





Securing Wireless Communication in Critical Infrastructure: Challenges and Opportunities

Jörn Bodenhausen¹, Christian Sorgatz², Thomas Vogt¹, Kolja Grafflage³,
Sebastian Rötzel⁴, Michael Rademacher², and Martin Henze^{1,2}

¹ Security and Privacy in Industrial Cooperation, RWTH Aachen University, Aachen, Germany, {bodenhausen, vogt, henze}@spice.rwth-aachen.de

² Cyber Analysis & Defense, Fraunhofer FKIE, Wachtberg, Germany, {christian.sorgatz, michael.rademacher, martin.henze}@fkie.fraunhofer.de

³ ATS Elektronik GmbH, Wunstorf, Germany, kolja.grafflage@atsonline.de

⁴ Bonn-Netz GmbH, Bonn, Germany, sebastian.roetzel@bonn-netz.de

Abstract. Critical infrastructure constitutes the foundation of every society. While traditionally solely relying on dedicated cable-based communication, this infrastructure rapidly transforms to highly digitized and interconnected systems which increasingly rely on wireless communication. Besides providing tremendous benefits, especially affording the easy, cheap, and flexible interconnection of a large number of assets spread over larger geographic areas, wireless communication in critical infrastructure also raises unique security challenges. Most importantly, the shift from dedicated private wired networks to heterogeneous wireless communication over public and shared networks requires significantly more involved security measures. In this paper, we identify the most relevant challenges resulting from the use of wireless communication in critical infrastructure and use those to identify a comprehensive set of promising opportunities to preserve the high security standards of critical infrastructure even when switching from wired to wireless communication.

Keywords: Critical Infrastructure · Wireless Communication · Security

1 Introduction

Critical infrastructure encompasses all physical and cyber assets that are essential to maintain vital societal functions. Common examples are smart grids (i.e., electricity and water distribution) [43, 67] and smart city services (i.e., intelligent traffic and transportation) [22, 74]. Over the past decades, this infrastructure has transformed towards highly digitized and interconnected intelligent systems [15, 68, 73] to capitalize on benefits such as efficiency improvements, better visibility into the network, and increased flexibility [6], while at the same time meet increasing complexity, e.g., resulting from distributed energy resources [5, 36].

Traditionally, critical infrastructure relied on private wired communication infrastructure to interconnect assets (e.g., fiber optic networks) [36]. More recently, we observe an increasing incorporation of wireless communication in critical infrastructure, supplementing and partially replacing wired communication,

Authors' version of a paper accepted for publication in *Proceedings of the 20th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous)*. Cite as: J. Bodenhausen, C. Sorgatz, T. Vogt, K. Grafflage, S. Rötzel, M. Rademacher, and M. Henze, "Securing Wireless Communication in Critical Infrastructure: Challenges and Opportunities", in *Proceedings of the 20th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous)*, 2023.

fueled by various complementing developments [24]: ① Significant advances in the fundamental technology underlying wireless communication enable increased throughput and low latency [40, 51], energy efficient transmissions over long-distances [49], and a significantly higher density of devices [34]. ② A fundamental shift to highly digitized and interconnected systems, where many existing facilities are not connected to a private wired network yet and new emerging entities that do not have an established dedicated wired network at all [36]. ③ The emergence of new usage scenarios where wired communication is technically or economically infeasible, e.g., in the context of smart cities and Internet of Things (IoT) deployments, where large numbers of mobile and resource-constrained devices are deployed over large areas [59].

While the resulting increasing use of *wireless* communication in critical infrastructure provides tremendous benefits, it also poses serious challenges for security. Most importantly, critical communication might now take place over publicly accessible or at least visible networks outside the physical control of the critical infrastructure operator, much unlike the traditional security assumptions of dedicated private networks with strong perimeter protection [36]. Consequently, to sustainably capitalize on the advantages of wireless communication in critical infrastructure, a thorough understanding of these resulting security challenges as well as opportunities to address them is required.

Related Work. Various works study and systematize the security challenges resulting from modern wireless communication (not specific to critical infrastructure) [52, 61, 66], (mostly) wired communication in distinct critical infrastructure [3] such as water systems [67] or power grids [36, 68], as well as highly digitized and interconnected systems such as smart cities [22, 43] and the (industrial) IoT [11, 59]. While these works provide a comprehensive overview of the respective research fields, they do not generalize the unique challenges of securing wireless communication in critical infrastructure. Contrary, different works focus on isolated challenges and possible solutions to address these, e.g., by analyzing path-loss of electromagnetic waves in urban environments [49], studying the performance of Transport Layer Security (TLS) for IoT [50, 54], evaluating low latency but secure communication for the IoT [28], and securing IoT devices with secure elements [58]. Still, these works do not focus on deriving a comprehensive picture of the challenge and solution space. This contrast results in a gap between an overview of relevant challenges for the particular case of wireless communication in critical infrastructure and the potential benefit from solutions for individual challenges.

Contributions. In this paper, we fill this gap by comprehensively studying the relevant challenges resulting from the use of wireless communication in critical infrastructure and identifying opportunities to uphold a strong level of security even under these challenging conditions. More precisely, our contributions are:

1. We systematize the use of wireless communication in critical infrastructure and provide an overview of relevant technology and its properties (Section 2).
2. We categorize and summarize security challenges that are specifically applicable to wireless communication in critical infrastructure (Section 3).

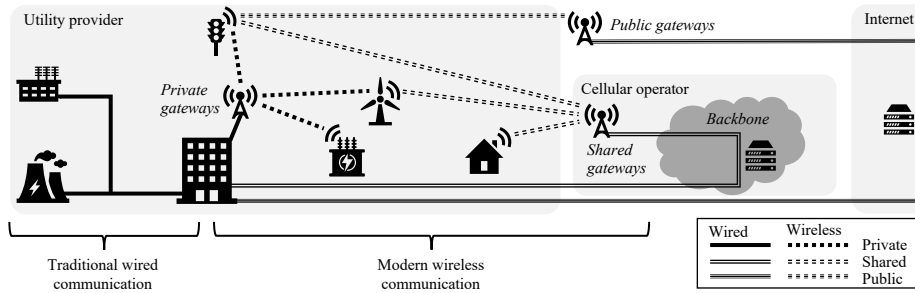


Fig. 1. Communication in critical infrastructure shifts from dedicated private wired networks to heterogeneous wireless communication, encompassing all means of private, public, and shared communication networks as well as dual-homed devices.

