Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

A systematic literature review on wireless security testbeds in the cyber-physical realm

Vyron Kampourakis*, Vasileios Gkioulos, Sokratis Katsikas

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 2802 Gjøvik, Norway

ARTICLE INFO

Article history:
Received 30 April 2023
Revised 26 June 2023
Accepted 4 July 2023
Available online 7 July 2023

Keywords:
SLR
CPS
CI
Security testbeds
Wireless technologies
Cybersecurity

ABSTRACT

The Cyber-Physical System (CPS) lies in the core of Industry 4.0, accelerating the convergence of formerly barricaded operational technology systems with modern information technology ones. Nevertheless, the increased connectivity in terms of both wired and wireless links and associated attack surfaces that comes along, requires higher security for safeguarding critical industrial systems and manufacturing lines from cyberattacks. In this rapidly evolving ecosystem, security testbeds have emerged as a versatile, cost-effective solution for investigating potential attack vectors and devising appropriate countermeasures, without putting the real system at risk. The present work seeks to address a prominent literature gap, namely, the lack of a systematic review regarding the use of wireless-oriented security testbeds in CPS. We contribute an overarching, manifold review on this topic from 2016 onward, examining the various literature works from diverse angles, namely, the wireless technologies used, the implemented attacks, the employed security controls, and more. The analysis is done on a per-sector basis, including water and wastewater systems, healthcare, transportation, agriculture, energy, maritime, unmanned aircraft systems, and others. Finally yet importantly, we discuss key takeaways, open issues, and challenges. The key observations of our analysis, including almost 50 articles, can be wrapped up into two salient points: on the one hand, wireless technologies are increasingly penetrating into the CPS domain as an orthogonal, versatile solution to their wired counterparts, but on the other, they widen the window of opportunity for threat actors targeting wireless links. In this context, testbed thoroughness and security as a trade-off seem to be of major importance, alongside a modular, possibly sector-neutral reference architecture that overarches the peculiarities of CPS. Overall, to our knowledge, this work provides the first full-fledged survey on the use of wireless-oriented security testbeds in CPS, and it is therefore anticipated to serve as a groundwork and touchstone for several stakeholders at different levels.

1. Introduction

According to NIST (Griffor et al., 2017), “cyber-physical systems are smart systems that include engineered interacting networks of physical and computational components”, therefore they are integrations of computation, networking, and physical processes. A typical CPS is composed of sensors used to perceive changes in the physical environment, actuators to control or influence these changes, and computing and control units to analyze the impacts of such changes, make decisions, and promptly respond in an automated way. Nowadays, in the era of Industry 4.0, manufacturers are gradually incorporating modern technologies, including Internet of Things (IoT) or Industrial IoT (IIoT), Artificial Intelligence (AI) and Machine Learning (ML), and cloud computing and analytics into their operations.

These advancements have placed CPS at the epicenter of Industrial Systems (IS) and Critical Infrastructures (CI), rendering them an even more alluring target for a variety of threat actors. That is, the penetration of contemporary Information Technology (IT) devices, networks, and services into the traditional Operational Technology (OT)-oriented IS intensifies complexity and significantly augments the attack surface of the entire system. Simply put, the very same connectivity of OT equipment that improves manufacturing processes inevitably creates new opportunities for diverse categories of threat actors. In this context, the digital transformation to Industry 4.0, stresses the need for a cybersecurity approach that considers both IT and OT equipment and networks in a holistic manner.

* Corresponding author.
E-mail addresses: vyron.kampourakis@ntnu.no (V. Kampourakis), vasileios.gkioulos@ntnu.no (V. Gkioulos), sokratis.katsikas@ntnu.no (S. Katsikas).

https://doi.org/10.1016/j.cose.2023.103383

In the same vein, wireless technologies are gradually and consistently adopted in CPS, IS, and CI ecosystems (Ahmadi et al., 2018; Li et al., 2017; Makrakis et al., 2021). For instance, the IEEE 802.11 protocol, commercially known as Wireless-Fidelity (Wi-Fi), is used for enabling communications among the physical components, say, sensors, actuators, controllers, and eventually their handler's Human Monitoring Interface (HMI). Another wireless technology that is often utilized for data transfer amongst the physical components and their controllers, say, Programmable Logic Controllers (PLC) and a collection of sensors and actuators, creating a wireless Low-Rate Wireless Personal Area Network (LR-WPAN), is the IEEE 802.15.4 standard. For example, the well-known ZigBee protocol is an IEEE 802.15.4-based specification. Several other wireless protocols, including IEEE 802.15.6, ITU-T G.99, ISA100.11a, WIA-PA, and Radio Frequency Identification (RFID), are oftentimes met in CPS, thus increasing susceptibility to attacks that are either specific to the inherently open wireless medium or the particular underlying wireless technology. Apart from augmenting the attack surface, with previously uncommon to the CPS realm attacks, wireless technologies do not require physical access to the network backbone, unlike their wired counterparts. In this context, wireless technologies exhibit increased susceptibility to a wide range of attack vectors, including eavesdropping, Man-in-the-Middle (MitM), unauthorized access, and Denial-of-Service (DoS) at the lower layers of the protocol stack. For instance, the openness of the wireless communication medium makes passive and active attacks, say, jamming (Adil et al., 2020; Almaiah, 2021; Mpitziopoulos et al., 2009; Vadlamani et al., 2016), much easier than in legacy wired environments. Under this prism, any malevolent actor in the vicinity of a wireless network may be in a position to attack and possibly penetrate the system; next, they can move laterally towards high-value targets (Smiliotopoulos et al., 2022; 2023). Moreover, as several wireless technologies are still quite new, their security features need to go through the test of time. Putting it another way, zero-days in wireless protocols proliferate. Notwithstanding this threatening mix of wired and wireless domains in the CPS terrain, so far, little attention has been given to the literature regarding security issues.

The penetration of wireless technologies into the CPS domain turn CPSs into more flexible, agile, and cost-effective systems. However, from a security perspective, such technologies have been mostly scrutinized in non-critical settings, i.e., houses, small office/home (SOHO), or business premises. Hence, a key question arises: how do wireless technologies affect the security of other systems, and even more, system-of-systems (e.g., a smart city), when integrated with legacy wired infrastructures, including CPS? Despite the urgency of contemplating appropriate answers, the literature scarcely considers works with a focus on wireless security aspects in CPS ecosystems. It is true however that, as this survey identified, in the last three years an increasing number of works addresses such aspects in CPS by means of security testbeds.

To this end, the focus of the present work is on wireless-oriented testbeds destined to CPS security evaluation. As a general rule, the main goal of such testbeds is to either evaluate attacks, countermeasures (also referred to as "controls" in the following), or both. This is because real-time experimentation with the real system, especially a CI one, for security evaluation purposes is considered risky; a disruption of its normal operation could be catastrophic, possibly endangering human lives or causing physical destruction. In this context, security testbeds have emerged as a proper complementary solution, fitted for identifying and addressing any related risk without jeopardizing the operation of the real system.

In view of the above, this work offers the first to our knowledge Systematic Literature Review (SLR) on testbeds concentrating on wireless security issues, either for assessing certain attacks or devising and evaluating appropriate countermeasures. Briefly, the main question that the current work seeks to answer is: What is the state-of-the-art regarding the utilization of wireless-oriented security testbeds in the CPS realm? Particularly, as explained further down, the focus is on the wireless technologies used, the associated hardware and software tools, the attacks and countermeasures considered, and the possible limitations and challenges. The survey spans a period of eight years, i.e., from 2016 to 2023, and only considers testbeds that involve CPS; works in this ecosystem before 2016 are scarce and not CPS-focused. Particularly, vis-á-vis similar survey works, the current one contributes to the below key points.

- The survey is all-encompassing, incorporating relevant testbeds across multiple sectors of application; water and wastewater systems, healthcare, transportation, agriculture, energy, unmanned aircraft systems, maritime, and others.
- The analysis of the included testbeds is done in a manifold, comprehensive manner. That is, we not only detail the various wireless protocols used throughout the testbeds, but also provide overarching categorizations regarding the attacks and countermeasures considered by each of them. The software and hardware tools used in each testbed are also summarized on a per-sector-of-application basis.
- On the basis of our analysis, we summarize deficits, open issues, and challenges regarding the creation and deployment of such testbeds, which can serve as breakthrough points for future studies and practical implementations.

The rest of the paper is organized as follows. The next section presents related surveys and comparative studies in this field. Section 3 details our methodology. The literature review regarding the various identified wireless testbeds is provided in Section 4. Section 5 elaborates on three key aspects of the testbeds, namely, wireless protocols, attacks, and countermeasures, providing also classifications for the latter two. Takeaways, open issues, and challenges are given in Section 6. The last section concludes and gives pointers to future work.

2. Related work

This section summarizes relevant surveys that at least touch upon wireless security testbeds in the context of CPS. Under this basic restriction, works like the ones presented in Al Nafea and Almaiah (2021); Alamer and Almaiah (2021); Almaiah et al. (2021); Bubukayr and Almaiah (2021); Nazir et al. (2021) are deliberately excluded due to insufficient coverage of wireless-oriented testbeds in the context of CPS. We only consider contributions published between 2016 and 2023 and elaborate on wireless security, either from a defensive or offensive viewpoint. As shown in Table 1, the included works are categorized in reverse chronological order based on up to what degree each of them addresses four key aspects, namely wireless technologies, security testbeds, attacks, and controls (countermeasures).

The recent work by Agrawal and Kumar (2022) discussed a variety of security features in terms of Industrial CPS (ICPS), focusing on vulnerabilities and attacks against CPS components. They performed a decade-wide survey, resulting in a comparative analysis of the identified literature. Namely, they compared the various works based on each work's objective, the defensive approach used, the experimental testbed or simulator used, and the derived conclusions. Moreover, with reference to system resilience, they pinpointed several security issues that are omnipresent in industrial CPS settings. Nevertheless, the authors insufficiently examined the literature regarding wireless technologies in the context of modern CPS.

Table 1
Comparative analysis of relevant surveys. A ●, ◐, or ○ symbol indicates that the corresponding work fully, partially, or not at all addresses one of the four key topics, respectively.

Year	Security testbeds	Wireless	Attacks	Controls
2022 Agrawal and Kumar (2022), 2021 Conti et al. (2021)	●	○	●	●
2022 Kayan et al. (2022); Kim et al. (2022b), 2017 Humayed et al. (2017)	○	◐	●	●
2022 Lydia et al. (2022), 2017 Xu et al. (2017)	◐	○	●	●
2021 Yadav and Paul (2021), 2016 McLaughlin et al. (2016)	◐	◐	●	●
2021 Makrakis et al. (2021)	○	◐	●	◐
2022 Altulaihan et al. (2022), 2020 Yaacoub et al. (2020)	○	●	●	●
2017 Li et al. (2017)	○	●	○	○
2017 Burg et al. (2017)	○	●	●	○
2017 Giraldo et al. (2017)	○	○	●	●
2016 Cintuglu et al. (2016)	●	◐	○	○
This work	●	●	●	●

The study by Kayan et al. (2022) reviewed ICPS from the lens of cybersecurity. They meticulously examined the ICPS cybersecurity attack surface to pinpoint current threats, challenges, and countermeasures. Their review work is one of the few that addressed wireless protocols in industrial settings, specifically in the era of Industry 4.0. To this end, a detailed classification of the wireless communication protocols according to standard availability, communication type, and network topology was suggested. They also proposed an attack taxonomy, evaluating real-life ICPS cyber incidents. Last but not least, they examined similar studies with an eye towards defensive mechanisms and how they could be utilized against imminent cyber threats in ICPS. Despite the completeness of their work, the authors did not consider security testbeds in their survey, focusing only on past cyber incidents in the ICPS domain.

Lydia et al. (2022) surveyed several works, indicating the need for securing CPS. First off, they analyzed a plethora of attacks linked with CPS. To clarify the diversity among individual attacks, they categorized them as data integrity, delay, intrusion, replay, and sensor and actuator oriented. This classification facilitated the modeling and detection of attacks that commonly affect CPS. They also provided an overview of the various CPS security scenarios, emphasizing the urgency to confront such threats. From their analysis, it is derived that CPS security testbeds are instrumental in developing proper security controls; they also offer a brief listing of the available testbeds destined for CPS. Whilst the authors also considered sensors and actuator-related attacks, they did not elaborate on relevant wireless threats.

In their survey, Kim et al. (2022b) discussed key threats and adjacent controls toward building resilient CPS. Their major contribution is a taxonomy of the identified cyber-physical attacks based on three features: attack surface, attack location, and stealthiness. The purpose of this classification, along with an analysis of the impact of such cyber-physical attacks, is to aid the interested parties in recognizing key requirements. In the same mindset, they reviewed existing anomaly detection techniques against the identified cyber-physical attacks. Despite that their survey sufficiently mapped the attack surface alongside an analysis of proper controls, they scarcely mentioned security testbeds as an appropriate way to scrutinize a CPS. Moreover, they referred to a rather small number of attack incidents that exploited existing vulnerabilities in wireless technologies.

Altulaihan et al. (2022) conducted an SLR towards identifying the commonest threats in IoT environments. They classified the identified threats across the three layers of IoT architecture, namely, perception, network, and application. No less important, they included relevant countermeasures and mitigation techniques along with standard methods to safeguard IoT infrastructures. Their review considered multiple aspects of wireless technologies, nevertheless they did not touch upon security testbeds as a means to identify and evaluate cyber threats relevant to the IoT realm.

The work by Yadav and Paul (2021) focused on Supervisory Control and Data Acquisition and Industrial Control Systems (SCADA/ICS). Specifically, they investigated pertinent assaults with the aim to shed light on the evolving security terrain regarding SCADA systems. They also provided a brief analysis of relevant Intrusion Detection Systems (IDS) along with a short study about SCADA testbeds. Precisely, they pinpointed that IDS can be improved in terms of placement policy, validation strategy, attack coverage, low latency, and false-positive detection rate. In addition, they mention other significant factors, including cost, scalability, and high fidelity, which should be considered during the development phase of any SCADA testbed. No less significantly, motivated by the evolution of SCADA from a monolithic architecture to an IoT-based SCADA, they discussed wireless technologies and the associated attack surface. They concluded by mentioning future trends, security gaps, and challenges.

Another comprehensive review targeting the security research in the ICS field was presented in Conti et al. (2021). The authors collected and classified security testbeds and datasets used in ICS literature. Their testbed-wise categorization was based on the functional elements involved in the testbed, separating them into three clusters, namely, physical, virtual, and hybrid. The different requirements and challenges in developing an ICS testbed were considered as well. Moreover, they summarized legacy attacks against ICS and discussed the way such attacks are implemented in different testbeds and datasets. From a defensive standpoint, they examined the so far used IDS in the context of the considered datasets. They concluded by providing empirical advisories and sound practices, regarding the development and utilization of testbeds, datasets, and IDSs. Nevertheless, they ignored the gradual penetration of wireless technologies in the ICS domain.

Major real-life cyberattacks against ICS and CI were presented in Makrakis et al. (2021). Particularly, the authors elaborated on several types of malicious actions against ICS and CI, pinpointing the root cause of each incident. A categorization of the relevant threats and the corresponding vulnerabilities based on various criteria were also given. On the downside, their analysis is confined to ICS, leaving aside other critical CPS like transportation and healthcare. Moreover, while the authors did refer to wireless technologies and protocols used in ICS from a security viewpoint, they did not focus on relevant testbeds.

A survey about CPS security in terms of limitations, issues, and future trends was presented by Yaacoub et al. (2020). Based on the generally admitted layering of CPS, namely perception, transmission, and application layer, they reviewed and categorized CPS-oriented threats, attacks, and vulnerabilities. In more detail, they separately investigated physical- and cyber-exploitable vulnerabilities that could materialize a threat, and eventually end up in a successful assault. Additionally, existing controls were presented and analyzed following a qualitative risk assessment method to identify the exposure magnitude for a CPS. The proposed method takes into account cryptographic, non-cryptographic, and forensics-based solutions in an effort to comprehend how each attack is performed. The authors correctly highlight the tight relation between CPS and IoT devices, therefore with wireless technologies across the three foregoing layers as well. On the other hand, their study excluded research done through security testbeds and is confined to qualitative analysis, including past cybersecurity incidents.

Li et al. (2017) offered a synopsis of the existing Industrial Wireless Networks (IWN) by discussing their architectural features and techniques. They also proposed a Quality of Service (QoS) and Quality of Data (QoD)-oriented architecture, concentrating on Industry 4.0 and IWN. Additionally, they highlighted key challenges that still need to be addressed within Industry 4.0; these include topology control, signal interference, communication protocols, and the interaction or interplay between IWN and other wireless or wired technologies. Nevertheless, they hardly discussed security and privacy issues that arise following the use of IWN in IS. Contrary to the present work, they also neglected security testbeds as an indirect means to assess a real-life IWN in the context of a CPS.

Humayed et al. (2017) examined the CPS security literature with the aim to establish a unified framework with a special focus on four representative CPS applications, namely ICS, smart grids, medical devices, and smart cars. Their survey spans three axes, namely, i) a taxonomy for threats, vulnerabilities, attacks, and controls, ii) CPS cyber, physical, and cyber-physical components, and iii) general CPS aspects as well as representative systems. Next, they elaborated on security aspects in the context of CPS, proposing a framework to better apprehend how an attack affecting the physical domain of a CPS can have adverse ramifications on the cyber domain and vice versa. They also adequately addressed threats and vulnerabilities along with their root causes, with special reference to wireless communications among the CPS components. No less significantly, they argued that their suggested framework can be used for developing suitable controls to deter attacks against CPS. However, security testbeds were not discussed as assessing tools of such complex systems, i.e., as a means to evaluate CPS-relevant attacks, vulnerabilities, and controls.

Burg et al. (2017) examined wireless technologies and communication protocols with an eye towards the blending of CPS and IoT. They surveyed the most relevant wireless standards, concentrating on the key security issues and features they integrate. To facilitate their analysis, they exhibited several existing vulnerabilities with examples and recent real-life attack incidents. They noticed that security breaches exposing wireless protocols and security inconsistencies in such systems happen increasingly frequently. On the other hand, their work did not elaborate on relevant security controls that can be applied for remediating such threats. CPS security testbeds were also left out of the scope of that work.

A survey of surveys regarding the security of CPSs was presented by Giraldo et al. (2017). The authors conducted a per CPS application domain study, including smart grid, ICS/SCADA systems, manufacturing, etc., examining attacks, defenses, research trends, network security, and more. They summarized their results by providing a comparison among the different key features considered by each survey. Wireless technologies and relevant security testbeds were not considered in the context of their survey.

Cintuglu et al. (2016) presented a study for smart grid cyber-physical testbeds. They concentrated on smart grid applications, test platforms, and communication infrastructure, also providing a comprehensive synopsis of existing testbeds. Additionally, they offered a theoretical appraisal per testbed in terms of support capacity, communication capability, security and privacy awareness, protocol support, and remote access capabilities. Even though the authors did consider wireless-oriented testbeds, they only did so for smart grids.

McLaughlin et al. (2016) discussed ICS cybersecurity in terms of hardware, firmware, software, network, and processes from both an offensive and defensive viewpoint. They emphasized vulnerability assessment methodologies, ICS testbeds, and attack vectors. From the defensive standpoint, they concluded that vulnerability assessment in ICS settings requires the deployment of multilayered testbeds with multiple pathways between the IT and OT components in the ICS. Nevertheless, their analysis regarding the wireless protocols' security in the context of ICS is incomplete.

Looking also through the ICS lens, Xu et al. (2017) revisited the vulnerabilities of ICS protocols with a reference to relevant real-life attack incidents. That is, the authors elaborated on proposed controls and various security testbeds that can be used to study such systems from both an offensive and defensive standpoint. However, their work did not address wireless technologies that can be exploited in the context of IoT, which are gradually coupled with ICS.

With reference to Table 1, it is obvious that the majority of the relevant surveys concentrate on either attacks or security controls, or both. This is done by either providing a taxonomy or classification scheme or detailing real-life security incidents. Some of them do describe, or at least touch upon, security testbeds (Agrawal and Kumar, 2022; Cintuglu et al., 2016; Conti et al., 2021; Lydia et al., 2022; McLaughlin et al., 2016; Xu et al., 2017; Yadav and Paul, 2021) as an appropriate way to scrutinize the resilience of a CPS system against cyberattacks. This is achieved by mentioning prominent examples of such testbeds in the literature. Moreover, from the third column of Table 1, it is rather clear that wireless technologies are indeed considered across the related works, but only four studies (Altulaihan et al., 2022; Burg et al., 2017; Li et al., 2017; Yaacoub et al., 2020) thoroughly examined wireless technologies present in the CPS realm. The wireless aspect in the context of CPS is also discussed in seven studies (Cintuglu et al., 2016; Humayed et al., 2017; Kayan et al., 2022; Kim et al., 2022b; Makrakis et al., 2021; McLaughlin et al., 2016; Yadav and Paul, 2021), but only partially. Collectively, to the best of our knowledge, so far, no survey sufficiently addressed all the criteria listed in the rightmost four columns of Table 1.

