imec
embracing a better life

WHITE PAPER

Secure and Accurate Distance Bounding for Bluetooth Secure Access

Mohieddine El Soussi, PhD, Aysajan Abidin, PhD, Jac Romme, PhD, Pepijn Boer, MSc, Christian Bachmann, PhD, Dave Singelee, PhD

Contents

Why you need to read this

Are you involved in the design and development of products that rely on secure proximity systems such as keyless entry, contactless payment or real-time location systems (RTLS)? Then security is without a doubt one of your major concerns. More specifically, the threat of relay attacks that allow criminals to decrease the measured proximity between two legitimate entities, giving them unauthorized access to vehicles, buildings or data.

This white paper describes a method to successfully deflect any such relay attack. It consists of a distance bounding protocol for Bluetooth Low Energy (BLE) radios, and its feasibility and practicality are established by the implementation of the solution on an NXP KW36 Bluetooth Low Energy radio platform.

Are you interested in implementing this technology in your own solutions? Or do you have any other questions or remarks?

Please contact Li Huang, Senior Business Development Manager, at **li.huang@imec.nl**.

Keywords

distance bounding, time of flight, phase difference, relay attack, BLE, narrow-band ranging, secure ranging, High Accuracy Distance Measurement, Bluetooth Channel Sounding, BT HADM / CS

Abstract

In tomorrow's world, we will rely on secure location and proximity information to perform an increasing list of daily actions such as:

SECURE ACCESS TO OUR HOMES

KEYLESS ENTRY INTO OUR VEHICLES AND PASSIVE ENTRY PASSIVE START (PEPS)

CONTACTLESS PAYMENT OF OUR GROCERIES

In all these scenarios, we will use wireless technology to establish secure proximity between our 'key' – a smartphone, smartwatch or other smart devices – and the device we want to access, such as an electric lock or payment terminal.

Which wireless technology is best suited for secure location and proximity? Ultra-wideband (UWB) solutions show some promise, but the technology is not yet widely used. Bluetooth, on the other hand, is already supported by a vast commercial ecosystem, and often built into smart devices. Combined with its ultra-low power and low-cost wireless functionality [1], that makes Bluetooth an ideal candidate for future secure proximity solutions. In this white paper, we demonstrate how such solutions can be realized.

One of the major challenges to overcome is vulnerability to relay attacks or relay station attacks [2]. Such relay stations are not necessarily restricted by the same communication range limits as legitimate entities. That gives them the ability to simply decrease the measured proximity between two legitimate entities by relaying their mutual communications.

Such an attack does not require any knowledge of the actual data that is being transmitted, which means you cannot prevent it by using cryptographic measures. The way to effectively mitigate such relay attacks is by implementing secure distance bounding (SDB) protocols. They allow a device to authenticate another device and securely determine its physical proximity.

This white paper describes such an accurate SDB protocol – the first one for Bluetooth Low Energy (BLE) radios. It is based on a combination of:

- novel phase-based distance measurement capabilities that provide high ranging accuracy;
- time of flight (distance bounding) estimations that provide security;

This protocol comprises three stages:

01 **Authenticated Key Exchange (AKE)** – The communicating entities securely agree on a symmetric session key.

02 **High-accuracy ranging and distance bounding** – A combination of timestamps, amplitude measurements and phase measurements ensures secure ranging.

03 **Authentication and authorization** – Based on the obtained results, one of the entities makes the authentication decision. Is it successful? Then that entity authorizes the other one to access the requested resources.

After a detailed description of the SDB protocol, this white paper analyzes how it manages to mitigate existing and foreseeable future relay attacks such as phase manipulation and Early-Detect and Late-Commit (ED/LC).

Finally, this white paper demonstrates the practicality of the protocol through an actual implementation of the entire solution on an NXP KW36 Bluetooth Low Energy chip. The results of this demonstration are also presented, including an accuracy of < 10 cm in a practical multi-path indoor environment. The security of the accurate distance bounding protocol has been analyzed by an independent third-party expert in wireless security.

The proposed protocol combines accurate ranging with guaranteed security for systems such as keyless locks, contactless payment terminals and real time location systems.


VERIFIER
PROVER

INTRODUCTION

This white paper focuses on secure and accurate ranging protocols for narrowband wireless systems – in this case Bluetooth. The systems involve two entities which are typically denoted as verifier and prover. The verifier controls access to a resource and the prover is trying to gain access to the resource controlled by the verifier. By default, such systems are vulnerable to relay attacks. In a relay attack, an adversary attempts to fool a legitimate verifier into believing that the legitimate prover entity is close, while it is in fact far away. The adversary does this by putting a proxy device close to the legitimate prover and another proxy device close to the legitimate verifier. It then relays the communication between these illegitimate entities.

A real-life example is a relay attack on the passive keyless entry system of your car. Suppose the car is locked and parked in front of your house. The car key is inside the house, far enough from the car to ensure that your car stays locked. Nevertheless, it is possible that an attacker unlocks your car, starts the engine and drives away. How? By simply using relay boxes that can receive wireless signals through walls, windows, doors ... and relay the signals from your car to your key – and vice versa. Figure 1 illustrates this process:

That this example is anything but theoretical, is proven by the rising number of such successful car thefts [3]. According to a recent BBC news article [4], keyless cars from several leading car brands performed poorly in anti-theft tests. All tested cars were vulnerable to relay attacks, which can be successfully performed in less than a minute.

Evidently, relay attacks pose serious security threats, leading to financial damages to individuals, organizations and society. We need a foolproof solution that combines accurate ranging with guaranteed security for systems such as keyless locks, contactless payment terminals and real time location systems (RTLS). This white paper will outline such a solution based on low-power, low-cost Bluetooth radios.

