INSA TOULOUSE

UWB and Relay Attacks

Securing Vehicle Entry Systems Based on UWB

Report Members

Amine Benchekroun
Badr Diani
Samia Boukouiss
Baptiste Henriet
Paul Jaulhiac

1 Relay Attack Scenario for Unlocking a Car

Passive Keyless Entry Systems (PKES) are designed to provide maximum convenience to users by allowing them to unlock and start their vehicles without taking out their key. However, these systems are vulnerable to relay attacks, a technique that enables an attacker to bypass proximity mechanisms.

In a typical relay attack, two attackers work in coordination:

- The first attacker (Attacker 1) positions themselves near the car and uses a device to relay the car's signals to a second attacker.
- The second attacker (Attacker 2) positions themselves near the legitimate key, often inside a building, to capture and retransmit the key's signals to the car.

The attack works by exploiting the trust of the PKES system, which assumes that communication between the key and the car implies physical proximity. By relaying the signals between the car and the key over a long distance, attackers can deceive the system into unlocking and starting the vehicle, even if the key is far from the car.

This scenario is illustrated in Figure 1, where the steps of the attack are detailed:

1. The car sends signals to search for a legitimate key.
2. Attacker 2 captures these signals and retransmits them to Attacker 1.
3. Attacker 1 relays the key's responses to the car, thereby unlocking the vehicle and potentially starting the engine.

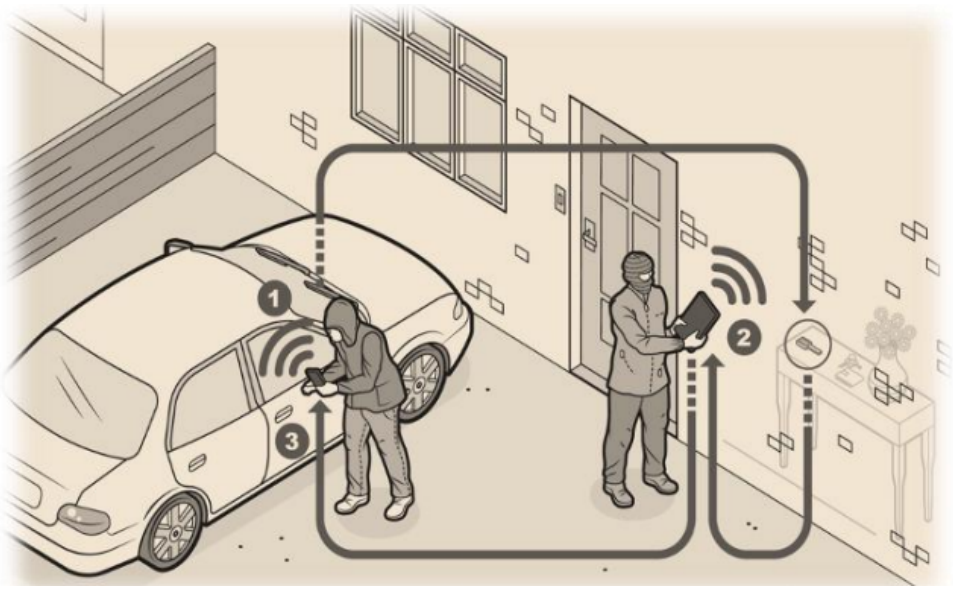

Figure 1: Illustration of a relay attack enabling vehicle unlocking.

2 Introduction to UWB: An Innovative Communication Technology

Ultra-Wideband (UWB) is a wireless communication technology that operates across a wide frequency spectrum, typically ranging from 3.1 GHz to 10.6 GHz. Unlike traditional

technologies such as Bluetooth or Wi-Fi, which use narrowband signals, UWB transmits short pulses across a broad range of frequencies. This transmission method offers unique advantages, particularly in terms of precision, reliability, and security.

2.1 Characteristics of UWB

The distinctive characteristics of UWB include:

- **High Precision**: UWB can measure distances with centimeter-level accuracy through Time of Flight (ToF) measurement, making it an ideal technology for applications requiring precise localization.
- **Low Interference**: Due to its wide frequency band and low spectral power density, UWB is less susceptible to interference from other wireless technologies, ensuring reliable communication in congested environments.
- **High Data Rates**: The ability to transmit data at high rates makes UWB suitable for applications requiring fast and large data exchanges.
- **Low Power Consumption**: With its low power level, UWB is well-suited for portable and embedded devices.

2.2 Comparison with Traditional Technologies

Figure 2 illustrates the difference between UWB and traditional wireless technologies, such as Wi-Fi and Bluetooth, in terms of frequency spectrum and transmission power.

