INVITED PAPER

Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things

This paper looks at wireless communication used for CPS and IoT; the authors identify gaps between the vulnerabilities posed by cyber–physical and IoT applications and the security measures provided by wireless standards.

By Andreas Burg, *Member IEEE*, Anupam Chattopadhyay, *Senior Member IEEE*, and Kwok-Yan Lam

ABSTRACT | Wireless sensors and actuators connected by the Internet-of-Things (IoT) are central to the design of advanced cyber–physical systems (CPSs). In such complex, heterogeneous systems, communication links must meet stringent requirements on throughput, latency, and range, while adhering to tight energy budget and providing high levels of security. In this paper, we first summarize wireless communication principles from the perspective of the connectivity needs of IoT and CPS. Based on these principles, we then review the most relevant wireless communication standards before focusing on the key security issues and features of such systems. In particular, the gap between the security features in the communication standards used in CPSs and IoT and their actual vulnerabilities are pointed out with practical examples and recent attacks. We emphasize the need for a more in-depth study of the security issues across all the protocol layers, including both logical layer security and physical layer security.

KEYWORDS | 5G; communication; cyber–physical system (CPS); Internet-of-Things (IoT); machine-type communication (MTC); security; wireless

I. INTRODUCTION

Cyber–physical systems (CPSs)[1] are complex, heterogeneous distributed systems typically consisting of a large number of sensors and actuators, which are connected to a pool of computing nodes. With the fusion of sensors, computing nodes, and actuators, which are connected through various means of communications, CPSs aim to perceive and understand changes in the physical environment, analyze the impacts of such changes to their operation, and make intelligent decisions to respond to the changes by issuing commands to control physical objects in the system, thereby influencing the physical environment in an autonomous way [1]. The connection between actuation and sensing through the physical environment, and between sensors and actuators through one or multiple (distributed) computing or intelligent control node(s) forms a feedback loop which aims at achieving a desired objective or steady state. As such, a CPS either acts with full autonomy or at least provides support for a human-in-the-loop mechanism as part of semi-autonomous control functions. This distributed closed-loop process allows a CPS to remotely influence, manage, automate, and control many man-made (but also natural) small-, medium-, and large-scale systems. Due to the operational nature of CPSs in most industrial control processes, CPSs are also known as operational technology systems (OT systems) which will be discussed in further detail in Section V-B.

[1]The term "cyber–physical systems" was coined by Helen Gill around 2006 at the National Science Foundation of the United States.

Manuscript received May 6, 2017; revised August 31, 2017; accepted November 19, 2017. Date of current version December 20, 2017. *(Andreas Burg and Anupam Chattopadhyay contributed equally to this work.) (Corresponding author: Andreas Burg.)*

A. Burg is with the École Polytechnique Fédérale de Lausanne (EPFL), 1015 Lausanne, Switzerland (e-mail: andreas.burg@epfl.ch).

A. Chattopadhyay and **K.-Y. Lam** are with Nanyang Technological University, Singapore 639798 (e-mail: anupam@ntu.edu.sg; kwokyan.lam@ntu.edu.sg).

Digital Object Identifier: 10.1109/JPROC.2017.2780172

The massive adoption of internet protocol (IP)-enabled devices (i.e., IP sensors and actuators) in CPSs and the increasing wireless connectivity has thereby blurred the boundary between CPSs and the Internet-of-Things (IoT).

The concept of IoT stems from connected smart devices [2], which may or may not be interacting with a physical object. Hence, there are application scenarios even in the classical IoT domain that can already be conveniently classified under either the IoT or the CPS domain, e.g., distributed set of sensor nodes to monitor and control the energy usage of a manufacturing plant. Famous examples for CPSs and IoT systems and corresponding applications [3], include but are not limited to, large-scale environmental systems (e.g., natural resource management), power and energy generation and distribution, transportation infrastructure, home automation, autonomous driving, personal healthcare, logistics, or industrial manufacturing. Due to the diverse variety of applications, CPSs are expected to have a tremendous economic impact [4] through their critical role in OT as well as intelligent control systems. In the following, while discussing these applications, we use the collective term as CPSs to stress the rich interaction with the physical world and the consequent security issues that originate from this interaction.

Besides sensors, actuators, and computation nodes, connectivity is an essential part of CPSs which are typically highly distributed over various scales from local environments such as the human body, all the way to a global scale. While fixed wired networks (e.g., the Ethernet) can cover this task for some applications, many relevant recent applications and CPS components are based on battery operated or even energy-autonomous devices that rely on wireless communications. Interestingly, this trend toward physically fully detached nodes is experienced not only in an increasing number of cases where wires are unacceptable, but also for cases where power supply from the mains and wired network connections would in principle be feasible or even available. Reasons for preferring wireless connectivity are often simply the reduced installation cost or the desire to ease the installation. The increasing availability of a wide range of wireless technologies, optimized for different communication scenarios and requirements (also those specifically relevant to CPSs) has therefore been an important driver for the success and rapid adoption of CPSs in our society and will remain of critical importance for its future evolution.

An abstract view of the CPS/IoT layers is depicted in Fig. 1. The sensing/actuation layer that is enabled by IoT sensors and actuators is supported by a transport/communication layer by interconnecting the nodes to the system application layer with a pool of computation nodes for data analytics and decision making to support a wide varieties of OT applications. The different components in these layers can be connected through different wireless and wired communication protocols, including also the frequently cited "IP-based IoT infrastructure." When such systems also act on the physical world through the integration of connected actuators, they

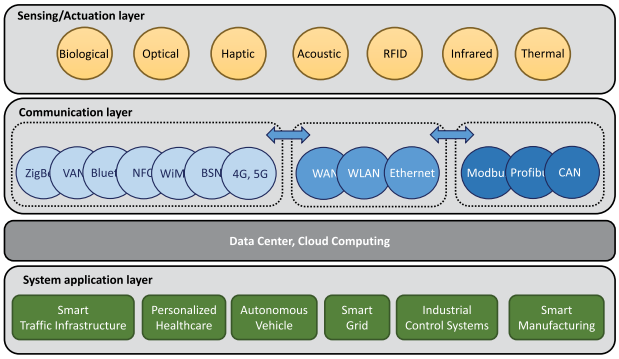

Fig. 1. ***Layered view of CPSs and IoT.***

form a CPS. Hence, the IoT forms the basis for many modern complex CPSs. In essence, CPSs carry their name due to their interaction with the physical environment through sensing and actuation devices. However, while some CPSs may also be known as IoT systems from the protocol perspective, if the sensing and actuation devices are IP-capable, we note that many other local CPSs exist today that are still fully detached from the global IP network (a situation that will change over time). Yet, a CPS may be viewed from the functional perspective and be known as an OT system if it is used for supporting the operation of industrial control processes.

Unfortunately, albeit the obvious advantages of wireless connectivity, eliminating the wires also comes with a number of difficulties and challenges regarding communication performance (e.g., latency, range, and throughput), power consumption of the node, and security. Together with the requirements of a CPS, these concerns dictate the choice of the right wireless communication standard and set the stage for research on the next-generation secure wireless connectivity of CPSs through all layers of the network stack.

In this paper, we draw attention to the myriad of wireless communication systems and standards utilized in CPSs and in IoT. We discuss their technologies and properties from a communications perspective, and also the security practices for CPSs which interface with wireless communication security standards/protocols. In this context, we focus exclusively on the security of CPSs and IoT systems, for which we point inquisitive readers also to [5]–[7]. The study of physical side-channel attacks, which pertains to the implementation security of CPS or IoT devices are left outside the scope of this paper and can be referred to in [8] and [9].

The rest of this paper is organized as follows: In Section II, we summarize the wireless communication and security properties and requirements of CPSs and IoT systems. In Section III, we first turn our attention to the communication aspect and we discuss some fundamental technologies of the different communication layers as a basis for understanding the properties of different standards. In Section IV, we describe the most important communication standards for CPSs and IoT based on the previously discussed fundamentals and together with their most important properties

as a basis for selecting the right standard for a particular system with respect to the initially described requirements. Section V then proceeds to the security issues and measures of CPSs and IoT in general, while Section VI-A is more specifically concerned with the security issues of wireless CPSs and IoT systems. Section VII summarizes the conclusions and identifies challenges for future work.

II. COMMUNICATION AND SECURITY FOR IoT AND CPSs

The communication and security requirements of CPSs and IoT are supported by a diverse wireless and wireline communication infrastructure that provides the connectivity of their various fixed and mobile system components [10]. Depending on the nature of the CPS and its individual nodes, this connectivity often spans multiple layers of the OSI network stack and includes multiple types of networks that are connected through inter-network routers and gateways on various layers [11]. The global internet and the associated TCP/IP and IPv6 protocols typically serve, for example, as a unified global communication backbone with worldwide reach and almost infinite capacity through its supporting infrastructure and its high-speed wireline and optical links. This traditional backbone infrastructure is today complemented with many different classes of wireless links and networks. These collectively provide connectivity to the individual CPS nodes through different standards and technologies, and link them directly among one another and/or with the global backbone as illustrated in Figs. 1 and 2.

A. CPS and IoT Requirements

To understand the properties and tradeoffs between the different communication technologies in the context of CPSs, and to facilitate the selection of the right communication standard and security measures for a particular CPS domain or application, it is useful to define a list of properties and requirements. These requirements are summarized in Table 1 and are explained later.

1) Communications Requirements: The communication requirements impact the physical (PHY) layer, the medium-access control (MAC) layer, and the network (NTW) layer while the application layer is typically not covered by the wireless communication standards. In essence, three main issues need to be considered:

- the properties of the individual radio link of each device to a router or another device;
- the overall capacity and load of the network which has an influence on the individual links;
- the power and complexity of both the device and also the network side.

In the first part of Table 1, we provide a more detailed list of these communication requirements and we link them to the relevant layers of the network stack. These requirements later dictate the choice of the right communication standard.

2) Security Requirements: The security requirements impact different layers depending on the specific security principles, e.g., confidentiality or integrity to be enforced. We note that there is a gap between the information-theoretic security techniques, which are applied at the physical layer and the cryptographic techniques, which are applied at the medium-access control, network, and application layers. The main challenges toward achieving the security requirements are as follows:

- consistent security technique deployed at multiple layers;
- tradeoff between better security and the inherent performance overhead.

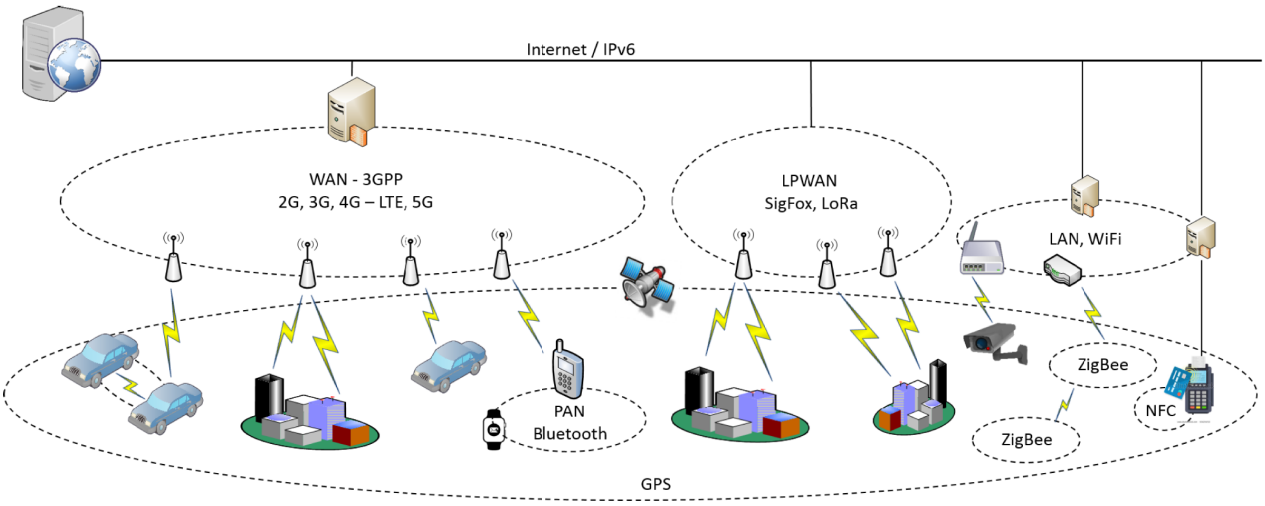

Fig. 2. ***Various types of wireless networks, hierarchically connected.***

Table 1 Properties and Requirements for Wireless Communication in CPSs

Property / Requirement	Layer	Description
Network reach	NTW	Area which can be reached within a network itself, i.e., without crossing network boundaries
Radio link range	PHY	Distance that is covered with a single point-to-point link, in a typical application scenario[2]
Max. coupling loss	PHY	Maximum signal attenuation (including propagation loss and loss due to obstacles) for reliable reception. Derived from transmit power (transmitter), attenuation (environment), and sensitivity, i.e., minimum received signal strength (receiver)
Peak throughput	PHY	Maximum achievable data rate of a link: often dependent on the actual received signal strength in standards that support multiple data rates
Link traffic load	All	Average amount of traffic generated over a longer time frame (e.g., per day)
Traffic type	All	Traffic pattern of a node: streaming (continuous), bursty (short high throughput), occasional (low rate) bursts
Latency	MAC & NTW	Time required to access the network and to deliver data within the network
Number of devices	All	PHY/MAC: Number of devices that can be present in the same radio link coverage area and access a single point of connection (e.g., access point or base station), NTW: number of devices that can be present in the same wireless network
System capacity	PHY	Overall amount of traffic supported for all nodes (often optimistically related to peak data rate)
Physical security	PHY	Operational technology (OT) security to be provided by the PHY, for example by guarding the sensitive infrastructure
Device power	All	Maximum and average power consumption of a device and its target lifetime
Device complexity	All	Cost and complexity (form factor) of a network node
Network complexity	All	Effort/cost to purchase and deploy a the network infrastructure. Complex networks can only be deployed by operators and are generally used and shared by multiple subscribers which has serious implications on the available services and service guarantees, as well as on the security and access management.
Confidentiality	PHY	Information theoretic principles are to be used to minimise the information leakage to an eavesdropper.
	MAC & NTW	Cryptographic primitives are to be used for encoding the message. Further mechanisms to hide other information leakage, e.g., traffic pattern, routing pattern.
Integrity	MAC & NTW	Message should be accompanied with cryptographic hash to detect tampering
Authenticity	MAC & NTW	Participating nodes should be authenticated, e.g., through key exchange certification. Messages can be accompanied with digital signatures.
Availability	All	Reliability of a network, including possible PHY/MAC/NTW layer connectivity issues, but also other (e.g., infrastructure related issues, network jamming, DoS)

In the second part of Table 1, we provide a detailed list of these requirements and link them to the most relevant layer of the network stack.

