Physical Layer & Telecommunications Security Knowledge Area

Version 1.0.1

Srdjan Čapkun | ETH Zurich

EDITOR
George Danezis | University College London
Awais Rashid | University of Bristol

REVIEWERS
Robert Piechocki | University of Bristol
Kasper Rasmussen | University of Oxford

COPYRIGHT

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at **contact@cybok.org** to let the project know how they are using CyBOK.

Version 1.0.1 is a stable public release of the Physical Layer & Telecommunications Security Knowledge Area.

CHANGELOG

Version date	Version number	Changes made
July 2021	1.0.1	Updated copyright statement; amended “issue” to “version”; amended typos
October 2019	1.0	

INTRODUCTION

This Knowledge Area is a review of the most relevant topics in wireless physical layer security. The physical phenomenon utilized by the techniques presented in this Knowledge Area is the radiation of electromagnetic waves. The frequencies considered hereinafter consist of the entire spectrum that ranges from a few Hertz to frequencies beyond those of visible light (optical spectrum). This Knowledge Area covers concepts and techniques that exploit the way these signals propagate through the air and other transmission media. It is organised into sections that describe security mechanisms for wireless communication methods as well as some implications of unintended radio frequency emanations.

Since most frequencies used for wireless communication reside in the radio frequency spectrum and follow the well-understood laws of radio propagation theory, the majority of this Knowledge Area is dedicated to security concepts based on physical aspects of radio frequency transmission. The chapter therefore starts with an explanation of the fundamental concepts and main techniques that were developed to make use of the wireless communication layer for confidentiality, integrity, access control and covert communication. These techniques mainly use properties of physical layer modulations and signal propagation to enhance the security of systems.

After having presented schemes to secure the wireless channel, the Knowledge Area continues with a review of security issues related to the wireless physical layer, focusing on those aspects that make wireless communication systems different from wired systems. Most notably, signal jamming, signal annihilation and jamming resilience. The section on jamming is followed by a review of techniques capable of performing physical device identification (i.e., device fingerprinting) by extracting unique characteristics from the device's (analogue) circuitry.

Following this, the chapter continues to present approaches for performing secure distance measurements and secure positioning based on electromagnetic waves. Protocols for distance measurements and positioning are designed in order to thwart threats on the physical layer as well as the logical layer. Those attack vectors are covered in detail, together with defense strategies and the requirements for secure position verification.

Then, the Knowledge Area covers unintentional wireless emanations from devices such as from computer displays and summarises wireless side-channel attacks studied in literature. This is followed by a review on spoofing of analogue sensors. Unintentional emissions are in their nature different from wireless communication systems, especially because these interactions are not structured. They are not designed to carry information, however, they also make use of—or can be affected by—electromagnetic waves.

Finally, after having treated the fundamental concepts of wireless physical security, this Knowledge Area presents a selection of existing communication technologies and discusses their security mechanisms. It explains design choices and highlights potential shortcomings while referring to the principles described in the earlier sections. Included are examples from near-field communication and wireless communication in the aviation industry, followed by the security considerations of cellular networks. Security of global navigation systems and of terrestrial positioning systems is covered last since the security goals of such systems are different from communication systems and are mainly related to position spoofing resilience.

CONTENT

1 PHYSICAL LAYER SCHEMES FOR CONFIDENTIALITY, INTEGRITY AND ACCESS CONTROL

[1, 2, 3, 4, 5, 6]

Securing wireless networks is challenging due to the shared broadcast medium which makes it easy for remote adversaries to eavesdrop, modify and block the communication between devices. However, wireless communication also offers some unique opportunities. Radio signals are affected by reflection, diffraction, and scattering, all of which contribute to a complex multi-path behaviour of communicated signals. The channel response, as measured at the receiver, can therefore be modelled as having frequency and position dependent random components. In addition, within the short time span and in the absence of interference, communicating parties will measure highly correlated channel responses. These responses can therefore be used as shared randomness, unavailable to the adversary, and form a basis of secure communication.

It should be noted that modern-day cryptography provides many different protocols to assure the confidentiality, integrity and authenticity of data transmitted using radio signals. If the communicating parties are associated with each other or share a mutual secret, cryptographic protocols can effectively establish secure communication by making use of cryptographic keying material. However, if mere information exchange is not the only goal of a wireless system (e.g., in a positioning system), or if no pre-shared secrets are available, cryptographic protocols operating at higher layers of the protocol stack are not sufficient and physical-layer constructs can be viable solutions. The main physical layer schemes are presented in the following sections.

1.1 Key Establishment based on Channel Reciprocity

The physical-layer randomness of a wireless channel can be used to derive a shared secret. One of the main security assumptions of physical-layer key establishment schemes is that the attacker is located at least half a wavelength away from the communicating parties. According to wireless communication theory, it can be assumed that the attacker's channel measurements will be de-correlated from those computed by the communicating parties if they are at least half a wavelength apart. The attacker will therefore likely not have access to the measured secret randomness. If the attacker injects signals during the key generation, the signal that it transmits will, due to channel distortions, be measured differently at communicating parties, resulting in key disagreement.

Physical layer key establishment schemes operate as follows. The communicating parties (Alice and Bob) first exchange pre-agreed, non-secret, data packets. Each party then measures the channel response over the received packets. The key agreement is then typically executed in three phases.

Quantisation Phase: Alice and Bob create a time series of channel properties that are measured over the received packets. Example properties include RSSI and the CIR. Any property that is believed to be non-observable by the attacker can be used. The measured time series are then quantised by both parties independently. This quantisation is typically based on fixed or

dynamic thresholds.

Information reconciliation phase: Since the quantisation phase is likely to result in disagreeing sequences at Alice and Bob, they need to reconcile their sequences to correct for any errors. This is typically done leveraging error correcting codes and privacy amplification techniques. Most schemes use simple level-crossing algorithms for quantisation and do not use coding techniques. However, if the key derivation uses methods based on channel states whose distributions are not necessarily symmetric, more sophisticated quantisation methods, such as approximating the channel fading phenomena as a Gaussian source, or (multi-level) coding is needed [2].

Key Verification Phase: In this last phase, communicating parties confirm that they established a shared secret key. If this step fails, the parties need to restart key establishment.

Most of the research in physical-layer techniques has been concerned with the choice of channel properties and of the quantisation technique. Even if physical-layer key establishment techniques seem attractive, many of them have been shown to be vulnerable to active, physically distributed and multi-antenna adversaries. However, in a number of scenarios where the devices are mobile, and where the attacker is restricted, they can be a valuable replacement or enhancement to traditional public-key key establishment techniques.

1.2 MIMO-supported Approaches: Orthogonal Blinding, Zero-Forcing

Initially, physical-layer key establishment techniques were proposed in the context of single-antenna devices. However, with the emergence of MIMO devices and beam-forming, researchers have proposed to leverage these new capabilities to further secure communication. Two basic techniques that were proposed in this context are orthogonal blinding and zero forcing. Both of these techniques aim to enable the transmitter to wirelessly send confidential data to the intended receiver, while preventing the co-located attacker from receiving this data. Although this might seem infeasible, since as well as the intended receiver, the attacker can receive all transmitted packets. However, MIMO systems allow transmitters to 'steer' the signal towards the intended receiver. For beam-forming to be effective, the transmitter needs to know some channel information for the channels from its antennas to the antennas of the receiver. As described in [5], these channels are considered to be secret from the attacker. In Zero-Forcing, the transmitter knows the channels to the intended receiver as well as to the attacker. This allows the transmitter to encode the data such that it can be measured at the receiver, whereas the attacker measures nothing related to the data. In many scenarios, assuming the knowledge of the channel to the attackers is unrealistic. In Orthogonal Blinding, the transmitter doesn't know the channel to the attacker, but knows the channels to the receiver. The transmitter then encodes the data in the way that the receiver can decode the data, whereas the attacker will receive data mixed with random noise. The attacker therefore cannot decode the data. In order to communicate securely, the transmitter and the receiver do not need to share any secrets. Instead, the transmitter only needs to know (or measure) the channels to the intended receivers. Like physical-layer key establishment techniques, these techniques have been show to be vulnerable to multi-antenna and physically distributed attackers. They were further shown to be vulnerable to known-plaintext attacks.

1.3 Secrecy Capacity

Secrecy capacity is an information-theoretical concept that attempts to determine the maximal rate at which a wireless channel can be used to transmit confidential information without relying on higher-layer encryption, even if there is an eavesdropper present. A famous result by Shannon [7] says that, for an adversary with unbounded computing power, unconditionally secure transmission can only be achieved if a one-time-pad cipher is used to encrypt the transmitted information. However, Wyner later showed that if the attacker's channel slightly degrades the information, that is, the channel is noisy, the secrecy capacity can indeed be positive under certain conditions [8]. This means it is possible to convey a secret message without leaking any information to an eavesdropper. Csiszár and Korner extended Wyner's result by showing that the secrecy capacity is non-zero, unless the adversary's channel (wiretap channel) is less noisy than the channel that carries the message from the legitimate transmitter to the receiver [9]. These theoretical results have been refined for concrete channel models by assuming a certain type of noise (e.g., Gaussian) and channel layout (e.g., SIMO and MIMO). Researchers have managed to derive explicit mathematical expressions and bounds even when taking into account complex phenomena such as fading which is present in wireless channels [10].

A practical implementation of the concept of secrecy capacity can mainly be achieved using the two methods described above. Either the communicating parties establish a secret key by extracting features from the wireless channel (see 1.1) or they communicate with each other using intelligent coding and transmission strategies possibly relying on multiple antennas (see 1.2). Therefore, the study of secrecy capacity can be understood as the information-theoretical framework for key establishment and MIMO-supported security mechanisms in the context of wireless communication.

1.4 Friendly Jamming

Similar to Orthogonal Blinding, Friendly Jamming schemes use signal interference generated by collaborating devices to either prevent an attacker from communicating with the protected device, or to prevent the attacker from eavesdropping on messages sent by protected devices. Friendly Jamming can therefore be used for both confidentiality and access control. Unlike Orthogonal Blinding, Friendly Jamming doesn't leverage the knowledge of the channel to the receiver. If a collaborating device (i.e., the friendly jammer) wants to prevent unauthorised communication with the protected device it will jam the receiver of the protected device. If it wants to prevent eavesdropping, it will transmit jamming signals in the vicinity of the protected device. Preventing communication with a protected device requires no special assumptions on the location of the collaborating devices. However, protecting against eavesdropping requires that the eavesdropper is unable to separate the signals from the protected device from those originating at the collaborating device. For this to hold, the channel from the protected device to the attacker should not be correlated to the channel from the collaborating device to the attacker. To ensure this, the protected device and the collaborating device need to be typically placed less than half a carrier wavelength apart. This assumption is based on the fact that, in theory, an attacker with multiple antennas who tries to tell apart the jamming signal from the target signal requires the two transmitters to be separated by more than half a wavelength. However, signal deterioration is gradual and it has been shown that under some conditions, a multi-antenna attacker will be able to separate these signals and recover the transmitted messages.

