White Paper on Physical Layer Security

IEEE Focus Group on Physical Layer Security
Editors: Arsenia Chorti, Stefano Tomasin, Marco Baldi,
Stephane Delbruel, and Gunes Karabulut Kurt

January 12, 2026

Contents

Editors

Arsenia Chorti, *École nationale supérieure de l'électronique et de ses applications, Cergy, France*

Stefano Tomasin, *University of Padova, Italy*

Marco Baldi, *Università Politecnica delle Marche, Italy*

Stephane Delbruel, *University of Bordeaux, France*

Gunes Karabulut Kurt, *Polytechnique Montréal, Canada*

Focus Group Member Contributors

Angeliki Alexiou
Matthieu Bloch
Gaojie Chen
Stephane Delbruel
Ashotush Dutta
Gerhard Fettweis
Camilla Hollanti
Nigel Jefferies
Vinod Kumar
Laura Luzzi
Parthajit Mohapatra
Miroslav Mitev
Andre Noll Barreto
Nikolaos Pappas
Jay Prakash
Rafael Felix Schaefer
Linda Senigagliesi
Muhammad Shehzad
Rohit Singh
Muralikrishnan Srinivasan
Himanshu Tyagi
Zoran Utkovski
João Vilela
Shihao Yan
Junqing Zhang
Igor Bjelakovic
Kanapathippillai Cumanan
Daniel Costa
Simone Delprete
Elza Erkip
Eman Hammad
Eduard Jorswieck
Stefan Koepsell
Pin-Hsun Lin
Mahtab Mirmohseni
Lorenzo Mucchi
Diana Moya Osorio
Berna Özbek
Vince Poor
Philippe Sehier
Mahdi Shakiba Herfeh
Dave Singelee
Slawomir Stanczak
Minh Thuy Pham
Sennur Ulukus
Hua Wang
Arlyn Yener

List of Acronyms

AoA angle of arrival

AGV automated guided vehicle

CSI channel state information

DET detection error tradeoff

FA false alarm

GNSS global navigation satellite system

KPI key performance indicator

KVI key value indicator

KL Kullback-Leibler

MD misdetection

PDF probability density function

PLA physical-layer authentication

PLS physical-layer security

PUF physical unclonable function

ROC receiver operating characteristic

RSSI received-signal strength indicator

SKG secret key generation

SNR signal-to-noise ratio

TDD time-division duplex

UAV unmanned aerial vehicle

1 — Physical-Layer Security: Why Now?

Physical-layer security (PLS) exploits the physical characteristics of the communication medium to provide security. It provides security mechanisms in three main domains: secrecy, authentication, and secret key generation.

Secrecy refers to the ability to transmit information from a legitimate sender to a legitimate receiver in a way that prevents an unauthorized eavesdropper from decoding the message. Unlike cryptography, which relies on computational complexity, physical-layer secrecy improves the legitimate receiver's channel while degrading the eavesdropper's channel. Authentication mechanisms ensure that a message has not been tampered with and comes from the claimed sender. In physical-layer security, authentication often relies on the unique and reciprocal nature of the channel impulse response between two communicating parties. This "channel fingerprint" acts as a unique signature that is difficult for an imposter to replicate. Secret key generation mechanisms enable two parties, Alice and Bob, to establish a shared secret key without any pre-existing shared information. Physical-layer key generation leverages the shared randomness of the wireless channel. Since the channel fading coefficients are highly correlated between Alice and Bob, but not with a distant eavesdropper, this shared randomness can be used to generate a secure, symmetric key.

Studies on PLS first emerged from information theory and then evolved into practical applications in signal processing and code design. The information-theoretic foundation begins with Claude Shannon's 1949 paper [1]. In this paper, Shannon introduced the concept of perfect secrecy, demonstrating that a message could be made perfectly secure if the secret key were as long as the message and used only once (the one-time pad). Although not directly focused on the physical layer, the paper established a mathematical framework for measuring secrecy in an information-theoretic sense.

The true birth of physical-layer security is widely attributed to Aaron Wyner's 1975 paper [2]. Wyner introduced a formal model in which a transmitter communicates with a legitimate receiver and an eavesdropper. He proved the existence of secrecy capacity: the maximum rate at which information can be transmitted securely without a shared secret key as long as the legitimate channel is better than the eavesdropper's channel. This concept was revolutionary, demonstrating that security could be an intrinsic property of the physical channel itself.

Following Wyner's lead, U. Maurer provided the theoretical framework for secret key generation in 1993, [3]. Maurer showed that two parties could agree on a secret key by publicly discussing correlated information unknown to an eavesdropper. This provided the blueprint for later works applying this concept to the physical properties of a communication channel.

After Wyner's initial work, the information-theoretic community expanded the "wiretap channel" model to more complex and realistic scenarios.

MIMO and Multiuser Systems: The introduction of multiple-input, multiple-output (MIMO) systems using multiple antennas at the transmitter and receiver offered new opportunities for secrecy.

Researchers demonstrated that MIMO could be employed to establish a favorable channel for the authorized user while simultaneously degrading the eavesdropper's channel.

Cooperative Security: This area of research explores using relay nodes to enhance security. A friendly relay can amplify the signal to help the legitimate receiver while simultaneously sending interfering signals to confuse the eavesdropper. This cooperative strategy creates a more robust secrecy channel.

Artificial Noise Injection: The information-theoretic perspective also led to the concept of using artificial noise as a security tool. The core idea is for the legitimate transmitter to inject carefully crafted interference in the null space of the legitimate receiver, meaning it won't affect their signal, but will disrupt the eavesdropper. This guarantees security even when the legitimate channel is not strictly better than the eavesdropper's channel.

Information theory set the bounds, and signal processing provided the practical means to achieve them. This is where theoretical concepts were translated into implementable algorithms and techniques. In the context of signal secrecy, beamforming and precoding are signal processing techniques that steer the signal to the intended receiver while simultaneously creating a null in the direction of the eavesdropper. This maximizes the signal-to-noise ratio at the intended receiver and minimizes it at the eavesdropper—a perfect application of Wyner's original idea. In physical-layer authentication, the unique and reciprocal nature of the channel impulse response is leveraged for device authentication. By analyzing the channel's characteristics, a receiver can verify the transmitter's identity because it is nearly impossible for an imposter to perfectly mimic the channel signature. Signal processing is also crucial for secret key generation, turning noisy channel measurements into a shared secret key. Researchers have developed practical protocols for this process. Their work involved steps such as channel probing, quantizing the channel coefficients into a binary string, and a reconciliation phase to correct any discrepancies in the generated key. These protocols are fundamental to the widespread adoption of physical-layer key generation.

1.1 Current Security Landscape and the Need for PLS

Undoubtedly, 5G security enhancements are a significant improvement over LTE, especially with the introduction of public key infrastructure (PKI) protocols for authentication and key agreement (AKA). However, as application scenarios become more complex with the introduction of ultra-reliable, low-latency communications (URLLC) and massive machine-type communications (mMTC), as well as in Internet of Things (IoT)-related verticals, new security challenges arise that may be difficult to address using standard, complexity-based, classic cryptographic protocols. The limited computational power and reduced connectivity of IoT devices may prevent the execution of complex encryption and decryption algorithms and the distribution of encryption keys.

Looking ahead, sixth-generation (6G) systems will need to operate under diverse constraints. Meeting overly aggressive latency constraints while operating in massive connectivity regimes with a low energy footprint and low computational effort and providing explicit security guarantees can be challenging. The massive deployment of low-end IoT nodes that are produced using diverse supply chains, non-homogeneous production processes, and have expected lifespans exceeding 10 years poses pressing questions regarding long-term IoT security.

Additionally, the extensive introduction of artificial intelligence (AI), machine learning (ML), and rapid advances in quantum computing will increase the attack surface of 6G systems, necessitating quantum-resistant solutions. Since quantum computers can break the most widely used asymmetric encryption protocols (RSA, El Gamal, and Diffie-Hellman), lightweight quantum-resistant security is necessary. In

August 2024, NIST published the first standards for digital signature (ML-DSA) and key encapsulation mechanisms (ML-KEM) for post-quantum cryptography[1]. However, the current lattice-based schemes might not be suitable for constrained wireless devices, since the required computations are still heavy[2]. Moreover, the security of these algorithms is based on conjectures regarding the hardness of the approximate shortest vector problem in module lattices, whilst there is currently some concern that new lattice reduction attacks exploiting the ideal lattice structure could be developed [4,5]. Therefore, there is still a need for lightweight quantum-resistant alternatives.

At the same time, the quality of security (QoSec) is expected to provide a flexible security framework for future networks. This framework will introduce different security levels and move away from the static security controls that are currently used. Meanwhile, the integration of communications and sensing, along with embedded and edge AI, can lay the groundwork for autonomous and adaptive security controls. Within this framework, physical layer security (PLS) schemes can be incorporated into 6G security protocols for the first time, introducing security controls at all layers while providing opportunities for lightweight, quantum-resistant security.

Introduction of PLS mechanisms in 6G networks has also been endorsed by the International Telecommunication Union (ITU) in [6], stating "There is a need to ensure security, and resilience when allowing for a legitimate exchange of sensitive information through network entities. Potential technologies to enhance security include those for RAN, such as distributed ledger technologies, differential privacy and federated learning, quantum technology with respect to the RAN, and physical-layer security technologies."

However, this exciting prospect does not come without challenges. Despite more than two decades of intense research interest in PLS, its incorporation into actual security products has been elusive, with a few exceptions in terms of RF fingerprinting (physec.de) and multi-factor authentication (silencelaboratories.com). Nevertheless, recent advances will enable the widespread deployment of PLS solutions in 6G, as discussed next.

1.2 Enabling Technologies and Added Value From PLS

The fundamental theoretical limits for the secure transmission of confidential information, the distillation of secrets from shared randomness, authentication exploiting physical unclonable functions, biometrics, and RF fingerprinting have long been studied and understood. In order, however, to bring these schemes to life, only today can we confidently make the case that some crucial conditions are met. In detail:

- Propagation conditions can be learned in an online, continuous mode by a trusted agent, e.g., an authenticated base station (BS), and this online "view of the channel" can allow us to identify which PLS solutions are pertinent without relying on arbitrary channel models.
- The channel can be engineered and controlled. In particular, the wide deployment of massive multiple-input multiple-output (mMIMO) systems at sub 6GHz and the envisioned deployments at mmWaves and THz bands, provide a concrete and provable scenario for the wiretap channel. Further enabling technologies include reflective intelligent surfaces (RIS).
- PLS technologies have matured in terms of technological readiness, e.g., localization will be a default service in forthcoming releases of 5G and 6G, we are expecting on-chip demonstrators

[1] https://csrc.nist.gov/publications/fips.

[2] Source: NIST Post Quantum Cryptography Forum, https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/dLe2k2H55MA

of wiretap codes for mmWaves, active attacks, e.g., on secret key generation, have been studied and mitigated, and physical unclonable functions have been embraced by industry.

- Softwarization, virtualization (ORAN, NFV, SDN), provides flexibility and adaptability, which is required for the deployment of PLS.
- Integrated communications and sensing will benefit PLS as an enabler of context awareness and alternative sources of entropy.
- The vision of zero-touch deployment can be facilitated by certain PLS schemes, e.g., location-based authentication.

On the road towards 6G, there are novel opportunities and potential new issues. As the attacker profiles evolve and the attack surface expands, we will move towards a new paradigm of smart and adaptive security that will be context-aware. PLS, being inherently adaptive, fits perfectly in this vision.

2 — Threat Model and Attack Surface

Threat modeling is an exercise in which a systematic analysis of potential security risks of systems is performed. Starting with the system's elements and weaknesses, a.k.a. attack surface, that could be targeted, it examines adversaries' capabilities and techniques they might leverage to cause negative impacts on the target system. Threat modeling focuses on potential adversarial actions that violate one or more of the system's security requirements and consequently impact the system's functional objectives. Threat modeling leverages understanding of the system and the security mechanisms to present well-articulated risk scenarios, accompanied by measurable metrics reflecting the likelihood and the potential impact should the risk scenarios materialize.

Performing a proper and systematic threat modeling for physical layer security (PLS) is necessary to better understand the applicable risk scenarios, elements, and impacts, and to better map the potential benefits of existing PLS approaches in risk reduction. Most importantly, this is critical for highlighting any existing gaps in the context of corresponding alternatives and compensating security controls.

We focus this chapter on PLS specific risk scenarios and outline the threat modeling approach, considering the existing security mechanisms and proposals.

2.1 Security Requirements

In general, secure services or protocols must meet a set of defined high-level security requirements. Those requirements establish a reference that facilitates describing cybersecurity risks and mitigations, including:

- Confidentiality, which describes the ability of the system/security mechanisms to ensure that only authorized parties are able to access and understand the information.
- Integrity, which describes the ability of the system/security mechanisms to enable detection of unauthorized changes or manipulation of the information.
- Availability, which describes the ability of the system/security mechanism to ensure services remain adequately available for use by authorized parties.
- Authentication and non-repudiation. Authentication describes the ability of the system/security mechanism to verify the unique identities of parties (user, device, system) before authorizing access to resources. Non-repudiation establishes the means to prove the origin and integrity of data such that a party cannot deny related actions.

Various models considered in PLS provide the mathematical framework to capture attacks that violate these requirements. Some of the models are able to capture some of these requirements jointly.

2.2 Threat Modeling

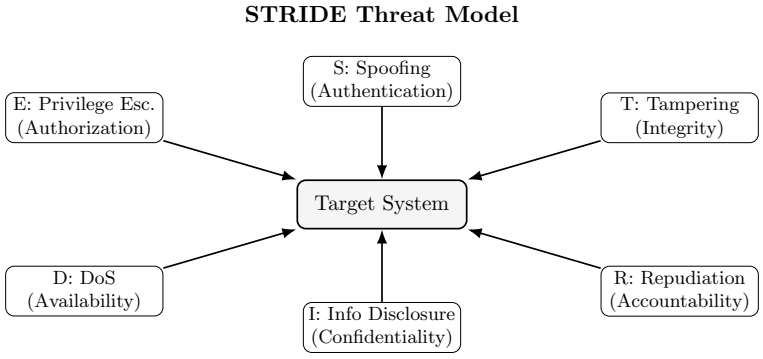
In this work, the adopted approach is based on existing threat modeling frameworks, which have been proposed and endorsed by various government agencies and standards bodies. Threat modeling involves the identification of potential risk scenarios that may be executed by specific threat actors, utilizing a variety of techniques and mechanisms, to cause an impact against a given business objective or target. By scrutinizing the attack surface of a system, threat modeling offers valuable insights for risk assessment and risk mitigation. Risk assessment, in turn, involves the evaluation of the likelihood of threats and their associated impacts, in order to gauge the potential magnitude of negative outcomes, either qualitatively or quantitatively. In summary, threat modeling provides a systematic approach to frame and validate assumptions on threat vectors and proposed mitigation approaches. Thus, it is vital to adopt a good threat modeling framework to help inform and scope subsequent research on PLS mitigation approaches and techniques. In this context, we will explore the most commonly employed frameworks, focusing on their suitability for use in a PLS setting.

2.2.1 Standard Threat Modeling Approaches

There are a variety of standard frameworks available to model the threats associated with PLS in mobile communication systems. Below, we will provide a brief overview of the most prevalent ones, with a more comprehensive discussion of each, as we believe that they may be beneficial in the context of PLS.

STRIDE

The STRIDE framework, developed by Microsoft, is commonly used. STRIDE is an acronym that stands for **S**poofing, **T**ampering, **R**epudiation, **I**nformation **D**isclosure, **D**enial of Service, and **E**levation of Privilege [1] as shown in Fig. 2.2.1.



This framework can be used to identify potential PLS threats, such as wireless jamming, eavesdropping, unauthorized access to mobile communication infrastructure sites, and physical tampering with devices or infrastructure. More specifically, the various stages can be analyzed in the following manner and illustrated using pertinent examples:

- Spoofing: is a threat that involves the imitation or replication of a legitimate entity, such as a user, device, or network, by an attacker to gain unauthorized access to the physical layer of mobile communications. For example, an attacker may create a fraudulent base station to intercept and manipulate mobile traffic.

[1] https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach

- Tampering: involves a form of physical manipulation of devices, or perhaps even infrastructure, to gain illicit access or alter communications traffic. For example, an attacker may connect a device to a base station to intercept or manipulate communications traffic.
- Repudiation: is a threat that involves an attacker denying responsibility for a security breach. For example, they may refuse to acknowledge culpability for exploiting PLS vulnerabilities on the mobile communications infrastructure.
- Information Disclosure: threats entail an attacker gaining access to sensitive information transmitted over mobile networks. For example, they may intercept unencrypted communications traffic to obtain access to confidential data.
- Denial of Service: involves an attacker's capacity to disrupt cellular services, such as using a jamming device to interfere with wireless signals.
- Elevation of Privilege: is characterized by an attacker extending gradually its initial set of privileges by exploiting vulnerabilities in the physical layer of mobile communications, gaining unauthorized access to a system or device. For example, an attacker may utilize a software-defined radio to impersonate a legitimate device and obtain unauthorized access to the mobile network.

PASTA

Another framework that can be useful in threat modeling for PLS is the **P**rocess for **A**ttack **S**imulation and **T**hreat **A**nalysis (PASTA)[2]. It follows a step-by-step approach to detect possible threats and their effects on the system, and then suggests countermeasures to handle them. PASTA can also be utilized to analyze threats to mobile infrastructure, such as attacks on base stations, and to evaluate the security of mobile devices themselves. The threat and vulnerability assessment process is conducted through a structured approach in PASTA. The following points offer a concise illustration of how an assessment would proceed, serving as an example:

1. Define the target system by identifying the specific physical layer components of the mobile communications system under review.
2. Identify potential threats that could threaten the PLS of the mobile communications system, such as wireless jamming or other similar attacks.
3. Assess the impact of each potential threat on the security of the physical layer of the mobile communication system.
4. Identify vulnerabilities that exist within the physical layer of the mobile communications system, which could be exploited by an attacker.
5. Assess the likelihood of exploitation of each vulnerability by an attacker.
6. Identification of countermeasures: to mitigate the risks associated with the identified threats and vulnerabilities.

DREAD

Moreover, the **D**amage, **R**eproducibility, **E**xploitability, **A**ffected Users, and **D**iscoverability (DREAD)[3] framework can be used to assess the danger posed by PLS threats in mobile communication systems.

[2] https://versprite.com/blog/what-is-pasta-threat-modeling/

[3] https://shostack.org/files/papers/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf

This framework considers the potential harm caused by a security breach, the probability of the breach being exploited, the number of affected users, and the ease of detecting the breach. Thus, it offers a structured approach to assessing the risk associated with security threats in the physical layer of mobile communications systems. The framework comprises several key components, namely:

- **D**amage assessment: which involves evaluating the potential impact of a PLS breach, such as loss of sensitive information or disruption of mobile communication services.
- **R**eproducibility evaluation: which measures the likelihood of an attacker repeating the security breach of the physical layer.
- **E**xploitability description: which determines the level of ease with which an attacker could exploit a vulnerability in the physical layer of the mobile communications system.
- **A**ffected user estimation: which estimates the number of users who would be impacted by the security breach within the system, such as all subscribers of a mobile service.
- **D**iscoverability measurement: which determines the ease of discovering the vulnerability.

In summary, there exist various standard frameworks for threat modeling that can evaluate the PLS in mobile communication systems. These standards enable the identification of potential threats, the assessment of associated risks, and the proposal of effective countermeasures to reduce risks. The appropriate selection of a threat modeling standard for PLS necessitates an understanding of the system-specific requirements and objectives. Different standards have unique methodologies, strengths, and weaknesses, and can be applied to diverse threats and systems. Hence, while choosing a threat modeling standard, one must consider factors such as the scope of the analysis, system complexity, level of detail required, and available resources. Furthermore, it is recommended to review the existing literature and case studies to determine best practices and potential challenges.