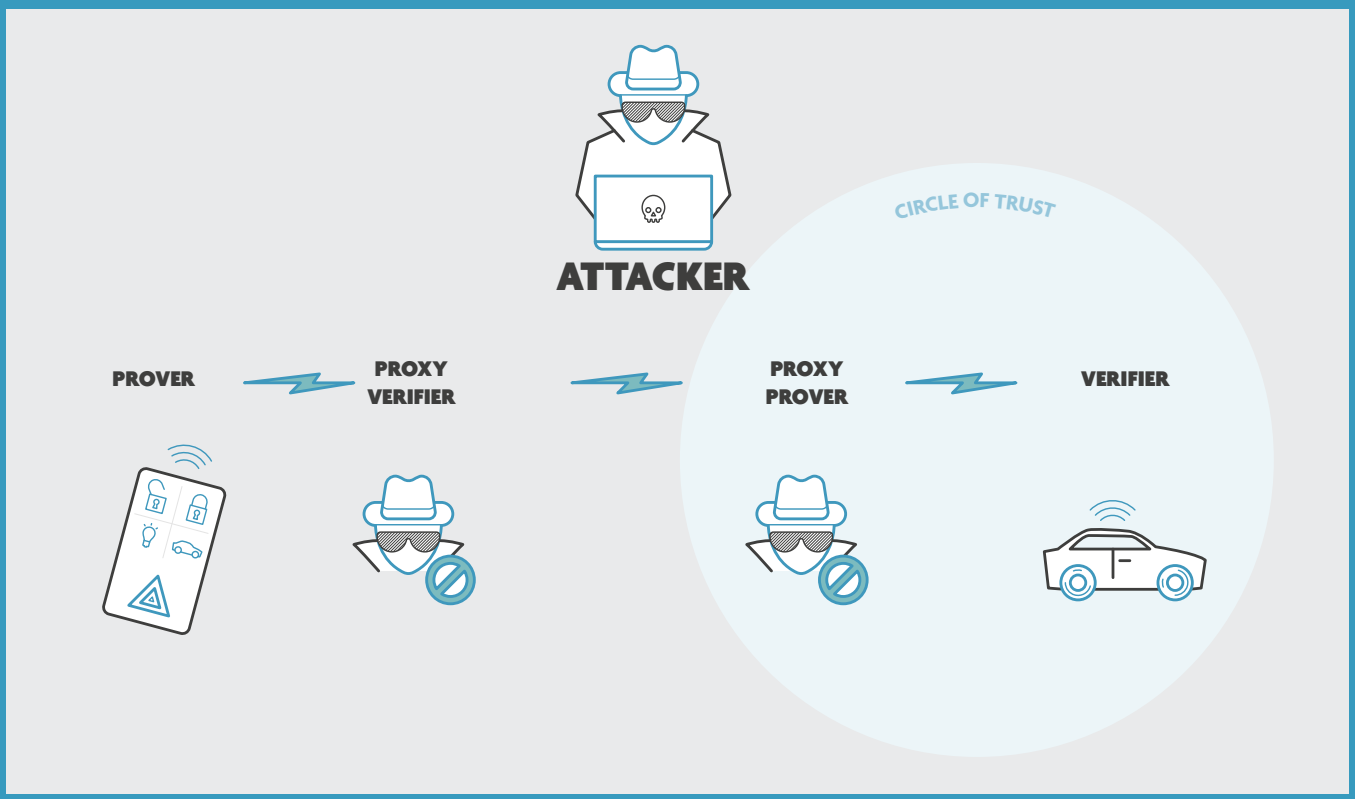
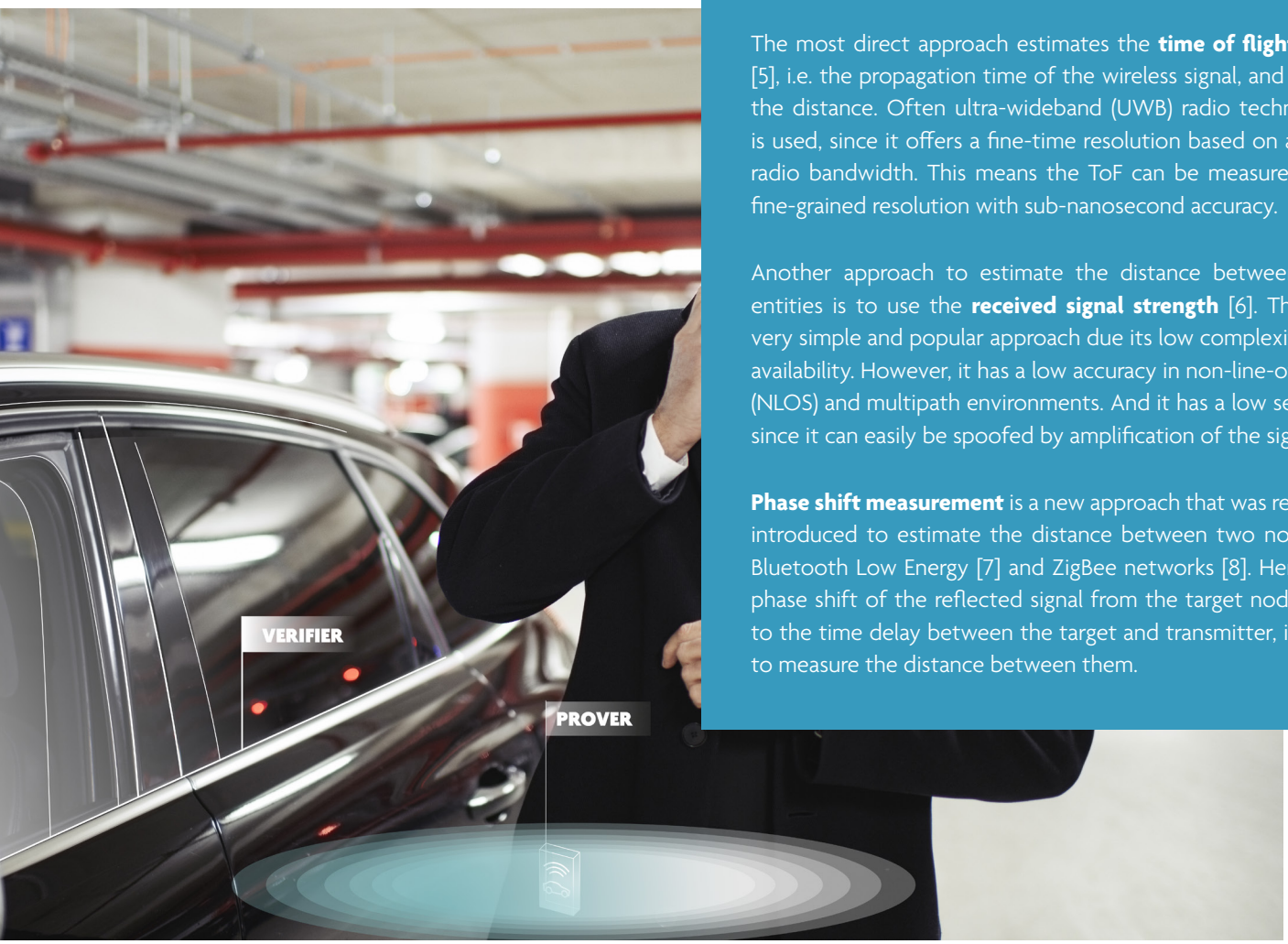


Figure 1 | Relay attack

Wireless distance measurements and secure distance bounding



Radio frequency (RF)-based distance measurement – or 'ranging' – can be achieved in different ways:

The most direct approach estimates the **time of flight** (ToF) [5], i.e. the propagation time of the wireless signal, and hence the distance. Often ultra-wideband (UWB) radio technology is used, since it offers a fine-time resolution based on a wide radio bandwidth. This means the ToF can be measured at a fine-grained resolution with sub-nanosecond accuracy.