Friendly jamming was originally proposed for the protection of those medical implants (e.g., already implanted pacemakers) that have no abilities to perform cryptographic operations. The main idea was that the collaborating device (i.e. 'the shield') would be placed around the user's neck, close to the pacemaker. This device would then simultaneously receive and jam all communication from the implant. The shield would then be able to forward the received messages to any other authorised device using standard cryptographic techniques.

1.5 Using Physical Layer to Protect Data Integrity

Research into the use of physical layer for security is not only limited to the protection of data confidentiality. Physical layer can also be leveraged to protect data integrity. This is illustrated by the following scenario. Assuming that two entities (Alice and Bob) share a common radio communication channel, but do not share any secrets or authentication material (e.g., shared keys or authenticated public keys), how can the messages exchanged between these entities be authenticated and how can their integrity be preserved in the presence of an attacker? Here, by message integrity, we mean that the message must be protected against any malicious modification, and by message authentication we mean that it should be clear who is the sender of the message.

One basic technique that was proposed in this context is *integrity codes*, a modulation scheme that provides a method of ensuring the integrity (and a basis for authentication) of a message transmitted over a public channel. Integrity codes rely on the observation that, in a mobile setting and in a multi-path rich environment, it is hard for the attacker to annihilate randomly chosen signals.

Integrity codes assume a synchronised transmission between the transmitter and a receiver, as well as the receiver being aware that it is in the range of the transmitter. To transmit a message, the sender encodes the binary message using a unidirectional code (e.g., a Manchester code), resulting in a known ration of 1s and 0s within an encoded message (for Manchester code, the number of 1s and 0s will be equal). This encoded message is then transmitted using on-off keying, such that each 0 is transmitted as an absence of signal and each 1 as a random signal. To decode the message and check its integrity, the receiver simply measures the energy of the signal. If the energy in a time slot is above a fixed threshold, the bit is interpreted as a 1 and if it is below a threshold, it is interpreted as a 0. If the ratio of bits 1 and 0 corresponds to the encoding scheme, the integrity of the message is validated. Integrity codes assume that the receiver knows when the transmitter is transmitting. This means that their communication needs to be scheduled or the transmitter needs to always be transmitting.

1.6 Low probability of intercept and Covert Communication

LPI signals are such signals that are difficult to detect for the unintended recipient. The simplest form of LPI is communication at a reduced power and with high directionality. Since such communication limits the range and the direction of communication, more sophisticated techniques were developed: Frequency Hopping, Direct Sequence Spread Spectrum and Chirping. In Frequency Hopping the sender and the receiver hop between different frequency channels thus trying to avoid detection. In Direct Sequence Spread Spectrum the information signal is modulated with a high rate (and thus high bandwidth) digital signal, thus spreading across a wide frequency band. Finally, Chirps are high speed frequency sweeps that carry information. The hopping sequence or chirp sequence constitute a secret shared between

receiver and transmitter. This allows the legitimate receiver to recombine the signal while an eavesdropper is unable to do so.

Covert communication is parasitic and leverages legitimate and expected transmissions to enable unobservable communication. Typically, such communication hides within the expected and tolerated deviations of the signal from its nominal form. One prominent example is embedding of communicated bits within the modulation errors.

2 JAMMING AND JAMMING-RESILIENT COMMUNICATION

[11, 12]

Communication jamming is an interference that prevents the intended receiver(s) from successfully recognising and decoding the transmitted message. It happens when the jammer injects a signal which, when combined with the legitimate transmission, prevents the receiver from extracting the information contained in the legitimate transmission. Jamming can be surgical and affect only the message preamble thus preventing decoding, or can be comprehensive and aim to affect every symbol in the transmission.

Depending on their behaviour, jammers can be classified as *constant* or *reactive*. Constant jammers transmit permanently, irrespective of the legitimate transmission. Reactive jammers are most agile as they sense for transmission and then jam. This allows them to save energy as well as to stay undetected. Jammer strength is typically expressed in terms of their output power and their effectiveness as the jamming-to-signal ratio at the receiver. Beyond a certain jamming-to-signal ratio, the receiver will not be able to decode the information contained in the signal. This ratio is specific to particular receivers and communication schemes. The main parameters that influence the success of jamming are transmission power of the jammer and benign transmitter, their antenna gains, communication frequency, and their respective distances to the benign receiver. These parameters will determine the jamming-to-signal ratio.

Countermeasures against jamming involve concealing from the adversary which frequencies are used for communication at which time. This uncertainty forces the adversary to jam a wider portion of the spectrum and therefore weakens their impact on the legitimate transmission, effectively reducing the jamming-to-signal ratio. Most common techniques include Chirp, FHSS and DSSS. Typically, these techniques rely on pre-shared secret keys, in which case we call the communication 'coordinated'. Recently, to enable jamming resilience in scenarios in which keys cannot be pre-shared (e.g., broadcast), uncoordinated FHSS and DSSS schemes were also proposed.

2.1 Coordinated Spread Spectrum Techniques

Coordinated Spread Spectrum techniques are prevalent jamming countermeasures in a number of civilian and military applications. They are used not only to increase resilience to jamming, but also to cope with interference from neighboring devices. Spreading is used in practically all wireless communication technologies, in e.g.,802.11, cellular, Bluetooth, global satellite positioning systems.

Spread spectrum techniques are typically effective against jammers that cannot cover the entire communication spectrum at all times. These techniques make a sender spread a signal over the entire available band of radio frequencies, which might require a considerable

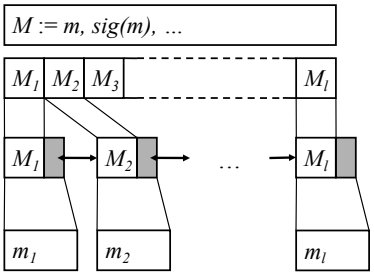

Figure 1: In UFH, the fragment linking protect against message insertion attack.

amount of energy. The attacker's ability to impact the transmission is limited by the achieved processing gain of the spread-spectrum communication. This gain is the ratio by which interference can be suppressed relative to the original signal, and is computed as a ratio of the spread signal radio frequency bandwidth to the un-spread information (baseband) bandwidth.

Spread-spectrum techniques use randomly generated sequences to spread information signals over a wider band of frequencies. The resulting signal is transmitted and then de-spread at the receivers by correlating it with the spreading sequence. For this to work, it is essential that the transmitter and receiver share the same secret spreading sequence. In FHSS, this sequence is the set of central frequencies and the order in which the transmitter and receiver switch between them in synchrony. In DSSS, the data signal is modulated with the spreading sequence; this process effectively mixes the carrier signal with the spreading sequence, thus increasing the frequency bandwidth of the transmitted signal. This process allows for both narrow band and wide band jamming to be suppressed at the receiver. Unless the jammer can guess the spreading code, its jamming signal will be spread at the receiver, whereas the legitimate transmission will be de-spread, allowing for its detection. The secrecy of the spreading codes is therefore crucial for the jamming resilience of spread spectrum systems. This is why a number of civilian systems that use spreading with public spreading codes, such as the GPS and 802.11b, remain vulnerable to jamming.

2.2 Uncoordinated Spread Spectrum Techniques

In broadcast applications and in applications in which communication cannot be anticipated as scheduled, there is still a need to protect such communication from jamming.

To address such scenarios, uncoordinated spread spectrum techniques were proposed: UFH and UDSSS. These techniques enable anti-jamming broadcast communication without pre-shared secrets. uncoordinated frequency hopping relies on the fact that even if the sender hops in a manner that is not coordinated with the receiver, the throughput of this channel will be non-zero. In fact, if the receiver is broadband, it can recover all the messages transmitted by the sender. UFH however, introduces new challenges. Given that the sender and the receiver are not synchronised, and short message fragments transmitted within each hop are not authenticated, the attacker can inject fragments that make the reassembly of the packets infeasible. To prevent this, UFH includes fragment linking schemes that make this reassembly possible even under poisoning.

UDSSS follows the principle of DSSS in terms of spreading the data using spreading sequences. However, in contrast to anti-jamming DSSS where the spreading sequence is secret and shared exclusively by the communication partners, in UDSSS, a public set of spreading sequences is used by the sender and the receivers. To transmit a message, the sender repeatedly selects a

fresh, randomly selected spreading sequence from the public set and spreads the message with this sequence. Hence, UDSSS neither requires message fragmentation at the sender nor message reassembly at the receivers. The receivers record the signal on the channel and despread the message by applying sequences from the public set, using a trial-and-error approach. The receivers are not synchronised to the beginning of the sender's message and thus record for (at least) twice the message transmission time. After the sampling, the receiver tries to decode the data in the buffer by using code sequences from the set and by applying a sliding-window protocol.

2.3 Signal Annihilation and Overshadowing

Unlike jamming where the primary goal of the attacker is to prevent information from being decoded at the receiver, signal annihilation suppresses the signal at the receiver by introducing destructive interference. The attacker's goal is to insert a signal which cancels out the legitimate transmitter's signal at the antenna of the receiver. This typically means that the attacker will generate a signal identical to the legitimate transmission only with a different polarity. Jamming attacks typically increase the energy on the channel and thus are more easily detected than signal annihilation which reduces the energy typically below the threshold of signal detection.

The goal of overshadowing is similar to jamming and signal annihilation in the sense that the attacker aims to prevent the receiver from decoding a legitimate signal. However, instead of interfering with the signal by adding excessive noise to the channel or cancelling out the signal (i.e., signal annihilation), the attacker emits their own signal at the same time and overshadows the legitimate signal. As a result, the receiver only registers the adversarial signal which is often orders of magnitude higher in amplitude than the legitimate signal. Practical overshadowing attacks were shown to be effective against QPSK modulation [13] and more recently against cellular LTE systems [14].

Malicious signal overshadowing can not only deceive the receiver into decoding different data than intended, it can also be used to alter any physical properties the receiver may extract during signal reception, such as angle of arrival or time of arrival. Overshadowing attacks have been shown to be particularly effective against systems that rely on physical layer properties including positioning and ranging systems.

3 PHYSICAL-LAYER IDENTIFICATION

[15]

Physical-Layer Identification techniques enable the identification of wireless devices by unique characteristics of their analogue (radio) circuitry; this type of identification is also referred to as Radio Fingerprinting. More precisely, physical-layer device identification is the process of fingerprinting the analogue circuitry of a device by analysing the device's communication at the physical layer for the purpose of identifying a device or a class of devices. This type of identification is possible due to hardware imperfections in the analogue circuitry introduced at the manufacturing process. These imperfections are remotely measurable as they appear in the transmitted signals. While more precise manufacturing and quality control could minimise such artefacts, it is often impractical due to significantly higher production costs.

