precision while the precision of CSS systems is of the order of 1-2 m. There are a number of commercially available wireless systems that use round-trip time-of-flight for distance measurement today (e.g., PulsON `www.timedomain.com`, 3db Midas `www.3db-technologies.com`, DecaWave `www.decawave.com`, Zebra `www.zebra.com`).

3 Are We Really Close? Attacking Proximity

All the above described proximity-based wireless access control and authentication systems are insecure and vulnerable to a variety of distance modifications attacks. An attacker can exploit both data-layer as well as physical-layer weaknesses to manipulate the distance. Data-layer attacks can be, to a large ex-

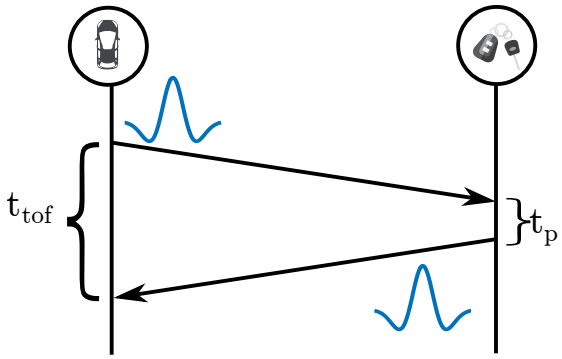

Figure 5: UWB TOF Ranging

tent prevented by implementing strong cryptographic primitives. However, physical-layer attacks are of significant concern as they can be executed independent of any higher-layer cryptographic primitive that is implemented. Today, with the increasing availability of low-cost software-defined radio systems, an attacker can eavesdrop, modify, compose, and (re)play radio signals with ease. This means that the attacker has full control of the wireless communication channel and therefore is capable of manipulating any message transmitted between the two entities. Therefore, in this article, we focus on the physical-layer distance manipulation attacks that are possible on today's proximity-based access control and authentication systems. More specifically, we focus on distance reduction attacks as they have been proven detrimental to the security of a wide variety of systems resulting in loss of property or even human life. As described previously, an attacker can steal a car or make fraudulent payments by simply reducing the distance measured even though the owner of the automobile or the payment card is far away. In this section, we describe how in each of the systems illustrated previously, an attacker can manipulate the measured distance independent of any higher-level cryptographic authentication implemented, thereby gaining unauthorised access. In order to maintain generality, throughout the remainder of this article we will refer to the entity that estimates the distance as the verifier (e.g., automobile, payment terminal) and the entity whose proximity is estimated as the prover (e.g., keyfob, contactless payment card).

3.1 Attacks on RSS- and Phase-based Proximity Systems

In an RSS-based distance estimation, an attacker can manipulate the measured distance by manipulating the received signal strength at the verifier. For example, as illustrated in Figure 6, the attacker can simply amplify the signal transmitted by the prover before relaying it to the verifier. This will result in a incorrect distance estimation at the verifier. Commercially available solutions such as SecuKey (`www.secukey.org`) claim to secure modern PKES systems against relay attacks by simply reducing or attenuating the power of the transmitted signal. An attacker can trivially circumvent such countermeasures by using higher gain amplifiers and receiving antennas.

Similarly, an attacker can also manipulate the estimated distance between the verifier and the prover in systems that use the phase or frequency property of the radio signal. For instance, the attacker can exploit the maximum measurable property of phase or frequency-based distance measurement systems and execute distance reduction attacks. The maximum measurable distance i.e., the largest value of distance d_{max} that can be estimated using a phase-based proximity system directly depends on the maximum measurable phase. Given that the phase values range from 0 to 2π and then rolls over, the maximum measurable distance also rolls over after a certain value.

