A Cross-Layer Survey on Secure and Low-Latency Communications in Next-Generation IoT

Marco Martalò, *Senior Member, IEEE*, Giovanni Pettorru, and Luigi Atzori, *Senior Member, IEEE*

***Abstract*—The last years have been characterized by strong market exploitation of the Internet of Things (IoT) technologies in different application domains, such as Industry 4.0, smart cities, and eHealth. All the relevant solutions should properly address the security issues to ensure that sensor data and actuators are not under the control of malicious entities. Additionally, many applications should at the same time provide low-latency communications, as in the case for instance of remote control of industrial robots. Low latency and security are two of the most important challenges to be addressed for the successful deployment of IoT applications. These issues have been analyzed by several scientific papers and surveys that appeared in the last decade. However, few of them consider the two challenges jointly. Moreover, the security aspects are primarily investigated only in specific application domains or protocol levels and the latency issues are typically investigated only at low layers (e.g., physical, access). This paper addresses this shortcoming and provides a systematic review of state-of-the-art solutions for providing fast and secure IoT communications. Although the two requirements may appear to be in contrast to each other, we investigate possible integrated solutions that minimize device connection and service provisioning. We follow an approach where the proposals are reviewed by grouping them based on the reference architectural layer, i.e., access, network, and application layers. We also review the works that propose promising solutions that rely on the exploitation of the QUIC protocol at the higher levels of the protocol stack.**

***Index Terms*—6G, Internet of Things (IoT), industrial IoT (IIoT), privacy, security, low latency, QUIC.**

I. Introduction

NEXT-GENERATION communication systems are promoting even higher spectral and energy efficiency, lower latency, and more massive connectivity, especially to satisfy the requests of the ever-increasing numbers of deployed Internet-of-Things (IoT) devices. By 2030, sixth-generation (6G) wireless networks aim at providing performance 10-100 times better than that of fifth-generation (5G) networks, i.e., peak data rates of at least 1 Tb/s, user-experienced data rates of 1-10 Gb/s, over-the-air latency of 10-100 μs, and connectivity of up to 10^7 devices/km^2 [1]. Thanks to these advancements, IoT devices are predicted to reach 25 billion by the year 2025 according to the most reliable predictions [2]. The resulting IoT is seen as one of the main key enablers for vertical applications in next-generation wireless systems [3].

The huge amount of IoT devices being deployed, as well as 6G enabling technologies, will lead to several advanced services, such as multi-modal traffic management, environmental monitoring and control, virtual/augmented reality, telemedicine, autonomous driving, drone communications, etc. [4]. One of the most interesting applications where next-generation communication networks will be predominant is that of Industry 4.0 [5], where traditional manufacturing processes are automated and empowered by means of Industrial IoT (IIoT)-based solutions. In particular, factory productivity will be boosted thanks to (among other functionalities) the collection and analysis of real-time data to enable (centralized and decentralized) factory control and automation [6]. Illustrative examples of relevant industrial use cases are the food supply chain, transportation and logistics, and workplace safety [7]. Several IIoT frameworks exist and are characterized by various characteristics, such as the pursued objectives, the devised architectural and technical solutions, the target application, and their market. A deeper analysis of the most up-to-date relevant frameworks is given in [8].

IIoT solutions are characterized by two main issues. On the one hand, communications have to be protected as very often sensitive data is carried out throughout public networks together with several data flows to which malicious nodes may also have access. As an illustrative example, IoT devices monitoring a machine in an industrial plant producing highly innovative devices with secret procedures can transmit data containing sensitive parameters describing the operations performed by the machine itself. An attacker may intercept this data and glean relevant industrial secrets. On the other hand, communications may have stringent latency requirements for proper plant functioning. As another example, remote control on industrial robots requires the human operator to instantly receive the stimuli that are generated in the industrial plant to react accordingly; additionally, plant monitoring and predictive maintenance require the exchange of data in a few milliseconds, so that the machines can properly work without any

Manuscript received 14 June 2023; revised 11 December 2023, 13 March 2024, and 10 April 2024; accepted 10 April 2024. Date of publication 17 April 2024; date of current version 21 August 2024. The work of Marco Martalò was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union, NextGenerationEU. The work of Giovanni Pettorru was supported by M.D. 351, National Recovery and Resilience (NRRP) funded by the European Union, NextGenerationEU. This work was also partially supported by the Italian Ministry of Enterprises and Made in Italy (MIMIT), within the 5G technology support program, on axis 1 "House of Emerging Technologies" (CTE), Project Name "Cagliari Digital Lab" (ID: G27F22000040008). The associate editor coordinating the review of this article and approving it for publication was H. Habibi Gharakheili. *(Corresponding author: Marco Martalò.)*

The authors are with the Department of Electrical and Electronic Engineering, University of Cagliari, 09124 Cagliari, Italy, and also with the Research Unit of Cagliari, Consorzio Nazionale Interuniversitario per le Telecomunicazioni, 43124 Parma, Italy (e-mail: marco.martalo@unica.it; giovanni.pettorru@unica.it; l.atzori@unica.it).