Physical-layer device identification systems aim at identifying (or verifying the identity of) devices or their affiliation classes, such as their manufacturer. Such systems can be viewed as pattern recognition systems typically composed of: *an acquisition setup* to acquire signals from devices under identification, also referred to as identification signals, a *feature extraction module* to obtain identification-relevant information from the acquired signals, also referred to as fingerprints, and a *fingerprint matcher* for comparing fingerprints and notifying the application system requesting the identification of the comparison results. Typically, there are two modules in an identification system: one for enrollment and one for identification. During enrollment, signals are captured either from each device or each (set of) class-representative device(s) considered by the application system. Fingerprints obtained from the feature extraction module are then stored in a database (each fingerprint may be linked with some form of unique ID representing the associated device or class). During identification, fingerprints obtained from the devices under identification are compared with reference fingerprints stored during enrollment. The task of the identification module can be twofold: either recognise (identify) a device or its affiliation class from among many enrolled devices or classes (1:N comparisons), or verify that a device identity or class matches a claimed identity or class (1:1 comparison).

The identification module uses statistical methods to perform the matching of the fingerprints. These methods are classifiers trained with Machine Learning techniques during the enrollment phase. If the module has to verify a 1:1 comparison, the classifier is referred to as binary. It tries to verify a newly acquired signal against a stored reference pattern established during enrollment. If the classifier performs a 1:N comparison, on the other hand, it attempts to find the reference pattern in a data base which best matches with the acquired signal. Often, these classifiers are designed to return a list of candidates ranked according to a similarity metric or likelihood that denotes the confidence for a match.

3.1 Device under Identification

Physical-layer device identification is based on fingerprinting the analogue circuitry of devices by observing their radio communication. Consequently, any device that uses radio communication may be subject to physical-layer identification. So far, it has been shown that a number of devices (or classes of devices) can be identified using physical-layer identification. These include analogue VHF, Bluetooth, WiFi, RFID and other radio transmitters.

Although what enables a device or a class of devices to be uniquely identified among other devices or classes of devices is known to be due to imperfections introduced at the manufacturing phase of the analogue circuitry, the actual device's components causing these have not always been clearly identified in all systems. For example, VHF identification systems are based on the uniqueness of transmitters' frequency synthesisers (local oscillators), while in RFID systems some studies only suggested that the proposed identification system may rely on imperfections caused by the RFID device's antennas and charge pumps. Identifying the exact components may become more difficult when considering relatively-complex devices. In these cases, it is common to identify in the whole analogue circuitry, or in a specific sub-circuit, the cause of imperfections. For example, IEEE 802.11 transceivers were identified considering modulation-related features; the cause of hardware artefacts can be then located in the modulator subcircuit of the transceivers. Knowing the components that make devices uniquely identifiable may have relevant implications for both attacks and applications, which makes the investigation of such components an important open problem and research direction.

3.2 Identification Signals

Considering devices communicating through radio signals, that is, sending data according to some defined specification and protocol, identification at the physical layer aims at extracting unique characteristics from the transmitted radio signals and to use those characteristics to distinguish among different devices or classes of devices. We define identification signals as the signals that are collected for the purpose of identification. Signal characteristics are mainly based on observing and extracting information from the properties of the transmitted signals, like amplitude, frequency, or phase over a certain period of time. These time-windows can cover different parts of the transmitted signals. Mainly, we distinguish between data and non-data related parts. The data parts of signals directly relate to data (e.g., preamble, midamble, payload) transmission, which leads to considered data-related properties such as modulation errors, preamble (midamble) amplitude, frequency and phase, spectral transformations. Non-data-related parts of signals are not associated with data transmission. Examples include the turn-on transients, near-transient regions, RF burst signals. These have been used to identify active wireless transceivers (IEEE 802.11, 802.15.4) and passive transponders (ISO 14443 HF RFID).

The characteristics extracted from identification signals are called features. Those can be predefined or inferred. Predefined features relate to well-understood signal characteristics. Those can be classified as in-specification and out-specification. Specifications are used for quality control and describe error tolerances. Examples of in-specification characteristics include modulation errors such as frequency offset, I/Q origin offset, magnitude and phase errors, as well as time-related parameters such as the duration of the response. Examples of out-specification characteristics include clock skew and the duration of the turn-on transient.

Differently from predefined features, where the considered characteristics are known in advance prior to recording of the signals, we say that features are inferred when they are extracted from signals, for example, by means of some spectral transformations such as Fast Fourier Transform (FFT) or Discrete Wavelet Transform (DWT), without a-priori knowledge of a specific signal characteristic. For instance, wavelet transformations have been applied on signal turn-on transients and different data-related signal regions. The Fourier transformation has also been used to extract features from the turn-on transient and other technology-specific device responses. Both predefined and inferred features can be subject to further statistical analysis in order to improve their quality and distinguishing power.

3.3 Device Fingerprints

Fingerprints are sets of features (or combinations of features, that are used to identify devices. The properties that fingerprints need to present in order to achieve practical implementations are (similar to those of biometrics):

1. Universality. Every device (in the considered device-space) should have the considered features.
2. Uniqueness. No two devices should have the same fingerprints.
3. Permanence. The obtained fingerprints should be invariant over time.
4. Collectability. It should be possible to capture the identification signals with existing (available) equipments.

When considering physical-layer identification of wireless devices, we further consider:

5. Robustness. Fingerprints should not be subject, or at least, they should be evaluated with respect to external environmental aspects that directly influence the collected signal like radio interference due to other radio signals, surrounding materials, signal reflections, absorption, etc., as well as positioning aspects like the distance and orientation between the devices under identification and the identification system. Furthermore, fingerprints should be robust to device-related aspects like temperature, voltage level, and power level. Many types of robustness can be acceptable for a practical identification system. Generally, obtaining robust features helps in building more reliable identification systems.
6. Data-Dependency. Fingerprints can be obtained from features extracted from a specific bit pattern (data-related part of the identification signal) transmitted by a device under identification (e.g., the claimed ID sent in a packet frame). This dependency has particularly interesting implications if the fingerprints can be associated with both devices and data transmitted by those devices. This might strengthen authentication and help prevent replay attacks.

3.4 Attacks on Physical Layer Identification

The large majority of research works have focused on exploring feature extraction and matching techniques for physical-layer device identification. Only recently the security of these techniques started being addressed. Different studies showed that their identification system may be vulnerable to hill-climbing attacks if the set of signals used for building the device fingerprint is not carefully chosen. This attack consists of repeatedly sending signals to the device identification system with modifications that gradually improve the similarity score between these signals and a target genuine signal. They also demonstrated that transient-based approaches could easily be disabled by jamming the transient part of the signal while still enabling reliable communication. Furthermore, impersonation attacks on modulation-based identification techniques were developed and showed that low-cost software-defined radios as well as high end signal generators could be used to reproduce modulation features and impersonate a target device with a success rate of 50-75%. Modulation-based techniques are vulnerable to impersonation with high accuracy, while transient-based techniques are likely to be compromised only from the location of the target device. The authors pointed out that this is mostly due to presence of wireless channel effects in the considered device fingerprints; therefore, the channel needed to be taken into consideration for successful impersonation.

Generally, these attacks can be divided into two groups: *signal re(P)lay* and *feature replay attacks*. In a signal replay attack, the attacker's goal is to observe analogue identification signals of a target device, capture them in a digital form (digital sampling), and then transmit (replay) these signals towards the identification system by some appropriate means. The attacker does not modify the captured identification signals, that is, the analogue signal and the data payload are preserved. This attack is similar to message replay in the Dolev-Yao model in which an attacker can observe and manipulate information currently in the air at will. Unlike in signal replay attacks, where the goal of the attack is to reproduce the captured identification signals in their entirety, feature replay attack creates, modifies or composes identification signals that reproduce only the features considered by the identification system. The analogue representation of the forged signals may be different, but the features should be the same (or at the least very similar).

4 DISTANCE BOUNDING AND SECURE POSITIONING

[16, 17, 18, 19, 20, 21, 22, 23]

Secure distance measurement (i.e., distance bounding) protocols were proposed to address the issue of the verification of proximity between (wireless) devices. Their use is broad and ranges from the prevention of relay attacks to enabling secure positioning.

Securing distance measurement requires secure protocols on the logical layer and a distance measurement technique resilient to physical layer attacks. To attack distance measurement, an attacker can exploit both data-layer as well as physical-layer weaknesses of distance measurement techniques and protocols. Data-layer attacks can be, to a large extent, prevented by implementing distance bounding protocols. However, physical-layer attacks are of significant concern as they can be executed independently of any higher-layer cryptographic primitive that is implemented.

4.1 Distance Bounding Protocols

Secure distance measurement protocols aim at preventing distance shortening and enlargement attacks. When they only prevent distance shortening, they are also called distance bounding protocols, where at the end of the protocol a secure upper bound on the distance is calculated. These protocols are typically executed with different trust assumptions. Devices measuring the distance (typically named verifier and prover) can be mutually trusted, in which case the protocol aims at preventing distance manipulation by an external attacker. If one of the devices, the prover, is untrusted, it will try to manipulate the measured distance. Other scenarios include the untrusted prover being helped by third parties to cheat on its distance. Distance bounding literature describes four main types of attacks 'frauds' corresponding to the above scenarios: distance fraud, mafia fraud, terrorist fraud and distance hijacking.

First investigations of distance bounding protocols started with the work of Beth and Desmedt [17], and by Brands and Chaum [18]. These protocols, as well as many that followed, are designed as cryptographic challenge-response protocols with RTT of flight measurements. One of the key insights of Brands and Chaum was to minimise the processing at the prover so that the prover cannot cheat on its distance to the verifier. Namely, this protocol requires that the prover only computes single bit XOR during the time-critical phase of the protocol. This translates into strong security guarantees as long as the prover cannot implement a faster XOR than assumed by the verifier. Hancke and Kuhn [24] proposed an alternative protocol that uses register selection as a prover processing function. This design reduces the number of protocols steps by allowing the verifier and the prover to pre-agree on the nonces that will be used in the protocol exchange. Many protocols followed these two designs, notably addressing other types of frauds (especially terrorist fraud), as well as the robustness to message loss, performance in terms of protocol execution time, and privacy of distance measurement.

4.2 Distance Measurement Techniques

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.

A radio signal experiences a loss in its signal strength as it travels through the medium. The amount of loss or attenuation in the signal's strength is proportional to the square of the distance travelled. The distance between the transmitter and the receiver can therefore 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 and passive keyless entry and Start Systems) use the strength of the received Bluetooth signal also referred to as the Received Signal Strength Indicator (RSSI) value as a measure of proximity.

Alternatively, the devices can measure the distance between them by estimating the phase difference between a received continuous wave signal and a local reference signal. The need for keeping track of the number of whole cycles elapsed is eliminated by using signals of different frequencies typically referred to as multi-carrier phase-based ranging. Due to their low complexity and low power consumption, phase based ranging is used in several commercial products.

Finally, the time taken for the radio waves to travel from one point to another can be used to measure the distance between the devices. In RF-based RTT based distance estimation the distance d between two entities is given by $d = (t_{rx} - t_{tx}) \times c$, 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 synchronised. The errors due to mismatched clocks are compensated in the round-trip time-of-flight measurement.