3. We identify and discuss complementary opportunities to address the challenges of secure wireless communication in critical infrastructure (Section 4).

2 Wireless Communication in Critical Infrastructure

In recent years, critical infrastructure increasingly relies on wireless communication [3]. To lay the foundation to identify and address resulting security challenges, we first identify developments and motivations that fuel this trend (cf. Section 2.1), before we introduce and discuss various wireless communication technology that is especially relevant for critical infrastructure (cf. Section 2.2).

2.1 From Wired to Wireless Communication

For decades, critical infrastructure relied on private *wired* communication networks [36], as exemplified for a typical (municipal) utility provider in the left part of Figure 1. With advancements in wireless communication technology and the push towards digitization, critical infrastructure increasingly relies on a confluence of heterogeneous *wireless* communication networks, which are no longer necessarily private, but potentially shared with other critical infrastructure or the public (right part of Figure 1). While wireless communication will likely serve as a complement to existing wired communication, it mainly serves as an enabler for novel use cases and a remedy for the increasing need for communication capabilities of assets. Notably, the choice of a wireless communication technology within one critical infrastructure will neither be homogeneous nor exclusive, i.e., multiple technologies will coexist and individual devices or assets might connect over different wireless networks [74].

Exemplarily focusing on a (municipal) utility provider as depicted in Figure 1, we discuss and highlight the reason and motivation as well as different incarnations of the shift to wireless communication. Most notably, the shift towards an increasing use of wireless communication would not be possible without tremendous advancements in the underlying technologies [34, 51]. These advancements

have improved wireless networks, enhancing reliability, efficiency, and capacity, making their integration into critical infrastructure more feasible.

Complementing these developments, there has been a fundamental transformation towards highly digitized and interconnected systems, exemplified by the emergence of smart grids [13], where existing facilities that were previously devoid of communication requirements now need connectivity. Moreover, an increasing amount of entities such as heat pumps, tiny solar power installations, and charging stations have arisen that lack an established dedicated wired network altogether. This trend is carried to the extreme by completely new smart city scenarios (i.e., smart recycling and parking, intelligent transportation [74]) where wired communication may prove technically or economically unviable.

Overall, the shift from wired to wireless communication enables a multitude of new use cases and applications. To illustrate this, we will briefly reference the most prominent applications for secure wireless communication in critical infrastructure. In general, applications can be grouped into categories such as energy, environment, industry, living, and services [74]. Here, critical infrastructure mainly affects energy [13, 62], industry [42], and services [62]. The dominant critical infrastructure application is smart grids [13, 62], i.e., the monitoring of energy generation, transmission, and consumption [35, 36, 68]. In the field of services, applications arise due to the possibility of mobile sensors, which allows, e.g., for the monitoring of transportation services [62]. Moreover, the paradigm of Industry 4.0 leads to interesting use cases and demands for very dense wireless networks to interconnect machines and computational capabilities [20, 42].

In summary, the incorporation of wireless communication within critical infrastructure has gained traction due to significant technological advancements, the shift towards interconnected systems such as smart grids, and the rise of new scenarios where wired communication is infeasible. As depicted in Figure 1, in contrast to wired communication which predominantly relies on dedicated private fiber optic and copper wire networks, wireless communication in critical infrastructure can rely on a plethora of cellular radio technology in private, public, and shared deployments.

2.2 Heterogeneous Wireless Networks

The range of different cellular radio technologies potentially suitable for critical infrastructure is immense. The most common technologies are Long Term Evolution (LTE), Narrowband IoT (NB-IoT), Global System for Mobile Communications (GSM), Terrestrial Trunked Radio (TETRA), Long Range Wide Area Network (LoRaWAN), Wi-Fi, 450 MHz LTE Machine Type Communication (LTE-M), 5G and in the future 6G. Choosing a suitable technology is challenging since they have widely differing characteristics and capabilities.

What all these wireless networks have in common is, that they are cellular radio networks, i.e., their topology can be summarized as interconnected base stations. Each base station typically serves a certain area, while overlaps are possible and desired. Base stations require an exposed location, a stable power supply, and a backhaul connection typically realized via wired networks.

The characteristics and capabilities of the different technologies are mainly determined by the maturity level of the technology, the frequency used, and the available bandwidth. At Sub-GHz bands (e.g., 450 MHz LTE-M or LoRaWAN), a higher range (cell size) and better penetration of structures can be achieved. However, the bandwidth is scarce which reduces throughput and scalability and therefore limits the potential applications [17, 50, 65]. At higher frequency bands (e.g., mmWave for 5G), the throughput is comparable or even superior to wired technologies but the range of each base station and device is limited [51].

In wireless communication, frequency bands are heavily regulated. There are frequency bands that are strictly assigned to certain entities, i.e., Mobile Network Operators (MNOs), while others are generally accessible. Receiving the exclusive right to use a certain band (e.g., 450 MHz LTE-M, 5G) requires significant investment costs, which need to be generated. However, due the exclusive control, the operator can also guarantee a certain Quality of Service (QoS). License-exempt bands reduce the operation costs (e.g., Wi-Fi, LoRaWAN). However, particularly in urban scenarios, these bands can become uncontrollably crowded which compromises their applicability for critical infrastructure [48].

Similar considerations hold for the operation model of the different wireless technologies. As visualized in Figure 1, there are three possibilities: public, shared, and private. Interestingly, there are technology advancements such as 5G network slicing which blur the boundaries between public and private network infrastructures [38]. *Public* network infrastructure is operated by entities (MNOs) not directly associated with critical infrastructure. 3rd Generation Partnership Project (3GPP) technologies (LTE, 5G) are widely used and the network is shared with others (e.g., smartphones). Recently, a new type of public network infrastructure, driven by a shared community approach, emerged. Most prominently, The Things Network [64] builds a wide-range LoRaWAN network. *Shared* infrastructure is operated by entities directly associated to critical infrastructure. While building and operating a wireless network is not feasible for a single critical infrastructure operator, multiple operators can form an association and share costs, e.g., the nationwide 450 MHz LTE network for critical infrastructure in Germany [8]. Compared to public networks, the network is not shared outside the association. *Private* networks are directly operated by critical infrastructure operators. These networks are limited to certain areas where a huge device density renders a network economically feasible (e.g., plants, smart cities) or where there is a lack of other solutions (e.g., offshore wind farms). Technologies operating in license-exempt bands are preferred (e.g., Wi-Fi, LoRaWAN), however, private 5G campus networks provide an interesting alternative.