Another approach to estimate the distance between two entities is to use the **received signal strength** [6]. This is a very simple and popular approach due its low complexity and availability. However, it has a low accuracy in non-line-of-sight (NLOS) and multipath environments. And it has a low security since it can easily be spoofed by amplification of the signal.

Phase shift measurement is a new approach that was recently introduced to estimate the distance between two nodes in Bluetooth Low Energy [7] and ZigBee networks [8]. Here, the phase shift of the reflected signal from the target node, due to the time delay between the target and transmitter, is used to measure the distance between them.

These diverse approaches have one thing in common: a vulnerability to relay attacks. To provide the needed security, distance bounding (DB) protocols allow you to establish an upper bound on the physical distance between two entities, essentially adding authentication to ranging.

The first distance bounding protocol to mitigate relay attacks was designed by Brands and Chaum [9]. This protocol comprises three stages: initialization, distance bounding and verification, as shown in Figure 2:

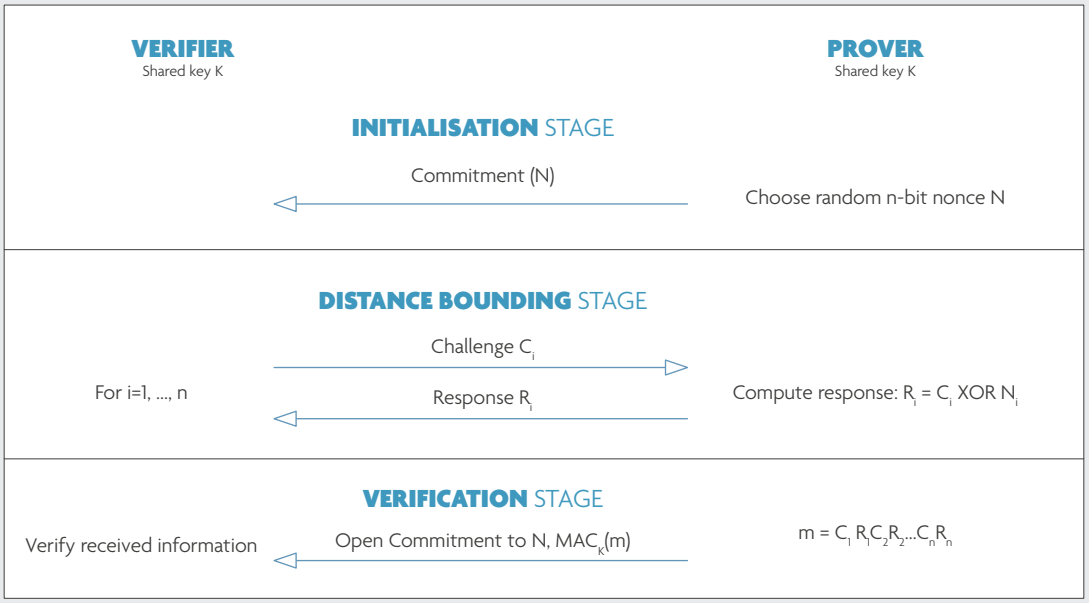


Figure 2 | The Brands-Chaum protocol [9]

01

INITIALIZATION STAGE

During the initialization stage, the prover selects at random a nonce (number used once) and commits it to the verifier using a secure commitment scheme. This is a cryptographic primitive that allows one to commit to a chosen number while hiding it from others and later to reveal the number by opening it.

02

DISTANCE BOUNDING STAGE

In the DB stage (composed of many fast rounds), the verifier and prover exchange random challenges and responses, respectively. The response which is sent by the prover is evaluated using the challenge and the nonce. The verifier, during this stage, estimates the time between sending a challenge and receiving a response.

03

VERIFICATION STAGE

In the verification stage, the prover sends to the verifier a MAC (message authentication code) of a message which is composed of the concatenated values of the challenges and responses exchanged during the DB stage. Finally, the verifier checks all the received information and then estimates an upper bound on the distance of the prover.

Proposed Bluetooth secure distance bounding

Based on the Brands-Chaum protocol, we propose a secure distance bounding (SDB) protocol for future Bluetooth systems, summarized in Figure 3.

The SDB protocol is built upon phase-based accurate ranging principles, while incorporating ToF estimates and distance bounding for security. Note that the SDB protocol starts after the two nodes exchange ranging request/acknowledgment, scheduling information and others. In order to perform the SDB protocol:

- The verifier needs to possess its own public and private keys and the public key of the prover.
- The prover needs to possess its own public and private keys and the public key of the verifier.

One way to enable the prover and the verifier to possess the required keys is to let each party generate its own public-private key pair and then exchange the public key with each other in a pre-setup stage.

The SDB protocol consists of three stages:

01 **AUTHENTICATED KEY EXCHANGE**

02 **DISTANCE BOUNDING**

03 **AUTHENTICATION & AUTHORIZATION**

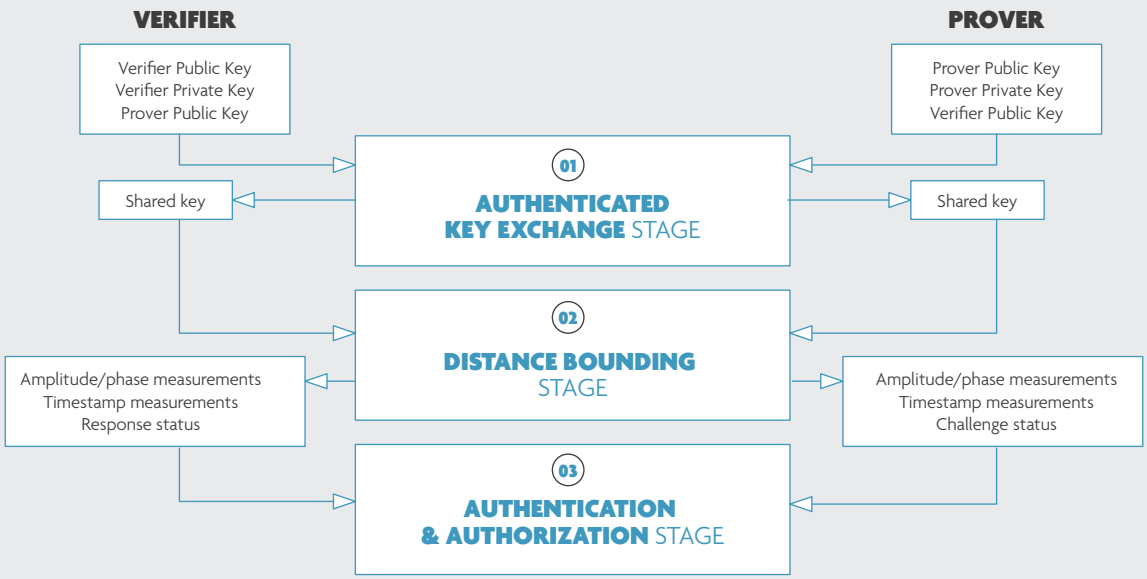


Figure 3 | Summary of the secure distance bounding protocol

01 AKE STAGE

During this stage, the verifier and the prover authenticate each other using their private and public keys and establish a shared secret key. The shared key is used to secure the communication and the distance measurements between the two nodes.

Various protocols are suited for this, such as the SIGMA protocol [10], an authenticated Diffie-Hellman key exchange protocol which provides mutual authentication.

02 DISTANCE BOUNDING STAGE

During this stage, the verifier and prover exchange continuous tone signals and packets:

- The tone signals are used to accurately estimate the distance, based on the multi-carrier phase difference (MCPD) [7] method.
- The packets are used to securely measure and estimate the ToF.

MCPD method

In the MCPD method, the verifier transmits a tone signal at a given frequency. The prover can measure the phase difference between its local oscillator and the received signal without modifying the phase. It then transmits back a tone signal that has a phase that depends solely on the prover's local oscillator. Subsequently, one of the nodes – typically the prover – sends his measurements (in the last stage of the proposed SDB protocol) to the other node. This last node estimates the range, using all the measurements obtained on all the frequencies. See [7] for more details.

The estimate for the range using the MCPD method is given by [7],

$$\hat{r} = -\frac{c_0}{4\pi\Delta f}\,\hat{\Delta}\phi \bmod \frac{c_0}{2\Delta f}$$

c_0 is the speed of light

Δf is the frequency step size – equal to the difference between two adjacent used carrier frequencies.

$\hat{\Delta}\phi$ is the phase shift between two adjacent frequencies averaged over multiple frequencies.

$\frac{c_0}{2\Delta f}$ is the range ambiguity.

Note that by transmitting multiple tone signals at different frequencies, the bandwidth has effectively been increased. In other words, the measurements at different frequencies are stitched together to create a wideband view on the channel. The MCPD method is designed for half-duplex devices and uses narrowband constant-envelope signals. This means it can be easily implemented on Bluetooth Low Energy compliant radio chips.

In the Bluetooth standard, the total bandwidth is 80 MHz, which can be divided into 40/80/160 channels, each with a bandwidth of 2 MHz/1 MHz/0.5 MHz, respectively. This wide bandwidth helps to improve the range accuracy and to mitigate the effect of multipath, especially in an indoor environment. The range ambiguity is inversely proportional to the frequency step size, Δf, hence the range ambiguity is equal to 75 m, 150 m and 300 m for a frequency step size of 2 MHz, 1 MHz and 0.5 MHz, respectively.

The MCPD method risks to falsely estimate the range if the signal was simply delayed by an adversary, potentially allowing access to unauthorized persons. This problem is due to the range ambiguity bound which is 150 m in the case of 1 MHz step size. An adversary can use this knowledge and delay the signal to introduce an additional delay, reducing the estimated distance. In order to prevent this and other problems, ToF is implemented in addition to MCPD to detect the rollover of the phase.

ToF method

In order to estimate the ToF, packets will be exchanged between the two nodes. A typical Bluetooth Low Energy packet, which consists of a preamble, an access address, protocol data units and a cyclic redundancy check, can be used. During the exchange of packets, the transmitting node measures the packet time of departure (ToD) and the receiving node the packet time of arrival (ToA). The access address can be used to estimate the ToD and ToA. Then, one of the nodes, typically the verifier, evaluates the ToF by using the timestamps at both nodes as shown in Figure 4.

Note that the timestamp measurements taken at the prover should be sent to the verifier. Also note that this process can be repeated using several frequencies as in the case of the MCPD method. This will help to have better ToF estimates and reduce the effect of multipath.

In order to achieve a good ToF estimation, errors, due to noise, sampling artifacts, multipath and others, need to be minimized. These errors can be reduced by oversampling the signal at the receiver, filtering or averaging over different measurements and using multiple phase offset measurements [11].

Distance bounding

The security of the system is improved by adding the distance bounding protocol to the MCPD and ToF methods.

In the case of MCPD, a random phase difference is used per frequency. This phase difference does not have to be a priori agreed between the two nodes since it will cancel out once the measurements are combined.

In the case of ToF, the Bluetooth Low Energy access address will contain a pseudorandom bit sequence that is only known by the verifier and the prover. This sequence is different on each transmission and on each frequency. The pseudorandom sequence is generated by taking the shared key established during the AKE stage as a seed, together with a counter that depends on the used frequency. Therefore, the sequence is only known to the verifier and the prover, and is different for each frequency. The sequence from the verifier to the prover transmission acts as a challenge bit sequence and the transmission from the prover to the verifier acts as a response bit sequence. Thus, the access address will be used for three purposes:

1. **to synchronize;**
2. **to estimate ToA and ToD;**
3. **to authenticate the packets or the measurements.**

After estimating the ToA of the received packets, the decoded access address bits will be checked bit by bit and the prover node will notify the verifier whether the received challenge bits are correct or not.