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. The ranging precision is roughly 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 1–2m. There are a number of commercially available wireless systems that use chirp and UWB round-trip time-of-flight for distance measurement today.

4.3 Physical Layer Attacks on Secure Distance Measurement

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 all messages transmitted between the two entities. In RSSI-based distance estimation, an attacker can manipulate the measured distance by manipulating the received signal strength at the verifier. The attacker can simply amplify the signal transmitted by the prover before relaying it to the verifier. This will result in an incorrect distance estimation at the verifier. Commercially available solutions claim to secure against relay attacks by simply reducing or attenuating the power of the transmitted signal. However, 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 value ranges 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 (amplifies and forwards) 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. The attacker then receives the prover's response signal and forwards it to the verifier, however with a time delay. The attacker chooses the time delay such that the measured phase differences reaches its maximum value of 2 and rolls over. In other words, the attacker was able to prove to the verifier that the prover is in close proximity (e.g., 1m away) even though the prover was far from the verifier.

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. Given that the radio signals travel at a speed of light, a 1 ns decrease in the time estimate can result in a distance reduction of 30cm.

The first type of attack on time-of-flight ranging leverages the predictable nature of the data contained in the ranging and the acknowledgement packets. 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 their own ranging or acknowledgment signal. An attacker can transmit the acknowledgment packet even before receiving the challenge ranging packet. Several works have shown that the de-facto standard for IR-UWB, IEEE 802.15.4a does not automatically provide security against distance decreasing attacks. In [25] 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. In a 'Cicada' attack, the attacker continuously transmits a pulse 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. In order to prevent such attacks it is

important to avoid predefined or fixed data during the time critical phase of the distance estimation scheme.

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 localisation system. An attacker can predict the bit (early detect) even before receiving the symbol completely. Furthermore, the attacker can leverage the robustness property of modern receivers and transmit arbitrary signal until the correct 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. In such a scenario, the attacker needn't wait for the entire series of pulses to be received before detecting the data being transmitted. After just a time period, the attacker would be able to correctly predict the symbol.

As described previously, round-trip time-of-flight systems are implemented either using chirp or impulse radio ultrawideband signals. Due to their long symbol lengths, both implementations have been shown to be vulnerable to early-detect and late-commit attacks. In the case of chirp-based systems, an attacker can decrease the distance by more than 160 m and in some scenarios even up to 700 m. Although IR-UWB pulses are of short duration (typically 2–3 ns long), data symbols are typically composed of a series of UWB pulses. Furthermore, IEEE 802.15.4a IR-UWB standard allows long symbol lengths ranging from 32 ns to as large as 8μs. Therefore, even the smallest symbol length of 32 ns allows an attacker to reduce the distance by as much as 10 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.

Design of a physical layer for secure distance measurement remains an open topic. However, research so far has yielded some guiding principles for its design. Only radio RTT with single-pulse or multi-pulse UWB modulation has been shown to be secure against physical layer attacks. As a result, the IEEE 802.15.4z working group started the standardization of a new physical layer for UWB secure distance measurement.

The first attempt at formalizing the requirements for secure distance measurement based on the Time of Arrival (ToA) of transmitted messages can be found in [23]. Said work presents a formal definition of Message Time of Arrival Codes (MTACs), the core primitive in the construction of systems for secure ToA measurement. If implemented correctly, MTACs provide the ability to withstand reduction and enlargement attacks on distance measurements. It is shown that systems based on UWB modulation can be implemented such that the stated security requirements are met and therefore constitute examples of MTAC schemes.

4.4 Secure Positioning

Secure positioning systems allow positioning anchors (also called verifiers) to compute the correct position of a node (also called the prover) or allow the prover to determine its own position correctly despite manipulations by the attacker. This means that the attacker cannot convince the verifiers or the prover that the prover is at a position that is different from its true position. This is also called spoofing-resilience. A related property is the one of secure position verification which means that the verifiers can verify the position of an untrusted prover. It is generally assumed that the verifiers are trusted. No restrictions are posed on the attacker as it fully controls the communication channel between the provers and the verifiers.

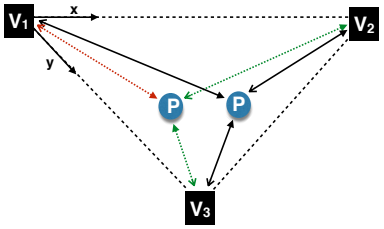

Figure 2: If the computed location of the prover is in the verification triangle, the verifiers conclude that this is a correct location. To spoof the position of prover inside the triangle, the attacker would need to reduce at least one of the distance bounds.

The analysis of broadcast positioning techniques, such as GNSS has shown that such techniques are vulnerable to spoofing if the attacker controls the signals at the antenna of the GNSS receiver.

These type of approaches have been proposed to address this issue: *Verifiable Multilateration* and *Secure Positioning based on Hidden Stations*.

Verifiable Multilateration relies on secure distance measurement / distance bounding. It consists of distance bound measurements to the prover from at least three verifiers (in 2D) and four verifiers (in 3D) and of subsequent computations performed by the verifiers or by a central system. Verifiable Multilateration has been proposed to address both secure positioning and position verification. In the case of secure positioning, the prover is trusted and mafia-fraud-resilient distance bounding is run between the prover and each of the verifiers. The verifiers form verification triangles / triangular pyramids (in 3D) and verify the position of the prover within the triangle / pyramid. For the attacker to spoof a prover from position P to P' within a triangle/pyramid, the attacker would need to reduce at least one of the distance bounds that are measured to P. This follows from the geometry of the triangle/pyramid. Since Distance bounding prevents distance reduction attacks, Verifiable Multilateration prevents spoofing attacks within the triangle/pyramid. The attacker can only spoof P to P' that is outside of the triangle/pyramid, causing the prover and the verifiers to reject the computed position. Namely, the verifiers and the prover only accept the positions that are within the area of coverage, defined as the area covered by the verification triangles/pyramids. Given this, when the prover is trusted, Verifiable Multilateration is resilient to all forms of spoofing by the attacker. Additional care needs to be given to the management of errors and the computation of the position when distance measurement errors are taken into account.

When used for position verification, Verifiable Multilateration is run with an untrusted prover. Each verifier runs a distance-fraud resilient distance bounding protocol with the prover. Based on the obtained distance bounds, the verifiers compute the provers' position. If this position (within some distance and position error bounds) falls within the verification triangle/pyramid, the verifiers accept it as valid. Given that the prover is untrusted, it can enlarge any of the measured distances, but cannot reduce them since this is prevented by the use of distance bounding protocols. Like in the case of secure positioning, the geometry of the triangle/pyramid then prevents the prover from claiming a false position. Unlike in the case of secure positioning, position verification is vulnerable to cloning attacks, in which the prover shares its key to its clones. These clones can then be strategically placed to the verifiers and fake any position by enlarging distances to each individual verifier. This attack can be possibly addressed by tamper resistant hardware or device fingerprinting.

Another approach to secure positioning and position verification is to prevent the attacker

from deterministically spoofing the computed position by making the positions of the verifiers unpredictable for the attacker (either a malicious prover or an external attacker). Verifier positions can therefore be hidden or the verifiers can be mobile. When the verifiers are hidden they should only listen to the beacons sent by the nodes to not disclose their positions. Upon receiving the beacons, the base stations compute the nodes location with TDOA and check if this location is consistent with the time differences.

5 COMPROMISING EMANATIONS AND SENSOR SPOOFING

[26, 27, 28, 29, 30, 31, 32, 33, 34]

Electronic devices emit electromagnetic waves in the form of radio and audio signals, produce heat and create vibration, all of which could correlate with confidential information that the devices process or store. Such emanations, or more generally referred to as side channels, are prevalent and have been extensively studied.

Remote sensor spoofing is the (physical) opposite of compromising emanations. Instead of eavesdropping on electromagnetic leakage, an attacker injects signals that spoof the value measured by a sensor or receiver and thereby (adversely) affects the system relying on the sensor readings and measurements. This is particularly critical in autonomous and other cyber-physical systems that have direct consequences on the safety of the surrounding people and infrastructure.

5.1 Compromising Emanations

In the military context, techniques for exploiting and protecting against unwanted emission in communication systems date back to World War II and have over the time have been collected in an umbrella-term called TEMPEST. The first public demonstration of low-cost attacks on commercial systems using compromising emanations was done in 1985 by Wim van Eck [35]. This attack demonstrated that information displayed on CRT monitors can be successfully eavesdropped from a distance of hundreds of meters. This demonstration prompted research into the sources of such emanations as well as into protective measures. It also highlighted that not only radio emissions leak information. In general, there are four categories of such emanations: acoustic, optical, thermal, and electromagnetic.

Detailed studies of the sources and features that lead to such compromises have been carried out over the years, and on multiple occasions, it was demonstrated that compromising emanations from analogue and digital displays resulted from information being transmitted through analogue video cables and through high-speed Digital Serial Interface (DVI) cables. However, more recent works show that such emanations are not restricted to cables and, to aggravate the situation, compromising emissions are not necessarily caused by analogue or digital displays only.

Some attacks described in research showed that high-frequency sounds caused by vibration of electronic components (capacitors and coils) in the computer's voltage regulation circuit can be used to infer prime factors and therefore derive RSA encryption keys. Sounds emanating from key presses on a keyboard were used to infer what a user is typing. The resulting vibrations can, for instance, be sensed by the accelerometer of a phone located nearby. Finally,

reflections from different objects in the vicinity of computer screens, such as spoons, bottles and user's retina were used to infer information show on a display.

The increasing availability of phones that integrate high quality sensors, such as cameras, microphones and accelerometers makes it easier to mount successful attacks since no dedicated sensor equipment needs to be covertly put in place.

To avoid unwanted signal emissions, devices can be held at a distance, can be shielded and signals that are transmitted should be filtered in order to remove high-frequency components that might reflect switching activity in the circuitry. Moreover, it is generally advised to place a return wire close to the transmission wire in order to avoid exploitation of the return current. In general, wires and communication systems bearing confidential information should be separated (air-gapped) from non-confidential systems.

5.2 Sensor Compromise

Analogue sensors have been shown to be particularly vulnerable to spoofing attacks. Similar to compromising emanations, sensor spoofing depends on the type of the physical phenomena the sensor captures. It can be acoustic, optical, thermal, mechanic or electromagnetic.

Nowadays, many electronic devices, including self-driving cars, medical devices and closed-loop control systems, feature analogue sensors that help observe the environment and make decisions in a fully autonomous way. These systems are equipped with sophisticated protection mechanisms to prevent unauthorised access or compromise via the device's communication interfaces, such as encryption, authentication and access control. Unfortunately, when it comes to data gathered by sensors, the same level of protection is often not available or difficult to achieve since adversarial interactions with a sensor can be hard to model and predict. As a result, unintentional and especially intentional EMI targeted at analogue sensors can pose a realistic threat to any system that relies on readings obtained from an affected sensor.