NIST threat modelling

The NIST threat modeling framework constitutes a rigorous methodology for systematically identifying, characterizing, and mitigating threats to information systems within the broader discipline of risk management. Grounded in publications such as NIST SP 800-154, the framework advocates for a disciplined progression that begins with a precise definition of the system boundaries, operational context, and critical assets. Subsequent decomposition of the system into its constituent components and data flows enables a granular understanding of potential attack surfaces. This analytical foundation facilitates the structured identification of threats by considering adversarial capabilities, intent, and likely attack vectors in conjunction with system vulnerabilities. The framework further prescribes the evaluation of threats in terms of both likelihood and potential impact, thereby supporting risk-informed prioritization of defensive measures. By embedding threat modeling into the system development life cycle (SDLC) and aligning it with the NIST Cybersecurity Framework, the approach ensures that security considerations are not relegated to reactive measures but are instead integrated proactively and iteratively. Ultimately, the NIST framework advances not only technical robustness but also organizational resilience, establishing a repeatable, evidence-based process for anticipating and mitigating an evolving spectrum of cyber threats.

2.2.2 MITRE Frameworks

The MITRE Corporation has developed two cybersecurity frameworks, namely MITRE ATT&CK and MITRE FiGHT, to enhance the security posture of organizations. Although both frameworks aim to achieve this objective, they differ in scope. The FiGHT model is designed based on the ATT&CK

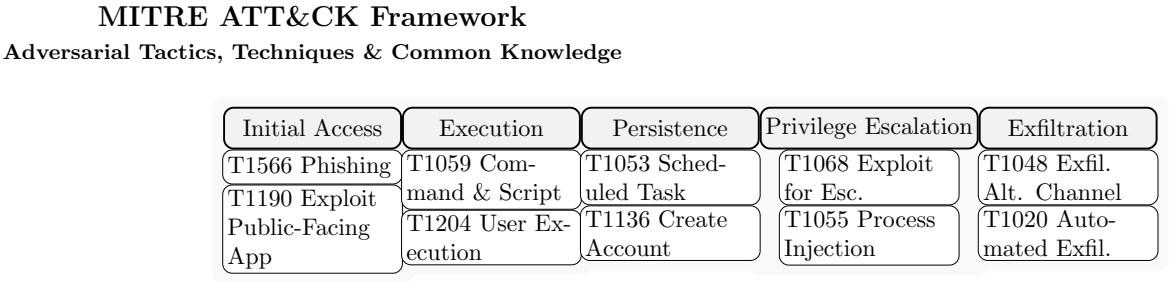


Figure 2.1: Simplified representation of the **MITRE ATT&CK Framework**, illustrating the relationship between adversarial *tactics* (high-level attack objectives) and representative *techniques* (specific methods used to achieve those objectives). The framework models real-world cyberattack behavior from initial access through execution, persistence, privilege escalation, and data exfiltration.

framework and serves as a supplementary approach to the methodologies and procedures employed in ATT&CK.

MITRE ATT&CK has a broader coverage of the entire attack lifecycle for various scenarios, while MITRE FiGHT currently focuses primarily on the context of fifth-generation (5G) networks. Therefore, the suitability of each framework depends on the specific needs and objectives of the organization.

In general, both frameworks are essential tools for improving cybersecurity. When evaluating risks in PLS, both frameworks should be considered to achieve a comprehensive security posture. However, implementing this approach may be challenging in the current state of the frameworks. To achieve PLS analyses, organizations may have to make an initial effort to utilize MITRE FiGHT or other approaches, as dynamic threat modeling for core networks in 5G is already achievable using the new Tactics, Techniques, and Procedures (TTPs) knowledge base for MITRE ATT&CK.

MITRE ATT&CK

The MITRE ATT&CK Framework, known as **A**dversarial **T**actics, **T**echniques **&** **C**ommon **K**nowledge [4] shown in Fig. 2.1 exemplifies a structured matrix of cyberattack behavior — how real-world adversaries compromise and operate within systems. It is a globally recognized framework utilized to elucidate the tactics and techniques employed by threat actors in cyber attacks. It is a framework that classifies cyber threats based on seven stages of the attack lifecycle, which include reconnaissance, initial access, execution, persistence, privilege escalation, defense evasion, credential access, detection, lateral movement, collection, exfiltration, and command and control. While primarily designed for use in cybersecurity, this framework can also be tailored for security research at the physical layer of mobile communication systems. Below are several ways in which MITRE ATT&CK can be employed for security research in mobile communication systems at the PLS:

- Mapping threats and attack techniques:
  A possible application of the framework in security research for the physical layer involves mapping threats and attack techniques to different stages of mobile communication systems. This can enable researchers to grasp how attackers can exploit vulnerabilities in the system's physical layer and develop countermeasures to mitigate such attacks.
- Vulnerability identification:
  MITRE ATT&CK can aid in identifying vulnerabilities in the physical layer of mobile communication systems. By linking attack techniques with specific vulnerabilities in the system,

[4] https://attack.mitre.org/

researchers can determine areas that need to be strengthened to improve overall system security. However, an initial declaration of the fundamental vulnerabilities of the PLS system is necessary to establish more detailed statements.

- Development of countermeasures:
  The framework can be leveraged to develop countermeasures that can prevent attacks on the physical layer of mobile communication systems. By understanding how attackers can exploit system vulnerabilities, researchers can devise strategies to deter such attacks and enhance system security.
- Testing security controls:
  Attack simulations can be conducted to test the effectiveness of security controls in mobile communication systems. Through such tests and by assessing the efficiency of different security controls in preventing these attacks, researchers can identify areas where the system can be improved and refine security controls to offer better protection against attacks.
- Sharing best practices:
  Sharing the best practices and knowledge regarding PLS in mobile communication systems is an important aspect of this framework. By developing a common framework for understanding threats and attack techniques, researchers and practitioners can exchange knowledge and work together to develop effective security strategies for mobile communication systems.

In essence, MITRE ATT&CK presents an opportunity to investigate the PLS of mobile communication systems through the delineation of threats and attack techniques, identification of vulnerabilities, development of countermeasures, testing of security controls, and exchange of best practices. This framework offers a systematic approach to comprehending and mitigating PLS threats that may arise in mobile communication systems.

MITRE FiGHT

MITRE FiGHT (**Fi**ve **G** **H**ierarchy of **T**hreats)[5] is a security framework that provides a comprehensive and proactive approach to detect, analyze, and mitigate security threats in mobile communication systems. Specifically, it can be utilized to identify and counteract threats targeted at the physical layer of the communication network, including wireless signals exchanged between connected devices and base stations.

This framework presents an opportunity for organizations to evaluate the confidentiality, integrity, and availability of both 5G networks and the applications built on top of them.

MITRE FiGHT is essentially based on MITRE ATT&CK and serves as a powerful tool that empowers security professionals to improve the physical security of mobile communication systems. To achieve this, similar to the MITRE ATT&CK approach, key use cases such as defensive gap assessment, behavioral analytics to detect suspicious activity, adversary emulation, or red teaming can be performed on the framework matrix to provide insights to 5G infrastructure operators.

The framework matrix identifies and classifies tactics used in attacks in relational columns, where for each column, tactics can be of three types: theoretical, proof-of-concept, or observed in the wild. The columns address multiple *genres* of tactics, including Reconnaissance, Initial Access, Execution, Privilege Escalation, Collection, Impact, and more.

As MITRE FiGHT is a fairly recent framework oriented towards 5G, the theoretical and proof-of-concept tactics are overly represented compared to the observed ones. This framework is in an active

[5] https://fight.mitre.org/

development state, and each security researcher, engineer, or infrastructure operator is encouraged to participate in its development through observations, analysis, or attack scenario replays.

Next, we will make a reference to threat semantics as threat semantics and threat modeling are deeply interconnected. Semantics provides the formal language and conceptual precision needed to represent threats in a structured, analyzable manner, while modeling applies those representations to practical security analysis.

2.2.3 Threat Semantics

Threat semantics is a discipline intersecting with computer science that focuses on the examination of threats to computer systems and networks and the methods and techniques used to identify, evaluate, and address these threats. It is a multidisciplinary field that encompasses concepts from computer science, security, psychology, sociology, and economics. By defining threats in terms of their actors, intentions, capabilities, and potential system impacts, threat semantics enables consistent interpretation across different contexts and tools. Threat modeling then leverages these semantic structures to identify, classify, and reason about potential attack vectors within a system, ensuring that analysis is not ad hoc but grounded in well-defined meaning. In this way, semantics underpins the rigor and repeatability of threat modeling, transforming abstract security concerns into systematically analyzable risks.

Threats to computer systems and networks may take various forms, including malware (viruses, worms, trojans, etc.), phishing attacks, denial of service attacks, insider threats, and physical attacks. Threat semantics aim to strengthen the understanding of these threats, their mode of execution, and strategies for prevention or mitigation. To identify threats, threat analysts can use a variety of tools and techniques such as network scanners, vulnerability scanners, threat intelligence, threat hunting, and log analysis tools. They may also conduct risk assessments, penetration testing, and other types of security testing to detect potential vulnerabilities and weaknesses in a system. Once threats have been identified, threat analysts can employ a variety of techniques to mitigate or prevent them, including implementing security controls, establishing security policies and procedures, and educating users on how to recognize and avoid potential threats. Threat semantics aim at keeping coherent semantic models and terminologies in every step, bringing consistency for all involved actors. As such, it is a crucial field in the realm of computer security as it assists organizations and individuals in protecting themselves against the various threats that exist in the online world.

Following different approaches to threat semantics [7], we assume that a threat model must have deterministic semantics and clear ontologies for the following elements:

- Threat actor: identifying the applicable threat actor helps clarify and confirm assumptions into their capabilities, tactics, objectives, and resources. For example, if we are considering an insider threat actor, then it is safe to assume that they have physical access to the system and some internal knowledge and potentially access privileges to parts of the system.
- Threat scenario: understanding the threat scenario reveals a sequence of attack steps that can be stopped by defense and security mechanisms. When the defense mechanisms fail to stop a specific threat scenario, vulnerabilities will appear. Multiple threat scenarios can co-exist toward the same goal.
- Business objective or target: identifying the target of a threat scenario, whether it be a resource or mechanism a threat actor aims to steal, corrupt, or disrupt, will shed light on the motivation of an attacker.
- Tools: understanding through traces or analysis the different tools used by a threat actor will

refine the understanding of the threat scenario and the design of the threat model in general. Not only will this shed light on actor capabilities, but also enable the defender to reliably detect the attacker's tools, regardless of minor functionality changes to the tool.

2.2.4 Example Scenario

We consider a hypothetical scenario in which physical layer authentication (PLA) and secret key generation (SKG) are employed in order to illustrate the threat modeling and semantics discussed above. PLA and SKG can be combined in the physical layer authentication (PLA) and key agreement (AKA) protocol, referred to as PHY-AKA for simplicity. We assume a smart factory setting in which both low-end, power, memory, and computing-constrained devices are present, as well as high-end devices such as autonomous robots. The devices are connected to any of the multiple access points equipped with massive multiple-input multiple-output (mMIMO) arrays and can further engage in direct machine-to-machine (M2M) type communication under severe delay constraints (e.g., ≤ 1 ms).

As a special note regarding the suitability of PLA and SKG under very aggressive delay constraints, we note that:

- For PLA based on fast positioning approaches, including fast angle of arrival (AoA) estimation, recent variants of the multiple signal classification (MUSIC) algorithm have been proposed. As an example, for a 100 antenna element automotive radar mMIMO scenario, wall-clock runtimes of less than 0.4 milliseconds have been reported in [8]. It can be envisioned that such technologies can be incorporated in a smart factory setting.
- For fast SKG, the use of long short-term memory (LSTM) networks can decisively speed up privacy amplification, aided by an enhanced feature space including physical attributes of the environment (line-of-sight, LoS or non LoS, NLOS, slow fading vs fast fading, etc.). As an example, for the experimental SKG campaign in [9] with a symbol period of Ts = 17.1875 μs, a $K = 16$ filter-bank along with a $Q = 3$-bit quantizer, suffices for real-time estimation of the hashing rate in less than 0.2 msec with a 500 sample LSTM network.

We assume that PLA and SKG are jointly employed for PHY-AKA between any device and a given access point, as well as for device pairing when engaging in M2M-type communications. We want to model the threat that a mobile adversarial actor presents inside this limited geographic area, mounting several possible attacks on the PHY-AKA. In this given scenario, we follow the NIST threat modeling framework:

- **Identification of the data assets of interest.** We consider the threat actor's motivation to i) eavesdrop on exchanged data; ii) impersonate legitimate devices or access points; iii) disrupt communication links (denial of service). Here, we consider out of scope the collection of metadata related to device communications or gaining physical access to the devices themselves.
- **Identification of attack vectors.** Given an attacker able to coordinate multiple malicious devices with advanced hardware capabilities (e.g., mMIMO arrays) able to perform signal collection and analysis, along with tailored emissions at any time, we identify multiple attack vectors on the PHY-AKA as follows:
  1. By transmissions of carefully designed pilot sequences and signals, the attacker(s) aim at forging their identity and being authenticated as legitimate devices.
  2. By the transmission of carefully designed injection signals, the attackers aim at controlling the keys generated between the devices and the access points and therefore compromise confidentiality in subsequent sessions.

3. By perturbing signal exchanges with carefully designed signals, the attacker aims at disrupting the PHY-AKA by bringing down the wireless links' quality.

- **Threat mitigation and solutions.** Given the previously described threat vector, the following statements regarding possible mitigation approaches can be made:

  1. For the impersonation attack, the choice of the PLA approach used impacts whether mitigation is possible or not. More specifically, it has been shown in literature that the channel impulse response, RF fingerprints, the frequency channel response, and the AoA when analog array MIMO is used are not robust against impersonation attacks [10], [11]. On the other hand, digital array MIMO systems using the AoA as an authentication feature are robust against impersonation [12].

  2. SKG with deterministic pilot sequences is vulnerable to injection attacks. On the other hand, SKG with randomized pilot sequences is robust against injection attacks [13].

  3. Wireless jamming can, in general, lead to poor quality links, unless frequency hopping or beamforming are used as mitigation approaches [14].

- **Analysis of the model.** Our analysis of the model reveals that, depending on the implementation of the PHY-AKA an attacker might be able to downgrade the security of the assessed system. We identified three different attack vectors for the chosen implemented mechanisms. For each of these vectors, we identified countermeasures in the form of alternative implementations of the same mechanisms. According to the state of the art, these countermeasures fully cover the proven vulnerable attack vectors.

2.3 Known Attacks on PLS Schemes

In the next part of our systematic analysis of potential security risks we focus on the attack surface of PLS schemes. Understanding the attack surface requires a systematic examination of the attack vectors that exploit possible present vulnerabilities. Attackers can target various aspects of the physical layer, ranging from passive collection of signals to active manipulation of channel properties in order to compromise confidentiality, integrity or availability. We categorize these attacks in four categories, passive, active without disrupting communication, active preventing communication and hardware-targeting. This classification delineates the most prevalent and impactful attacks on PLS schemes, analysing their mechanisms, implications and the research questions their counter-measures raise.

2.3.1 Passive attacks

Passive attacks on the PLS involve the interception and monitoring of the correlation between the eavesdropped channel properties and the legitimate radio frequency signals exchanged between two entities, without actively altering or disrupting the transmission. These types of attacks can utilize software-defined radios to analyze the communication channel, and are often difficult to detect due to the lack of overt actions taken by the attacker.

Eavesdropping in Keyless Transmissions

There has been a lot of focus on eavesdropping attacks for wiretap channels; in essence, the capacity-equivocation regions for various channel models account for exactly this type of passive attacker. Today, with the introduction of transmissions at higher frequency bands over reduced distances, the use of an ultra massive number of antennas for pencil sharp beamforming, or alternatively the use of

visible light communications or similar, there is hope that it is possible to use wiretap coding for zero information leakage. However, we note the following open issues:

- Even when employing a very large number of antennas, there are beam sidelobes with non-negligible energy. Therefore, up to now, it is not possible to fully disengage the use of wiretap coding from assumptions regarding the positioning of the eavesdropper or channel state information of the eavesdropper. When the attacker is active, estimation of the channel state information of the attacker may still be possible if the attack is unidentified. Probabilistic secrecy maps may allow for characterization of secure (or insecure) regions in which wiretap coding approaches can successfully be employed [15, 16].
- It remains to be seen whether the use of metamaterials and reflective intelligent surfaces (RISs) can indeed alleviate problems stated above; initial results seem promising.
- The use of cell-free MIMO might be another hurdle in this direction, i.e., channel hardening without sharp beamforming could favour potential eavesdroppers.
- Although wiretap coding based on information-theoretic principles will result in zero information leakage for sufficiently long blocklengths, there will always be information leakage for shorter blocklengths [17]. Such small but non-negligible leakage needs to be taken into account when it comes to practical implementation.

Eavesdropping in SKG

Small-scale fading, e.g., assuming a Rayleigh channel, is assumed to decorrelate over distances of the order of a few wavelengths, i.e., around 10-20 cm for a standard sub-6GHz system. However, shadowing is known to be spatially correlated, and further, path loss is in principle predictable for a given environment. Therefore, a first issue arises due to correlations and spatial dependencies between the observations at legitimate and adversarial nodes.

In his study, Edman *et al.* [18] discussed the security of physical layer key extraction techniques used to derive a shared symmetric cryptographic key between two wireless devices based on the principle of channel reciprocity or strong signal envelope correlation. Results show that there is a strong correlation between the measurements observed by the attackers and that the attackers are able to exploit such correlations to derive parts of the key extracted between the two devices. Therefore, the need for accurate estimation of the conditional min entropy in a given environment is paramount. As an example, in [9], an eavesdropper at a distance of one wavelength (8 cm) from the legitimate node was considered, and robust key extractions were demonstrated.

2.3.2 Active attacks – man in the middle (MITM)

MITM attacks on keyless transmission

Such attacks could be implemented as a form of malicious pilot contamination during beamforming training and have been demonstrated experimentally, i.e., an adversarial node can divert transmission to itself. Approaches to overcome these attacks could incorporate user localization through multiple sensing inputs, e.g., radar and camera, to aid the training. An attacker can also use RIS / metamaterials to impact the signal-to-noise ratio at the legitimate receiver.

MITM attacks on SKG

Since the early days of SKG, it has been demonstrated experimentally that it is possible to perform "injection" attacks, i.e, the insertion of strong known signal components at both legitimate users.

In the first demonstration of such an attack, a MITM roughly in line-of-sight mid-way between the legitimate nodes transmitted a strong signal, received at roughly the same level by the legitimate nodes. If such components are not identified and removed, the output of reconciliation SKG decoders can be partially controlled by the attacker. This raises the possibility of a brute force attack at the *input* of the privacy amplification (conditional min entropy estimation cannot account for this). Such attacks can be overcome with pilot randomization techniques during advantage distillation, reducing the injection attack to a jamming attack [19]. In Fig. 2.2 we recap the SKG procedure and in Fig. 2.3 we demonstrate the injection attack during the advantage distillation.

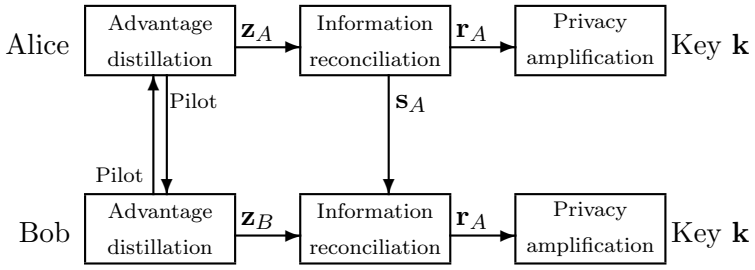


Figure 2.2: Secret key generation process between Alice and Bob.