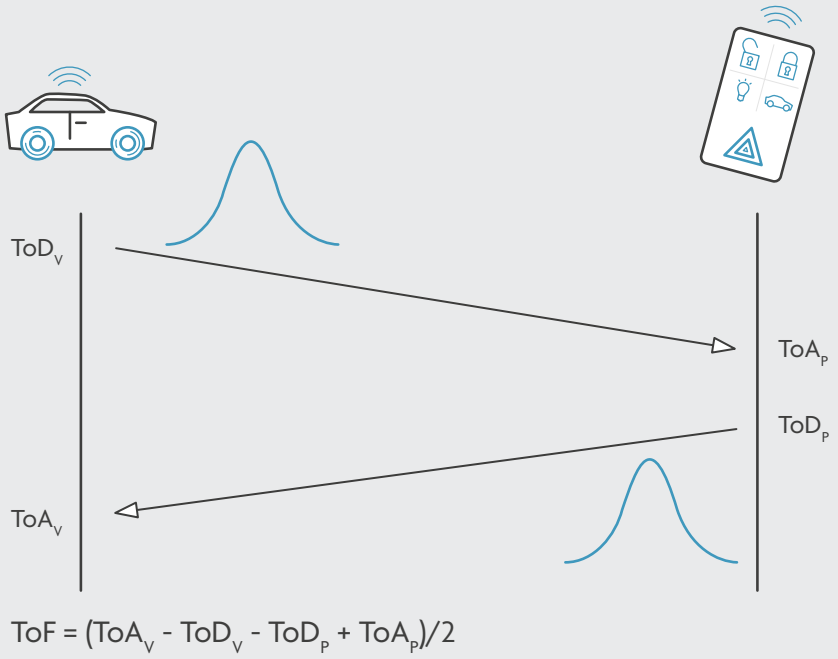


Figure 4 | Ranging based on ToF estimation

03 AUTHENTICATION AND AUTHORIZATION STAGE

During this stage, the prover sends its (amplitude, phase, and timestamp) measurements and the status of the received challenges (i.e., whether they are correct or not) in an encrypted packet to the verifier using the shared key generated in the AKE stage.

The verifier then evaluates the security and the distance based on the available measurements and data. For instance, the security level is high if both MCPD and ToF distance estimations are close. If not, the security level is low.

Security analysis: attacks & mitigations

The aim of the presented secure distance bounding solution is to prevent relay attacks. Thus, it is assumed that the verifier and the prover are trusted already, and that there is an intruder in the middle who wants to perform a relay attack so that the estimated distance is decreased.

The security of the accurate distance bounding protocol described in this white paper has been analyzed by an independent third-party expert in wireless security.

Table 1 lists potential attacks along with their implementation complexity.

Attacks/Protocols	Complexity	Phase/MCPD	ToF	SDB
Impersonation attack	Low	✗	✗	✓
Range extender attack	Low	✗	✓	✓
Phase manipulation attack	Medium to high	✗	✓	✓
Early detect, late commit	High	✓	✗	✓
Early detect, late commit + phase manipulation attack	Very high	✗	✗	✓

Table 1 | List of attacks on the defined protocols

Three different protocols – MCPD, ToF and SDB (DB + MCPD + ToF) – are listed and compared with respect to their immunity to the listed attacks. In this table, ✕ means that the protocol does not provide immunity against the attack and ✓ means it provides immunity.

These are the attacks and countermeasures:

- The **impersonation attack** is an attack where the adversary attempts to break the authentication by impersonating the legitimate devices. This attack can be prevented using good cryptography and a state-of-the-art authentication/signature protocol.

- The **range extender attack** is a simple attack, as shown in Figure 5, in which an adversary will modify neither the phase nor the frequency but only amplify the signal. The MCPD protocol cannot always prevent such an attack since an adversary can amplify the signal of the prover who is located beyond the ambiguity bound. However, ToF can prevent such attack since it is not based on signal strength and time does not roll over.

- The **phase manipulation attack** [12] can be any attack that manipulates the phase of the constant tone signal to reduce the estimated distance, such as:

  - a phase slope rollover attack – The adversary delays the tone signals with a fixed time delay so that the measured phase difference between the tone signals reaches its maximum value of 2π and rollover.

  - an on-the-fly phase manipulation attack – The adversary manipulates the phase of the tone signals in real time by mixing them with a special signal which results in an appropriate phase difference at the verifier/prover and a decrease of the estimated distance. In order to successfully manipulate the phase, the adversary must have a priori knowledge of the initial phase of the verifier/prover and the distance between the adversary and the nodes.

  - a tone generation attack – The adversary generates and then transmits his own strong tone signals to both the verifier and the prover. Just like in the previous attack, the adversary must have a priori knowledge of the initial phase of the verifier/prover and the distance between the adversary and the nodes in order to successfully decrease the estimated distance.

These attacks only affect the phase and not the time. In order to prevent these attacks, an independent random phase shift per frequency per node can be introduced to the tone signals before being transmitted. The adversary cannot guess the introduced phase-shift and thereby cannot generate a corresponding tone signal to reduce the distance. This will result in large fluctuations in the measured phase difference across the carrier frequencies. Moreover, since time is not affected by this attack, the ToF estimation will prevent such attacks and will add a security layer.

Figure 5 | Range extender attack -- The car receives an amplified signal.