EMI has been used to manipulate the output of medical devices as well as to compromise ultrasonic ranging systems. Research has shown that consumer electronic devices equipped with microphones are especially vulnerable to the injection of fabricated audio signals [31]. Ultrasonic signals were used to inject silent voice commands, and acoustic waves were used to affect the output of MEMS accelerometers. Accelerometers and intertial systems based on MEMS are, for instance, used extensively in (consumer-grade) drones and multi-copters.

Undoubtedly, sensor spoofing attacks have gained a lot of attention and will likely impact many future cyber-physical devices. System designers therefore have to take great care and protect analogue sensors from adversarial input as an attacker might trigger a critical decision on the application layer of such a device by exposing it to intentional EMI. Potential defence strategies include, for example, (analogue) shielding of the devices, measuring signal contamination using various metrics, or accommodating dedicated EMI monitors to detect and flag suspicious sensor readings.

A promising strategy that follows the approach of quantifying signal contamination to detect EMI sensor spoofing is presented in [34]. The sensor output can be turned on and off according to a pattern unknown to the attacker. Adversarial EMI in the wires between sensor and the circuitry converting the reading to a digital value, i.e., the ADC, can be detected during the times the sensor is off since the sensor output should be at a known level. In case there are fluctuations in the readings, an attack is detected. Such an approach is thought to

be especially effective when used to protect powered or non-powered passive sensors. It has been demonstrated to successfully thwart EMI attacks against a microphone and a temperature sensor system. The only modification required is the addition of an electronic switch that can be operated by the control unit or microcontroller to turn the sensor on and off. A similar sensor spoofing detection scheme can be implemented for active sensors, such as ultrasonic and infrared sensors, by incorporating a challenge-response like mechanism into the measurement acquisition process [36]. An active sensor often has an emitting element and a receiving element. The emitter releases a signal that is reflected and captured by the receiver. Based on the properties of the received signal, the sensor can infer information about the entity or the object that reflected the signal. The emitter can be turned off randomly and during that time the receiver should not be able to register any incoming signal. Otherwise, an attack is detected and the sensor reading is discarded.

6 PHYSICAL LAYER SECURITY OF SELECTED COMMUNICATION TECHNOLOGIES

[37, 38, 39, 40]

This section presents security mechanisms of a selection of existing wireless communication techniques that are in use today. The main focus is on physical-layer security constructs as well as any lack thereof. The communication techniques that are discussed in detail are near-field communication, air traffic communication networks, cellular networks and global navigation satellite systems.

6.1 Near-field communication (NFC)

Near-field communication commonly refers to wireless communication protocols between two small (portable) electronic devices. The standard is used for contact-less payment and mobile payment systems in general. NFC-enabled devices can also exchange identity information, such as keycards, for access control, and negotiate parameters to establish a subsequent high-bandwidth wireless connection using more capable protocols.

NFC is designed to only transmit and receive data to a distance of up to a few centimeters. Even if higher-layer cryptographic protocols are used, vanilla NFC protocols do not offer secure communication and can not guarantee that two communicating devices are indeed only a short distance apart. NFC is vulnerable to eavesdropping, man-in-the-middle attacks and message relay attacks.

Even nowadays, standard NFC is deployed in security-critical contexts due to the assumption that communicating devices are in close proximity. Research has shown, however, that this assumption can not be verified reliably using NFC protocols. The distance can be made almost arbitrarily large by relaying messages between NFC-enabled devices. The attack works as follows: The benign NFC devices are made to believe that they are communicating with each other, but they are actually exchanging data with a modified smartphone. An adversary can strategically place a smartphone next to each benign NFC device while the smartphones themselves use a communication method that can cover long distances, such as WiFi. They simply forward the messages the benign devices are sending to each other. Such an attack is also referred to as a wormhole attack where communicating parties are tricked into assuming

that they are closer than they actually are. This is a problem that cannot be solved using techniques on the logical layer or on the data layer.

Obviously, most of the described attacks can be mitigated by shielding the NFC devices or enhance the protocol with two-factor authentication, for example. Such mechanisms unfortunately transfer security-relevant decisions to the user of an NFC system. Countermeasures that do not impose user burden can roughly be categorised into physical layer methods and the augmentation with context- or device-specific identifiers [37].

Protocol augmentation entails context-aware NFC devices that incorporate location information into the NFC system to verify proximity. The location sensing can be implemented with the help of a variety of different services, each with its own accuracy and granularity. Conceivable are, for instance, GNSS/GPS based proximity verification or leveraging the cell-ID of the base station to which the NFC device is currently closest in order to infer a notion of proximity.

Physical layer methods that have been suggested in research literature are timing restrictions and distance bounding. Enforcing strict timing restraints on the protocol messages can be understood as a crude form of distance bounding. As discussed in Section 4.1, distance bounding determines an upper bound on the physical distance between two communicating devices. While distance bounding is considered the most effective approach, it still remains to be shown if secure distance bounding can be implemented in practice for small NFC-enabled devices.

6.2 Air Traffic Communication Networks

Throughout different flight phases commercial and non-commercial aviation uses several wireless communication technologies to exchange information with aviation authorities on the ground as well as between airborne vehicles. Often legacy systems are still in use and security has never been part of the design of such systems.

While new proposals suggest to overhaul these systems and to tightly integrate security measures into the data layer, such as encryption and message authentication, air traffic communication networks are not only used for information transmission, but also to extract physical layer features from the signal in order to perform aircraft location positioning.

A prominent example is ADS-B. An ADS-B transponder periodically (or when requested) broadcasts the aircraft's position information, such as coordinates, that have been obtained through an on-board GNSS receiver. Most versions of ADS-B only support unauthenticated messages and therefore, this technology suffers from active and passive attacks, i.e., eavesdropping, modifying, injecting and jamming messages. It is, for instance, possible to prevent an aircraft's location from being tracked by Air Traffic Control (ATC) by simply jamming the respective messages. Similarly, an adversary could create ghost planes by emitting fabricated transponder messages. A sophisticated attacker could even fully distort the view ATC has on its airspace.

Multilateration (MLAT) can be seen as a technology that mitigates some of the shortcomings of unauthenticated ADS-B and is therefore usually deployed in conjunction with ADS-B. MLAT does not rely on the transmitted information encapsulated in the message, but makes use of the physical and geometrical constellation between the transmitter (i.e., transponder of the aircraft) and several receivers. MLAT systems extract physical layer properties from the received messages. The time of arrival of a message is recorded at different co-located receivers and, using the propagation speed of the signal, the location of the aircraft's transponder can be

estimated. Multilateration techniques infer the aircraft's location even if the contents of the ADS-B messages are incorrect and thus MLAT provides a means to crosscheck the location information disseminated by the aircraft's transponder.

Although MLAT offers additional security based on physical layer properties, a distributed adversary can still manipulate ADS-B messages. In addition to altering the location information, an attacker can modify or inject signals that affect the time-of-arrival measurement at the receivers. If the attacker has access to multiple distributed antennas and is able to coordinate adversarial signal emission precisely, attacks similar to those on standard ADS-B are feasible. However, the more receivers used to record the signals, the more difficult such attacks become. Unfortunately, MLAT is not always an effective solution in aviation as strategic receiver placement is crucial and time of arrival calculations can be susceptible to multi-path interference [38].

6.3 Cellular Networks

Cellular networks provide voice, data and messaging communication through a network of base stations, each covering one or more cells. The security provisions of these networks are mainly governed by the standards that were adopted in the GSM Association and later in the Third Generation Partnership Plan (3GPP).

Second Generation (2G) 'GSM' networks were introduced during the 1990s, and restricted their services to voice and text messaging. 2G networks were capable of carrying data via a Circuit-Switched Data Service (CSD) which operated in a manner similar to the dial-up modems, just over cellular networks. Further development of email and web services resulted in a need for enhanced speeds and services

3GPP improved 2G GSM standard with packet switched data service, resulting in the general packet radio service (GPRS). Like GSM, GPRS made use of the Home Location Register (HLR), a component that was responsible for subscriber key management and authentication. However, GPRS enhanced GSM by adding the Serving GPRS Support Node (SGSN) for data traffic routing and mobility management for better data traffic delivery. Third Generation (3G) of cellular networks, also known as Universal Mobile Telecommunications Systems (UMTS), introduced a number of improvements over 2G networks, including security enhancements, as well as increased uplink and downlink speeds and capacities. Fourth Generation (4G) cellular networks, also known as Long Term Evolution (LTE) introduced further increase in transmission speeds and capacities.

One of the main security properties that cellular networks aim to protect is the confidentiality of the communication of the link between the mobile station, and the base station and correct billing. The security of cellular networks has evolved with network generations, but all generations have the same overarching concept. Subscribers are identified via their (Universal) subscriber identity modules their International Mobile Subscriber Identity (IMSI) number and its related secret key. IMSI and the keys are used to authenticate subscribers as well as to generate the necessary shared secrets to protect the communication to the cellular network.

2G security focused on the confidentiality of the wireless link between the mobile station and the base station. This was achieved through the authentication via a challenge-response protocol, 2G Authentication and Key Agreement (AKA). This protocol is executed each time when a mobile station initiates a billable operation. 2G AKA achieved authentication based on a long term key K_i shared between the subscriber SIM card and the network. This key is used

by the network to authenticate the subscriber and to derive a session key K_c. This is done within in a challenge response protocol, executed between the SGSN and the mobile station. Before the execution of the protocol, SGSN receives from the HLR the K_c, a random value $RAND$ and an expected response $XRES$. Both K_c and $XRES$ are generated within the HLR based on $RAND$ and K_i. When the mobile station attempts to authenticate to the network it is sent $RAND$. To authenticate, the mobile station combines its long term key K_i (stored on its SIM card) with the received $RAND$ to generate RES and K_c. The mobile station sends RES to the SGSN which compares it to $XRES$. If the two values match, the mobile station is authenticated to the network. The SGSN then sends the K_c to the base station to which the mobile station is connected in order to protect the mobile to base station wireless link.

2G AKA offered very limited protection. It used inadequate key size (56-64 bits), and weak authentication and key generation algorithms (A3,A5 and A8) which were, once released, broken, allowing for eavesdropping and message forgery. Furthermore, AKA was designed to provide only one-way authentication of the mobile station to the network. Since the network did not authenticate to the mobile stations this enabled attacks by fake base stations violating users location privacy and confidentiality of their communication.

In order to address the 2G security shortcomings, 3G networks introduced new 3G Authentication and Key Agreement (3G AKA) procedures. 3G AKA replaced the weak cryptographic algorithms that were used in 2G and provided mutual authentication between the network and the mobile stations. Like in 2G, the goal of the protocol is the authentication (now mutual) of the network and the mobile station. The input into the protocol is a secret key K shared between the HLR and the subscriber. The outcome of the protocol are two keys, the encryption/confidentiality key CK and the integrity key IK. The generation of two keys allows the network and the mobile station to protect the integrity and confidentiality of their communication using two different keys, in line with common security practices. CK and IK are each 128 bits long which is considered adequate.