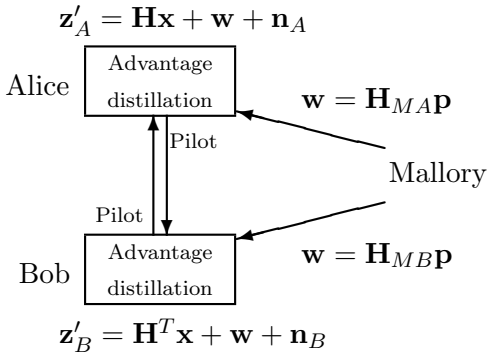


Figure 2.3: Injection attack performed by Mallory: While Alice and Bob exchange pilot signals $\mathbf{x}$ over a Rayleigh fading channel with realization $\mathbf{H}$ Mallory injects a signal $\mathbf{p}$, such that the received signals at both Alice and Bob coincide $\mathbf{w} = \mathbf{H}_{MA}\mathbf{p} = \mathbf{H}_{MB}\mathbf{p}$.

MITM attacks on localization

Localization utilizing multiple carriers but not multiple antennas has been shown to be prone to impersonation attacks. The use of higher-dimensional data for positioning, e.g., including the AoA [20], [21], multiple independent sources for localization estimation, etc., can be incorporated towards robust and trustworthy localization. As an example, using 2 uniform planar arrays (UPAs) receivers, we can inadvertedly localize a transmitter [22] (accuracy depends on the number of antennas and SNR), as shown in Fig. 2.4.

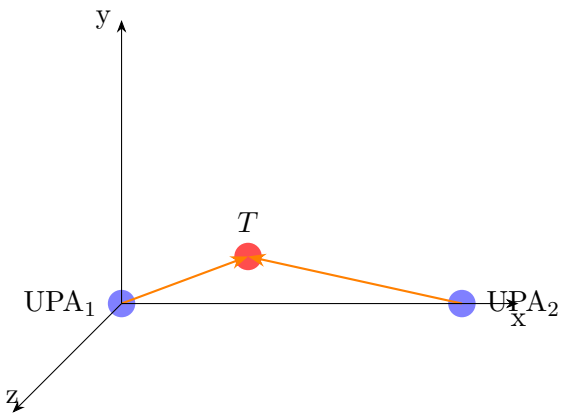


Figure 2.4: Two UPAs with AoA only. Transmitter at the intersection of AoA lines.

MITM attacks on RF fingerprinting and channel-based authentication

Authentication based on the physical layer relies on either identifying unique imperfections in signals transmitted by radio devices to isolate their fingerprint or on the exploitation of the channel characteristics as a fingerprint of the link. Recent results demonstrated that with careful selection of the signal, an unauthorized transmitter can still be classified as authentic using a deep-learning-based approach. However, the attacker needs information about the signal sent from the authenticator and the modulation and pulse shaping used by the authorized transmitters.

MITM attacks on PUFs

Physically unclonable function (PUF) is a hardware-based security primitive for the purpose of secret key generation, identification, or authentication. Cloning attacks have been considered as one of the major threats to weak PUFs. In a cloning attack, it is not required to clone the PUF in complete detail; rather, it is sufficient to clone the same challenge response pair (CPR). On the other hand, strong PUFs are not susceptible to cloning attacks. The relevant attack on the strong PUF belongs to the category of modeling attacks, with Machine learning (ML) one of the favorite tools to carry out modeling attacks. Electrical strong PUF, the general Arbiter PUF, has been found to be prone to ML-based attacks. This does not mean that all strong PUFs are prone to attacks, and by adding additional non-linearity, one can increase the complexity of designing such attacks.

MITM attacks on position privacy

The integration of sensing and communications may rise serious privacy concerns, as adversaries may leverage sensing information to violate privacy of users and launch active attacks. Thus, a careful design is of paramount importance to prevent location, tracking, and even imaging of indoor activities of vulnerable targets. For instance, MIMO-based dual-functional radar and communication (DFRC) systems based on transmit beamformer design present advantages in comparison with waveform designs, by allowing communication and sensing to use their individual waveforms, thus ensuring higher data rates and improved radar performance. However, DFRC transmit beamformers contain information on the position of the targets, which is sent to communication users. It was shown in [23] that an adversary, acting as a communication user, can infer the location of targets with reasonable accuracy given the transmitted precoding matrix; thus, further research is required to tackle privacy concerns in DFRC systems.

By tracking the movements of users, an attacker may obtain sensitive information such as health

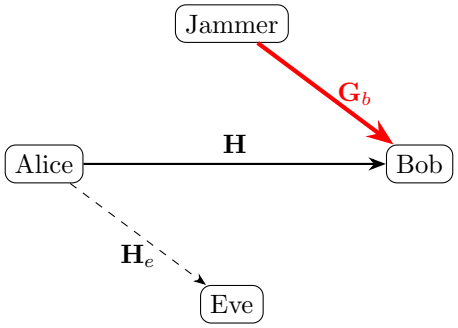
and work conditions, acquaintances, and belonging to groups and associations. Current and future communication networks are designed to obtain more precise locations of users, with an accuracy that has gone from hundreds of meters to centimeters over the last 20 years. Indeed, due to the broadcast nature of the wireless channel and the possibility of localizing users based on their transmitted signals, localization can be performed not only by network operators but also by external attackers. In such a scenario, operating at the physical layer where the wireless signal originated is a good option to prevent localization and protect user privacy.

A recent perspective paper [24] has, for example, examined the various location privacy vulnerabilities of 5G cellular networks and highlighted several solutions that can be adopted in future standard releases. At the physical layer, when using multiple antennas, the transmitted signal can be beamformed to mask at the receiver the angles of departure, thus preventing triangulation-based localization [25]: this, however, requires the knowledge of the channel from the transmitter to the receiver. Another approach is based on the concept of signal relaying, where the user willing to protect his privacy transmits low-power signals to dedicated relays or nearby users (in both cases, trusted), which in turn retransmit (possibly by multiple hops) the packet to the intended destination (e.g., the base station of a cellular system), [24]. In this case, the transmitted signal remains confined in a smaller area, thus limiting the location privacy leakage.

2.3.3 Active attacks – Jamming attacks

Jamming attacks on keyless transmission

Considering attacks on critical IT infrastructure such as hospitals, power plants, traffic control, etc., becomes increasingly important, [26]. As many relevant communication channels of interest, such as the wireless channel, are inherently vulnerable to jamming attacks at the physical layer (denial of service at the physical layer). The arbitrarily varying wiretap channel provides a suitable model for such jamming attacks and provides information theoretic results and insights on how much information can be transmitted reliably and securely, even in the presence of active and passive adversaries [27,28]. Jamming attacks result in a severe reduction in the corresponding transmission rate. If the adversary is able to completely disrupt the legitimate communication, it is a so-called denial-of-service (DoS) attack [29–34], exemplified in Fig. 2.3.3.



Jamming attacks on SKG

Key generation rate rapidly decreases with increasing attacker signal strength used for jamming [30]. However, such attacks can be detected at the legitimate user, while coordinated jamming to interfere with key exchange protocols is also possible [31,35,36]. Jamming during channel probing phase called "reactive jamming" - force low or high receive signal strength indicator (RSSI) values, recover up to 47.4% of the generated key [31]. Pilot randomization can be used to reduce the impact of injection attacks on the key generation rate. *Session hijacking* attack is another category of jamming attack,

where the attacker injects a high-power signal, and the legitimate user and attacker end up agreeing on a secret key [37].

Jamming attacks on positioning

Jamming attack is one of the major security threats to global navigation satellite systems (GNSS) such as GPS, and it can impact the services of IoT systems that rely on time, location, or navigation information. This fact can be used by attackers, such as jammers, to disrupt the location services. Besides jamming attacks, GNSS is susceptible to spoofing attacks. In the existing literature, it has been shown that commercial as well as military receivers are prone to spoofing attacks. Most of the receivers need to be very sensitive to receive the weak signals coming from the satellites. To carry out a successful spoofing attack, one of the requirements is to acquire knowledge of the target receiver antenna's position and velocity. Without this knowledge, spoofing attacks can be detected easily.

2.3.4 Supply chain attacks – Hardware trojan attacks

Over recent years, the risk of analog/RF hardware Trojan attacks has been explored in wireless networks. For the hardware Trojan attack, the malicious entity is residing in the analog/RF front end of the device. The hardware Trojan has been implemented either during the design or during integrated circuit fabrication.

As a result of the disaggregation and increased complexity of 5G wireless networks, equipment vendors and carriers rely more and more on a diverse set of components manufactured across the globe. While this global electronic supply chain allows for controlling the costs, it also introduces security vulnerabilities. One particular concern is the ability of third-party manufacturers to insert hardware trojans into the RF chain. Unlike security attacks launched from the outside, such as eavesdropping or jamming, the hardware trojan is able to control the operation of the radio itself, potentially leading to rogue transmissions to disrupt the network, or leaking/stealing of sensitive information. Threat model related to amplitude-modulating analog/RF hardware Trojan circuits and its countermeasures have been previously discussed [38].

3 — Use Cases

This part gives an overview of relevant use cases for physical layer security (PLS), with a description of the addressed threats and the security countermeasures implemented at the physical layer. We also discuss the main pros and cons of the PLS solutions when compared to other approaches. The chapter showcases five use cases, namely: 1) authentication and spoofing detection, 2) positioning integrity, 3) secret key generation, 4) jamming detection and rejection, and 5) geofencing and confidentiality. We then describe three specific application domains where PLS solutions can be of special interest: heterogeneous access, visible-light communications, and backscatter communications.

3.1 Authentication and Spoofing Detection

Message authentication is a security service by which, upon reception of a message, a device verifies the identity of the message sender. The attack against authentication is impersonation (or spoofing), wherein the attacker forges messages claiming to be another sender.

PLS offers mechanisms for message authentication based on the physical properties of the channel over which the message is transmitted. The basic assumptions are: a) different users have different channels (because they are in different positions with respect to the receiver), and b) the channel characteristics do not change over time. The first assumption is typically well-verified as long as users are distant by at least a few wavelengths. The second assumption is strong and can be replaced by the weaker assumption that the channel is changing slowly over several message transmission intervals.

Under the two hypotheses, a tag-based authentication approach can be deployed, comprising two steps: the tag *association*, by which a tag is associated with a user, and the tag *verification*, by which the authenticity is verified by detecting the tag. For PLS authentication, the tag is a set of channel features satisfying the above hypotheses. Therefore, upon reception of a first message, the channel features are estimated, associated with the legitimate transmitter, and stored at the receiver (tag association). Then, the channel features are estimated over a message to be authenticated; the features are compared with the stored ones: if they match, the message is authenticated, otherwise not (tag verification). Note that for the tag association phase, some other authentication techniques are needed (e.g., based on cryptographic approaches at higher layers) to ensure that the channel features of the legitimate user, rather than those of the attackers, are stored. The whole process is similar to the verification of signatures on bank cheques: the bank has stored the signature of its customers (in front of a bank officer, who has previously identified the customer by other means), and the,n upon reception of a cheque, the new signature is compared with the stored one for identity verification.

Application examples: Physical-layer PL authentication provides a lightweight solution that can be suitable for authentication messages between Internet of Things sensors and devices with energy constraints. It is useful in contexts where access to infrastructure for the exchange and renewal of keys for encryption-based authentication is problematic. It also enables the detection of spoofing attacks

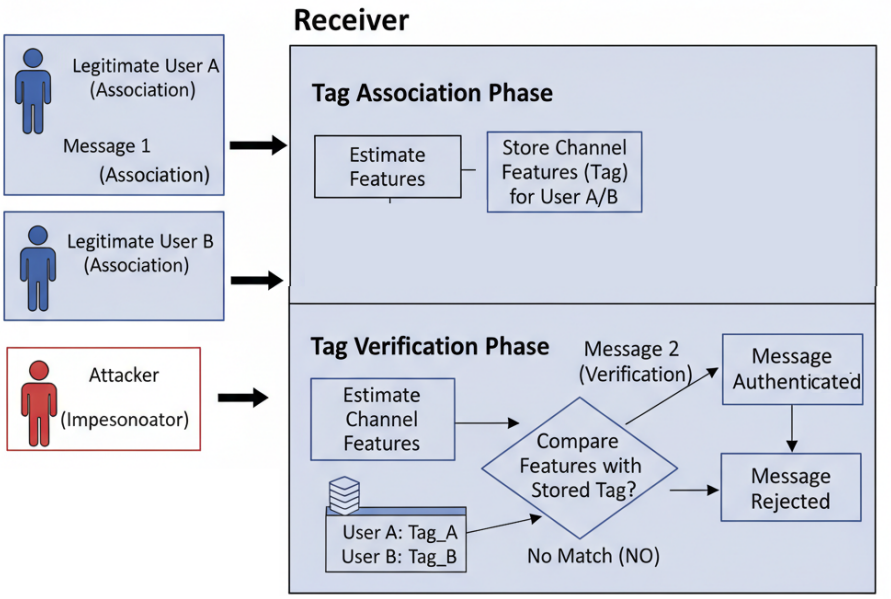


Figure 3.1: Physical-Layer Authentication diagram.

of global navigation satellite system (GNSS) signals aiming at altering the position estimated by a victim receiver. It can be used at the early stage of a communication process, with constraints on the use of channel resources. For example, PL authentication can be deployed to identify a rogue base station in a cellular network by checking from early transmissions that the transmission channel has well-known features. A few companies are already providing products, including PL authentication by channel fingerprinting.

Pros of PLS authentication: The main advantage of PLS authentication is that it does not require additional signal exchanges (such as keys or cryptographic protocols overhead), thus it is suitable for low-rate low-energy communications. The engineering community has investigated it extensively, and its definition and characterisation (including performance metrics) are simpler than those of other security mechanisms. A further advantage is that it operates at the physical layer, which is the first layer of a communication protocol: a non-authentic message can then be quickly discarded (even before its complete reception) by the receiver, avoiding useless computations. Such a feature can be particularly useful in energy-constrained devices. It also contributes to withstanding denial of service (DoS) attacks, since if the attacker does not pass the authenticity verification, the receiver's resources are not exhausted.

Cons of PLS authentication: Although PLS has been well studied in the literature, wider field tests may be needed before implementation to establish its accuracy in realistic scenarios and include not only the radio propagation characteristics but also the peculiarities of the transmitting and receiving devices. Moreover, attacks based on more sophisticated tools (e.g., antenna arrays or ray tracing algorithms) should be better investigated. Lastly, privacy issues should be better considered since PLS authentication obtains a fingerprint of both the transmitter and channel.

3.2 Positioning Integrity Solutions

Geolocation is a key component of fifth and sixth-generation (5G and 6G) cellular networks. Some of the targeted applications using geolocation are safety-critical; thus, it is necessary to ensure the validity of the position information before exploiting it. Such applications include, in particular, automotive,

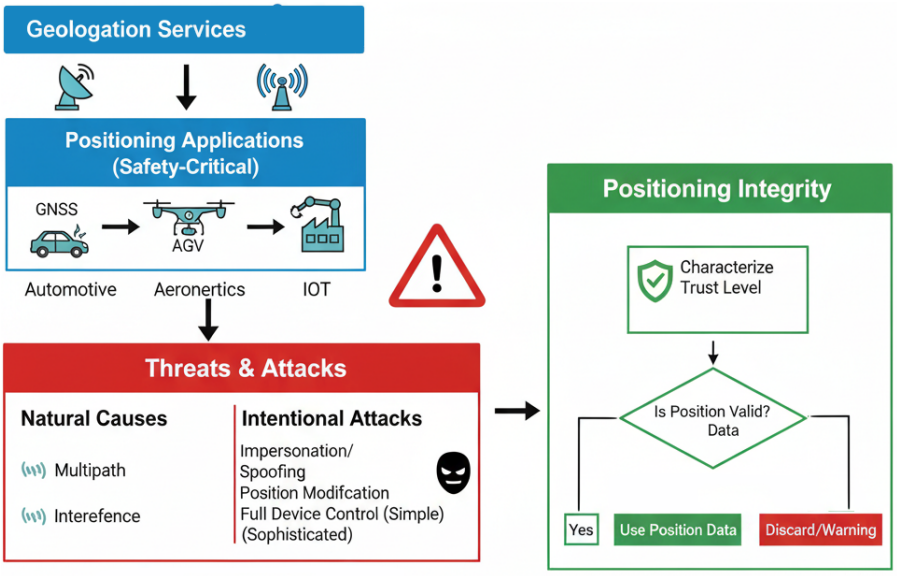


Figure 3.2: Position integrity flowchart.

aeronautics, and IoT, where human lives are at stake. The objective of positioning integrity is to characterize the level of trust for each calculated position so that the user can decide how to use the position information.

Integrity is a well-known domain in both civil and military aeronautics, which are used to resort to GNSS. However, the mechanisms used for several decades may not be fully effective against future sophisticated threats. Furthermore, 5G and 6G define positioning methods using base stations instead of or in addition to satellites. This opens up new angles of attack and requires new countermeasures. New threats include natural causes like multi-path or interference, as well as intentional attacks, the most classic being the impersonation of legal transmitters by spoofers. These attacks, in their simplest form, modify the calculated position, and in their most sophisticated form, can take full control of the device. The first category of attack results in a modification of the position calculated by the device, possibly resulting in a crash in the case of a car, unmanned aerial vehicle (UAV), or automated guided vehicle (AGV). The latter category of attack can have even more dramatic consequences when applied, for example, to missiles or armed drones.

A first countermeasure consists of analyzing the coherence of all information sources and eliminating the outliers. This method is effective against multipath, synchronization errors, as well as spoofing. Also, time and angle of arrival measurements and information collected with other technologies (WiFi or Bluetooth) can be combined for this end. About spoofing attacks, one approach consists of authenticating the ranging signal sources (using PL authentication solutions as described earlier), and making replay attacks ineffective, while preserving interoperability with the devices that do not support authentication. Watermarking techniques, consisting of applying small perturbations on the signal driven by a secret key, and then detecting such perturbations at the receiver, can also be used to authenticate the signal.

Application examples: Wireless transmissions are subject to various disturbances due to the transmission channel (multi-path and propagation) as well as interference. Localization is vulnerable to these problems, as much for satellite positioning as for positioning by terrestrial means. About spoofing, consisting of impersonating one or several authentic signal sources, several cases of attacks have been reported, mostly in the military domain. They are typically aimed at taking control of devices.

Pros of PLS positioning integrity: Considering that location perturbations, whether from natural causes or intentional attacks, affect the physical layer, it is natural to think that countermeasures should also operate at the physical layer. These methods exploit spatial processing (beamforming) as well as the analysis of the channel impulse responses or the coherence of the measurements (such as ranging and estimation of the angle of departure/arrival).

Cons of PLS positioning integrity: To improve the integrity, it may be necessary to combine the methods at the physical layer with others using information sources such as GNSS or cameras. This will require the integration of PLS solutions with methods operating at higher layers.

3.3 Secret Key Generation

In wireless communications, channel state information (CSI) can be used as a random number generator, as its state depends on multiple reflections and scattering from objects in the radio environment. Particularly at high frequencies, small changes in the location or orientation of objects (including the transmitter) may result in substantial changes. Thus, by observing the mutual CSI, a transmitter and a receiver may obtain a random number that is confidential to them, as an attacker in another position will experience a different (partially independent) channel. Such a procedure is denoted as secret key generation (SKG). Note, however, that in principle, if an attacker had perfect knowledge of the physical environment, antenna patterns, and locations of the legitimate transmitter and receiver, he may compute the state information of the channel between the legitimate devices. In practice, though, such accurate ray tracing is nearly impossible, and the channel can be safely considered to be random. Another advantage of using the wireless channel as a random source is that it varies over time, and, hence, new secret bits can be generated constantly.