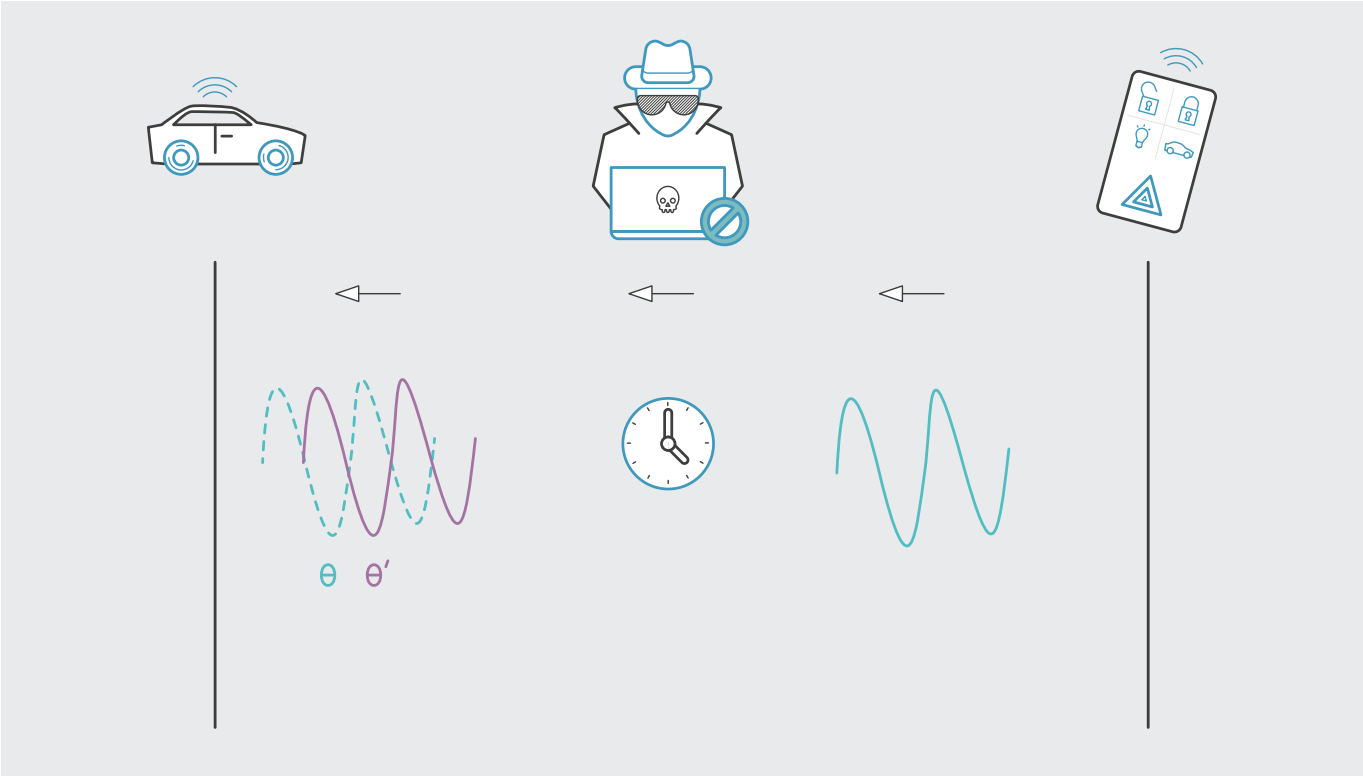


Figure 6 | Phase Manipulation Attack -- The car receives a signal with a modified phase.

- The **Early-Detect and Late-Commit (ED/LC) attack** typically targets the ToF estimation. The maximum distance that the adversary can decrease depends on the signal to noise ratio, the pulse shaping filter, the decoding method and other factors. Note that the distance obtained using the MCPD is not affected by an ED/LC [13]. This means it can offer protection against the ED/LC as long as the adversary cannot decrease the ToF estimation by more than the ambiguity bound. Thus, the maximum distance that the adversary can decrease using an ED/LC needs to be minimized. The ED/LC attack can be detected and prevented, for example, by increasing the product of bandwidth and symbol time of Gaussian pulse.
- The last one is a **hybrid attack** combining phase manipulation with ED/LC. In this attack, the adversary manipulates both the time and the phase. Using the prevention techniques presented above, this attack will be detected and mitigated.

Demonstration

The described SDB protocol has been implemented and demonstrated on an NXP KW36 radio platform as shown in Figure 7.

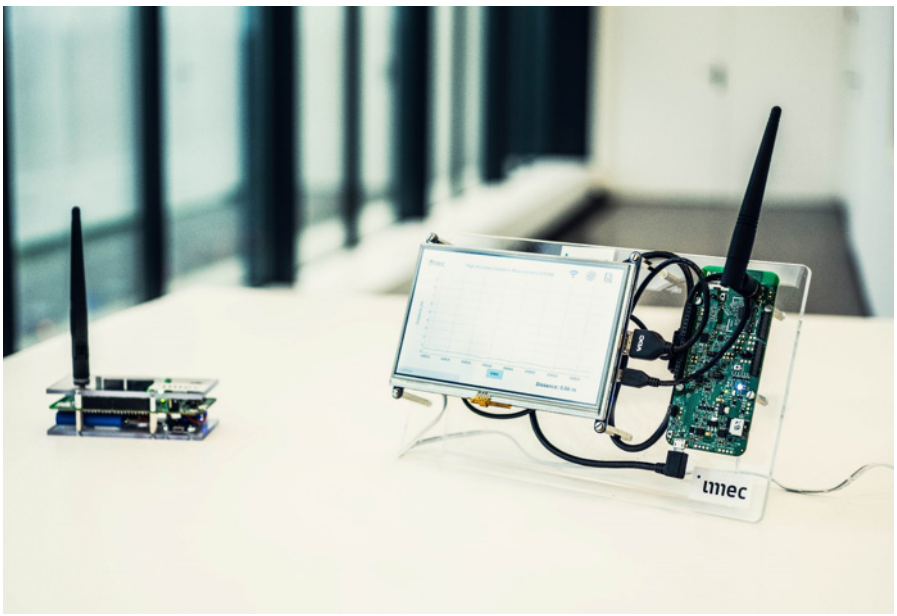


Figure 7 | imec SDB implementation on NXP KW36

The SDB protocol can be implemented on any other radio platform. The obtained precision in a wired setup is up to 2 cm using MCPD and up to 2.5 m using ToF.

In order to demonstrate the relay attack mitigation, we built a model in which the verifier and the prover are not within communication range and the adversaries between them are delaying the signals, as shown in Figure 8.

For this demonstration, the frequency step size is 4 MHz, thus there are 20 frequencies within the 2.4 GHz ISM band and the ambiguity bound is 37.5 m. The ToF estimation is averaged over the 20 frequencies.

Figure 8 | Relay attack model

Figure 9 and Figure 10 show the estimated distances using MCPD and ToF without a relay attack. Note that in these two figures the prover and the verifier are within communication range. In Figure 9, both MCPD and ToF based distance estimations are comparable, hence the security level is high. The prover is authenticated because it is close to the verifier. In Figure 10, both MCPD and ToF based distance estimations are comparable, hence the security level is high, but the prover is not authenticated since it is far from the verifier.

Figure 11 shows the estimated distances using MCPD and ToF with a relay attack. In this figure, the security level is low since the gap between the two distance estimations is large. In this scenario, the MCPD distance estimation is rolled over the ambiguity bound. Thanks to the ToF distance estimation, the attack will be detected, and the adversary will not be authenticated.

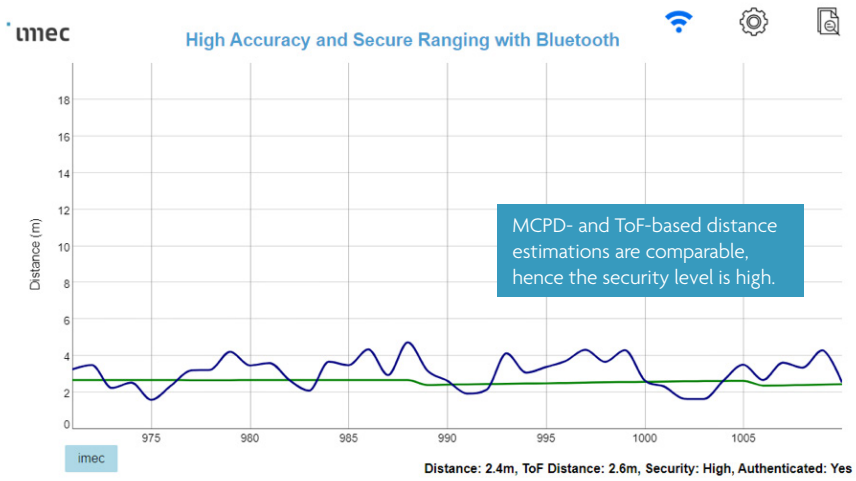


Figure 9 | Estimated MCPD (green) and ToF (blue) distances without a relay attack. Prover is close to Verifier.