B. System Examples for Communication and Security Requirements of IoT and CPSs

To better appreciate how these requirements are met in actual working systems, a few CPS/IoT examples are provided with particular focus on their communication and security issues.

[2]Note that this characteristic can vary widely, even for a given technology, depending on the assumptions on the application scenario. For example, the radio link range under the assumption of line-of-sight propagation differs radically from the network reach in an indoor environment.

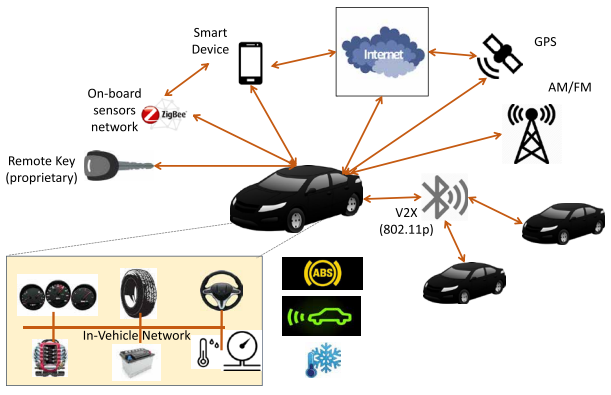

Fig. 3. ***Exemplary networked vehicle.***

1) (Semi)Autonomous Vehicle: A typical networked vehicle is depicted in Fig. 3. The car is connected to the outside world with vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication links. These provide for example traffic-status information or link the autonomous driving or driver assist systems of the cars on the road. Such links need to operate at high speeds, detect and associate quickly with new nodes, and especially the V2V connections require highly reliable operation. In addition, connections to the internet can provide entertainment and feedback status information of the car to the car manufacturer. While the former needs to provide high data rates, the latter may need high availability/coverage to ensure that, for example, emergency calls can be issued at any place. The internals of a car present multiple independent and overlapping CPSs, such as adaptive cruise control, anti-lock braking, and automated temperature control. These CPSs are supported by actuators and sensors, such as tire pressure, temperature, crankshaft position, light, and collision sensors. Today, this CPS control and data communication happens mostly through wired connections since integrity and 100% availability must be ensured. The internal communication protocol follows the controller area network (CAN) bus standard or the more recent FlexRay standard, which are again classified based on power train connection, high-speed connection, and diagnostic purposes. For different use cases, such as for multimedia, standards such as media-oriented systems transport (MOST) are adopted. Depending on the level of autonomy, more functionalities are exposed to

the internal controllers with limited requirement of human intervention. Unfortunately, even the communication through these wireline standards is susceptible to security breaches [12], [13]. Moreover, sensor spoofing poses a serious risk as has been demonstrated in [14]. Nevertheless, in the future, secure, highly-reliable, short-range standards may replace the wired connections.

2) Personal Healthcare: Personal healthcare is another prominent IoT or even CPS application. An example of such a setting is depicted in Fig. 4. Implanted medical devices (IMDs) are mixed with sensors worn on the body for recording vital parameters. The data is sent from the sensors to a smartphone through short distance links for long-term recording or for detecting potential acute health issues. From there, information can be synchronized with doctors or hospitals anywhere in the world over global wireless networks and eventually over the internet [15]. These can advise the patient or even remotely administer drugs, completing the feedback loop. The overall system thereby comprises again various types of links (local and global) which need to support prolonged operation while being battery operated. At the same time, the system is subject to stringent security requirements to protect the privacy of the patient (even including the fact that these devices are present) and avoid intrusion into devices that can directly influence its health (such as drug administration devices). It is often hard for these resource-constrained devices to execute computation-heavy security protocols for device authentication, public-key encryption, and rule out information leakage. As a result, they expose system-level vulnerabilities, which are not tackled by standalone wireless communication protocols. Examples of such attacks are a replay attack or denial of service (DoS) through man-in-the-middle (MITM) [16].

3) Smart Home System: A wide range of connected devices power the modern smart home, which is portrayed in Fig. 5. There are several small-scale CPSs, e.g., heating, ventilation, and air conditioning (HVAC) that can be automatically controlled and need to be linked to a central hub through short-range latency insensitive and reasonably fault-tolerant

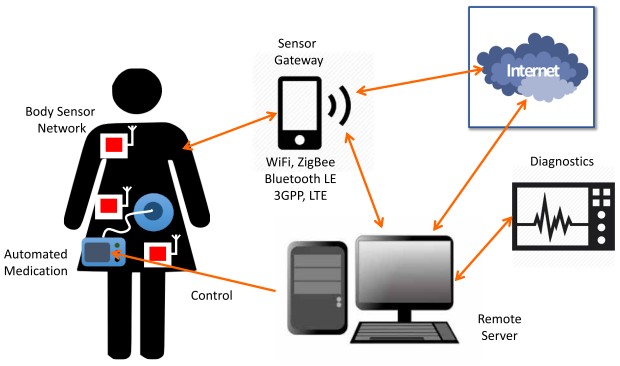

Fig. 4. ***Exemplary implantable personal medical device.***

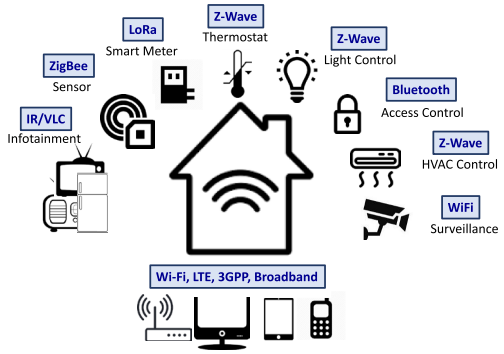

Fig. 5. ***Smart home connectivity.***

wireless protocols. This hub can connect through a wired connection to the internet which links it to the smartphone of the homeowner anywhere in the world. In addition to this remotely accessible home network, autonomous sensors may be distributed throughout the home, for example, for metering which communicate their readings directly to public services or energy suppliers in short daily data telegrams. While such devices have long duty cycles, their number can be very high in a densely populated area and deep indoor coverage must be ensured. From a security perspective, the proximity of the home provides some protection, but smart access control that authenticates and unlocks with a biometric identification needs to adhere to high standards. Overall, many different wireless systems coexist in a home. Naturally, this situation is not only susceptible to radio interference, but also to security breaches through seemingly innocuous, yet connected, devices [17]. Often the control is delegated to a smart device with a complex application stack, which eventually could enable sophisticated attacks [18].

4) Energy Distribution System: Arguably, the system that provides the greatest complexity in terms of variety of communication protocols, number and range of components, and system criticality is the smart grid system. A variety of communication systems on different scales support both the management of the grid itself on a large, country-wide scale, as well as the coordination between individual devices on a small scale that are connected to the grid and that influence its state. Sophisticated cyber attacks on the grid-management scale [19]–[21] demonstrate the practicality, severity, and penetration through the protocol layers, while the vulnerability of emerging attack techniques are also explored [22]. Indeed, the earlier examples of CPSs and IoT systems, e.g., smart home and semiautonomous vehicles only capture a part of the larger smart grid systems. In order to assess the threats associated with a smart grid, a cumulative smart grid model is proposed in [23]. Fig. 6 represents a simplified form of it, which shows the different levels of energy-distribution flow and the corresponding communication standards. This cumulative model also reflects the unbalanced risk

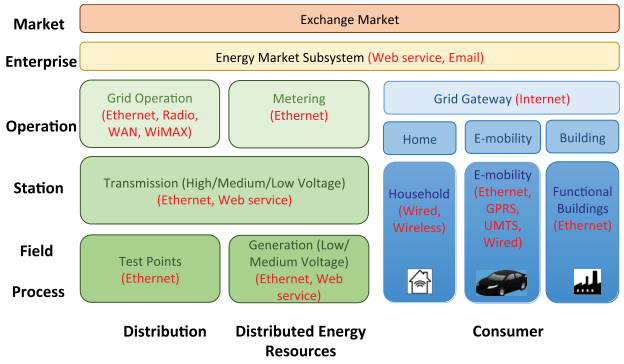

Fig. 6. ***Cumulative smart grid model (adapted from [23]).***

mitigation strategy that is adopted in the current smart grid systems. The components associated with field/process levels, e.g., smart meter and automotive charging station, are the ones that are often least protected and are still connected to the backbone through myriad communication protocols, thereby exposing the entire system to risks.

III. WIRELESS COMMUNICATION TECHNOLOGIES

Most CPSs and IoT systems are designed on the basis of existing communication networks and standards rather than with custom communication links. Hence, ultimately it is necessary to find the best match between the individually defined properties and requirements of a system and the given properties of available standards that are set by a rigid combination of technologies. In that sense, only limited flexibility is available to the designer to freely choose the best combination of technologies, e.g., for different layers of the network stack. Nevertheless, it is instructive to first consider some key technologies and the associated tradeoffs and properties in isolation to better understand the properties and issues of the plethora of existing and new standards under different operating conditions and to ultimately support the right standard selection for a given application. In the following, we therefore briefly discuss different system architectures and technologies which later find applications in some of the most prominent standards discussed in Section IV.

A. Classification of Wireless Networks

Since, in this paper, we are concerned with providing an overview of the communication technology foundations for a wide range of standards for CPS and IoT applications, we also start with a very broad classification of wireless networks. The most widely established classification is derived from the reach or coverage of a network that must not be confused with the radio link range of its associated physical layer, which may be significantly different. While the physical layer radio link range merely characterizes the maximum distance of a single point-to-point link, the reach of a network class refers to the area that can be covered without crossing the network boundary. For example, cellular networks have a global coverage, while the maximum physical layer range from user equipment to a base station is only a few kilometers. We generally distinguish between short-range communication such as personal or home area networks (PANs/HANs), midrange local area networks (LANs), and (low-power) wide area networks (WANs/LPWANs) as well as cellular networks as illustrated in Fig. 2. For each of these network categories, there are a number of different standards, which typically define only the physical layer (PHY) and the data link layer (DLL) of the OSI stack. The DLL thereby comprises the medium-access control (MAC) sublayer, which is particularly important for wireless systems which operate on a shared medium and and the logical link control (LLC) layer, which is often only a thin adaptation layer.

B. Wireless Spectrum for Communication

While all wireless communication is based on electromagnetic waves, it is useful to distinguish between different regions of the radio-frequency (RF) spectrum. The main reasons for this distinction are regulatory requirements, the propagation characteristics, signal attenuation, and the available bandwidth. These properties have a distinct impact on key requirements such as the radio link range and the peak throughput as well as on the system capacity. For example, more bandwidth allows for higher throughput, but the throughput is also determined by the received signal strength which also depends on the propagation characteristics (attenuation) and the maximum transmit power. For example, more bandwidth is available at higher frequencies which allows for higher capacity, but signal attenuation also increases proportional to the frequency which limits the range at a given transmit power and higher frequencies are generally more attenuated by obstacles such as walls or windows. An overview of different radio frequencies and technologies with their associated radio range is given in Fig. 7 where it is also put into perspective to the different network classes.

Most wireless communication systems today operate in the microwave spectrum which extends from few tens of MHz up to 30 GHz, but is used mostly between 400 MHz and 6 GHz. The lower frequency bands are generally used to achieve a longer range, while the higher

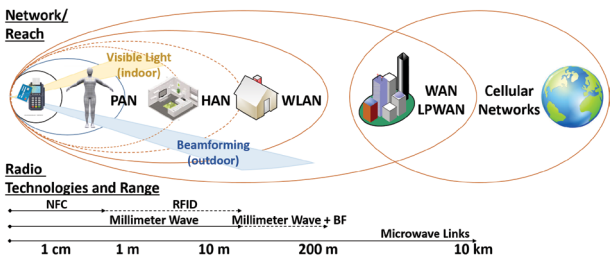

Fig. 7. ***Overview of radio technologies.***

bands are more suitable for high-speed data communication at a shorter range. When choosing a communication frequency, it is mandatory to distinguish between licensed and unlicensed frequency bands, as assigned and regulated by national or regional regulation bodies under the supervision of the International Telecommunications Union (ITU). The majority of the spectrum is covered by licensed bands. Access to transmit in these bands is restricted to the license owner (such as a mobile operator) which can grant access to its subscribers. While licensing bands is expensive, the exclusive access is key to avoid uncontrolled interference between users of the shared medium to provide reliable quality-of-service guarantees. Also, regulations often allow for larger power budgets in licensed bands than in unlicensed bands since interference is better controlled. In addition to the licensed spectrum, some frequency bands can be used freely by anyone. These unlicensed parts of the spectrum are referred to as industrial, scientific, and medical (ISM) bands. Regulations merely define a minimum set of rules to enable coexistence. These rules typically restrict the maximum amount of transmit power to limit the range of each transmitter to enable spatial reuse of the spectrum and a certain amount of duty cycling or a listen-before-talk policy to avoid permanent occupation of the resource.

