Towards Wireless Communications in Automation: An Overview

Lisa Underberg*, Michael Karrenbauer†, Philipp Schulz‡, Qiaohan Zhang‡, Andreas Weinand†, Niklas Bulk§,
Philipp Rosemann†, Parva Yazdani*, Armin Dekorsy§, Gerhard Fettweis‡ and Hans D. Schotten†

*Institute for Automation and Communication, Magdeburg, Germany, Email: {lisa.underberg, parva.yazdani}@ifak.eu
†Institute for Wireless Communication and Navigation, University of Kaiserslautern-Landau, Germany,
Email: {michael.karrenbauer, andreas.weinand, philipp.rosemann, schotten}@rptu.de
‡Vodafone Chair Mobile Communications Systems, Technische Universität Dresden, Germany,
Email: {philipp.schulz2, qiaohan.zhang, gerhard.fettweis}@tu-dresden.de
§Dept. of Communications Engineering, University of Bremen, Germany, Email: {bulk, dekorsy}@ant.uni-bremen.de

***Abstract*—Industrial Ethernet networks are well-established communication systems in industrial production facilities. They are used in particular in applications with high demands on real-time capability and transmission reliability. In the context of applications with mobility requirements, such as mobile robots or rotating machine parts, however, they reach their practicable limits. In these cases, wireless communication systems are necessary. In addition to enabling the aforementioned applications, they promise further advantages, such as cost savings through simplified installation. However, the same requirements are placed on wireless systems as on their wired counterparts. This paper structures these requirements' implications on industrial communication systems by deriving four mandatory properties that need to be fulfilled by any communication system for industrial applications. Current commercially available technologies are reviewed with respect to the mandatory properties. Addressing their shortcomings, an overview of current research approaches aiming to improve industrial wireless systems in the automation applications is given.**

***Index Terms*—Industrial Communication Networks, Automation, Machine Type Communication**

I. Introduction

Industrial Ethernet networks (IENs) have long been the backbone of communication in factories. However, the growing complexity of manufacturing processes and the rise of Industry 4.0 necessitate a paradigm shift towards more flexible and adaptable solutions. Therefore, this work explores the potential of wireless industrial communication networks (ICNs) to complement and extend traditional IENs.

Wireless ICNs offer significant advantages, particularly in their ease of deployment. Setting up new facilities or retrofitting existing ones becomes significantly faster and less disruptive compared to wired solutions. This allows for easier integration of additional sensors, enabling real-time monitoring of plant status and facilitating predictive maintenance strategies. Furthermore, wireless ICNs can seamlessly integrate with existing, long-lived IENs, offering the flexibility of independent deployments or seamless network extensions.

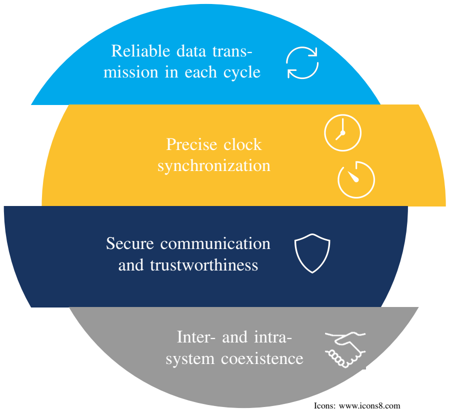
Beyond extending IENs and accommodating mobile production resources, a crucial shift is occurring in communication priorities. Traditionally, high data throughput dominated design considerations. However, industrial applications increasingly prioritize reliability and low latency over raw data rate. This paper emphasizes the need for further research to unlock the full potential of wireless ICNs. In order to achieve this, we highlight the importance of tailoring ICNs to specific industrial applications. Further, we examine the current state of the art in wireless ICN technologies and identify existing gaps and limitations within existing technologies. Finally, ongoing research and standardization efforts are discussed which are addressing these gaps.

II. Properties of Industrial Communication Networks

The desired properties of ICNs originate in the industrial applications they are serving. Consequently, the industrial application has to be analyzed with respect to its requirements. Sec. II-A therefore summarizes how to create application profiles. Then, mandatory properties of ICNs are derived as shown in Sec. II-B. Performance profiling as referred to in Sec. II-C can be a basis to investigate a communication solution's suitability for a specific application profile.

A. Industrial Application Profiling

Industrial applications exhibit diverse requirements, even when restricting the view to those applications which are traditionally handled by IENs. In order to systematically and comprehensively describe their individual requirements, it is crucial to follow a well-defined terminology and provide a complete set of parameters. When defining target use cases for mobile communications, the 3rd Generation Partnership Project (3GPP) distinguishes characteristic parameters and influencing quantities in TS 22.104 [1]. Characteristic parameters are, e.g., transmission time and message loss ratio, while the influencing quantities, e.g., spatial extend, number of wireless devices and their communication behavior. It is necessary to describe the conditions under which the characteristic parameters are required to put the developed requirement profile into perspective. For example, if an automated guided vehicle (AGV) fleet is to be operated, its operating environment might vary broadly (intralogistics, agriculture, mining, etc.).