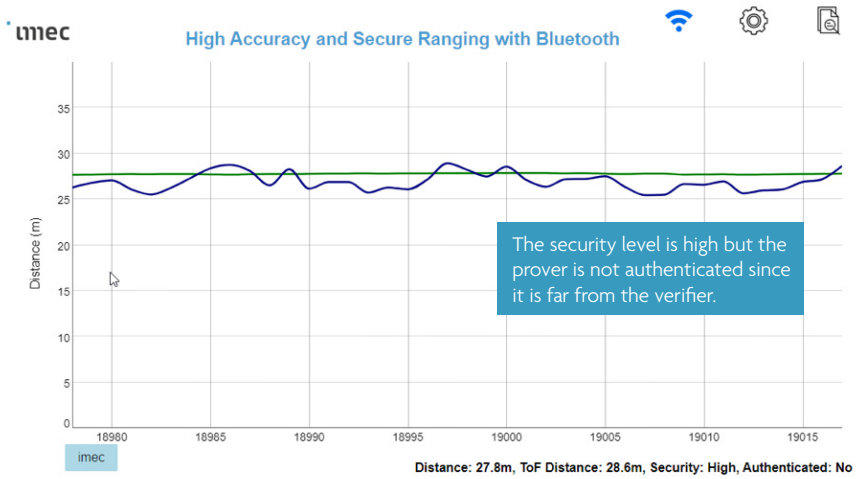


Figure 10 | Estimated MCPD (green) and ToF (blue) distances without a relay attack. Prover is far from Verifier.

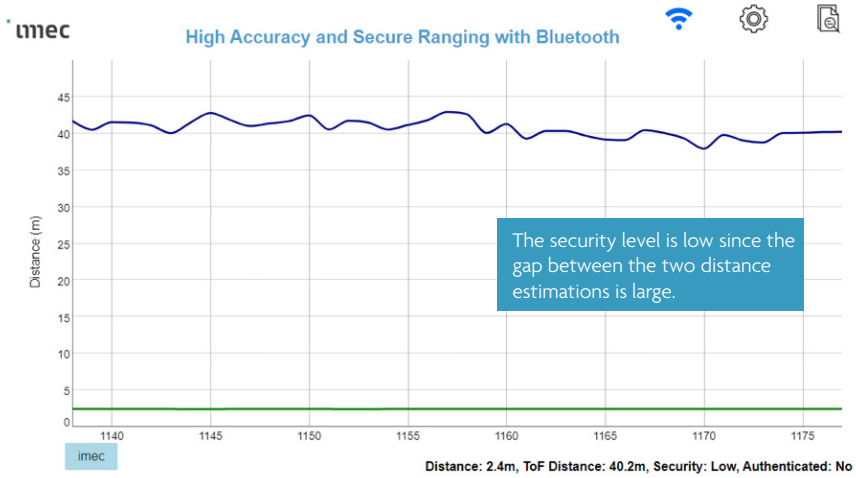
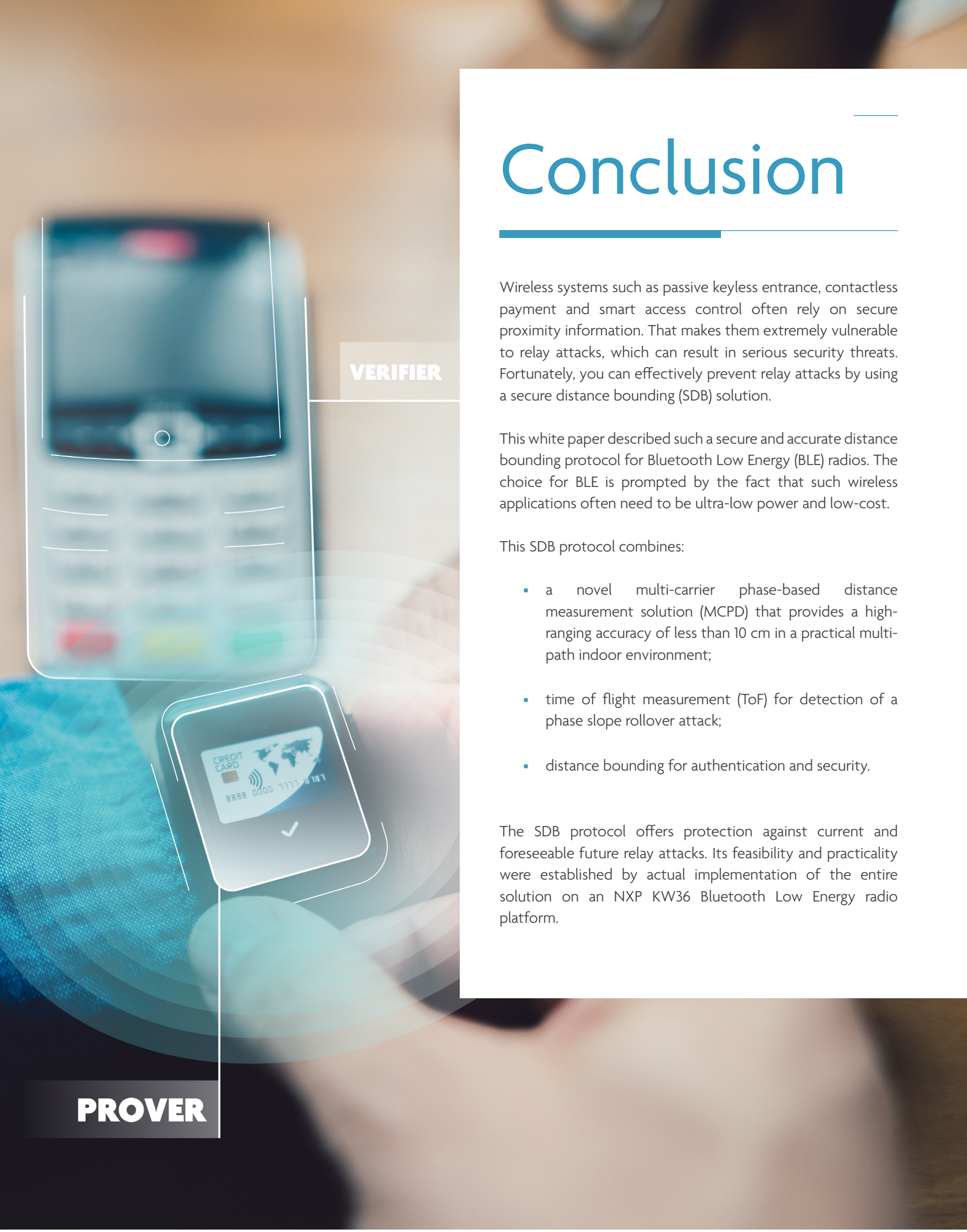


Figure 11 | Estimated MCPD (green) and ToF (blue) distances with a relay attack.