The severe bandwidth limitations in the microwave spectrum motivate the step to proceed to use higher (millimeter wave) frequencies at or beyond 28 GHz.[3] While these frequencies were initially inaccessible for low-cost (consumer electronics) hardware since corresponding circuits could only be manufactured in exotic and expensive technologies, they can be realized today with commodity CMOS processes [24]. Another recent push toward millimeter waves was the worldwide availability of almost 7 GHz of bandwidth as ISM band around 60 GHz. Compared to microwaves, millimeter waves suffer more from the dependency of the free-space signal attenuation on the frequency. The attenuation difference between the 5- and the 60-GHz ISM band amounts for example to roughly 20 dB. In addition to this loss, millimeter-wave frequencies are strongly attenuated by obstacles and therefore have difficulties penetrating even thin walls or windows. Furthermore, the 60-GHz ISM band lies at the oxygen absorption frequency for electromagnetic waves, which adds an additional attenuation of almost 16 dB/km. While the poor propagation properties of millimeter waves appear at first sight as discouraging, they can also be an advantage, since they simplify the frequency reuse and limit the range of a system, which increases their operational security. An important concept in millimeter-wave systems is the use of beamforming. This technique employs antenna arrays on transmit and/or receive side to focus the energy in a particular direction as illustrated also in Fig. 7. The beamforming gain is thereby proportional to the number of antenna elements.

[3]Strictly speaking the millimeter-wave bands start only at 30 GHz, but the 28-GHz ISM band is generally already considered to be a millimeter-wave band.

Far beyond the RF bands lies the visible (and invisible, typically infrared) light spectrum where terahertz of bandwidths are readily available. As opposed to RF signals, light has a very well-defined field of view and does not penetrate objects or walls, which leads to a small and very well-defined coverage area for each light source. With the recent shift from incandescent light sources (such as light bulbs) to light-emitting diodes, modulation of these light sources at high rates has become possible. This ability allows blending of illumination with communication and other applications such as localization and sensing. However, as opposed to radio waves, light used for illumination is usually noncoherent, hence, only its amplitude can be modulated and can be used to carry information.[4]

C. Modulation Techniques

The modulation determines data rate, spectral efficiency, range, bandwidth, and robustness of a signal and can also have an impact on security. On the device level, the modulation also has a considerable impact on complexity and power consumption. Wideband and spread-spectrum modulation schemes that are more robust and more suitable for high symbol/data rates (baud rate) generally involve digital receiver structures which are more complex than the purely analog receivers for very basic low-rate narrowband modulation. In the following, we describe three rather broad categories of modulation schemes which capture their most important properties without going into the specific details or realizations.

1) Narrowband Modulation: Narrowband modulation schemes are characterized by the fact that the data symbols are directly modulated onto the phase or amplitude of the carrier signal (often referred to as single-carrier modulation). The advantage of this scheme is its simplicity and that transmitters and receivers can be realized at very low cost and with very low power consumption. The bandwidth of the resulting signal is inversely proportional to the symbol rate and the data rate is determined by the number of bits that are encoded with each symbol. A drawback of any narrowband modulation system is its sensitivity to interference since the transmitted signal is located in a single dimension of the time-frequency signal space. Hence, it is difficult to separate any type of interference or a jammer from the desired signal. A further issue results from frequency-selective fading: When the signal propagates along multiple paths of different length, these copies may arrive out of phase at the receiver and cancel out, which results in time- and location-dependent variations of the received signal strength of 20–30 dB. These variations must be accounted for in the link budget to ensure reliable reception. Furthermore, when baud rates are high, narrowband modulation suffers from intersymbol

[4]Modulation of phase as it is used sometimes in fiber–optic systems or pinpoint optical communication links requires lasers, which are more expensive and are ill suited for illumination.

interference (ISI) due to multipath propagation, which deteriorates the quality of the received signals and makes it more difficult/complex to recover the data.

2) Wideband OFDM Modulation: OFDM modulation is a modulation technology that is used to avoid the problems of ISI when signaling at high communication bandwidths. It splits the large required bandwidth for high rates into multiple narrow subbands that individually do not suffer from ISI. This technology finds applications in a variety of modern standards that support high data rates and target a long radio link range. It also provides the option to multiplex multiple users into the same band (OFDMA) which is useful for multiuser systems such as the 3rd Generation Partnership Project (3GPP) fourth-generation long-term evolution (4G-LTE).

3) Spread-Spectrum Modulation: As opposed to narrowband modulation, spread-spectrum modulation distributes or spreads a signal over a bandwidth that is larger than the minimum required bandwidth for a given baud rate. With this measure, the signal is distributed across multiple dimensions in the time-frequency signal space. This distribution renders the transmitted signal more robust against various types of interference since, for example, a narrowband jammer affects only a small part of the spectrum, while the remaining part remains undistorted. There are several possible ways to perform this spreading: for example, direct-sequence spread-spectrum (DSSS) modulation multiplies the original narrowband signal with a wider band PN sequence. This process can then be reversed at the receiver. Another approach is frequency hopping (FH). With this technique, the transmitter changes the carrier frequency in regular intervals and thereby distributes the transmitted data across multiple bands over time. If one of these bands is occupied or corrupted, for example, by channel fading, the signal can still be received after changing to another frequency location. Finally, coded OFDM can also be considered as a special form of spread-spectrum modulation, where the code is responsible for recovering the data across different subbands.

D. Medium-Access Control Mechanisms

In a wireless network, devices communicate through a shared medium. Hence, coordination among devices and between up- and down-link is required to control the access to this medium to avoid collisions and interference, at least between the nodes of a single network and potentially also between nodes of different independent networks that coexist in the same radio coverage area and in the same frequency band. The medium-access control layer is responsible for this task. From a link perspective, it has a significant influence on the latency introduced by a wireless connection and on potential minimum throughput guarantees which are important for certain traffic types such as streaming applications. From a hardware perspective, it also has important implications on the power consumption due to MAC layer communication overhead, especially in systems with low link traffic load, short data bursts, and long duty cycles.

While a variety of MAC layer protocols exist, we only consider three general strategies. We also limit our discussion to time-division duplexing (TDD) rather than frequency-division duplexing (FDD) for multiplexing the uplink and downlink communication between a node and a central access point or another node. TDD is more common than FDD in most low-power wireless systems since it allows for a more flexible resource allocation between the two directions and avoids the cost/power overhead for concurrently operating on two different carrier frequencies. In addition to the medium access, the MAC layer is also responsible for ensuring reliable data transmission. To this end, most MAC protocols support an automatic repeat request (ARQ) protocol which checks the integrity of the data by means of a checksum (CRC) and acknowledges the successful reception of a data packet. If no acknowledgment is received, the transmitter retransmits the packet.

1) Contention-Based Access: Contention-based channel access avoids the need or at least reduces the complexity of a central control entity or coordinator that orchestrates the access among the nodes in the network, including its own access and the sometimes required common time base. The distributed access provides maximum flexibility and robustness against single point of first failure when the transmission of a central coordinator is impaired. The most basic contention-based access scheme is the ALOHA protocol, which blindly accesses the channel whenever data is available. If data is received successfully, the receiver sends an acknowledgment. If no acknowledgment is received within a given time window, the transmitter resends the data. In a lightly loaded network, the ability to access the channel at almost any time can provide short latencies since a node that needs to transmit data will not have to wait for an allocated time slot. Unfortunately, in a more heavily loaded network, blindly transmitting data at any time increases the risk of collisions that corrupt the transmitted data. In this case, overall access latency increases rapidly and network capacity is degraded. As a result, such networks can generally never achieve their full system capacity. We also note that in any case the receiver needs to remain alert at all times.

Carrier-sense multiple-access (CSMA) schemes aim at avoiding frequent collisions. To this end, a node that wants to access the channel first checks if no other transmission is ongoing by listening to the channel. If the channel is free, access is granted. This carrier sense procedure is often accompanied by a collision avoidance protocol (CSMA/CA) that keeps track of other ongoing transmissions and to avoid unnecessary access attempts. While these measures greatly reduce the number of collisions, they also come with a non-negligible overhead, since CSMA requires a sensing (receive)

period prior to each transmission and collision avoidance is usually associated with the need to also follow (receive) other transmissions which prevents the radio interface of a node from sleeping. Similar to the ALOHA protocol, CSMA provides a short, but never guaranteed access latency for light network loads. As the network approaches its capacity, this latency and the latency uncertainty increase.

2) Coordinated (Beacon Enabled) Access: An important issue of random-access-based communication is the uncertainty in the access latency and the deterioration of the system capacity due to collisions in a heavily loaded network. To alleviate this problem, many systems introduce a coordinated access scheme. The idea behind this scheme is to synchronize all nodes in the network (e.g., by means of a regular beacon that is broadcast by a central node). A central controller assigns timeslots with dedicated uplink transmission opportunities for each node. This coordination guarantees a minimum capacity for each node and a minimum guaranteed channel access latency. A period for contention-free access is then often followed by a random access period for nodes which have no dedicated time slot (yet) or for additional data transmissions. Devices only wake up in regular intervals to listen to the controller which enables them to sleep most of the time, while still being able to receive and react on spontaneous downlink messages.

E. Network Topologies

A network of wireless nodes can be organized in different topologies in which the radio range of different nodes may even overlap. On one hand, more basic topologies are typically more efficient in terms of their system capacity and in terms of latency guarantees. On the other hand, more complex topologies offer more flexibility and greater range at the cost of more complex coordination and routing protocols, more overhead on the network layer, and more frequent collisions which degrade capacity and latency. An overview of the most prominent network topologies is shown in Fig. 8.

1) Star Networks: The most simple network configuration is a start topology in which all nodes only communicate directly with a central access point or base station. All traffic is routed through this node and all nodes need to be in the radio reach of this central point.

2) Tree Networks: To increase the range of a network, a tree (or multihop) configuration can be established in which nodes communicate with a designated neighboring router or node which forwards the data traffic. The advantage of this topology is that it extends the range since each node/router only needs to be in the radio reach of its neighbor, while the routing itself is straightforward.

3) Mesh Networks: A drawback of a star topology is that all traffic is routed through a single point. This routing increases the risk of a network failure, increases latency, and incurs a potentially large overhead which degrades network capacity. Allowing nodes and routers to connect to multiple other routers creates a more flexible and more robust network with shorter latency and more system capacity, but also increases routing complexity.

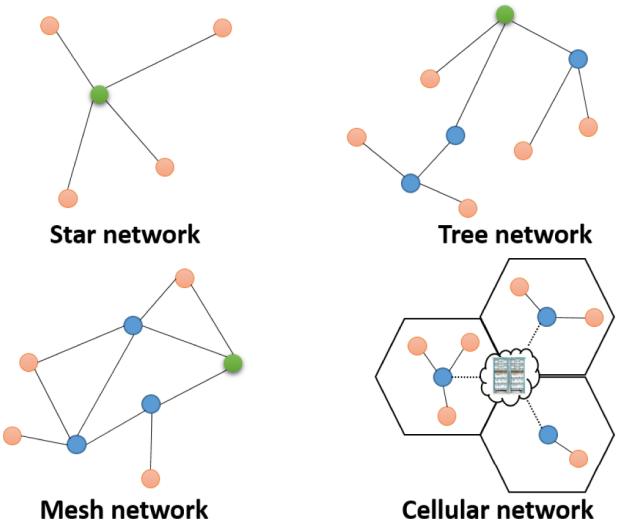

Fig. 8. ***Overview of main network topologies.***

4) Cellular Networks: Cellular networks are a specific type of star topology in which multiple stars are arranged to avoid overlap of the radio reach of their central points, which are referred to as base stations in the context of 3GPP mobile cellular networks. The routing between the different base stations is then handled through a separate (often wired) core network. The advantage of this arrangement is that the coexistence of multiple nonoverlapping cells allows for frequency reuse without collisions which allows for a large network capacity at the cost of a complex/costly managed infrastructure.

IV. WIRELESS COMMUNICATION STANDARDS FOR CPSs AND IoT

The variety of communication scenarios and requirements of CPSs and the IoT as well as all the different corresponding communication technology options cannot be covered by a single standard. Instead, a variety of standards exists which combine different technologies on different layers of the stack to cover various regions of the communication subsystem design space. A high-level overview of this design space which only considers radio range and throughput for some of the most prominent standards and network classes is provided in Fig. 9. Table 2 links the most frequently used and most relevant such standards to the principals discussed in the previous section and to the application needs and communication scenarios they cover.

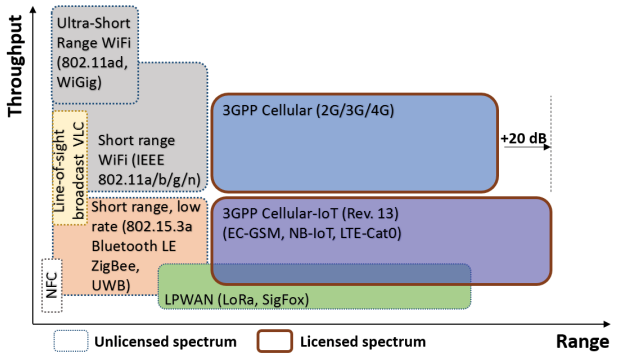

Fig. 9. ***Overview of standards for IoT and CPSs.***

In the following, we provide more details on these standards and relate them to the key communication technologies as outlined in Section III.

A. UHF RFID and Near-Field Communication (NFC)

UHF RFID and NFC systems are designed for applications that require a very large number of low-cost "tags" to be read by a potentially more costly and power-hungry "reader," for example, for tracking goods in supply chain management systems [25] or for payment systems. The technology can establish a unidirectional link or a bidirectional link between the reader and one or multiple simple tags. This is achieved with a communication scheme, where only the reader is actually emitting an RF signal for both sending and receiving. When data is transmitted from the reader to the tag (downlink), the emitted signal is simply modulated accordingly. To create an uplink, the tag modulates the impedance of its antenna, which can be detected by the reader that emits the radio signal. The advantage of this method is a tag which can not only receive, but also send data without complex RF circuitry and with very low power consumption. The power for the processing and for the load modulation at the tag can either be extracted from the received radio signal (passive tags) or from a local battery (active tags). However, since the energy in the field to supply the tag decays rapidly with the distance, the range of passive tags is usually limited to 10 m (often less), while communication with active tags is only limited by the sensitivity and power of the reader and can reach up to 100 m.

In addition to the distinction between active and passive tags, it is also convenient to distinguish between RFID systems that operate in different frequency ranges. The most common protocol for these frequencies are described in the different versions of the ISO18000 standard [26].