Furthermore, if the legitimate parties use the same carrier frequency, for instance with time-division duplex (TDD), then the channel can be considered to be reciprocal, i.e., it will be the same in both transmission directions. Reciprocity can be used to obtain the same CSI at both the legitimate devices, each operating in turn as transmitter and receiver: by quantizing the obtained CSIs at both devices, the same bit sequence can be extracted, which will represent a common and secret random number. An eavesdropper could also be located in the same environment and measure the channel at their location. However, we can usually assume that the channel observations become uncorrelated at a few wavelengths away from the legitimate devices, and an eavesdropper closer to them than such a small distance would probably be noticed. Therefore, the attacker will have a different CSI than the legitimate parties, and he will obtain a different bit sequence. Hence, the sequence obtained by the legitimate parties can be considered a secret key.

Note that CSI estimation is nevertheless an essential step in data detection, and is usually obtained by means of pilot symbols, which are available in most communication systems. Thus, it does not represent an overhead in most communication systems. Furthermore, in some situations, we do not even have to know or transmit the pilots, since we only need some observation that is correlated to the CSI, like the power spectral density, which can be obtained in most cases just by measuring the received data signal.

The described procedure encounters in practice several problems that are properly addressed by the secret key generation (SKG) protocol, which usually follows the following steps.

In the first step, the legitimate parties estimate the channel at regular intervals. Samples can consist only of a scalar value (typically the received-signal strength indicator (RSSI)) or multiple values (as the channel impulse or frequency responses, with or without phase information). Thus, to generalize, the legitimate devices will obtain vector signals containing the channel information at each time instant.

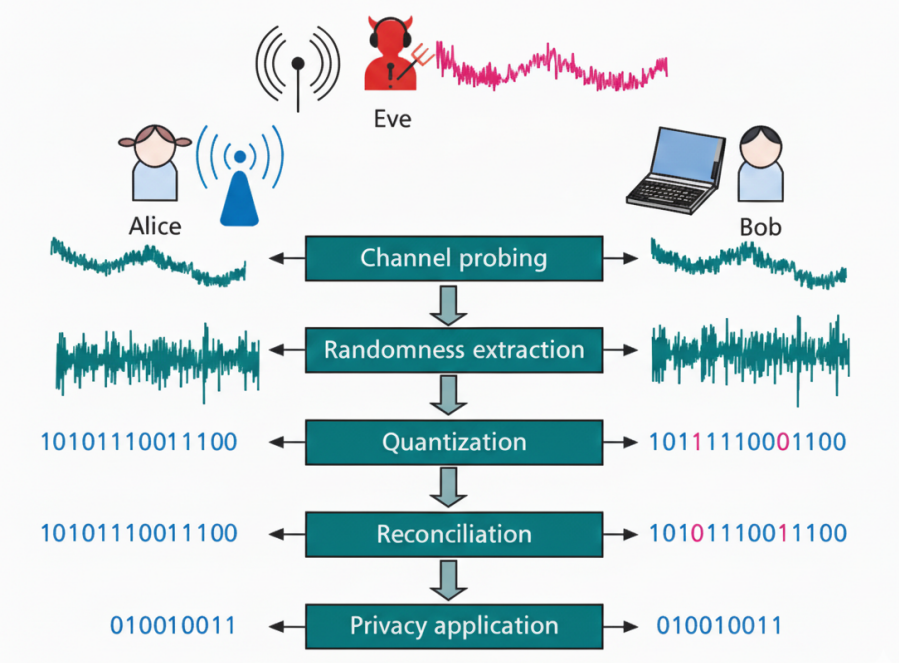


Figure 3.3: Physical-layer secret key generation procedure, see [39].

The second step of the SKG protocol provides the conversion of the channel information vectors at each node into a sequence of bits through a quantization procedure, which can be performed in several ways. Each vector element can be individually quantized with a uniform quantizer, but this can concentrate samples in a few quantization levels. To avoid that, we could have equally-probable sampling intervals, which, however, may require the knowledge of the underlying probability distribution. Since different elements in the channel estimation metric may be strongly correlated, vector quantization can also be employed. At the end of this step, we should have two-bit sequences.

Bearing in mind that the CSI samples are noisy, errors may occur, i.e., we may select a quantization interval that is different from the one corresponding to the actual CSI. A trade-off should be made in the quantizer resolution. A higher resolution increases the number of generated bits, but it also increases the probability of errors, and that will have consequences in the next step, reconciliation.

The channel may be reciprocal, but the channel measurements in general are not. This may happen for several reasons: i) in a TDD system, channel measurements are performed at different instants at the two parties; ii) the devices suffer different noise and interference realizations; and iii) the analog hardware is not ideal, and the receivers are different. Thus, the obtained sequences are not exactly the same, and a reconciliation procedure is performed to make them match. This is usually achieved by means of error-correction codes: the syndrome of the sequence obtained at one device is exchanged over a public channel, allowing the other to align its sequence so that both devices agree on the same codeword, as long as the Hamming distance between the two sequences is not too large.

The last step of the SKG protocol is privacy amplification, and its goal is to ensure that any leaked information, e.g., due to the public syndrome transmission in the previous step, is suppressed and cannot be linked to the final key. This is achieved by passing the bit sequence through a one-way collision-resistant compression function, i.e., a hash function. Note that this operation is performed locally, and no information exchange is needed. The hash function produces a uniform secret *key* with a length strictly shorter than the input bit sequence. While this operation decreases the size of the shared information, it increases the entropy per bit, i.e., the key appears random to eavesdroppers.

The security of privacy amplification has been information theoretically proven through the leftover hash lemma.

Application Examples There are many arguments for having a potential infrastructure-less key management system, e.g., communicating in the presence of a repressive government, avoiding industrial espionage, circumventing malicious intrusion into processing steps of factories, or enabling communications between unmanned vehicles. SKG from physical-layer features is a key enabler for resilient, safe, and scalable industry solutions, as well as consumer communications.

Pros of PLS SKG: Physical signals are a good source of randomness, and the SKG protocol enables the generation of provably secret random bits. In time-varying channels, in particular, new secret bits can be constantly generated. PLS SKG provides a scalable solution, where keys are always known only by the two legitimate parties (no trusted external entity involved). Moreover, existing symmetric encryption methods using the generated keys are quantum-resistant security mechanisms. We also note that PLS SKG is not restricted to communication channels, but can be applied to any common source of randomness.

Cons of PLS SKG: The main drawback of PLS SKG is the lack of extensive field trials. A second issue is that the generation procedure is vulnerable to man-in-the-middle attacks and ray tracing attacks. Moreover, under severe correlation of the observed samples at the legitimate parties and the attacker, the number of secret key bits becomes very small. Indeed, the observations of the legitimate users need to have some advantage over those of the eavesdropper to provide a positive secret key rate. Moreover, at the moment, the generation procedure works only between device pairs or groups but not over multiple transmission hops. Lastly, the secret key rate depends on the channel statistics in time/delay/frequency (and it is not exactly known how) and may vary by many orders of magnitude. In particular, a slowly varying common randomness may not be able to generate a sufficiently high key rate.

3.4 Jamming Detection and Rejection

With jamming, an attacker transmits a signal that prevents two legitimate devices from properly communicating. For example, the jammer generates noise that reduces the signal-to-noise ratio (SNR) at the receiver, which will not be able to correctly demodulate/decode the legitimately transmitted signals. Thus, jamming is a denial-of-service attack.

Jamming typically operates at the physical layer, where it can be most easily detected and possibly rejected. For example, a sharp drop in SNR is an indication of a possible attack. Among rejection techniques, an effective solution is beamforming, where a receiver equipped with multiple antennas focuses reception in the direction of the legitimate transmitter while attenuating the signal coming from the attacker in another spatial direction. Another rejection approach is frequency hopping, where the transmitter changes the carrier frequency (which is known to the receiver but not to the attacker) from time to time, mitigating the effects of a jammer transmitting a narrowband jam signal around a specific carrier.

Jamming techniques are typically designed to limit power consumption and have an intermittent behavior while being effective in disrupting communications. Indeed, transmitting a wideband powerful noise signal (brute force attack) causes severe harm to ongoing communication, but it becomes quickly expensive; it may also disrupt communications relevant for the jammer, and it is prone to easier detection and localization. An intermittent behavior instead reduces such drawbacks and is more effective. For example, scrambling the signal that gives essential information about the network (SSB) or saturating the RACH channel prevents any new connection to the network and introduces

various disturbances. Specific countermeasures can also be deployed against such intermittent behavior: these include a better design of the legitimate transmitted signal to make it more robust to the loss of specific parts, and detection techniques to infer anomalous behavior of the interference/noise signal. A special case of intermittent jamming is reactive jamming, where the attacker senses the channel and transmits the jamming signal only in correspondence with the legitimate transmission (or part of it).

Application examples: Considering the long history of jamming, there are several examples where it has been applied. The most relevant and old example is military communications, where it is used to disrupt enemy transmissions. In the civil domain, it may be used to disrupt security communications, such for example wireless surveillance cameras, to confuse navigation systems using GNSS signals, and to provoke malfunctioning in industry automation, in particular in Industry 4.0. Moreover, the jamming method can be used for UAVs to provide security robustness in wireless communications [40, 41].

Pros of PL jamming detection/rejection: Eventually, the jammer needs to be localized, then neutralized, but temporary solutions are spatial rejection, multipath transmission, and obfuscation. It is also important to make the transmitted signal more robust, avoiding single points of failure. In all these domains, jamming detection and mitigation techniques typically operate on PL signals, that is, where the jamming signal is generated. Extensive literature and historical practice make this security threat and related PL solutions well-known and continuously investigated.

Cons of PL jamming detection/rejection A relevant downside of jamming is that we can only detect/reject jamming, while we cannot prevent it entirely. This is because communications (in particular those using the wireless medium) are intrinsically vulnerable to strong (and also unstructured) interference signals. Thus, jamming mitigation typically operates at the lower layers, i.e., as close as possible to the communication medium itself.

3.5 Geofencing and Confidentiality

Geofencing is a technique by which we limit the decoding of a message within a target geographical area while preventing message reception outside of this area. When geofencing is implemented at the PL, the transmitter typically processes the message signal (e.g., using multiple antennas and beamforming) so that it is received with a high power inside the target area, while the power is significantly lower outside. Since the correct decoding of messages requires the reception of signals with a power large enough with respect to the noise and interference power at the receiver, by unbalancing the power between the inside and outside of the area, we obtain geofencing.

Confidentiality refers to the security objective of preventing an attacker from decoding a message transmitted among legitimate parties. Note that geofencing is a technique to ensure confidentiality for all the devices that are inside the target area, against all attacker devices that are outside. In confidentiality (and geofencing), the attacker is also denoted as an eavesdropper, as it aims at overhearing the message.

Note that the border of the target area is typically blurred since the power degradation is not sharp. Also, the wireless propagation is significantly affected by obstacles, reflectors, and scatterers, making it difficult the exact estimation or predict the geofenced area.

A case of particular interest occurs when the position of the eavesdropper (or, better, the wireless channel from the legitimate source to the attacker) is known. In this case, the security target is similar to geofencing, since we aim at preventing reception in the particular position of the eavesdropper (or, better, over the channel to the eavesdropper). This happens, for example, when the eavesdropper

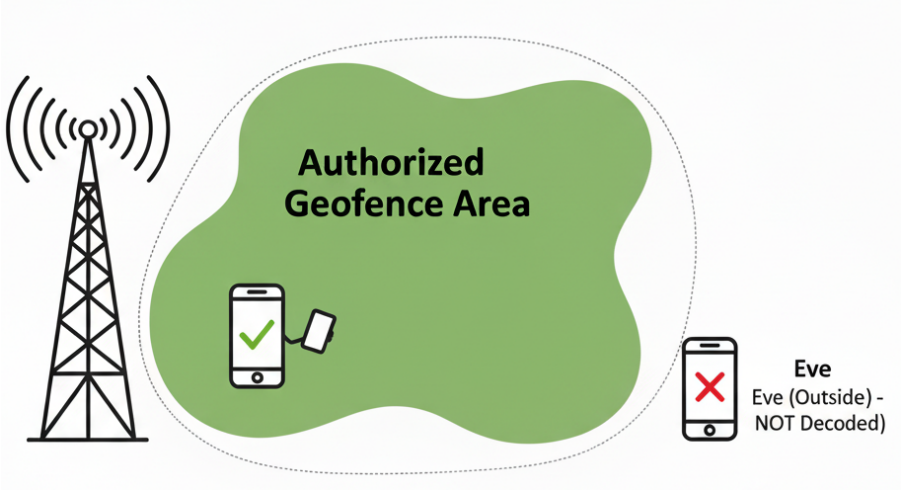


Figure 3.4: Physical-layer geofencing.

is honest but *curious*, i.e., it complies with communication protocols and rules (e.g., of the wireless networks it belongs to) but it is also interested in overhearing messages intended for other devices. In this scenario, the legitimate parties may estimate the attacker channel and deploy confidentiality solutions at the physical layer. When the eavesdropper does not belong to the same network as the legitimate parties, it may be difficult even to know the eavesdropper's existence at all. In this latter scenario, it may be more useful to make proper assumptions on its position *outside* an area, and the security objective of geofencing is more meaningful.

Several PLS confidentiality mechanisms have been proposed and studied when the eavesdropper is known (such as in the case of a curious device), and solid results based on information theory have been developed. More recently, PLS techniques have also been developed for geofencing purposes, with more relaxed assumptions on the eavesdropper channel.

Application examples: The main application sees the limitation of communications of a private network within a specific area, where no attackers are supposed to be. Such an area can be, for example, a building or a campus with access control systems: this application is especially suitable for industrial automation.

Pros of PLS geofencing and confidentiality: PLS provides a robust solution against other approaches to obtain geofencing based on the detected receiver position: indeed, since it is easy to fake the GNSS location in the phone, relying on such information to deliver confidential messages may not be secure enough. PLS geofencing instead prevents devices outside the target are to decoding the message, irrespective of the level of control the attack has on the device itself. All well-investigated PLS results, like performance bounds and many different transmission models, as well as the well-developed schemes including channel coding and signal processing, can be simply applied.

Cons of PLS geofencing and confidentiality: It relies on the strong assumption of the location of the legitimate users and eavesdroppers inside and outside a specific area. Hence, it has higher deployment costs with less flexibility than other solutions not refer to a specific space. Also, it requires the worst-case design, i.e., the eavesdropper's SNR is assumed as the one measured at the fence, which is higher than any values measured behind the fence. As a result, the secrecy rate may be highly limited, depending on the physical topology of the fence.

We now describe three domains where PLS can be particularly suitable to support security.

3.6 Heterogeneous Access Domain

This section describes the effect of PLS involving heterogeneous access, namely cellular and Wi-Fi. PLS is enhanced by designing new authentication protocols while leveraging RF features of various types of radio access networks. RF fingerprinting and beamforming for unique identification of devices are some of the examples of PLS common to both 5G and Wi-Fi 6. While these work well in isolated mode, there are still challenges contributed by RF propagation channels, and uncertainty and variability over device, time, and RF propagation channels. However, PLS targets only isolated networks and is not effective in co-existence environments due to various challenges posed by unknown devices from outside the network domain. Some of the PLS mechanisms can also allow adversaries to employ more effective attacks. An attacker can effectively use beamforming to simulate a hidden-node interference attack. The attacker can also use beamforming in the appropriate direction and eavesdrop on the communication from the victim. Hence, the base station cannot receive the messages from the user due to interference. Due to co-existence conditions, the base station cannot distinguish the interference as malicious or legitimate, and the user is also not aware of the presence of the attacker.

PLS for heterogeneous access aims to ensure secure communication in environments which consider multiple types of radio access technologies coexist. In future wireless communications, devices often utilize heterogeneous access that combines cellular communication and Wi-Fi technologies, such as 6G and Wi-Fi 6. This convergence brings challenges for introducing PLS in wireless communications because of the differences in device functions and network structures. Although there are the above challenges, heterogeneous access networks can offer distinct advantages for PLS, particularly in environments that require high levels of security while ensuring high spectrum efficiency.

RF fingerprinting is one of the main PLS approaches used in heterogeneous access environments. This technology involves identifying devices based on unique physical characteristics of their transmission signals. RF fingerprinting is an effective method in wireless communications because every transmitter, whether cellular or Wi-Fi-based, exhibits subtle and unique differences in signal properties due to imperfections in hardware. Therefore, by utilizing these physical differences, network operators can recognize legitimate users and potential attackers in highly dynamic wireless environments. Moreover, beamforming is another main technology employed for enhancing PLS performance in heterogeneous access networks. It utilizes focused signal transmission to reduce the probability of eavesdropping.

However, the heterogeneous networks introduce other specific vulnerabilities in wireless communications. Coexistence issues between different network types may provide opportunities for attackers. For example, an attacker could use beamforming to create a hidden-node interference attack, where interference is selectively targeted, making it appear as legitimate transmission errors. This kind of attack could significantly reduce network secrecy performance without immediately raising suspicions.

Moreover, it becomes challenging for a base station or access point to differentiate between legitimate interference (such as that from neighboring cells or overlapping Wi-Fi access points) and malicious attacks due to the heterogeneous access features. In some cases, a malicious attacker can leverage the coexisting nodes to inject jamming signals or spoof messages, making it difficult for the security system to recognize the malicious attackers. Therefore, PLS mechanisms must be designed to adapt in real-time, combining physical layer features with higher-layer techniques (such as machine learning-based anomaly detection) to mitigate these risks.

Application examples: PLS for heterogeneous access plays a key role in smart cities where multiple networks coexist, including Wi-Fi, 5G, 6G, and other IoT communication standards. In such scenarios, PLS can help prevent unauthorized access to core infrastructures such as transportation control systems and security systems. Another example is enterprise wireless networks where both cellular and Wi-Fi access are adopted for internal communications. In this scenario, PLS can help reduce the

risk of switching between different access networks for employee devices to protect sensitive private and business data.

Pros of PLS for heterogeneous access: PLS offers a lightweight and scalable security solution for a variety of heterogeneous access networks, and it reduces the dependency on traditional cryptographic methods. PLS can be implemented without extensive computational and communication overhead, it is well-suited for dynamic wireless environments with constrained resources. Furthermore, PLS operates at the physical layer to offer early-stage detection and rejection of illegitimate access attempts, which helps to prevent unnecessary computational burdens on higher layers.

Cons of PLS for heterogeneous access: One major challenge is the difficulty in detecting malicious interference in heterogeneous environments. Furthermore, integrating PLS mechanisms into existing networks can be challenging due to the complexity of managing diverse RF environments. Moreover, PLS cannot always provide sufficient protection against high-level attacks, such as those employing advanced beamforming techniques to circumvent security methods.

3.7 Visible Light Communications Domain

Visible light communication (VLC) is a promising technology for high-speed wireless connectivity, offering an alternative to radio frequency (RF) systems, which are increasingly facing issues of overcrowded spectrum. The broadcast nature of VLC, however, makes it vulnerable to potential eavesdroppers, especially when deployed in public spaces. Thus, this is another area in which PLS can play a role in securing next-generation wireless networks. Significant attention has been devoted to this issue, and a variety of physical layer approaches to securing VLC links have been proposed. Examples include secure pre-coding, wiretap codes, artificial noise, etc., some of which are extensions of approaches developed for PLS for RF systems, while others exploit the particular physical characteristics of VLC (see, e.g., the recent paper [42] for a discussion of progress in this area).

In some contexts, such as a hospital, it is crucial to ensure secure transmission while preventing any unauthorized access, even within the same room. Using null-space beamforming, the VLC system can selectively direct the light signal toward a specific user (e.g., a doctor near a patient bed), creating signal nulls in other directions within the room where unauthorized devices could be present. This spatial targeting ensures that only intended receivers can access the signal, effectively reducing the risk of an intruder intercepting sensitive data. To further enhance security, the VLC system can deploy controlled jamming signals in non-essential areas, like hallway doors or nearby windows. Jamming involves transmitting noise signals that create interference, making it nearly impossible for unauthorized users in those areas to decode the VLC signal. By transmitting controlled noise signals in these areas, the VLC system creates interference zones where the main signal cannot be reliably decoded. This proactive jamming prevents any eavesdroppers from capturing or decoding the transmitted data even if they are within physical proximity of the room, as their devices would receive a corrupted signal filled with interference. This technique is especially useful in settings where patients or visitors could have mobile devices that might inadvertently receive VLC signals. By creating jamming zones around sensitive areas, the VLC system minimizes the chance of signal leakage beyond authorized zones.