Digital Object Identifier 10.1109/TNSM.2024.3390543

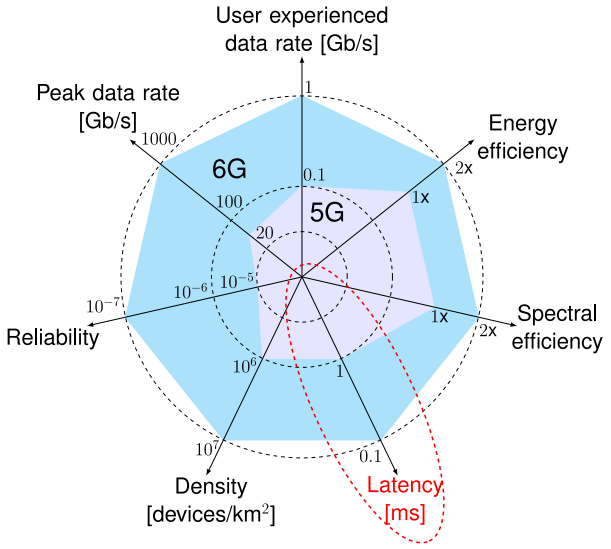

Fig. 1. Improvement of the 6G requirements with respect to those in 5G networks. A particular highlight is given on the latency aspects.

undesired stop. The two requirements may be in contrast, in the sense that adding security features to a communication typically leads to a longer delay. However, these need often to be jointly addressed.

Moreover, the advent of future 6G technologies would open innovative applications and services with much more stringent requirements than actual 5G networks, as graphically illustrated in Fig. 1.

In particular, to successfully deploy delay-sensitive real-time applications (such as mixed reality or tactile Internet) end-to-end latency should be improved, as highlighted by the red dashed ellipse, by an order of magnitude. To this end, proper delay management should be performed in all the transmission components in wireless and wireline links, as well as in the computation procedures at both client and server side [9]. In this context, the impact of such stringent latency requirements on the security workflows has to be considered to guarantee sufficient service quality of service. This poses the question of a radical change in the overall architecture, as well pointed out in [10], [11].

According to [10], [11], the requirements on latency and security are then considered to be two of the most critical ones for the future successful deployment of IoT applications for the benefit of society. In particular, secure-by-design network architectures should not be obtained at the price of an increased latency [12]. The focus of this survey is, therefore, the analysis of the literature dealing with security and latency requirements in IoT scenarios enabled by 5G and beyond (e.g., 6G) network architectures, such as IIoT [13]. Therefore, we refer to next-generation IoT as the next-generation IoT-enabled 6G technologies [14]. These have been analyzed by several scientific papers and key surveys that appeared in the last decade with the intent of reviewing the reached advancements (see, e.g., [10] and references therein). However, as it is clarified in Section II, the previous literature focuses on security in specific application domains or protocol levels. Moreover, the latency issues are typically investigated only at low layers (e.g., physical, access, and network) and not together with the security aspects. With the intent to address this shortcoming, this survey provides a complete examination of the technical solutions that could address both requirements as demanded by most of the future solutions in the field. To do so we follow an approach where the proposals are reviewed by grouping them based on the reference architectural layer, i.e., access, network, and application layers.

The rest of this survey is structured as follows. In Section II, we illustrate the survey perspective through the methodological approach we have followed in our review, a summary of the state of the art in terms of surveys touching the security or low-latency issues in IoT, and the description of the reference scenario. In Section III, we focus on secure and low-latency communications at the access layer. In Section IV, we extend the analysis to the routing layer. In Section V, the application layer is considered. In Section VI, we discuss novel solutions, that recently appeared in the literature and based on QUIC protocol, for combining the two aspects. Finally, concluding remarks are given in Section VII. A list of the acronyms used throughout the manuscript is given in Table I to make easier the reading.

TABLE I
LIST OF USED ACRONYMS (IN ALPHABETICAL ORDER)

Acronym	Definition
AMQP	Advanced Message Queuing Protocol
CoAP	Constrained Application Protocol
CHLO	ClientHelLO
CPS	Cyber-Physical System
D2D	Device-to-Device
DDoS	Denial of Service
DNS	Domain Name System
IDS	Intrusion Detection System
IoMT	Internet of Medical Things
IIoT	Industrial Internet of Things
MEC	Mobile Edge Computing
MitM	Man-in-the-Middle
MQTT	Message Queue Telemetry Transport
NOMA	Non-Orthogonal Multiple-Access
OCF	Open Connectivity Foundation
PUF	Physically Unclonable Function
QoS	Quality of Service
RAN	Radio Access Network
REJ	REJect
RFID	Radio Frequency IDentification
RPL	Routing Protocol for Low power and lossy network
RTT	Round Trip Time
SDN	Software-Defined Networking
SHLO	ServerHelLO
TLS	Transport Layer Security
URLCC	Ultra-Reliable and Low-Latency Communications

II. PROPOSED SURVEY PERSPECTIVE

A. Methodological Approach of the Survey

From a bibliometric point of view, our approach is characterized by the following aspects. The main search database is IEEE Xplore, supplemented by the analysis of other databases such as Elsevier, ACM, and MDPI, where papers were selected according to keywords, impact and publication dates. In particular, the related surveys and general topics were filtered by keywords *security*, *IoT*, *5G*, *6G*, and *low-latency*. Surveys