An attacker can leverage this maximum measurable distance property of the system in order to execute the distance decreasing relay attack. During the attack, the attacker simply relays (amplify and forward) the verifier's interrogating signal to the prover. The prover determines the phase of the interrogating signal and re-transmits a response signal that is phase-locked with the verifier's interrogating signal. Then, as illustrated in Figure 6, the attacker receives the prover's response signal and forwards it to the verifier, however with a time delay (Δt). The attacker chooses the time delay such that measured phase differences reaches its maximum value of 2π and rolls over. Prior work [5] has shown that it is possible to reduce the measured distance by over $50\,\mathrm{m}$. In other words, the attacker was able to prove to the

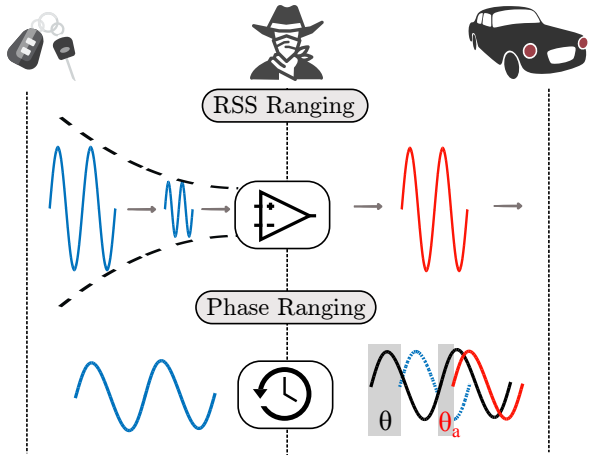

Figure 6: Attacks on RSSI Ranging and Phase Ranging

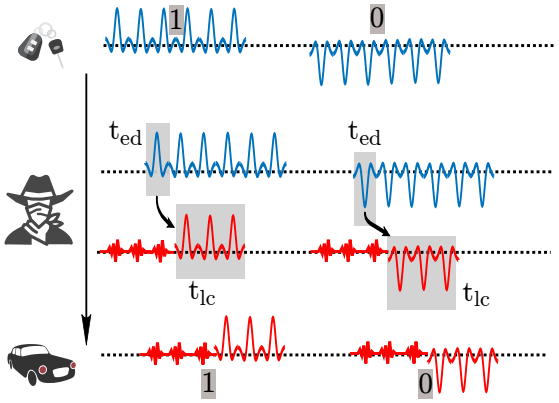

Figure 7: Early Detect and Late Commit Attack

verifier that the prover is in close proximity ($\approx 1\,\mathrm{m}$ away) even though the prover was more than $50\,\mathrm{m}$ from the verifier.

3.2 Attacks on Time of Flight Systems

From the above discussions we may conclude that estimating proximity based on the variations in the signal's amplitude, phase or frequency is vulnerable to distance modification attacks. We will now analyze the security of time of flight based distance measurement. Recall that in Time-of-flight (ToF) based ranging systems, the distance is estimated based on the time elapsed between the verifier transmitting a ranging packet and receiving an acknowledgement back from the prover. In order to reduce the distance measured, an attacker must decrease the signal's round trip time of flight. Based on the implementation, an attacker can reduce the estimated distance in a time-of-flight based ranging system in more than one way. Remember than a $10\,\mathrm{ns}$ decrease in the time estimate can result in a distance reduction of 1.5 m.

Leveraging Deterministic Signalling. First type of attack leverages the predictable nature of the data contained in the ranging and the acknowledgement packets. For instance, a number of time-of-flight ranging systems use pre-defined data packets for ranging, making it trivial for an attacker to predict and generate his own ranging or acknowledgment signal. An attacker can transmit the acknowledgment packet even before receiving the challenge ranging packet. Several prior works [6, 7, 8] have shown that the de facto standard for IR-UWB, IEEE 802.15.4a does not automatically provide security against distance decreasing attacks. It was shown that an attacker can potentially decrease the measured distance by as much as 140 meters by predicting the preamble and payload data with more than 99% accuracy even before receiving the entire symbol. For example, in a Cicada attack, the attacker continuously transmits a "1" impulse with a power greater than that of the prover. This degrades the performance of energy detection based receivers, resulting in reduction of the distance measurements as illustrated in the Figure 8. In order to prevent such attacks it is important to avoid pre-defined or fixed data during the time critical phase of the distance estimation scheme.