Application examples: In a hospital environment, the PLS-enabled VLC can be used to provide reliable, efficient, and comfortable lighting to support patient care, staff activities, and patient well-being, and it can also transmit sensitive patient information between doctors, nurses, and medical devices. LED light sources mounted on the ceiling provide VLC signals to designated user areas, such as doctors' tablets or diagnostic machines beside each patient's bed.

Pros of PLS for VLC system: Implementing these PLS techniques in an indoor VLC setup

provides dual functionality in terms of illumination and robust, multi-layered security communications. The combination of beamforming, jamming, and dynamic power control, along with device-specific authentication, can create a secure communication environment where only authorized participants or medical devices can receive and decode the patient data. The signal is focused directly on authorized devices, and the addition of jamming and noise insertion ensures that anyone attempting to intercept the communication will face significant challenges. In addition, the PLS-enabled VLC system can minimize opportunities for unauthorized access by creating nulls and interference zones, making it difficult for any unintended recipient to capture useful data.

Cons of PLS for VLC system: The light beams are susceptible to indoor blockages, such as furniture, equipment, or the human body, which may cause interruptions and fluctuations in the received SNRs. The PLS techniques, like beamforming and power control, are most effective when the LOS channel is stable. Any obstruction can reduce the effectiveness of these techniques, weakening the system's security performance. In addition, it will also face the challenges with the uplink transmission mechanism of VLC. The uplink of VLC typically relies on RF-based technologies to send data back from the device to the access point. This hybrid approach can compromise security, as the uplink communication becomes vulnerable to RF-based security risks, which PLS techniques for VLC cannot mitigate. Moreover, ambient light sources, such as sunlight and other indoor lighting, can interfere with VLC signals, thus degrading communication quality and affecting the effectiveness of PLS techniques. As the ambient light increases, background noise, the signal may be more difficult to secure, allowing unintended receivers to pick up data. Furthermore, PLS techniques like beamforming, power control, and dynamic jamming always require advanced hardware components (such as directional LED arrays or precision control modules) to manage the signal effectively, which could significantly increase installation costs and additional power computational demands.

3.8 Backscatter Communications Domain

Wireless backscatter communication is a useful technique for low-cost, low-power deployments in passive systems such as RFID. Such systems typically involve a reader or interrogator communicating with passive or semi-passive tags. The low complexity of the tags in such systems and the typical proximity-based implementations make PLS an ideal way of securing these systems. Approaches to PLS in backscatter communications that have been explored include artificial noise injected by the reader to confuse eavesdroppers [43], as well as analyses of the natural security provided by proximity-based systems [44]. Although this area has not been studied extensively, it is a natural setting for PLS approaches.

In backscatter communications, typically passive or semi-passive tags reflect signals transmitted by a reader to communicate. Since these systems have very small power and limited computational resources, traditional cryptographic technologies with high computational complexity are impractical. Thus, PLS becomes an attractive solution for enhancing the security performance in backscatter communications.

Devices in backscatter communications are easily attacked due to their low power and simplicity. To address this issue, current works have proposed several PLS techniques in backscatter communications. One approach is artificial noise; this technique sends controlled noise to potential eavesdroppers in wireless communications, ensuring that unauthorized receivers have a significantly degraded SNR to protect the confidentiality of the information. A patent has also been deposited on this topic [45].

Another security mechanism for backscatter communications is considering the wireless channels and distance. In backscatter communications, the transmitted signals are usually weak and do not travel far, so an attacker needs to be in close physical proximity to intercept the signals. This natural

characteristic can be utilized in PLS methods. For example, using channel reciprocity allows the legitimate users to share a secret key without the need for complex encryption. Since the eavesdropper is in a different location, they observe a different channel state, making it difficult to derive the same key as the legitimate parties.

Backscatter systems also benefit from beamforming techniques, where the reader directs its transmission towards the tag, effectively reducing the likelihood that unintended receivers can intercept the signal. Although beamforming is traditionally associated with more sophisticated systems, adapting these techniques to backscatter communication can further strengthen security without significantly increasing complexity.

Application examples: Backscatter communication with PLS is used in RFID-based access control systems for secure building entry management. These tags provide authentication while maintaining a low power footprint, ideal for deployment in resource-constrained environments. Another application is found in smart agriculture, where backscatter sensors can be used to communicate crucial information, such as soil moisture and temperature, to a central system. In such scenarios, PLS helps ensure the data remains confidential and protected from unauthorized interception, even when devices lack sophisticated encryption capabilities.

Pros of PLS for backscatter communications: The main advantage of using PLS for backscatter communications is that it provides a lightweight security framework that aligns well with the low power and simplicity of backscatter tags. Techniques like artificial noise are particularly effective at confounding potential eavesdroppers without needing complex encryption, making it suitable for environments where conventional security methods are impractical. Additionally, PLS is scalable because it relies on the inherent physical properties of the communication channel, eliminating the need for centralized key management systems.

Cons of PLS for backscatter communications: Despite its advantages, PLS in backscatter communications has limitations. The primary challenge is the vulnerability to man-in-the-middle (MITM) and relay attacks, which are difficult to counter given the passive nature of tags and the lack of active verification mechanisms. Additionally, the limited range of backscatter communication restricts its application. Although the limited range provides some natural security, it also means that if an attacker can get close enough, they could potentially intercept the signal. Moreover, the computational simplicity of tags restricts the complexity of PLS methods that can be deployed, leaving them susceptible to more sophisticated adversaries.

4 — Physical-Layer Security Technologies

In this chapter, we discuss the main technological solutions adopted in physical layer security (PLS). They include coding and signal processing solutions to support confidentiality, secret-key generation solutions, and authentication solutions. The chapter is completed by some emerging implementation examples of PLS technologies.

4.1 Coding Solutions

For discrete memoryless channels, wiretap code constructions based on low-complexity binary linear codes, such as low-density parity-check (LDPC) and polar codes, are widely studied in the literature [46,47]. A different approach based on invertible extractors combines the notions of cryptography and coding theory [48], and provides a polynomial-time modular scheme where a secrecy layer is added to any black-box error-correcting code to achieve the optimal secrecy rate. The authors also show that the proposed scheme achieves semantic security. A modular capacity achieving the construction of wiretap codes with a key shared by the sender and the receiver, which also provides semantic security, is proposed in [49], with efficient encoding and decoding schemes. The assumptions about the channel of the eavesdropper play a key role in the wiretap code designs. This modular approach was further developed in [50], which takes into account the uncertainties on the eavesdropper's channel statistics and presents a code construction to achieve the optimal rate without the presence of a pre-shared secret. Clearly, alleviating the requirements on the assumptions improves the application potential of wiretap codes. Further information quantifying the costs of the encoding and the decoding schemes in terms of the power consumption and the associated computational resources is expected to pave the way for the wide-scale deployment of the wiretap codes.

For continuous channels such as Gaussian and fading channels, coset coding constructions based on nested lattices are particularly well-suited to wiretap coding. They were first proposed in [51] under an eavesdropper's correct decision probability (ECDP) criterion. In [52], it was shown that (random) lattice codes achieve semantic security over the Gaussian wiretap channel. Moreover, [52] proposed the *flatness factor*[1] of a lattice as a fundamental design criterion; this can be extended to fading and multiple antenna channels [54]. Both the ECDP and the mutual information between the received and transmitted message are upper bounded by the flatness factor, hence raising a call for lattices with minimal/small flatness factors (equivalently, lattice theta functions). It was demonstrated in [55] that the problem of finding such wiretap lattice codes in fixed dimensions can be restricted to the set of well-rounded lattices. Constructions of well-rounded ideal lattices from number fields with small average flatness factors were also provided in [55]. The flatness factor and its variants are also relevant to the design of lattices for key generation from correlated Gaussian sources, which achieve the optimal trade-off between the secret key rate and the public key rate [56]. Other non-algebraic lattice code

[1]The flatness factor is closely related to the well-known *smoothing parameter* [53] in lattice-based cryptography [52].

constructions include *polar lattices* [57], which are built from polar codes and achieve strong secrecy and semantic security over Gaussian wiretap channels with low encoding/decoding complexity.

4.2 Secrecy Promoting Signaling Solutions

Numerous signaling-based techniques have been introduced in order to improve physical security in wireless systems, including beamforming, the use of artificial noise, relay-based solutions, and full-duplex jamming receivers [58–62]. Their main goal is to create a difference in the signal-to-noise ratio (SNR) between the legitimate channel and the channel of the eavesdropper. For relay systems, the transmission design of buffer-aided relays can leverage the advantage of allowing data packets to wait in the buffer, thereby selecting an optimal time slot for transmission to enhance the performance of PLS in wireless communications [63]. The novel max-ratio-based scheme was proposed to leverage the advantages of the buffer for cooperative networks in [64]. To further exploit the PLS potential of buffer-aided relay systems, combined with innovative artificial intelligence algorithms and jamming techniques, a deep reinforcement learning algorithm was first introduced in [65] to optimize resource allocation, such as power allocation and buffer-aided relay selection, thereby maximizing the throughput in cognitive communications while ensuring communication security. In [66], a reflective intelligent surface (RIS) was first introduced into buffer-aided relay systems, and multi-agent deep reinforcement learning was also applied for the first time in this system to enhance the secrecy performance. These approaches not only cover the radio-frequency (RF) communications but extend to visible light communication (VLC) systems [67, 68].

The concept of a full-duplex jamming receiver for secrecy was introduced [61], thus avoiding dependence on third-party jammers, which may or may not be available to cooperate, since jamming for the security benefit of others comes at a non-negligible energy cost [69]. A prototype implementation of the concept [70] shows that full-duplex jamming by a receiver employing self-interference cancellation mechanisms is feasible, leading to an advantage to the legitimate receiver over an eavesdropper. In particular, a bit error rate (BER) of 8.5×10^{-6} and 2.4×10^{-1} was achieved, respectively, for the legitimate receiver and the eavesdropper, even when the eavesdropper is in a favorable situation. This advantage can provide an edge for the legitimate receiver with respect to the eavesdropper, which is the basis of many PLS techniques.

RIS is embedded with programmable elements to control the propagation environment of electromagnetic waves, and it has shown significant potential in improving PLS for wireless communications [71–73]. In [74], a UAV-communication scenario is studied to indicate the potential of using RIS to enhance the secrecy rate of the legitimate receiver. The dual-side RIS was utilized in [75] to enhance the secrecy performance in downlink non-orthogonal multiple access networks. Moreover, the dual-side RIS capable of simultaneous reflection and transmission was creatively employed in full-duplex systems, offering significant self-interference cancellation performance [76–78]. The case study in [79] shows the dual-side RIS can significantly reduce the self-interference in full-duplex systems, thus enhancing the achievable rate at the receiver.

The space-time uniqueness of channel responses can be exploited to increase the equivocation of non-legitimate adversaries while sustaining reliable reception at legitimate receivers. In particular, a link-signature-based discriminatory channel estimation scheme for orthogonal frequency division modulation transceivers was proposed [80] that exploits channel impulse response uniqueness to enable disparate signal recovery performance between legitimate and adversary devices. To induce a discrepancy in the detection error probabilities, the pilot sequence of the channel estimation phase is contaminated with the link signature of the legitimate channel. A prototype software-defined radio (SDR) implementation and evaluation were performed, both in an indoor/office environment as

well as an outdoor/vehicular environment, leading to a BER at the adversary above 0.47 and 0.43, respectively, for the indoor and the outdoor setup.

Noise-loop (NL) modulation [81] exploits the inherent noise of electronic equipment and received from the radio channel to modulate the information exchanged by two devices. In this technique, a closed-loop communication is employed, in which each device modulates with its own noise and information, the noisy version from the other device. This mechanism was theoretically analyzed and experimentally evaluated [60], showing the feasibility to withstand eavesdroppers with complete knowledge of the NL system, with a reported BER of 0.51 in the experimental evaluation through an SDR implementation.

Recognizing that several signaling solutions for security are dependent on channel state information that may be imperfect or even unavailable, and that some of such techniques impose energy costs and depend on hardware components that may not be accessible in low-cost devices, a waveform-defined security framework [59] is proposed. The framework tunes waveform patterns to cause inter-carrier interference that renders failed signal demodulation and detection by adversaries. Three impact factors were studied/assessed (training data feature, oversampling factor, and bandwidth compression factor offset) to cause waveform patterns to be undiscoverable at eavesdroppers, conditioned on a pre-shared bandwidth compression factor between legitimate devices. A prototype evaluation with low-cost SDR devices was performed, showing that the proposed framework is capable of limiting eavesdropper reception (BER close to 0.4), even in comparable conditions to the legitimate receiver.

Overall, practical systems have been demonstrated in the literature, verifying the theoretical expectations. However, they are mostly confined within well-controlled laboratory environments, and they need specialized equipment (frequently in the form of a software-defined radio). The main reason for this is the layered architecture of conventional transceivers. It can be envisioned that the accessibility of the physical layer information (including in-phase/quadrature data, angle of arrival/departure...) for configuring the transmitter and/or receiver is the key to integrating PLS solutions through adaptive approaches that can enable potential commercial deployments.

4.3 Secret-Key Generation Solutions

Secret key generation (SKG) at the physical layer relies on the randomness of the wireless channel. For key-based PLS systems, the wireless transmission medium is important for privacy realization due to the presence of different multipath fading for each channel. This channel is considered a random source. Thus, with simple hardware, highly efficient systems with low computational complexity can be realized by extracting the channel's randomness. PLS-based keys can be generated dynamically with changing environmental conditions, which increases the confidentiality of the shared key, as illustrated in Figure 4.1. The secrecy performance of key generation was studied in cooperative networks with a cooperative jamming method in [82]. RIS was used to help enhance the secrecy key generation rate in [83]. A one-time pad encrypted transmission scheme with one-way self-interference was proposed to address a vulnerability in secrecy key generation for wireless communications [84]. Below, we provide an overview of the leading practical solution for the Bluetooth standard.

4.3.1 Bluetooth 5.1 (and beyond)

Bluetooth transceivers are already available for billions of IoT devices around the world. The Bluetooth standard has built-in functionality to measure RSS values, which, due to its reciprocity, have been used as a source for SKG. However, RSS values have a strong correlation to the path-loss between devices, which makes them a low-entropy source (resulting in low SKG rates). In 2019, a new Bluetooth standard emerged, i.e., Bluetooth 5.1. One of the new features, as compared to previous generations,

Figure 4.1: An illustration of secret key generation (SKG) system making use of the randomness of the wireless channel.

is the support of direction finding. The approach works as follows: i) the transmitter appends a constant tone extension (CTE) to the end of packets[2]; ii) a receiver equipped with an antenna array measures in-phase and quadrature (IQ) samples over the received CTE; iii) from the IQ data, the receiver estimates the angle of arrival (direction). Thanks to the newly introduced host controller interface (HCI), within the Bluetooth protocol stack, upper layers can now freely access PHY and link layer information (such as IQ samples). In this sense, IQ data, along with RSS values, can now be used towards both localization techniques and SKG schemes. Similarly, to RSS, IQ samples are symmetric and are a valid source of entropy. Furthermore, multiple studies have demonstrated that SKG based on IQ information can greatly enhance key generation rates, as compared to RSS-based schemes.

4.4 Authentication Solutions

Among the experimental studies, authentication solutions require special attention due to various forms of applications. Similar to the case of key generation, both the channel-specific and device-specific features can be used for physical-layer aided authentication solutions.

Channel-specific solutions aim to generate a shared randomness based on channel-specific parameters, which include the gain, phase, and round-trip time. The above-mentioned difficulties in terms of the estimation error somehow limit the wide-scale application of these solutions. On the other hand, location-based authentication [85] emerges as a widely accepted approach, as exemplified in Figure 4.2. They are shown to be practically relevant, especially in outdoor areas where global navigation satellite systems (GNSSs) function with sufficient accuracy. Their extension to multi-factor authentication is also promising [86].

In channel-based physical-layer authentication (PLA), as an alternative feature, some studies have considered the angle of arrival (AoA) as a source of identity, considering the fact that many existing

[2]Bluetooth uses binary frequency modulation, hence, a constant tone is transmitted using a single frequency - this improves the reliability of measurements.

Figure 4.2: An illustration of location based authentication, making use the of the range and distances of a user to a number of anchor nodes.

base stations are equipped with multiple antennas. Concerning digital antenna arrays, in [12], the authors have proven that an effective impersonation attack on AoA-based PLA can only succeed under very stringent conditions on the attacker in terms of location and hardware capabilities. The validity of these findings in practical implementations has been demonstrated through tests on an experimental dataset provided by Nokia. However, it has been shown in [87] that these considerations do not apply to analogue arrays, where impersonation attacks are still possible. The AoA has demonstrated robustness as a feature for PLA in various scenarios and could serve as a viable component in multi-factor authentication frameworks, as discussed earlier.

Device-based authentication approaches are also investigated in the literature in an experimental manner. Their application scale can vary greatly, starting with the circuit level. As an example, physical unclonable functions (PUFs) designs that exploit inherent delay characteristics of wires and transistors that differ from chip to chip are investigated in [88]. RF front-end impairments, such as the in-phase/quadrature imbalance and amplifier non-linearities, also constitute a promising means for authentication solutions through device fingerprinting [89].

4.5 Emerging Implementation Examples

4.5.1 Hybrid PLS & Cryptography Solutions

Despite the clear connection between PLS and cryptography [90], the related literature on this intersection of two important topics is very sparse. As a straightforward combination of PLS and embedded keys, the secret keys generated from the channel fading observations of two distant nodes (or any other shared randomness) can also be utilized with an embedded key that is pre-shared between legitimate nodes. The hybrid key is termed in [91] as a composite security key. This approach can provide a compromise between the classical approaches and the PLS-based key generation. In [92], key extraction is performed using software-defined radio, and Raspberry Pi units are used for key normalization and harmonization, demonstrating the lightweight structure. The two main issues include the reduction in final key size due to the elimination of some correct bits and placing the same embedded key to

all parties, and also the use of different platforms. However, with the evolution of the transceiver units and the availability of cross-layer data transition, the second disadvantage is expected to be eliminated. It also needs to be noted that this gap in the literature needs to be addressed in the future.

4.5.2 THz Communication Systems

A recurrent theme of future communications systems is the use of frequencies in the terahertz (THz) band (>100 GHz) for wireless high bandwidth communications. While 5G networks (operating <100 GHz) are expected to reach peak data rates of ∼20 Gbps, THz researchers are aiming at breaking the Tbps barrier, with experimental implementations already demonstrating hundreds of Gbps. In 2017, the first standard that covers the THz band – IEEE 802.15.3d-2017 – was approved, thus leading to an intense research activity in the field. Operating at such high frequencies brings its own set of challenges. Propagation losses are extremely high in the THz band; free-space path loss in particular reaches ∼80 dB at 300 GHz over a 1-m distance. To counter these losses, high-gain antennas are required, which in turn make THz links highly directional, sometimes with pencil-like radiation patterns and beamwidths of a few degrees. Of course, this becomes challenging because it requires precisely localizing and tracking users in real-time. However, this challenge can also be transformed into an opportunity for PLS. Indeed, having narrow beams makes it *naturally* difficult for eavesdropping [93]. And this happens without the need to resort to complex beamforming techniques. Man-in-the-middle attacks are still possible but require the use of partially reflecting objects precisely placed in the beam path, which may cause blockage and alert the receiver to the intrusion. Therefore, in general, THz communications offer unique PLS opportunities, but also specific threats that require new countermeasures.