TABLE II
COMPARATIVE ANALYSIS OF SURVEYS DEALING WITH SECURITY AND LOW-LATENCY COMMUNICATIONS

Topic	Year	Reference	Considered technology and contribution
Security	2019	[15]	New security threats and challenges in IoT
		[16]	Authentication, access control, data protection, and trust in IoT networks
	2020	[18]	Security threat classification in innovative IoT architectures
		[22]	Security requirements and challenges in Fog-assisted IIoT
		[25]	Secure architectures in mobile IoT
		[26]	Anomaly detection in IoT time series
	2021	[17]	Honeypots and honeynets in IoT, IIoT, and CPSs
		[20]	Privacy threats and countermeasures for Edge-assisted IoT
		[21]	Security threats and privacy vulnerabilities in different IoT platforms
		[23]	Integration of blockchain in Edge- assisted IIoT
		[27]	Differential privacy for IIoT
		[28]	Lightweight cryptographic protocols for IoT
		[29]	Reinforcement learning algorithms for security in IoT
	2022	[19]	Public encryption for Cloud-assisted IoT
		[24]	Blockchain in Edge-assisted IoT for security and forensics management
	2023	[30]	Deep reinforcement learning algorithms for security in IoT
Low-latency communications	2019	[33]	URLLC in IIoT applications
	2021	[31]	URLLC in 6G-enabled UAV networks
		[32]	Emerging technologies and applications in 6G
		[36]	MEC in 5G for URLCC
		[38]	Deep learning for URLCC in 6G
		[40]	Clustered IoT network architectures for low-latency data collection and routing
	2022	[4]	Emerging technologies and applications in 6G IoT
		[35]	Transmission techniques for 5G RAN
		[39]	URLCC, resource allocation, and traffic management in IoT
		[41]	Operating modes to achieve low-latency by means of RPL
	2023	[34]	Artificial intelligence for tactile Internet IoT
		[37]	MEC resource allocation in 5G and beyond

are filtered on the publication date starting from 2019. When a specific level of the protocol stack is analyzed (as explained in Section II-C, we have divided the analysis into three architectural layers), specific keywords were added, such as:

- *URLLC*, *resource allocation*, *physical layer security*, and *edge computing* (access layer);
- *routing*, *clustering*, and *data collection* (network layer);
- *lightweight cryptography*, *blockchain*, *Physically Unclonable Function*, and *certificateless* (application layer).

For each level of the protocol stack, only a few representative papers (published from 2019 on) are considered. These have been selected to cover all the proposed approaches that characterize the analyzed layer. In each case, we included IEEE Xplore articles with the highest impact, while for works in other sources, priority was given to the most recent considered and innovative studies. The final part of the survey, where the novel QUIC-based solutions for IoT are presented, is based on *QUIC IoT* as the reference search string. In this case, the literature review starts once more with the IEEE Xplore database, and then other databases from other publishers have been considered by looking at recent works in the corresponding fields. Note that the survey discussion is more focused on journal papers rather than conference ones; in particular, the former category contains almost three times the number of references than the latter one.

B. Review of Related Survey Works

Several surveys exist in the literature focusing on either security or latency issues, with specific attention to a small part of the protocol stack. Most of such surveys cover the topics separately, even if a few study the problem jointly. However, the picture is always limited to a few layers of the protocol stack. A comparative analysis of these works is presented in Table II, where the major focus has been highlighted. These are briefly summarized in the following.

Regarding security, the peculiar IoT features make it vulnerable to new threats and introduce novel challenges with respect to more *traditional* Internet applications [15]. In [16], a deep literature review on security aspects of IoT is proposed, focusing on four main security aspects, namely: authentication, access control, data protection, and trust.

From an architectural point of view, in [17] the main approaches related to the use of honeypots and honeynets as defense mechanisms, complementary to Intrusion Detection Systems (IDSs), for IoT, IIoT, and Cyber-Physical Systems (CPSs) are surveyed. The authors of [18] introduce an optimized and simplified IoT architecture, supported by a new classification of security threats and attacks aligned to the proposed framework. The use of privacy and security in Cloud/Edge/Fog-assisted IoT architectures is of interest in several works. In [19], public encryption mechanisms for Cloud-assisted scenarios are deeply analyzed. In [20], privacy threats and corresponding countermeasures are considered for Edge-assisted scenarios. Different IoT platforms across diverse application domains are examined in [21], with particular attention given to the analysis of security threats and privacy vulnerabilities. Security requirements and challenges in Fog-assisted IIoT networks are investigated in [22]. The integration of blockchain technologies into Edge-assisted IIoT networks is the topic discussed in [23]. Blockchain with Edge-assisted IoT networks is also considered in [24] with a focus on security and forensics management aspects. An overview of different

methods and technologies to provide a secure architecture to mobile IoT is provided in [25].

From a data processing point of view, anomaly detection in IoT is the topic analyzed in [26]. In particular, the authors investigate different signal processing methods to identify anomalies in sensor time series, which may be due to cyber-physical attacks. Another possible efficient approach is differential privacy, whose use is surveyed in [27]. Efficient cryptographic methods are an essential ingredient to provide privacy and security in IoT resource-constrained devices. A deep analysis of the topic is given in [28]. A cutting-edge research area in this field is related to the application of methods based on artificial intelligence. One of the key solutions is the use of reinforcement learning for efficient defense against attacks in IoT scenarios, as surveyed in [29], [30].

Low-latency communications have been also reviewed in several works, typically limiting the analysis to technologies working at lower levels of the protocol stack (physical, access, and network). In [4], the main technologies for IoT-enabled 6G networks are analyzed. Among all, massive Ultra-Reliable and Low-Latency Communications (URLLC) are discussed as expected to support future IoT services, e.g., the timely and highly reliable delivery of massive data for facilitating remote healthcare or automating mission-critical processes in smart factories. The application of URLLC for flying objects is well-investigated in [31]. Another survey using an approach similar to that in [4] is [32], where the authors shed light on the main applications (IoT, virtual reality, and tactile Internet) which can benefit of URLLC. The investigation outlined in [33] focuses on a specific application, highlighting the critical role of URLLC in aligning with the evolution and requirements of the IIoT. The use of artificial intelligence to enable tactile Internet services in next-generation wireless systems is the scope of the survey in [34].