Leveraging Long Symbol Lengths. In addition to having the response packet dependent on the challenge signal, the way in which these challenge and response data are encoded in the radio signals affects the security guarantees provided by the ranging or localization system. An attacker can predict the bit (early-detect) even before receiving the symbol completely [9]. Furthermore, the attacker can leverage the robustness property of modern receivers and transmit arbitrary signal until the cor-

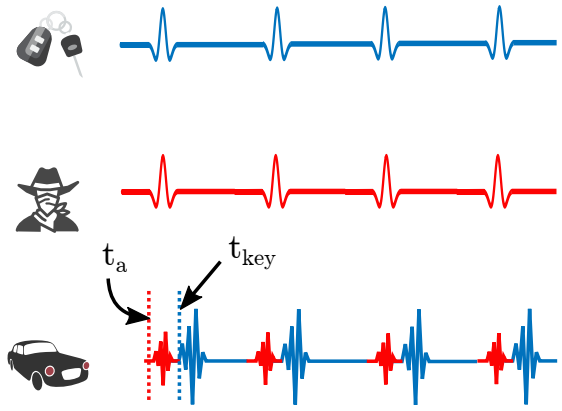

Figure 8: Cicada attack

rect symbol is predicted. Once the bit is predicted (e.g., early-detection), the attacker stops transmitting the arbitrary signal and switches to transmitting the bit corresponding to the predicted symbol, i.e., the attacker "commits" to the predicted symbol, commonly known as late commit. We illustrate the early detect and late commit attacks in Figure 7. Consider the key fob transmits '1' and '0' using a series of UWB pulses. In such a scenario, the attacker needn't wait for the entire series of pulses to be received befor detecting the data being transmitted. After just a time period t_{ed}, the attacker would be able to correctly predict the symbol as illustrated. Meanwhile, the attacker can transmit an arbitrary signal towards the car while trying to determine the signal transmitted by the key. Once the symbol is determined, the attacker transmits the correct signal to the car. Modern receivers are designed to be robust. Therefore, they are capable of detecting the symbol correctly even if all the pulses are not completely received. The attacker exploits this property and therefore even though the received symbol contains arbitrary signal in the beginning, the car will decode the symbol correctly with the data that was committed late by the attacker.

As described previously, round-trip time-of-flight systems are implemented either using chirp or impulse-radio ultra wideband signals. Due to their long symbol lengths, both implementations have shown to be vulnerable to early-detect and late-commit attacks [10, 6]. In the case of chirp-based systems, an attacker can decrease the distance by more than $160\,\mathrm{m}$ and in some scenarios even upto $700\,\mathrm{m}$. Although IR-UWB pulses are of short duration (typically 2–3 ns long), data symbols (e.g., challenges and responses) are typically exchanged using a series of UWB pulses. Furthermore, IEEE 802.15.4a IR-UWB standard allows long symbol lengths ranging from $32\,\mathrm{ns}$ to as large as $8\,\mu\mathrm{s}$. Therefore, even the smallest symbol length of $32\,\mathrm{ns}$ allows an attacker to reduce the distance by as much as $10\,\mathrm{m}$ by performing early-detect and late-commit attacks.

Thus, it is clear that in order to guarantee proximity and secure a wireless proximity system against early-detect and late-commit attacks, it is necessary to keep the symbol length as short as possible.

4 Proving Proximity

As we see, proving proximity in wireless systems is not a trivial task and must satisfy a number of design requirements in order to be secure. Based on the observations, in this section we draw conclusions on the design requirements for proving proximity in wireless systems.

Round Trip Time-of-Flight. First, it is important to select a distance estimation approach that makes it hardest for the attacker to manipulate. Both RSS- and Phase-based distance estimation techniques allow the attacker to falsify proximity by simply amplifying or delaying the radio signals without any knowledge of the actual data that is being exchanged. However, in time-of-flight based distance estimation, it is not possible for the attacker to succeed by just forwarding the signals but he is required to actively receive, interpret, reconstruct and transmit the appropriate signal back to the verifier. Thus, round trip time of flight based distance estimation rises and the bar for the attacker and hence can be considered as a first design choice for proving proximity in wireless systems.