1) Near-Field Communication (NFC) [27]: In the low-frequency range with carrier frequencies of 125 kHz and 13.56 MHz (ISO18000 Part3), the tag is in the near field of the reader. In this case, the two sides interact through electromagnetic coupling and the tag can directly modulate the impedance perceived by the reader. This direct coupling creates a strong point-to-point link which provides resilience against interference. However, data rates are low (up to 424 kb/s for ISO18000 Part3) and the the range is limited to below 1 m. On the positive side, this short range also helps to create a physical operational security. Hence, NFC

Table 2 Properties of Wireless Standards

Standard	Frequency	Modulation	Medium Access	Network	Data rate	Range	Suitable for
NFC	13.56 MHz	Narrow Band	-	P2P	423.75 kbit/s	0.1–1 m	Secure communication over very short range with batteryless tags
UHF RFID	0.9 GHz	Narrow Band	Contention	Star	40–640 kbit/s	<100 m	Identification and communication with ultra-low cost (batteryless) tags
ZigBee	0.9/2.4 GHz	Spread Spectrum	Contention/ Coordinated	Star/Tree/ Mesh	20–250 kbit/s	10–20 m	Large number of low power nodes with low data rates
Z-Wave	0.9 GHz	Narrow Band	Contention	Mesh	9.6–40 kbit/s	30–40 m	Medium number of nodes with good indoor coverage
EnOcean	0.9 GHz	Narrow Band	Contention	Tree	125 kbit/s	20 m	Medium number of energy-autonomous nodes
Bluetooth (LE)	2.4 GHz	Freq. Hopping	Coordinated	Star	0.7 MBit/s (0.27 MBit/s)	1–100 m	Streaming applications with real-time guarantees
802.11a/g/n	2.4/5.8 GHz	OFDM	CSMA	Star	11–600 Mbit/s	30 m	High speed local connectivity
802.11ad	60 GHz	OFDM	Coordinated	Star	6 Gbit/s	5–10 m	Gigabit line-of-sight connectivity
3GPP LTE Cat-0	0.9–3.6 GHz	OFDM	Contention/ Coordinated	Cellular	20 MBit/s	300 m	Worldwide high-speed connectivity with medium coverage
3GPP 2G	0.4–1.9 GHz	Narrow Band	Contention/ Coordinated	Cellular	64–384 kbit/s	15 km	Worldwide connectivity with very good coverage and medium data rate
NB-IoT	0.4–1.9 GHz	OFDM	Contention/ Coordinated	Cellular	250 kbit/s	15 km	Worldwide coverage with low duty cycle and low data rate
LoRa	0.9 GHz	Spread Spectrum	Contention	Star	0.25–11 kbit/s	15 km	Regional coverage with low duty cycle and low data rate for long battery lifetime
SigFox	0.9 GHz	Narrow Band	Contention	Star	100 bit/s	30 km	Regional coverage with very low duty cycle and very low data rate for very long battery lifetime

is a useful means to support, for example, the secure establishment of trust between a new device and a network trust server without human intervention through location-based authentication.

2) UHF RFID: UHF RFID systems employ frequencies in the 433-MHz band and in the microwave ISM bands of 860–960 MHz and 2.45 GHz. These systems are designed to operate in the far field of the reader (i.e., at distances that are greater than one wavelength). In this case, there is no direct coupling between the reader and the tag and the uplink is realized by backscattering. The radio link range of these systems starts with 1–2 m for high-frequency bands and extends up to 20–100 m for the lower frequency bands. The most frequently used band is the 860/960-MHz ISM band with the ISO18000 Part 6 standard which is also known as the EPCGlobal Gen 2 specification, defining data rates of 26–128 kb/s in the downlink and 40–640 kb/s in the uplink. Since in such UHF RFID systems multiple tags can be present within the range of a single reader, the corresponding standards use a slotted ALOHA protocol to enable communication with multiple tags in a star network topology.

B. ZigBee/Z-Wave/EnOcean

ZigBee [28], Z-Wave [29], and EnOcean [30] are standards for wireless networks with low peak throughput requirements and low complexity nodes [31]. All three target similar application areas such as home networks or remote monitoring and control.

1) ZigBee: ZigBee [28] has been designed for wireless sensor networks [32], [33] with a traffic type that is characterized by short irregular bursts with long sleep periods that allow the leaf nodes of the network to operate for multiple months or years on a single battery charge. A ZigBee network can also accommodate a very large number of nodes (up to 65 000) which can be arranged in a star, tree, or mesh topology with multiple (redundant) routers which extends the range of a network well beyond the range of a single point-to-point link. Furthermore, in a mesh topology, connectivity can be restored even when individual routers fail. To support these complex topologies, ZigBee adds a network layer (and an application layer) to the PHY and MAC layer of either the IEEE 802.15.4 [34] standard or the IEEE 802.15.4a standard. Devices are categorized either as reduced function devices which form the periphery of the network or full-function devices which can also act as routers and as central network coordinator. The former are significantly less complex than the latter and require less memory [35] which extends their battery lifetime and reduces cost. The IEEE 802.15.4 PHY layer [34] used in ZigBee systems operates in the 868-MHz, 915-MHz, or 2.4-GHz ISM bands and supports data rates from 20–250-kb/s with DSSS spread-spectrum modulation which provides robustness against interference (in particular when operating in the crowded 2.4-GHz band), some robustness against fading, and a tradeoff between data rate and radio range. With a transmit power of –25 dBm to 0 dBm and at the lowest data rate, the radio range covers a distance of up to 10–20 m. For higher data rates, the range of a single point-to-point link is reduced and multiple routing hops (e.g., in a tree or mesh network configuration) are required to cover a longer distance. Since the bandwidth is lower than the width of the ISM bands, multiple ZigBee networks can coexist without interference at different frequencies. The MAC layer [34] is based on a CSMA protocol and relies either on contention-based random access or on a coordinated (beacon enabled) access scheme [36]. The former is combined with a polling scheme, where energy sensitive nodes (reduced function devices) on the periphery of the network sleep most of the time without the need to always listen to the communication medium to capture packets that are addressed to them. These nodes only wake up when they have data to transmit or in periodic intervals to query less energy sensitive near-by routers for any pending downlink traffic. In such a network setup, the individual routers must buffer any downlink traffic and listen to the network continuously until the data can be delivered on request. Their complexity and power consumption is therefore higher for the benefit of their associated child nodes. A disadvantage of such a polling-based access scheme is the potentially large downlink access latency as well as a deterioration of the overall downlink system capacity. Hence, this strategy is mainly employed in systems where uplink traffic is dominant. The alternative IEEE 802.15.3e MAC layer [37] alleviates this problem by introducing a time schedule to meet latency, throughput, and reliability requirements in particular for industrial applications.

2) Z-Wave: Z-Wave [29] is mainly targeted toward home automation, but has still a similar application profile as the above-described ZigBee standard, however with lower data rates of 9–40 kb/s, which leads to a slightly larger indoor radio range of 30–40 m. As opposed to ZigBee, Z-Wave is a proprietary system. It relies on a physical layer with low-complexity frequency shift keying (FSK) narrowband modulation in the 868- and 915-MHz ISM bands. Medium-access control is based on CSMA. The network layer supports fewer devices compared to ZigBee and does not rely on polling for the downlink, which results in a shorter downlink latency, but increases power consumption of the nodes on the periphery which need to stay alert to not miss any downlink traffic. In turn, network slaves cannot initiate a transmission and need to be polled, which leads to less congestion on the uplink, but also to longer uplink latency.

3) EnOcean: Similar to Z-Wave, EnOcean [30] is also a proprietary standard, which primarily targets home automation. While also operating in the ISM bands around 900 MHz, the system supports a throughput of 125 kb/s which lies in between that of Z-Wave and ZigBee with an indoor range of roughly 20 m. A specialty of this standard is

that the available devices are geared toward energy autonomy. The necessary energy efficiency is partially achieved with a very basic medium-access control mechanism based on the ALOHA protocol without acknowledgement, at the expense of reliability. Since this scheme results in a high probability of a packet loss, telegrams are kept short and are repeated several times [38] to reduce the loss rate.

C. Bluetooth and Bluetooth Low Energy

As opposed to the ZigBee, Z-Wave, and EnOcean standards, which are optimized for irregular, short traffic bursts, Bluetooth [39] (also known as IEEE 802.15.1 [39]) has been designed mostly with real-time streaming applications in mind. A Bluetooth network is organized in a star topology in which slave nodes communicate only with a central master. This master sends a beacon and assigns time slots to the nodes in the network, which facilitates real-time operation and provides bandwidth guarantees. To reduce power consumption of the slaves, they can enter different low-power sleep modes, which differ in the time that is required to rejoin the network after wakeup. Compared to ZigBee, the time for rejoining is generally long (100 ms), which renders short and frequent duty cycles inefficient in terms of energy consumption. The Bluetooth physical layer offers an application throughput up to 0.7 Mb/s [2.1 Mb/s with enhanced data rate (EDR)]. Different power classes reach from 1 m to 100 m for industrial applications with a typical range of 10 m for most devices. The system operates in the 2.4-GHz ISM band and is therefore colocated with many other wireless systems, most prominently with WiFi WLAN. To avoid interference with other standards and with other Bluetooth networks, the physical layer is based on frequency-hopping spread-spectrum technology. Coexistence of multiple Bluetooth networks in the same area is achieved by using different hopping patterns.

1) Bluetooth LE: The Bluetooth LE [40] standard has been developed to close the energy-efficiency gap between ZigBee and Bluetooth for nonstreaming sensor-node-type applications. Besides modifications in the baud rate and the number of channels used for frequency hopping as well as a reduction of the application throughput to 270 kb/s, Bluetooth LE reduces the wakeup time from its sleep mode from 100 ms to only 3 ms. This improvement renders even short sleep periods more energy efficient and has a dramatic impact on the overall battery lifetime.

2) WISAN: The Bluetooth physical layer IEEE 802.15.1 is also used as the basis for the wireless interface for sensors and actuators network (WISAN) developed by ABB. The purpose of this system is to provide reliable, high-speed, and low-latency connectivity for up to 120 devices in an industrial setting. To this end, it adds frequency-division duplexing to the physical layer, which enables better coordination of the devices and simultaneous uplink and downlink transmission. Devices have fixed allocated time slots which allows for latency guarantees and low latency channel access.

D. IPv6 Over Personal Area Networks (6LoWPANs)

An important drawback of both ZigBee and Bluetooth in the context of CPSs is that these networks can only connect to an IP backbone through the application layer since their network layer is incompatible with IPv4 and IPv6. However, especially IPv6 is widely considered to be the future baseline protocol for the IoT which should allow even the smallest devices to participate directly in the global network. To enable participation of small-scale sensing applications in this global network, the Internet Engineering Task Force (IETF) defines 6LoWPAN as an encapsulation layer to split large IPv6 packets into smaller packets which are compatible with the IEEE 802.15.4 standard that is also used in ZigBee and the RPL standard defines a suitable multihop routing protocol. With these extensions, convergence is achieved between isolated sensor networks and CPSs and the global IoT. An extensive survey on this topic and the associated standards which considers the entire stack for industrial applications can be found in [41].

E. WiFi: IEEE 802.11a/b/g/n

Wireless local area networks based on the IEEE 802.11 [42] series of standards (referred to as WiFi) are omnipresent in home, in office, and in industrial environments, as well as in public areas. This often already available and easy to install infrastructure, as well as the natural integration with the internet render such WiFi systems a frequent basis for IoT connectivity, despite the relatively high modem cost and power consumption. Most basic WiFi networks are built as a star network around a central access point (AP) surrounded by mobile stations which forms a basic service set (BSS). In this configuration, all nodes communicate only with and through the AP. An extension of this BSS is the extended service set (ESS) in which nodes can wonder between multiple APs. Finally WiFi also allows for a direct connection between two nodes, which is referred to as independent BSS. The WiFi standard series supports multiple PHY layers which operate mostly in the 2.4-GHz and the 5.8-GHz ISM bands. The 5.8-GHz band is often more available but implies a slightly reduced radio reach. Different amendments (a/b/g/n) represent the various steps in the standard evolution which are mostly geared toward increasing throughput, driven by the requirements of home and office networking. Throughout this evolution, bandwidth occupancy has evolved from originally 20 MHz to 40 MHz and more sophisticated modulation schemes have been added to support data rates between 11 Mb/s for IEEE 802.11b to up to 600 MHz for IEEE 802.11n. With a 20 dBm output power, the systems achieve an outdoor

range of 100–200 m or can cover one to two floors of a typical home (50 m) with decreasing data rates. The MAC layer of WiFi is based on the CSMA protocol with collision avoidance. To reduce power consumption, later versions of the standard also define various sleep modes which allow terminals to register their absence with the AP to avoid missing packets during sleep periods. Despite these sleep modes, an important drawback of WiFi systems is their significant modem complexity and high power consumption due to the complex MAC and PHY layers. Commercial chipsets consume 0.5–1 W [35], [43] in active mode and up to 50–100 mW in sleep mode [35].

In addition to the various baseline versions of the PHY and MAC layer in the amendments a/b/g/n, the standard includes various other recent amendments that are specifically geared toward CPSs and IoT: For example, IEEE 802.11s extends the IEEE 802.11 MAC layer with multihop capabilities to enable more complex networks with a greater range. The IEEE 802.11ah amendment specifically targets large scale low-power WiFi sensor networks with medium throughput as a competitor to Bluetooth and even ZigBee. To this end, this amendment introduces a new PHY layer with a larger radio range (1 km) in the sub-gigahertz regime, a protocol that supports multihop routing, and a MAC protocol that minimizes contention and shortens the transition between active and sleep periods to maximize sleep-mode power savings.

F. WiFi: IEEE 802.11ad

The IEEE 802.11ad [44] standard is an extension of the set of WiFi standards to millimeter-wave frequencies and to the 60-GHz ISM band. Since in this frequency range, considerable bandwidth is available, the standard allocates 1.7 GHz per channel, which allows for a peak throughput of up to 6 G b/s. The limited range due to the high frequencies can be partially compensated for by using beamforming, however, walls and other obstacles mainly limit communication to a single room for indoor scenarios. This limitation, however, also facilitates frequency reuse and reduces signal leakage to a potential eavesdropper which provides a certain amount of physical security and privacy. An important disadvantage, which limits the use of the technology to rather specific IoT and CPS applications that absolutely require high data rates, is the high power consumption of corresponding transceivers, even when compared to microwave-based WiFi systems [45].