Other specific radio access technologies to achieve low-latency communications are reviewed in other surveys; the most important are the following: [35] focuses on network slicing in 5G Radio Access Network (RAN), [36], [37] shed light on the use of Mobile Edge Computing (MEC), and [38] analyzes the use of deep learning techniques. In [39], latency issues in a wireless IoT environment are investigated at lower-intermediate levels of the protocol stack, e.g., physical, Medium Access Control (MAC), and network layers, and the main related technologies are discussed. Low latency from the routing and data collection point of view is also an interesting topic and has been analyzed in several works. For instance, in [40] clustered architectures are reviewed to achieve such a goal in IoT networks. In such a survey, security issues are also discussed. In [41], the operating modes of the Routing Protocol for Low power and lossy network (RPL), which is a reference protocol for secure and low-latency routing in IoT, is reviewed. Even if [40], [41] cover both topics as in this paper, their analysis is limited to clustering methods and, therefore, to the network level, as discussed in Section IV.

C. Reference Scenario

The reference scenario for our analysis is illustrated in Fig. 2.

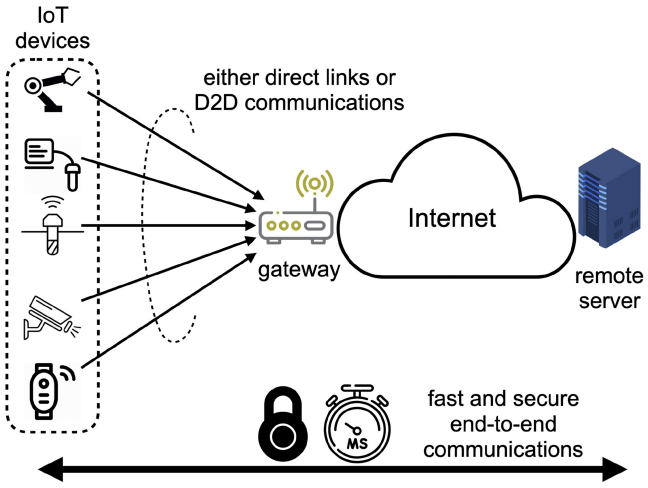

Fig. 2. Reference scenario for the proposed analysis.

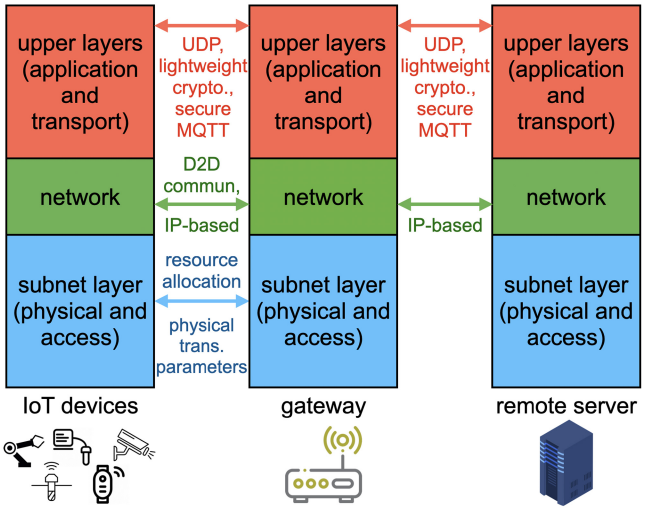

Fig. 3. Protocol stack of the communications envisioned in the reference scenario. For each layer, the main characteristics are highlighted.

It represents an IoT network populated by several (possibly heterogeneous) devices that cooperate to monitor the status of an environment of interest, e.g., an industrial plant in IIoT applications. The IoT devices are resource- and energy-constrained and have to communicate with a remote server hosting the service or application which also provides the user interface. Communications from the IoT devices to the remote server pass through an IoT gateway.

From an architectural point of view, secure low-latency communications are required at all the layers of the protocol stack, as highlighted in Fig. 3.

At the subnet layer (i.e., physical and access), the communications between the IoT devices and the gateway represent the most challenging in terms of latency and security. Herein, the appropriate setting of the physical transmission parameters and of resource allocation are the issues of major interest. Less stringent issues are encountered in the server-gateway communications which are assumed to rely on a high-capacity backbone network. At the network layer, lightweight Internet Protocol (IP)-based solutions are typically investigated for secure and low-latency communications. At

the upper (transport and application) layers, several security solutions may be applied, whereas lightweight communications are guaranteed by means of simple protocols, such as User Datagram Protocol (UDP), Message Queue Telemetry Transport (MQTT), and Constrained Application Protocol (CoAP).

As previously highlighted, low latency and security issues have been analyzed by several scientific papers and key surveys that appeared in the last decade. However, few of the existing surveys consider the two challenges jointly. Moreover, the security aspects are primarily investigated only in specific application domains or protocol levels, whereas latency is typically investigated only at low layers (e.g., physical and access). The goal of this survey is, instead, to provide a bottom-up comprehensive overview of these aspects in IoT networks at all possible levels of the architectural stack. For each architectural level, we provide an overview of the most relevant recent solutions. In particular, we start from the problem at the access layer, e.g., from the sensors to the sink (or gateway). Then, we move to analyze the problem at the network level that requires the design of proper routing strategies. Finally, we consider the higher levels (i.e., transport and application). A similar approach is partially pursued in [42], where a few considerations on security at different levels of the protocol stack are applied, which however does not consider the requirement of low-latency communications as we do in this survey.