Overall, it can be stated that due to their versatility, heterogeneous wireless networks offer enormous potential to be utilized for a wide variety of applications. However, this versatility also leads to significant complexity that affects operators and their clients. The huge diversity in wireless technologies, frequency regulation, and operation models not only complicates the deployment and operation of wireless communication in critical infrastructure but also fundamentally challenges security.

3 Challenges of Securing Wireless Communication

Wireless communication in critical infrastructure places high demands on security. At the same time, various significant challenges must be addressed that differ depending on the particular setting and influences such as operation models, particular technologies, network topology, and utilized devices. Thus, each particular use case can shift the focus to certain challenges or create new ones.

Methodology. We strive to identify those challenges that are particularly relevant to wireless communication in critical infrastructure. To this end, we study various literature providing an overview of security challenges resulting from various aspects relevant to wireless communication in critical infrastructure: (i) modern wireless communication in general, i.e. not focusing on critical infrastructure [52, 61, 66] (ii) wired communication in specific, isolated branches of critical infrastructure [3, 36, 67, 68], as well as (iii) fully interconnected and digitized intelligent (future) systems [10, 11, 22, 43, 59]. We complement these more holistic surveys with highly specialized works focusing on isolated challenges of securing wireless communication in critical infrastructure, especially with respect to (iv) network and device constraints alongside various dimensions [16, 49, 50, 54], (v) a wide range of security challenges [14, 43, 47, 55, 60], as well as (vi) legal and deployment considerations [2, 3].

Overall, using this methodology, we identify twelve overarching challenges of securing wireless communication in critical infrastructure, which we broadly categorize into four groups: ① constraints of the utilized network and devices (Section 3.1), ② security of networks (Section 3.2), ③ security of the utilized devices (Section 3.3), and ④ application-specific challenges (Section 3.4). To provide the foundation to adequately address these challenges, in the following, we further discuss and analyze them in more detail.

We intentionally chose this ordering and categorization to make the section structured and coherent. Our ordering does not necessarily resemble the difficulty or importance of the identified challenges, which mostly depends on the specific situation and perspective. Thus, some of those challenges are more fundamental and tangible while others might be considered rather conceptual. For instance, the challenges grouped in the categories ① and ③ could be considered fundamental, as these stem from the devices as well as the environment and are thus entirely rigid. The challenges in the categories ② and ④ on the other hand are not as rigorous and depend more on design decisions and requirements than on actual limitations. In any case, a detailed use case analysis of each particular application and its environment is necessary to determine the magnitude and importance of each challenge and thus derive a specific prioritization.

3.1 Network and Device Constraints

Securing wireless communication is first and foremost challenged by constraints of the employed network and devices. Most importantly, wireless networks are challenged w.r.t. reliability and mobility. Furthermore, especially in IoT settings,

both network and devices can be restricted with regard to available resources such as bandwidth, computing power, or energy.

C1 - Reliability is a crucial aspect for critical infrastructure, where seamless communication and real-time data transmission are paramount to prevent disruptions and ensure smooth operation and safety. Any interruptions or failures in the wireless network can have far-reaching consequences, including power outages, equipment malfunctions, and delays in emergency response. Therefore, building and maintaining a reliable mobile network infrastructure is essential to ensure the smooth operation of critical infrastructure systems. Due to the inherent characteristics of wireless communication, this is particularly difficult to achieve as wireless connections are susceptible to various environmental factors that can drastically affect signal strength and quality. Most importantly, obstacles such as terrain, buildings, or other structures as well as distance can reduce the reliability of the wireless connection by causing signal attenuation and propagation loss [49]. Furthermore, wireless networks are prone to interference caused by other radio technologies operating on the same frequencies or from inter-cell interference caused by the same technology [16]. These difficulties must be considered during the planning of any mobile network intended for use in critical infrastructure.

C2 - Mobility additionally leads to non-uniform connection quality that depends on the device position and corresponding local influences on reliability, influenced by factors such as distance from the base station, physical obstructions, device interference, and signal propagation characteristics [49]. This variability in network quality poses challenges for both mobile nodes and devices that are permanently deployed in unfavorable positions. Seamless roaming between different coverage areas is critical to maintaining an uninterrupted connection when devices move between cells. A challenge for devices in motion is the potentially increased power consumption when they remain connected to a cell at its edge [63], despite a better signal being available from another nearby cell [33]. The ability to switch between cells presents an opportunity for attackers to target User Equipments (UEs) by using fake/rogue base stations [31]. Another challenge with mobility is the availability of wireless technology in any location where the device may be present. Therefore, not only roaming between cells but also between wireless technologies is an important aspect to address. The security vulnerabilities of all supported technologies become critical when devices have the ability to switch between them, especially if they can be forced into switching from external sources. For instance, if 5G coverage is limited, then a device or UE can downgrade to an earlier generation of mobile communication, such as LTE or GSM, so that the device can maintain uninterrupted access to the network.

C3 - Network Limitations imposed by the particular technology can further restrict the network beyond the challenges of wireless technologies in general. Most notably, the throughput is limited compared to a wired network since throughput requires bandwidth and spectrum is scarce. This limitation holds for licensed (e.g., 450 MHz LTE [41]) as well as unlicensed bands (e.g., Lo-

RaWAN [50]) and in particular restricts the acceptable bandwidth overhead that can be added by security mechanisms. Furthermore, devices compete for this bandwidth, which becomes a problem when particularly many devices are part of the network, as the available bandwidth is shared among all devices and thus even more limited. This challenge was exemplarily illustrated for LoRaWAN, where numerous devices might even make a timely TLS connection establishment infeasible [50]. As a result, latency is also an issue, as it takes longer to transmit the full message, which can have significant implications for safety-related mechanisms such as an emergency shutdown. This is reinforced by the technology-specific maximum message size (e.g., 256 bytes for LoRaWAN), through which larger messages might be fragmented and delayed even if the wireless network is currently not busy. Furthermore, the communication range of different wireless technologies can differ significantly and thus restrict their usability (cf. Section 2.2).