G. Visible Light Communication and Localization

The ability to modulate light used for illumination provides a number of new opportunities to seamlessly incorporate sensing and communications [46], [47] into the environment for CPSs. Two specific CPS-related examples for such systems in consumer electronics and transportation can be found in [48] and [49].

1) IEEE 802.15.7: A PHY layer for visible light for communication [50] is described in the IEEE 802.15.7 standard which defines different modulation schemes that are compatible with illumination infrastructure and support data rates from 11 kb/s to 96 Mb/s. The main application for this standard are broadcast systems since the directivity and the inherent asymmetry of the setup render bidirectional communication difficult. Nevertheless, some studies have been conducted on uplink communication based on visible light [51] that indicate that this is feasible. An important property of visible light communication is the small and very well-defined coverage area for each light source and the fact that a large number of sources is required to cover, for example, an entire room. This well-defined field of view severely limits the range, but also allows for extensive spectrum reuse, which leads to very large system capacity through coexistence of many different links. Furthermore, the well-defined illumination cone can serve as a physical security feature for a link, since its range can not only be controlled, but can also be checked.

2) Localization: In addition to communication, modulated (directional) light sources can also be used for localization [52]. By imprinting, for example, unique signatures onto the various light sources that cover different regions of an area, a receiver can determine its position. In addition to this 2-D localization, high-frequency modulation even allows for rather accurate distance measurements.

H. IEEE 802.11p

An important domain for CPSs are intelligent transportation systems (ITSs) which essentially involve two different types of connectivity: On the one hand, intravehicle connectivity solutions provide the wireless communication infrastructure for avoiding expensive cabling in today's vehicles which are themselves already complex CPSs. On the other hand, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication connects the vehicle with the outside world and integrates it into a larger global CPS through wireless links with very specific requirements. A detailed discussion of the different communication requirements in ITSs can be found in [53]. While the intravehicle communication can build on established standards for short-range communication, a new dedicated standard is clearly required for the specific requirements of V2V and V2I connectivity.

The corresponding IEEE 802.11p standard [54] for V2V and V2I communication is derived from IEEE 802.11a and can operate in a dedicated band from 5.85 GHz to 5.925 GHz. The PHY layer occupies a reduced bandwidth of 10 MHz to accommodate channels with longer delay spread than the indoor environments for which 802.11a was designed. The data rates range from 3 to 27 Mb/s with a range of up to 1000 m. The MAC layer is also modified, to facilitate rapid association with roadside access points from a moving vehicle, which only remains within range for a short time.

I. 2G/3G/4G Cellular Systems for IoT and CPSs

The extensive proliferation of cellular wireless systems based on the 3GPP standards and the corresponding global network provide an excellent basis for nonstationary connectivity and greatly facilitate the global *ad hoc* deployment of nodes based on a managed and globally available infrastructure. This third-party infrastructure and the operation in licensed bands ensures excellent and guaranteed quality of service. Hence, these networks have been used extensively in a variety of applications to provide connectivity to the internet. However, the data modes of second-generation (2G), third-generation (3G), and fourth-generation (4G) mobile communication systems have been designed primarily for high-speed data traffic. Nevertheless, all three generations of cellular systems offer opportunities for machine-type communication (MTC) and are already in use for a variety of IoT and CPS applications. An illustration of key properties of the various current and emerging 3GPP modes for IoT and CPS is provided in Fig. 10.

The last three generations of the 3GPP cellular network standards thereby offer various tradeoffs between throughput performance, modem complexity, and availability/coverage: The legacy 2G and 2.5G standards have the lowest modem complexity and power consumption and the network is available almost worldwide with not only a good population overage, but also with a very high area coverage, even in rural areas. The limitations lie in the low data rates which span a range of 64 kb/s for GPRS to 384 kb/s with EGPRS to a maximum of 1 Mb/s with the latest EGPRS2A system (cf., Fig. 10). A 3G modem achieves between 384 kb/s and 24.8 Mb/s, however with a modem complexity and power consumption, that is significantly higher. Moreover, while 3G coverage is almost as good as 2G coverage in densely populated areas, it still lacks behind in regions with low population density. Finally, the 4G-LTE system supports data rates up to 150 Mb/s on the downlink and 50 Mb/s on the uplink, however, at the expense of a costly and power-hungry Cat-4 modem. Since such high data rates are usually not required for many CPS and IoT applications, the 4G-LTE standard defines reduced-complexity categories such as LTE Cat-0 (Rel.-12), which still achieves up to 10 Mb/s on the downlink (cf., Fig. 10) and 5 Mb/s on the uplink with a significantly reduced complexity, which, however, still lies above that of a 2G modem. Furthermore, as for 3G systems, 4G coverage is incomplete, which requires the presence of a 3G or even a 2G fallback mode. In addition to that, besides holes in the network coverage, the support of high data rates limits the sensitivity of 3G and 4G systems. This sensitivity limitation can even pose a problem in 2G systems and in a generally well-covered area, for example, when a sensor is placed in the basement of a building which is very typical for smart-meter applications.

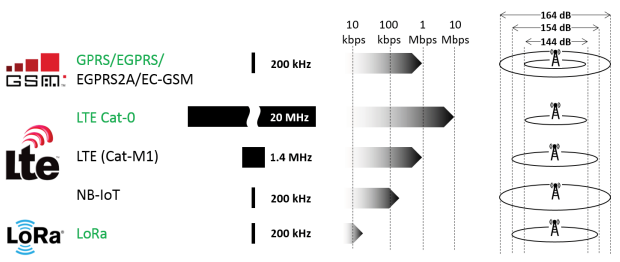

Fig. 10. ***Overview of 3GPP standards and LoRa LPWAN for IoT and CPSs.***

J. 3GPP Cellular IoT: EC-GSM and NB-IoT

To address some of the aforementioned issues that arise when operating low-power IoT sensor nodes with low or even very low peak throughput requirements over the cellular network, the recent releases of the 3GPP standards series introduces a number of specific features for MTC. These modes aim at improving the link budget and sensitivity and at reducing modem complexity and power consumption. While in the following we only summarize the most prominent new features, we refer to [55] for a more detailed discussion on the evolution of 3GPP toward supporting CPS and IoT communication and the associated large number of devices in the network.

A first additional feature introduced in Release-13 of the standard is an evolution of LTE toward IoT. The new LTE Cat-M1 standard targets modems that only require a data rate of up to 1 Mb/s, but require less than 50% of the complexity of a conventional LTE Cat-0 modem. To achieve better coverage and to support devices with a weak link, the new standard also provides an almost 10-dB better link margin (cf., Fig. 10).

A second, more radical enhancement is the addition of the new NB-IoT standard. This standard targets data rates of 250 kb/s with a sensitivity that is 20 dB better than that of an LTE Cat-0 (cf., Fig. 10) modem and a modem complexity that is almost cut in half. An important property of the new mode is that it occupies only 200 kHz of bandwidth. This reduced bandwidth not only contributes to reducing the modem complexity, but also allows to operate the system in the guardband of a regular 4G-LTE system or in a refarmed band that was originally used for 2G voice or data communication.

A third new mode is an extension of the 2G GPRS/EDGE system. The extended coverage GSM (EC-GSM) mode is based on the legacy GSM/GPRS system, but provides a 20 dB sensitivity improvement with data rates below 6 kb/s (cf., Fig. 10). The sensitivity enhancements are achieved with simple repetition coding, which is easy to add and allows for a straightforward upgrade of the legacy infrastructure. The fact that the system is based on the legacy 2G standard enables very low complexity modems [56] with multimode operation to offer a wide range of low-to-high data rates depending on the channel conditions.

The last common additional feature which affects most existing and above-described new 3GPP standards is the introduction of the extended discontinuous reception (eDRX) mode. This mode allows the user equipment to remain registered without being reachable to enter long sleep periods of up to 40 minutes. This power save mode is crucial to achieve battery liefetime of multiple years. It is claimed that with this mode, an LTE Cat-M1 modem that performs one transmission per day and wakes up every 10 minutes to receive commands can operate almost five years on a single AA battery.

K. Low-Power Wide Area Networks (LPWANs)

In parallel to the recent and ongoing extension of cellular networks to better support CPS and IoT communication, a new class of communication standards and networks has recently emerged. The two most prominent proprietary standards of this class are LoRa (cf., Fig. 10) and SigFox. The objective of both systems is to support a massive number of ultra-low-rate and ultra-low-power wireless sensors and devices. These low-power wide area networks are similar to cellular networks, but operate in the unlicensed ISM bands, which simplifies and opens the deployment of the necessary infrastructure to anyone. The LPWAN structure resembles more a mesh network than a cellular network since signals can be picked up by multiple base stations (gateways), which improves reliability, especially in an unmanaged network. Further, as opposed to the original 3GPP standards and even to the 3GPP amendments for IoT, LPWAN systems have a significantly lighter PHY and MAC layer and target applications that require ultra-low data rates in bursts with a low link traffic load (very low duty cycle), but with a potentially large number of devices. This type of traffic is typically found, for example, in metering applications. An important focus of the PHY layer of these systems is to achieve a high sensitivity to maximize the radio reach. This strategy guarantees a good coverage even in occluded areas and reduces the number of gateways and hence the cost of the required infrastructure.

V. Security Requirements of CPS and IoT

Standard security policies are guided by confidentiality, integrity, and availability, also known as the CIA triad. These policies are reinforced with application-specific security requirements and are eventually implemented with cryptographic primitives and security protocols. Prominent cryptographic primitives include: symmetric-key cryptography, one-way functions, and public-key or asymmetric-key cryptography. Further cryptographic primitives such as digital signatures achieve the dual purpose of verifying sender (nonrepudiation) and the integrity of the message.

An alternative approach toward security design is to model the potential threats. Microsoft has proposed a threat classification model based on the following six categories, also termed as the STRIDE threat model.

- Spoofing of user identity.
- Tampering of stored or communicated data.
- Repudiation, i.e., denying of actions performed where other users cannot prove otherwise.
- Information disclosure or breach of confidentiality.
- Denial of service (DoS) which makes a network/server unavailable.
- Elevation of privilege for a user to perform unauthorized actions.

In modern CPS and IoT systems, this threat model is discussed together with the so-called attack surfaces. An attack surface provides an entry point for an attacker to gain control of or exfiltrate information from the target system. For example, a detailed study of automotive attack surfaces is presented in [12]. Incorrectly designed protocols often succumb to trivial attacks and present unforeseen attack surfaces as illustrated by the following example.

Example 1: The wireless standard 802.11b is susceptible to various DoS attacks [57]. There, a wireless network client can send a disassociation message to the station for freeing up the resources once the network usage for the client is over. However, this message is sent without any authentication, which essentially enables any user to send this message on behalf of another one. By this, the attacker can stop another user from connecting to the network. In the context of a CPS, this DoS can manifest into a serious availability issue, e.g., through network jamming or MITM attacks [58].

A. Security Standards

Standardization is a common approach for policy makers to enforce a practice, where the security domain is no exception. Basic information security standards such as ISO/IEC 27002 [59] are used as a template, which is then adopted as well as further extended to suit the purpose of an application. In the domain of CPSs, there are standardization efforts that specifically target security, e.g., to protect critical infrastructure [60], such as power plants, power grids, or traffic management systems. ISA/IEC-62443 defines a set of standards/recommendations for implementing industrial automation and control systems. These standards are defined across different layers, such as component, system, policy, and general. Compliance with this standard is managed by the ISA Security Compliance Institute (ISCI). A high-level CPS security perspective has been presented recently via a set of recommendations from the National Institute of Standards and Technology (NIST) [61] to caution against the rising number of cases of IoT attacks. However, it should be noted that, unlike the Payment Card Industry Data Security Standard (PCI DSS) or the Federal Information Processing

Standard (FIPS), the standardization of security in CPS/IoT systems and their compliance is only in nascent phase. In fact, a bill to improve cybersecurity of IoT devices has been introduced in the U.S. Senate recently [62], whereas in the European Union, there is a consolidated effort by the European Union Agency for Network and Information Security (ENISA) to achieve a common standard across all the member states [63].

It is important to note that despite the enforcement of these standards, it is nontrivial to capture the entire protocol of a complex CPS and guard it against subtle vulnerabilities. This is reflected on the experimental studies of attacks on relatively new CPSs such as (semi)autonomous vehicles [12] as well as attacks against systems such as manufacturing plants [64]. It can be argued that the task of standardization is hard due to 1) emergence of new application scenarios combining CPS/IoT; 2) increasing scope of domains that range from manufacturing to IT to wireless; 3) increasing role of autonomous agents in these systems; and 4) the merger of OT security and IT security principles. We illustrate this situation with the following example.

> **Example 2:** In current Android-based smartphones, a plethora of internal sensors provide accurate data about motion, gravity, positioning, environment, and phone orientation, among others. Access to these sensors is unrestricted and not managed. In a recent attack [65], it was demonstrated that by logging in the sensing data surreptitiously and by using that as a training data, it is possible to infer the keywords typed by a user, e.g., the pin, or any other sensitive data, with reasonable accuracy.

Essentially, standards are often adopted/enhanced in the aftermath of an attack and, therefore, can only provide the first-level resistance. The growing penetration of smart components in our everyday lives can enormously increase the risk of a security incident. These concerns, which are often exacerbated by the CPS manufacturers' inability to address the security challenges, led to complementary legal developments in parallel with CPS/IoT security standards. For example, an exemption of copyright protection for the software executing on a CPS/IoT component was announced recently [66]. This permits a user to examine the software in an electronic control unit (ECU) or programmable logic controller (PLC) of the CPS, in order to detect flaws and mitigate it, if identified, independently. Such an approach paves way for security auditing, with eventual growth of security-as-a-service in CPSs. Along the same lines, the U.S. Food and Drug Administration (U.S. FDA) has released guidance for management of devices in case of a cybersecurity threat [67].