Moreover, as an illustrative example for the reference scenario, we analyze the emerging application of the new transport layer protocol QUIC [43], initially designed and implemented by Google for Web applications, which is gaining more and more attention in the IoT community to provide fast and secure communications. The major key features are related to the fact that it works over UDP but still adopts a connection-oriented approach with a short connection setup of only 1 RTT, which significantly reduces the overall latency. Additionally, in this short connection setup timeframe, the two end-points are able to set up secure communications thanks to preshared keys which are then replaced soon by the final ones.

The choice of QUIC as a promising IoT solution to jointly address the challenges of security and low latency in the upper layer is supported by a growing literature. Our analysis of the main databases shows a clear trend: while in 2018-2019, about 33 papers were published on this topic, the following years 2020-2021 showed a remarkable increase, with almost 60 papers available, corresponding to a growth of 81.81%. Furthermore, from 2022 to the present, the number increased to 209 papers, representing a significant increase of 243.33% compared to the previous two years. Finally, in recent years, standardization efforts for QUIC have accelerated, culminating in the publication of RFC 9000 in May 2021. QUIC standardization efforts extend beyond IoT to include areas such as multimedia communications through initiatives such as the Media Over QUIC IETF working group.[1] Even if QUIC is treated in Section VI as an emerging topic in the field of secure and low-latency IoT communications, the authors are aware that it is not the only solution. Therefore, references to other alternative approaches at the application layer are introduced in Section V.

[1]https://datatracker.ietf.org/wg/moq/documents/

TABLE III
CATEGORIZATION OF TRANSMISSION AND ACCESS METHODS FOR SECURE AND LOW-LATENCY IOT NETWORKS

Topic	Low latency	Security
Optimization of the transmission parameters	[44]–[48]	–
Messaging compression in medium access	[49]–[51]	–
Optimization of resource allocation	[52]–[55]	–
Optimization of resources in Fog/Edge computing	[56], [57], [66]	[64], [65]
Physical layer IoT security	[61]	[58]–[61]
Secure resource allocation	–	[62], [63]
Trust management in the Cloud/Edge/MEC	–	[64], [65]

Fig. 4 shows the considered logical flow and the survey organization, together with the main considered topics.

As one can observe, several topics are recurrent among the different layers, such as trust management, analysis of network topologies, and the exploitation of different architectural solutions (Fog/Edge/MEC and Cloud). Moreover, the security mechanisms analyzed at the upper layers are also at the basis of the integration of security services at the other (lower) levels.

III. SECURE AND LOW-LATENCY ACCESS IN IOT

The network access layer is responsible for giving users reliable access to the communication medium and for defining the transmission techniques (including modulation format and channel coding) to allow users to transmit at the highest speed possible. At this level, URLLC is one of the key enablers of innovative services envisioned in 5G networks and beyond.

The major proposed approaches deal with either reducing latency or improving security, whereas very seldom these two aspects are treated jointly. These can be categorized as follows (as also highlighted in Fig. 5):

1) low-latency communications
   - optimization of the transmission parameters at the physical layer;
   - enhancement of medium access strategies by either compressing messaging or optimizing resource allocation, mostly about the following scenarios: random/centralized access, Non-Orthogonal Multiple-Access (NOMA), Fog/Edge computing;
2) secure communications
   - physical layer IoT security;
   - improved resource allocation for secure access;
   - trust management in Cloud/Edge/MEC access.

The analyzed works are summarized in Table III according to the above categorization and are briefly reviewed in the following.

The low latency constraint in URLLC services is often formulated together with also the reliability and decoding