Reliable data transmission in each cycle
Precise clock synchronization
Secure communication and trustworthiness
Inter- and intra-system coexistence

Icons: www.icons8.com

Fig. 1. Four mandatory properties (MP) of industrial communication.

Besides the quantitative requirements, the qualitative requirements are decisive when it comes to what to apply in a real-world application. Here, e.g., usability, scalability, security of investment and user acceptance are addressed.

B. Deriving Mandatory Properties of ICNs

From the technical point of view, the quantitative requirements are in focus of this paper. Summarizing them, four mandatory properties (MPs) of industrial communication solutions - be them wired, wireless or hybrid - are derived extended from [2] as shown in Fig. 1.

MP1 Reliable data transmission in each cycle – An industrial communication network basically needs to supply a sufficient data rate, which not only covers the application data rate, but also necessary mechanisms to enable the required reliability like forward error correction (FEC) redundancy or retransmissions. The industrial application’s cycle time must be maintained.

MP2 Precise clock synchronization – Distributed clocks located in each device have to be precisely synchronized since each device schedules its sampling points according to its own clock. Basically, there are two possibilities to synchronize these distributed clocks in the network. The first option is to transmit additional packets, the second is to inherently provide the synchronization by the communication system.

MP3 Secure communication and trustworthiness – In converging information and communication technology (ICT) and operational technology (OT) networks and especially wireless networks, securing and authenticating the communication is a prerequisite to their deployment.

MP4 Inter- and intra-system coexistence – Coexistence refers to the industrial applications themselves, which must coexist either within one communication system or using various communication systems. If applications coexist, their requirements are met simultaneously.

C. Performance Profiling

The application profiles described, e.g., in 3GPP TS 22.104, are only one step among several. The methodology is extended in [3] by distinguishing three sets of characteristic parameters and influencing quantities: One set describing the requirements, one set recording the assurance of the communication network and a third set determining the current state of a communication network. Consequently, the characteristic parameters required by an application, the assured ones during planning an ICN and the ones measured during its operation could be quantitatively compared. It is important to mention that often, even in the application profiles in 3GPP TS 22.104 [1], it remains unspoken that the values refer only to describing the requirements. They do not imply an assurance or measured 5G performance profile.

In performance profiling, the same comprehensive parameter set, the assured or measured characteristic parameters are described. It is crucial to stick to the same parameter set as only then the application and performance profile are comparable. A key condition to ensure comparability is the use of the same reference interface, i.e., the interface the characteristic parameters refer to. This means that both application and requirement profile have to refer, for example, to the interface closest to the application device, since comparing user-perceived data rate to physical data rate is not reasonable. Again, it needs to be stressed that the requirements originate from the industrial application. When planning performance testing, at first a check of to what extent the MPs are met helps to decide which solutions of which technologies to submit to a performance test.

A methodology for conducting comprehensive performance tests from an industrial application’s perspective is described in guideline VDI/VDE 2185-4 [4] and, relating to 5G but universally applicable, in 5G-ACIA’s white paper on performance testing [5]. Example results of performance tests following these guidelines can be found in [6] for PROFINET over Bluetooth, while in [7] a 5G system was subjected to testing.

III. State of the Art

This section will present commercially available solutions and examine their capabilities with respect to the four MPs derived in Sec. II. In a second step, we will look at what has been launched in this respect in the standardization process and will thus find its way into commercially available products in the foreseeable future. The landscape of wireless systems can be roughly divided into three areas, as shown in Fig. 2: Cellular systems, short range devices (SRDs) such as wireless local area networks (WLANs) and Bluetooth, and low power wide area networks (LPWANs). The latter are primarily suitable for massive machine-type scenarios due to their low energy consumption, but on the other hand they do not support real-time communication and are therefore of limited suitability as ICNs for industrial applications. They will therefore not be examined in more detail in the following. Moreover, in the light of recent trends towards convergence, wireless networks offering the simultaneous support of multiple applications with diverse requirements are of increasing interest. Due to this, the latter focuses on cellular communication, i.e., 5G Release 15, and Wi-Fi based on IEEE 802.11 as both technologies promise a sophisticated resource management with diverse traffic classes.