C4 - Device Limitations further impose challenges beyond the limitations of the network. Especially in an IoT-like setting, device resources such as compute power, memory, storage, or energy can be rather restricted [7]. Such limitations can have a significant impact on the system. For instance, they can limit the applicability of authentication and encryption mechanisms, especially asymmetric ones, as these are commonly computationally expensive [54]. Memory constraints limit the possible complexity of a system and its ability to cache information. Moreover, especially for battery-powered devices, energy efficiency is of utmost importance. As transmission and reception are particularly energy-intensive, messages should be kept as short as possible and bandwidth efficiency is crucial. All those factors also limit the applicability of mechanisms that address security concerns.

3.2 Network Security Concerns

While the challenges discussed so far primarily affect the usability of wireless technology, concerns also arise for the security of transmitted data. Naturally, conventional security considerations, i.e., the CIA triad consisting of confidentiality, integrity, and availability, also apply here. Moreover, proper authentication is a fundamental challenge that needs to be addressed.

S1 - Confidentiality and Integrity protect data from unauthorized access (confidentiality) and unauthorized alteration (integrity). Such protection is particularly relevant for wireless communication in critical infrastructure, where sensitive data from both the customer and the critical infrastructure operator is transmitted over a wireless medium that can be accessed by anyone in communication range. In some cases, such as the transmission of generic machine instructions, confidentiality might be optional, but integrity is of utmost importance to mitigate the manipulation and insertion of messages. However, assuring confidentiality and integrity can be challenging in constrained environments, as suitable security mechanisms add overhead [43]. Furthermore, it must be considered that hop-by-hop mechanisms, as usually integrated into wireless technology,

do not suffice if the subsequently traversed infrastructure is not private, often calling for the use of end-to-end security.

S2 - Availability ensures that resources can be accessed when needed. Unlike wired networks, the wireless medium can be used easily and unrestricted by anyone in range, allowing for a multitude of attacks on availability. Malicious interference in the form of jamming can cause a disturbance in the wireless network such that legitimate communication is partially or completely disrupted [46]. Moreover, energy depletion of battery-powered devices is possible by preventing the system from sleeping [47]. Hence, protecting wireless networks from such attacks is exceptionally challenging, especially considering critical infrastructure.

S3 - Authentication ensures that only authorized devices participate in communication. While wired networks can be secured to some extent through their architecture and segmentation, cryptographic methods must inevitably be used in a wireless network to ensure that only authenticated devices can access it. Such cryptographic methods usually rely on asymmetric mechanisms, which are demanding for resource-constrained devices [36]. Furthermore, proper authentication is required in various contexts (e.g., network connection, end-to-end security, system updates [27]). Overall, such methods must therefore be designed in a resource-efficient way and devices must receive appropriate credentials.

3.3 Device Security and Challenges

The changes in security requirements and network environment due to wireless communication in critical infrastructure also impose challenges on individual devices. One such challenge is the more difficult deployment with cryptographic material. As credentials weaken over time or become otherwise insecure, revocation mechanisms must be utilized. Moreover, easier physical access of adversaries to devices deployed in more or less public spaces must be considered.

A1 - Deployability of devices is significantly impeded by the need for credentials for subsequent authentication. In particular root credentials are required to authenticate all subsidiary credentials and, moreover, all connections and firmware upgrades. Devices need to be equipped and configured with root credentials during production or deployment [14]. This deployment may be automated or require manual work, but in any case, makes the deployment process more difficult and expensive.

A2 - Device Exclusion allows to remove previously authorized devices from a network, e.g., when credentials get stolen or otherwise compromised as well as when underlying cryptographic primitives lose their promised security level. Especially credential theft could occur rather frequently in critical infrastructure due to the easier physical access to devices that are increasingly deployed in public spaces. For such cases, there is a need for revocation mechanisms and by extension the exclusion of compromised devices from the network. While there are solutions that address this issue for subsidiary credentials, they usually require trust in the utilized root credentials. Protection and revocation of root credentials thus is an open challenge [25, 26, 60].

A3 - Physical Access to Devices refers to an adversary’s ability to physically extract, e.g., keying material from a device. While devices were conventionally inaccessible on private premises, they are increasingly being deployed in openly accessible spaces [55], e.g., in the context of smart cities. An illustrative example would be smart metering systems, that are deployed in private homes and are thus easily accessible to the residents. Furthermore, the wireless characteristic allows for devices to be moved while still being connected to the network. This results in special requirements and challenges for the physical protection of the devices themselves and the critical information stored on them.

3.4 Application-Specific Requirements

In addition to these challenges that follow from the use of wireless communication in critical infrastructure in general, further use-case-specific requirements might need consideration. Most importantly, this concerns potential legal requirements as well as a certain flexibility to allow for seamless operation.

R1 - Legal Requirements are imposed on a wide range of domains and in particular critical infrastructure. For example, a guideline of the German Federal Office for Information Security (BSI) that is applicable for smart meter infrastructure [2] demands the use of TLS with mutual certificate-based authentication, limits session lifetime to 48 hours, and restricts the choice of cryptographic algorithms and parameters. Such requirements can also cover aspects outside security, e.g., functional safety or interoperability, and significantly limit the possibility of specialized and optimized solutions.

R2 - Flexibility ensures the seamless operation of the system. For once, the interoperability of the system must be considered, since the infrastructure might not be controlled by a single entity. Moreover, the updatability of and access to the system, i.e., serviceability, must be taken into account [3]. As it might be impracticable or impossible to access devices that are deployed in the field, remote access and update solutions must be utilized. Furthermore, the use of several wireless technologies in parallel could enhance the redundancy and robustness of the system. Lastly, as the use case might not yet be precisely defined, the system should allow for adaptability to changing conditions.

4 Opportunities to Secure Wireless Communication

To address the identified crucial challenges for securing wireless communication in critical infrastructure, we move forward by identifying and examining potential opportunities to secure wireless communication but also point out their shortcomings and promising potential for further research. For easier reference, Table 1 gives an overview of the challenges that are addressed by the various discussed approaches, which we structured into four categories: ① security for the network technology (Section 4.1), ② security for the encapsulated communication (Section 4.2), ③ security of the devices themselves (Section 4.3), and ④ enhancing security using detailed knowledge of the network (Section 4.4).

Table 1. Various opportunities to secure wireless communication in critical infrastructure exist to address the identified fundamental security challenges (marked by ■).