3. Methodology

As already mentioned, the current work contributes an SLR, discussing security testbeds that concentrate on one or more wireless technologies; such testbeds are basically used to identify, evaluate, and classify pertinent threats and security controls, without interfering with the real-life system. Precisely, as already explained in Section 1, the scope of the SLR at hand can be briefly outlined as follows:

- To identify the wireless protocols used in the CPS realm, especially in CI environments.
- To identify and classify prominent attacks and the corresponding controls investigated through the use of a testbed.
- To pinpoint the types of the utilized testbeds, also listing hardware and software tools and relevant equipment.
- To identify pertinent shortcomings, open issues, and challenges.

The present SLR abides by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Moher et al., 2015; Page et al., 2021) methodology, detailing the steps that should be followed when conducting an SLR. More precisely, the succession of steps followed to conduct the SLR is detailed below.

First, we searched major scientific databases as follows:

Table 2
List of inclusion and exclusion criteria.

	Inclusion-Exclusion	Description
Inclusion	Wireless-oriented testbeds	The testbed needs to be based on wireless technologies.
	CPS-relevant testbeds	Consider works that only describe testbeds that contain CPS components and concentrate on one or more CI sectors.
	Security-oriented testbeds	The testbed must have a cybersecurity focus.
	Comprehensiveness	Each testbed must cover adequately a number of attacks; note that some works refer only to attacks, omitting any discussion about the respective controls.
	Papers written in English	-
Exclusion	Type of literature	Conference abstracts, book reviews, conference info, discussion, editorials, mini-reviews, news, blogs, etc.

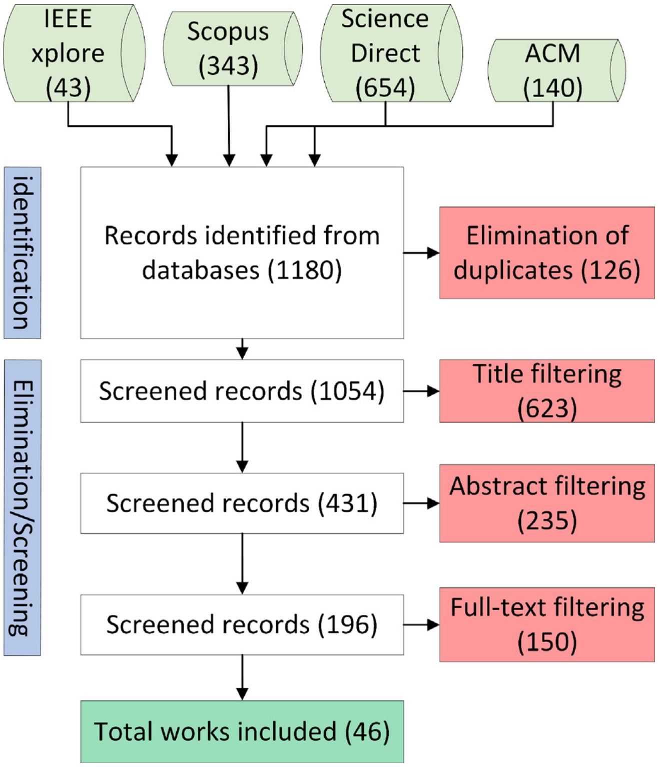

Fig. 1. A bird's eye view on the articles' screening and selection process.

- The relevant literature was approached through multiple major databases, namely, IEEE Xplore, ScienceDirect, Scopus, and ACM.
- The keywords used for compiling the search query were: "wireless" **AND** ("testbed" **OR** "test bed") **AND** ("cyber physical system" **OR** "critical infrastructure") **AND** "security".
- The examined literature spans a period of eight years, i.e., from 2016 to 2023.
- The duration for the completion of the SLR was approximately four calendar months, from Nov. 2022 to Apr. 2023.

Second, as presented in Table 2, the selection process was facilitated through a list of key inclusion/exclusion criteria. Based on these criteria, the literature was searched as depicted in Figure 1. As observed from the figure, the article selection procedure involved four consecutive phases and resulted in 46 publications. As a last step, each CPS-oriented security testbed described in each publication was analyzed in Section 4 based on six axes: the type of the testbed, the wireless protocol(s) used, the considered attacks, the utilized respective control(s), the attack entry point(s), and the employed evaluation metric(s).

4. Testbeds

As already mentioned in Section 3, this work deliberately excludes testbeds that are not explicitly destined to security. For testbeds that center on different aspects, including performance, robustness, or efficiency, the interested reader is referred to works like (Jecan et al., 2018; Kashef et al., 2021). Essentially, following a reverse chronological order, the current section is split into six subsections, each one concentrating on a diverse CI sector. That is, the identified testbeds are categorized based on the CI they belong to, and subsequently analyzed in accordance with their type, the wireless protocol(s) used, the considered attacks, the utilized respective control(s), and the attack entry point(s). For the sake of completeness, typically for testbeds that consider some countermeasure, we also include any evaluation metric used in the context of the respective work. Moreover, Table 9 outlines the key software or hardware components used for building each testbed.

Regarding attack entry points, it should be noted that a typical CPS is a multi-layered system comprising several components and networking elements. Therefore, from an attack surface viewpoint, an assailant can exploit numerous vulnerabilities and misconfigurations that may reside in different layers of the CPS close-loop as depicted in Figure 2. Particularly, this figure stems from the Purdue model (Williams, 1994), concentrating on the latter's bottom three layers, namely, physical process, intelligent devices, and control systems zones. This was done because the present work is interested mostly in the OT realm and the use of wireless technologies in these lower layers. Simply put, the emphasis is on the possible attacker's entry points, while the Purdue model offers a more generic framework for segmenting ICS networks. Note that not all the investigated CPSs, in the context of the identified testbeds, implemented all the layers of Figure 2, howbeit, for reasons of completeness, the figure illustrates all the layers that are within the scope of this work.

With reference to Figure 2, following a bottom-up approach, a threat actor can aim at the lower levels of a CPS entity, targeting the sensors and actuators and their interplay with the environment. Moving upwards, they can also aim for the communication links between the sensors/actuators and the control units to, say, manipulate the data transmitted from the sensors to the controller or vice versa. Last but not least, an attacker that resides in the top layer has analogous capabilities, as they can leverage the communication between the supervisory and the respective control units. In any case, the convergence of typical OT-oriented CPS systems with modern IT ones allows a threat actor to impose multiple layers of the underlying system.

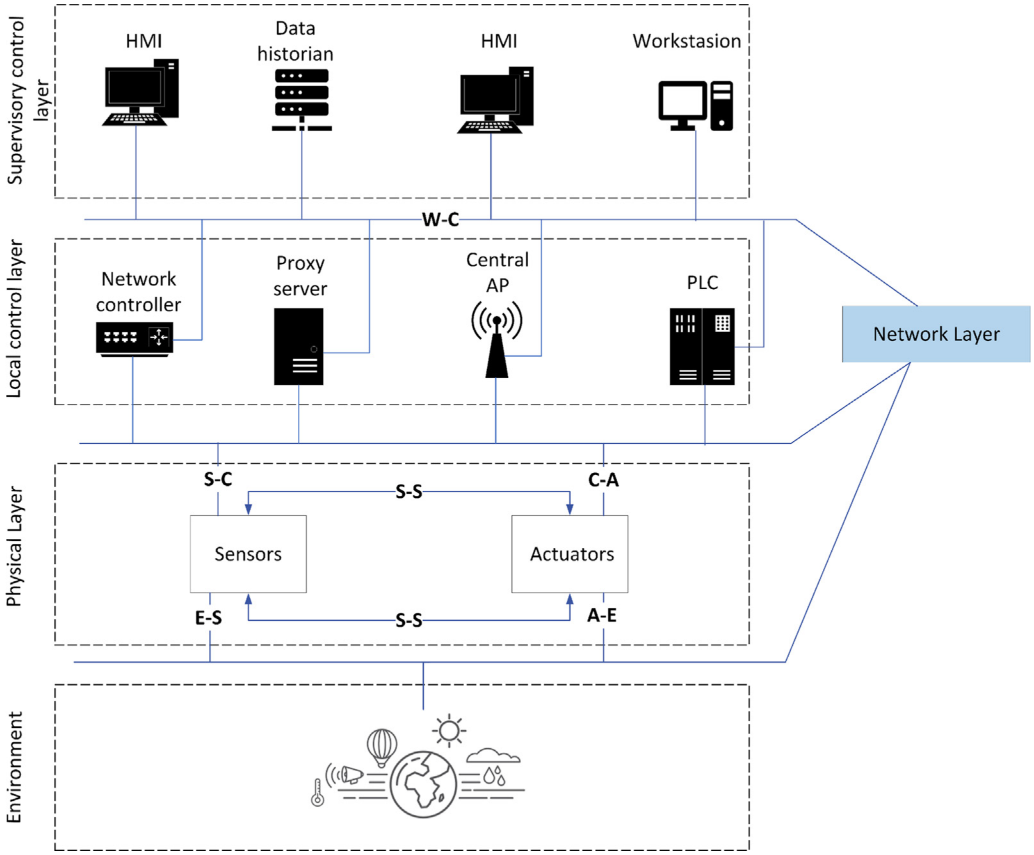

Fig. 2. Cyber-physical system close loop; A-E, E-S, S-S, S-C, C-A, W-C indicate potential entry points for an attacker. The acronyms represent the initial letter per stage of the loop: A-E, E-S, S-S, S-C, C-A, W-C, stand for Actuator-Environment, Environment-Sensor, Sensor-Sensor, Sensor-Control, Control-Actuator, Workstation-Control, respectively.

4.1. Water and Wastewater Systems

The work of Tomić et al. (2018a) focused on the resilience of CPS against jamming attacks exercised in the physical (PHY) layer. Such assaults aim to interfere with the system's wireless channels with the intention to disrupt them. To safeguard against this threat, they considered the classic time-triggered (Åström and Wittenmark, 2013) and other resource-aware event-triggered defensive (Heemels et al., 2012) schemes. The first scheme is used to provide safety and performance to the underlying system as they periodically receive sensor data and transmit control (corrective) signals. The second receives new measurements and transmits control signals only when stability and performance are unbalanced. To evaluate the robustness of these schemes they devised three different jamming attack scenarios, namely, constant, random, and protocol aware; in the first the attacker transmits constantly, in the second at random time periods, and in the third based on period and signal phase. The performance of the proposed schemes was evaluated based on two metrics; the deviation of the water level from a steady-state value and the Packet Delivery Ratio (PDR) in correlation with the percentage of time the jammer spends when transmitting the signal. They experimented on a smart water network, part of the *Waterbox* testbed (Kartakis et al., 2015), demonstrating that both the above-mentioned schemes are susceptible to constant and random jamming, while only the time-triggered control ones are susceptible to protocol-aware jamming. Finally, they proposed an enhancement by adding a dynamical estimator on top of each defensive scheme.

Prakash and Ahmed (2017) experimented on a wireless water treatment environment, focusing on Wi-Fi links. Specifically, their testbed is a wireless-only version of the Secure Water Treatment *SWaT* testbed (Mathur and Tippenhauer, 2016); a description of *SWaT* is given below. They showed that MitM attacks are feasible, therefore in-transit data can be compromised by both insiders and outsiders. Moreover, they showcased that an evildoer can place a rogue Access Point (AP) to intercept and possibly alter the communications between a PLC and the respective SCADA system. To mitigate this threat, namely to detect the presence of a rogue AP, they provided a fingerprint-based anomaly detection scheme based on the Received Signal Strength (RSS). Particularly, they used the mean and variance of the RSS along with its deviation from the normal pattern, revealing the presence of a rogue AP both inside and outside the plant premises. Finally, given a threshold value, they evaluated their scheme by means of True Positive Rate (TPR) and False Positive Rate (FPR) metrics.

Adepu et al. (2017) also relied on the *SWaT* testbed as an experimentation platform. They discussed jamming attacks, centering on the weakest wireless communication links from a jammer's perspective, also pinpointing possible ramifications to the targeted system; based on Mathur and Tippenhauer (2016), every wireless link in *SWaT* is governed through an industrial AP, thus creating a centralized Wireless Local Access Network (WLAN). Their experiments were conducted with the aid of a Software-Defined Radio (SDR) device, using Additive White Gaussian Noise (AWGN) and pulse tones (single or multiple) to create interference. They performed the jamming attacks in two different layers of *SWaT*, i.e., between the physical process and the PLCs, and between the PLCs and the respective Human-Machine Interface (HMI). We argue that, although this work examined such attacks only against *SWaT*, the underlying ideas are generic and can be applied to other CIs as well.

The well-known *SWaT* testbed was introduced by Mathur and Tippenhauer (2016). This testbed comprises a total of 46 sensors and actuators. Its main merit is that it enables experimental re-

Table 3
Testbeds identified in the water and wastewater systems sector. The "tag" column is used for the classification of works in Figures 5 and 6; the same stands for the rest of the tables in this section.

Tag	Year	Protocol	Attack	Entry point	Control	Evaluation metrics	Type
1	2018 Tomić et al. (2018a)	IEEE 802.11	Jamming	S-C, C-A	Time- and event-triggered control schemes	Deviation of water level, PDR	Physical
2	2017 Prakash and Ahmed (2017)	IEEE 802.11	Evil-twin	W-C	Anomaly detection through signal power deviations	TPR, FPR	Physical
3	2017 Adepu et al. (2017)	IEEE 802.11	Jamming	S-C, C-A, W-C	N/A	N/A	Physical
4	2016 Mathur and Tippenhauer (2016)	IEEE 802.11	Eavesdropping, brute force, evil-twin	S-C, C-A	N/A	N/A	Physical
5	2016 Adepu and Mathur (2016)	IEEE 802.11	ARP spoofing, data manipulation	S-C, C-A	Distributed detection based on physical invariants	N/A	Physical

search, spurring security by design for virtually any ICS. Specifically, *SWaT* represents a minimized version of a large modern water treatment system. Communications among sensors, actuators, and PLCs can be either wired or wireless via Ethernet or Wi-Fi links, respectively. With reference to wireless technologies, *SwaT* enables communications through an industrial AP, namely MOXA AWK-5222-EU, which is Wi-Fi Protected Access 2 (WPA2)-certified. Hence, the various components of *SwaT* are connected directly to the AP, creating a WLAN. By exploiting the *SWaT* topology, the authors demonstrated that legacy attacks stemming from the Wi-Fi domain, say, evil-twin (Chatzoglou et al., 2021a; Roth et al., 2008) or dictionary-based brute force to reveal the network's passphrase, is rather straightforward in a real-world ICS environment.

The *SWaT* testbed was also examined by Adepu and Mathur (2016). In more detail, they proposed a distributed attack detection method to reconnoiter Single-Stage Multi-Point (SSMP) attacks against infrastructures, similar to *SWaT*. Note that an SSMP attack aims at compromising one or more sensors or actuators residing at any layer of a CPS. After that, moving laterally, the attacker may be able to assault a PLC and prevent it from detecting and timely reacting to abnormalities in the system. As an attack vector, the particular study considered the wireless links between sensors and the corresponding PLCs. To this end, they exploited two basic attack mechanisms, namely, sensor data manipulation utilizing Address Resolution Protocol (ARP) spoofing as a means to achieve MitM. The novelty of the suggested detection method lies in observations regarding "physical process invariants", to determine whether the system is under attack or not. For example, in a water treatment system, this process pertains to the correlation between the level of water in a tank and the flow rate of incoming and outgoing water across the tank. Therefore, such invariants aid in the inspection of a system's state. These processes are hardcoded in each of the PLCs, facilitating the detection of potential attacks. On the downside, the authors concluded that the detection process on top of the various controllers' workload increases the computational demands, leaving room for future improvements.

Table 3 summarizes the basic testbed-related aspects per work included in this subsection. As observed from the table, all the testbeds concentrate on 802.11 links and consider a variety of attacks exercised on three different entry points with reference to Figure 2. Additionally, two of them introduce some security control, assessing it through the respective evaluation metrics. On a final note, all of them consider the *SWaT* testbed as their experimentation testbed.

4.2. Healthcare

Khadr et al. (2022) introduced a Parallel-Channel Security-aware Medium Access Control (PCS-MAC) for Cognitive Radio (CR) IoT-based networks. A CR caters for dynamic spectrum access to improve its utilization. The proposed algorithm confronts jamming attacks without the requirement for additional hardware. They specifically focused on the applicability of CR IoT-based networks in the healthcare sector, including remote patient monitoring systems and wearable IoT devices for health readings. PCS-MAC was evaluated against jamming attacks using the *FIT-IoT* testbed (Fambon et al., 2014). The latter is a multi-user, open-source testbed comprising 2,700 low-power wireless IoT sensor nodes equipped with the AT86RF231 radio chip, which is IEEE 802.15.4 compliant. Two jamming scenarios were considered: proactive and reactive. The first attempts to corrupt the CR-IoT transmissions over the available channels by transmitting jamming signals in fixed intervals. The second jams the channel only when a legitimate transmission is detected. The performance of PCS-MAC was evaluated against the MAX-POS (Salameh, 2012; 2013) and greedy algorithms, using throughput curves as the main metric. They showcased that their algorithm augments the network performance under jamming attacks, surpassing other algorithms like MAX-PoS.

Pu et al. (2022) contributed an Authentication Key Agreement protocol (AKA) scheme, called *liteAuth*. To achieve mutual authentication and session key agreement, the authors used the Tinkerbell map-based random shuffling, Physically Unclonable Functions (PUF), and Bitwise Exclusive OR (XOR) operation. Their scheme mutually authenticates a wireless medical device against the respective control network node, establishing a shared key used to protect the traffic; this is done with the aid of a proxy residing in the cloud. *LiteAuth* was formally verified through AVISPA (AVI, 0000), indicating that it is resilient against legacy attacks, as shown in Table 4. In addition, a physical testbed was developed for further evaluating the proposed AKA scheme. This was done in terms of security robustness and performance, comparing it with similar schemes, including PSLAP (Alzahrani et al., 2021) and HARCI (Alladi et al., 2020). Particularly, a Latte Panda microcomputer was used to simulate the medical device and the control node, while a laptop PC emulated the cloud server. They demonstrated that *LiteAuth* outperforms the PSLAP and HARCI schemes, using communication overhead, computation time, energy consumption, CPU time, and CPU cycles, as performance metrics.

We observed that the relevant literature contains several works similar to Pu et al. (2022). All of them suggest variants of AKA schemes originally proposed by others, with the aim to make them more efficient in terms of performance and increase their resilience against attacks. For instance, the work in Pu et al. (2022) stemmed from the PSLAP (Alzahrani et al., 2021) and HARCI (Alladi et al., 2020) AKA schemes, while that in Yu and Park (2022) provided an improvement of the AKA protocol initially proposed in Wang et al. (2021). Similarly, the authors in Almaiah et al. (2022) and Ali et al. (2022) proposed a hybrid trustworthy decentralized authentication and data preservation model and an IoT-based blockchain-enabled secure search-

Table 4
Testbeds identified in the healthcare sector.

Tag	Year	Protocol	Attack	Entry point	Control	Evaluation metric	Type
6	2022 Khadr et al. (2022)	ZigBee	Jamming	S-S	Parallel-Channel Security-aware Medium Access Control (PCS-MAC) algorithm	Throughput	Physical
7	2022 Yu and Park (2022)	IEEE 802.15.6	Eavesdropping, brute force, service disruption, masquerading	E-S, S-C	Authentication protocol based on blockchain technology and PUFs	Computation time, communication overhead	Simulated
8	2022 Pu et al. (2022)	IEEE 802.15.6	Eavesdropping, data manipulation, replay, service disruption, masquerading	E-S, S-C	Lightweight, anonymous authentication and key agreement protocol	Communication overhead, computation time, energy consumption, CPU time, CPU cycles	Simulated
9	2021 Alzahrani et al. (2021)	IEEE 802.15.6	Eavesdropping, brute force, replay, masquerading	E-S, S-C	Authenticated key agreement based on Burrows-Abadi-Needham (BAN) Burrows et al. (1990) logic	Computation time, communication overhead, energy consumption	Simulated
10	2021 Wang et al. (2021)	IEEE 802.15.6	Eavesdropping, data manipulation, replay, service disruption, masquerading	E-S, S-C	Authentication protocol based on blockchain technology and PUFs	Computation time, communication overhead	Simulated
11	2021 Hussain et al. (2021)	IEEE 802.11	Eavesdropping, data manipulation	S-C, W-C	Physical layer scheme (Gray code)	N/A	Physical
12	2021 Surminski et al. (2021)	IEEE 802.11	Eavesdropping, buffer overflow	C-A	Remote attestation	Runtime, energy consumption, communication overhead, race conditions	Hybrid
13	2020 Alladi et al. (2020)	IEEE 802.15.6	Eavesdropping, data manipulation, masquerading, ARP spoofing, replay	S-C, W-C	Two-way, two-stage authentication protocol using PUFs	Computation time	Simulated

able encryption approach, respectively. Overall, these works only used software-based tools and platforms to evaluate the proposed schemes, without providing dedicated testbeds to examine actual adversarial scenarios or proposing respective security controls. Nevertheless, for reasons of completeness, we opt to include such schemes in Table 4.