A. Cellular Communication Systems

A key feature of cellular communication systems is the use of licensed and thus exclusive frequency bands, so that sources of interference can be eliminated at least from a regulatory point of view. The previous tie to a mobile communications provider

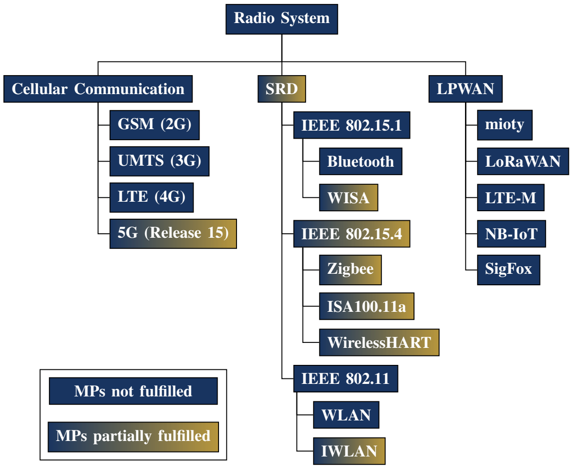


Fig. 2. Commercially available solutions and their fulfillment of the MPs.

is being relaxed with 5G, which makes cellular systems a more cost-efficient solution. Current research is already focusing on the sixth generation of mobile communications (6G), whose commercial introduction is expected around 2030 [8]. With regard to industrial communications, the main issue in this context is to ensure a high degree of backward compatibility in order to protect investments made in 5G technologies and long life cycles. 6G should continue the current trend toward open interfaces and scalable architectures. To this end, machine learning (ML) methods in particular will also be investigated to enable intelligent self-management. For industrial applications, the latency must be reduced below the target of 1 ms [1]. Energy and cost efficiency must also be increased in the process. To achieve this, it is also planned to supplement the network with sensory capabilities, for example for high-precision localization, so that an infrastructure also offers other functionalities in addition to communication. With regard to the four mandatory properties derived in Sec. II-A, cellular communication systems can be evaluated as follows:

1) MP1 - Reliable data transmission in each cycle: Even though 5G initially placed a major focus on enhanced mobile broadband (eMBB) applications, i.e., especially on high data rates, foundations were also laid for industrial radio communications through new numerologies with shorter symbol lengths and transmission time intervals (TTIs) for shorter latencies or modulation and coding schemes (MCSs) with extremely low block error rates (BLERs) [9] for high reliability. The latter can also be enhanced by redundant transmission of duplicated packets (5G Rel. 15).

2) MP2 - Precise clock synchronization: Initial time-sensitive networking (TSN) functionalities have been supported by 5G since Rel. 16, so that end-to-end synchronization can be ensured and transparent communication at ICN level is thus in principle realizable. In the standardization of Rel. 17, these functionalities are extended and improved, for example by correcting propagation delays.

3) MP3 - Secure communication and trustworthiness: With 5G, more and more countries are issuing licenses for local frequency bands in order to enable self-hosted campus networks. With this it is assured, that critical infrastructure can be deployed operator independently and thus allowing for more trustworthiness and data privacy. Radio equipment and service authentication can be achieved by standard 3GPP functionalities based on, e.g., eSIM. Data protection of transmitted messages in form of confidentiality and integrity protection is however typically not enabled.

4) MP4 - Inter- and intra-system coexistence: In addition to coverage via a mobile network provider, local 5G networks can also be operated independently (or hybrid). A key advantage here over traditional mobile communications is that edge cloud servers are very close to the devices in this case, resulting in lower latencies. With 5G, also the concept of network slicing was introduced to cellular communications. Thereby, services can operate on different network slices, which are separated logical networks on the same shared infrastructure. Each slice can be tailored to the application’s needs by assigning appropriate resources and does not interfere with other services thanks to the logical isolation.

B. IEEE 802.11 - Wireless Local Area Networks

Just like cellular radio, IEEE 802.11 is undergoing a development, which was traditionally characterized by a striving for higher data rates [10]. Wi-Fi 6 (IEEE 802.11ax) brought a paradigm shift in this area. While the maximum data rate makes only a relatively small leap compared to previous generations, Wi-Fi 6 primarily emphasized higher efficiency and flexibility. With regard to the four MPs derived in Sec. II-A, IEEE 802.11 can be evaluated as follows:

1) MP1 - Reliable data transmission in each cycle: Significantly relevant for industrial applications is the extension of quality of service (QoS) management to include a dedicated category for deterministic, low-latency, and reliable communications to prioritize such traffic. In addition, Wi-Fi 7 (IEEE 802.11be) is expected to include the ability to use multiple connections in parallel to increase data rates or improve reliability.

2) MP2 - Precise clock synchronization: The achievable wireless time synchronization in a Wi-Fi network depends on the messaging scheme of the synchronization protocol, the timestamping technique, and the specific wireless conditions. The timestamping technique is the strongest limiting factor in synchronization performance. The IEEE 802.11 standard defines two messaging schemes, timing measurements (TM) and fine timing measurements (FTM). The timestamping technique can be software (SW) or hardware (HW). SW timestamps provide low performance, while HW timestamps reach synchronization levels in the order of 10 ns to 40 ns. Although wireless propagation phenomena pose a significant limitation to the synchronization level that can be achieved, the current performance is sufficient to meet the performance targets of wireless TSN [11].