Another important security threat faced by THz systems is jamming [94]. One of the benefits of the THz band is the large available bandwidth, which provides high data rates. However, this can also be detrimental as it can increase the susceptibility of the link to interference, and thus jamming. Furthermore, while coherent phase-modulated systems are universally adopted at lower frequencies, making similar efficient THz systems at low cost is still an ongoing research topic. This had led IEEE 802.15.3d-2017 to adopt an on-off keying (OOK) physical layer mode to cover the cases where low-complexity devices are preferred over a large bandwidth coherent system. Still, tens of Gbps are possible with the OOK mode, but these systems, which rely on the amplitude transmission of logical 0s and 1s, are particularly vulnerable to jamming attacks in intriguing ways. For example, the jamming occurs only on the logical 1, i.e., only when the pulse is present. This asymmetric behavior widens the higher part of the eye diagram and forces the receiver to constantly adjust his decision threshold for error-free reception. Another vulnerability lies in the fact that even a constant single-tone jammer can completely disrupt the link, as long as its frequency is located within the transmitter's bandwidth. By beat interference, wide portions of the intended signal can be overlapped, meaning that the jamming cannot be filtered out without also filtering important parts of the data.

Nevertheless, eavesdropping and jamming at THz frequencies are more difficult than at lower frequencies because of the spatially narrow nature of the THz links. Some of the features mentioned here are unique in some regards; therefore, research in the field is also focusing on unveiling the threats. Countermeasures must be developed, and other techniques mentioned in this whitepaper can *a priori* be used to further protect the channel. They must be adapted to the THz band, keeping in mind the specific vulnerabilities of THz communications.

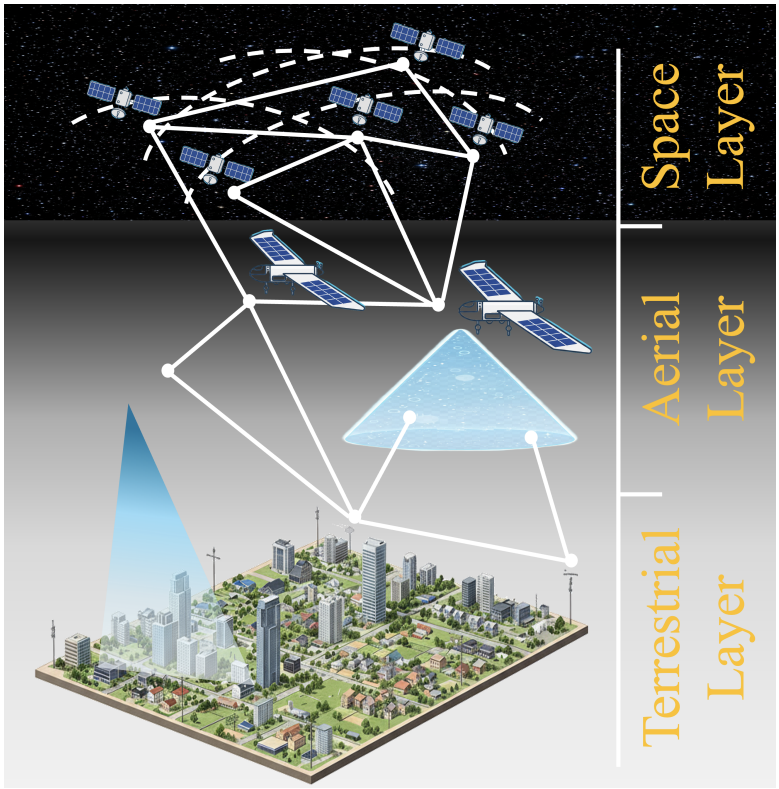


Figure 4.3: A simplified illustration of Space, air ground integrated network (SAGIN).

4.5.3 SAGIN Systems

The space-air-ground integrated network (SAGIN) is a promising communication framework that aims to provide seamless and global coverage for mobile users by integrating three different layers: space (satellites), air (UAVs or high altitude platforms), and ground (terrestrial wireless networks), as shown in Figure 4.3. SAGIN is an essential part of next-generation wireless applications like 6G, smart cities, and IoT. By leveraging the strengths of each layer, SAGIN can overcome the limitations of terrestrial wireless networks, offering enhanced connectivity, scalability, and reliability, even in remote areas.

However, due to the complex and heterogeneous features of SAGIN, it faces significant security challenges, particularly in data transmissions. PLS is one of the key areas in SAGIN security, it protects communications using the intrinsic characteristics of the physical communication channel rather than relying solely on traditional cryptographic techniques. With the diverse layers of space, air, and ground components, SAGINs exhibitbit a mixture of propagation effects such as fading, shadowing, and multipath. PLS techniques can leverage these variations to ensure transmission confidentiality by making it difficult for eavesdroppers to reconstruct the transmitted signal without knowledge of the legitimate communication channels.

5 — Metrics and Validation

This chapter is aimed at providing an overview of current definitions of metrics and security notions for the identification of target levels of physical-layer security (PLS) and the validation of PLS solutions in general. The following sections provide a classification of current approaches, along with the corresponding bibliographic references.

5.1 Measuring secrecy in wiretap channels: limiting an adversary's inference

In the wiretap channel setting, represented in Figure 5.1, a sender applies a coding function to its message (plaintext) M and transmits the obtained codeword (ciphertext) X^n over the channel. Due to the effect (and differences) of the channel on the transmitted codeword, the legitimate receiver observes Y^n, while the adversary eavesdrops the channel and obtains Z^n [2]. The goal of security metrics is to measure the adversary's advantage in breaching the secrecy of the message.

5.1.1 Perfect Secrecy and Total Variation Distance

The perfect secrecy condition guarantees that the adversary obtains no knowledge about the message M by observing Z^n. This is achieved when M and Z^n are statistically independent, making random guessing the adversary's best strategy. In terms of the mutual information between M and Z^n, perfect secrecy corresponds to $I(M; Z^n) = 0$.

The concept of perfect secrecy was first introduced in Shannon's cipher system [1], where the adversary observes the ciphertext X^n without noise (i.e., $Z^n = X^n$). In that setting, shared secrets are required to achieve perfect secrecy. In more detail, to prevent the eavesdropper from retrieving the transmitted message, the sender enciphers its message into a ciphertext by means of a shared secret key K, which is known to the legitimate receiver but unknown to the eavesdropper.

In this setup, it was shown that: (i) perfect secrecy can be achieved using one time pad encryption; (ii) the secret key needs to have at least the same entropy as the message, and, consequently, is at

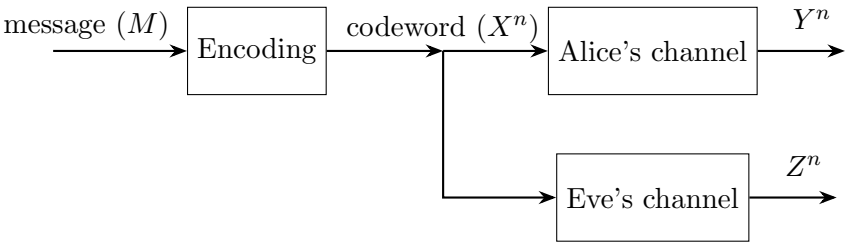


Figure 5.1: Wiretap channel setting

least the same size as the message. As a result, perfect secrecy is impractical and has only been used in niche applications, e.g., for critical diplomatic communications.

In the wiretap channel setting, we aim at avoiding the need for a pre-shared key by taking into account the communication channel and exploiting the difference between Z^n and Y^n. However, perfect secrecy remains very difficult to obtain and impractical.

Note that the mutual information $I(M; Z^n)$ is equal to the average Kullback-Leibler divergence between the distribution P_M of the message and its conditional distribution $P_{M|Z^n}$ given the eavesdropper's observation. Alternatively, one can replace the Kullback-Leibler (KL) divergence by the total variation distance (TVD) [95, 96]. On a finite domain S, the TVD between two probability distributions P and Q is defined as $\max_{A \subset S} |P(A) - Q(A)|$. Unlike the Kullback-Leibler divergence, TVD is more appropriate for the finite blocklength regime, as it does not increase with the blocklength, and it is directly related to the operational limits of hypothesis testing at the adversary [95].

5.1.2 Strong and Weak Secrecy

The statistical independence condition in perfect secrecy can be relaxed by requiring a vanishing information leakage to the eavesdropper in an asymptotic sense. Strong secrecy is guaranteed if the message and the eavesdropper's observation are asymptotically independent, meaning that the information leakage to the eavesdropper will vanish as the ciphertext's length (as well as the plaintext's length) increases, i.e., $\lim_{n\to\infty} I(M; Z^n) = 0$. However, a weaker condition can be imposed, where only the rate of information leaked to the eavesdropper is required to vanish, and is called weak secrecy. In this case, by increasing n, the leaked information can increase sublinearly with n. Weak secrecy is guaranteed if $\lim_{n\to\infty} \frac{1}{n} I(M; Z^n) = 0$.

As an example, let us consider a transmission over a wiretap channel in which blocks of n symbols are transmitted and for each transmitted block n^α symbols are leaked to an eavesdropper, with $0 \leq \alpha < 1$. In such a case, the weak secrecy condition is satisfied, despite the fact that some symbols are leaked out of every finite block of n transmitted symbols. However, the total amount of leaked information tends to infinity and the strong secrecy condition is not satisfied.

Secrecy Capacity and finite-blocklength bounds on secrecy rate The *secrecy capacity* is defined as the maximum achievable communication rate such that both reliability and secrecy conditions are satisfied in the asymptotic regime where the blocklength tends to infinity. Either the strong or weak secrecy condition can be imposed, resulting in the strong or weak secrecy capacity, respectively.

Considering that many applications use short packages or are latency-limited, a penalty on the secrecy capacity is incurred due to coding at a finite block length. Over wiretap channels, an exact characterization of the maximal secrecy rate at a given block length n, error probability ϵ, and information leakage δ is infeasible; however, tight bounds and accurate approximations are provided in the literature [97]. The proposed bounds establish a connection between two achievability proofs of information-theoretic security: privacy amplification and channel resolvability. An optimal tradeoff between reliability and secrecy was established in the finite blocklength regime for the special case of semi-deterministic wiretap channels, while this remains an open problem for general wiretap channels.

Secrecy outage probability In the asymptotic regime where $n \to \infty$, the legitimate receiver can recover the messages with an arbitrarily low decoding error probability as far as the codeword rate R is lower than the channel capacity. However, perfect secrecy cannot always be guaranteed in the absence of instantaneous CSI of the eavesdropping link. Thus, for transmission over wireless fading channels, where classical information-theoretic secrecy is not always achievable, the *secrecy outage probability*

metric measures the probability of failing to achieve classical information-theoretic secrecy [98], that is, when the secrecy capacity C_S is below the secrecy rate R_S.

In finite block length, a coding rate below the secrecy capacity cannot guarantee perfectly successful and secure communication. Then, when classical information-theoretic secrecy is not achievable, confidential information is leaked to the eavesdropper, which can be measured through the *information leakage probability*. Thus, giving an SNR γ_E at the eavesdropper and $R_E = R - R_S$, the information leakage probability can be

5.1.3 Distinguishing Security and Semantic Security

Another subdivision can be made between information-theoretic security metrics and cryptographic metrics. The former ones rely on statistical averages and do not require any assumption on the opponent's computing power, while the latter ones rely on worst-case assumptions and consider a computationally limited opponent. Equivalently, we can say that information-theoretic security metrics usually assume that transmitted messages are random.

As observed in [48], both in the finite length and asymptotic regimes, classical information-theoretic security metrics rely on mutual information between the secret message and the eavesdropper's observation, under the assumption that secret messages are uniformly distributed. Such a PLS metric is denoted as MIS-R, while it is denoted as MIS if we remove the assumption of uniformly distributed messages and consider the maximum mutual information over all possible secret message distributions.

A PLS metric derived from cryptography is the so-called *distinguishing security* (DS) metric, derived from the cryptographic notion of indistinguishability. It measures how much the probability of identifying which one of two possible messages has been transmitted deviates from the ideal value 0.5.

Another PLS metric borrowed from cryptography is that of *semantic security* (SS) [48,99], which aims to quantify the advantage of the attacker's observation-based inference about the transmitted message compared to pure guessing without observing the channel.

Each possible eavesdropper's objective is described as a partition of the message set $\mathcal{M}$ into subsets. The attacker's goal is to guess to which subset the transmitted message M belongs to. For example, if her objective is the reconstruction of the entire message, the set $\mathcal{M}$ will be partitioned into singleton sets. More generally, the objective might be to compute a function of the message. For instance, if the eavesdropper wants to reconstruct the first bit of the message, the set $\mathcal{M}$ will be partitioned into two subsets, corresponding to messages starting with 0 or with 1, respectively.

Given the eavesdropper's observation Z^n, the *eavesdropper's advantage* $\mathrm{Adv}(M, Z^n)$ is the maximum gain, over all possible probability distributions P_M of the message and all possible partitions, in terms of her optimal *a posteriori* probability of making a correct guess when knowing Z^n, compared to the optimal *a priori* probability of guessing correctly based on the knowledge of P_M only. Namely, if the advantage is small, for any choice of the eavesdropper's goal and any distribution P_M, the attacker cannot do much better than pure guessing. In PLS, a sequence of wiretap codes is said to be semantically secure if the eavesdropper's advantage tends to zero when the code length tends to infinity. We note that in the above definition, there is no computational limitation on the eavesdropper's capability of guessing. Therefore, this definition of semantic security is more stringent than the one usually adopted in cryptography, where the adversary's guessing function is restricted to the set of probabilistic polynomial-time functions [100]. Moreover, no assumption is made on the distribution of the message, reflecting the fact that real-life messages are often not uniformly random, and might have low entropy[1].

[1] As noted in [99], contrary to a common belief, compression doesn't render the data uniformly random.

As shown in [48], the MIS, DS and SS security notions are basically equivalent. Instead, while MIS implies MIS-R, the converse does not hold. In summary we have:

$$\text{MIS-R} \Leftarrow \text{MIS} \underset{\Rightarrow}{\overset{\Leftarrow}{}} \text{DS} \underset{\Rightarrow}{\overset{\Leftarrow}{}} \text{SS} \tag{5.1}$$

5.1.4 Network Security and Secrecy Pressure

Many metrics for measuring the security at the physical layer assume that the location of the attacker or its channel is known. In a real case, it is not an easy task to detect that a passive attacker is present and/or to estimate the quality of its channel.

Dropping this impractical assumption is not easy, and mainly two approaches are possible. The first approach is based on the definition of a *network security* metric: users, base stations, and eavesdroppers are deployed following stochastic distributions, and the security is derived by averaging over the distribution of the eavesdropping nodes [101]. In this case, the metric defines how secure a network is in delivering information through its legitimate nodes.

Another recently proposed metric is the *secrecy pressure* [102]. In this case, to drop the assumption of knowing where the eavesdropper is located, the security is defined over a surface. In other words, the secrecy capacity of the legitimate link between Alice and Bob is averaged over the entire surface, as we suppose that Eve is located at every point (x, y) of the surface with uniform probability. The metric allows for the measurement of the intensity of secrecy over a given surface (secure bit/s/Hz for square meters), and it depends on the locations of the legitimate users and interfering nodes, but not on the eavesdroppers. The secrecy pressure metric cloud can also be appreciated under a different shape: the *secure area* (5.2), i.e., the set of points of the environment where the secrecy capacity is over a specific threshold [103]

$$A^{[\text{sec}]} = \left\{ (x, y) \in \mathcal{A} \,|\, C^{[\text{sec}]}(x, y) \geq C^{[\text{sec}]}_{\text{target}} \right\}, \tag{5.2}$$

where $\mathcal{A}$ is the entire surface area, $C^{[\text{sec}]}(x, y)$ is the secrecy capacity in the specific (x, y) point of the area $\mathcal{A}$, and $C^{[\text{sec}]}_{\text{target}}$ is the desired target secrecy rate. Different eavesdroppers' distributions over the area under investigation can also be considered in the metric, as an alternative to a uniform distribution.

5.1.5 Secrecy Maps as Enablers for Network Security

From the perspective of a particular security metric (e.g., semantic secrecy), the wireless environment can be characterized via any-to-any (A2A) radio maps, by associating *security levels* to the legitimate wireless communication links. This characterization results in so-called *secrecy maps* [104], [102], that may be considered as a generalization of the concept of radio maps for physical layer security. The physical layer security characterization relates to the concept of spatial availability of services in wireless networks, by indicating the locations in a given area where the security metric would surmount a given threshold. To account for the inherent uncertainty of the wireless environment (including the uncertainty in the location of potential eavesdroppers and their associated channels as in the example with secrecy pressure), the security guarantees should ideally be defined in a statistical sense (providing a connection to statistical learning approaches [105]). The characterization of the wireless environment via this form of secrecy maps provides a quality-of-service (QoS) notion for physical layer security in a spatial context. In practice, the set of physical layer security-related QoS levels could, for example, correspond to a prescribed set of modulation and coding schemes (MCS), thus providing a relation to system aspects such as resource allocation and link adaptation. This opens the door to treat *security*

as a service, where users can negotiate the security level based on their requirements and the cost. Accordingly, the network can dedicate the necessary resources, i.e., allocate time-frequency slots, or configure additional network resources (e.g., access points or reconfigurable intelligent surfaces) to support the agreed service levels.

5.2 Secret key generation: leakage estimation

The model for the secret key generation (SKG) setting includes two legitimate users, Alice and Bob, who wish to agree on a secret key by observing a common entropy source. In addition, Alice and Bob have access to a public and authenticated channel, which can be considered to be a two-way channel with unlimited capacity. This channel serves for the exchange of side information.

The SKG protocol, first described by Maurer, consists of three phases [106, 107]. In the first phase, referred to as *shared randomness distillation*, Alice and Bob observe dependent random variables denoted by Y_A^n, Y_B^n while an eavesdropper, referred to as Eve, observes Y_E^n. In wireless channels, a readily available source of shared randomness is the multipath fading due to the reciprocity of the wireless medium during the channel's coherence time [108]. In the next phase, known as *information reconciliation*, side information S_A is exchanged between Alice and Bob, generated by corresponding encoders f_A, f_B [109], [110]. Any information leakage due to the public exchange of side information is addressed through hashing in the third phase, called *privacy amplification*.

The goal of SKG is to generate a common key $K \in \mathcal{K}$ at Alice and Bob such that asymptotically, the following reliability, secrecy and uniformity constraints are satisfied [111, 112]:

$$\lim_{n\to\infty} \mathbb{P}\left\{K = f_A\left(Y_A^n, S_A\right) = f_B\left(Y_B^n, S_A\right)\right\} = 1, \tag{5.3}$$

$$\lim_{n\to\infty} I(K; S_A, Y_E^n) = 0, \tag{5.4}$$

$$\lim_{n\to\infty} \log|\mathcal{K}| - H(K) = 0. \tag{5.5}$$

The first condition ensures that the probability of mismatch in the generated keys at the Alice and Bob vanishes asymptotically by increasing the length of the key. The second constraint ensures that the leaked information to Eve (through the adversary's channel as well as the public discussion) is negligible. Finally, the third constraint guarantees that the key is close to uniform (i.e., its entropy is close to maximum)[2].

A secret-key rate is achievable if its generation scheme satisfies the above conditions. The secret-key capacity is the supremum of achievable secret-key rates.

While the basic system model requires an authenticated side channel, subsequent works have shown that this assumption can be relaxed [114–117]. Furthermore, the basic threat model with an eavesdropping adversary can be extended to include active attackers and respective mitigation approaches: i) injection of signals during pilot exchange [19], ii) jamming attacks during pilot exchange [118], iii) spoofing attacks during side information exchange [119].

5.3 Physical Layer Authentication: hypothesis testing

The authentication problem involves an agent Bob, who wants to ensure that the messages he receives are coming from the legitimate agent Alice rather than an intruder Trudy. In turn, the attacker

[2]We note that the last constraint differs from cryptography, where the min-entropy is typically used to evaluate key strength rather than the Shannon entropy [113].