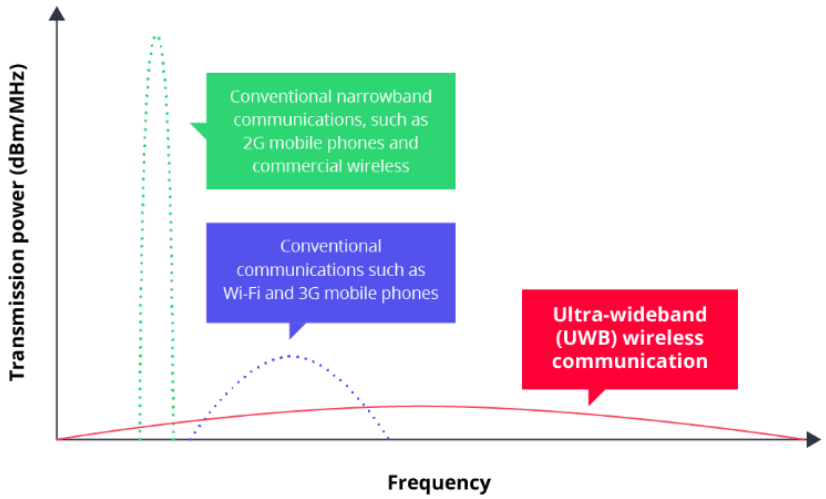

Figure 2: Comparison of Frequency Bands and Transmission Power Between Conventional Technologies and UWB.

As shown in the figure, UWB occupies a much wider frequency band compared to technologies like Wi-Fi or Bluetooth. This allows UWB to transmit signals with significantly lower transmission power, thereby reducing the risk of interference while ensuring robust communications.

3 Practical Applications of UWB

UWB is utilized across various sectors due to its unique capabilities:

- **Automotive Industry**: Used in keyless entry systems to enhance security. UWB ensures that the vehicle only unlocks when the legitimate key is detected within an authorized range, thereby preventing relay attacks.
- **Consumer Electronics**: Integrated into devices like Apple AirTags for precise object tracking and secure communication between devices.
- **Industry and Healthcare**: Leveraged in Real-Time Location Systems (RTLS) for tracking assets and people, as well as in medical imaging applications.

3.1 Conclusion

UWB is revolutionizing the field of wireless communications with its unique features, such as precision, reliability, and the ability to function in complex environments. This technology is particularly promising for applications where security and precision are critical, such as keyless entry systems or object tracking devices.

4 Why UWB is Immune to Relay Attacks

Relay attacks occur when the signal between an electronic key and a car is extended via a "tunnel" created by a pair of devices controlled by an attacker. This is possible because communication between the key and the car in traditional systems is not time-sensitive. However, UWB technology is largely immune to relay attacks due to its high temporal resolution and precise Time of Flight (ToF) measurements.

4.1 Illustration of a Relay Attack and UWB Response

In a relay attack, attackers attempt to relay the key's signal by introducing additional delay. UWB can detect this attempt through its precision in ToF measurement. For example:

- For a key located 1 meter from the car, the Time of Flight (ToF) is approximately 3.33 ns.
- For a key located 5 meters away, this ToF increases to 16.67 ns.

If the key is supposed to be within a 1-meter radius but the system measures a significantly higher ToF, as in the case of an attack, the signal is rejected. Figure 1 illustrates this process.

Thanks to this capability, UWB secures keyless entry systems by detecting temporal discrepancies introduced by attackers.

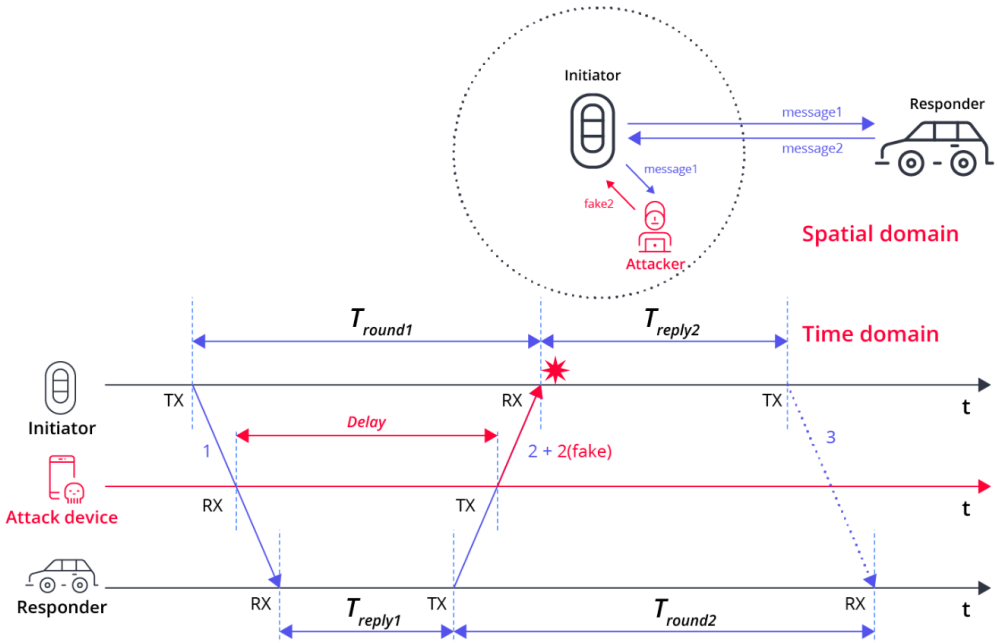

Figure 3: Illustration of a Relay Attack and the Role of UWB in Detecting Artificial Delays.