The work of Hussain et al. (2021) presented a lightweight PHY layer security scheme (a flip bit technique), namely the gray code, to secure transmitted patient readings in IoT-based health monitoring systems. They elaborated on the resilience of the proposed mechanism through a testbed. Precisely, they implemented two attack scenarios. The first placed the attacker anywhere in the cloud, enabling them to intercept the transmitting data between a patient and a hospital. The second placed the attacker between the wearable sensors used to collect data from the patient and the local wireless AP. Simply put, both these scenarios are typical cases of MitM attacks, where the assailant can eavesdrop on the packets and potentially alter their content or inject spurious information. Their testbed comprised a HealthyPi v4 shield (Hea, 0000) attached to a Raspberry Pi 4 Model B, and several medical sensors. They also proposed countermeasures based on the perceived changes in the RSS; any noticeable deviation in the RSS is an indication of eavesdropping attempts on the Wi-Fi link. Based on the previous assumption, the Raspberry Pi will either apply or not the gray code prior to forwarding any medical data to the cloud services.

Surminski et al. (2021) presented *RealSWATT*, a software-based remote attestation system for real-time embedded devices. Recall that remote attestation is a security mechanism that allows a party to verify the correct functionality of an untrusted remote device, creating a prover-verifier relation. The difference between *RealSWATT* and other similar systems is that it is designed to work within real-world IoT networks, connected through Wi-Fi, without the aid of custom hardware extensions or third-trusted computing components. *RealSWATT* was evaluated via a testbed comprising simulated IoT devices on NodeMCU ESP32 microcontrollers, a Wi-Fi AP acting as the IoT gateway, and a Raspberry Pi 3 as the verifier. The tested attack scenario was a MitM attack against a syringe pump (Wijnen et al., 2014), i.e., a medical device that injects medication into a patient at pre-defined time intervals. The performance of *RealSWATT* was assessed in terms of total runtime, power consumption, communication overhead, and others.

Table 4 recaps the basic characteristics of the identified testbeds for each work included in this subsection. From a quick look, five of the testbeds concentrated on 802.15.6, two of them on 802.11, and one on 802.15.4 (Zigbee). Moreover, with reference to Figure 2, all the considered attacks leverage five different entry points. All the proposed controls but one were evaluated by means of some conventional metric. On a final note, most of the deployed testbeds were simulated, and only two were fully physical.

4.3. Transportation

Shawky et al. (2023) proposed a PHY layer-based secret key extraction for AKA in Vehicular Ad-hoc Networks (VANETs). The suggested scheme utilizes the inherent randomness of the wireless channels to extract a secret cryptographic shared key. The authors incorporated blockchain technology to effectively distribute correction data pertinent to inconsistencies generated by the reciprocity aspects of the wireless channel. The utilized protocol for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) scenarios was IEEE 802.11p. They showcased that their approach aids

Table 5
Testbeds identified in the transportation sector.

Tag	Year	Protocol	Attack	Entry point	Control	Evaluation metrics	Type
14	2023 Shawky et al. (2023)	IEEE 802.11	Sybil, masquerading, data manipulation, replay	S-S, S-C	Blockchain-based secret key extraction	Computation time, communication overhead	Simulated
15	2022 Hidalgo et al. (2022)	IEEE 802.11	Service disruption	E-S, S-S, S-C	SDN-based framework	Accuracy, detection time	Hybrid
16	2022 Strohmeier et al. (2022)	ADS-B and GPS	Data manipulation	E-S	N/A	N/A	Physical
17	2021 Koroniotis et al. (2021)	IEEE 802.11, Z-wave, ZigBee, NFC, BLE, and LoRaWAN	Eavesdropping, service disruption, eternalblue, data manipulation, fuzzing, ARP spoofing, reverse TCP shell	E-S, S-C	N/A	N/A	Hybrid
18	2020 Petrillo et al. (2020)	IEEE 802.11	ARP Spoofing, data manipulation, service disruption	S-S	Adaptive synchronization-based algorithm	Mean-square position error	Simulated
19	2019 Kim et al. (2019)	IEEE 802.11	ARP spoofing	W-C	SDN-based	Time intervals between attack initiation and recovery	Hybrid
20	2019 Li et al. (2019b)	ZigBee	Eavesdropping	S-S, S-C	Secret key agreement	BMMR	Physical
21	2019 Basiri et al. (2019)	ZigBee	Eavesdropping, data manipulation	S-S, S-C	Graph theory solution (attacker-detector game)	N/A	Physical

in the detection of Sybil attacks, where the attacker masquerades as multiple innocent vehicles. Moreover, their scheme appears to be resilient against impersonation, on-path modification, and replay attacks. After checking the security properties of the proposed scheme through the AVISPA tool (AVI, 0000), the authors implemented a fully simulated testbed by means of the OMNeT++ (OMN, 0000), Veins (Vei, 0000), and SUMO (SUM, 0000) simulators. They evaluated their scheme based on two metrics, namely overall computation time and communication overhead. The results revealed that the proposed scheme was superior to previous studies (Li et al., 2019a; Sutrala et al., 2020; Zheng et al., 2019) in high-density traffic environments.

Hidalgo et al. (2022) presented *SerIoT* (Ser, 0000), a security framework that can be utilized in connected autonomous vehicle environments. *SerIoT* is based on Software-Defined Network (SDN) technology, equipped with path optimization mechanisms and anomaly detection modules to ensure the uninterrupted operation of the underlying system. The authors evaluated *SerIoT* in a Connected Intelligent Transportation Systems (C-ITS) setting. Particularly, vehicle fleet management and smart intersection were implemented, utilizing onboard units on each fleet member for intercommunication and roadside units for enabling the optimal flow of traffic, respectively. They evaluated the above-mentioned scenario, implementing a hybrid testbed. The latter included a virtually represented vehicle with the Dynacar (DYN, 0000) simulator and a Renault Twizy 80 (Twi, 0000) as an additional vehicle. Through the testbed, they showcased that with security modules like fleet management and smart intersections, DoS attacks can be prevented and continuous and safe traffic flow can be ensured. The distributed anomaly detection modules were evaluated based on two standard metrics, i.e., detection accuracy and detection time.

The work of Strohmeier *et al.* (Strohmeier et al., 2022), described a fully physical avionics security lab. Creating such a nearly full-fledged avionics testbed, they aim to provide a realistic environment for experimentation against several threat actors, including the ones described in Costin and Francillon (2012). By utilizing SDR technologies, they assessed their testbed against air traffic control and radar-oriented attacks, such as Automatic Dependent Surveillance-Broadcast (ADS-B) and Global Positioning System (GPS) spoofing. The testbed was built with real aircraft hardware to ensure its fidelity and offer realistic results. Some of the hardware components incorporated in their testbed were a Garmin GTX 3000 aircraft transponder and a Garmin GTS 8000 collision avoidance system. For a full list of the components used in the testbed, the reader is referred to Table 9.

Koroniotis et al. (2021) constructed a realistic smart airport testbed called *SAir-IIoT* comprising a diversity of IIoT sensors and communication protocols. *SAir-IIoT* is a hybrid testbed since it incorporates both physical off-the-shelf IIoT devices along with a plethora of simulated services, mostly hosted in Virtual Machines (VM). *SAir-IIoT* was tested against multiple attack scenarios as listed in Table 5. Although quite complex, *SAir-IIoT* is easily reproducible, extendable, and mutable, as it is based on open-source tools, and easily acquirable sensors, accompanied by sufficient documentation. Moreover, *SAir-IIoT* can be accessed remotely as-a-service, enabling researchers and practitioners to remotely execute attack or defense scenarios. No less important, the testbed is coupled with a data management mechanism for collecting, analyzing, and tagging heterogeneous data from diverse data sources, including IIoT devices and network flows. This facilitates researchers to further devise and evaluate attacks or countermeasures.

The focus of Petrillo et al. (2020) was on autonomous connected vehicles. In detail, they tackled the problem of secure tracking for a cohesive vehicle formation, commonly referred to as a platoon, which may be under a variety of cyberattacks. Precisely, they examined adversarial scenarios such as spoofing, message injection, and DoS to test the resilience of their proposed solution. Particularly, their approach leveraged an adaptive synchronization-based control algorithm that embeds a distributed mitigation mechanism for the detection of malicious data. The experiments took place on a simulated testbed on the Veins (Vei, 0000) open-source tool, using the extension PLEXE (Segata et al., 2014), that is, a cooperative driving system simulator. The communication among seven simulated autonomous connected vehicles was based on the IEEE 802.11p amendment, also known as Wireless Access for Vehicular Environments (WAVE). They concluded that the proposed algorithm can be effective against an array of cyberattacks. The authors compared their algorithm with similar works, using the mean-square position error in the vehicle formation within the platoon as a metric.

Kim et al. (2019) concentrated on train control systems. They investigated the current standard regarding train systems, namely Communication-Based Train Control (CBTC). To assess the standard's endurance against cyber threats, they utilized a realist CBTC testbed. The testbed comprises the core parts of a legacy CBTC system, providing a mixture of simulated and physical infrastructure. In detail, the testbed spans three layers, that is physical, network, and supervision, with the attack scenario involving the latter two. For example, the train dynamics were simulated on a desktop Personal Computer (PC). Also, the authors built an SDN with four bridges using Raspberry Pi 3; SDNs constitute the network layer between the physical and supervision ones. They considered a MitM attack, with the entry point being the wireless link between the Onboard Automatic Train Protection (OATP) and the SDN network. They showed that the attacker can modify the data related to a train's Movement Authority (MA) information, possibly provoking a collision with another train. As a countermeasure, they altered the SDN-based network, introducing a remote host who is not exposed to the attacker. By doing so, the remote host can issue an emergency stop command to OATP, even if the communication is exposed to a middleman. The performance of the authors' countermeasure was assessed by considering the time interval from the moment the first malicious packet arrives at OATP until the train emergency stop packet is transmitted.

Li et al. (2019b) proposed a cooperative secret key agreement called *CoopKey* for protecting control messages in inter-vehicle communications; the secret key is generated based on the quantized fading channel randomness. The suggested scheme is destined to Platoon-based Vehicular Cyber-Physical Systems (PVCPSs), where the platoon-based driving pattern assumes that the lead vehicle is manually driven, and the others follow in a fully automated manner. *CoopKey* was tested against an eavesdropping attack scenario through a platooning testbed with autonomous robotic vehicles that integrated TelosB wireless nodes for onboard data processing and multi-hop dissemination. The testbed was built with a platoon of four ARVs based on a low-cost robot Wi-FiBOT (Wi, 0000), and was equipped with an IEEE 802.15.4-compliant Radio Frequency (RF) transceiver. For evaluating their proposal, the authors measured the Bit MisMatch Rate (BMMR) of PVCPS with relevance to inter-ARV distances, RSS quantization intervals, and the number of iterations of the *CoopKey*.

Basiri et al. (2019) suggested a security solution based on a game-theoretic approach in a vehicle platooning setting. Their approach included an attacker-detector game, with the attacker targeting a number of vehicles and the detector deploying monitoring sensors on some of them. The attacker's goal is to stay hidden, avoiding the sensors placed by the detector. On the other hand, the detector attempts to place the monitoring sensors as aptly as possible to detect the attack in a prompt manner. To the detectors' aid, the Nash Equilibrium (NE) strategies were utilized, assisting them to choose appropriately the vehicles on top of which they put the monitoring sensors. Furthermore, the authors investigated the effect of altering communication weights among vehicles. To evaluate the suggested attacker-detector game, they experimented on a 3-vehicle platoon equipped with Xbee modules that utilize the ZigBee protocol. Two different adversarial scenarios, namely, acceleration-brake and brake-acceleration were tested showing the effectiveness of the proposed scheme.

The basic aspects per testbed per work included in this subsection are recapitulated in Table 5. As observed from the table, most of these contributions focus on 802.11 and ZigBee communication links. Moreover, with regard to Figure 2, four attack entry points were exploited. Five studies consider fitting controls for the examined attacks, while regarding the type of testbed, six out of eight are physical and hybrid, equally split.

4.4. Unmanned Aircraft Systems

Chinthi-Reddy et al. (2022) considered privacy-preserving strategies for drone communications. Particularly, their threat model assumed an adversary who controls a drone, and through it, he may passively eavesdrop on communications, actively inject false data, or modify the packet header information misleading the ground user and the drone. They proposed three target tracking mechanisms to obscure a legitimate drone from the malicious one, namely the shortest path, random locations, and dummy locations. In detail, these strategies attempt to obfuscate the position of a legitimate drone by randomizing its trajectory, so that the attacker's drone is unable to locate and track the legitimate one. Privacy aspects in terms of the drone's location and trajectory were also examined; this was done using entropy-based anonymity. To evaluate the proposed mechanisms, the authors conducted customized discrete-event-driven simulations using OMNeT++ (OMN, 0000). Precisely, they deployed a testbed comprising a rectangular network comprising three main components: a ground user, a drone, and a location target. They assumed that the user and the drone are within a radius of 150m, so that they can communicate directly and without the use of proxies. In this case, the communication is held over the IEEE 802.11 protocol. The proposed target tracking mechanisms were evaluated in terms of diverse metrics, including entropy-based anonymity, the size of the convex hull area, the number of paths, drone traces, detection delay, and the average number of packets exchanged with the server.

Secure data exchange in autonomous drones' was also investigated by Li et al. (2021). They focused on safeguarding Bluetooth Low Energy (BLE)-connected autonomous drones by providing a Received Signal Strength (RSS)-based key generation, namely *BloothAir*. They suggested a channel-based secret key generation, where the RSS is broadcasted from the drones to the ground devices and vice versa, and subsequently quantized to generate the secret keys. They also introduced some dynamic programming-based techniques for minimizing the secret Key Bit Mismatch Rate (KBMR). *BloothAir* was assessed through a multi-hop aerial relay testbed comprising an MX400 (mx4, 0000) drone platform, two autonomous drones, and two ground devices, all of them equipped with a BLE-capable Gust radio transceiver (Air, 0000). The *BloothAir* system's performance was compared against two RSS-based secret key generation schemes using three metrics, namely KBMR, data delivery latency, and energy consumption. The derived results showcased that *BloothAir* achieves a significantly lower KBMR maintaining equivalent key generation time and energy consumption with similar schemes based on Fixed Quantization Intervals (FQI) (Yasukawa et al., 2008) and Median RSS Quantization (MRQ) (Aono et al., 2005).

Abichandani et al. (2020) introduced an Ethereum blockchain-based software and hardware architecture that allows secure data exchange between multiple small Unmanned Aerial Vehicles (UAVs). They evaluated their architecture through a physical testbed comprising three DJI M100 quadrotors, each of them equipped with suitable hardware to communicate with each other. One of the quadrotors acted as the Ethereum miner, integrating an NVIDIA Graphics Processing Unit (GPU). All the quadrotors embedded Wi-Fi enabled antennas, a Raspberry Pi 4, and a 915-MHz mesh radio. The scheme under which the quadrotors exchanged data is a four-step procedure: applying asymmetric cryptography for encrypting the collected data, an InterPlanetary File System (IPFS) to store the cryptographic hashes of the data in a decentralized manner, and an Ethereum blockchain to share the hashes. They showcased that data transmission under their scheme provides data confidentiality, integrity, and non-repudiation, mainly because of the Ethereum smart contracts. To assess the performance of the proposed architecture, they relied on the average time taken to transfer an image across the network as a function of the image size, the consensus algorithm, and the Ethereum difficulty level, i.e., “how many hashes must be generated to find a valid solution to solve the next Ethereum block.”

Table 6
Testbeds identified in the Unmanned Aircraft Systems sector.

Tag	Year	Protocol	Attack	Entry point	Control	Evaluation metrics	Type
22	2022 Chinthi-Reddy et al. (2022)	IEEE 802.11	Eavesdropping, data manipulation	W-C	Attacker cyber deception	Entropy-based anonymity, size of convex hull area, number of paths, drone traces, detection delay, PDR	Simulated
23	2021 Li et al. (2021)	BLE	Eavesdropping, data manipulation	S-C, S-S, C-A	RSS-based key generation	KBMR, data delivery latency, energy consumption	Physical
24	2020 Abichandani et al. (2020)	IEEE 802.11	Service disruption	S-S, S-C	Ethereum blockchain	Transmission average time, energy consumption	Physical

Similar to the previous subsections, Table 6 outlines the key aspects of each testbed per examined work. At a glance, two out of the three testbeds concentrate on 802.11 links, while the remaining one focuses on BLE. Additionally, with reference to Figure 2, four attack entry points are utilized. Notably, all the works in the table propose and evaluate some security control. Last but not least, two testbeds are fully physical and only one is simulated.

4.5. IoT and WSN

The work by Sharma et al. (2022) suggested a security mechanism for detecting black hole attacks in IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN) that utilize the Routing Protocol for Low-Power and Lossy Networks (RPL) (Thubert and Richardson, 2021). A black hole attack supposes that a node inside the network absorbs all the receiving network packets instead of forwarding them further into the network. As a countermeasure, the authors proposed a time-based mechanism to perform malicious node detection. They evaluated this mechanism through the Cooja network simulator (Osterlind et al., 2006) showcasing that the detection of black holes can be estimated with high accuracy, resulting in a packet loss decrease. The simulated testbed included 16 network nodes, each of them representing a wireless sensor in a Wireless Sensors Network (WSN). For evaluating their proposal, they relied on three metrics, namely, accuracy, response receive rate, and detection time. Altogether, they concluded that black holes can be detected timely and with high accuracy to avoid a detrimental impact on the availability of the network.

Righetti et al. (2022) examined the security robustness of the 6P protocol (Wang et al., 2018), used for resource negotiation at the core of the IPv6 over the Time Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e (6TiSCH) (Thubert, 2021) architecture. They analyzed and implemented two attacks against the 6P, namely traffic dispersion and overloading attacks. The first aims at disrupting the communications between two neighboring nodes, one of them being the victim; this is done by dispersing messages on behalf of the victim node. The second attack attempts to increase energy consumption at the victim by allocating unneeded Central Processing Unit (CPU) processes. Both attacks were highly effective, altering the communication paths of victim nodes and circumventing the network's basic functionalities. The authors tested the attacks through both a simulated and a physical testbed. The simulated testbed was delivered through the Cooja network simulator of the Contiki-NG operating system. On the other hand, the physical testbed comprised 23 wireless nodes on the Zolertia RE-Mote board (zol, 0000) and a Raspberry Pi embedded system. Moreover, they investigated mitigation strategies to soothe the impact of the examined assaults. To this end, they proposed an extended version of the Minimal Scheduling Function (MSF), namely, the reference scheduling algorithm for 6TiSCH. For quantifying the attack impact and the efficiency of the proposed mitigation strategies, they considered three metrics, i.e., PDR, energy consumption, and CPU cell consumption.

Cheng et al. (2021) showcased a new type of smart selective jamming against WirelessHART networks. From an attacker's perspective, compared to the constant jamming and random jamming, this stealthy assault is energy efficient and hardly detectable, and can significantly reduce network reliability. Precisely, after the attacker disrupts the wireless channel usage and muddles the network routing tables, she finally jams in fixed time slots specific radio channels. To demonstrate their attack, they implemented a TelosB motes 50-node network spread across a floor of an office building. Each node ran on an open-source WirelessHART implementation.

Gao et al. (2021) examined spoofing and jamming attacks based on Cross-Technology Communication (CTC). For instance, Wi-Fi devices that communicate with analogous ZigBee devices without any hardware alterations or additional gateway equipment, constitute a CTC. In this regard, they introduced *SamBee*, a new spoofing and jamming attack strategy that takes advantage of the bandwidth discrepancy that Wi-Fi and ZigBee utilize; that is, Wi-Fi occupies a much wider bandwidth (20MHz) than ZigBee (2MHz). Particularly, *SamBee* is a parallel attack scheme, where a single Wi-Fi frame can be used either to spoof ZigBee devices operating in two different channels or to jam the same devices operating in five distinct channels. To assess this attack, they physically deployed a testbed comprising 40 ZigBee nodes and a Wi-Fi SDR. That is, a USRP-N210 with Wi-Fi functionality acted as the attacker, and 40 MiCAz-based nodes were employed to form a ZigBee WSN. The key remark of their analysis is that spoofing and multichannel jamming attacks based on CTC can be executed concurrently.

The work by Samaddar et al. (2020) investigated timing attacks against a WirelessHART network. They showed that due to the repetitive nature of the communication schedule decided by the centralized network manager, WirelessHART is vulnerable to timing attacks. As a countermeasure, they proposed *SlotSwapper*, a moving target defense mechanism that randomizes the communication slots over a hyper period schedule, without violating the feasibility constraints of real-time flows. Concisely, the proposed moving target defense algorithm randomizes the time slots to lessen the predictability of time slots, while still conserving all the genuine characteristics of real-time flows in the network. They evaluated the suggested mechanism through a simulated testbed using the Cooja simulator (Osterlind et al., 2006). The performance of their algorithm was measured by the upper-bound K-L divergence and prediction probability of the slots in the generated schedules, also considering power and memory consumption.

Babun et al. (2020) introduced a fingerprinting framework, called *Z-IoT*, for IoT devices that communicate with either the ZigBee or Z-wave protocols. They consider a scenario where an unauthorized insider can remain incognito by impersonating a legitimate device, while performing malevolent activities. To defend against such an attack, *Z-IoT* allows the network administrator to detect such rogue devices by comparing their type with a legitimate device type. This is achieved by means of network-based fingerprinting mechanisms. Nevertheless, *Z-IoT* considers neither devices that are clones of authorized devices nor compromised authorized devices. To evaluate the framework, they created two testbeds utilizing 39 Z-IoT devices, which were used in industrial settings, such as water and motion sensors. The performance of Z-IoT was evaluated against multiple ML classifiers in terms of TPR, FPR, Precision, Recall, Receiver Operator Characteristic (ROC) curve, and Precision-Recall Curve (PRC).