3) MP3 - Secure communication and trustworthiness: Within IEEE 802.11 based technologies, the implementation of an authentication system such as IEEE 802.1X is left to the network operator or user. Due to scalability and security reasons, consumer oriented solutions such as pre-shared key (PSK) are not applicable within industrial scenarios. However, privacy and trustworthiness can be achieved due to the absence of third parties such as network providers. Data transmissions on the radio interface are secured by standard cipher suites such as advanced encryption standard (AES) including confidentiality, integrity and replay protection. Due to latency and real-time requirements of the data traffic, the cipher mode should be counter mode in order to prevent deciphering delays due to out-of-order receptions.

4) MP4 - Inter- and intra-system coexistence: With the introduction of OFDMA (orthogonal frequency-division multiple access), radio resources can be allocated on a very fine-granular basis in both the downlink and the uplink, which is particularly advantageous for a larger number of devices and small packet sizes. The allocation of resources (scheduled access), which was previously known mainly from mobile communications, also helps to avoid collisions between different transmissions. In addition, multiple antennas at transmitters and receivers are now also used in the uplink. This provides even more flexibility in the simultaneous connection of multiple devices by exploiting spatial diversity, allowing them to use eight spatially separated data streams - so-called spatial streams (multi-user multiple input multiple output, MU-MIMO). This functionality was reserved for the downlink in previous Wi-Fi versions. In the upcoming Wi-Fi 7 standard, the plan is to further extend the above innovations and thus flexibility [12]. That is, devices can now be assigned more than one radio resource at a time, as well as a wider channel bandwidth (up to 320 MHz). In addition, 16 spatial streams are now available. Finally, an expected major innovation is the coordination between different access points (APs). This can be used to avoid collisions or increased latency between the devices of different APs, to distribute loads or to switch access from one AP to the next as seamlessly as possible.

C. Off-the-shelf Industrial Wireless Systems

There are already various approaches for the use of wireless communication systems in industrial environments. In general, standardized wireless systems from the consumer sector are used, i.e., Bluetooth and WLAN-based systems in particular. For PROFINET, for example, IEC 61784-1 specifies requirements for the use of these two technologies. The firmware is often adapted to industrial requirements and conditions, and modified media access methods, e.g., in iWLAN, and WIA-FA (based on IEC 62948) are used. Problems arising from passive and active environmental conditions are countered with antenna arrangements such as directional antennas, leaky waveguides or slotted waveguides. Siemens uses its Scalance 5G routers and security appliances with virtual extensible LAN (VXLAN) transmission technology to facilitate real-time transmission of PROFINET IO data for industrial applications via a private 5G network. For process automation, various standards are available that use components of the IEEE 802.15.4 (LR-WPAN) standard, such as IEC 62591 (WiHart) or IEC 62601 (WIA-PA). In addition, solutions based on the IEEE 802.15.1 or Bluetooth standard also exist, such as WISA or IO-Link.

IV. State of Research and Open Issues

Research has already been carried out on the above-mentioned topics in relevant current research projects, and initial results have been achieved.

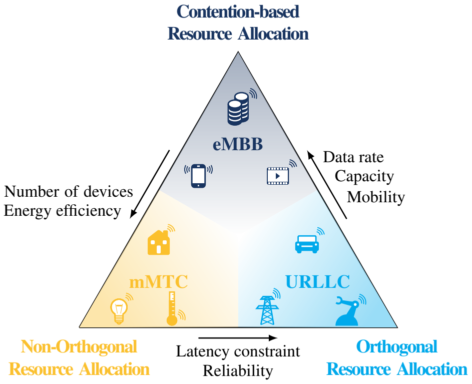


Fig. 3. Different service classes and suitable resource allocation strategies

A. Latency

As defined in MP1, data has to be transmitted within each cycle time, leading to a requirement on the allowed latency. Since cycle times may vary (see Sec. II-B) for different applications, the latency requirements also differ. Latency is induced in practically every part of the (wireless) communications system. It occurs as processing, queuing, transmission, and propagation delays. Whereas some of these components are almost constant for a specific system, e.g., the ones resulting from the numerology or processing functions, others are probabilistic and can vary a lot. For instance, queuing or scheduling delays depend on the network load and re-transmissions of lost packets randomly result from bad channel conditions. As such random behavior may harm latency bounds and is not desired, not only the absolute value of the latency, but also its determinism is crucial. Because latency always occurs as a byproduct of a certain component, it cannot be treated separately but is always a constraint that needs consideration in all the aspects discussed in the following subsections.