Conclusion

Wireless systems such as passive keyless entrance, contactless payment and smart access control often rely on secure proximity information. That makes them extremely vulnerable to relay attacks, which can result in serious security threats. Fortunately, you can effectively prevent relay attacks by using a secure distance bounding (SDB) solution.

This white paper described such a secure and accurate distance bounding protocol for Bluetooth Low Energy (BLE) radios. The choice for BLE is prompted by the fact that such wireless applications often need to be ultra-low power and low-cost.

This SDB protocol combines:

- a novel multi-carrier phase-based distance measurement solution (MCPD) that provides a high-ranging accuracy of less than 10 cm in a practical multi-path indoor environment;
- time of flight measurement (ToF) for detection of a phase slope rollover attack;
- distance bounding for authentication and security.

The SDB protocol offers protection against current and foreseeable future relay attacks. Its feasibility and practicality were established by actual implementation of the entire solution on an NXP KW36 Bluetooth Low Energy radio platform.

About COSIC, an imec research group at KU Leuven

The Computer Security and Industrial Cryptography (COSIC) research group was founded in 1979 and currently has 7 professors, 6 support staff members, 7 research experts/managers and over 60 researchers. The group is headed by Prof. Bart Preneel. COSIC is part of the Department of Electrical Engineering at the KU Leuven. During the last 15 years, COSIC obtained more than 1200 international reviewed publications in journals and conferences, 13 edited books and 10 patents, and has graduated over 60 PhD students. It offers a broad expertise in digital security. Based on this know-how, it develops innovative security solutions that take into account both privacy and usability. COSIC's research focuses on the design, evaluation and implementation of cryptographic algorithms and protocols, the development of security architectures for information and communication systems, the creation of security mechanisms for embedded systems and the design and analysis of privacy-preserving solutions. Technologies that are being developed include post-quantum cryptography, Fully Homomorphic Encryption, Multi-Party Computation (MPC) and blockchain. Application areas of COSIC's research include electronic payments and cryptocurrencies, mobile authentication, e-voting, biometrics, implantable medical devices, smart cars and smart cities. COSIC has been active in the research area of distance bounding protocols for more than a decade. COSIC is part of the Smart Applications and Innovation Services of imec, a high-tech research and innovation hub for nanoelectronics and digital technologies.

About imec

Imec is a world-leading research and innovation hub in nanoelectronics and digital technologies – unique because of the combination of its widely acclaimed leadership in microchip technology and profound software and ICT expertise. By leveraging a world-class infrastructure and local and global ecosystem of partners across a multitude of industries, imec creates groundbreaking innovation in application domains such as healthcare, smart cities and mobility, logistics and manufacturing, energy and education.

As a trusted partner for companies, start-ups and universities, imec bring together more than 5,000 brilliant minds from over 97 nationalities. Imec is headquartered in Leuven, Belgium and has distributed R&D groups at several Flemish universities, in the Netherlands, Taiwan, USA, and offices in China, India and Japan. In 2021, imec's revenue (P&L) totaled 730 million euro.

Imec's wireless IoT R&D group addresses a wide range of wireless circuit and system innovations for high-capacity and ultra-low power communications, wireless ranging and localization, and wireless sensing (radar). It targets key application areas from potential user domains such as medicine and lifestyle, industrial process monitoring & control, agriculture, mobile gaming, automotive, home and industrial buildings, transportation/logistics/asset management.

Imec actively participates in high-impact standardization bodies such as Bluetooth Special Interest Group (SIG), IEEE and others.

Find out more at

www.imec-int.com/en/5G-and-wireless-iot-communication

www.imec-int.com/en/79GHz-140GHz-radar-systems

www.imec-int.com/en/expertise/sensors-for-iot/secure-system-solutions

References

[1] "Imec Boosts Bluetooth Battery Life", IEEE Spectrum, Feb 2018, https://spectrum.ieee.org/tech-talk/computing/hardware/imec-boosts-bluetooth-battery-life, accessed 2019-10-25.

[2] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," Proc. Network and Distributed System Security Symp. (NDSS 11), 2011;

[3] https://bit.ly/2LP343m, accessed 2019-10-25.

[4] https://www.bbc.com/news/business-49273028, accessed 2019-10-25.

[5] A. F. Molisch, V. Poor, Z. Sahinoglu, S. Gezici, Z. Tian, G. B. Giannakis, H. Kobayashi, A. F. Molisch, H. V. Poor, and Z. Sahinoglu. Localization via Ultra-wideband Radios. In IEEE Signal Processing Magazine, 2005.

[6] Mautz, R. Indoor Positioning Technologies. Ph.D. Thesis, ETH Zürich, Zürich, Switzerland, 2012

[7] Zand, Pouria & Romme, Jac & Govers, Jochem & Pasveer, W.F. & Dolmans, Guido. (2019). A high-accuracy phase-based ranging solution with Bluetooth Low Energy (BLE).

[8] Rapinski, J.; Smieja, M. ZigBee Ranging using Phase Shift Measurements. J. Navig. 2015, 68, 665–677.

[9] S. Brands and D. Chaum, "Distance-bounding protocols (extended abstract)," in EUROCRYPT, 1993, pp. 344–359.

[10] H. Krawczyk, "SIGMA: The 'SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and Its Use in the IKE-Protocols," in CRYPTO 2003, ser. LNCS, 2003, pp. 400–425.

[11] K. I. Ahmad and G. Heidari-Bateni, "Improving Two-Way Ranging Precision with Phase-offset Measurements," EEE Globecom 2006, San Francisco, CA, pp. 1-6, 2006.

[12] Olafsdóttir, Hildur, Aanjhan Ranganathan, and Srdjan Capkun. "On the security of carrier phase-based ranging." – CHES 2017

[13] HANCKE, Gerhard P.; KUHN, Markus G. "Attacks on time-of-flight distance bounding channels". In: Proceedings of the first ACM conference on Wireless network security. ACM, 2008. p. 194-202.