In their work, Yasaei et al. (2020) proposed an adaptive anomaly intrusion detection model to safeguard the integrity of IoT sensors' data. Their model utilized a context-aware sensor association algorithm, i.e., a method to classify the involved sensors that encounter similar contextual variation. Briefly, the authors designed their model to recognize and locate anomalies without reliance on prior knowledge, taking also cognizance of the fluctuations in an IoT system. They assessed their method through a testbed consisting of an ad-hoc network of 62 IoT sensors, an SDR, a gateway, and a laptop PC. The communication between the SDR and the sensors network was based on the IEEE 802.15.4 standard. In this way, the SDR was used for collecting the WSNs' data and sending commands back to it. A Raspberry Pi board operated as the base station, bridging the IoT network and the SDR with a respective monitor unit through a Wi-Fi router. The anomaly intrusion detection model was implemented on the monitor unit, which receives the data from the base station and performs the computations as a fog node in the IoT system. To estimate the detection accuracy of their model, the authors used standard metrics, including precision, recall, F0.5, and F1.

The work by Airehrour et al. (2019) introduced *SecTrust-RPL*, a time-based trust-aware RPL routing protocol. *SecTrust-RPL* was tested against two routing attacks, namely, rank and sybil attacks. A rank attack occurs when a malicious node advertises a routing path by changing its rank, thereby attracting neighbor nodes to route their traffic through it. On the other hand, a sybil attack places the malicious node masquerading as several entities, overwhelming the network and distorting its topology. To repel such attacks, *SecTrust-RPL* uses a trust-based mechanism to discern and isolate malicious nodes, while optimizing network performance at the same time. *SecTrust-RPL* was assessed through a simulated testbed. The simulation exploited the Contiki/Cooja (Con, 0000; Osterlind et al., 2006) environment, enabling 30 nodes, with three of them being malicious. To validate the simulation results, they also implemented a physical smart home testbed comprising 14 AS-XM1000 motes, with two of them being malicious. *SecTrust-RPL* was evaluated vis-à-vis the standard RPL routing protocol by estimating the attack detection time and PDR. Overall, the authors argued that trust-based mechanisms like *SecTrust-RPL* can be an effective weapon against routing attacks in IoT networks.

Li et al. (2018) suggested a secret key generation protocol for securing real-time data distribution in a CPS setting. To prove their point, they tested their protocol through a 2-hop WSN testbed. Specifically, the secret key generation for data encryption is based on the randomness that characterizes a wireless fading channel. To this end, two sensor nodes of the testbed extracted secret bits from the inherently random spatial and temporal variations of the wireless channel between them. In this respect, their scheme can tackle eavesdropping and message modification attacks, which are omnipresent in a WSN. No less important, the proposed protocol can be applied to more sensitive environments, as the key is generated in a distributed way, thus avoiding single points of failure.

Tomić et al. (2018b) introduced a lightweight, distributed solution to detect and recover from network-level attacks in a WSN ecosystem, named *Antilizer*. The proposed security control refers to networks that utilize the RPL routing protocol (Thubert and Richardson, 2021) in 6LoWPAN. Particularly, the basis of *Antilizer* is a self-referenced trust model that facilitates all the sensor nodes to map their neighborhood using network overhearing. Therefore, if a compromised sensor is detected, neighbor collaboration routing decisions are determined to avoid any affected region in the network. Furthermore, an agent-based notification scheme in terms of “antilizer notification tickets” is used to inform the base station about the malicious nodes in the vicinity. *Antilizer* was tested against three well-known attacks, namely, sinkhole, black hole, and hello flood attacks, through the Contiki simulator Cooja (Osterlind et al., 2006). The authors exploited different metrics to measure the efficiency of *Antilizer*, including End-to-End (E2E) data loss, average E2E Delay, communication overhead, and TPR/FPR.

Ge et al. (2018) developed two SDN-oriented proactive defense mechanisms that reconfigure the IoT network topology. Their approach was to alter the attack surface of the IoT network to augment the attacker's effort and the exploitation level of non-patchable vulnerabilities. According to their scenario, the attacker can acquire access using one node as the entry point; through pivoting, they can inject and run arbitrary codes to move laterally to other nodes, eventually reaching the base station. Precisely, the authors' scheme was evaluated through simulations. Their testbed included an SDN consisting of 100 sensor nodes and 1 base station, with the results showing that the proactive defense mechanisms effectively increase the attacker's effort, while maintaining the average shortest path length. For evaluating their proposal, except for considering the overall risk and attack impact, they relied on several individual metrics, including the attack success probability, attack cost, mean-time-to-compromise, and mean-attack-path-length before and after applying their scheme.

Fröhlich et al. (2018) aimed at enhancing the fault-tolerance of a WSN present in a CPS environment. They suggested a replicated gateway architecture to face Byzantine-based attacks such as Distributed Denial-of-Service (DDoS) and refusal-to-forward attacks. Byzantine attacks can be performed by an already authenticated trusted node that at some point is turned rogue. Their solution spans sensor and gateway levels. At the sensors level, they introduced the Fault-Tolerant Trustful Space-Time Protocol (FT-TSTP), a routing protocol capable of delivering data to multiple gateways and tolerant to network holes caused by exposed or defective nodes. At the gateway level, they devised *ByzCast*, a multi-gateway synchronization protocol, which can deliver data across CPS applications, despite some gateways having been compromised. The efficiency of the proposed solution against DDoS and refusal-to-forward attacks was tested in OMNet++ OMN (0000) simulator and the Castalia (Cas, 0000) framework. *ByzCast* detection performance was assessed through a number of metrics, i.e., PDR, E2E transmission time, and energy consumption. Based on the simulation results, the authors concluded that their scheme increases the robustness of the system in terms of data availability, CPS energy, timeliness, and security demands.

An interesting hands-on work on IoT security was given by in Kolias et al. (2016b). They highlighted the ongoing penetration of IoT in CPS and the industry in general and presented three different IoT testbeds. Specifically, they leveraged different attack entry points in the testbeds, namely, Wi-Fi, ZigBee, and BLE links. Based on their assessment, it was made clear that these kinds of

Table 7
Testbeds identified in the IoT & WSN sectors.

Tag	Year	Protocol	Attack	Entry point	Control	Evaluation metrics	Type
25	2022 Sharma et al. (2022)	6LoWPAN	Black hole	S-S	Timer-based mechanism	Accuracy, response receive rate, detection time	Simulated
26	2022 Righetti et al. (2022)	6LoWPAN	Traffic dispersion and overloading	S-S	Minimal scheduling function	PDR, energy consumption, CPU cell consumption	Hybrid
27	2021 Cheng et al. (2021)	WirelessHART	Jamming	S-S	N/A	N/A	Physical
28	2021 Gao et al. (2021)	ZigBee, IEEE 802.11	Jamming	S-S	N/A	N/A	Physical
29	2020 Samaddar et al. (2020)	WirelessHART	Eavesdropping, timing, jamming	S-C, C-A	Moving target defence	Upper-bound K-L divergence, prediction probability, energy & memory consumption	Simulated
30	2020 Babun et al. (2020)	Z-wave (based on ITU-T G.9959) and ZigBee	ARP spoofing, data manipulation	S-S, S-C	Network-based fingerprinting mechanisms	TPR, FPR, Precision, Recall, ROC, PRC	Physical
31	2020 Yasaei et al. (2020)	IEEE 802.11, ZigBee	Data manipulation	E-S	Context-aware adaptive anomaly detection	Precision, recall, F0.5, F1	Physical
32	2019 Airehrour et al. (2019)	6LoWPAN	Rank, sybil	S-S	Time-based trust-aware RPL routing protocol	Detection time and PDR	Hybrid
33	2018 Li et al. (2018)	ZigBee	Eavesdropping	S-S, S-C	Secret key generation protocol	N/A	Physical
34	2018 Tomić et al. (2018b)	6LoWPAN	Sink hole, black hole, and ICMP flood	S-S	Self-referenced trust model	E2E data loss, average E2E Delay, communication overhead, TPR, and FPR	Simulated
35	2018 Ge et al. (2018)	ZigBee	Buffer overflow	S-S, S-C	IoT network topology reconfiguration	Mean time to compromise, mean attack path length, average shortest path length	Simulated
36	2018 Fröhlich et al. (2018)	ZigBee	Byzantine (DDoS, refusal-to-forward variations)	S-S	Replicated gateway architecture	PDR, E2E transmission time, energy consumption	Simulated
37	2016 Kolias et al. (2016b)	IEEE 802.11, ZigBee, and BLE	Jamming, eavesdropping, service disruption, ARP spoofing, buffer overflow, XSS, SQL injection	E-S, S-C, C-A, A-E	N/A	N/A	Physical

networked devices often lack security countermeasures for common attacks, like jamming, eavesdropping, message injection, DoS, and ARP spoofing, which in turn can lead to leakage of Personally Identifiable Information (PII), leakage of sensitive user information, and unauthorized execution of functions. An additional conclusion is that the limited computational power of IoT devices makes it difficult to provide strong security. The testbeds employed in the context of that work were fully physical, comprising a set of sensors, wireless APs, and smart IoT devices, all of them listed in Table 9.

Table 7 summarizes the basic aspects of each testbed included in this subsection. A first remark is that there exists a variety of wireless protocols, with the majority of them being two different 802.15.4 implementations, i.e., ZigBee and 6LoWPAN. All the attacks were exercised on five different entry points with reference to Figure 2. From a defensive viewpoint, 10 out of 13 of the testbeds propose and evaluate respective countermeasures. Lastly, five testbeds were simulated, while six of them were fully physical.

4.6. Others

4.6.1. Energy

Stan et al. (2020) extended the MulVAL Ou et al. (2005) network security model. More precisely, their extension spans three axes, namely, network modeling, classification of multiple network attack scenarios, and implementation of a dedicated agent that automatically collects network configurations. As recapitulated in Table 8, they investigated multiple adversarial scenarios relevant to the IEEE 802.11 and Bluetooth protocols. To demonstrate the applicability of the proposed model extensions, they deployed a dedicated testbed, representing a simplified industrial ecosystem of a thermal power plant. That testbed was fully physical, including five generators, a boiler, a control panel, three PLCs, and an HMI. The wireless attack vectors examined against this testbed were a WPA3 downgrade attack and the blueborne set of attacks (Seri and Livne, 2019). The first vector refers to the Dragonblood attack (Vanhoef and Ronen, 2020), while the second is a set of eight separate vulnerabilities that affect all unpatched devices with Bluetooth capabilities.

The work of Kauer et al. (2018) suggested a dual-radio architecture supporting the coexistence of both non-real- and real-time tasks. They proposed an architecture that comprises two independent radio technologies, namely, an IEEE 802.15.4 mesh network for bidirectional communications and a unidirectional radio system that enables network nodes' reachability within a single network hop. To evaluate their scheme from a security resilience viewpoint, they exploited a number of attacks, including brute force and re-

Table 8
Testbeds identified in the other sectors.

Tag	Year	Sector	Protocol	Attack	Entry point	Control	Evaluation metrics	Type
38	2023 Costin et al. (2023)	Satellite, Avionics, Maritime, UAS	IEEE 802.11, ADS-B, GPS	Service disruption, replay, fuzzing, jamming, eavesdropping, data manipulation	E-S, A-E, S-S, S-C, C-A, W-C	N/A	N/A	Physical
39	2023 Færøy et al. (2023)	Maritime	IEEE 802.11	Service disruption, evil-twin	S-C	N/A	N/A	Physical
40	2022 Kim et al. (2022a)	N/A	IEEE 802.11	ICMP flood	S-C, C-A	Real-time controller reconfiguration	MA of RTT, IAE	Hybrid
41	2022 Agarwal et al. (2022)	Agriculture	IEEE 802.11, Bluetooth	Data manipulation, eavesdropping, service disruption, FTP bounce, masquerading	S-C, C-A, W-C	N/A	N/A	Physical
42	2022 Jacovic et al. (2022)	Transportation, UAS, IoT	IEEE 802.11, ZigBee	Jamming	E-S, S-S, S-C	N/A	N/A	Hybrid
43	2020 Stan et al. (2020)	Energy	IEEE 802.11, Bluetooth	ARP spoofing, Dragonblood, heartbleed, blueborne, SYN flood	S-C, C-A, W-C	N/A	N/A	Physical
44	2018 Kauer et al. (2018)	Energy	ZigBee	Jamming, eavesdropping, brute force, replay, service disruption	E-S	Message integrity code	PRR, FPR, energy consumption	Physical
45	2017 Aras et al. (2017)	N/A	LoRaWAN	Jamming, replay	S-S, S-C	N/A	N/A	Physical
46	2016 Si et al. (2016)	N/A	ZigBee	Service disruption, jamming	E-S, S-C	Hybrid wired/wireless scheduling protocol	PDR, throughput, average delay time	Physical

play. In this respect, they proposed the use of Message Integrity Codes (MIC) which include a timestamp. Their observations were derived through experimentation with a real-life solar tower power plant equipped with a dual-radio transceiver. The performance of the suggested scheme was assessed by means of the Packet Reception Ratio (PRR), FPR, and energy consumption.

4.6.2. Agriculture

Agarwal et al. (2022) argued that the agricultural sector keeps evolving at a fast pace introducing contemporary technologies, both wired and wireless. This, however, augments the attack surface, making the need for security increasingly pressing. In addition, the authors observed that there is a lack of realistic testbeds which can be utilized for evaluating the security level of modern digital agricultural devices. In this context, they presented a smart dairy farming security testbed. The latter is a rudimentary environment to scrutinize the security resilience of smart farming without experimenting on live farms. As detailed in Table 9, the developed testbed comprised several devices that are typically used in the agricultural ecosystem. Based on the testbed, the authors tested several well-known assaults, namely, eavesdropping, data manipulation, and DoS (CVE-2018-7449).

4.6.3. Maritime

By utilizing the Execution Plan (EP) model proposed in Yamin and Katt (2022), Færøy *et al.* Færøy et al. (2023) executed in an automated way two legacy assaults, namely deauthentication and evil-twin, against the 802.11 wireless protocol. Their testbed comprised an Automatic Identification System (AIS) (AIS, 0000) as the target IoT device, a personal laptop mimicking the attacker, and the Aircrack-ng (air, 0000) software suite. Note that AIS is an automatic tracking system that uses transceivers on ships and is exploited by vessel traffic services. The well-known hostapd (hos, 0000), a user space daemon for the access point, was used to implement the rogue AP in the context of the evil-twin attack. After mounting the attacks manually, the authors developed an automated assault agent. That is, they fabricated the attack's EP, which was verified through the Temporal Logic of Actions (TLA)+ language, and implemented in Python. They concluded that their EP model can be used to automate penetration testing, and that such a scheme in conjunction with other security tools and processes could promptly identify and exploit new vulnerabilities in maritime systems.

4.6.4. Cross-sector CPS

Costin et al. (2023) contributed a Unified Cybersecurity Testing Lab for Satellite, Aerospace, Avionics, Maritime, Drone (SAAMD) technologies and communications. SAAMD constitutes an extensible security platform capable of creating payloads according to each protocol's specifications, e.g., ADS-B for avionics and AIS for maritime. To simulate a real-life scenario, the authors used off-the-self hardware equipment, combined with an extensible RF software suite for the required network functionalities. Through SAAMD, they experimentally evaluated a plethora of attack scenarios per sector of interest, including spoofing, DoS, and jamming against satellite, avionics, and maritime ecosystems. During their experiments, they demonstrated that satellite systems are susceptible to replay, spoofing, and fuzzing attacks, avionics to DoS and fuzzing assaults, and maritime systems to DoS attacks.

In Kim et al. (2022a) Sangjun *et al.* focused on Internet Control Message Protocol (ICMP) flooding, a delay type of attack, in the context of CPS. To this end, they simplified the structure of the examined CPS to a Network Control System (NCS) (Gautam et al., 2021). Specifically, the basic parts of an NCS are a physical system, a network, and a computing/control system. In their study, the physical system was an emulated Direct Current (DC) motor, while the exchange of data between the physical process and the control system was done over two IEEE 802.11 APs; the motor was periodically sending state messages to the controller over an 802.11 link. The attack was exercised at the network layer by injecting large-size ICMP packets with high frequency. Moreover, the authors came up with two possible countermeasures. The first is based on the computing system reconfiguration; the controller guarantees the stability of the physical system by increasing its gain with a larger delay bound vis-à-vis that of the attack. The second reconfigures the topology of the network, re-routing the data through the second AP. Overall, both these schemes rely on the controller's real-time reconfiguration to ensure the stability of the physical system in terms of data availability. To evaluate the efficiency of the proposed countermeasures under an ICMP flood attack, they considered the Round Trip Time (RTT) for every sensing period by means of a Moving Average (MA) formula. They also utilized an Integrated Absolute Error (IAE) as a metric to evaluate the recovery performance.

Jacovic et al. (2022) scrutinized the cyber resilience of a number of CPS against an active threat, namely, radio frequency jamming. Such an active attack can disrupt communication and harm the normal operation of a CPS. Their testbed included a variety of CPS devices and concentrated on wireless links, i.e., the Wi-Fi and ZigBee protocols, therefore offering an emulation environment for assessing radio frequency jamming attacks in complex scenarios, including vehicular, UAV, and IoT. Particularly, among others, the testbed comprised SDRs and open-source tools for testing wireless communications. Several radio jamming scenarios pertinent to the aforementioned three settings were developed and evaluated.

Aras et al. (2017) demonstrated that Long Range Wide Area Networks (LoRaWAN) are susceptible to jamming attacks because of inherent deficiencies of LoRa transmissions. Precisely, the long airtime of such messages allows the attacker to intercept the transmission and emit jamming messages while the original traffic is still on-air. Apart from the legacy jamming attack, i.e., broadcast with higher signal strength, the authors introduced a selective jamming variation and a rather sophisticated jamming-wormhole attack. The second requires the attacker to deploy two different malicious nodes: the first sniffs the network and notifies the second through low-latency links in case a certain type of message is detected, while the second immediately jams upon receiving. No less important, the first node caches the sniffed messages for further exploitation by replay attacks. The authors evaluated the proposed attacks through a real LoRa testbed with radio modules capable of sending and receiving LoRa packets.

Despite that a Controller Area Network (CAN) is a vehicle bus standard innately used in wired environments, Si *et al.* Si et al. (2016) designated that it can be associated with wireless technologies too. Precisely, the authors offered a hybrid wired/wireless protocol that schedules packet transmissions on the wired and wireless links to mitigate priority-based DoS attacks, feasible due to the CANs scheduling mechanisms. The proposed countermeasure is fairly simple; when the link quality on the CAN bus drops significantly, it schedules packet transmissions via the wireless link. To evaluate the effectiveness of their proposal, the authors implemented a physical testbed comprising CAN and ZigBee transceivers. As expected, apart from DoS attack mitigation, the authors' scheme also aids in relieving congestion from the CAN bus under normal operation. On top of everything else, the authors examined the resilience of their scheme against radio jamming attacks. To this end, they considered PDR, throughput, and average delay time in correlation with the packet generation and attacking rates as suitable metrics.

The key aspects per testbed per work included in this subsection are recapitulated in Table 8. As observed, six testbeds focus on 802.11 links, three of them on ZigBee, and two on Bluetooth. Furthermore, with regard to Figure 2, six attack entry points are exploited, while only three works proposed and assessed matching security controls. As for the type of each testbed, seven out of nine are physical and two are hybrid.

Table 9 recapitulates the software and hardware tools used in each testbed identified in Section 4. As observed, there is a great diversity in the utilized tools, not only within the same sector of application but across different ones.

Table 9
Tools & equipment utilized per identified testbed categorized by sector of application.