B. Multiple Access

As has been shown so far, the use of wireless systems in industrial environments requires that the multiple access method supports real-time communication. For this purpose, it is necessary that the user separation takes place through the exclusive allocation of orthogonal resources and thus a determinism is guaranteed with regard to the timing of the resource allocation. The performance of standardized and some medium access control (MAC) schemes considered in the current research with respect to industrial use cases has already been investigated in the literature [13]. In the future, industrial network subscribers will not only depend on a single service, but will rely on several services simultaneously. Consequently, there is a greater requirement for wireless technologies to support inter- and intra-system coexistence to ensure seamless performance and efficiency of multiple services, cf. Sec. II-A. The ITU generally distinguishes between three different classes of services: enhanced mobile broadband (eMBB), ultra-reliable low latency communications (URLLC) and massive machine type communications (mMTC). These classes all have their own unique requirements for the multiple access method used. While a technical solution is known to support each service class alone, see Fig. 3, it is still a technological challenge to support more than one service class at a time in the same radio system.

Hybrid MAC protocols based on CSMA-based common code systems and methods based on partially overloaded spreading sequences [14] have been investigated to enable simultaneous support of different classes of services.

In high-density industrial environments, relying solely on orthogonal resources is found to be ineffective and insufficient. To address this challenge, non-orthogonal multiple access (NOMA) has emerged as a promising solution. NOMA adopts a superposition technique at the transmitter to send multiple service messages, while successive interference cancellation (SIC) is used at the receiver to separate these messages. However, achieving optimal performance with NOMA requires careful power allocation to support two or more users, and this is an area of active research. A recent publication proposed a NOMA scheme that follows a service-based approach is [15].

Mao et al. introduced rate-splitting multiple access (RSMA) to exploit spatial diversity in wireless communication systems [16]. The RSMA method divides the transmitted messages into two parts: a common part and a private part. The common part is encoded using superposition coding, which is similar to the approach used in NOMA, while the private part uses spatial division to transmit messages to different users. As a result, the receiver needs to have separate radio channels to demodulate the signals and separate the original messages.

Both NOMA and RSMA utilize SIC. However, it is important to note that SIC can introduce error propagation and delay in the receiver’s structure, which can be counterproductive for an URLLC service.

Further investigation is necessary to understand how infrequent transmission of short packets can be efficiently supported by NOMA and RSMA. Additionally, the use of ML algorithms to enable multiple access through learned resource allocation structures is a promising research direction, as suggested in a previous study [17].

C. *Reliability*

Many of the considered applications will pose high or extremely high requirements on the reliability of wireless communications. In order to achieve this, diversity has to be exploited. Due to the strict latency requirements, spatial and frequency diversity are preferred over redundancy in the time domain. As for the diversity in space, different propagation paths of the transmitted signal will be utilized by employing multiple antennas. Frequency diversity utilizes the fact that the destructive superposition of different propagation paths are dependent on the frequency. This can be exploited by transmitting with a large bandwidth (e.g. through spread spectrum techniques or multi-carrier wave forms), simultaneous transmissions on different frequencies (multi-connectivity) and the pseudo-random or smart frequency hopping.

Multi-connectivity is already employed in standards, e.g., as packet duplication [18] for mobile communications. However, simply duplicating the same information, which is also called selection combining, is far from the most efficient transmission scheme. More elaborate approaches are studied in the literature, employing the more sophisticated maximal-ratio combining (MRC) or joint decoding (JD). For instance, the authors in [19] provide an analytical framework to study the performance of the different schemes for Rayleigh fading channels. Those results were later validated in [20] trough simulations for a WLAN physical layer (PHY). Finally, in [21], it was investigated whether it should be employed on PHY or on MAC, with conclusions depending on the signal-to-interference-plus-noise ratio (SINR) and network load.

However, even though approaches like MRC or JD significantly increase the efficiency of multi-connectivity, they still multiply the required number of radio resources for each device by the number of utilized links. In other words, multi-connectivity decreases the spectral efficiency by this factor. Thereby, the system capacity will be reduced allowing for fewer devices, which limits the application in industrial scenarios. This issue can be addressed in systems, which have high bandwidth or multiple frequencies available, but do not assign several resources to each device in parallel, and rather let the devices switch between them. Concepts like frequency hopping or resource allocation are well known, but studies regarding high reliability through an adaptive assignment of resources appeared only recently and rarely. For instance, the authors in [22] proposed and studied a frequency hopping scheme in order to reduce burst errors for periodic and deterministic communications. In [23], the authors even employed a predictor that estimates the quality of the available resources in order to optimally allocate them to the devices.