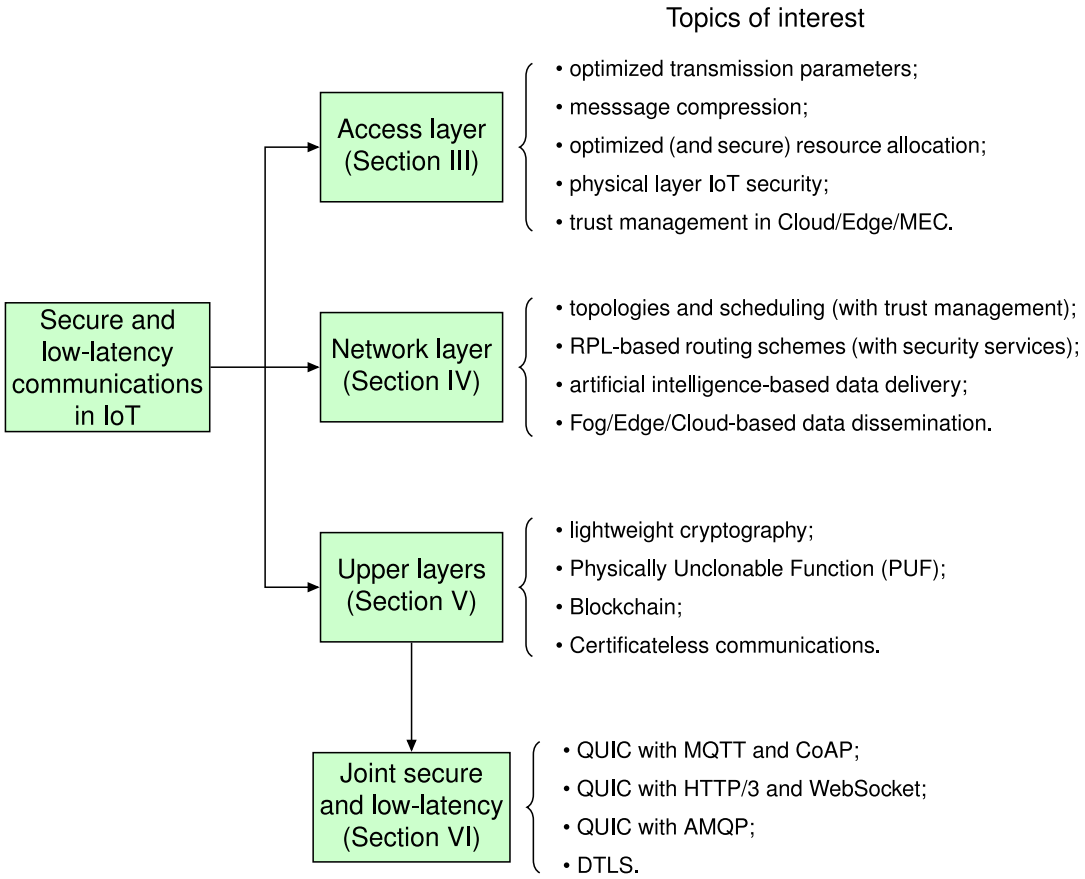

Fig. 4. Survey logical flow and organization.

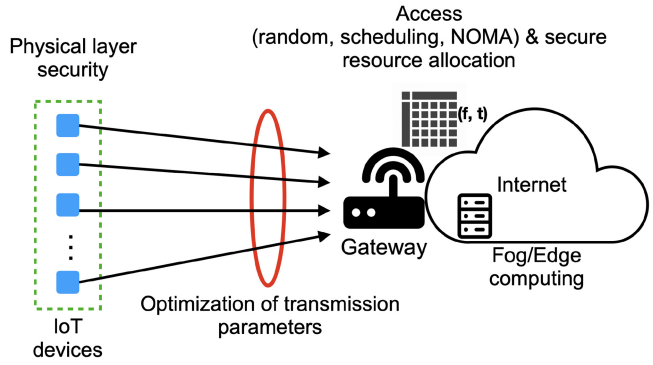

Fig. 5. Access scenarios in IoT networks with main approaches for low latency and security highlighted.

complexity and achieved through the optimization of the transmission parameters. The optimization may focus on setting several parameters, such as: the combination of *transmission rate* and *transmission power* [44], [45], the *spreading factor* in LoRa networks [46] and the *retransmission parameters* in Automatic Repeat-reQuest (ARQ) or Hybrid ARQ (HARQ) scenarios [47]. The formulation of the mentioned constraints is found to be a major challenge in this context, especially in terms of latency that has to consider the achievable error rate [44]. A key question of such transmission schemes is their effective energy efficiency, defined as the ratio between the effective capacity and the required power consumption. The authors in [48] provide a framework for such a quantity under fading environments and finite-blocklength transmissions.

Other solutions work at the medium access level, where the major advancements for latency reduction have been achieved by proposing either *the compression of the messaging* in some relevant medium management procedures or the *optimization of radio resources allocation*. To the first category belongs the paper [49], which, with reference to the Long Term Evolution (LTE), has focused on the random access protocol and proposed the key idea to send the preamble and bandwidth request messages at the same time. This significantly reduces the overall signaling time, which may be crucial in delay-sensitive applications. On the other hand, in [50] the focus is on an enhanced version of the Time Slotted Channel Hopping (TSCH) used for IIoT applications. The key idea is to aggregate more sensor packets in one payload, due to the fact that each of them is typically short. This leads to a significant latency saving, as experimented on tree topology. TSCH can be combined with multiple physical layer technologies (with proper transmission technique selection) to meet stringent latency requirements, as investigated in [51]. To the second category belongs the paper [52], which addresses the joint energy-efficient subchannel assignment and power control in a scenario with massive access requests from IoT devices. Herein, maximizing the network energy efficiency

is a target that guarantees that the latency constraint is fulfilled. The optimization problem is modelled as a multi-agent reinforcement learning problem which is addressed with a distributed cooperative massive access approach. Another modified version of this scheduling method to minimize data gathering latency in IIoT applications is proposed in [53]. A further alternative solution for massive access in IoT networks is given by NOMA, where a user receives a superimposition of the signals of all the other users and then applies proper interference cancellation strategies, thus allowing for increased throughout. In [54], the authors investigate the combined use of NOMA and short packet transmissions to enable URLL services. A similar target is pursued by the authors of [55], who combine NOMA with UAVs to establish a high-capacity IoT uplink network suitable for URLLC applications.

Since Fog/Edge communications, as well as the implementation of MEC in the RAN of 5G/6G networks, are expected to play a key role in providing services with extremely low-latency requirements, a relevant portion of the research community is also investigating URLLC in such contexts. These resources are often used to execute operations that cannot be implemented in devices with limited resources and to avoid involving cloud computing resources which would require high transmission delays. However, how and which operations are assigned may heavily influence on the final latency. Accordingly, *tasks can be partitioned into sub-tasks* (dependent or independent of each other) to be performed at different levels of the network and then merged. The method proposed in [56] can halve the latency with respect to traditional methods where tasks are entirely performed on some portion of the network (either Edge or Cloud). Some solutions rely on the use of *reinforcement learning to offload IoT tasks* to the MEC, such as in [57]. The key point of this approach is to model the MEC subsystems as an acyclic graph on which the task allocation policy determines the graph state transition.