Sector	Tool	Brief description
Water and Wastewater Systems	Physical machinery	See SWa (2023)
	Aircrack-Ng	Suite of tools to assess Wi-Fi network security
	MOXA AWK-5222-EU	Wireless industrial access point
	USRP 2952 series SDR (2023)	SDN board
	Waterbox Kartakis et al. (2015)	Testbed for monitoring and controlling smart water networks
	Tshark TSH (2023)	Network protocol analyzer
	RTl8821ae RTL (2023)	Single-chip controller
	USRP B210 SDR (2023)	SDN board
	GNU radio GNU (2023)	Open-source software development toolkit
Energy	SL9000A RFI (2023)	Sensor tag and data logger
	Nuvlabox (SixsQ) RFI (2023)	Cloud-in-a-box appliance
	Ubertooth UBE (2023)	Open-source wireless development platform
	ATmega256RFR2 ATm (2023)	Microchip
	CC110L CC1 (2023)	Wireless transceiver
Healthcare	FIT IoT-LAB	See Fambon et al. (2014)
	FreeRTOS Fre (2023)	Real-time operating system for microcontrollers
	HealthyPi v4 shield Hea (2022)	Device that can measure human vital signs
	Raspberry Pi	Small single-board computer
	D-Link DIR-822	Wireless access point
	AVISPA AVI (2022)	Automated validation of internet security protocols and applications
	MIRACL MIR (2022)	Multi precision integer and rational arithmetic cryptographic library
	Latte Panda Lat (2023)	Small single-board computer
	LiClipse LiC (2023)	IDE
	NodeMCU ESP32 ESP (2023)	System on a chip microcontroller

(*continued on next page*)

Table 9 (*continued*)

Sector	Tool	Brief description
	NodeMCU V3 Nod (2023)	Breadboard-friendly open-source ESP8266 development kit
	ESP8266 NodeMCU ESP (2023) V1.0 ESP-12E Wi-Fi	Open-source Lua based development board
	TP-Link TL-WDR4300	Wireless access point
	Syringe pump Wijnen et al. (2014)	Open-source syringe pump library
	MCU Arm Cortex-M4 Cor (2023)	Microcontroller
Transportation	Raspberry Pi	Small single-board computer
	Ettercap	Software suite for mounting MitM attacks
	ONOS ONO (2023)	Open network operating system
	Open vSwitch Ope (2023)	Multi-layer virtual switch
	Nmap	Network discovery and security auditing
	Metasploit	Penetration testing framework
	Scapy	Packet manipulation program
	sFuzz sFu (2023)	Black box testing suite
	Node-Red Nod (2023)	Programming tool
	ZigBee2MQTT Zig (2023)	Gateway application
	Aviation machinery	See Strohmeier et al. (2022)
	USRP SDR (2023) (B210 and X300)	SDN board
	FLARM FLA (2023)	Traffic awareness and collision avoidance technology
	LabSat Lab (2023)	Multi-global navigation satellite systems (GNSS) simulators
	EVK-M8 GNSS EVK (2023)	GNSS evaluation kit
	TelosB Tel (2023)	Open-source platform
	Chipcon CC2420 CC2 (2023)	RF Transceiver
	MSP430 MSP (2023)	Microcontroller
	Wi-FiBOT Wi (2023)	Low cost robot
Unmanned Aircraft Systems	ROS ROS (2023)	Robot operating system
	XBee module XBe (2023)	Wireless connectivity modules
	DYNACAR DYN (2023)	Real-time simulation environment
	Renault Twizy 80 Twi (2023)	Electric quadricycle
	Veins Vei (2023)	Open-source vehicular network simulation framework
	PLEXE Segata et al. (2014)	Open-source extension
	MGEN MGE (2023)	Network test tool
	OMNeT+ OMN (2022)	Simulation library and framework
	SUMO SUM (2023)	Open source traffic simulation package
	DJI Matrice M100 DJI (2023)	Drone
	Raspberry Pi	Small single-board computer
	NVIDIA Jetson TX2 Jet (2023)	Embedded computing device
	OrbittyBox Orb (2023)	Carrier board
	Verizon 4G LTE Wi-Fi	Wireless access point
	TP-Link AC1750	Wireless access point
	EA9500 Max-Stream	Wireless access point
	Solidity Sol (2023)	Object-oriented for smart contracts
	OMNeT+ OMN (2022)	Simulation library and framework
	MX400 Mx4 (2022)	Drone
	AirMind Gust radio transceiver Air (2023)	-
	RALA Patron and Dandekar (2014)	Reconfigurable alford loop antenna
	GNU radio GNU (2023)	Open-source software development toolkit
	MGEN MGE (2023)	Network testing tool
Agriculture	TCPDump	Command-line packet analyzer
	Wireshark	Network protocol analyzer
	FDX-B FDX (2023)	RFID reader/writer
	Ruuvi Ruu (2023)	Wireless temperature, humidity, air pressure, and motion sensor
Maritime	Linksys AE1200	Wireless-N USB Adapter
	Aircrack-ng Air (2023)	WiFi network security software suite
	Hostapd Hos (2023)	host access point daemon
	A200 AIS Class A A20 (2023)	AIS
	OpenCPN Ope (2023)	Chart plotter navigation software
	Pyrcrack Pyr (2023)	Python API
	Cooja Osterlind et al. (2006)	Network simulator
	Indriya2 Appavoo et al. (2019)	Wireless sensor network testbed
	TelosB Tel (2023)	Open-source platform
	USRP X310 and N210 SDR (2023)	SDN board
	DYSE Dys (2023)	Dynamic spectrum environment emulator
	Dragon Radio Dra (2023)	Software-defined radio built

(*continued on next page*)

Table 9 (*continued*)

Sector	Tool	Brief description
Cross-sector	Linksys WRT54GL	Wireless access point
	Hardware & software tools for avionics, satellite, and maritime systems	See Costin et al. (2023)
	Semtech Sx1276 Sem (2023)	Long Range Low Power Transceiver
	Hope RFM95/9 RFM (2023)	Long Range Low Power Transceiver
	Raspberry Pi	Small single-board computer
IoT and WSN	Beagle Bone Bea (2023)	Small single-board computer
	Various Z-IoT devices	See Babun et al. (2020)
	Samsung SmartThing hub	IoT Gateway
	AVR RS UZB AVR (2023)	USB network sniffer
	Killerbee Kil (2023)	Framework, tools for testing & auditing ZigBee
	Wireshark	Network protocol analyzer
	USB Z-Wave 500 Zniffer USB (2023)	Z-Wave network sniffer
	Weka Wek (2023)	Neural network implementation
	Sensors and smart devices	See Kolias et al. (2016b)
	Arduino Uno Ard (2023)	Open hardware development board
	Arduino Wi-Fi shield Wi- (2023)	Enables Arduino to wirelessly connect to the Internet
	Contiki-NG Con (2023)	Open-source, cross-platform operating system
	Cooja Osterlind et al. (2006)	Network simulator
	TelosB Tel (2023)	Open-source platform
	JamLab Boano et al. (2011)	Add-on to sensornet testbed
	Sensors and smart devices	See Yasaei et al. (2020)
	TinyOS Tin (2023)	Open-source operating system
	USRP-B210 SDR (2023)	SDN board
	ZOOM-H6 ZOO (2023)	Handheld recorder
	Qotom Mini PC Q500G6 Qot (2023)	Wireless access point
	Raspberry Pi	Small single-board computer
	USRP-N210 SDR (2023)	SDN board
	MICAz MIC (2023)	Mote module
	TinyOS 2.1.2 Tin (2023)	Open-source operating system
	Zolertia RE-Mote Zol (2023)	Hardware development platform
	AS-XM1000 mote AS: (2023)	Mote module
	Akaroa2 McNickle et al. (2010)	Simulation controller
	CC2530 CC2 (2023)	Wireless microcontroller
	CC2500 CC2 (2023)	RF Transceiver
	SDN-WISE SDN (2023)	SDN manager
	OMNeT+ OMN (2022)	Simulation library and framework
	Castalia Cas (2023)	Simulator for WSN and Body Area Networks
	EPOS EPO (2023)	Embedded parallel operating system
	WARP WAR (2023)	Programmable wireless platform

5. Analysis and discussion

With reference to Section 4 and Figure 3, it becomes apparent that the literature works regarding security testbeds focusing on wireless technologies follow an increasing trend from 2020 onward. Naturally, this reflects the gradual transformation of previously more or less siloed CPS into a mixture of both OT and IT infrastructure with direct or indirect access to the Internet. Amongst others, this drift progressively brings wireless technologies into the cyber-physical terrain. According to the discussion of Section 4, such technologies are typically used to realize personal or local area wireless networks like Zigbee, Bluetooth, LoWPAN, or Wi-Fi, respectively.

An explanation for this ascendant trajectory is that due to their straightforward benefits, including flexibility and cost savings, wireless technologies have rapidly penetrated the market, therefore inevitably the CPS ecosystem. Nevertheless, as already pointed out, the tight integration of wired and wireless realms significantly augments the attack surface of the underlying system. This is because, typically, wireless network domains do not afford any kind of access control to the medium, so the adversary can be anywhere in the area depending on the type of their equipment. In addition, several wireless technologies or protocols are still fresh, therefore prone to 0-days. In this respect, any wireless domain used in the context of a CPS is made susceptible to legacy attacks specific to this wireless protocol. Especially for CIs, this integration should be done with extra caution, say, a wireless domain should be a priori considered as a non-trusted zone, at least until it is properly secured and integrated into the rest of the system. To this end, security testbeds are especially handy for identifying vulnerabilities, assessing attacks, and testing countermeasures, without jeopardizing the operation of the real system.

In an effort to provide a more complete and systematic view of the literature review conducted in Section 4, the following three subsections approach the identified testbeds from three different prisms, namely wireless protocols, attacks, and countermeasures. A classification of attacks and countermeasures is also offered in the respective subsections.

5.1. Wireless protocols

As observed from the second column of Tables 3 to 7 and the third column of Table 8, a great variety of wireless communication protocols have been used either for machine-to-machine or human-to-machine communication in the context of the testbeds included in Section 4. Table 10 summarizes the basic characteristics per identified protocol, while Figure 4 depicts the percentage of each protocol within the total set. Specifically, with reference to Figure 4, the most utilized protocols with a share of approximately 39% and 32% implement the technologies developed in the IEEE 802.11 and 802.15.4 (ZigBee, 6LoWPAN, WirelessHART) families of standards, respectively. For instance, 802.11 is no more confined to houses, small office/home (SOHO), and business premises,

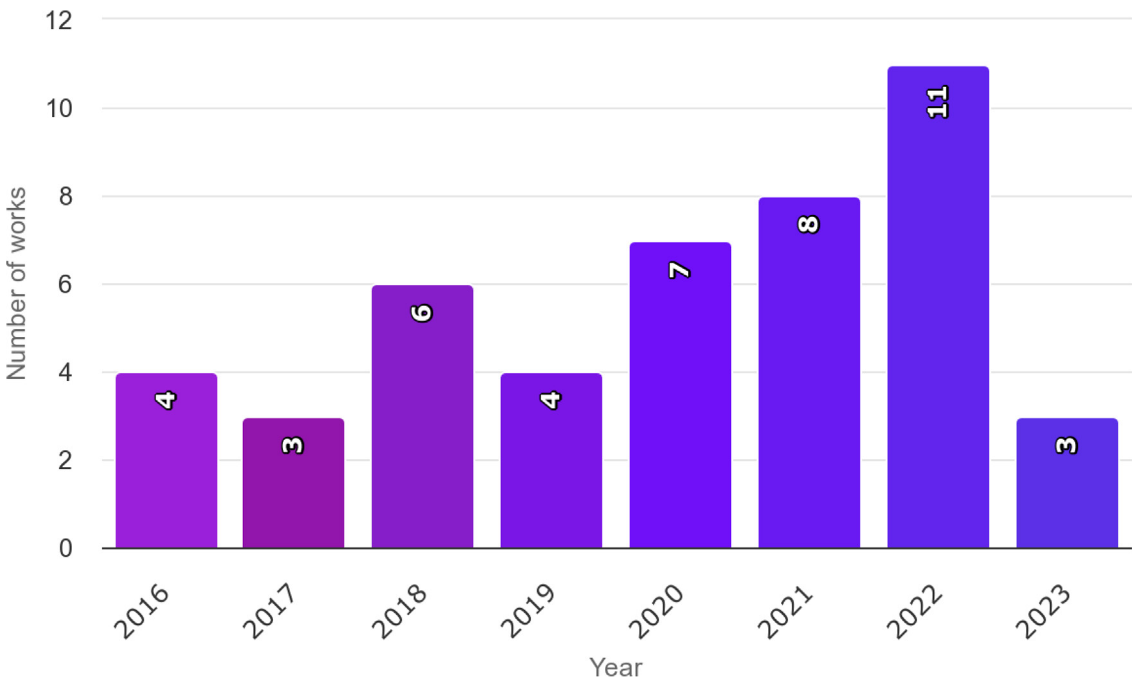

Fig. 3. Number of wireless-focused testbeds in the literature in the period from 2016 to 2023.

Table 10
Key features of wireless protocols.

Name	Frequency band	Data rate	Range	Topology	Physical modulation	Medium access method
Wi-Fi	2.4/5/6 GHz	1/2/5.5/11/6/9/18/24/36/48/54/ $\geq$ 288 & $\leq$ 9608 Mbits/s	30-120m	Star	BPSK/QAM	CSMA/CA & (MU-)MIMO OFDM(A)
ZigBee	2.4 GHz & 915/868 MHz	20/40/250 Kbits/s	10-75m	Star/tree/mesh	BPSK/OQPSK (DSSS)	CSMA/CA & TDMA
WirelessHART	2.4 GHz	250 Kbits/s	30-90m	Mesh	OQPSK (DSSS)	TSMP/TDMA
6LoWPAN	2.4 GHz	250 Kbits/s	10-75m	Mesh	OQPSK (DSSS)	CSMA/CA
Z-wave	868/908 MHz	9.6-40 Kbits/s	30-100m	Mesh	FSK	TDMA
IEEE 802.15.6	2.4GHz & 800/900/400 MHz	2 Mbits/s	0.1-1m	Star	DBPSK/DQPSK/GMSK	ALOHA & CSMA/CD
Bluetooth	2.4 GHz	1-3 Mbit/s	1-100m	P2P/scatternet	FSK (FHSS)	TDD-TDMA
BLE	2.4 GHz	125/500 Kbit/s & 1/2 Mbit/s	1-100m/1000m (BLE 5.0)	P2P/mesh	FSK (FHSS)	FDMA/TDMA
NFC	13.56 MHz	424 Kbit/s	0.1-1m	P2P	ASK	N/A
LoRaWAN	868-915 MHz	50 Kbits/s	11km	Star	CSS	LoRa
GPS	1575.42/1227.6/1176 MHz	50bits/s	10m	N/A	BPSK (DSSS)	CDMA
ADS-B	978/1030/1090 MHz	1 Mbit/s	463 km	N/A	PPM	N/A

but thanks to its several amendments, it can be utilized in different CI sectors, as discussed in Section 4. Taking smart cities as an example, Wi-Fi is a key enabler; every "thing" such as cameras, lights, smart meters, and vehicles may be connected to the Internet through 802.11 links. More specifically, the IEEE 802.11s amendment extends the IEEE 802.11 Medium Access Controls (MAC) layer with multi-hop capabilities, enabling more complex networks. On the other hand, the 802.11ah amendment, known as "Wi-Fi HaLow", typically uses the 900MHz band (sub-1GHz unlicensed bands), thus offering extended-range Wi-Fi networks vis-á-vis WLANs operating in the 2.4, 5, or 6GHz bands. Moreover, the IEEE 802.11p is specifically designed for vehicular ad-hoc networks.

In view of the discussion of Section 4, another wireless standard that is used in CPS and CI environments is IEEE 802.15.4. This standard is the basis for several well-known protocols, including Zigbee, WirelessHART, 6LoWPAN, ISA100.11a, Thread, and others. Precisely, IEEE 802.15.4 specifies the PHY and MAC layers for short-range, LR-WPAN, thus targeting low-cost, low-speed, ubiquitous communication between devices. For more in-depth analysis on short- or mid-range wireless protocols in terms of security, the reader is referred to Burg et al. (2017); Kambourakis et al. (2020); Montori et al. (2018); Zou et al. (2016). A final yet important remark is that no testbed was oriented towards the latest two generations of cellular networks, namely 4G and 5G.

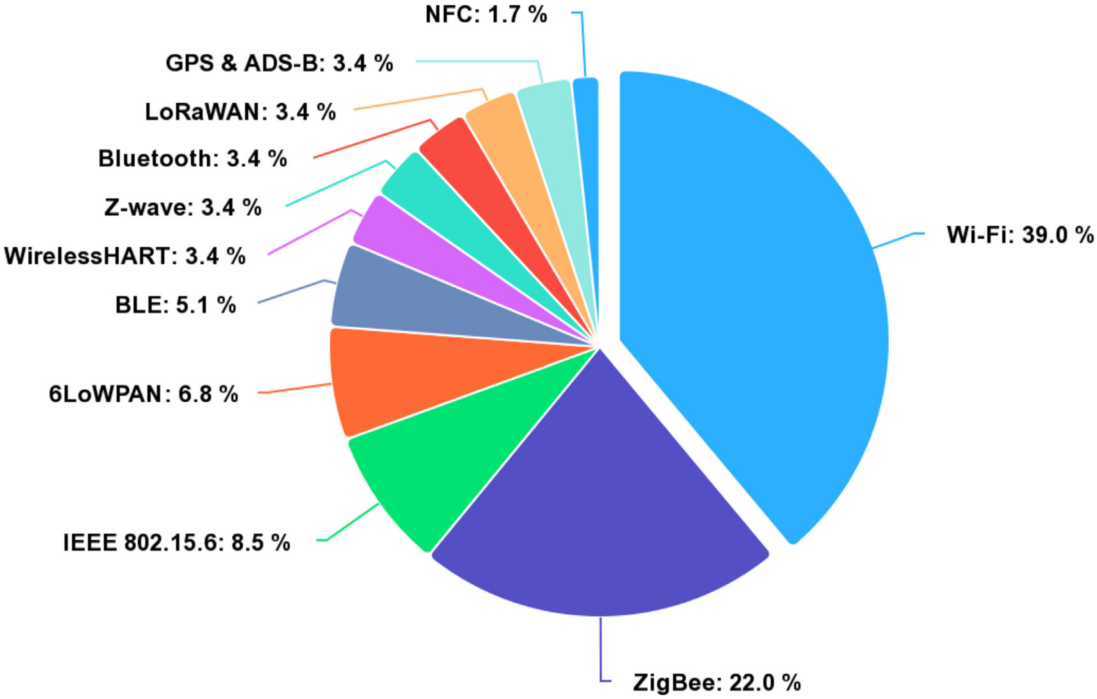

Fig. 4. Percentage of each identified wireless protocol within the testbeds of Section 4.

5.2. Classification of attacks

The attacks considered in each testbed of Section 4 are contained in the third column of Tables 3 to 7 and the fourth column of Table 8. For the needs of the present subsection, the various attacks are organized in relation to five layers of the Open Systems Interconnection (OSI) model, namely, PHY, data link, network, transport, and application. An overview of the compiled attack classification as derived from the various testbeds is illustrated in Figure 5. Moreover, for reasons of completeness, a secondary dual-level classification based also on the well-known Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (STRIDE) model is given in Table 11. Given that on a top-level view, also according to NIST (NIS, 0000), the risk is defined as “a function of the adverse impacts that would arise if [an adverse] circumstance or event occurs and the likelihood of occurrence”, the twofold classification of Table 11 can serve as a means to sketchily assess the likelihood parameter (as an estimation of threats per OSI layer) in the previous function. In other words, as the information of Table 11 stems from the study of a significant mass of research works in the CPS ecosystem, it can be exploited by diverse parties towards identifying threats pertinent to wireless domains incorporated in CPS realms.

From the latter figure, it is clear that the majority of the attacks are concerned with the data link layer. This is mainly due to the different way wireless protocols implement layer 2 in comparison to their wired counterparts; recall that this reason applies to the PHY layer as well. Moreover, several wireless protocols are still new, not having passed the test of time; as wireless technologies evolve at a fast pace, new vulnerabilities emerge, and attackers plot novel penetration methodologies. With reference to Figure 5, a representative example of this situation is the plethora of different kinds of DoS attacks exercised at the MAC layer of, say, IEEE 802.11. These, for example, include the well-known deauthentication or disassociation assaults owing to unprotected management or control frames (Kolias et al., 2016a), and others identified more recently in the literature (Chatzoglou et al., 2022; 2023; Kampourakis et al., 2022).

No less importantly, DoS attacks in the wireless terrain may serve as a springboard for the evildoer. This is because, once disconnected due to a DoS assault, a wireless station will probably scan or probe for an alternate network, which the attacker can insidiously provide by means of a rogue AP. After that, they can use phishing techniques to acquire private information (Chatzoglou et al., 2021b). As expected, with reference to Figure 5, another commonly exercised attack method at layer 2 is ARP spoofing. It is abundantly used as a first step towards mounting MitM by enabling the attacker to masquerade as the default router. On the other hand, a masquerade attack allows the opponent to impersonate a legitimate node, e.g., by spoofing its MAC address or presenting themselves as multiple nodes in the same network. If successfully done, the attacker’s quiver is equipped with a range of further exploitation options. For instance, they can manipulate or simply pollute the in-transit data, drop the network traffic or tunnel it to a remote node and subsequently replay it, and many more.