Challenges of securing wireless communication in critical infrastructure (Section 3)	Netw./Dev. Constr.				Netw. Sec. Concerns			Dev. Security/Chall.			App.-Spec. Require.	
	C1 - Reliability	C2 - Mobility	C3 - Network Limit.	C4 - Device Limit.	S1 - Conf./Integrity	S2 - Availability	S3 - Authentication	A1 - Deployability	A2 - Device Exclusion	A3 - Phy. Acc. to Dev.	R1 - Legal Require.	R2 - Flexibility
Opportunities to secure wireless communication in critical infrastructure (Section 4)												
Network Security Lower Layer Security Mechanisms Secure Communication Channel	■ □ □ □	□ □ ■ □	□ □ ■ □	□ □ ■ □	□ □ □ □	□ □ □ □	□ □ □ □	□ □ □ □	□ □ □ □	□ □ □ □	□ □ □ □	□ □ □ □
Communication Security Resource-Conscious E2E Security E2E Security Extensions Cryptography Optimizations	□ □ □ □	□ □ ■ □	□ □ ■ □	□ □ ■ □	■ □ □ □	□ □ □ □	□ □ □ □	□ □ □ □	□ □ □ □	□ □ □ □	■ □ □ □	■ □ □ □
Device Security Hardware Security Mechanisms Authenticated Code and Secure Boot Root of Trust	□ □ □ □	□ □ □ □	□ □ □ □	□ □ ■ □	□ □ □ □	□ □ □ □	□ □ □ □	□ □ □ □	□ □ ■ □	□ □ ■ □	■ □ □ □	□ □ □ □
Network Knowledge Propagation Conditions Context Awareness Roaming and Redundancy	□ □ ■ □	■ □ ■ □	■ □ ■ □	□ □ ■ □	□ □ ■ □	□ □ ■ □	□ □ ■ □	□ □ □ □	□ □ □ □	□ □ □ □	□ □ □ □	□ □ □ □

4.1 Network Security

Wireless networks are built upon diverse technologies, each equipped with its own set of inherent security mechanisms. As critical infrastructure becomes more interconnected, wireless network security becomes increasingly important.

Lower Layer Security Mechanisms are particularly relevant for wireless communication, i.e., using a shared medium. Even if end-to-end security on a higher layer is utilized, the lower layer security of the particular communication technology has to be addressed, for which various mechanisms exist. With LTE and 5G, etc., radio traffic typically takes place in licensed frequencies and heavy regulations ensure reduced interference from other radio technologies. To further mitigate unintended interference, frequency planning [16] can be used. To combat jamming, employing advanced modulation schemes is an effective countermeasure [32]. Thus, reliability (C1) can be improved [3] while addressing network limitations (C3).

Secure Communication Channels ensure that data is protected while traversing a network. To secure data transport from the MNO to the customer, a Virtual Private Network (VPN) or a dedicated physical connection can be used. This can be combined with private Access Point Names (APNs) or network slic-

ing [38] on the access part to isolate data from different classes of users [21]. IoT devices typically only require communication with specific servers, allowing to restrict communication, which mitigates the risks of integrating compromised UEs into botnets as it would require communication with unauthorized servers. Such mechanisms address confidentiality and integrity (**S1**) on the network layer by establishing secure channels for data transmission, ensuring that data remains confidential and intact during network traversal. However, on this layer, it is particularly important to address network and device limitations (**C3**, **C4**). IoT devices often send little data, making it inefficient to send it as an Internet Protocol (IP) packet. Cellular mobile technologies such as LTE-M or NB-IoT provide Non-IP Data Delivery (NIDD) as a security mechanism, where data packets are sent without IP address and other headers [21], eliminating typical IP-based attack scenarios. However, for NIDD and similar approaches, existing implementations for higher-layer protocols need to be adapted to work with changes to the layer directly below [39].

4.2 Communication Security

Security mechanisms and authentication provided by utilized communication technology commonly operate in a hop-by-hop fashion. However, especially for public networks, further protection mechanisms are required to secure the communication between nodes in an end-to-end manner [12]. The commonly used approach to realize this is TLS [53], which is a secure and application-independent protocol that provides confidentiality, integrity protection, and moreover authentication, if a proper root of trust is used for both peers, for end-to-end communication. However, such approaches cause additional overhead, especially with respect to bandwidth and computing power.

Resource-Conscious End-to-End Security aims to provide confidentiality (**S1**) while respecting limitations of devices (**C4**) and the network (**C3**). In critical infrastructure, TLS is often without alternatives due to legal requirements (**R1**) and the requirement for interoperability with other systems (**R2**). However, the overhead of TLS is not fixed and varies depending on the configuration and utilized cryptographic algorithms [50, 54], allowing for optimization through proper configuration and selection of parameters [50]. Still, further research is required to determine the most beneficial options in a certain scenario and verify the effectiveness of resulting optimizations. In this context, it has to be considered that some options for optimization come at the cost of reducing the interoperability and updatability.

End-to-End Security Extensions provide further optimizations beyond what is possible through parametrization and algorithm choice alone. For instance, the optional TLS session resumption mechanism makes subsequent connections more efficient by cryptographically linking them to the initial connection [53]. Session sharing between applications allows to make better use of session resumption, conserve system resources (**C4**), and improve latency [29]. Likewise, latency can be improved by pre-computing certain cryptographic operations [28]. Lastly, caching of information allows to reduce the amount of transmitted data,

further countering network limitations (**C3**). For TLS, e.g., an extension allows to cache parts of the handshake, which can then be omitted in subsequent handshakes [56]. Still, further research is required to assess the practical application and interoperability of these mechanisms, in particular for critical infrastructure depending on the device and the network properties like bandwidth. This is required as especially interoperability is low for multiple of the extensions proposed for constrained devices.