Finally, time diversity may also be utilized by employing suitable channel coding. However, the codes have to meet high requirements. On one hand, they have to achieve extremely high reliability, while still having a low and deterministic processing time on the other hand. Digital fountain codes are known to be able to serve these requirements and deliver promising performance for channels with significant erasure properties, which are expected in the industrial environment. For this purpose, the wireless channel exhibiting bit error characteristics must first be transformed into an erasure channel by a suitable inner coding. This mandatory concatenated coding raises the question of the choice of the ideal operating point in terms of code rates, which has already been investigated in the literature [24]. Typically, this has been investigated with a view to maximum throughput, i.e., for very large packet sizes. The work in [25] instead focuses on the application of rateless coding in industrial environments, and thus in the context of very short packets. The extent to which the application of rateless coding in this context provides benefits in terms of packet error rate has been investigated.

D. *Synchronization of Distributed Application Clocks*

In wired ICNs, i.e., IENs such as PROFINET or Sercos III, the data exchange is organized in fixed and invariant cycles. The controller of the IEN generates messages with fixed transmission intervals, e.g., 1 ms. The transmission and processing times are deterministic since the network topology and the message routing are, once engineered, invariant. As a consequence, each device is able to adjust its local clock to the controller’s clock with an accuracy of $< 1\,\mu s$ using the reception time stamp [26]. At a specified point in time called global sampling point (GSP) the current measured values are recorded and the last received control parameters are adopted.

In [2] and [27], key challenges of distributed clock synchronization for ICN were identified with respect to clock synchronization in a wireless communication system.

The first challenge of nondeterministic timing behavior arises from inherent properties of wireless communication. The propagation delay is variable, since the distance between two communication participants can vary, whereas the wire length is fixed in wired networks. Unlike wired networks, the wireless interface can be easily overheard, i.e., encryption and authentication is mandatory, see Sec. IV-E. Also, the wireless interface is prone to interference leading to a higher error probability, i.e., sophisticated FEC mechanisms are necessary. Both security and FEC mechanisms take typically a varying amount of time, which renders them additional sources of nondeterminism.

Especially in cascaded, hybrid ICNs, which combine wireless and wired networks, clock synchronization poses a sophisticated challenge [28]. This is even worsened, if the communication cycles of the different subnetworks are not synchronized, resulting in a large variance in transmission time [7]. In order to tackle this, [2] analyzes the degrees of freedom of wireless ICN with respect to providing a precise synchronization inherently by the ICN itself. It is concluded that processing times have to be deterministic and the best result would be reached when the wireless ICN has the master clock. Based on this recommendation, [29] investigates the impact of scheduling within a hybrid ICN.

Other approaches are based on messaging protocols to synchronize the distributed clocks: precision time protocol (PTP) in accordance with IEEE 1588 [30] and TSN, especially time synchronization as specified in IEEE 802.1AS-2020 [31].

E. Security and Resilience

Existing wireless solutions can typically only be partly exploited for industrial radio applications or have to be completely redesigned due to the special demands and QoS requirements as outlined in Sec. II. Compared to wire-based systems, there is particular risk of cyber attacks due to the open nature of the wireless channel. Network security has therefore to be considered during the design process of wireless ICNs. Therefore, possible security solutions for wireless ICNs are proposed in the following after deriving requirements respectively.

Due to the sensitive application payloads transmitted on the interfaces of wireless ICNs, security measures are required in order to prohibit any active or passive attacks. One of the primary security goals is therefore the confidentiality, integrity and availability (CIA) triad. Further, authenticity is another important requirement. In order to ensure these requirements, a trust anchor is needed in form of an authentication framework which manages the access of users. In order to protect the transmitted information from passive cyber attacks, confidentiality protection has to be applied. Integrity and authenticity is further needed in order to prohibit active cyber attacks. Prior, secure exchange of cryptographic material is required. The flexible configuration of wireless ICNs should be possible in order to ensure resilience, i.e., addition or replacement of user devices should be easily possible without any interruptions in service. Further, the configuration of wireless ICNs should fulfill the requirements of low costs and high usability simultaneously. Automated routines, e.g., for user authentication and revocation, are required. Additionally, resource and energy efficiency have to be optimized and the solutions need to be ICN technology-agnostic.

Within state-of-the-art technologies, only a subset of the security requirements is typically met. Most ICN technologies provide a variety of security features such as secure message transmission, device authentication, and key management. However, several drawbacks are still existing in the current protocol versions, respectively. Some technologies, e.g., provide simplified mechanisms for user authentication such as passphrase or PIN (e.g., WPA2-PSK within IEEE 802.11, Bluetooth). This is mainly due to the primary application area in consumer scenarios of these technologies. Within wireless ICNs, there is however typically a higher number of user devices and such solutions do not scale well. Several technologies provide functionalities such as device management schemes, e.g., within IEEE 802.1X or LoRaWAN Join Server. The deployment of such functionalities requires, however, advanced knowledge and skilled personnel or third-party support since it is left to the owner or operator of the network. This is in conflict with the industrial radio security requirement of high usability and low cost. In order to overcome that issue, PKI based solutions for industrial radio have been proposed. These enable automated authentication routines (e.g., Plug&Trust protocols) [32]. Further, secure and efficient message transmission on wireless interfaces can be enabled by physical layer security (PhySec) techniques [33] and optimized cipher algorithms for this purpose [34].