As already pointed out, similar to the data link layer, the PHY layer is also very differently implemented in wireless protocols. In addition, due to the difficulty of applying any access control, wireless links remain exposed to a variety of attacks. Anyone in the vicinity or further afield can interfere with the communications by simply leveraging the openness of the transmission medium. Simply put, in the general case, wireless protocols are easy targets to deliberate jamming attacks, and this is despite the frequency hopping mechanisms these protocols typically utilize. Generally, a powerful enough transmitter tuned to the same frequency and using the same type of modulation as that of the targeted device can override any signal at the victim’s side. In this context, wireless jamming for, say, Bluetooth or Wi-Fi signals is feasible with low power. In the simplest case, the adversary can opportunistically inject noise into the wireless channel. For instance, as mentioned in subsection 4.1, through the AWGN noise model, the attacker can transmit white noise, i.e., a random signal having equal intensity at different frequencies, making it impossible for the receiver to separate the data from the noise (Adepu et al., 2017). Additionally, the coding and modulation schemes used in the PHY layer can be

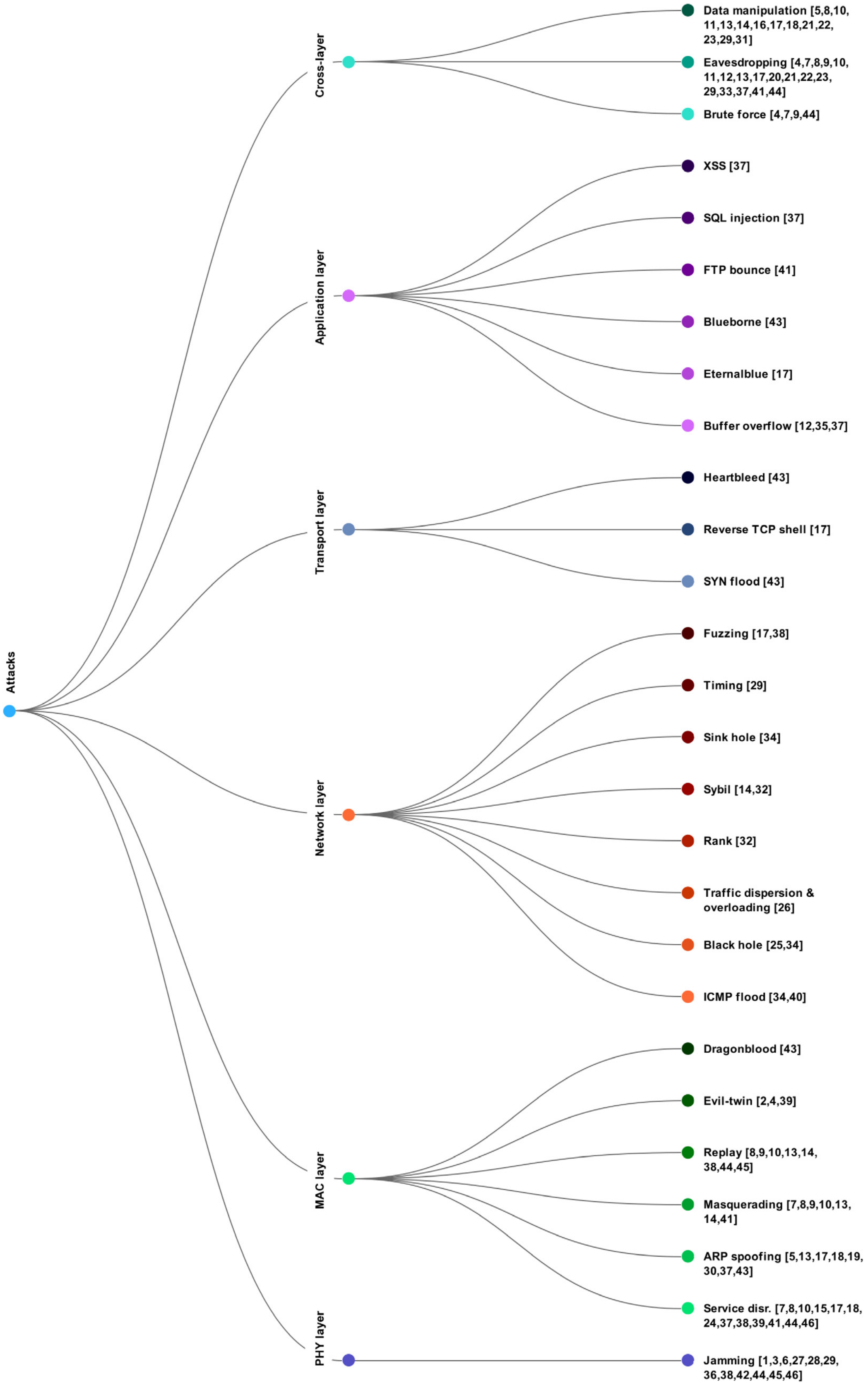
Attacks
Cross-layer
Data manipulation [5,8,10, 11,13,14,16,17,18,21,22, 23,29,31]
Eavesdropping [4,7,8,9,10, 11,12,13,17,20,21,22,23, 29,33,37,41,44]
Brute force [4,7,9,44]
Application layer
XSS [37]
SQL injection [37]
FTP bounce [41]
Blueborne [43]
Eternalblue [17]
Buffer overflow [12,35,37]
Transport layer
Heartbleed [43]
Reverse TCP shell [17]
SYN flood [43]
Network layer
Fuzzing [17,38]
Timing [29]
Sink hole [34]
Sybil [14,32]
Rank [32]
Traffic dispersion & overloading [26]
Black hole [25,34]
ICMP flood [34,40]
MAC layer
Dragonblood [43]
Evil-twin [2,4,39]
Replay [8,9,10,13,14, 38,44,45]
Masquerading [7,8,9,10,13, 14,41]
ARP spoofing [5,13,17,18,19, 30,37,43]
Service disr. [7,8,10,15,17,18, 24,37,38,39,41,44,46]
PHY layer
Jamming [1,3,6,27,28,29, 36,38,42,44,45,46]

Fig. 5. Classification of attacks identified in the testbeds of Section 4.

Table 11
A dual-level classification of the attacks of Figure 5 based also on the STRIDE model.

Layer	Attack	S	T	R	I	D	E
Physical	Jamming	-	-	-	-	✓	-
	Service disruption	-	-	-	-	✓	-
	ARP spoofing	✓	-	-	-	-	-
	Masquerade	✓	✓	✓	✓	-	✓
Data link	Replay	-	✓	✓	-	-	-
	Evil-twin	✓	✓	✓	✓	-	✓
	Dragonblood	-	-	-	✓	-	✓
	ICMP flood	-	-	-	-	✓	-
	Sink hole	-	-	-	-	✓	-
	Black hole	-	-	-	-	✓	-
Network	Rank	-	✓	-	-	-	-
	Traffic dispersion & overloading	-	-	-	-	✓	-
	Sybil	✓	✓	✓	✓	-	✓
	Timing	-	-	-	✓	-	-
	Fuzzing	-	-	-	-	✓	✓
	Eavesdropping	-	-	-	✓	-	-
Cross-layer	Data manipulation	-	✓	-	-	-	-
	Brute force	-	-	-	✓	-	✓
Transport	SYN flood	-	-	-	-	✓	-
	Reverse TCP shell	-	-	-	-	-	✓
	Heartbleed	-	✓	-	✓	-	-
	Buffer overflow	-	-	-	-	-	✓
	Eternalblue	-	-	-	-	-	✓
	Blueborne	-	-	-	-	-	✓
Application	FTP bounce	-	-	-	-	-	✓
	SQL injection	-	✓	-	-	-	-
	XSS	-	✓	-	-	-	-

exploited by a middleman who eavesdrops on the radio channel with the aim of extracting useful information regarding the communications in the network (Gao et al., 2021; Strohmeier et al., 2022; Yasaei et al., 2020).

A significant mass of the identified attacks in Section 4 concerns the network layer; most of them target the underlying routing protocol. Regardless that generally the same operational principles apply to both the wired and wireless protocols in this layer, for the latter category, there is a great diversity in the utilized routing protocols. This situation is apparent in the case of infrastructureless wireless networks. For instance, works like (Sharma et al., 2022; Tomić et al., 2018b) examined black hole attacks against 6LoWPAN. Similar studies (Airehrour et al., 2019; Righetti et al., 2022) elaborated on assaults against similar routing protocols, including 6P and RPL, demonstrating their feasibility and hazardous effects depending on the case. Apart from routing attacks, there is a rich repertoire of legacy attacks that can be mounted in the network layer as well. With reference to subsections 4.3 and 4.6.4, these include ICMP flooding (Kim et al., 2022a; Tomić et al., 2018b) and fuzzing (Koroniotis et al., 2021). Nevertheless, as a rule of thumb, the latter attack tactics are not essentially different from their equivalent in wired network domains.

As depicted in Figure 5 and detailed in Section 4, a number of attacks occur in multiple layers, commonly data link, network, transport, and application (Kauer et al., 2018; Mathur and Tippenhauer, 2016; Yu and Park, 2022). By way of illustration, passive eavesdropping may enable the opponent to collect information stemming from various sources (layers): the frame's header (e.g., MAC addresses), the packet's header (e.g., IP addresses), the packet's payload (e.g., TCP/UDP ports and application data), and so on. Furthermore, an active assailant can perform a wide range of on-path attacks, say, spoofing and replay, which also may pertain to multiple layers of the stack. Overall, from Figure 5, eavesdropping and data manipulation are the most frequently met ones in the testbeds of Section 4. On top of that, due to the wireless nature of communications in such testbeds, the attacker can additionally devise side-channel attacks to analyze the physical parameters of interest. For instance, they can study how long it takes for the system to respond to different inputs, and then perform a timing attack (Samaddar et al., 2020).

Regarding the top two layers of the stack, namely transport and application, it is obvious from Figure 5 that the number of studies per identified attack is smaller. As already pointed out, this is because both these layers operate more or less the same way, in spite of the communication medium. Therefore, although an adversary can abuse or take advantage of transport or application layer protocols like Transmission Control Protocol (TCP) or Hypertext Transfer Protocol (HTTP), respectively, all of them are medium-agnostic.

Lastly, with reference to Table 11, the majority of the included attacks in Figure 5 are concerned with the elevation of privileges threat, followed by tampering, information disclosure, DoS, and spoofing and repudiation, in that order.

Altogether, as observed from Figure 5, 27 different attacks were identified throughout the analysis of testbeds in Section 4. Given that wireless protocols differentiate mostly in PHY and data link layers from their wired counterparts, the majority of the examined attacks congregated in these two layers. Indicatively, DoS (either via jamming or in layer 2) and evil-twin are two of the most frequently met attacks in wireless environments. Albeit such attacks are not due to the "wirelessness" of CPS per se, the cyber kill chain, including attack vectors, vulnerabilities, and so on may be significantly different. Regarding the network layer, black hole, sinkhole, and similar attacks, are common against reputation-based networks, regardless of the system's orientation; put simply, they are not specific to CPS. The same applies to legacy attacks exercised at the network, transport, or application layers.

5.3. Classification of controls

This subsection elaborates on the security controls proposed in the testbeds of Section 4. The various controls are summarized in the form of a classification diagram in Figure 6. Specifically, the classification spans three axes, namely controls oriented on network, hardware, and cryptography. Given that not every testbed of Section 4 examined a security control, the respective classification is smaller vis-à-vis that of Figure 5.

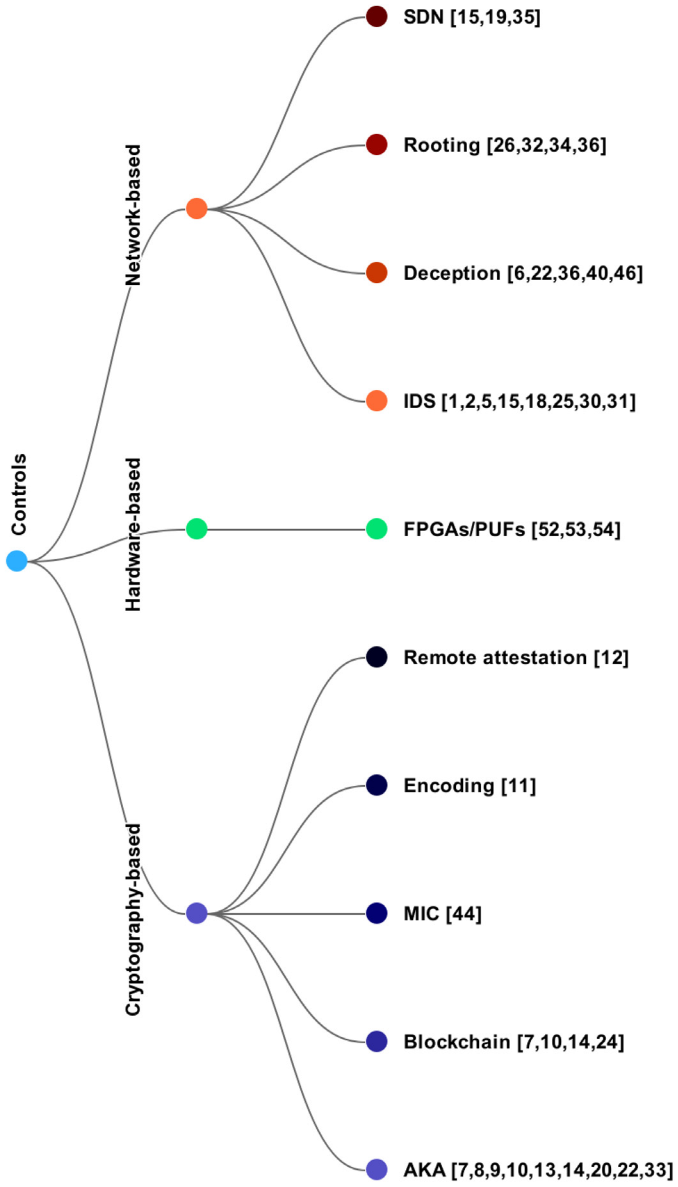

Fig. 6. Classification of controls identified in the testbeds of Section 4.

As observed from Figure 6, the majority of the considered countermeasures are network-based. Focusing on the network perimeter, several works propose the use of IDS. Lying in the front line of network security infrastructure, such systems have a key role in the security of any type of communications technology and are considered essential ingredients of contemporary networks. These systems can be basically classified as either misuse or anomaly detection. The first category aims at differentiating legitimate traffic from malicious based on previously identified patterns, while the second targets at discerning uncommon divergences from a normal profile of behavior. From the analysis given in Section 4, the proposed IDS systems rely on ML techniques, either supervised (Adepu and Mathur, 2016; Babun et al., 2020; Petrillo et al., 2020; Sharma et al., 2022; Tomić et al., 2018a) or unsupervised (Hidalgo et al., 2022; Prakash and Ahmed, 2017; Yasaei et al., 2020).

Another network-based security control considers routing protocols utilized in wireless ad-hoc environments (Airehrour et al., 2019; Fröhlich et al., 2018; Righetti et al., 2022; Tomić et al., 2018b). Specifically, such protocols are particularly attractive to malevolent actors because they are inherently prone to a range of DoS attacks, including black hole (Sharma et al., 2022; Tomić et al., 2018b), Sybil (Airehrour et al., 2019), sinkhole (Tomić et al., 2018b), and flooding (Kim et al., 2022a). The relevant works in Section 4 attempt to mitigate this threat by proposing amended, more secure versions of such protocols (Airehrour et al., 2019). This is done by either introducing additional security mechanisms or through modifications in the scheduling mechanisms (Fröhlich et al., 2018; Righetti et al., 2022; Tomić et al., 2018b) of the routing process. Another cluster of network-oriented security controls takes advantage of SDN technology. SDN is an emerging network architecture approach where the control and data planes are decoupled, enabling the network to be centrally managed through software applications. This results in highly scalable, flexible networks, where the underlying network infrastructure is abstracted from the applications. From a security standpoint, routing the network traffic through an SDN allows the network administrator to monitor in a centralized way the SDN nodes for possible deviations, and thus cope with cyberattacks (Ge et al., 2018; Hidalgo et al., 2022; Kim et al., 2019) in a timely manner.

Most of the current defense practices mainly focus on reactive response, namely, they concentrate on the latter phases of the cyber kill chain, those after the reconnaissance phase. An alternative, but complementary, defensive strategy is to proactively engage with attackers already from the early stages of their cyber kill chain with the aim to obstruct or neutralize possible attacks. Such strategies typically fall into two categories, namely, moving target defense and cyber deception (Wang and Lu, 2018). The first disrupts opponents' reconnaissance and attack preparation by adding complexity, perplexity, diversity, and randomness to the targeted system, while the second offers seemingly believable yet deceiving information to trick attackers. In this context, as shown in several works of Section 4, moving target defense is also considered as a countermeasure (Chinthi-Reddy et al., 2022; Fröhlich et al., 2018; Kim et al., 2022a). For instance, as detailed in Khadr et al. (2022); Si et al. (2016), in the presence of any communication delay or disruption, say, due to an ongoing DoS attack, the network traffic is rerouted through an alternative path. Equally interestingly, a typical way of implementing cyber deception is through honeypots. That is, honeypots pose as alluring (and sometimes vulnerable) service hosts, thus having increased chances of attracting attackers. Based on the data collected by honeypots, defenders can profile adversaries, further engage with them in a deceptive manner, and improve system security overall. Nevertheless, no work of Section 4 implemented cyber deception through honeypots.

A significant portion of the classification diagram depicted in Figure 6 concentrates on cryptographic solutions, with AKA protocols having the lion's share. Briefly, an AKA protocol provides authenticated key agreement in such a way that all the participants influence the resulting shared symmetric key. Especially for (I)IoT and WSN applications, where all or at least some of the devices can be resource-constrained, lightweight but still robust security controls for safeguarding communications in terms of confidentiality and integrity are of the essence. In this regard, several testbeds detailed in Section 4 in the healthcare and UAS sectors elaborate on AKA schemes based on either hardware (Alladi et al., 2020; Pu et al., 2022), blockchain (Shawky et al., 2023), or both (Wang et al., 2021; Yu and Park, 2022) solutions. Moreover, the cryptographic category contains works that utilize legacy schemes to protect wireless communications. These include the use of MIC for providing source authentication on the one hand, and ensuring the integrity of the payload and selected sensitive fields of the frame's header on the other (Kauer et al., 2018). Additionally, as shown in Figure 6, remote attestation has been also utilized in one testbed (Surminski et al., 2021) of Section 4 for authenticating real-time embedded devices. Recall that the aim of remote attestation is to allow a remote system acting as a challenger to securely check the internal state of a remote untrusted device acting as an attestator or prover. Simply put, through this process, the challenger can detect compromised devices. A last countermeasure that falls under the same category of solutions concerns a flip bit technique applied at the PHY layer (Hussain et al., 2021). With reference to Section 4, this defensive scheme is triggered upon sensing conspicuous fluctuations in the RSS of the Wi-Fi signal.

Last but not least, the only purely hardware-based control identified among the works of Section 4 refers to the use of PUF (Alladi et al., 2020; Wang et al., 2021; Yu and Park, 2022). The latter comprises a physical object among others used in the context of high-security lightweight AKAs. Specifically, PUFs capitalize on the physical differences of every integrated circuit, such as Field Programmable Gate Arrays (FPGAs) and microprocessors. For a given input and conditions, a PUF will respond with a PHY digital fingerprint which uniquely identifies the device.

Overall, all the controls depicted in Figure 6 are more or less customary defensive techniques that can be exploited regardless of the network's nature and depending on the case at hand. Nevertheless, as already mentioned, wireless protocols are natively different due to the absence of access control. In addition, any cryptographic-based control applied to a wireless protocol should not significantly saturate network bandwidth, thus, typically, a lightweight variation is considered. On top of that, the addition of extra controls goes in tandem with increased delay and a diminished level of responsiveness, which in turn may be unacceptable for CPS. Especially for CI, availability and timeliness are critical, thus any applied control must consider the above-mentioned limitations and be adjusted appropriately.

Interestingly, all but four of the works that proposed security controls, also provided some sort of performance evaluation. Precisely, most of them utilized network-oriented metrics, such as RTT, PDR, PRR, communication overhead, data delivery latency, throughput, and data loss, among others. On the other hand, studies that suggested an IDS predicated their evaluation on legacy classification performance metrics, including accuracy, TPR, FPR, precision, recall, ROC, and F1. Furthermore, a fair amount of the identified countermeasures were assessed through the use of computing resources consumption metrics, such as energy and memory depletion, CPU cycles, and others. Overall, with reference to figure 6, network-based controls are typically evaluated through packet-, time-, or classification-based metrics, while cryptography- and hardware-powered controls are mostly evaluated by means of CPU or memory consumption, and time-related performance criteria.

6. Takeaways and Challenges

The present section briefly summarizes the discussion given in the previous two sections and rolls it up into takeaway points and challenges.