Cryptography Optimizations allow to further tailor security when communicating only with a limited set of services (at the cost of flexibility). However, such solutions must be adequate for and tailored to the particular setting and requirements. For instance, if confidentiality is not required, a solution focused solely on integrity protection (**S1**) could significantly reduce resource requirements. To this end, aggregation of message authentication codes [72], especially using progressive message authentication [4,69], improves the bandwidth overhead (**C3**) of integrity protection (**S1**) through cleverly designed shorter integrity tags, where the reduced security of shorter tags is improved upon over time. BP-MAC [71], on the other hand, precomputes integrity protection tags to better utilize computing resources (**C4**) and significantly improve latency. From a different perspective, RePeL [70] leverages unused header fields of (industrial) communication protocols to embed integrity protection tags to retrofit integrity protection (**S1**) in the face of network limitations (**C3**). However, such approaches generally do not allow for communication with arbitrary systems, as is the case for standardized solutions such as TLS. To enable severely resource-constrained devices to still communicate securely using TLS, delegation approaches offload the particularly resource-intensive connection establishment to a more powerful, trusted device [30]. The established connection state is then handed to the constrained device and it can thus benefit from the high level of security. Overall, if the given communication scenario allows for optimizing cryptography, especially resource constraints of devices and networks can be addressed. However, since this might impact interoperability, it should be further examined how those can be integrated into established protocols.

4.3 Device Security

Besides securing the network and communication, also individual devices need to be secured (cf. Section 3.3). In particular, the potentially easier physical access to devices in critical infrastructure (**A3**) poses a significant threat. The device security must be considered on various levels to ensure trust in the system. This includes hardware and software security as well as a proper root of trust.

Hardware Security Mechanisms are inevitable for trust into systems that are deployed in hostile environments to protect against manipulation of systems through direct physical access (**A3**). One prominent approach are secure elements [58], which implement security-related mechanisms such as tamper-proof memory to store keys and certificates as well as secure random number generation in hardware. Furthermore, secure elements can also improve performance through hardware acceleration and thus relieve resource-constrained de-

vices (**C4**). Most notably, such optimizations concern rather resource-intensive algorithms such as those used in TLS, making it easier to meet the legal requirement (**R1**) to use this protocol. However, it is important to consider that embedded secure elements can reduce updatability as only current security functions are implemented in hardware. Further research in the area of hardware security mechanisms could improve on yet unsolved aspects such as the detection and prevention of hardware trojans and the protection against intellectual property theft through reverse engineering [55].

Authenticated Code and Secure Boot are further fundamental building blocks for the security of the overall system. They are used to protect the software integrity of systems and thus, by extension, assure the authenticity (**S3**) of any interaction with that system and mitigate its manipulation through remote or direct physical interaction (**A3**). For this, any code is authenticated via digital signatures or similar, which are then used during the boot process of the system to ensure that only authenticated code is executed [18]. However, a recent paper on secure boot in an automotive setting outlines various challenges that still need to be addressed [57]. In particular, an unbroken and properly rooted chain of trust throughout the entire boot process is of utmost importance.

A Root of Trust is inevitable for authentication (**S3**) across various levels and to enable further secure communication with the system. When relying on root credentials, challenges during deployment (**A1**) and exclusion (**A2**) of devices have to be considered. Certificates, as extensively used in TLS [53], cryptographically link an identity to a public key, which can then be used for authentication and key agreement, but revocation is non-trivial. Subscriber Identity Module (SIM) and embedded SIM (eSIM) cards, are commonly used for authentication in mobile networks, but several security issues arise from a lack of authentication and protection of the communication between SIM and modem [75]. Physical Unclonable Functions (PUF) promise to be an invaluable tool to securely bind keys to a device. Here, developments in the area of nanotechnology-based PUFs and asymmetric keys derived from PUFs are particularly interesting [19]. As PUFs might also provide tamper-resistance, such mechanisms further address the challenge of easier access to the system (**A3**). Moreover, recent open-source projects such as OpenTitan [1], promise to close the remaining gaps between hardware and software security. Here, updatability (**R2**) is also considered on the lowest layers and built into the architecture [18].

4.4 Network Knowledge

Finally, detailed knowledge about a wireless network, especially w.r.t. topology and capabilities, provides ample opportunities to strengthen its secure and reliable use. Beneficial knowledge ranges from general propagation conditions over context awareness of devices to redundancy considerations for applications.

Propagation Conditions lead to an irregular availability (**S2**) of a wireless network. In addition, reaching a desired throughput to tackle network limitations (**C3**) requires sufficient signal power. Therefore, detailed network planning

is mandatory for secure wireless communication. For public networks, this planning process is conducted by an MNO and the users are confronted with the results. For shared and private networks, the critical infrastructure operator can optimize the receptions based on its applications and needs. Conducting such an optimization is challenging and requires knowledge about the expected reception at different locations or areas. Propagation models are well researched and can assist in this task [51]. However, conducting a targeted measurement campaign is often desirable [49]. The resulting data (from models or campaigns) can be used to tackle the challenges of availability (**S2**) and mobility (**C2**).

Context Awareness of a device in a wireless network plays a fundamental role in adjusting security mechanisms to current requirements and conditions. The most prominent context is the position (geographical coordinates) of a device, which is particularly relevant when considering mobility (**C2**). Coordinates can be obtained either manually during roll-out (for stationary devices), automatically via technologies such as Global Positioning System (GPS), or even with the communication technology itself [9]. For 6G, the combination of communication and sensing is regarded as one major innovation [37]. Other relevant context informations are the criticality of the application the device is used for, if the device has been recently moved, or even other environmental data such as the temperature. In particular, such context information is useful to detect manipulation or unwanted movement of the devices, which addresses the challenge of easier physical access to devices (**A3**). In addition, context information provides the opportunity to dynamically influence security parameters such as cryptographic algorithms based on the current context [23] to adjust to varying network limitations (**C3**) and available system resources (**C4**).

Roaming and Redundancy through the utilization of multiple wireless network technologies can be highly beneficial for critical infrastructures to improve reliability (**C1**) and availability (**S2**) in case of network failures or targeted attacks such as jamming. To this end, a self-configuring multi-access gateway can be employed to meet the strict requirements in critical infrastructure [45]. In general, there are two possible scenarios for such a gateway. First, multiple technologies are used simultaneously, which is particularly beneficial for mobility (**C2**) but also enhances confidentiality (**S1**). However, a mechanism is needed which distributes communication over the different technologies which increases the system complexity [44]. When this mechanism is aware of the application context, delay-critical applications may use technologies such as 5G while low-priority data is transferred via LoRaWAN. Second, one technology is preferred and the others function purely as backup, thereby increasing the availability (**S2**) without additional system complexity.