Secure message transmission is a critical issue within industrial radio systems due to the possibility of cyber attacks as mentioned above. Cryptography-based solutions, however, have drawbacks due to challenging QoS requirements especially in URLLC applications (e.g., latency and resource efficiency). Therefore, alternative solutions can be provided by PhySec, e.g., physical layer authentication (PLA). Herein, physical characteristics of the wireless channel are evaluated for the purpose of message integrity (e.g., man-in-the-middle (MitM) attack prevention) and authenticity (e.g., spoofing attack prevention) [33]. Further, customized cryptographic implementations can be utilized for security functionalities which cannot be implemented using PhySec. E.g. for confidentiality protection, latency-optimized ciphers can be utilized.

To make the wireless ICN resilient, not only the aforementioned traditional threats must be addressed, but also other potential adverse events need to be considered. For instance, such events comprise the impact of natural disasters, blackouts, or jamming attacks on the spectrum in addition to the cyber attacks described before. A resilient system should maintain essential functionalities as far as possible, initiate safe modes, mitigate the threat, and recover as soon as possible. A major challenge here is to provide a holistic concept instead of a patchwork of single solutions for individual aspects [35].

V. Conclusion

This paper explored the potential of wireless ICNs for automation applications. The ideal wireless ICN would seamlessly extend existing wired networks while functioning independently

– a prospect with substantial economic benefits. However, achieving this ideal remains a technological hurdle. Current wireless systems offer advantages, but limitations exist. Cellular solutions excel in wide-area coverage and mobility, but latency and cost can be drawbacks. Conversely, Wi-Fi boasts high data rates and low latency, ideal for real-time applications within smaller, cost-sensitive environments. However, Wi-Fi’s limited range and susceptibility to interference hinder its suitability for larger industrial settings.

This analysis underscores the need for continued exploration of wireless ICNs. While current solutions offer opportunities to expand the range of supported applications, particularly challenging industrial scenarios may still necessitate specialized radio systems. The emergence of tailored 5G mobile communication reflects the growing importance of industrial applications in wireless networking, and further research is crucial to unlock the full potential of wireless ICNs in the automation landscape.

Acknowledgment

This work has been funded by the Federal Ministry of Education and Research of the Federal Republic of Germany (contract numbers 16KIS1010K, 16KIS1011, 16KIS1012 and 16KIS1013, Industrial Radio Lab Germany). The authors alone are responsible for the content of the paper.

References

[1] 3GPP, “ETSI TS 122 104 V17.7.0 (2022-05) 5G; Service requirements for cyber-physical control applications in vertical domains (3GPP TS 22.104 version 17.7.0 Release 17,” Tech. Spec. TS 22.104 V17.7.0, 2022.

[2] L. Underberg *et al.*, “Towards hybrid wired-wireless networks in industrial applications,” in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 2018, pp. 768–773.

[3] G. Cainelli, O. Albert, and L. Underberg, “Specification of future wireless communication systems and 6G for industrial automation - how to consider the time and error behaviour of the communication and its constraints?” *2022 European Conference on Networks and Communications (EuCNC)*, 2022.

[4] VDI/VDE, “Radio-based communication in industrial automation - metrological performance rating of wireless solutions for industrial automation applications,” Guideline, 03 2019.

[5] 5G-ACIA, “Performance testing of 5G systems for industrial automation,” 5G-ACIA, White Paper, 2021.

[6] G. Cainelli and L. Underberg, “Performance analysis of Bluetooth Low Energy in hybrid network with PROFINET,” in *2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2021, pp. 01–08.

[7] G. Cainelli, L. Underberg, and L. Rauchhaupt, “Influences of logical link design in 5G campus systems,” *2022 IEEE Future Networks World Forum (FNWF)*, pp. 373–378, 2022.

[8] 5G-ACIA, “Our view on the evolution of 5G towards 6G,” 5G-ACIA, Position Paper, 5 2021.

[9] 5G Americas, “Understanding 5G & time critical services,” 5G Americas, White Paper, 8 2022.

[10] E. Khorov, I. Levitsky, and I. F. Akyildiz, “Current status and directions of IEEE 802.11be, the future Wi-Fi 7,” *IEEE Access*, vol. 8, pp. 88 664–88 688, 2020.

[11] M. K. Atiq *et al.*, “When IEEE 802.11 and 5G meet time-sensitive networking,” *IEEE Open Journal of the Industrial Electronics Society*, vol. 3, pp. 14–36, 2022.

[12] C. Chen *et al.*, “Overview and performance evaluation of Wi-Fi 7,” *IEEE Communications Standards Magazine*, vol. 6, no. 2, pp. 12–18, 2022.