The authentication and key derivation is performed as follows. The HLR first generates the random challenge $RAND$, from it the expected response $XRES$, the keys CK and IK and the authentication token $AUTN$. It then sends these values to the SGSN. The SGSN sends the $RAND$ as well as the $AUTN$ to the mobile station (also denoted as User Equipment (UE)), which will then use its long term key K to generate the response RES and to verify if $AUTN$ was generated by the HLR. The $AUTN$ is from the shared key and the counter maintained by both the HLR and the mobile station. Upon receiving the RES from the mobile station, SGSN will compare it with the $XRES$ and if they match, will forward the CK and IK to the base station. The base and mobile station can now use these keys to protect their communication.

3G, however, still didn't resolve the vulnerabilities within the operator's networks. CK and IK are transmitted between different entities in the network. They are transmitted between SGSN and the associated base station as well as between different base stations during mobility. This allows network attackers to record these keys and therefore eavesdrop on wireless connections.

4G (LTE) security architecture preserved many of the core elements of 2G and 3G networks, but aimed to address the shortcomings of 3G in terms of the protection of the in-network traffic through the protection of network links and redistribution of different roles. For example, the long term key storage was moved from the HLR to the Home Subscriber Server (HSS). Mobility management was moved from the SGSN to the Mobility Management Engine (MME).

5G security architecture evolves 4G but follows a similar set of principles and entities. 5G

introduces a new versions of Authentication and Key Agreement (AKA) protocols that was designed to fix the issues found in 4G, however with mixed success [41].

6.4 GNSS Security and Spoofing Attacks

GNSS such as GPS and Galileo provide global navigation service through satellites that are orbiting the earth approximately 20,000km above the ground. Satellites are equipped with high-precision atomic clocks which allows the satellites to remain synchronised. Satellites transmit navigation messages at central frequencies of 1575.42MHz (L1) and 1227.60MHz (L2). direct sequence spreading is used to enable acquisition and to protect the signals carrying those messages from spoofing and jamming attacks. Civilian codes are public and therefore do not offer such protection, whereas military and special interest codes are kept confidential. Navigation messages carry data including satellite clock information, the ephemeris (information related to the satellite orbit) and the almanac (the satellite orbital and clock information). Satellite messages are broadcasted and the reception of messages from four of more satellites will allow a receiver to calculate its position. This position calculation is based on trilateration. The receiver measures the times of arrival of the satellite signals, converts them into distances (pseudoranges), and then calculates its position as well as its clock offset with respect to the satellite clocks.

A GPS signal spoofing attack is a physical-layer attack in which an attacker transmits specially crafted radio signals that are identical to authentic satellite signals. Civilian GPS is easily vulnerable to signal spoofing attacks. This is due to the lack of any signal authentication and the publicly known spreading codes for each satellite, modulation schemes, and data structure. In a signal spoofing attack, the objective of an attacker may be to force a target receiver to (i) compute an incorrect position, (ii) compute an incorrect time or (iii) disrupt the receiver. Due to the low power of the legitimate satellite signal at the receiver, the attacker's spoofing signals can trivially overshadow the authentic signals. In a spoofing attack, the GPS receiver typically locks (acquires and tracks) onto the stronger, attacker's signal, thus ignoring the satellite signals.

An attacker can influence the receiver's position and time estimate in two ways: (i) by manipulating the contents of the navigation messages (e.g., the location of satellites, navigation message transmission time) and/or (ii) by modifying the arrival time of the navigation messages. The attacker can manipulate the receiver time of arrival by temporally shifting the navigation message signals while transmitting the spoofing signals. We can classify spoofing attacks based on how synchronous (in time) and consistent (with respect to the contents of the navigation messages) the spoofing signals are in comparison to the legitimate GPS signals currently being received at the receiver's true location.

Non-Coherent and Modified Message Contents: In this type of attack, the attacker's signals are both unsynchronised and contain different navigation message data in comparison to the authentic signals. Attackers who use GPS signal generators to execute the spoofing attack typically fall under this category. An attacker with a little know-how can execute a spoofing attack using these simulators due to their low complexity, portability and ease of use. Some advanced GPS signal generators are even capable of recording and replaying signals, however not in real-time. In other words, the attacker uses the simulator to record at one particular time in a given location and later replays it. Since they are replayed at a later time, the attacker's signals are not coherent and contain different navigation message data than the legitimate signals currently being received.

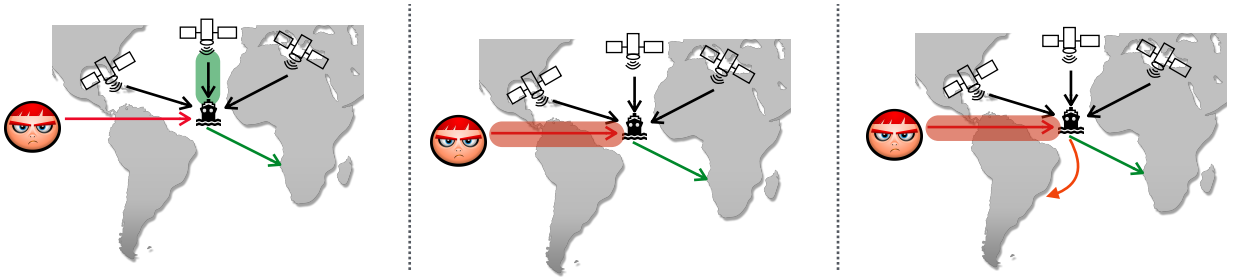

Figure 3: Seamless takeover attack on GPS. The spoofing aligns its signal with the legitimate signal and slowly increase the transmit power. Once receiver locks on to attacker's signal, he starts to manipulate it.

Non-Coherent but Unmodified Message Contents: In this type of attack, the navigation message contents of the transmitted spoofing signals are identical to the legitimate GPS signals currently being received. However, the attacker temporally shifts the spoofing signal thereby manipulating the spoofing signal time of arrival at the target receiver. For example, attackers capable of real-time recording and replaying of GPS signals fall under this category as they will have the same navigation contents as that of the legitimate GPS signals, however shifted in time. The location or time offset caused by such an attack on the target receiver depends on the time delay introduced both by the attacker and due to the propagation time of the relayed signal. The attacker can precompute these delays and successfully spoof a receiver to a desired location.

Coherent but Modified Message Contents: The attacker generates spoofing signals that are synchronised to the authentic GPS signals. However, the contents of the navigation messages are not the same as that of the currently seen authentic signals. For instance, phase-coherent signal synthesisers are capable of generating spoofing signals with the same code phase as the legitimate GPS signal that the target receiver is currently locked on to. Additionally, the attacker modifies the contents of the navigation message in real-time (and with minimal delay) and replays it to the target receiver. A variety of commercial GPS receivers were shown to be vulnerable to this attack and in some cases, it even caused permanent damage to the receivers.

Coherent and Unmodified Message Contents: Here, the attacker does not modify the contents of the navigation message and is completely synchronised to the authentic GPS signals. Even though the receiver locks on to the attacker's spoofing signals (due to the higher power), there is no change in the location or time computed by the target receiver. Therefore, this is not an attack in itself but is an important first step in executing the seamless takeover attack.

The seamless takeover attack is considered one of the strongest attacks in literature. In a majority of applications, the target receiver is already locked on to the legitimate GPS satellite signals. The main steps are highlighted in Figure 3. The goal of an attacker is to force the receiver to stop tracking the authentic GPS signals and lock onto the spoofing signals without causing any signal disruption or data loss. This is because the target receiver can potentially detect the attack based on the abrupt loss of GPS signal. In a seamless takeover attack, first, the attacker transmits spoofing signals that are synchronised with the legitimate satellite signals and are at a power level lower than the received satellite signals. The receiver is still locked on to the legitimate satellite signals due to the higher power and hence there is no change in the ships route. The attacker then gradually increases the power of the spoofing signals until the target receiver stops tracking the authentic signal and locks on to the spoofing

signals. Note that during this takeover, the receiver does not see any loss of lock, in other words, the takeover was seamless. Even though the target receiver is now locked on to the attacker, there is still no change in the route as the spoofing signals are both coherent with the legitimate satellite signals as well as there is no modification to the contents of the navigation message itself. Now, the attacker begins to manipulate the spoofing signal such that the receiver computes a false location and begins to alter its course. The attacker can either slowly introduce a temporal shift from the legitimate signals or directly manipulate the navigation message contents to slowly deviate the course of the ship to a hostile destination.

If an attacker controls all the signals that arrive at the receiver's antenna(s) the receiver cannot detect spoofing. However, if the attack is remote, and the attacker cannot fully control the signals at the receiver, anomaly detection techniques can be used to detect spoofing. In particular, Automatic Gain Control (AGC) values, Received Signal Strength (RSS) from individual satellites, carrier phase values, estimated noise floor levels, number of visible satellites all can be used to detect spoofing. Particularly interesting are techniques based on tracking and analysis of autocorrelation peaks that are used for the detection of GNSS signals. Distortion, the number and the behaviour over time of these peaks can be used to detect even the most sophisticated seamless takeover attacks.

The detection of GNSS spoofing can be improved if spoofing signals are simultaneously received by several receivers. This can be used for the detection of spoofing as well as for spoofer localisation. If the receivers know their mutual distances (e.g., are placed at fixed distances), the spoofer needs to preserve those distances when performing the spoofing attack. When a single spoofer broadcasts its signals, it will result in all receivers being spoofed to the same position, therefore enabling detection. This basic detection technique can be generalised to several receivers, allowing even the detection of distributed spoofers.

Finally, GNSS spoofing can be made harder through the authentication and hiding of GNSS signals. Although currently civilian GNSS systems do not support authentication, digital signatures as well as hash-based signatures such as TESLA can be added to prevent the attacker from generating GNSS signals. This would, however, not prevent all spoofing attacks since the attacker can still selectively delay navigation messages and therefore modify the computed position. This attack can be prevented by the use of spreading with delayed key disclosure. Even this approach still does not fully prevent against spoofing by broadband receivers that are able to relay full GNSS frequency band between locations.

Military GPS signals are authenticated, and try to achieve low-probability of intercept as well as jamming resilience via the use of secret spreading codes. This approach prevents some of the spoofing attacks, but still fails to fully prevent record-and-relay attacks. In addition, this approach does not scale well since secret spreading codes need to be distributed to all intended receivers, increasing the likelihood of their leakage and reducing usability.

In conclusion, although newly proposed and deployed countermeasures make it more difficult for the attacker to spoof GNS systems like GPS, currently no measure fully prevents spoofing under strong attacker models. This is an area of active research.

CONCLUSION

As we have shown in this knowledge area, the wireless physical layer presents both challenges and opportunities. Challenges typically come from the broadcast nature of wireless communication and from it not being protected against confidentiality and integrity violations. Physical layer is typically application agnostic. Opportunities stem from the stochastic nature of the channel as well as from its robustness to fine-grained manipulations. Under different attacker models, physical layer can support both highly usable and secure solutions.