5 Potential Attacks Targeting UWB and Solutions

Although UWB is robust against relay attacks, it is not completely invulnerable. A known attack called *UWB accurate deafening* can disrupt the distance measurement function by introducing malicious messages within the time frame designated for communication between devices.

5.1 Mitigating Random Delay Attacks

To mitigate attacks such as *UWB accurate deafening*, a solution involves introducing a random delay between the reception and transmission of signals. This makes the message timings unpredictable for the attacker, causing their messages to fall outside the expected time frame and thus rendering them ineffective.

Figure 4 illustrates this countermeasure. By introducing random delays, malicious messages sent by the attacker arrive either too early or too late, and are therefore ignored by the legitimate system.

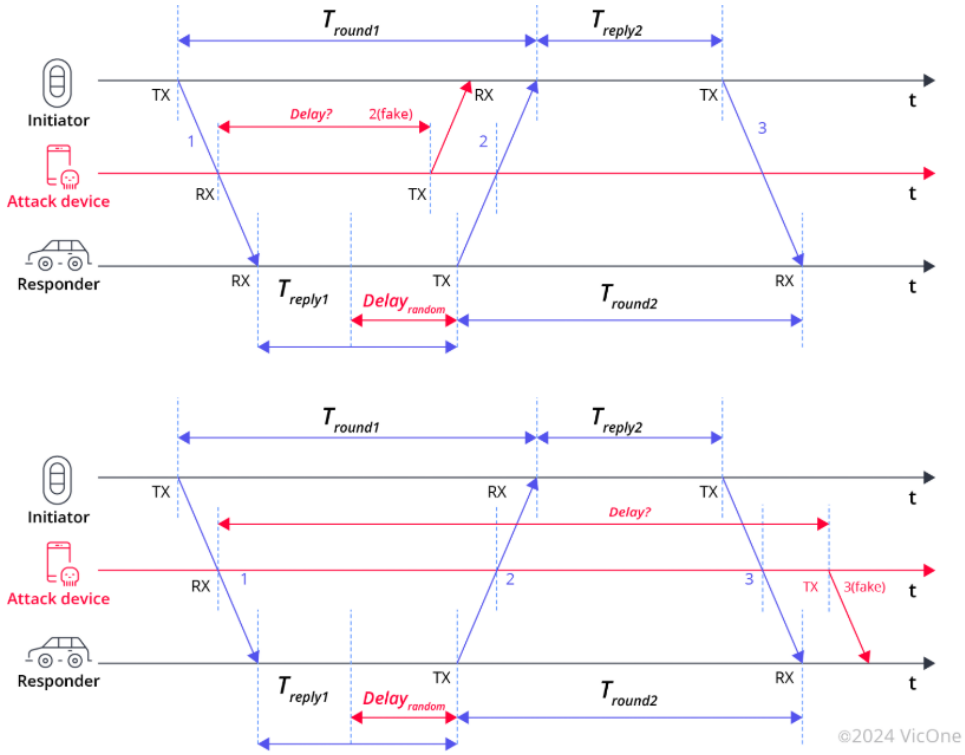

Figure 4: Attack Targeting UWB (*UWB Accurate Deafening*) and Mitigation Through Random Delays.

5.2 Conclusion

UWB provides enhanced security against relay attacks due to its ability to detect artificial delays. However, for more complex attacks like *UWB accurate deafening*, introducing random delays serves as an effective solution to ensure communication integrity.

6 Conclusion

Ultra-Wideband (UWB) represents a significant advancement in the field of wireless communications, particularly for the security of keyless entry systems. With its high temporal precision and ability to detect artificial delays, UWB offers robust protection against relay attacks, a critical issue for traditional PKES systems. However, while UWB is largely immune to such attacks, certain vulnerabilities remain, such as jamming or timing offset attacks. These weaknesses require complementary solutions, such as the introduction of random delays or secure positioning techniques.

By exploring the benefits and limitations of UWB, this report has highlighted its key role in securing modern systems. With continued advancements, UWB promises to set new standards for the security and reliability of wireless technologies.

7 References

- **VicOne**, *From Key Fob to UWB: Explaining and Securing Ultra-Wideband in Vehicles*, available online: `https://www.vicone.com/`.

- Francillon, A., Danev, B., Capkun, S., *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars*, ETH Zurich, 2010. Available online: `https://www.researchgate.net/publication/228961509_Relay_Attacks_on_Passive_Keyless_Entry_and_Start_Systems_in_Modern_Cars`.