[13] M. Karrenbauer *et al.*, “On industrial MAC protocols: State of the art systems and recent approaches,” *IFAC-PapersOnLine*, vol. 51, no. 10, pp. 40–45, 2018.

[14] ——, “Network slicing in local non-cellular wireless networks: A MC-CDMA-based approach,” in *2018 15th International Symposium on Wireless Communication Systems (ISWCS)*. IEEE, 2018, pp. 1–5.

[15] N. Bulk *et al.*, “Equidistant power allocation for a service-based NOMA scheme,” in *27. VDE-ITG-Fachtagung Mobilkommunikation (MKT’23)*, Osnabrueck, Germany, May 2023.

[16] Y. Mao *et al.*, “Rate-splitting multiple access: Fundamentals, survey, and future research trends,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2073–2126, 2022.

[17] S. Gracla, C. Bockelmann, and A. Dekorsy, “A multi-task approach to robust deep reinforcement learning for resource allocation,” in *International ITG 26th Workshop on Smart Antennas and 13th Conference on Systems, Communications, and Coding*, Feb 2023.

[18] 3GPP, “Technical specification group radio access network; evolved universal terrestrial radio access (E-UTRA); study on small cell enhancements for E-UTRA and E-UTRAN – higher layer aspects (rel. 12),” TR 36.842 V1.0.0, 11 2013.

[19] A. Wolf *et al.*, “How reliable and capable is multi-connectivity?” *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1506–1520, 2019.

[20] N. Schwarzenberg *et al.*, “Quantifying the gain of multi-connectivity in wireless LAN,” in *2018 European Conference on Networks and Communications (EuCNC)*, 2018, pp. 16–20.

[21] M.-T. Suer *et al.*, “Comparison of multi-connectivity schemes on different layers for reliable low latency communication,” in *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2021, pp. 1357–1362.

[22] J. Gebert and A. Wich, “Alternating transmission of packets in dual connectivity for periodic deterministic communication utilising survival time,” in *2020 European Conference on Networks and Communications (EuCNC)*, 2020, pp. 160–164.

[23] A. Traßl *et al.*, “On the outage probability of channel prediction enabled max-min radio resource allocation,” in *IEEE Wireless Communications and Networking Conference (WCNC)*, Austin, USA, Apr 2022.

[24] C. R. Berger *et al.*, “Optimizing joint erasure-and error-correction coding for wireless packet transmissions,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4586–4595, 2008.

[25] M. Karrenbauer *et al.*, “A Study on the Application of Rateless Coding in Non-Cellular MIMO Systems for Machine-Type Communication,” *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 8243–8248, 2020.

[26] S. Dietrich *et al.*, “Performance indicators and use case analysis for wireless networks in factory automation,” in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2017, pp. 1–8.

[27] D. Krummacker *et al.*, “Intra-network clock synchronization for wireless networks: From state of the art systems to an improved solution,” in *2020 2nd International Conference on Computer Communication and the Internet (ICCCI)*. IEEE, 2020, pp. 36–44.

[28] J. von Hoyningen-Huene *et al.*, “Comparison of wireless gateway concepts for industrial real-time-communication,” in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2016, pp. 1–4.

[29] S. Dietrich *et al.*, “Optimized resource allocation for cascaded communication networks in factory automation,” in *2018 IEEE International Conference on Industrial Technology (ICIT)*, 2018, pp. 1616–1621.

[30] “IEEE standard for a precision clock synchronization protocol for networked measurement and control systems,” *IEEE Std 1588-2019 (Revision of IEEE Std 1588-2008)*, pp. 1–499, 2020.

[31] “IEEE standard for local and metropolitan area networks–timing and synchronization for time-sensitive applications,” *IEEE Std 802.1AS-2020 (Revision of IEEE Std 802.1AS-2011)*, pp. 1–421, 2020.

[32] A. Weinand, M. Karrenbauer, and H. D. Schotten, “Security solutions for industrial radio systems,” in *3rd IFSA Winter Conference on Automation, Robotics & Communications for Industry 4.0 / 5.0 (ARCI’ 2023), Chamonix-Mont-Blanc, France*, Feb 2023.

[33] A. Weinand *et al.*, “Naïve Bayes supervised learning based physical layer authentication: Anti-spoofing techniques for industrial radio systems,” in *18th International Conference on Cyber Warfare and Security (ICCWS), Towson (MD), USA*, Mar 2023.

[34] C. Bockelmann *et al.*, “HiFlecs: Innovative technologies for low-latency wireless closed-loop industrial automation systems,” in *22. VDE-ITG-Fachtagung Mobilkommunikation*, May 2017.

[35] P. Smith *et al.*, “Network resilience: a systematic approach,” *IEEE Commun. Mag.*, vol. 49, no. 7, pp. 88–97, 2011.