CROSS-REFERENCE OF TOPICS VS REFERENCE MATERIAL

The table below lists the reference material that serves as the basis for for this chapter and explains how it relates to the different topics. Whenever possible, references are further divided into sub-topics.

Topic	Key references	Other references
1 Physical Layer Schemes for Confidentiality, Integrity and Access Control		
1.1 Key Establishment based on Channel Reciprocity	[1, 2, 3]	[42, 43, 44, 45, 46, 47]
1.2 MIMO-supported Approaches: Orthogonal Blinding, Zero-Forcing	[1, 5]	[48, 49, 50, 51]
1.3 Secrecy Capacity	[7, 8, 10, 9]	[52, 53, 54, 55]
1.4 Friendly Jamming	[1, 4]	[56, 57, 58, 59]
1.5 Using Physical Layer to Protect Data Integrity	[1, 6]	[60]
1.6 Low probability of intercept and Covert Communication	[1]	[61, 62, 63]
2 Jamming and Jamming-Resilient Communication	[11, 12]	[64, 65, 66, 67]
3 Physical-Layer Identification	[15]	[68, 69, 70]
4 Distance Bounding and Secure Positioning		
4.1 Distance Bounding Protocols	[16, 17, 18]	[71, 24, 72, 73, 74, 75]
4.2 Distance Measurement Techniques	[16, 20]	[76, 77, 78, 79]
4.3 Physical Layer Attacks on Secure Distance Measurement	[16][20, 19, 21]	[80, 81, 82, 25, 83]
4.4 Secure Positioning	[22]	[84, 85, 86, 87, 88]
5 Compromising Emanations and Sensor Spoofing		
5.1 Compromising Emanations	[26, 27, 28, 29, 30]	[89, 90, 91, 92, 93]
5.2 Sensor Compromise	[31, 32, 33, 34, 36]	[94, 95, 96, 97, 98]
6 Physical Layer Security of Selected Communication Technologies		
6.1 Near-field communication (NFC)	[37]	[99, 100, 101]
6.2 Air Traffic Communication Networks	[38]	[102, 103, 104, 105]
6.3 Cellular Networks	[39]	[106, 107, 108]
6.4 GNSS Security and Spoofing Attacks	[40]	[109, 110, 111, 112, 113]

ACKNOWLEDGEMENTS

The author would like to specially thank Marc Roeschlin for his valuable input. Thanks to Aanjhan Ranganathan, Davide Zanetti, Boris Danev, Christina Popper, Kasper Rasmussen and Nils Tippenhauer for allowing the reproduction of selected text and figures from their publications within this document.

REFERENCES

[1] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, 1st ed. Springer Publishing Company, Incorporated, 2009.

[2] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[3] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in *Computer Security – ESORICS 2012*, S. Foresti, M. Yung, and F. Martinelli, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 235–252.

[4] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *Proceedings of the ACM SIGCOMM 2011 Conference*, ser. SIGCOMM '11. New York, NY, USA: ACM, 2011, pp. 2–13.

[5] N. Anand, S.-J. Lee, and E. W. Knightly, "Strobe: Actively securing wireless communications using zero-forcing beamforming," in *2012 Proceedings IEEE INFOCOM*, March 2012, pp. 720–728.

[6] S. Čapkun, M. Čagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava, "Integrity codes: Message integrity protection and authentication over insecure channels," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 4, pp. 208–223, Oct 2008.

[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[8] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[9] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[10] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[11] D. Adamy, *EW 101: a first course in electronic warfare*. Artech House, 2001.

[12] C. Popper, "On secure wireless communication under adversarial interference," PhD thesis, ETH Zurich, 2011.

[13] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Čapkun, "Investigation of signal and message manipulations on the wireless channel," in *Proceedings of the European Symposium on Research in Computer Security*, 2011.

[14] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on LTE," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 55–72. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/yang-hojoon

[15] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surv.*, vol. 45, no. 1, pp. 6:1–6:29, Dec. 2012.

[16] G. Avoine, M. A. Bingöl, I. Boureanu, S. čapkun, G. Hancke, S. Kardaş, C. H. Kim, C. Lauradoux, B. Martin, J. Munilla, A. Peinado, K. B. Rasmussen, D. Singelée, A. Tchamkerten, R. Trujillo-Rasua, and S. Vaudenay, "Security of distance-bounding: A survey," *ACM Comput. Surv.*, vol. 51, no. 5, pp. 94:1–94:33, Sep. 2018.

[17] T. Beth and Y. Desmedt, "Identification tokens—or: Solving the chess grandmaster

problem," in *Conference on the Theory and Application of Cryptography*. Springer, 1990, pp. 169–176.
[18] S. Brands and D. Chaum, "Distance-bounding protocols," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1993, pp. 344–359.
[19] 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*, L. Buttyán, V. D. Gligor, and D. Westhoff, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 83–97.
[20] A. Ranganathan and S. Capkun, "Are we really close? Verifying proximity in wireless systems," *IEEE Security & Privacy*, vol. 15, no. 3, pp. 52–58, 2017.
[21] M. Singh, P. Leu, and S. Capkun, "UWB with pulse reordering: Securing ranging against relay and physical layer attacks." *IACR Cryptology ePrint Archive*, vol. 2017, p. 1240, 2017.
[22] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, Feb 2006.
[23] P. Leu, M. Singh, M. Roeschlin, K. G. Paterson, and S. Capkun, "Message time of arrival codes: A fundamental primitive for secure distance measurement," *IEEE Symposium on Security and Privacy*, 2020.
[24] G. P. Hancke and M. G. Kuhn, "An RFID distance bounding protocol," in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*. IEEE, 2005, pp. 67–73.
[25] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "Distance bounding with IEEE 802.15. 4a: Attacks and countermeasures," *IEEE Transactions on Wireless Communications*, vol. 10, no. 4, pp. 1334–1344, 2011.
[26] M. G. Kuhn and C. M. G. Kuhn, "Compromising emanations: Eavesdropping risks of computer displays," 2003.
[27] M. G. Kuhn, "Electromagnetic eavesdropping risks of flat-panel displays," in *International Workshop on Privacy Enhancing Technologies*. Springer, 2004, pp. 88–107.
[28] M. Backes, T. Chen, M. Duermuth, H. P. A. Lensch, and M. Welk, "Tempest in a teapot: Compromising reflections revisited," in *2009 30th IEEE Symposium on Security and Privacy*, May 2009, pp. 315–327.
[29] D. Genkin, A. Shamir, and E. Tromer, "RSA key extraction via low-bandwidth acoustic cryptanalysis," in *Advances in Cryptology – CRYPTO 2014*, J. A. Garay and R. Gennaro, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 444–461.
[30] P. Marquardt, A. Verma, H. Carter, and P. Traynor, "(sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 551–562.
[31] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *2013 IEEE Symposium on Security and Privacy*, May 2013, pp. 145–159.
[32] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "DolphinAttack: Inaudible voice commands," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 103–117.
[33] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, April 2017, pp. 3–18.
[34] Y. Zhang and K. Rasmussen, "Detection of electromagnetic interference attacks on sensor systems," in *IEEE Symposium on Security and Privacy (S&P)*, May 2020.
[35] W. van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers & Security*, vol. 4, no. 4, pp. 269 – 286, 1985. [Online]. Available:

http://www.sciencedirect.com/science/article/pii/016740488590046X
[36] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "Pycra: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 1004–1015.
[37] L. Francis, G. P. Hancke, K. Mayes, and K. Markantonakis, "Practical relay attack on contactless transactions by using NFC mobile phones." *IACR Cryptology ePrint Archive*, vol. 2011, p. 618, 2011.
[38] M. Strohmeier, "Security in next generation air traffic communication networks," Ph.D. dissertation, University of Oxford, 2016.
[39] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi, *LTE Security*, 2nd ed. Wiley Publishing, 2012.
[40] A. Ranganathan, "Physical-layer techniques for secure proximity verification and localization," PhD thesis, ETH Zurich, 2016.
[41] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: ACM, 2018, pp. 1383–1396. [Online]. Available: http://doi.acm.org/10.1145/3243734.3243846
[42] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on mobile Computing*, vol. 12, no. 5, pp. 917–930, 2012.
[43] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: proximity-based secure pairing using ambient wireless signals," in *Proceedings of the 9th international conference on Mobile systems, applications, and services*. ACM, 2011, pp. 211–224.
[44] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *Ieee access*, vol. 4, pp. 614–626, 2016.
[45] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Transactions on Communications*, vol. 64, no. 6, pp. 2578–2588, 2016.
[46] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 401–410.
[47] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, 2008, pp. 64–78.
[48] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4599–4615, 2014.
[49] Y. Zheng, M. Schulz, W. Lou, Y. T. Hou, and M. Hollick, "Profiling the strength of physical-layer security: A study in orthogonal blinding," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2016, pp. 21–30.
[50] M. Schulz, A. Loch, and M. Hollick, "Practical known-plaintext attacks against physical layer security in wireless mimo systems." in *The Network and Distributed System Security Symposium (NDSS)*, 2014.
[51] P. Robyns, P. Quax, and W. Lamotte, "PHY-layer security is no alternative to cryptography," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2017, pp. 160–162.
[52] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using

polar codes," *arXiv preprint arXiv:1007.3568*, 2010.
[53] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.* IEEE, 2005, pp. 2152–2155.
[54] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.
[55] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," in *2007 IEEE International Symposium on Information Theory*. IEEE, 2007, pp. 1306–1310.
[56] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," in *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 174–188.
[57] D. S. Berger, F. Gringoli, N. Facchi, I. Martinovic, and J. Schmitt, "Gaining insight on friendly jamming in a real-world IEEE 802.11 network," in *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*. ACM, 2014, pp. 105–116.
[58] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, 2011.
[59] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 160–173.
[60] S. Capkun, M. Cagalj, G. Karame, and N. O. Tippenhauer, "Integrity regions: Authentication through presence in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 11, pp. 1608–1621, 2010.
[61] A. Polydoros and K. Woo, "LPI detection of frequency-hopping signals using autocorrelation techniques," *IEEE journal on selected areas in communications*, vol. 3, no. 5, pp. 714–726, 1985.
[62] R. F. Mills and G. E. Prescott, "Waveform design and analysis of frequency hopping LPI networks," in *Proceedings of MILCOM'95*, vol. 2. IEEE, 1995, pp. 778–782.
[63] L. Frikha, Z. Trabelsi, and W. El-Hajj, "Implementation of a covert channel in the 802.11 header," in *2008 International Wireless Communications and Mobile Computing Conference*. IEEE, 2008, pp. 594–599.
[64] C. Popper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp. 703–715, June 2010.
[65] W. Xu, W. Trappe, and Y. Zhang, "Anti-jamming timing channels for wireless networks," in *Proceedings of the First ACM Conference on Wireless Network Security*, ser. WiSec '08. New York, NY, USA: ACM, 2008, pp. 203–213.
[66] M. Strasser, C. Pöpper, and S. Čapkun, "Efficient uncoordinated FHSS anti-jamming communication," in *Proceedings of the Tenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '09. New York, NY, USA: ACM, 2009, pp. 207–218.
[67] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: a survey," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.
[68] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2091–2106, 2016.