Challenge-Response Protocol. Even though round trip time-of-flight based distance estimation significantly rises the bar for the attacker, securing

Distance Estimation Method	Type of Attack	Proof of Proximity
Received Signal Strength	Amplify & Relay	None
Phase or Frequency	Delay & Relay	None
Time-of-flight (802.15.4a CSS)	Early-detect, Late-commit	Partial
Time-of-flight (802.15.4a IR-UWB)	Early-detect, Late-commit	Partial
Time-of-flight (Short symbol IR-UWB)	No attack[‡]	Yes

[‡] In addition to keeping symbol durations short, it is also necessary to implement specialized modulation and decoding techniques to prevent attacks like Cicada [7].

Table 1: Summary of distance estimation methods and their ability to prove proximity

it is not easy. As illustrated previously, one of the primary attack vector in such systems is to exploit the fixed response or acknowledgement that is used today by several wireless systems. Therefore, it is essential to prevent the attacker from guessing and transmitting acknowledgement packet even before receiving the request from the verifier. In other words, a challenge-response protocol must be implemented in which the round trip time is measured as the time elapsed between transmitting a randomly chosen challenge and receiving a corresponding response back from the prover.

Short Symbol Duration. As a final requirement, it is essential to keep the symbol duration as small as possible to prevent attacks such as the early-detect and late-commit attacks. Impulse-radio ultra wideband (IR-UWB) systems use pulses of very short time duration (typically $2-3\,\mathrm{ns}$ long) to transmit and receive data. This physical characteristic of IR-UWB make them a preferred choice over other signalling techniques for securely proving proximity. However, currently proposed standards (IEEE 802.15.4a/f `www.ieee802.org`) allow long symbol durations and therefore, system implementations based on these standards are still vulnerable to distance reduction attacks such as early-detect and late-commit. On the other hand short symbol durations restrict the devices from operating reliably over longer distance measurements. Some commercial systems (`www.3db-technologies.com`) implement a proprietary IR-UWB physical-layer with short symbol lengths in addition to specialized modulation and time-of-arrival estimation techniques and claim a maximum possible distance reduction of *less than a meter* while still being able to estimate proximity over $200\,\mathrm{m}$.

5 Summary

We summarize our observations in Table 1 and conclude that distance estimation techniques based on RSS, phase or frequency measurements do not provide any security guarantees on the physical proximity between the two entities. In these systems, an attacker can successfully prove close proximity irrespective of the true distance between the prover and the verifier by simply executing a passive relay attack. Time-of-flight based distance estimation methods significantly raises the bar for the attacker. An attacker is no longer able to manipulate the distance by simply relaying the signals, but has to actively predict and generate the corresponding symbol to execute the attack successfully. In order to prevent attackers from performing early-detect and late-commit attacks, it is essential to keep the symbol lengths as short as possible while estimating the time-of-flight. Thus we conclude by stating that time-of-flight based distance measurement using short symbol length IR-UWB signals are the most capable of guaranteeing proximity that is imperative in a number of modern wireless access control and authentication systems.

References

[1] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," 2011.

[2] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical nfc peer-to-peer relay attack using mobile phones," in *Radio Frequency Identification: Security and Privacy Issues*, 2010.

[3] D. Vasisht, S. Kumar, and D. Katabi, "Decimeter-level localization with a single wifi access point," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, 2016.

[4] R. Miesen, A. Parr, J. Schleu, and M. Vossiek, "360 degree carrier phase measurement for uhf rfid local positioning," in *RFID-Technologies and Applications (RFID-TA), 2013 IEEE International Conference on*, IEEE, 2013.

[5] H. Ólafsdóttir, A. Ranganathan, and S. Capkun, "On the Security of Carrier Phase-based Ranging," *ArXiv e-prints*, 2016.

[6] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. L. Boudec, "Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures," 2011.

[7] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. L. Boudec, "The Cicada Attack: Degradation and Denial of Service in IR Ranging," 2010.

[8] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. L. Boudec, "Effectiveness of Distance-Decreasing Attacks Against Impulse Radio Ranging," 2010.

[9] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, "So near and yet so far: Distance-bounding attacks in wireless networks," in *Security and Privacy in Ad-hoc and Sensor Networks*, Springer, 2006.

[10] A. Ranganathan, B. Danev, A. Francillon, and S. Capkun, "Physical-layer attacks on chirp-based ranging systems," in *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, ACM, 2012.