- *Wireless technologies in CPS:* Wireless technologies have quickly penetrated into the CPS domain, and it is rather deterministic that they will be also progressively adopted consistently across the industry and IIoT and CI realms. Besides, modernization is key to the successful implementation and growth of Industry 4.0. Due to this transition, wireless IIoT networks and WSNs are expected to become omnipresent across multiple CPS sectors. Nevertheless, the inclusion of wireless technology comes alongside a rich repertoire of threats and vulnerabilities, which in turn intensifies complexity and substantially augments the attack surface. What is more, the coexistence of wired and wireless technologies under the same umbrella broadens further the attack surface, increasing the complexity of the underlying system at the same time. Besides, it is not to be neglected that as wireless technologies advance at an accelerated pace, new vulnerabilities surface, and aggressors devise increasingly sophisticated cyber kill chains. On top of that, as explained in subsection 5.2, threat actors oftentimes exploit wireless networks as a stepping stone toward more perilous attacks. Last but not least, wireless (I)IoT systems include resource-constrained devices that as a rule of thumb are sensitive to interference and jamming in particular. This inherent weakness is especially important in several sectors, including smart cities, Internet of vehicles (IoV), UAS, and others. Based on the findings in Section 4, it is true that major CI sectors, including energy and manufacturing, have not yet integrated wireless technologies, at least to a significant degree. This is because (a) typically, it is a time-consuming and costly process to perform drastic changes in such complex infrastructures, (b) most of the infrastructure in use, namely, physical machinery and OT/IT networks have a multi-year prospect and their expiry time is often prolonged, and (c) such changes would require for large parts of the facility to be shut-off for a considerable time, something that will very likely provoke disruption of the normal functions, subsequently leading to financial losses.
- *Testbed thoroughness:* Security testbeds and, by extension, digital twins, are generally considered an efficient way of scrutinizing the security level of a real system without directly interfering with it, say, conducting red teaming on a real CI system while in operation. Nevertheless, for this process to be fruitful, several key issues must be considered and dealt with. First, the development of a full-fledged or at least complete enough and scalable testbed is in most cases costly and time-consuming. Indeed, almost none of the wireless-focused testbeds contained in Section 4 is full-grown and scalable; the *SWaT* testbed (Mathur and Tippenhauer, 2016) is an exception to this generalization. That is, as shown in Table 9, most of the testbeds utilize either open-source software, low-cost physical equipment, or both to experimentally test the system's resilience against specific attacks or evaluate the effectiveness of a particular countermeasure. Overall, as expected, the great majority of the testbeds examined are inflexible and have a very narrow, academic scope, making them largely unsuitable for conducting 360-degree security appraisals, especially when it comes to IIoT and CI. On top of that, with reference to the same table, the high diversity among the hardware and software tools used among the different wireless-oriented testbeds, even if the testbeds concern the same CI sector, makes it hard to properly decide which of them are the most appropriate for the development of a similar testing platform. This means that, especially for IIoT and CI, researchers need to tightly collaborate with the industry to better comprehend the nature of real systems and subsequently reflect them in their testbeds. Third, no testbed was built with a dual purpose in mind; systematic hands-on security assessment and cybersecurity education and training. Based on the findings of this work, even more important is the fact that currently the literature largely misses a unified, layered model guiding in an abstract way the creation of such testbeds. Putting it another way, a key gap in the literature is the lack of a reference architecture for designing and developing cross-sector CI security testbeds and cyber-physical ranges.
- *Heterogeneous data and distributed nature:* (I)IoT data comprise multi-variant, time-series data, typically collected via a heterogeneous network of sensors with diverse data types, sampling rates, and specifications. From a radio interface perspective, and with reference to the second column of Tables 3 to 7 and the third column of Table 8, a plethora of technologies may co-exist; cellular, IEEE 802.11, IEEE 802.15.4, IEEE 802.15.6, ITU-T G.9959, to mention just a few. Moreover, in wireless net-

works the nodes are inherently distributed and potentially mobile, meaning that the underlying monitoring facilities and security controls should be also distributed, but simultaneously able to apply filtering and minimize the exchange of security-related information with central nodes. For ML-driven security controls, say, in the context of an IDS, this distributed terrain means that the analysis of data must either occur at a central location after gathering it from the network sensors or topically through collaboration by dealing with the task through a distributed ML outlook.

- *Threat intelligence and datasets:* Although there exist some recent efforts to track the assignment of Common Vulnerabilities and Exposures (CVE) identifiers specifically for ICS and medical device vendors (CIS, 0000; 0000; 0000), this endeavor should be further systematized and intensified to include as many stakeholders and sources of information as possible. That is, threat intelligence in this ecosystem is a sine qua non for providing a deep insight into adversary behavior and offering the necessary context for decision-making processes. Another noteworthy observation stemming from Section 4 is that no testbed has been used also with the aim to create proper publicly available datasets to be used by the security community. Precisely, such datasets facilitate researchers and practitioners to better comprehend and analyze the corresponding attacks and devise and test countermeasures. This result corroborates the observation that the literature largely lacks datasets specifically destined to CPS security research and training.
- *Security as a trade-off:* Undoubtedly, security controls are generally beneficial when it comes to protecting CPS. However, despite their advantages in terms of ameliorating the overall security level of the underlying system, one has to also reckon with the potential negative impacts. That is, as availability and direct data access are essential in a CPS, the application of countermeasures could affect normal operation and add significant overhead. Put simply, a countermeasure may affect the performance or usability of certain CPS components. For instance, encryption comes at a cost in terms of computing and network resources. Moreover, adding security controls on top of a CPS increases power consumption, especially with reference to resource-constrained CPS and devices, such as WSN. This in turn means that the lifespan of such systems is reduced, also upsizing the maintenance costs. On the other hand, in regard to availability, the use of heavyweight cryptographic mechanisms may have unfavorable side effects, increasing transmission delay; for certain CPSs this may be intolerable. Naturally, under a usable security mindset and at least for the IT systems, the most advantageous security measures should allow for transparent protection while improving user experience. Lastly, as already pointed out, in several cases, CPSs comprise heterogeneous and complex systems that mostly incorporate diverse hardware and software components. Depending on the particular situation, this may induce compatibility issues with the employed countermeasures.

7. Conclusions

The CPS is considered a principal ingredient in the ongoing evolution of Industry 4.0. IoT, AI, advanced analytics, digital twins, and others also play a key role within this ecosystem. On the other hand, few would dispute that the use of CPS has also led to a much augmented attack surface, mainly due to the increased connectivity, and sometimes complexity. In this setting, security testbeds have arisen as a valuable means of assessing the security posture of a real system without interfering with its internal structures and procedures. In this context, the current work contributes the first to our knowledge SLR, concentrating on literature works that elaborate on wireless security testbeds used in the CPS realm to either evaluate attacks or countermeasures. We examined the relevant works published between 2016 and 2023 and categorized them according to the CPS sector they refer to. The analysis conducted on the included works spans three axes per identified testbed: attacks, countermeasures, and software and hardware tools. Regarding attacks and countermeasures, we additionally offer respective classifications based either on the layers of the OSI model or the orientation of the solution, respectively.

Through our analysis of almost 50 articles, we resulted in a couple of key observations. First, it was corroborated that wireless technologies are gradually penetrating into the CPS domain as a flexible means to complement the functionality provided by their wired counterparts. Second, the provided attack classification in Section 5 showcases that the capacity of a threat actor targeting wireless links of CPS is at least significant. That is, owing mostly to the inherent openness of the wireless communication medium, legacy wireless attacks are valid in a CPS context and can always be adapted to better reflect the underlying system, as the case may be. No less important, we arrive at an additional list of pivotal remarks regarding overarching issues about the examined testbeds, including testbed thoroughness and security as a trade-off. Based on the outcomes of this SLR, a particularly interesting direction for future work is establishing an overarching reference architecture for designing and developing security testbeds or cyber ranges (Kampourakis, 2023). This is envisioned to facilitate future initiatives and provide homogeneity among different CRs and security testbeds. Overall, we anticipate this work will provide more insight into this rapidly evolving and interesting research area and serve as a solid reference point for future work.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.cose.2023.103383

References

Abichandani, P., Lobo, D., Kabrawala, S., McIntyre, W., 2020. Secure communication for multiquadrotor networks using ethereum blockchain. IEEE Internet of Things Journal 8 (3), 1783–1796.

Adepu, S., Mathur, A., 2016. Distributed detection of single-stage multipoint cyber attacks in a water treatment plant. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pp. 449–460.

Adepu, S., Prakash, J., Mathur, A., 2017. Waterjam: An experimental case study of jamming attacks on a water treatment system. In: 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, pp. 341–347.

Adil, M., Almaiah, M.A., Omar Alsayed, A., Almomani, O., 2020. An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. Sensors 20 (8), 2311.

Agarwal, S., Rashid, A., Gardiner, J., 2022. Old macdonald had a smart farm: Building a testbed to study cybersecurity in smart dairy farming. In: Proceedings of the 15th Workshop on Cyber Security Experimentation and Test, pp. 1–9.

Agrawal, N., Kumar, R., 2022. Security perspective analysis of industrial cyber physical systems (i-cps): A decade-wide survey. ISA transactions.

Ahmadi, A., Moradi, M., Cherifi, C., Cheutet, V., Ouzrout, Y., 2018. Wireless connectivity of cps for smart manufacturing: A survey. In: 2018 12th International Conference on Software, Knowledge, Information Management & Applications (SKIMA). IEEE, pp. 1–8.

Airehrour, D., Gutierrez, J.A., Ray, S.K., 2019. Sectrust-rpl: A secure trust-aware rpl routing protocol for internet of things. Future Generation Computer Systems 93, 860–876.

Al Nafea, R., Almaiah, M.A., 2021. Cyber security threats in cloud: Literature review. In: 2021 International Conference on Information Technology (ICIT). IEEE, pp. 779–786.

Alamer, M., Almaiah, M.A., 2021. Cybersecurity in smart city: A systematic mapping study. In: 2021 International Conference on Information Technology (ICIT). IEEE, pp. 719–724.

Ali, A., Almaiah, M.A., Hajjej, F., Pasha, M.F., Fang, O.H., Khan, R., Teo, J., Zakarya, M., 2022. An industrial iot-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors 22 (2), 572.

Alladi, T., Chamola, V., et al., 2020. Harci: A two-way authentication protocol for three entity healthcare iot networks. IEEE Journal on Selected Areas in Communications 39 (2), 361–369.

Almaiah, M.A., 2021. A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In: Artificial Intelligence and Blockchain for Future Cybersecurity Applications. Springer, pp. 217–234.

Almaiah, M.A., Al-Zahrani, A., Almomani, O., Alhwaitat, A.K., 2021. Classification of cyber security threats on mobile devices and applications. In: Artificial Intelligence and Blockchain for Future Cybersecurity Applications. Springer, pp. 107–123.

Almaiah, M.A., Hajjej, F., Ali, A., Pasha, M.F., Almomani, O., 2022. A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare iot based cps. Sensors 22 (4), 1448.

Altulaihan, E., Almaiah, M.A., Aljughaiman, A., 2022. Cybersecurity threats, countermeasures and mitigation techniques on the iot: Future research directions. Electronics 11 (20), 3330.

Alzahrani, B.A., Irshad, A., Albeshri, A., Alsubhi, K., 2021. A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. Wireless Personal Communications 117 (1), 47–69.

Aono, T., Higuchi, K., Ohira, T., Komiyama, B., Sasaoka, H., 2005. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. IEEE Transactions on Antennas and Propagation 53 (11), 3776–3784.

Appavoo, P., William, E.K., Chan, M.C., Mohammad, M., 2019. Indriya2: A heterogeneous wireless sensor network (wsn) testbed. In: International Conference on Testbeds and Research Infrastructures. Springer, pp. 3–19.

Aras, E., Small, N., Ramachandran, G.S., Delbruel, S., Joosen, W., Hughes, D., 2017. Selective jamming of lorawan using commodity hardware. In: Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 363–372.

Arduino wifi shield, Visited on 2023-01-11. https://docs.arduino.cc/retired/shields/arduino-wifi-shield.

Åström, K.J., Wittenmark, B., 2013. Computer-controlled systems: theory and design. Courier Corporation.

A200 series class a, Visited on 2023-04-07. https://em-trak.com/products-a200/.

Aircrack-ng, Visited on 2023-04-07. https://www.aircrack-ng.org/.

Airmind, Visited on 2023-01-11. https://airmind.mindpx.net/.

Arduino, Visited on 2023-01-11. https://www.arduino.cc/.

Atmega256rfr2, Visited on 2023-01-11. https://www.microchip.com/en-us/product/ATMEGA256RFR2.

Automated validation of internet security protocols and applications, Visited on 2022-12-20. https://www.avispa-project.org/.

Avr-rs-uzb, Visited on 2023-01-11. https://community.element14.com/?oldJiveUrl=community/docs/DOC-67532/l/avr-rz-usb-stick-module-pifragment-12485=6.

Babun, L., Aksu, H., Ryan, L., Akkaya, K., Bentley, E.S., Uluagac, A.S., 2020. Z-iot: Passive device-class fingerprinting of zigbee and z-wave iot devices. In: ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, pp. 1–7.

Basiri, M.H., Pirani, M., Azad, N.L., Fischmeister, S., 2019. Security of vehicle platooning: A game-theoretic approach. IEEE Access 7, 185565–185579.

Boano, C.A., Voigt, T., Noda, C., Römer, K., Zúñiga, M., 2011. Jamlab: Augmenting sensornet testbeds with realistic and controlled interference generation. In: Proceedings of the 10th ACM/IEEE International Conference on Information Processing in Sensor Networks. IEEE, pp. 175–186.

Bubukayr, M.A.S., Almaiah, M.A., 2021. Cybersecurity concerns in smart-phones and applications: A survey. In: 2021 international conference on information technology (ICIT). IEEE, pp. 725–731.

Burg, A., Chattopadhyay, A., Lam, K.-Y., 2017. Wireless communication and security issues for cyber–physical systems and the internet-of-things. Proceedings of the IEEE 106 (1), 38–60.

Burrows, M., Abadi, M., Needham, R., 1990. A logic of authentication. ACM Transactions on Computer Systems (TOCS) 8 (1), 18–36.

Beagleboard, Visited on 2023-04-20. https://beagleboard.org/bone.

Zigbee and ieee, 802.15.4 wireless mcu with 256kb flash and 8kb ram. Visited on 2023-01-13. https://www.ti.com/product/CC2530.

Chatzoglou, E., Kambourakis, G., Kolias, C., 2021. Empirical evaluation of attacks against ieee 802.11 enterprise networks: The awid3 dataset. IEEE Access 9, 34188–34205.

Chatzoglou, E., Kambourakis, G., Kolias, C., 2021. Wif0: All your passphrase are belong to us. Computer 54 (7), 82–88.

Chatzoglou, E., Kambourakis, G., Kolias, C., 2022. How is your wi-fi connection today? dos attacks on wpa3-sae. Journal of Information Security and Applications 64, 103058.

Chatzoglou, E., Kampourakis, V., Kambourakis, G., 2023. Bl0ck: Paralyzing 802.11 connections through block ack frames. arXiv preprint arXiv:2302.05899.

Cheng, X., Shi, J., Sha, M., Guo, L., 2021. Launching smart selective jamming attacks in wirelesshart networks. In: IEEE INFOCOM 2021-IEEE Conference on Computer Communications. IEEE, pp. 1–10.

Chinthi-Reddy, S.R., Lim, S., Choi, G.S., Chae, J., Pu, C., 2022. Darksky: Privacy-preserving target tracking strategies using a flying drone. Vehicular Communications 35, 100459.

Cintuglu, M.H., Mohammed, O.A., Akkaya, K., Uluagac, A.S., 2016. A survey on smart grid cyber-physical system testbeds. IEEE Communications Surveys & Tutorials 19 (1), 446–464.

Conti, M., Donadel, D., Turrin, F., 2021. A survey on industrial control system testbeds and datasets for security research. IEEE Communications Surveys & Tutorials 23 (4), 2248–2294.

Costin, A., Francillon, A., 2012. Ghost in the air (traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices. black hat USA 1, 1–12.

Costin, A., Turtiainen, H., Khandker, S., Hämäläinen, T., 2023. Towards a unified cybersecurity testing lab for satellite, aerospace, avionics, maritime, drone (saamd) technologies and communications. arXiv preprint arXiv:2302.08359.

Castalia: A simulator for wireless sensor networks and body area networks, Visited on 2023-01-25. https://github.com/boulis/Castalia.

Cc110l, Cc110l. Visited on 2023-01-11. https://www.ti.com/product/CC110L.

Chipcon cc2420, Visited on 2023-01-10. https://www.ti.com/product/CC2420.

Cisa to oversee cve numbering authorities for industrial control systems and medical devices, Visited on 2023-03-02. https://www.cisa.gov/news-events/news/cisa-oversee-cve-numbering-authorities-industrial-control-systems-and-medical.

Contiki-ng: The os for next generation iot devices, Visited on 2023-01-11. https://github.com/contiki-ng/contiki-ng.

Cyber incident reporting for critical infrastructure act of 2022 (circia), Visited on 2023-03-04. https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

Dragonradio, Dragonradio. Visited on 2023-01-23. https://drexelwireless.github.io/dragonradio/.

Dynacar, Visited on 2023-01-13. https://dynacar.es/en/home.php.

Dyse-dynamic spectrum environment emulator, Visited on 2023-01-23. https://www.echoridgenet.com/products/dyse.

Epos: Embedded parallel operating system, Visited on 2023-01-23. https://epos.lisha.ufsc.br/HomePage.

Esp8266 nodemcu v1.0 esp-12e wifi module, Visited on 2023-01-11. https://protosupplies.com/product/esp8266-nodemcu-v1-0-esp-12e-wifi-module/.

Evk-8/evk-m8, Visited on 2023-01-09. https://www.u-blox.com/en/product/evk-8evk-m8.

Fdx-b animal identification protocol description, Visited on 2023-01-11. https://www.priority1design.com.au/fdx-b_animal_identification_protocol.html.

Flarm technology, Visited on 2023-01-09. https://www.flarm.com/.

Freertos real-time operating system for microcontrollers, Visited on 2023-03-06. https://www.freertos.org/.

Gnu radio, -the free & open source radio ecosystem. Visited on 2023-01-23. https://www.gnuradio.org/.

Færøy, F.L., Yamin, M.M., Shukla, A., Katt, B., 2023. Automatic verification and execution of cyber attack on iot devices. Sensors 23 (2), 733.

Fambon, O., Fleury, E., Harter, G., Pissard-Gibollet, R., Saint-Marcel, F., 2014. Fit iot-lab tutorial: hands-on practice with a very large scale testbed tool for the internet of things. 10èmes journées francophones Mobilité et Ubiquité, UbiMob2014.

Fröhlich, A.A., Scheffel, R.M., Kozhaya, D., Veríssimo, P.E., 2018. Byzantine resilient protocol for the iot. IEEE Internet of Things Journal 6 (2), 2506–2517.

Gao, D., Wang, S., Liu, Y., Jiang, W., Li, Z., He, T., 2021. Spoofing-jamming attack based on cross-technology communication for wireless networks. Computer Communications 177, 86–95.

Gautam, M.K., Pati, A., Mishra, S.K., Appasani, B., Kabalci, E., Bizon, N., Thounthong, P., 2021. A comprehensive review of the evolution of networked control system technology and its future potentials. Sustainability 13 (5), 2962.

Ge, M., Hong, J.B., Yusuf, S.E., Kim, D.S., 2018. Proactive defense mechanisms for the software-defined internet of things with non-patchable vulnerabilities. Future Generation Computer Systems 78, 568–582.

Giraldo, J., Sarkar, E., Cardenas, A.A., Maniatakos, M., Kantarcioglu, M., 2017. Security and privacy in cyber-physical systems: A survey of surveys. IEEE Design & Test 34 (4), 7–17.

Griffor, E.R., Greer, C., Wollman, D.A., Burns, M.J., et al., 2017. Framework for cyber-physical systems: Volume 1, overview. NIST Special Publication 1500-201 doi:10.6028/NIST.SP.1500-201.

Heemels, W.H., Donkers, M., Teel, A.R., 2012. Periodic event-triggered control for linear systems. IEEE Transactions on automatic control 58 (4), 847–861.

Hidalgo, C., Vaca, M., Nowak, M.P., Frölich, P., Reed, M., Al-Naday, M., Mpatziakas, A., Protogerou, A., Drosou, A., Tzovaras, D., 2022. Detection, control and mitigation system for secure vehicular communication. Vehicular Communications 34, 100425.

Humayed, A., Lin, J., Li, F., Luo, B., 2017. Cyber-physical systems security-a survey. IEEE Internet of Things Journal 4 (6), 1802–1831.

Hussain, A.M., Abualsaud, K., Yaacoub, E., Khattab, T., Gehani, A., Guizani, M., 2021. A testbed for implementing lightweight physical layer security in an iot-based health monitoring system. In: 2021 International Wireless Communications and Mobile Computing (IWCMC). IEEE, pp. 486–491.

hostapd, and wpa_supplicant. Visited on 2023-04-07.https://w1.fi/

Jacovic, M., Liston, M.J., Pano, V., Mainland, G., Dandekar, K.R., 2022. Experimentation framework for wireless communication systems under jamming scenarios. IET Cyber-Physical Systems: Theory & Applications.

Jecan, E., Pop, C., Padrah, Z., Ratiu, O., Puschita, E., 2018. A dual-standard solution for industrial wireless sensor network deployment: Experimental testbed and performance evaluation. In: 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS). IEEE, pp. 1–9.

Jetson tx2 module, Visited on 2023-01-11. https://developer.nvidia.com/embedded/jetson-tx2.

Kambourakis, G., Kolias, C., Geneiatakis, D., Karopoulos, G., Makrakis, G.M., Kounelis, I., 2020. A state-of-the-art review on the security of mainstream iot wireless PAN protocol stacks. Symmetry 12 (4), 579. doi:10.3390/sym12040579.

Kampourakis, V., 2023. Secure infrastructure for cyber-physical ranges. In: Research Challenges in Information Science: Information Science and the Connected World - 17th International Conference, RCIS 2023, Corfu, Greece, May 23-26, 2023, Proceedings. Springer, pp. 622–631. doi:10.1007/978-3-031-33080-3_45.

Kampourakis, V., Chatzoglou, E., Kambourakis, G., Dolmes, A., Zaroliagis, C., 2022. Wpaxfuzz: Sniffing out vulnerabilities in wi-fi implementations. Cryptography 6 (4), 53.

Kartakis, S., Abraham, E., McCann, J.A., 2015. Waterbox: A testbed for monitoring and controlling smart water networks. In: Proceedings of the 1st ACM International Workshop on Cyber-Physical Systems for Smart Water Networks, pp. 1–6.

Kashef, M., Liu, Y., Montgomery, K., Candell, R., 2021. Wireless cyber-physical system performance evaluation through a graph database approach. Journal of Computing and Information Science in Engineering 21 (2).