B. CPS Security

The close integration between cyber systems and physical processes led to the notion of CPSs. As such, due to the intervention of the physical processes, the scope of CPSs goes beyond traditional information and communication technologies and into the area of operational technology (OT) depicted in Fig. 11, which is typically found in industrial process control systems, e.g., industrial control system (ICS), distributed control system (DCS), and supervisory control and data acquisition (SCADA).

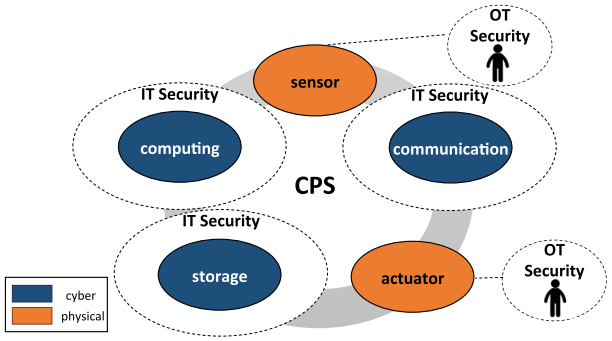

Fig. 11. ***CPSs: IT and OT security.***

In a typical OT deployment, the networking components play a crucial role for interconnecting devices (such as sensors and actuators) and computer systems in order to facilitate networked monitoring and control functions of the industrial operations. Sensors and actuators in such systems are needed for monitoring some physical characteristics of the industrial operations which are critical for the control systems to make timely and effective decisions through some supervisory and control interfaces such as SCADA. Unlike a traditional IT system, security compromise in a CPS often leads to disastrous consequences. The differences to traditional IoT systems are detailed in the following.

- *Physical interface:* The sensor and actuator interfaces of a CPS open up new attack surfaces [68], which also distinguish it from IT security. An attacker can exploit the physical interface to undermine the security of a CPS without actually needing to override the access control mechanism enforced in an OT security model. In traditional IT security, that could happen only if the data is transmitted through an open network.
- *Control system:* CPSs heavily depend on one or more underlying control networks, which are often integrated with physical sensors/actuators, such as an implantable medical device that collects user data and triggers operations in case of abnormal vital parameters. SCADA systems are an integral part of modern industrial CPSs, which face huge security issues [69], all the more due to internet-connected SCADA systems [70]. Many of such control networks and communication protocols were designed with purely OT security and security perimeter in mind, and thus, face difficulties to manage security through an internet-connected system.
- *Availability:* The severity of an availability breach in CPSs is much more than that of a standalone digital

system. An example of this is the power grid attack reported in 2015 [19]. It must be noted that for industrial control systems, any availability attack increases the attack's economic impact proportionally with the duration of unavailability.

- *Timing constraint:* Diverse sets of real-time constraints form an integral aspect of CPSs. The execution time between an event and its corresponding response is often dictated by a hard deadline, which, if missed, may lead to failure of the complete control flow. For example, smart energy monitoring systems deploy circuit breakers to estimate undercurrent/overcurrent. In case of a delay in detecting the surge in the current, the grid can be physically damaged, eventually causing the entire system to fail.
- *Sociotechnical model:* Traditional IT security only forms a part of the larger sociotechnical system security. For CPSs, in particular industrial scale systems, it is not only sufficient to define the access control but also the social and economic impacts of the security breach. This problem is less manifested in a classical information security paradigm due to its limited exposure to the physical interfaces and constraints. However, for CPSs, this becomes especially important due to the possibility of life-threatening situations or so-called kinetic attacks. A detailed discussion of these issues, covered under the OT security, is available in [71], [72].

C. IoT Security

In contrast to CPSs, the focus of IoT systems is on the connectivity and, consequently, toward the management of trustworthy devices interacting with each other.[5] In a startling difference from wired networks for IoT, the network often admits new members, and therefore needs to frequently establish secure communication channels. In the following, few distinguishing features for IoT security are summarized.

- *Trust management:* A prime use case scenario for IoT devices are *ad hoc* sensor networks that find applications in V2V and V2I communications, for example. In such networks, admitting a new node and detecting malicious nodes [73] are important prerequisites for maintaining security policies intact. There have been ample studies on the key management protocols for wireless sensor networks, e.g., via key predistribution [74], identity-based encryption [75], [76], certification authorities, and key exchange protocols. In general, these studies fall under the general theme of trust management [77], which is particularly challenging for low-end devices due to the performance overhead that a secure key storage or dynamic code attestation incurs.
- *Secure routing protocol:* IoT systems rely critically on static/dynamic routing protocols, which may be subjected to diverse forms of attacks [78]. Typical countermeasures for routing protocol attacks depend on: 1) a trusted base station that enables authentication and encryption; 2) multipath routing; and 3) secure geographic routing protocols [79].
- *Heterogeneous network integration:* IoT networks are usually associated with a heterogeneous mix of wireless communication systems, each of which comes with its own security protocols. Their interoperability may require conversion of data formats, which is difficult to undertake without partial knowledge of the message payload. Furthermore, the possibility and often undetected presence of diverse information channels remains a constant threat [80].
- *Privacy protection:* IoT nodes can request to maintain data/location privacy and also anonymity while participating in a network. This can be ensured by sensor security, e.g., RFID/NFC privacy [81] or privacy of general embedded sensors [82]. Anonymity is preserved, for example, by generating similar traffic volumes for a certain number of nodes surrounding the sink [83] or adopting a multiparent, fractal propagation that involves spreading fake messages at the intermediate nodes [84].

Example 3: In a recent demonstration of an attack against connected IoT devices, researchers took control over all the light bulbs in close proximity of each other by first infecting a light bulb with a malicious firmware [17]. The attack exploited the ZigBee protocol and the absence of any asymmetric-key cryptography for establishing secure communication channels to gain the ability to perform over-the-air updates of other light bulbs. In another variant of an IoT attack, researchers have been able to achieve undesired and potentially kinetic cyber attack functionalities [85].

VI. SECURITY IN WIRELESS COMMUNICATION FOR IoT AND CPSs

In principle, security in wireless systems can be provided on different levels of the network stack, using two very different approaches and philosophies.

1) Classical security measures are applied at the MAC/DLL, network, transport, and application layer and corresponding techniques are based on standard cryptographic principles. Corresponding algorithms assume that the underlying PHY and DLL layers provide a reliable link. At the same time, they do not make use of any further information on the received wireless signal and do not provide any control on the physical layer. The corresponding techniques are thereby mainly based on "conventional" measures that are often also known from wired networks.

[5]In the absence of a trust model, one may adhere to the consensus protocols and decision mechanisms arising thereof, as promoted through Blockchain technologies.

2) Physical layer security measures are applied at the physical layer following information-theoretic principles. Security is achieved and advanced through sophisticated signaling schemes and the analysis of mutual information between sender, receiver, and the eavesdropper under different channel condition assumptions. However, the physical layer interface to upper layers entails information loss and, therefore, renders propagation of information-theoretic ideas difficult. Furthermore, under realistic assumptions, information-theoretic principles often do not provide absolute security guarantees.

In a major contrast to the wireless systems, CPSs and IoT systems do not necessarily employ the entire OSI stack. Instead, due to the interaction with physical processes, they bring their own layers, e.g., perception layer, computation layer, and application layer, which interface with the OSI stack for the purpose of transport. This is depicted in Fig. 12, where some of the potential security vulnerabilities in the different layers are denoted.

A. Security of Wireless Communication

The origin of modern communication security is due to the information-theoretic studies of Shannon [99] and its extension to physical layer encryption by Wyner [100]. However, the notion established by Wyner has several caveats such as, assumption of sender's (Bob) knowledge of the secret channel established by the eavesdropper (Eve) and assumption of infinite packet length. Subsequently, several works have been done in this direction to generalize the channel model [101], adapt to multiple-input–multiple-output (MIMO) wireless systems [102], and achieve secrecy by directional modulation [103]. Nevertheless, for the capacity-bounded physical channel, under practical assumptions, a provably secure communication mode is currently not known. Therefore, state-of-the-art studies of physical encryption are based on the mutual information shared between the sender (Bob), the receiver (Alice), and the eavesdropper (Eve).

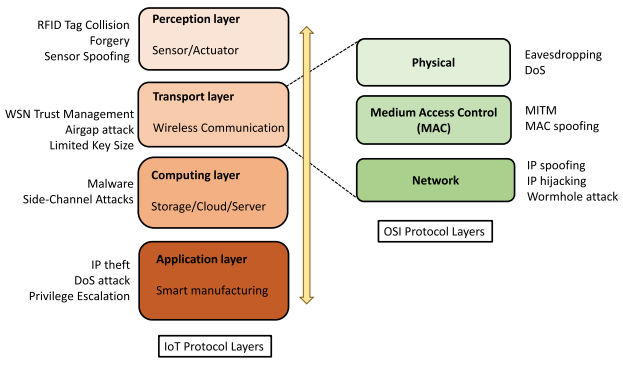

Fig. 12. ***IoT security issues with OSI layer view.***

Further challenges in security design arise from the fact that wireless communication adheres to the OSI layered protocol architecture and the physical layer encryption is not necessarily backed up with an adequate security mechanism in the upper layers of communication. A well-known example of such security breach is the MITM attack by spoofing the address resolution protocol (ARP) at MAC layer. Preventing such attacks requires detailed analysis of the wireless communication protocols. Indeed it has been pointed out in a detailed survey of security issues in wireless communication [104] that cross-layer and hybrid security issues in wireless communication are important open challenges. By extending the same issues toward potentially more layers of IoT and CPS protocols only calls for further aggravation of the situation. This has been demonstrated prominently through, e.g., hacking the Mitsubishi Outlander through a brute-force hack of the preshared WiFi key, exfiltrating sensitive data from a computer through a covered FM channel [80], a study of possible attacks for teleoperated surgical robots [105], and hacking of a wireless-controlled implantable medical device [106].

B. Security Incidents: Emerging Threats

Conventional CPSs ensure security through access restrictions, which relies on the physical protection of the sensitive devices, e.g., sensors and actuators. With the growing connectivity and autonomy of the systems, such protection cannot be guaranteed anymore. This gives rise to new threats on a regular basis. On the other hand, for IoT systems, the connectivity of multiple devices presents several challenges, e.g., undetected presence of malicious devices, covered communication channels, performance overhead, and vulnerability due to interoperability of protocols.

In Table 3, few representative security incidents/analyses are provided. Expectedly, with the growth of consumer applications in the IoT and CPS domain, more attacks are being reported there. While many such vulnerabilities do also exist in the infrastructural and industrial domain, these are still protected through OT security measures and thus, phishing emails or hacking airgapped networks are common techniques deployed in those scenarios.

C. Perspective and Recommendations

Historically, there have been attacks on wireless communication networks, which were focused on a standard, e.g., the WEP algorithm has been subjected to several passive and active attacks [107]. However, the current attack trends, building on top of the wireless communication system vulnerabilities, reach for an impact at the level of the application, e.g., causing malfunction of a PLC-controlled component in an industrial control system network. There are new challenges brought forward by these attacks, which are deeply application specific. For example, a replay

Table 3 Representative CPS and IoT Security Incidents/Analyses

Domain	Application	Attack Origin	Attack Type
Consumer	Healthcare	Wireless Network	Replay attack [16]
	Automotive	CAN bus, ECU	Eavesdropping, Privilege Escalation, MITM, DoS [86]
	Automotive	Speed sensor	ABS Spoof [14]
	Automotive	Bluetooth, WiFi, CAN bus	Sensor Spoof, DoS, Privilege Escalation [87]
	Digital Lock	Bluetooth sniffing	Eavesdropping, Privilege Escalation [88]
	Smart Home	ZigBee node	Eavesdropping, DoS [89]
	Smart Home	Lightbulb	Malware [17]
	Finance	Android NFC-capable device	Relay Attack [90]
Infrastructure	Transportation	GPS receiver	GPS Spoof [91]
	Energy	Computer system	Forced Update [92]
	Energy	Smart Meter	Eavesdropping, DoS, Integrity [93]
	DNS Service	IoT device	DDoS [94]
	Traffic	Radio network	DoS, Traffic Congestion [95]
Industrial	Manufacturing Control	USB devices, Phishing	Eavesdropping, Side Channel Attacks, Resonance Attacks [96]
	Additive Manufacturing	Acoustic sensor/Microphone	IP Theft [97]
	Manufacturing Control	Phishing	Privilege Escalation [98]

attack is harmless in a video conference, whereas it can be dangerous for an implantable medical device.

Based on the above studies, we propose a four-phased approach toward designing secure CPS/IoT systems as follows.

1) *Security policy:* Security policy design is to be done on the basis of the confidentiality–integrity–availability (CIA) triad, though higher focus can be given to a specific aspect as per the application requirement, e.g., anonymity in a V2V or V2I network.
2) *Secure network:* The choice of the network is primarily driven by the application requirements, e.g., proximity and bandwidth. Clearly, network interoperability, protocol-level security, access restrictions, and performance overhead due to security features should also be considered. An important aspect here is to maintain networks with a well-defined security perimeter, i.e., ruling out the presence of covered information channels.
3) *Secure component:* Individual components in the network range from sensors and routers to storage and computing devices, all of which have diverse security hazards. Careful selection of these devices is necessary, including the information leakage analysis and their connectivity analysis.
4) *Security auditing:* In absence of a system that is designed with security as a prime requirement, there is a steady growth of security auditing services, dedicated surveillance technologies [108]–[110], and even crowdsourcing [111]. However, a design for security approach that we advocate should be supported with security simulation and emulation [112].

VII. CONCLUSION AND FUTURE WORKS

The diversity and the heterogeneous nature of CPSs and the IoT poses a number of requirements on the communication systems (wired and wireless) that connect their components. In particular in a CPS, this connectivity and its requirements may even be different for various parts of the system. No single standard can meet all of the requirements. However, a plethora of different standards exist that cover a large part of the design space. Nevertheless, there is still a need for innovation in the development of future wireless systems. The main challenges in this area are as follows.