Trudy aims at forging messages that are mistaken as coming from Alice by Bob. A physical-layer authentication (PLA) mechanism enables Bob to make a decision on the basis of the characteristics of the received physical-layer signal. In particular, here we focus on PLA exploiting the features of the communication channel.

In tag-based PLA, the authentication protocol works as follows:

- in the *identification association phase* Alice transmits pilot signals to Bob, who estimates the Alice-Bob channel; such transmission is authenticated by other means, so that Bob is sure that the obtained estimate is relative to the channel from Alice (rather than that from Trudy);
- in the *identification verification phase* whenever Bob receives a message, it estimates the channel $\boldsymbol{r}$ from the pilots; then Bob checks if the estimated channel is *compatible* with that estimated in the preliminary phase: in the former case, the message is considered as authentic, otherwise it is discarded as fake.

For example, assuming a static scenario, the channel estimates performed in the two phases differ only for the estimation error when Alice is transmitting in both cases: typically, such error can be modeled as a Gaussian noise. However, in a time-varying scenario where either Alice or Bob is moving, the estimate in the identification verification phase also differs also because the channel is dynamic; thus, Bob must predict the new channel before comparing it with that estimated from the message.

In turn, Trudy can deploy several kinds of attacks. A naive attack might involve transmitting messages from a location close to Alice's, so that Bob will experience a similar channel. In a more sophisticated attack, Trudy pre-processes the signal before transmission so that, once it propagates through her channel to Bob, his estimate will be close to the expected (Alice-Bob) channel. The latter approach, however, requires that Trudy have some knowledge about the Alice-Bob channel. Considering that the channels to a common receiver for two transmitters at a distance of a few wavelengths are almost uncorrelated, effective attacks against tag-based PLA are not trivial.

5.3.1 False Alarm and Misdetection Probabilities

In the identification verification phase, the channel compatibility check by Bob is a hypothesis testing problem, where Bob has to decide between the two hypotheses that the received message is authentic (hypothesis $\mathcal{H}_0$) or not (hypothesis $\mathcal{H}_1$). In such a test, two errors are possible, namely false alarms (FAs) and misdetections (MDs). When a FAs occurs, an authentic message is rejected as coming from the impersonating attacker, and the probability of FA can be defined as

$$P_{\mathrm{FA}} = \mathbb{P}[\mathcal{D} = \mathcal{H}_1 | \mathcal{S} = \mathcal{H}_0], \tag{5.6}$$

where $\mathcal{S}$ is the true condition (either Bob or Trudy is transmitting) and $\mathcal{D}$ denotes the decision taken by Bob. When a MD occurs, a non-authentic message is accepted as coming from the legitimate transmitter, and the probability of MD can be defined as

$$P_{\mathrm{MD}} = \mathbb{P}[\mathcal{D} = \mathcal{H}_0 | \mathcal{S} = \mathcal{H}_1]. \tag{5.7}$$

Note that while the FA probability is defined (and can be computed) knowing only the statistics of the channel under legitimate conditions (when Alice is transmitting), the MD probability is specific for each attack; thus its computation requires to know Trudy's strategy.

It should be noted that the check performed in the identification verification phase can be considered as an hypothesis testing problem as long as Bob knows the statistics of the estimated channel $\boldsymbol{r}$ in one or both hypotheses (i.e., he knows $p_{\boldsymbol{r}|\mathcal{S}=\mathcal{H}_0}$ and $p_{\boldsymbol{r}|\mathcal{S}=\mathcal{H}_1}$). When both statistics are known, the

Neyman-Pearson optimal likelihood ratio test can be used, where Bob decides for the hypothesis $\mathcal{D} = \mathcal{H}_0$ if

$$\frac{p_{\boldsymbol{r}|\mathcal{S}}(\boldsymbol{r}|\mathcal{H}_0)}{p_{\boldsymbol{r}|\mathcal{S}}(\boldsymbol{r}|\mathcal{H}_1)} > \theta \tag{5.8}$$

and θ is a threshold set to obtain a desired FA probability. When instead only the statistics in legitimate conditions are known to Bob, he can, for example, resort to the (generally suboptimal) likelihood test, where Bob decides for the hypothesis $\mathcal{D} = \mathcal{H}_0$ if

$$p_{\boldsymbol{r}|\mathcal{S}}(\boldsymbol{r}|\mathcal{H}_0) > \theta. \tag{5.9}$$

A typical performance metric for PLA is therefore the couple of FA and MD probabilities, under a specific attack strategy: by varying testing parameters, various probability pairs can be achieved, all under a curve denoted the detection error tradeoff (DET) (FA vs MD probabilities) or receiver operating characteristic (ROC) (the complementary of MD probability vs FA probability).

5.3.2 Kullback-Leibler Divergence

In some cases, the derivation of the FA and MD probabilities is impractical, and we can instead resort to bounds on the set of feasible points in the $(P_{\text{FA}}, P_{\text{MD}})$ plane. For example, an outer bound on the region described by achievable values of $(P_{\text{FA}}, P_{\text{MD}})$ is given by the Kullback-Leibler (KL) divergence among channels estimated by Bob when Alice or Trudy are transmitting, and the channel expected by Bob from the association identification phase. In particular, let us indicate with $\boldsymbol{x}$ the channel expected by Bob in legitimate conditions (i.e., when Alice is transmitting): this is obtained from previous channel estimates at Bob. We indicate with $\boldsymbol{y}$ the effective channel estimated by Bob when Alice is transmitting, and $\boldsymbol{v}$ the channel estimated by Bob when Trudy is transmitting. Lastly, indicating with $\boldsymbol{r}$ the generic channel estimated by Bob in the second phase (thus $\boldsymbol{r} = \boldsymbol{y}$ or $\boldsymbol{r} = \boldsymbol{v}$), from the data processing inequality we obtain [120]

$$\mathbb{D}(p_{\mathcal{D}|\mathcal{S}=\mathcal{H}_1} \| p_{\mathcal{D}|\mathcal{S}=\mathcal{H}_0}) \leq \mathbb{D}(p_{\boldsymbol{rx}|\mathcal{S}=\mathcal{H}_1} \| p_{\boldsymbol{rx}|\mathcal{S}=\mathcal{H}_0}) = \mathbb{D}(p_{\boldsymbol{xv}} \| p_{\boldsymbol{xy}}), \tag{5.10}$$

where $\mathbb{D}(p\|q)$ is the KL divergence between probability density functions (PDFs) p and q. The symmetric bound

$$\mathbb{D}(p_{\mathcal{D}|\mathcal{S}=\mathcal{H}_0} \| p_{\mathcal{D}|\mathcal{S}=\mathcal{H}_1}) \leq \mathbb{D}(p_{\boldsymbol{rx}|\mathcal{S}=\mathcal{H}_0} \| p_{\boldsymbol{rx}|\mathcal{S}=\mathcal{H}_1}) = \mathbb{D}(p_{\boldsymbol{xy}} \| p_{\boldsymbol{xv}}). \tag{5.11}$$

also holds. Now, we can relate the KL divergence to the FA and MD probabilities by defining the function

$$h(P_{\text{MD}}, P_{\text{FA}}) \triangleq P_{\text{MD}} \log \frac{P_{\text{MD}}}{1 - P_{\text{FA}}} + (1 - P_{\text{MD}}) \log \frac{1 - P_{\text{MD}}}{P_{\text{FA}}}, \tag{5.12}$$

and then observing that (5.10) can be rewritten as

$$h(P_{\text{MD}}, P_{\text{FA}}) \leq \mathbb{D}(p_{\boldsymbol{xv}} \| p_{\boldsymbol{xy}}). \tag{5.13}$$

Now, we note that (5.13) provides a limit to the region of achievable $(P_{\text{FA}}, P_{\text{MD}})$ values as a function of $\mathbb{D}(p_{\boldsymbol{xv}} \| p_{\boldsymbol{xy}})$. Note that the bounds are not related to a specific hypothesis test adopted by Bob.

5.3.3 Classification Accuracy

When the statistics of the estimated channel in the second phase are not available to Bob, but some realizations of the estimated channel are available under one or both hypotheses, Bob's test can be considered in a machine-learning framework as a classification problem. In particular, we assume to

have two datasets of channel realizations under the two hypotheses, $\mathcal{H}_0$ and $\mathcal{H}_1$, and we aim at defining a model M that, given an estimated channel $\boldsymbol{r}$ provides a decision on authenticity, $\mathcal{D}$. Thus we have

$$\mathcal{D} = M(\boldsymbol{r}). \tag{5.14}$$

In such a scenario, the model classifies the estimated channel $\boldsymbol{r}$ in one of the two classes corresponding to the two hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$.

The model is trained with the datasets in a supervised manner, where the label of each sample, i.e., the state $\mathcal{S}$ associated to the channel realization, is the desired output $\mathcal{D}$ of the model. In such a framework, the FA and MD probabilities are still the preferred performance metrics. However, we can also consider the classification accuracy, i.e., the probability of correct prediction

$$A = \mathbb{P}[\mathcal{D} = \mathcal{S}]. \tag{5.15}$$

In [121] it has been shown that when the model is a neural network or a least-square support vector machine, for large models and large training datasets, the performance of the model (in terms of FA and MD probabilities) converges to that of the optimal Neyman-Pearson test.

5.3.4 Use of Reconciliation Decoders

Inspired by well-established practices in authentication using physical unclonable functions (PUFs), recently, there have been proposals for the use of Slepian-Wolf decoders to reconcile channel measurements spread in time. This alleviates the use of hypothesis testing and can result in a binary authentication decision based on the output of the reconciliation. During the identification association phase, it is required to store helper data (side information) that will be used during the identification verification phase.

6 — Future Directions and Perspectives

In this chapter, we provide some indications of approaches and problems in physical layer security (PLS) that should be further studied. Moreover, we provide a perspective on what we envision as the most promising applications for these mechanisms.

6.1 Bridge the Gap to Cryptography-Based Solutions

The design of PLS solutions has been based on different metrics and approaches than security mechanisms based on cryptography. In fact, the robustness of cryptographic solutions, which are based on the computational security paradigm, is usually measured in terms of the computational difficulty of mounting a successful attack. This requires the study of the best attack algorithms and their relative complexity, which is conducted as part of cryptanalysis.

In contrast, PLS solutions, adopting the information-theoretic rather than computational security paradigm, normally use much simpler and easier to characterize attack patterns. On the other hand, such attack patterns and the resulting security notions are hardly accepted by the cryptographic community. Such a gap makes it difficult to compare and integrate the two worlds. Then, common metrics and methodologies to assess security are needed. Moreover, the integration of solutions based on cryptographic and PLS approaches should be pursued to exploit benefits based on different bases.

A relevant example in this regard is quantum resistance. Indeed, it is well known that an attacker equipped with a quantum computer can easily compromise the computational security on which many of the cryptographic systems in use today are based. There are two ways of overcoming this vulnerability: replace computationally quantum-vulnerable problems with computationally quantum-resistant problems, which is the approach of post-quantum cryptography, or avoid basing security on computational problems, which is the approach followed by the physical layer and information-theoretic security techniques. Therefore, to ensure secure communications in the quantum computing era, combining these efforts to achieve higher levels of security and agility will be recommended.

Lastly, current system design principles follow the Shannon paradigm and consider the information to be processed as raw data or bits, abstracting and neglecting any semantics and meaning behind the information being processed. Accordingly, current PLS approaches follow these design principles to secure the raw data or bits only. There is a recent trend to go beyond the Shannon paradigm, taking the semantic level of communication into account by optimizing the transmission based on the context and significance of the message. PLS can be useful for new disruptive solutions to protect and secure the semantics and meaning as well.

6.2 On the Impact of Physical Parameters

Despite two decades of steady progress that have transformed PLS from a theoretical concept into concrete algorithms, PLS has yet to be adopted in standards and mainstream products. This lag can be attributed to both technical and conceptual challenges. On the technical side, adoption has been hindered by the absence of modular coding schemes that provide sufficient flexibility and guarantees in the finite block-length regime. However, this barrier has diminished with the emergence of concrete instantiations of wiretap codes, such as those based on invertible extractors, which integrate seamlessly with existing error control codes in current standards. On the conceptual side, PLS remains subject to criticism for its reliance on some degree of eavesdropper channel knowledge. While the required channel knowledge has significantly decreased over time, PLS, unlike traditional cryptographic methods, cannot provide guarantees without any assumption about the eavesdropper's signal quality. Nevertheless, this limitation underscores the need for a hybrid approach, where PLS coding techniques serve as an efficient overlay to enhance traditional cryptographic mechanisms.

For PLS solutions, it is important to understand the physical parameters or characteristics (e.g., the number of antennas, the degrees of freedom, the rank of multiantenna channels, etc.) that have an impact on the security of PLS solutions. Therefore, scaling laws should be derived, and then an assessment of the practical implementation and application scenarios where such security parameters can be exploited at best should be performed. Such an approach would clarify which parameters play a role equivalent for example to the length (in bits) of a secret key and indicate that we can trust a PLS solution when such parameters are large enough (e.g., the number of antennas, or the length of the codeword) and attacks become practically infeasible.

Indeed, when dealing with physical layer solutions, attention should be paid to the physical attack surface, i.e., to the possibility of deploying physical solutions (such as multiple antennas and low-noise amplifiers) to strengthen the attacks. Indeed, as wiretap coding solutions are based on the high noise level at the attack receiver, the security assumption is broken by deploying multiple antennas or using low-noise amplifiers. An effort to identify such vulnerabilities and provide suitable metrics to assess the difficulty of the attacker is still to be pursued.

A growing interest in PLS is evident in the increasing number of experimental studies focused on designing system engineering channels that provide advantages to legitimate users over eavesdroppers. Notably, there is a rising body of research on radio-frequency (RF) frontend chip design that integrates signal processing techniques inspired by PLS. While these efforts often lack the coding mechanisms necessary to ensure security guarantees, they lay the groundwork for the future integration of complete PLS solutions.

6.3 Integration of Sensing and AI to PLS

The desired trustworthiness in 6G networks must be extended to its radio access or wireless medium, as 6G is to control mobile or even flying objects (e.g., drones). Due to the limitations of traditional cryptographic methods, the achieved trustworthiness is far from sufficient in many resource-constrained usage scenarios of 6G. This, together with the opportunities offered by the newly introduced sensing function and artificial intelligence (AI), motivates us to seek complementary techniques, e.g., PLS, to provide trustworthiness for 6G networks over radio. For example, the sensing function and AI can be exploited to collect information on the communication surroundings to significantly facilitate guaranteeing trustworthiness by physical layer solutions, which aligns well with the concept of context-aware security for 6G wireless. The superiority of physical layer security do not come for free, and the guaranteed confidential level in physical layer security is determined by the available information on eavesdroppers (e.g., their statistical channel state information or location). This could also be

the main reason why PLS solutions face severe challenges in pragmatic implementations. However, these challenges could be potentially overcome in the upcoming 6G networks, as radar sensing and AI would be integral parts of 6G. The sensing function and AI have the capabilities to provide critical information on the communication surroundings, e.g., the number of eavesdroppers and their locations, for facilitating the implementation of physical layer security solutions. A few researchers have already attempted to utilize the sensing function of an integrated sensing and communication (ISAC) system to estimate an eavesdropper's location and then subsequently designed a beam pattern to achieve physical layer security. This demonstrates the potential of eliminating the requirement of prior information on eavesdroppers for achieving physical layer security in 6G.

In the context of key generation, a public discussion between the two transceivers for agreeing on an identical key is required in the information reconciliation step. This could cost extra resources, e.g., extra bandwidth or communication latency. The concept of a digital twin built upon AI could be exploited to eliminate or reduce the cost of information reconciliation.

Instead of exploiting the randomness in wireless channels, physical layer authentication leverages unique characteristics of hardware (e.g., a circuit) to verify a device's identity. AI techniques have the capability of automatically extracting desired unique characteristics from both the hardware and location of a transceiver for efficient authentication. Therefore, integrating AI as an enabler of 6G networks also offers new research opportunities for implementing AI-aided physical layer authentication in this context.

PLS can also play a key role in improving privacy as sensing and positioning solutions become more pervasive. Indeed, we are in the wake of unprecedented opportunities for governments and companies to trace our movements, and know our acquaintances and habits not only by digging into our data exchange but also by checking signals transmitted by our devices and even passively with solutions based on sensing, which operate as radars. Such technical solutions currently already have and will have in the future a relevant impact on the nature of our society, the level of personal and collective freedom, and the very basis of our communities. The use of AI scales such opportunities and problems at the highest level. PLS can play a significant role in the design of solutions to defend our privacy against unauthorized sensing of radio signals. The engineering community should be made conscious of the personal responsibility entangled with the design of solutions that can be used against basic rights [1] and should actively work to deliver antidotes, e.g., based on PLS that operates where the problem arises first.

6.4 Other Technical Challenges

The potential of the PLS solutions is not solely captured by their lower complexity. As the attackers get more powerful, a cross-layer integrated security approach will emerge as the sole solution for secure wireless networks. Yet, the full acceptance of the PLS solutions by the wider security research community is still in progress.

There are also technical challenges that are inherent to each approach. For instance, considering the key generation, in case the channel is static, the entropy that the users can extract is not related to the variability of the wireless channel, but it is caused by noise and hardware imperfections. Although the channel state information shows some variability, it is not a common source of randomness when the channel is static. Therefore, there is a need to focus the research on the key generation process when the channel is static.

[1] The recent history has shown that much of the research done on drone communications turned out to be used in military contexts, making engineers working on it somehow responsible for this outcome.

Overall, the main concerns are related both to the assumptions about the attacker models and to the wide-scale deployment challenges. Fueled by the lack of standardization, it is clear that additional studies will be needed for out-of-the-laboratory deployments.

6.5 Promising PLS Applications

From our overview of PLS technology applications, it can be concluded that all proposed solutions can find suitable applications in current and future communication systems, including next-generation cellular networks.

In particular, the eavesdropping coding solutions are particularly suitable in restricted areas where appropriate assumptions about the type and location of the eavesdropper are realistic to ensure that the obtained signal-to-noise ratio is low enough to support secret transmission. A similar principle applies to channel-based secret key generation solutions, which again exploit the presence of noise to give legitimate users an advantage over the attacker. As for the source-based secret key agreement and physical layer authentication techniques, since they are based on the statistics of the channels (including those of the eavesdropper/intruder), they may find application in contexts where devices have limited resources, as lightweight security measures. Again, we must ensure that the attacker has limited capabilities and knowledge of the environment for an effective defense.

In conclusion, the diversification of communication scenarios shortly (from the Internet of Things to non-terrestrial communications) and the proliferation of niche contexts (from industrial production to autonomous vehicles, from health-related applications to low-power IoT applications) will encourage new specific solutions that at best exploit the potential of physical layer signals for security, with advantages in terms of resilience to attacks, lightweight implementation, and intelligent use of communication resources.

Bibliography

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[4] O. Bernard and A. Roux-Langlois, "Twisted-PHS: using the product formula to solve approx-SVP in ideal lattices," in *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II 26*. Springer, 2020, pp. 349–380.

[5] R. Cramer, L. Ducas, and B. Wesolowski, "Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time," *Journal of the ACM (JACM)*, vol. 68, no. 2, pp. 1–26, 2021.

[6] ITU, "Recommendation itu-r m.2160-0 (11/2023) on "framework and overall objectives of the future development of imt for 2030 and beyond." [Online]. Available: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I%21%21PDF-E.pdf

[7] S. Bromander, A. Jøsang, and M. Eian, "Semantic cyberthreat modelling." *STIDS*, pp. 74–78, 2016.

[8] B. Li, S. Wang, J. Zhang, X. Cao, and C. Zhao, "Ultra-fast accurate aoa estimation via automotive massive-mimo radar," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 2, pp. 1172–1186, 2022.

[9] A. Mayya, M. Mitev, A. Chorti, and G. Fettweis, "A skg security challenge: Indoor skg under an on-the-shoulder eavesdropping attack," in *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, 2023, pp. 3451–3456.