5 Discussion and Conclusion

With the increasing trend towards wireless communication in general, a similar tendency and corresponding benefits can be observed for critical infrastructure. Most importantly, wireless communication affords the cost-effective interconnec-

tion of a multitude of devices without the need for rigid infrastructure. Moreover, it enables the mobility of devices and their deployment in remote areas. However, the diverse set of available wireless technologies and their different characteristics challenge the application of wireless communication in critical infrastructure. Most importantly, easy access to the transmission medium and the use of shared or public infrastructure give rise to serious security challenges.

In this paper, we categorized the relevant challenges that need to be addressed to enable the use of wireless communication in critical infrastructure alongside various dimensions. Network and device constraints arise from characteristics of wireless communication as well as limitations of the network and the utilized devices. Moreover, network security challenges must be addressed with a focus on (end-to-end) confidentiality and integrity protection, particularly critical availability, and authentication towards the network and communication peers. Novel device security challenges arise especially through the easier physical access to devices but also extend to the deployability and exclusion of devices. Lastly, application-specific requirements cover the need for flexibility of the system w.r.t. interoperability, updatability, and the consideration of future requirements to which a too-inflexible system cannot adapt. This includes the stringent legal and regulatory requirements for critical infrastructure which could further tighten over time.

Current approaches and research trends already provide a multitude of opportunities to secure the wireless communication of critical infrastructure by addressing the identified challenges. Network security mechanisms address reliability and limitations to some extent, but confidentiality and integrity protection are limited to hop-by-hop security. For communication security on a higher layer, several approaches promise to enhance efficiency and address network and device limitations through beneficial configuration, extension, or optimization. Within the scope of device security, several hardware and software security mechanisms can be identified as promising building blocks for the overall security. By combining them in a secure architecture with trust rooted in hardware, an unbroken chain of trust could be achieved. Moreover, detailed network knowledge is particularly promising for addressing challenges such as reliability and mobility.

Our work highlights the opportunities for securing wireless communication in critical infrastructure and identifies avenues for further research to fully capitalize on the benefits of wireless communication in critical infrastructure while guaranteeing strong security. Overall, no single approach is sufficient to overcome all the challenges nor is this necessary. Rather, an interplay of multiple solutions must be strived for to achieve a resilient and secure system. To this end, this paper aims to spark and guide further research efforts toward coherent yet adaptable solutions that address the unique challenges of securing wireless communication in critical infrastructure.

Acknowledgments This work has been funded by the German Federal Office for Information Security (BSI) under project funding reference numbers 01MO23003A, 01MO23003B, 01MO23003C and 01MO23003D (PlusMoSmart). The responsibility for the content of this publication lies with the authors.

References

1. OpenTitan Project. <https://opentitan.org>
2. Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3: Intelligente Messsysteme. TR 03116-3, Federal Office for Information Security (BSI) (2023)
3. Alcaraz, C., et al.: Critical infrastructure protection: Requirements and challenges for the 21st century. *Int. J. Crit. Infrastruct. Prot.* **8** (2015)
4. Armknecht, F., et al.: ProMACs: Progressive and Resynchronizing MACs for Continuous Efficient Authentication of Message Streams. In: *ACM CCS* (2020)
5. Bader, L., et al.: Comprehensively Analyzing the Impact of Cyberattacks on Power Grids. In: *IEEE EuroS&P* (2023)
6. Bader, L., et al.: METRICS: A Methodology for Evaluating and Testing the Resilience of Industrial Control Systems to Cyberattacks. In: *CyberICPS* (2023)
7. Bormann, C., et al.: Terminology for constrained-node networks. RFC 7228 (2014)
8. Bundesnetzagentur: 450 MHz. www.bundesnetzagentur.de/450mhz.
9. Conti, A., et al.: Location Awareness in Beyond 5G Networks. *IEEE Communications Magazine* **59**(11) (2021)
10. Dahlmanns, M., et al.: Easing the Conscience with OPC UA: An Internet-Wide Study on Insecure Deployments. In: *IMC* (2020)
11. Dahlmanns, M., et al.: Missed Opportunities: Measuring the Untapped TLS Support in the Industrial Internet of Things. In: *ACM ASIA CCS* (2022)
12. Dahlmanns, M., et al.: Transparent End-to-End Security for Publish/Subscribe Communication in Cyber-Physical Systems. In: *ACM SaT-CPS* (2021)
13. Dileep, G.: A survey on smart grid technologies and applications. *Renewable energy* **146**, 2589–2625 (2020)
14. Echeverría, S., et al.: Authentication and Authorization for IoT Devices in Disadvantaged Environments. In: *IEEE 5th WF-IoT* (2019)
15. Eggert, M., et al.: SensorCloud: Towards the Interdisciplinary Development of a Trustworthy Platform for Globally Interconnected Sensors and Actuators. In: *Trusted Cloud Computing* (2014)
16. Elayoubi, S.E., et al.: Performance evaluation of frequency planning schemes in OFDMA-based networks. *IEEE Trans. Wirel. Commun.* **7**(5) (2008)
17. Falanji, R., et al.: Range and Capacity of LoRa 2.4 GHz. In: *MobiQuitous* (2022)
18. Frazelle, J.: Securing the Boot Process: The Hardware Root of Trust. *Queue* (2020)
19. Gao, Y., et al.: Physical unclonable functions. *Nature Electronics* (2020)
20. Glebke, R., et al.: A Case for Integrated Data Processing in Large-Scale Cyber-Physical Systems. In: *HICSS* (2019)
21. GSMA: Security Features of LTE-M and NB-IoT Networks. Tech. rep., GSM Association (GSMA) (2019)
22. Hamid, B., et al.: Cyber security issues and challenges for smart cities: A survey. In: *MACS* (2019)
23. Hellaoui, H., et al.: Energy efficiency in security of 5G-based IoT: An end-to-end adaptive approach. *IEEE Internet of Things Journal* **7**(7) (2020)
24. Henze, M., et al.: Network Security and Privacy for Cyber-Physical Systems. In: *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications* (2017)
25. Henze, M., et al.: Maintaining User Control While Storing and Processing Sensor Data in the Cloud. *IJGHPC* **5**(4) (2013)
26. Henze, M., et al.: A Trust Point-based Security Architecture for Sensor Data in the Cloud. In: *Trusted Cloud Computing* (2014)