1) The rapidly increasing number of connected nodes which is expected to reach into the billions within the next decade: This humongous number of devices is posing a tremendous challenge not only for the pure physical layer capacity, but also and especially in terms of managing access of these devices to the channel in an efficient way with little overhead.
2) The increasing amount of data that is communicated wirelessly is in conflict with the limited available spectrum and the limited system capacity. More spectrally, efficient communication links need to be developed to support the need for more data traffic.
3) As wireless links are more and more integrated into critical control loops, latency becomes a very important issue. Today's wireless systems, and in particular those which are designed for low power consumption and large network capacity, have very long latencies, which are unacceptable for many emerging CPSs. Hence, developing new low-power communication systems with large system capacities is a pressing issue.
4) A main challenge in CPSs and IoT systems with wireless nodes is the need of energy autonomy or at least of multiple years of lifetime for the connected nodes. This need clearly increases with the increasing number of devices as supporting regular battery changes becomes infeasible. Hence, the design of low-power communication and communication with effective duty cycling remains a very important issue.

Security has become a major concern with increased communication and intelligence at low-end devices that directly interface with myriads of our day-to-day activities.

Indeed many of the present studies show that existing systems across all domains, when exposed to the connectivity, strictly fall short of the necessary security precaution [12], [64], [93], [95], [113]. Wireless communication, with its rapid strides in the past decades, has become the key driver in the smart world. Technologies such as IoT and CPSs are now commonplace with the prediction that the world will have 8.4 billion connected IoT devices [114] with the majority of these devices serving consumer applications. This staggering growth will cause havoc if the security issues are not properly addressed. In this paper, we have outlined the vast landscape of wireless communication protocols, how those interface with the CPSs and IoT systems, and studied the security requirements of these systems, which often take orthogonal paths. As a result, security breaches of these systems are observed on regular basis, often with potentially catastrophic consequences. With this background, the following issues need urgent research attention and should be considered as part of a large research framework.

1) It is well understood that, formally, wireless communication by itself does not guarantee security but, merely increases the difficulty of eavesdropping with certain cautionary steps. Besides, physical layer protection does not automatically prevent integrity or availability breaches. Therefore, physical layer protection must be complemented with appropriate protection at higher layers. This protection also needs to be extended toward different levels of a protocol that CPSs or IoT systems bring forth. A general issue in that direction is to ensure cross-layer protocol validation against a set of given security requirements.
2) Introduction of covert channels and/or malicious nodes is found to be a technique of choice behind numerous attacks. A basic authentication mechanism should be in place for any wireless communication system. Furthermore, it has to be ensured that the key size is sufficient to defeat an attacker with resources, and/or frequent key updates should be supported. For unconnected and redundant communication modes, tracking of promiscuous devices is necessary. This is especially important for heterogeneous networks that are commonplace now.
3) The analysis of side-channel information leakage is a relatively new field in cryptography, having originated from the rapid evolution of passive and active side-channel attacks. Nonetheless, the idea of mutual information analysis is applied to both and, therefore, could be adapted as a robust foundation for joint analysis of communication and security across all layers.
4) Policy design for secure CPS/IoT is a long-standing goal that is being pursued across multiple domains independently. An important step toward this direction is to ensure that security is not achieved through obscurity, which is apparently a major flaw in the current generation of smart CPSs and IoT systems. ■

REFERENCES

[1] J. Shi, J. Wan, H. Yan, and H. Suo, "A survey of cyber-physical systems," in *Proc. Int. Conf. Wireless Commun. Signal Process.*, Nov. 2011, pp. 1–6, doi: 10.1109/WCSP.2011.6096958.

[2] M. Weiser, "The computer for the 21st century," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 3, pp. 3–11, Jul. 1999.

[3] S. K. Khaitan and J. D. McCalley, "Design techniques and applications of cyberphysical systems: A survey," *IEEE Syst. J.*, vol. 9, no. 2, pp. 350–365, Jun. 2015, doi: 10.1109/JSYST.2014.2322503.

[4] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," in *Proc. IEEE Int. Conf. Sensor Netw. Ubiquitous Trustworthy Comput.*, Jun. 2008, pp. 1–9, doi: 10.1109/SUTC.2008.85.

[5] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surv. Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015, doi: 10.1109/COMST.2015.2388550.

[6] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *CoRR*, 2017.

[7] A. Chattopadhyay, A. Prakash, and M. Shafique, "Secure cyber-physical systems: Current trends, tools and open research problems," in *Proc. DATE*, 2017, pp. 1104–1109.

[8] F.-X. Standaert, *Introduction to Side-Channel Attacks*. Boston, MA, USA: Springer-Verlag, 2010, pp. 27–42.

[9] V. Pudi, A. Chattopadhyay, and K.-Y. Lam, "Secure and lightweight compressive sensing using stream cipher," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, 2017, doi: 10.1109/TCSII.2017.2715659.

[10] Y. Liu and G. Zhou, "Key technologies and applications of Internet of Things," in *Proc. 5th Int. Conf. Intell. Comput. Technol. Autom.*, Jan. 2012, pp. 197–200, doi: 10.1109/ICICTA.2012.56.

[11] V. Gazis, "A survey of technologies for the Internet of Things," in *Proc. Int. Wireless Commun. Mobile Comput. Conf.*, Aug. 2015, pp. 1090–1095, doi: 10.1109/IWCMC.2015.7289234.

[12] S. Checkoway, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Conf. Secur.*, 2011.

[13] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson, *A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay*. Berlin, Germany: Springer-Verlag, 2009, pp. 84–91.

[14] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, *Non-Invasive Spoofing Attacks for Anti-Lock Braking Systems*. Berlin, Germany: Springer-Verlag, 2013, pp. 55–72, doi: 10.1007/978-3-642-40349-1_4.

[15] M. Milis, "IcyHeart: Highly integrated ultra-low-power SoC solution for unobtrusive and energy efficient wireless cardiac monitoring: Research project for the benefit of specific groups (FP7, capacities)," in *Proc. IEEE 12th Int. Conf. Bioinf. Bioeng.*, Nov. 2012, pp. 105–109.

[16] N. Leavitt, "Researchers fight to keep implanted medical devices safe from hackers," *Computer*, vol. 43, no. 8, pp. 11–14, Aug. 2010.

[17] E. Ronen and C. O'Flynn, A. Shamir, and A.-O. Weingarten, "IoT goes nuclear: Creating a ZigBee chain reaction," Cryptology, Tech. Rep. 2016/1047, 2016. [Online]. Available: http://eprint.iacr.org/2016/1047

[18] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-phones attacking smart-homes," in *Proc. 9th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2016, pp. 195–200, doi: 10.1145/2939918.2939925.

[19] "Analysis of the cyber attack on the Ukrainian power grid," *EISAC*, 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[20] "Massive hack attack targets Israel electrical grid," *Fox News*, 2016. [Online]. Available: http://www.foxnews.com/world/2016/01/27/massive-hack-attack-targets-israel-electrical-grid.html

[21] "Hackers targeting UK energy grid, GCHQ warns," *The Telegraph*, 2017. [Online]. Available: http://www.telegraph.co.uk/technology/2017/07/18/hackers-targeting-uk-energy-grid-gchq-warns/

[22] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Towards threat of implementation attacks on substation security: Case study on fault detection and isolation," *IEEE Trans. Ind. Informat.*, 2017, doi: 10.1109/TII.2017.2770096.

[23] M. Kammerstetter, L. Langer, F. Skopik, F. Kupzog, and W. Kastner, "Practical risk assessment using a cumulative smart grid model," in *Proc. 3rd Int. Conf. Smart Grids Green IT Syst.*, 2014, pp. 31–42, doi: 10.5220/0004860900310042.

[24] C. Marcu, "A 90 nm CMOS low-power 60 GHz transceiver with integrated baseband circuitry," *IEEE J. Solid-State Circuits*, vol. 44, no. 12, pp. 3434–3447, Dec. 2009, doi: 10.1109/JSSC.2009.2032584.

[25] M. Tajima, "Strategic value of RFID in supply chain management," *J. Purchasing Supply Manage.*, vol. 13, no. 4, pp. 261–273, 2007.

[26] *Information Technology AIDC Techniques—RFID for Item Management, Parts 1–7*, International Organization Standardization, Geneva, Switzerland, Mar. 2013.

[27] R. Want, "Near field communication," *IEEE Pervasive Comput.*, vol. 10, no. 3, pp. 4–7, Mar. 2011.

[28] *ZigBee Specification, V1.0*, document 053474r06, ZigBee Alliance, Dec. 2004.

[29] *Z-Wave Devices and Standards*. [Online]. Available: http://www.z-wavealliance.org/

[30] *EnOcean Devices and Standards*. [Online]. Available: http://www.enoceanalliance.org/en/home/

[31] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," *IEEE Commun. Mag.*, vol. 48, no. 6, pp. 92–101, Jun. 2010, doi: 10.1109/MCOM.2010.5473869.

[32] A. Wheeler, "Commercial applications of wireless sensor networks using ZigBee," *IEEE Commun. Mag.*, vol. 45, no. 4, pp. 70–77, Apr. 2007, doi: 10.1109/MCOM.2007.343615.

[33] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," *Comput. Commun.*, vol. 30, no. 7, pp. 1655–1695, 2007.

[34] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Standard 802.15.4a, 2003, doi: 10.1109/IEEESTD.2003.94389.

[35] S. S. R. Ahamed, "The role of ZigBee technology in future data communication system," *J. Theor. Appl. Inf. Technol.*, vol. 5, no. 2, p. 129, 2009.

[36] M. Zhou and Z.-L. Nie, "Analysis and design of ZigBee MAC layers protocol," in *Proc. Int. Conf. Future Inf. Technol. Manage. Eng.*, vol. 2. Oct. 2010, pp. 211–215, doi: 10.1109/FITME.2010.5654824.

[37] *IEEE Standard for Local and Metropolitan Area Networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC Sublayer*, IEEE Standard 802.15.4e-2012, 2012.

[38] J. Ploennigs, U. Ryssel, and K. Kabitzsch, "Performance analysis of the EnOcean wireless sensor network protocol," in *Proc. 15th IEEE Conf. Emerg. Technol. Factory Autom.*, Sep. 2010, pp. 1–9, doi: 10.1109/ETFA.2010.5641313.

[39] *IEEE Standard for Information Technology—Local and Metropolitan Area networks—Specific Requirements—Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPAN)*, IEEE Standard 802.15.1-2005, Jun. 2005, pp. 1–700, doi: 10.1109/IEEESTD.2005.96290.

[40] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of Bluetooth low energy: An emerging low-power wireless technology," *Sensors*, vol. 12, no. 9, pp. 11734–11753, 2012.

[41] T. Watteyne, "Industrial wireless IP-based cyber–physical systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1025–1038, May 2016, doi: 10.1109/JPROC.2015.2509186.

[42] *IEEE Stadard for Information Technology–Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-2012, Mar. 2012, pp. 1–5229.

[43] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi," in *Proc. IEEE 33rd Annu. Conf. Ind. Electron. Soc.*, Nov. 2007, pp. 46–51.

[44] *IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Fast Initial Link Setup*, IEEE Standard 802.11ac-2013, Dec. 2013, pp. 1–425, doi: 10.1109/IEEESTD.2013.6687187.

[45] S. K. Saha, T. Siddiqui, D. Koutsonikolas, A. Loch, J. Widmer, and R. Sridhar, "A detailed look into power consumption of commodity 60 GHz devices," in *Proc. IEEE 18th Int. Symp. World Wireless, Mobile Multimedia Netw.*, Jun. 2017, pp. 1–10, doi: 10.1109/WoWMoM.2017.7974282.

[46] Q. Wang and M. Zuniga, Passive sensing and communication using visible light: Taxonomy, challenges and opportunities," 2017. [Online]. Available: https://arxiv.org/abs/1704.01331

[47] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, "Visible light communication, networking, and sensing: A survey, potential and challenges," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2047–2077, 4th Quart., 2015, doi: 10.1109/COMST.2015.2476474.

[48] G. Corbellini, K. Aksit, S. Schmid, S. Mangold, and T. Gross, "Connecting networks of toys and smartphones with visible light communication," *IEEE Commun. Mag.*, vol. 52, no. 7, pp. 72–78, Jul. 2014.

[49] T. Yamazato, "Image-sensor-based visible light communication for automotive applications," *IEEE Commun. Mag.*, vol. 52, no. 7, pp. 88–97, Jul. 2014.

[50] S. Rajagopal, R. D. Roberts, and S.-K. Lim, "IEEE 802.15.7 visible light communication: Modulation schemes and dimming support," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 72–82, Mar. 2012.

[51] S. V. Tiwari, A. Sewaiwar, and Y.-H. Chung, "Uplink bidirectional efficient multiuser visible light communications using TDD and diversity techniques," in *Proc. 8th Int. Conf. Ubiquitous Future Netw.*, Jul. 2016, pp. 225–230, doi: 10.1109/ICUFN.2016.7537022.

[52] G. Kail, P. Maechler, N. Preyss, and A. Burg, "Robust asynchronous indoor localization using LED lighting," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, May 2014, pp. 1866–1870.

[53] F. Qu, F.-Y. Wang, and L. Yang, "Intelligent transportation spaces: Vehicles, traffic, communications, and beyond," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 136–142, Nov. 2010, doi: 10.1109/MCOM.2010.5621980.

[54] *IEEE Draft Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment: Wireless Access in Vehicular Environments*, IEEE Standard P802.11p/D11.0, Mar. 2010.

[55] S. Andreev, "Understanding the IoT connectivity landscape: A contemporary M2M radio technology roadmap," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 32–40, Sep. 2015.

[56] B. Weber, "A SAW-less RF-SoC for cellular IoT supporting EC-GSM-IoT -121.7 dBm sensitivity through EGPRS2A 592 kbps throughput," in *Proc. IEEE Eur. Solid State Circuits Conf.*, Sep. 2017, pp. 340–343.

[57] M. L. Lough, "A taxonomy of computer attacks with applications to wireless," Ph.D. dissertation, Virginia PolyTech. Inst., Blacksburg, VA, USA, 2001.

[58] M. Vanhoef and F. Piessens, "Advanced Wi-Fi attacks using commodity hardware," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, New York, NY, USA, 2014, pp. 256–265.