As already highlighted, in all these mentioned articles that dealt with the latency aspects no explicit security enhancements are proposed. Indeed, specific proposals can be found in works that focus on the security aspects only. An important category of solutions is the one that deals with physical layer security, which relies on exploiting the imperfections in the physical layer of the protocol stack, such as noise, interference, and the variation of channel strength in wireless channels [58], [59]. An approach that is often used is to control the pilot subcarriers that are part of an Orthogonal Frequency Division Multiplexing (OFDM) transmission and which are essential for the pilot channel estimation process performed at the receiver. To make the communication secure, their position is changed in a way that is known only by the communicating entities, e.g., following a known probability distribution [60]. Another approach is to adopt a self-interference (SI) assisted encrypted data transmission scheme, where artificial noise and SI cancellation at the controller are used to conceal the randomness brought by the sensors [61]. This last solution has also been devised to keep the latency very low. Another category of work is the one that allocates resources to the end-user in a secure way. In [62], the authors deal with attacks that aim at tracing back along the data stream to capture the source node. Therefore, a counteract action is proposed based on an innovative scheduling algorithm, showing that privacy is preserved with reasonably bounded energy consumption and transmission delay. In [63], resource allocation under short packet transmission to attain secure URLLC in 6G-enabled IoT networks is considered and an analytical framework to evaluate reliability, based on the security rate formula under finite blocklength, is derived. Security in Cloud/Edge/Fog IoT scenarios is of crucial importance, since untrusted users may comprise the overall system performance. To this end, in [64] trust management for effective user authentication and access control in such a scenario is proposed. In [65], instead, trust management and security services in Edge-assisted (low-latency) networks are considered and a blockchain-based architecture is proposed to fulfill such requirements.

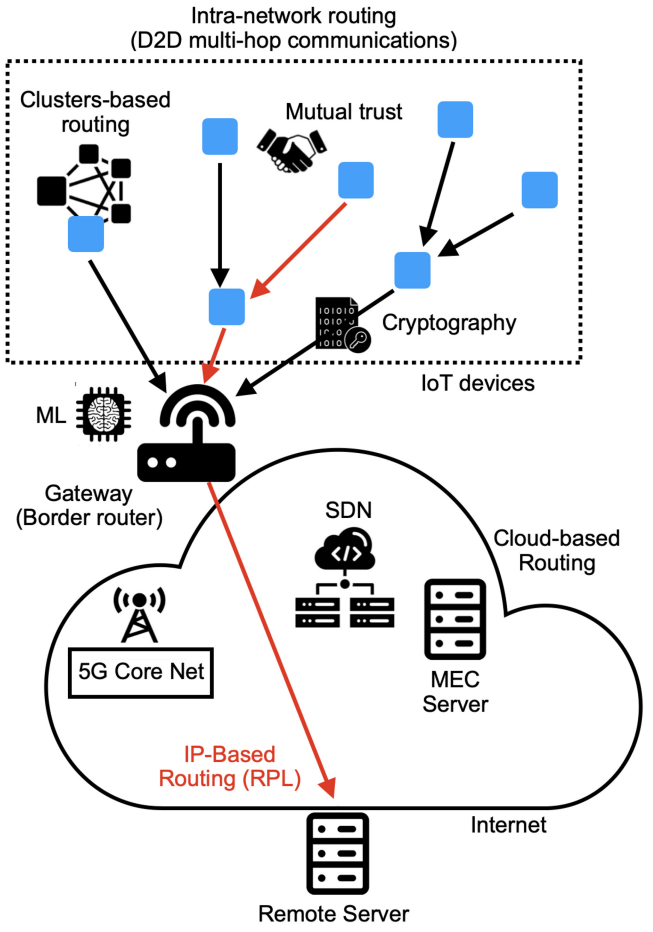

Fig. 6. Routing scenarios in IoT networks with main approaches for low latency and security highlighted.

IV. Secure and Low-Latency Routing in IoT

At the network level, the main performed operation is routing the information towards a destination node, e.g., a sink or a server, possibly exploiting multi-hop communications. We can categorize routing protocols for IoT according to the portion of the network on which they operate, as shown in Fig. 6 and summarized in the following.

TABLE IV
CATEGORIZATION OF ROUTING METHODS FOR SECURE AND LOW-LATENCY IOT NETWORKS

Type of routing	Topic	Low latency	Security
Intra-network	Definition of network topologies and scheduling	[67]–[69]	[67], [80]–[82]
IP-based	Design of RPL-based routing schemes	[71]–[74]	[83]–[92], [94]
Cloud-based	Management of Fog/Edge/MEC architectures	[75]–[79]	[95]

1) Intra-network routing, i.e., communications within the IoT network (between the sensors and the border gateway), where communications can be performed either directly (if allowed by the communication range) or exploiting Device-to-Device (D2D) multi-hop communications.
2) IP-based routing, especially needed in applications requiring to reach a remote server through the Internet.
3) Cloud-based routing, where the Cloud architecture (Fog/Edge/MEC) can be exploited to efficiently route data collected by IoT devices towards a remote server.

In these contexts, the major proposed approaches can be categorized as follows. Note that, unlike the discussion on the access layer in Section III joint low-latency and secure design is often performed at the network layer.