27. Henze, M., et al.: Distributed Configuration, Authorization and Management in the Cloud-based Internet of Things. In: IEEE TrustCom (2017)
28. Hiller, J., et al.: Secure Low Latency Communication for Constrained Industrial IoT Scenarios. In: IEEE LCN (2018)
29. Hiller, J., et al.: The Case for Session Sharing: Relieving Clients from TLS Handshake Overheads. In: IEEE LCN Symposium (2019)
30. Hummen, R., et al.: Delegation-based authentication and authorization for the IP-based Internet of Things. In: IEEE SECON (2014)
31. Hussain, S., et al.: LTEInspector: A systematic approach for adversarial testing of 4G LTE. In: NDSS Symposium (2018)
32. Jaitly, S., et al.: Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: A survey. In: Comptelix (2017)
33. Kanwal, K., et al.: Reduced early handover for energy saving in LTE networks. *IEEE Communications Letters* **20**(1), 153–156 (2015)
34. Khalifeh, A., et al.: A Survey of 5G Emerging Wireless Technologies Featuring LoRaWAN, Sigfox, NB-IoT and LTE-M. In: WiSPNET (2019)
35. Klaer, B., et al.: Graph-based Model of Smart Grid Architectures. In: SEST (2020)
36. Krause, T., et al.: Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors* **21**(18) (2021)
37. Liu, F., et al.: Integrated sensing and communications: Towards dual-functional wireless networks for 6G and beyond. *IEEE J-SAC* (2022)
38. Liu, R., et al.: Application of 5G network slicing technology in smart grid. In: ICBAIE (2021)
39. Lukić, M., et al.: Data flow in low-power wide-area IoT applications. In: 2018 26th Telecommunications Forum (TELFOR). pp. 1–4 (2018)
40. Luo, K., et al.: An Empirical Analysis of the Progress in Wireless Communication Generations. In: MobiQuitous (2020)
41. Lutze, L., et al.: A modular framework for evaluating smart grid communication protocols over mobile networks. In: IEEE SmartGridComm (2023)
42. Lyczkowski, E., et al.: Wireless communication in industrial applications. In: ETFA (2019)
43. Mecheva, T., et al.: Cybersecurity in intelligent transportation systems. *Computers* **9**(4) (2020)
44. Mogensen, R.S., et al.: Selective Redundant MP-QUIC for 5G Mission Critical Wireless Applications. In: VTC2019-Spring (2019)
45. Mogensen, R.S., et al.: Implementation and trial evaluation of a wireless manufacturing execution system for industry 4.0. In: VTC2019-Fall (2019)
46. Mpitziopoulos, A., et al.: A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys & Tutorials* **11**(4) (2009)
47. Osanaiye, O.A., et al.: Denial of Service Defence for Resource Availability in Wireless Sensor Networks. *IEEE Access* **6** (2018)
48. Rademacher, M., et al.: Quantifying the spectrum occupancy in an outdoor 5 GHz WiFi network with directional antennas. In: WCNC (2018)
49. Rademacher, M., et al.: Path Loss in Urban LoRa Networks: A Large-Scale Measurement Study. In: VTC2021-Fall (2021)
50. Rademacher, M., et al.: Bounds for the Scalability of TLS over LoRaWAN. In: ITG-Symposium Mobile Communication (2022)
51. Rappaport, T.S., et al.: Overview of millimeter wave communications for fifth-generation (5G) wireless networks—With a focus on propagation models. *IEEE Transactions on Antennas and Propagation* **65**(12) (2017)

52. Rathore, H., et al.: A review of security challenges, attacks and resolutions for wireless medical devices. In: IWCMC (2017)
53. Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446 (2018)
54. Restuccia, G., et al.: Low-Power IoT Communication Security: On the Performance of DTLS and TLS 1.3. In: PEMWN (2020)
55. Roy, A., et al.: Device-specific security challenges and solution in IoT edge computing: a review. *The Journal of Supercomputing* (2023)
56. Santesson, S., et al.: Transport Layer Security (TLS) Cached Information Extension. RFC 7924 (2016)
57. Sanwald, S., et al.: Secure Boot Revisited: Challenges for Secure Implementations in the Automotive Domain. Escar Europe: Embedded Security in Cars (2020)
58. Schläpfer, T., et al.: Security on IoT Devices with Secure Elements. In: Embedded World Conference (2019)
59. Serror, M., et al.: Challenges and Opportunities in Securing the Industrial Internet of Things. *IEEE Transactions on Industrial Informatics* **17**(5) (2021)
60. Sheffer, Y., et al.: Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). RFC 9325 (2022)
61. Somasundaram, R., et al.: Review of security challenges in healthcare internet of things. *Wireless Networks* **27** (2021)
62. Ta-Shma, P., et al.: An ingestion and analytics architecture for iot applied to smart city use cases. *IEEE Internet of Things Journal* **5**(2) (2018)
63. Tayyab, M., et al.: A survey on handover management: From LTE to NR. *IEEE Access* **7**, 118907–118930 (2019)
64. The Things Industries B.V.: The Things Network. <https://www.thethingsnetwork.org/>
65. Thomassen, M.S.E., et al.: A Study of Extensive LoRaWAN Downlink Communication in a Mobility Scenario. In: *MobiQuitous* (2022)
66. Touqeer, H., et al.: Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing* **77**(12) (2021)
67. Tuptuk, N., et al.: A systematic review of the state of cyber-security in water systems. *Water* **13**(1) (2021)
68. van der Velde, D., et al.: Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures. In: *IEEE ENERGYCon* (2020)
69. Wagner, E., et al.: Take a Bite of the Reality Sandwich: Revisiting the Security of Progressive Message Authentication Codes. In: *ACM WiSec* (2022)
70. Wagner, E., et al.: Retrofitting Integrity Protection into Unused Header Fields of Legacy Industrial Protocols. In: *IEEE LCN* (2023)
71. Wagner, E., et al.: BP-MAC: Fast Authentication for Short Messages. In: *ACM WiSec* (2022)
72. Wagner, E., et al.: When and How to Aggregate Message Authentication Codes on Lossy Channels? In: *ACNS* (2024)
73. Wolsing, K., et al.: IPAL: Breaking up Silos of Protocol-dependent and Domain-specific Industrial Intrusion Detection Systems. In: *RAID* (2022)
74. Zhang, K., et al.: Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine* **55**(1) (2017)
75. Zhao, J., et al.: SecureSIM: Rethinking Authentication and Access Control for SIM/ESIM. In: *MobiCom* (2021)