[69] T. J. Bihl, K. W. Bauer, and M. A. Temple, "Feature selection for RF fingerprinting with multiple discriminant analysis and using zigbee device emissions," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1862–1874, 2016.
[70] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Fingerprinting Wi-Fi devices using software defined radios," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2016, pp. 3–14.
[71] S. Capkun, K. El Defrawy, and G. Tsudik, "Group distance bounding protocols," in *International Conference on Trust and Trustworthy Computing*. Springer, 2011, pp. 302–312.
[72] N. O. Tippenhauer and S. Čapkun, "Id-based secure distance bounding and localization," in *European Symposium on Research in Computer Security*. Springer, 2009, pp. 621–636.
[73] M. Kuhn, H. Luecken, and N. O. Tippenhauer, "UWB impulse radio based distance bounding," in *2010 7th Workshop on Positioning, Navigation and Communication*. IEEE, 2010, pp. 28–37.
[74] L. Bussard and W. Bagga, "Distance-bounding proof of knowledge to avoid real-time attacks," in *IFIP International Information Security Conference*. Springer, 2005, pp. 223–238.
[75] D. Singelée and B. Preneel, "Distance bounding in noisy environments," in *European Workshop on Security in Ad-hoc and Sensor Networks*. Springer, 2007, pp. 101–115.
[76] K. B. Rasmussen and S. Capkun, "Realization of RF distance bounding." in *USENIX Security Symposium*, 2010, pp. 389–402.
[77] A. Ranganathan, N. O. Tippenhauer, B. Škorić, D. Singelée, and S. Čapkun, "Design and implementation of a terrorist fraud resilient distance bounding system," in *European Symposium on Research in Computer Security*. Springer, 2012, pp. 415–432.
[78] N. O. Tippenhauer, H. Luecken, M. Kuhn, and S. Capkun, "UWB rapid-bit-exchange system for distance bounding," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2015, p. 2.
[79] S. Drimer, S. J. Murdoch *et al.*, "Keep your enemies close: Distance bounding against smartcard relay attacks." in *USENIX security symposium*, vol. 312, 2007.
[80] C. Cremers, K. B. Rasmussen, B. Schmidt, and S. Capkun, "Distance hijacking attacks on distance bounding protocols," in *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012, pp. 113–127.
[81] G. P. Hancke and M. G. Kuhn, "Attacks on time-of-flight distance bounding channels," in *Proceedings of the first ACM conference on Wireless network security*. ACM, 2008, pp. 194–202.
[82] K. B. Rasmussen and S. Čapkun, "Location privacy of distance bounding protocols," in *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, 2008, pp. 149–160.
[83] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "Effectiveness of distance-decreasing attacks against impulse radio ranging," in *Proceedings of the third ACM conference on Wireless network security*. ACM, 2010, pp. 117–128.
[84] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.-P. Hubaux, "A practical secure neighbor verification protocol for wireless sensor networks," in *Proceedings of the second ACM conference on Wireless network security*. ACM, 2009, pp. 193–200.
[85] S. Čapkun and J.-P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *IEEE infocom*, no. CONF, 2005.
[86] J. T. Chiang, J. J. Haas, and Y.-C. Hu, "Secure and precise location verification using distance bounding and simultaneous multilateration," in *Proceedings of the second ACM conference on Wireless network security*. ACM, 2009, pp. 181–192.

[87] N. Basilico, N. Gatti, M. Monga, and S. Sicari, "Security games for node localization through verifiable multilateration," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 1, pp. 72–85, 2013.
[88] L. Lazos, R. Poovendran, and S. Čapkun, "Rope: robust position estimation in wireless sensor networks," in *Proceedings of the 4th international symposium on Information processing in sensor networks*. IEEE Press, 2005, p. 43.
[89] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic side-channel attacks on printers." in *USENIX Security symposium*, 2010, pp. 307–322.
[90] D. Balzarotti, M. Cova, and G. Vigna, "Clearshot: Eavesdropping on keyboard input from video," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, 2008, pp. 170–183.
[91] M. Backes, M. Dürmuth, and D. Unruh, "Compromising reflections-or-how to read lcd monitors around the corner," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, 2008, pp. 158–169.
[92] R. Raguram, A. M. White, D. Goswami, F. Monrose, and J.-M. Frahm, "iSpy: automatic reconstruction of typed input from compromising reflections," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 527–536.
[93] X. Liu, Z. Zhou, W. Diao, Z. Li, and K. Zhang, "When good becomes evil: Keystroke inference with smartwatch," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 1273–1285.
[94] C. Kasmi and J. L. Esteves, "IEMI threats for information security: Remote command injection on modern smartphones," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 6, pp. 1752–1755, 2015.
[95] Y. Park, Y. Son, H. Shin, D. Kim, and Y. Kim, "This ain't your dose: Sensor spoofing attack on medical infusion pump," in *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, 2016.
[96] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009, pp. 410–419.
[97] J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, M. Mina *et al.*, "Electromagnetic induction attacks against embedded systems," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. ACM, 2018, pp. 499–510.
[98] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," in *24th USENIX Security Symposium (USENIX Security 15)*, 2015, pp. 881–896.
[99] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC devices: Security and privacy," in *2008 Third International Conference on Availability, Reliability and Security*. IEEE, 2008, pp. 642–647.
[100] S. Burkard, "Near field communication in smartphones," *Dep. of Telecommunication Systems, Service-centric Networking, Berlin Institute of Technology, Germany*, 2012.
[101] N. Alexiou, S. Basagiannis, and S. Petridou, "Security analysis of NFC relay attacks using probabilistic model checking," in *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2014, pp. 524–529.
[102] A. Costin and A. Francillon, "Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," *Black Hat USA*, pp. 1–12, 2012.
[103] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in *International Conference on Applied Cryptography and Network Security*. Springer, 2013, pp. 253–271.
[104] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "Economy class crypto:

Exploring weak cipher usage in avionic communications via ACARS," in *International Conference on Financial Cryptography and Data Security*. Springer, 2017, pp. 285–301.
[105] M. Strohmeier, V. Lenders, and I. Martinovic, "Intrusion detection for airborne communication using phy-layer information," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2015, pp. 67–77.
[106] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," *arXiv preprint arXiv:1510.07563*, 2015.
[107] A. N. Bikos and N. Sklavos, "LTE/SAE security issues on 4G wireless networks," *IEEE Security & Privacy*, vol. 11, no. 2, pp. 55–62, 2012.
[108] J.-G. Remy and C. Letamendia, *LTE standards*. Wiley Online Library, 2014.
[109] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 75–86.
[110] A. Ranganathan, H. Ólafsdóttir, and S. Capkun, "SPREE: A spoofing resistant GPS receiver," in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*. ACM, 2016, pp. 348–360.
[111] C. Bonebrake and L. R. O'Neil, "Attacks on GPS time reliability," *IEEE Security & Privacy*, vol. 12, no. 3, pp. 82–84, 2014.
[112] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 450–461.
[113] J. V. Carroll, "Vulnerability assessment of the US transportation infrastructure that relies on the global positioning system," *The Journal of Navigation*, vol. 56, no. 2, pp. 185–193, 2003.

ACRONYMS

3GPP Third Generation Partnership Plan.

ADC Analogue-to-Digital Converter.

ADS-B Automatic Dependent Surveillance-Broadcast.

AGC Automatic Gain Control.

AKA Authentication and Key Agreement.

ATC Air Traffic Control.

CIR Channel Impulse Response.

CRT Cathode Ray Tube.

CSD Circuit-Switched Data Service.

CSS Chirp-Spread Spectrum.

DSSS Direct-Sequence Spread Spectrum.

DVI Digital Serial Interface.

DWT Discrete Wavelet Transform.

EMI Electromagnetic Interference.

FFT Fast Fourier Transform.

FHSS Frequency Hopping Spread Spectrum.

GNS Global Navigation Systems.

GNSS Global Navigation Satellite Systems.

GPRS General Packet Radio Service.

GPS Global Positioning System.

GSM Global System for Mobile Communications.

HLR Home Location Register.

HRL Hyper-V Replica Log.

HSS Home Subscriber Server.

IMSI International Mobile Subscriber Identity.

IR-UWB Impulse-Radio Ultra Wideband.

ISO Interational Organization for Standardization.

LPI Low Probability of Intercept.

LTE Long Term Evolution.

MEMS Microelectromechanical Systems.

MIMO Multi-Antenna, Multiple Input Multiple Output.

MLAT Multilateration.

MME Mobility Management Engine.

MTAC Message Time of Arrival Code.

NFC Near-Field Communication.

QPSK Quadrature Phase Shift Keying.

RF Radio Frequency.

RFID Radio-Frequency Identification.

RSA Rivest-Shamir-Adleman.

RSS Received Signal Strength.

RSSI Received Signal Strength Indicator.

RTT Round-Trip Time.

SGSN Serving GPRS Support Node.

SIM Subscriber Identity Module.

SIMO Single Input, Multiple Output.

TDOA Time-Difference Of Arrival.

ToA Time of Arrival.

ToF Time of Flight.

UDSSS Uncoordinated Direct-Sequence Spread Spectrum.

UE User Equipment.

UFH Uncoordinated Frequency Hopping.

UMTS Universal Mobile Telecommunications Systems.

UWB Ultra-Wideband.

VHF Very High Frequency.

GLOSSARY

WiFi A family of radio technologies that is used for the wireless local area networking (WLAN).

INDEX

KNOWLEDGE DEPENDENCIES

Knowledge dependencies outside the area of cyber security:

- *Signal processing and radio propagation:* Signal analysis and signal generation are relevant for most topics in wireless physical-layer security. In particular, physical layer schemes for confidentiality, integrity and access Control require a deep understanding of the transmitted signals. Apart from signal processing, wireless security also has considerable overlap with radio propagation and other sub-fields that study the effects of electromagnetic radiation.
- *Information Theory:* Knowledge in this field is especially relevant for key establishment based on wireless channels. Similarly, secrecy capacity has great overlap with information theory.
- *Machine learning and pattern recognition:* Expertise in this area is crucial for physical-layer identification where the classification of physical characteristics unique to a wireless transmitter is required to perform the identification of a wireless device. Machine Learning can also be a central part to detecting compromising emanations, establishing covert channels and mounting side channel attacks.

7 EXCLUSIONS

This KA specifically deals with physical layer security of wireless systems. Thus, all concepts covered in this KA have the radiation of electromagnetic signals common. Some of the (public) reviews suggested the inclusion of wired transmission methods, such as ADSL, as well as modulation techniques used in the context of those protocols. However, scenarios where signals are mostly confined to a conductor, such as wired transmission, have not been in the original scope of this KA and are therefore not covered.