[10] L. Senigagliesi, M. Baldi, and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1506–1521, 2021.

[11] M. Srinivasan, L. Senigagliesi, H. Chen, A. Chorti, M. Baldi, and H. Wymeersch, "Aoa-based physical layer authentication in analog arrays under impersonation attacks," in *2024 IEEE 25th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2024, pp. 496–500.

[12] T. M. Pham, L. Senigagliesi, M. Baldi, G. P. Fettweis, and A. Chorti, "Machine learning-based robust physical layer authentication using angle of arrival estimation," in *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, 2023, pp. 13–18.

[13] T. M. Pham, M. Mitev, A. Chorti, and G. P. Fettweis, "Pilot randomization to protect mimo secret key generation systems against injection attacks," *IEEE Wireless Communications Letters*, vol. 12, no. 7, pp. 1234–1238, 2023.

[14] H. Yang, Z. Xiong, J. Zhao, D. Niyato, Q. Wu, H. V. Poor, and M. Tornatore, "Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1963–1974, 2021.

[15] Z. Utkovski, P. Agostini, M. Frey, I. Bjelakovic, and S. Stanczak, "Learning radio maps for physical-layer security in the radio access," in *Proc. IEEE Int. Workshop Signal Process. Adv. Wireless Commun.*, Cannes, France, Jul. 2019, pp. 1–5.

[16] R. Schulz, O. Günlü, R. Elschner, R. F. Schaefer, C. Schmidt-Langhorst, C. Schubert, and R. F. H. Fischer, "Semantic security for indoor THz-wireless communication," in *Proc. 17th Int. Symp. Wireless Commun. Systems*, Berlin, Germany, Sep. 21, pp. 1–6.

[17] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Transactions on Information Theory*, vol. 65, no. 7, pp. 4069–4093, 2019.

[18] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proceedings of the Fourth European Workshop on System Security*, ser. EUROSEC '11. New York, NY, USA: Association for Computing Machinery, Apr. 2011, pp. 1–6. [Online]. Available: https://doi.org/10.1145/1972551.1972559

[19] T. M. Pham, L. Senigagliesi, M. Baldi, G. P. Fettweis, and A. Chorti, "Machine learning-based robust physical layer authentication using angle of arrival estimation," in *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, 2023, pp. 13–18.

[20] M. Srinivasan, L. Senigagliesi, H. Chen, A. Chorti, M. Baldi, and H. Wymeersch, "Aoa-based physical layer authentication in analog arrays under impersonation attacks," in *2024 IEEE 25th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2024, pp. 496–500.

[21] T. M. Pham, L. Senigagliesi, M. Baldi, G. P. Fettweis, and A. Chorti, "Machine learning-based robust physical layer authentication using angle of arrival estimation," in *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, 2023, pp. 13–18.

[22] G. K. Fischer, T. Schaechtle, A. Gabbrielli, J. Bordoy, I. Häring, F. Höflinger, and S. J. Rupitsch, "A systematic survey and comparative analysis of angular-based indoor localization and positioning technologies," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2025.

[23] I. W. G. da Silva, D. P. M. Osorio, and M. Juntti, "Privacy performance of MIMO dual-functional radar-communications with internal adversary," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2023.

[24] S. Tomasin, M. Centenaro, G. Seco-Granados, S. Roth, and A. Sezgin, "Location-privacy leakage and integrated solutions for 5g cellular networks and beyond," *Sensors*, vol. 21, no. 15, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/15/5176

[25] J. J. Checa and S. Tomasin, "Location-privacy-preserving technique for 5g mmwave devices," *IEEE Communications Letters*, vol. 24, no. 12, pp. 2692–2695, 2020.

[26] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 5–22, 2021.

[27] M. Wiese, J. Nötzel, and H. Boche, "A channel under simultaneous jamming and eavesdropping attack—Correlated random coding capacities under strong secrecy criteria," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3844–3862, Jul. 2016.

[28] J. Nötzel, M. Wiese, and H. Boche, "The arbitrarily varying wiretap channel—Secret randomness, stability, and super-activation," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3504–3531, Jun. 2016.

[29] 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, Jun. 2010, conference Name: IEEE Transactions on Information Forensics and Security.

[30] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of Generating a Secret Key Using Wireless Fading Under Active Adversary," *IEEE/ACM Transactions on Networking*, vol. 20, no. 5, pp. 1440–1451, Oct. 2012, conference Name: IEEE/ACM Transactions on Networking.

[31] 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*, ser. Lecture Notes in Computer Science, S. Foresti, M. Yung, and F. Martinelli, Eds. Berlin, Heidelberg: Springer, 2012, pp. 235–252.

[32] S. M. MirhoseiniNejad, A. Rahmanpour, and S. M. Razavizadeh, "Phase Jamming Attack: A Practical Attack on Physical layer-Based Key Derivation," in *2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, Aug. 2018, pp. 1–4, iSSN: 2475-2371.

[33] M. Mitev, A. Chorti, E. V. Belmega, and M. Reed, "Man-in-the-Middle and Denial of Service Attacks in Wireless Secret Key Generation," in *2019 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2019, pp. 1–6, iSSN: 2576-6813.

[34] H. Boche, R. F. Schaefer, and H. V. Poor, "Denial-of-service attacks on communication systems: Detectability and jammer knowledge," *IEEE Trans. Signal Process.*, vol. 68, pp. 3754–3768, 2020.

[35] R. Jin and K. Zeng, "Manipulative Attack Against Physical Layer Key Agreement and Countermeasure," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 475–489, Jan. 2021, conference Name: IEEE Transactions on Dependable and Secure Computing.

[36] ——, "Physical layer key agreement under signal injection attacks," in *2015 IEEE Conference on Communications and Network Security (CNS)*, Sep. 2015, pp. 254–262.

[37] Q. Hu and G. P. Hancke, "A session hijacking attack on physical layer key generation agreement," in *2017 IEEE International Conference on Industrial Technology (ICIT)*, Mar. 2017, pp. 1418–1423.

[38] K. S. Subramani, N. Helal, A. Antonopoulos, A. Nosratinia, and Y. Makris, "Amplitude-modulating analog/rf hardware trojans in wireless networks: Risks and remedies," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3497–3510, 2020.

[39] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.

[40] S. Fang, G. Chen, Z. Abdullah, and Y. Li, "Intelligent omni surface-assisted secure mimo communication networks with artificial noise," *IEEE Communications Letters*, vol. 26, no. 6, pp. 1231–1235, June 2022.

[41] Y. Wen, G. Chen, S. Fang, M. Wen, S. Tomasin, and M. D. Renzo, "Ris-assisted uav secure communications with artificial noise-aware trajectory design against multiple colluding curious users," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 3064–3076, 2024.

[42] E. Panayirci, M. Koca, H. Haas, and H. V. Poor, "Spatial modulation aided physical layer security for noma-vlc systems," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 8, pp. 10 286–10 301, 2023.

[43] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 6, pp. 3442–3451, 2014.

[44] X. Li, Y. Zheng, W. U. Khan, M. Zeng, D. Li, G. K. Ragesh, and L. Li, "Physical layer security of cognitive ambient backscatter communications for green internet-of-things," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1066–1076, 2021.

[45] Z. Han, W. Saad, and H. V. Poor, "System and method for securing backscatter wireless communication," Jun. 6 2017, uS Patent 9,672,394.

[46] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[47] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[48] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Annual Cryptology Conference*. Springer, 2012, pp. 294–311.

[49] S. Sharifian and R. Safavi-Naini, "A modular semantically secure wiretap code with shared key for weakly symmetric channels," in *2019 IEEE Information Theory Workshop (ITW)*. IEEE, 2019, pp. 1–5.

[50] R. A. Chou, "Explicit codes for the wiretap channel with uncertainty on the eavesdropper's channel," in *2018 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2018, pp. 476–480.

[51] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: Construction and analysis," *IEEE Trans. Inform. Theory*, vol. 62, no. 10, pp. 5690–5708, Oct. 2016.

[52] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Trans. Inform. Theory*, vol. 60, no. 10, pp. 6399–6416, Oct. 2014.

[53] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM (JACM)*, vol. 56, no. 6, pp. 1–40, 2009.

[54] L. Luzzi, R. Vehkalahti, and C. Ling, "Almost universal codes for MIMO wiretap channels," *IEEE Transactions on Information Theory*, vol. 64, no. 11, pp. 7218–7241, 2018.

[55] M. T. Damir, A. Karrila, L. Amoros, O. W. Gnilke, D. Karpuk, and C. Hollanti, "Well-rounded lattices: Towards optimal coset codes for gaussian and fading wiretap channels," *IEEE Transactions on Information Theory*, vol. 67, no. 6, pp. 3645–3663, 2021.

[56] L. Luzzi, C. Ling, and M. R. Bloch, "Optimal rate-limited secret key generation from gaussian sources using lattices," *IEEE Transactions on Information Theory*, vol. 69, no. 8, pp. 4944–4960, 2023.

[57] L. Liu, Y. Yan, and C. Ling, "Achieving secrecy capacity of the Gaussian wiretap channel with polar lattices," *IEEE Transactions on Information Theory*, vol. 64, no. 3, pp. 1647–1665, 2018.

[58] S. Gokceli, O. Cepheli, S. T. Basaran, G. Karabulut Kurt, G. Dartmann, and G. Ascheid, "How effective is the artificial noise? real-time analysis of a phy security scenario," in *2017 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2017, pp. 1–7.

[59] T. Xu, "Waveform-defined security: A low-cost framework for secure communications," *IEEE Internet of Things Journal*, 2021.

[60] L. Mucchi, S. Caputo, P. Marcocci, G. Chisci, L. Ronga, and E. Panayirci, "Security and reliability performance of noise-loop modulation: Theoretical analysis and experimentation," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 6335–6350, 2022.

[61] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, Oct 2013.

[62] G. Chen, J. P. Coon, and S. E. Tajbakhsh, "Secure routing for multihop ad hoc networks with inhomogeneous eavesdropper clusters," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 10 660–10 670, Nov 2018.

[63] Y. Nie, X. Lan, Y. Liu, Q. Chen, G. Chen, L. Fan, and D. Tang, "Achievable rate region of energy-harvesting based secure two-way buffer-aided relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1610–1625, 2021.

[64] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 719–729, April 2014.

[65] C. Huang, G. Chen, Y. Gong, and Z. Han, "Joint buffer-aided hybrid-duplex relay selection and power allocation for secure cognitive networks with double deep q-network," *IEEE Transactions on Cognitive Communications and Networking*, vol. 7, no. 3, pp. 834–844, Sep. 2021.

[66] C. Huang, G. Chen, and K.-K. Wong, "Multi-agent reinforcement learning-based buffer-aided relay selection in irs-assisted secure cooperative networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4101–4112, 2021.

[67] N. Cen, N. Dave, E. Demirors, Z. Guan, and T. Melodia, "Libeam: Throughput-optimal cooperative beamforming for indoor visible light networks," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 2019, pp. 1972–1980.

[68] A. R. Ndjiongue, T. M. Ngatched, O. A. Dobre, and H. Haas, "Toward the use of re-configurable intelligent surfaces in vlc systems: Beam steering," *IEEE Wireless Communications*, vol. 28, no. 3, pp. 156–162, 2021.

[69] J. P. Vilela, P. C. Pinto, and J. Barros, "Position-based Jamming for Enhanced Wireless Secrecy," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, no. 3, pp. 616–627, September 2011.

[70] A. Silva, M. Gomes, J. P. Vilela, and W. K. Harrison, "Sdr proof-of-concept of full-duplex jamming for enhanced physical layer security," *Sensors*, vol. 21, no. 3, 2021.

[71] J. Yuan, G. Chen, M. Wen, D. Wan, and K. Cumanan, "Security-reliability tradeoff in uav-carried active ris-assisted cooperative networks," *IEEE Communications Letters*, vol. 28, no. 2, pp. 437–441, Feb 2024.

[72] X. Sheng, X. Li, G. Chen, G. Huang, C. Han, and Z. Ding, "Performance analysis of star-ris assisted secure cognitive noma-harq networks," *IEEE Wireless Communications Letters*, vol. 13, no. 3, pp. 696–700, March 2024.

[73] Z. Yang, S. Zhang, G. Chen, Z. Dong, Y. Wu, and D. B. da Costa, "Secure integrated sensing and communication systems assisted by active ris," *IEEE Transactions on Vehicular Technology*, pp. 1–6, 2024.

[74] S. Fang, G. Chen, and Y. Li, "Joint optimization for secure intelligent reflecting surface assisted uav networks," *IEEE Wireless Communications Letters*, vol. 10, no. 2, pp. 276–280, Feb 2021.

[75] Y. Zhang, Z. Yang, J. Cui, P. Xu, G. Chen, Y. Wu, and M. D. Renzo, "Star-ris assisted secure transmission for downlink multi-carrier noma networks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 5788–5803, 2023.

[76] Y. Wen, G. Chen, S. Fang, Z. Chu, P. Xiao, and R. Tafazolli, "Star-ris-assisted-full-duplex jamming design for secure wireless communications system," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4331–4343, 2024.

[77] C. Huang, Y. Wen, L. Zhang, G. Chen, Z. Gao, and P. Xiao, "Reconfigurable intelligent surface empowered full duplex systems: Opportunities and challenges," *ArXiv: 2407.15782*, 2024.

[78] Y. Liu, G. Chen, Y. Wen, Q. Luo, C. Zhang, and D. Niyato, "Star-ris-enabled full-duplex integrated sensing and communication system," *ArXiv: 2410.18767*, 2024.

[79] S. Fang, G. Chen, P. Xiao, K.-K. Wong, and R. Tafazolli, "Intelligent omni surface-assisted self-interference cancellation for full-duplex miso system," *IEEE Transactions on Wireless Communications*, vol. 23, no. 3, pp. 2268–2281, March 2024.

[80] A. Albehadili, K. A. Al Shamaileh, A. Y. Javaid, and V. K. Devabhakuni, "Link-signature-based discriminatory channel estimation (ls-dce) for physical layer security in stationary and mobile ofdm transceivers," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8119–8131, 2020.

[81] L. Mucchi, L. S. Ronga, and L. Cipriani, "A new modulation for intrinsically secure radio channel in wireless systems," *Wireless personal communications*, vol. 51, pp. 67–80, 2009.

[82] P. Xu, J. Yang, G. Chen, Z. Yang, Y. Li, and M. Z. Win, "Physical-layer secret and private key generation in wireless relay networks with correlated eavesdropping channels," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 985–1000, 2024.

[83] Z. Ji, P. L. Yeoh, D. Zhang, G. Chen, Y. Zhang, Z. He, H. Yin, and Y. li, "Secret key generation for intelligent reflecting surface assisted wireless communication networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 1030–1034, Jan 2021.

[84] Z. Ji, P. L. Yeoh, G. Chen, J. Zhang, Y. Zhang, Z. He, H. Yin, and Y. Li, "Physical-layer-based secure communications for static and low-latency industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18 392–18 405, Oct 2022.

[85] E. Klein, "Geographical location authentication method," Jan. 3 2012, uS Patent 8,090,351.

[86] D. A. Pinski and P. Chowdhury, "Mobile network-based multi-factor authentication," Feb. 21 2017, uS Patent 9,578,025.

[87] M. Srinivasan, L. Senigagliesi, H. Chen, A. Chorti, M. Baldi, and H. Wymeersch, "Aoa-based physical layer authentication in analog arrays under impersonation attacks," in *2024 IEEE 25th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2024, pp. 496–500.

[88] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*. IEEE, 2007, pp. 9–14.

[89] J. Zhang, R. Woods, M. Sandell, M. Valkama, A. Marshall, and J. Cavallaro, "Radio frequency fingerprint identification for narrowband systems, modelling and classification," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3974–3987, 2021.

[90] W. K. Harrison and S. W. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *IEEE International Conference on Communications*, 2009, pp. 1–5.

[91] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 152–158, 2016.

[92] G. Karabulut Kurt, Y. Khosroshahi, E. Ozdemir, N. Tavakkoli, and O. A. Topal, "A hybrid key generation and a verification scheme," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 703–714, 2019.

[93] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, Nov. 2018.

[94] R. Shrestha, H. Guerboukha, Z. Fang, E. Knightly, and D. M. Mittleman, "Jamming a terahertz wireless link," *Nat. Commun.*, vol. 13, no. 1, p. 3045, Jun. 2022.

[95] X. Yu, S. Wei, and Y. Luo, "Finite blocklength analysis of Gaussian random coding in AWGN channels under covert constraint," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1261–1274, 2021.

[96] M. Nafea and A. Yener, "A new wiretap channel model and its strong secrecy capacity," *IEEE Transactions on Information Theory*, vol. 64, no. 3, pp. 2077–2092, 2018.

[97] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Transactions on Information Theory*, vol. 65, no. 7, pp. 4069–4093, 2019.

[98] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6913–6924, 2016.

[99] M. Bellare, S. Tessaro, and A. Vardy, "A cryptographic treatment of the wiretap channel," *arXiv preprint arXiv:1201.2205*, 2012.

[100] J. Katz and Y. Lindell, *Introduction to modern cryptography*. CRC press, 2020.

[101] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—part i: Connectivity," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 125–138, 2012.

[102] L. Mucchi, L. Ronga, X. Zhou, K. Huang, Y. Chen, and R. Wang, "A new metric for measuring the security of an environment: The secrecy pressure," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3416–3430, 2017.

[103] D. Marabissi, S. Morosi, and L. Mucchi, "Green security in ultra-dense networks," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 6, pp. 8736–8749, 2024.

[104] Z. Utkovski, P. Agostini, M. Frey, I. Bjelakovic, and S. Stanczak, "Learning radio maps for physical-layer security in the radio access," in *2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2019, pp. 1–5.

[105] L. G. Valiant, "A theory of the learnable," *Communications of the ACM*, vol. 27, no. 11, pp. 1134–1142, 1984.

[106] U. Maurer, "Secret key agreement by public discussion based on common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 5, pp. 733–742, May 1993.

[107] C. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory*, vol. 50, no. 2, pp. 394–400, Feb. 1995.

[108] A. Mukherjee, S.A.A., Fakoorian, H. Jing, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys and Tuts.*, vol. 16, no. 3, pp. 1550–1573, Third Quarter 2014.

[109] C. Bennet, G. Brassard, and J. Robert, "Privacy amplification by public discussion," *J. Computing*, vol. 17, no. 2, pp. 210–229, 1998.

[110] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology – EUROCRYPT*, 1994, pp. 410–423.

[111] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[112] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–154, Jun. 2010.

[113] M. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, "Recommendation for the entropy sources used for random bit generation, special publication (sp 800-90b)," NIST, Tech. Rep., 2018.

[114] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part I: definitions and a completeness result," *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.

[115] ——, "Secret-key agreement over unauthenticated public channels-part II: the simulatability condition," *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.

[116] ——, "Secret-key agreement over unauthenticated public channels-part III: privacy amplification," *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 839–851, Apr. 2003.

[117] U. Maurer, R. Renner, and S. Wolf, "Unbreakable keys from random noise," in *Security with Noisy Data*. Springer, 2007, pp. 21–44.

[118] E. V. Belmega and A. Chorti, "Protecting secret key generation systems against jamming: Energy harvesting and channel hopping approaches," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2611–2626, 2017.

[119] M. Mitev, M. Shakiba-Herfeh, A. Chorti, M. Reed, and S. Baghaee, "A physical layer, zero-round-trip-time, multifactor authentication protocol," *IEEE Access*, vol. 10, pp. 74 555–74 571, 2022.

[120] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Forensics Security*, vol. 46, no. 4, p. 1350–1356, 2000.

[121] A. Brighente, F. Formaggio, G. M. Di Nunzio, and S. Tomasin, "Machine learning for in-region location verification in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 11, pp. 2490–2502, 2019.