[59] (2013). *ISO/IEC 27002:2013 Standard*. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=54533

[60] *NERC Critical Infrastructure Protection Standard*. [Online]. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[61] R. Ross, M. McEvilley, and J. C. Oren, "Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems," Tech. Rep., 2016.

[62] *A Bill to Provide Minimal Cyber Security Operational Standards for Internet-Connected Devices Purchased by Federal Agencies, and for Other Purposes*. [Online]. Available: https://www.eenews.net/assets/2017/08/02/document_ew_01.pdf

[63] *ENISA: Cybersecurity Standards and Certification*. [Online]. Available: https://www.enisa.europa.eu/topics/standards

[64] D. Gollmann, P. Gurikov, A. Isakov, M. Krotofil, J. Larsen, and A. Winnicki, "Cyber-physical systems security: Experimental analysis of a vinyl acetate monomer plant," in *Proc. 1st ACM Workshop Cyber-Phys. Syst. Secur.*, 2015, pp. 1–12, doi: 10.1145/2732198.2732208.

[65] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "Stealing PINs via mobile sensors: Actual risk versus user perception," *Int. J. Inf. Secur.*, pp. 1–23, Apr. 2017, doi: 10.1007/s10207-017-0369-x.

[66] *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, document 2014-07. [Online]. Available: http://copyright.gov/fedreg/2015/80fr65944.pdf

[67] (2016). *Postmarket Management of Cybersecurity in Medical Devices*. [Online]. Available: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf

[68] M. Harris, "Researcher hacks self-driving car sensors," *IEEE Spectrum*, 2015. [Online]. Available: http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors

[69] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proc. Int. Conf. Internet Things 4th Int. Conf. Cyber Phys. Soc. Comput.*, Oct. 2011, pp. 380–388, doi: 10.1109/iThings/CPSCom.2011.34.

[70] (2015). *Dell Security Annual Threat Report*. [Online]. Available: https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf

[71] R. Anderson, *Measuring the Cost of Cybercrime*. Berlin, Germany: Springer-Verlag, 2013, pp. 265–300.

[72] K. Y. Lam, "IoT security: Cyber security from IT to OT," in *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers*. Singapore: Palo Alto Networks, 2016.

[73] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 266–282, 1st Quart., 2014, doi: 10.1109/SURV.2013.050113.00191.

[74] W. Bechkit, Y. Challal, A. Bouabdallah, and V. Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 2, pp. 948–959, Feb. 2013, doi: 10.1109/TWC.2012.010413.120732.

[75] C.-K. Chu, J. K. Liu, J. Zhou, F. Bao, and R. H. Deng, "Practical ID-based encryption for wireless sensor network," in *Proc. 5th ACM Symp. Inf. Comput. Commun. Secur.*, New York, NY, USA, 2010, pp. 337–340.

[76] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. 27th Conf. Comput. Commun.*, Apr. 2008, doi: 10.1109/INFOCOM.2008.58.

[77] T. Abera, "Invited: Things, trouble, trust: On building trust in IoT systems," in *Proc. 53rd ACM/EDAC/IEEE Design Autom. Conf.*, Jun. 2016, pp. 1–6, doi: 10.1145/2897937.2905020.

[78] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proc. 1st IEEE Int. Workshop Sensor Netw. Protocols Appl.*, May 2003, pp. 113–127, doi: 10.1109/SNPA.2003.1203362.

[79] M. García-Otero, "Secure geographic routing in ad hoc and wireless sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2010, no. 1, p. 975607, 2010.

[80] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici, "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," in *Proc. 9th Int. Conf. Malicious Unwanted Softw. Amer.*, Oct. 2014, pp. 58–67, doi: 10.1109/MALWARE.2014.6999418.

[81] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, Feb. 2006, doi: 10.1109/JSAC.2005.861395.

[82] T. Scheffler and B. Schnor, "Privacy requirements for embedded sensor devices," in *Proc. IEEE 16th Int. Symp. Pers. Indoor Mobile Radio Commun.*, vol. 2, Sep. 2005, pp. 790–794, doi: 10.1109/PIMRC.2005.1651551.

[83] G. Chai, M. Xu, W. Xu, and Z. Lin, "Enhancing sink-location privacy in wireless sensor networks through k-anonymity," *Int. J. Distrib. Sensor Netw.*, vol. 8, no. 4, p. 648058, 2012, doi: 10.1155/2012/648058.

[84] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *Proc. IEEE 1st Int. Conf. Secur. Privacy Emerg. Areas Commun. Netw.*, Sep. 2005, pp. 113–126, doi: 10.1109/SECURECOMM.2005.16.

[85] E. Ronen and A. Shamir, "Extended functionality attacks on IoT devices: The case of smart lights," in *Proc. IEEE Eur. Symp. Secur. Privacy*, Mar. 2016, pp. 3–12, doi: 10.1109/EuroSP.2016.13.

[86] K. Koscher, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 447–462.

[87] C. Valasek and C. Miller, "A survey of remote automotive attack surfaces," 2014. [Online]. Available: https://www.ioactive.com/pdfs/IOActive_Remote_Attack_Surfaces.pdf

[88] A. Rose and B. Ramsey, "Picking a Bluetooth low energy lock from a quarter mile away," 2016. [Online]. Available: https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Rose-Ramsey-Picking-Bluetooth-Low-Energy-Locks.pdf

[89] L. Jun and Y. Qing, "I'm a newbie yet I can hack Zigbee: Take unauthorized control over ZigBee Devices," 2015. [Online]. Available: https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Li-Jun-Yang-Qing-I-AM-A-NEWBIE-YET-I-CAN-HACK-ZIGBEE.pdf

[90] J. Vila and R. J. Rodríguez, "Practical experiences on NFC relay attacks with Android," in *Proc. 11th Int. Workshop Radio Freq. Identification*, 2015, pp. 87–103, doi: 10.1007/978-3-319-24837-0_6.

[91] M. L. Psiaki and T. E. Humphreys, "Protecting GPS from spoofers is critical to the future of navigation," *IEEE Spectrum*, 2016.

[92] B. Krebs, "Cyber incident blamed for nuclear power plant shutdown," Tech. Rep., Jun. 2008.

[93] F. M. Cleveland, "Cyber security issues for Advanced Metering Infrasttructure (AMI)," in *Proc. IEEE Power Energy Soc. Gen. Meeting-Convers. Del. Elect. Energy 21st Century*, Jul. 2008, pp. 1–5, doi: 10.1109/PES.2008.4596535.

[94] (Oct. 2016). *Dyn Analysis Summary of Friday October 21 Attack*. [Online]. Available: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[95] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: Analyzing the security of traffic infrastructure," in *Proc. 8th USENIX Conf. Offensive Technol.*, Berkeley, CA, USA, 2014, p. 7.

[96] D. Kushner, "The real story of Stuxnet," *IEEE Spectrum*, 2013. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[97] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic side-channel attacks on printers," in *Proc. 19th USENIX Conf. Security*, 2010, p. 20.

[98] M. J. A. M. Robert Lee and T. Conway (Dec. 2014). *German Steel Mill Cyber Attack*. [Online]. Available: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

[99] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, 2001.

[100] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975, doi: 10.1002/j.1538-7305.1975.tb02040.x.

[101] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008, doi: 10.1109/TIT.2008.921678.

[102] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011, doi: 10.1109/TIT.2011.2158487.

[103] M. Daly, "Physical layer encryption using fixed and reconfigurable antennas," Ph.D. dissertation, Univ. Illinois Urbana–Champaign, Champaign, IL, USA, 2013. [Online]. Available: http://hdl.handle.net/2142/42321

[104] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, doi: 10.1109/JPROC.2016.2558521.

[105] T. Bonaci, J. Herron, T. Yusuf, J. Yan, T. Kohno, and H. J. Chizeck, "To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots," *CoRR*, 2015.

[106] D. Halperin, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy*, May 2008, pp. 129–142, doi: 10.1109/SP.2008.31.

[107] *Security of the WEP Algorithm*. [Online]. Available: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[108] V. Sachidananda, S. Siboni, A. Shabtai, J. Toh, S. Bhairav, and Y. Elovici, "Let the cat out of the bag: A holistic approach towards security analysis of the internet of things," in *Proc. 3rd ACM Int. Workshop IoT Privacy Trust, Secur.*, New York, NY, USA, 2017, pp. 3–10.

[109] A. Cybertech. (May 2017).

[110] A. Lebrun and J.-C. Demay (2016). *CANSPY: A Platform for Auditing CAN Devices*. [Online]. Available: https://www.blackhat.com/docs/us-16/materials/us-16-Demay-CANSPY-A-Platorm-For-Auditing-CAN-Devices.pdf

[111] A. Greenberg, "GM asks friendly hackers to report its cars' security flaws," Aug. 2016.

[112] J. Tong, W. Sun, and L. Wang, *A Smart Home Network Simulation Testbed for Cybersecurity Experimentation*. Cham, Switzerland: Springer-Verlag, 2014, pp. 136–145.

[113] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security challenges for medical devices," *Commun. ACM*, vol. 58, pp. 74–82, Mar. 2015, doi: 10.1145/2667218.

[114] *Gartner Says 8.4 Billion Connected Things will be in use in 2017*. [Online]. Available: http://www.gartner.com/newsroom/id/3598917

ABOUT THE AUTHORS

Andreas Burg (Member, IEEE) was born in Munich, Germany, in 1975. He received the Dipl. Ing. degree from the Swiss Federal Institute of Technology (ETH) Zurich, Zurich, Switzerland, in 2000 and the Dr.Sc.Techn. degree from the Integrated Systems Laboratory, ETH Zurich, in 2006.

In 1998, he was with Siemens Semiconductors, San Jose, CA, USA. During his Ph.D. studies, he was with the Bell Labs Wireless Research for one year. From 2006 to 2007, he was a Post-doctoral Researcher with the Integrated Systems Laboratory and with the Communication Theory Group, ETH Zurich. In 2007, he cofounded Celestrius, an ETH spinoff in the field of MIMO wireless communication, where he was responsible for the ASIC development as the Director for VLSI. In 2009, he joined ETH Zurich as an SNF Assistant Professor and as the Head of the Signal Processing Circuits and Systems Group with the Integrated Systems Laboratory. Since 2011, he has been a Tenure Track Assistant Professor with the École Polytechnique Fédérale de Lausanne, where he leads the Telecommunications Circuits Laboratory.

Prof. Burg is a member of the EURASIP SAT SPCN and the IEEE TC-DISPS. In 2000, he received the Willi Studer Award and the ETH Medal for his diploma and his diploma thesis, respectively. He was also awarded an ETH Medal for his Ph.D. dissertation in 2006. In 2008, he received a 4-years grant from the Swiss National Science Foundation (SNF) for an SNF Assistant Professorship. With his students he received the Best Paper Award from the *EURASIP Journal on Image and Video Processing* in 2013 and best demo/paper awards at ISCAS 2013, ICECS 2013, and at ACSSC 2007. In his career, he was involved in the tapeout of more than 35 ASICs. He has served on the TPC of various conferences on signal processing, communications, and VLSI. He was a TPC Co-Chair for VLSI-SoC 2012 and the TCP Co-Chair for ESSCIRC 2016 and SiPS 2017. He served as an Editor of the IEEE Transactions on Circuits and Systems in 2013 and on the Editorial Board of the Springer *Microelectronics Journal*. He is an Editor of the Springer *Journal on Signal Processing Systems*, and the MDPI *Journal on Low Power Electronics and its Applications*.

Anupam Chattopadhyay (Senior Member, IEEE) received the B.E. degree from Jadavpur University, India, in 2000, the M.Sc. degree from ALaRI, Switzerland, in 2002, and the Ph.D. degree from RWTH Aachen, Germany, in 2008.

From 2008 to 2009, he worked as a Member of Consulting Staff in CoWare R&D, Noida, India. From 2010 to 2014, he led the MPSoC Architectures Research Group in RWTH Aachen as a Junior Professor. Since September 2014, he has been an Assistant Professor at the School of Computer Science and Engineering (SCSE), Nanyang Technological University (NTU), Singapore and also holds an honorary adjunct appointment at SPMS, NTU. In the past, he was a Visiting Professor at EPFL, Switzerland and Indian Statistical Institute, Kolkata. His research advances has been reported in more than 100 conference/journal papers (ACM/IEEE/Springer), multiple research monographs and edited books (CRC, Springer) and open-access forums. Together with his doctoral students, he proposed novel research directions like, domain-specific high-level synthesis for cryptography, high-level reliability estimation flows for embedded processors, generalization of classic linear algebra kernels, and multilayered coarse-grained reconfigurable architecture. His research in the area of emerging technologies has been covered by major news outlets across the world, including *Asian Scientist, Straits Times*, and *The Economist*.

Prof. Chattopadhyay received a Borcher's plaque from RWTH Aachen, Germany for outstanding doctoral dissertation in 2008 and the nomination for best IP award at DATE 2016.

Kwok-Yan Lam received the B.Sc. degree (first class honors) from the University of London, London, U.K., in 1987 and the Ph.D. degree from the University of Cambridge, Cambridge, U.K., in 1990.

He is a Professor of Computer Science at the Nanyang Technological University (NTU), Singapore. He is currently the Director of NTU's SPIRIT Smart Nation Research Centre, and the Program Chair (Secure Community) of the Interdisciplinary Graduate School of NTU. He has been a Professor of the Tsinghua University, China (2002–2010) and a faculty member of the National University of Singapore and the University of London since 1990. He was a Visiting Scientist at the Isaac Newton Institute of the Cambridge University and a Visiting Professor at the European Institute for Systems Security. In 1997, he founded PrivyLink International Ltd, a spinoff company of the National University of Singapore, specializing in e-security technologies for homeland security and financial systems. In 2012, he cofounded Soda Pte Ltd which won the Most Innovative Start Up Award at the RSA 2015 Conference. His research interests include distributed systems, IoT security infrastructure, distributed authentication, biometric cryptography, homeland security, and cybersecurity.

Prof. Lam received the Singapore Foundation Award in 1998 from the Japanese Chamber of Commerce and Industry in recognition of his R&D achievement in Information Security in Singapore.