Kauer, F., Kallias, E., Turau, V., 2018. A dual-radio approach for reliable emergency signaling in critical infrastructure assets with large wireless networks. International Journal of Critical Infrastructure Protection 21, 33–46.

Kayan, H., Nunes, M., Rana, O., Burnap, P., Perera, C., 2022. Cybersecurity of industrial cyber-physical systems: a review. ACM Computing Surveys (CSUR) 54 (11s), 1–35.

Khadr, M.H., Salameh, H.B., Ayyash, M., Elgala, H., Almajali, S., 2022. Jamming resilient multi-channel transmission for cognitive radio iot-based medical networks. Journal of Communications and Networks 24 (6), 666–678.

Kim, S., Lee, S., Park, K.-J., 2022. Real-time controller reconfiguration for delay-resilient cyber-physical systems. IEEE Access 10, 101220–101228.

Kim, S., Park, K.-J., Lu, C., 2022. A survey on network security for cyber–physical systems: From threats to resilient design. IEEE Communications Surveys & Tutorials 24 (3), 1534–1573.

Kim, S., Won, Y., Park, I.-H., Eun, Y., Park, K.-J., 2019. Cyber-physical vulnerability analysis of communication-based train control. IEEE Internet of Things Journal 6 (4), 6353–6362.

Killerbee, Killerbee. Visited on 2023-01-11. https://github.com/riverloopsec/killerbee.

Kolias, C., Kambourakis, G., Stavrou, A., Gritzalis, S., 2016. Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. IEEE Communications Surveys & Tutorials 18 (1), 184–208.

Kolias, C., Stavrou, A., Voas, J., Bojanova, I., Kuhn, R., 2016. Learning internet-of-things security" hands-on". IEEE Security & Privacy 14 (1), 37–46.

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., Janicke, H., 2021. The sair-iiot cyber testbed as a service: A novel cybertwins architecture in iiot-based smart airports. IEEE Transactions on Intelligent Transportation Systems.

Known exploited vulnerabilities catalog, Visited on 2023-03-02. https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

Li, J., Ji, Y., Choo, K.-K.R., Hogrefe, D., 2019. Cl-cppa: Certificate-less conditional privacy-preserving authentication protocol for the internet of vehicles. IEEE Internet of Things Journal 6 (6), 10332–10343.

Li, K., Kurunathan, H., Severino, R., Tovar, E., 2018. Cooperative key generation for data dissemination in cyber-physical systems. In: 2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS). IEEE, pp. 331–332.

Li, K., Lu, N., Zheng, J., Zhang, P., Ni, W., Tovar, E., 2021. Bloothair: A secure aerial relay system using bluetooth connected autonomous drones. ACM Transactions on Cyber-Physical Systems 5 (3), 1–22.

Li, K., Ni, W., Emami, Y., Shen, Y., Severino, R., Pereira, D., Tovar, E., 2019. Design and implementation of secret key agreement for platoon-based vehicular cyber-physical systems. ACM Transactions on Cyber-Physical Systems 4 (2), 1–20.

Li, X., Li, D., Wan, J., Vasilakos, A.V., Lai, C.-F., Wang, S., 2017. A review of industrial wireless networks in the context of industry 4.0. Wireless networks 23 (1), 23–41.

Lydia, M., Prem Kumar, G.E., Selvakumar, A.I., 2022. Securing the cyber-physical system: A review. Cyber-Physical Systems 1–31.

Labsat gnss simulators, Visited on 2023-01-09. https://www.labsat.co.uk/index.php/en/.

Lattepanda, Visited on 2023-01-09. https://www.lattepanda.com/.

Liclipse, Visited on 2023-01-09. https://www.liclipse.com/.

Low cost,low-power 2.4 ghz rf transceiver designed for low-power wireless apps in the 2.4 ghz ism b. Visited on 2023-01-13. https://www.ti.com/product/CC2500.

Makrakis, G.M., Kolias, C., Kambourakis, G., Rieger, C., Benjamin, J., 2021. Industrial and critical infrastructure security: Technical analysis of real-life security incidents. IEEE Access 9, 165295–165325.

Mathur, A.P., Tippenhauer, N.O., 2016. Swat: A water treatment testbed for research and training on ics security. In: 2016 international workshop on cyber-physical systems for smart water networks (CySWater). IEEE, pp. 31–36.

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A.-R., Maniatakos, M., Karri, R., 2016. The cybersecurity landscape in industrial control systems. Proceedings of the IEEE 104 (5), 1039–1057.

McNickle, D., Pawlikowski, K., Ewing, G., 2010. Akaroa2: A controller of discrete-event simulation which exploits the distributed computing resources of networks. In: ECMS, pp. 104–109.

Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., Stewart, L.A., 2015. Preferred reporting items for systematic review and meta-analysis protocols (prisma-p) 2015 statement. Systematic reviews 4 (1), 1–9.

Montori, F., Bedogni, L., Di Felice, M., Bononi, L., 2018. Machine-to-machine wireless communication technologies for the internet of things: Taxonomy, comparison and open issues. Pervasive and Mobile Computing 50, 56–81.

Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., Pantziou, G., 2009. A survey on jamming attacks and countermeasures in wsns. IEEE Communications Surveys & Tutorials 11 (4), 42–56.

Matrice 100 - dji, Visited on 2023-01-11. https://www.dji.com/no/matrice100.

Mcu arm cortex-m4, Visited on 2023-01-11. https://www.st.com/content/st_com/en/arm-32-bit-microcontrollers.html.

Micaz: Wireless measurement system, Visited on 2023-01-13. http://courses.ece.ubc.ca/494/files/MICAz_Datasheet.pdf.

Model as-xm1000 - mote module, Visited on 2023-01-13. https://www.environmental-expert.com/products/advanticsys-model-as-xm1000-mote-module-262761.

Msp430, Visited on 2023-01-10. https://www.ti.com/microcontrollers-mcus-processors/microcontrollers/msp430-microcontrollers/overview.html.

Multi-generator (mgen) network test tool, Visited on 2023-01-23. https://www.nrl.navy.mil/Our-Work/Areas-of-Research/Information-Technology/NCS/MGEN/.

Multiprecision integer and rational arithmetic cryptographic library, Visited on 2022-12-20. https://github.com/miracl/MIRACL.

Mx400 hardware, Visited on 2022-12-26. http://www.mindpx.net/assets/accessories/MX400usermanual_v12.pdf.

Nazir, R., Laghari, A.A., Kumar, K., David, S., Ali, M., 2021. Survey on wireless network security. Archives of Computational Methods in Engineering 1–20.

Osterlind, F., Dunkels, A., Eriksson, J., Finne, N., Voigt, T., 2006. Cross-level sensor network simulation with cooja. In: Proceedings. 2006 31st IEEE conference on local computer networks. IEEE, pp. 641–648.

Ou, X., Govindavajhala, S., Appel, A.W., et al., 2005. Mulval: A logic-based network security analyzer. In: USENIX security symposium, Vol. 8. Baltimore, MD, pp. 113–128.

Omnet++ documentation, Visited on 2022-12-17. https://omnetpp.org/documentation/.

Omnet++ documentation. Visited on 2022-12-17. https://omnetpp.org/documentation/.

Onos, Visited on 2023-01-09. https://wiki.onosproject.org/.

Opencpn chart plotter navigation, Visited on 2023-04-07. https://www.opencpn.org/.

Orbitty, carrier for nvidia® jetsonTH tx2/tx2i. Visited on 2023-01-11. https://connecttech.com/product/orbitty-carrier-for-nvidia-jetson-tx2-tx1/.

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., et al., 2021. The prisma 2020 statement: an updated guideline for reporting systematic reviews. Systematic reviews 10 (1), 1–11.

Patron, D., Dandekar, K.R., 2014. Planar reconfigurable antenna with integrated switching control circuitry. In: The 8th European Conference on Antennas and Propagation (EuCAP 2014). IEEE, pp. 2737–2740.

Petrillo, A., Pescape, A., Santini, S., 2020. A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks. IEEE transactions on cybernetics 51 (3), 1134–1149.

Prakash, J., Ahmed, C.M., 2017. Can you see me on performance of wireless fingerprinting in a cyber physical system. In: 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE). IEEE, pp. 163–170.

Pu, C., Zerkle, H., Wall, A., Lim, S., Choo, K.-K.R., Ahmed, I., 2022. A lightweight and anonymous authentication and key agreement protocol for wireless body area networks. IEEE Internet of Things Journal.

Production quality, multilayer open virtual switch, Visited on 2023-01-09. http://www.openvswitch.org/.

Protocentral healthypi v4, Visited on 2022-12-05. https://healthypi.protocentral.com/.

pyrcrack, Visited on 2023-04-07. https://github.com/XayOn/pyrcrack.

Qotom mini pc q500g6, Visited on 2023-01-11. https://www.qotom.net/product/28.html.

Renault twizy 80, Visited on 2023-01-13. https://www.renaultgroup.com/en/news-on-air/news/all-there-is-to-know-about-renault-twizy/.

Righetti, F., Vallati, C., Tiloca, M., Anastasi, G., 2022. Vulnerabilities of the 6p protocol for the industrial internet of things: Impact analysis and mitigation. Computer Communications 194, 411–432.

Roth, V., Polak, W., Rieffel, E., Turner, T., 2008. Simple and effective defense against evil twin access points. In: Proceedings of the first ACM conference on Wireless network security, pp. 220–235.

Rfm95: Long range low power transceiver, Visited on 2023-04-20. https://www.hoperf.com/data/upload/portal/20190801/RFM95W-V2.0.pdf.

Risk-nist glossary, https://csrc.nist.gov/glossary/term/risk. Visited on 2023-06-11.

Robot operating system, Visited on 2023-01-11. https://www.ros.org/.

Rtl8821ae - realtek, Visited on 2023-01-23. https://www.realtek.com/en/products/communications-network-ics/item/rtl8821ae.

Ruuvi, Visited on 2023-01-11. https://ruuvi.com/ruuvitag/.

Node-red, Visited on 2023-01-09. https://nodered.org/.

Nodemcu-esp32, Visited on 2023-01-09. https://joy-it.net/en/products/SBC-NodeMCU-ESP32.

Nodemcu v3 esp8266 12e development board ch340, Visited on 2023-01-11. https://circuit.rocks/nodemcu-v3-esp8266-development-board-ch340.html.

Secure water treatment (swat), Visited on 2023-01-09. https://itrust.sutd.edu.sg/testbeds/secure-water-treatment-swat/.

Semtech sx1276: Long range low power transceiver, Visited on 2023-04-20. https://www.semtech.com/products/wireless-rf/lora-connect/sx1276.

Seriot secure and safe internet of things, Visited on 2023-01-17. https://seriot-project.eu/.

sfuzz, Visited on 2023-01-09. https://www.kali.org/tools/sfuzz/.

Simulation of urban mobility, Visited on 2023-04-17. https://sumo.dlr.de/docs/index.html.

Sixsq, Visited on 2023-01-08. https://www.mf2c-project.eu/index.html@p=2026.html.

Sl900a epc gen2 sensor tag, Visited on 2023-01-08. https://ams.com/sl900a-tab/features.

Solidity, Visited on 2023-01-11. https://docs.soliditylang.org/en/v0.8.17/.

Sdr showdown: Hackrf vs. bladerf vs. usrp, Visited on 2023-01-08. https://www.ettus.com/sdr-software/.

Salameh, H.A.B., 2012. Probabilistic spectrum assignment for qos-constrained cognitive radios with parallel transmission capability. In: 2012 IFIP Wireless Days. IEEE, pp. 1–5.

Salameh, H.A.B., 2013. Resource management with probabilistic performance guarantees in opportunistic networks. AEU-International Journal of Electronics and Communications 67 (7), 632–636.

Samaddar, A., Easwaran, A., Tan, R., 2020. A schedule randomization policy to mitigate timing attacks in wirelesshart networks. Real-Time Systems 56 (4), 452–489.

Segata, M., Joerer, S., Bloessl, B., Sommer, C., Dressler, F., Cigno, R.L., 2014. Plexe: A platooning extension for veins. In: 2014 IEEE Vehicular Networking Conference (VNC). IEEE, pp. 53–60.

Seri, B., Livne, A., 2019. Exploiting blueborne in linux-based iot devices. Armis, Palo Alto, California.

Sharma, D.K., Dhurandher, S.K., Kumaram, S., Gupta, K.D., Sharma, P.K., 2022. Mitigation of black hole attacks in 6lowpan rpl-based wireless sensor network for cyber physical systems. Computer Communications 189, 182–192.

Shawky, M.A., Usman, M., Flynn, D., Imran, M.A., Abbasi, Q.H., Ansari, S., Taha, A., 2023. Blockchain-based secret key extraction for efficient and secure authentication in vanets. Journal of Information Security and Applications 74, 103476.

Si, W., Starobinski, D., Laifenfeld, M., 2016. Protocol-compliant dos attacks on can: Demonstration and mitigation. In: 2016 IEEE 84th vehicular technology conference (VTC-Fall). IEEE, pp. 1–7.

Smiliotopoulos, C., Barmpatsalou, K., Kambourakis, G., 2022. Revisiting the detection of lateral movement through sysmon. Applied Sciences 12 (15). doi:10.3390/app12157746.

Smiliotopoulos, C., Kambourakis, G., Barbatsalou, K., 2023. On the detection of lateral movement through supervised machine learning and an open-source tool to create turnkey datasets from sysmon logs. International Journal of Information Security.

Stan, O., Bitton, R., Ezrets, M., Dadon, M., Inokuchi, M., Ohta, Y., Yagyu, T., Elovici, Y., Shabtai, A., 2020. Extending attack graphs to represent cyber-attacks in communication protocols and modern it networks. IEEE Transactions on Dependable and Secure Computing 19 (3), 1936–1954.

Strohmeier, M., Tresoldi, G., Granger, L., Lenders, V., 2022. Building an avionics laboratory for cybersecurity testing. In: Proceedings of the 15th Workshop on Cyber Security Experimentation and Test, pp. 10–18.

Surminski, S., Niesler, C., Brasser, F., Davi, L., Sadeghi, A.-R., 2021. Realswatt: Remote software-based attestation for embedded devices under realtime constraints. In: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, pp. 2890–2905.

Sutrala, A.K., Bagga, P., Das, A.K., Kumar, N., Rodrigues, J.J., Lorenz, P., 2020. On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment. IEEE Transactions on Vehicular Technology 69 (5), 5535–5548.

The stateful software defined networking solution for the internet of things, Visited on 2023-01-13. https://sdnwiselab.github.io/.

Telosb mote platform, Visited on 2023-01-10. https://www.willow.co.uk/TelosB_Datasheet.pdf.

Tinyos, Visited on 2023-01-11. https://github.com/tinyos/tinyos-main.

tshark, Visited on 2023-01-23. https://www.wireshark.org/docs/man-pages/tshark.html.

Thubert, P., 2021. An Architecture for IPv6 over the Time-Slotted Channel Hopping Mode of IEEE 802.15.4 (6TiSCH). RFC 9030. https://www.rfc-editor.org/info/rfc9030. doi:10.17487/RFC9030.

Thubert, P., Richardson, M., 2021. Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves. RFC 9010. https://www.rfc-editor.org/info/rfc9010. doi:10.17487/RFC9010.

Tomić, I., Breza, M.J., Jackson, G., Bhatia, L., McCann, J.A., 2018. Design and evaluation of jamming resilient cyber-physical systems. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp. 687–694.

Tomić, I., Chen, P.-Y., Breza, M.J., McCann, J.A., 2018. Antilizer: run time self-healing security for wireless sensor networks. In: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 107–116.

Ubertooth, Ubertooth. Visited on 2023-01-08. https://github.com/greatscottgadgets/ubertooth.

Usb z-wave 500, Visited on 2023-01-11. https://www.silabs.com/products.

Vadlamani, S., Eksioglu, B., Medal, H., Nandi, A., 2016. Jamming attacks on wireless networks: A taxonomic survey. International Journal of Production Economics 172, 76–94.

Vanhoef, M., Ronen, E., 2020. Dragonblood: Analyzing the dragonfly handshake of wpa3 and eap-pwd. In: 2020 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 517–533.

Veins, Visited on 2023-01-25.https://veins.car2x.org/.

Wang, C., Lu, Z., 2018. Cyber deception: Overview and the road ahead. IEEE Security & Privacy 16 (2), 80–85.

Wang, Q., Vilajosana, X., Watteyne, T., 2018. 6TiSCH Operation Sublayer (6top) Protocol (6P). RFC 8480. https://www.rfc-editor.org/info/rfc8480. doi:10.17487/RFC8480

Wang, W., Chen, Q., Yin, Z., Srivastava, G., Gadekallu, T.R., Alsolami, F., Su, C., 2021. Blockchain and puf-based lightweight authentication protocol for wireless medical sensor networks. IEEE Internet of Things Journal 9 (11), 8883–8891.

Wijnen, B., Hunt, E.J., Anzalone, G.C., Pearce, J.M., 2014. Open-source syringe pump library. PloS one 9 (9), e107216.

Williams, T.J., 1994. The purdue enterprise reference architecture. Computers in industry 24 (2-3), 141–158.

Warp: Wireless open access research platform, Visited on 2023-01-23. https://warpproject.org/trac.

Weka, Visited on 2023-01-11. https://github.com/amten/NeuralNetwork.

Wifibot, Visited on 2023-01-03. https://wifibot.com/.

What is Automatic Identification System (AIS)- Types And Working (FAQs), https://www.marineinsight.com/marine-navigation/automatic-identification-system-ais-integrating-and-identifying-marine-communication-channels/. Visited on 2023-04-07.

Xbee modules, Visited on 2023-01-11. https://www.sparkfun.com/pages/xbee_guide.

Xu, Y., Yang, Y., Li, T., Ju, J., Wang, Q., 2017. Review on cyber vulnerabilities of communication protocols in industrial control systems. In: 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2). IEEE, pp. 1–6.

Yaacoub, J.-P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M., 2020. Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and microsystems 77, 103201.

Yadav, G., Paul, K., 2021. Architecture and security of scada systems: A review. International Journal of Critical Infrastructure Protection 34, 100433.

Yamin, M.M., Katt, B., 2022. Use of cyber attack and defense agents in cyber ranges: A case study. Computers & Security 122, 102892.

Yasaei, R., Hernandez, F., Faruque, M.A.A., 2020. Iot-cad: Context-aware adaptive anomaly detection in iot systems through sensor association. In: Proceedings of the 39th International Conference on Computer-Aided Design, pp. 1–9.

Yasukawa, S., Iwai, H., Sasaoka, H., 2008. A secret key agreement scheme with multi-level quantization and parity check using fluctuation of radio channel property. In: 2008 IEEE International Symposium on Information Theory. IEEE, pp. 732–736.

Yu, S., Park, Y., 2022. A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions. IEEE Internet of Things Journal.

Zheng, D., Jing, C., Guo, R., Gao, S., Wang, L., 2019. A traceable blockchain-based access authentication system with privacy preservation in vanets. IEEE Access 7, 117716–117726.

Zigbee2mqtt, Visited on 2023-01-09. https://www.zigbee2mqtt.io/.

Zou, Y., Zhu, J., Wang, X., Hanzo, L., 2016. A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE 104 (9), 1727–1765.

Zolertia re-mote platform, Visited on 2023-01-13. https://github.com/Zolertia/Resources/wiki/RE-Mote.

Zoom-h6 recorder, Visited on 2023-01-11. https://zoomcorp.com/en/us/handheld-recorders/handheld-recorders/h6-audio-recorder/.

Vyron Kampourakis received his M.Eng. degree in Computer Engineering and Informatics from the Department of Computer Engineering and Informatics, School of Engineering, University of Patras, Greece. He is currently a Ph.D. candidate at the Dept. of Information Security and Communication Technology, Norwegian University of Science and Technology. His research interests lie in the fields of network, critical infrastructure, and cyber-physical systems security.

Vasileios Gkioulos is an Associate Professor in secure systems engineering at the Norwegian University of Science and Technology and the Product Manager for OT security services at Telenor Norway AS. He holds a BSc in Electronics Engineering, a MSc in Wireless Communication Systems, and a PhD in Information Security. He developed and worked on several national and international R&D/I projects, as well as advisory projects and educational/training activities. His main competencies lie within the areas of critical infrastructure security and cyber-physical systems security, focusing particularly on secure systems engineering. Furthermore, he has experience in security awareness, education, and training, focusing primarily on critical infrastructure personnel, but also the society at large.

Sokratis K. Katsikas was born in Athens, Greece, in 1960. He is the Director of the Norwegian Centre for Cybersecurity in Critical Sectors and a Professor at the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Norway. He is also a Professor Emeritus of the Department of Digital Systems, University of Piraeus, Greece. In 2019 he was awarded a Doctorate Honoris Causa from the Department of Production and Management Engineering, Democritus University of Thrace, Greece. In May-June 2023 he served as Minister of Digital Governance in the interim (caretaking) government of the Hellenic Republic. In 2021 he was ranked 7th in the security professionals category of the IFSEC "Global influencers in security and fire" list. He has authored or co-authored more than 300 journal papers, book chapters and conference proceedings papers. He is serving on the editorial board of several scientific journals, he has co-authored/edited 46 books and conference proceedings and has served on/chaired the technical programme committee of more than 870 international scientific conferences. He chairs the Steering Committee of the ESORICS Conference and he is the Editor-in-Chief of the International Journal of Information Security (Springer).