1) low-latency communications
   - definition of dedicated clustered and multi-hop topologies for D2D communications and centralized scheduling algorithms to reduce collisions;
   - design of optimized RPL-based routing schemes for reducing the latency in IP networks;
   - implementation of artificial intelligence schemes in Fog/Edge/MEC architectures to optimize data delivery;
2) secure communications
   - management of trust relationship in network topologies;
   - inclusion of security services, lightweight cryptography, and trust management in RPL-based routing schemes;
   - joint design of secure RPL and Cloud-based architectures for securely disseminating data.

The analyzed works are summarized in Table IV according to the above categorization and are briefly reviewed in the following.

Regarding low-latency communications with intra-network routing, the definition of *dedicated and optimized network topologies*, as well as *data transmission scheduling mechanisms*, is of paramount importance. For instance, cluster-based multi-hop topologies can limit the communication overhead and, therefore, increase the network energy efficiency and reduce the latency in data delivery [67]. The same idea is also exploited in [68], where an enhanced version of the well-established Ad hoc On-demand Distance Vector (AODV) algorithm is designed for clustered network topologies to meet different priority requirements. Transmission scheduling can, instead, reduce collisions caused by multiple information flows, which is a typical IoT characteristic. An example of a paper belonging to this category is [69], where the design of a routing protocol with low latency and high reliability is proposed for IoT devices purely powered by ambient harvested energy.

From the IP-based perspective, the de facto standard for efficient data routing in resource-constrained devices is given by RPL, standardized by IETF with RFC 6550 in 2012 [70]. RPL is a distance vector routing protocol, in which end devices connect to the Internet via border routers. Communications follow bidirectional IPv6 data exchange over a tree-like topology. A comprehensive survey of RPL performance, with particular attention to the impact of users' mobility patterns on (among others) the end-to-end latency, is provided in [71]. Enhancing RPL to further reduce its end-to-end latency is a key solution in the literature. Existing solutions leverage different potential optimizations, i.e., *limiting the RPL overhead* to reduce the impact on the QoS in delay-tolerant applications, as done with HRPL [72], [73], or *explicitly include the latency as a design metric*, as for instance suggested by [74], where a cross-layer fuzzy-based design simultaneously based hop count, energy consumption, latency, and received power is proposed.

From the Cloud perspective, the application of the Software-Defined Networking (SDN) paradigm is also emerging in IoT networks, thus forming the so-called SDN-IoT architecture to meet stringent requirements in terms of low latency and high security. In this context, the latency minimization goal is achieved in a two-fold manner: (i) *introducing artificial intelligence management techniques*, as done in [75] using deep reinforcement learning, or (ii) *exploiting Fog/Edge/MEC capabilities*, as done in [76], [77], [78], [79].

Regarding the security perspective, the integration of mechanisms at different routing levels is typically performed jointly with the design of low-latency solutions. Optimized topologies are secured by managing *trust relationships* between involved nodes, i.e., by performing the classification of malicious behavior of network nodes and allowing nodes with higher trust to communicate, as suggested by [67], [80]. If D2D communications are instead used, access control mechanisms can be considered to secure IoT service provisioning. An example is provided by [81], where an attribute-based access control mechanism is proposed to support secure device discovery with fine-grained access control in IoT-oriented 5G applications. Finally, at the border gateway ML is a powerful tool to manage more complex topologies, such as those induced by the use of blockchain technology and onion routing as a cryptography strategy. An illustrative paper dealing with this strategy is [82], where a ML solution is devised to effectively feed the onion algorithm.

In IP-based routing, different security strategies are possible, see, e.g., [83] and references therein. On one hand, social relationships between network nodes and corresponding trust management can be exploited to route information through a secure path towards the destination, as suggested by [84]. Another relevant approach is that in [85], where trust is exploited in combination with lightweight cryptography to

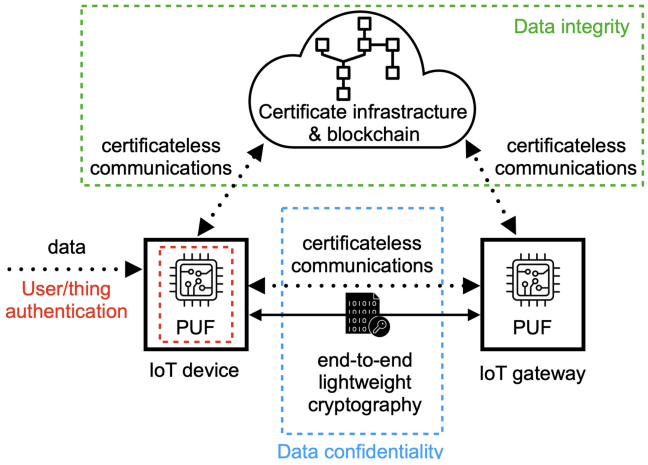

Fig. 7. Security mechanisms in IoT networks at upper layers of the protocol stack.

reduce routing computational complexity and overhead, thus leading to an overall secure and low-latency scheme. On the other hand, if RPL is considered, several threats are possible [86], [87] and, therefore, various secure approaches to counter-act them, either reactive or proactive, can be applied.

In the former, malicious behavior is detected and properly mitigated by avoiding extra overhead and adding simple security mechanisms (e.g., lightweight message authentication and limitation of the forwardable messages). This is effective against topology falsification [88], excessive resource consumption [89], number of exchanged messages [90]. In the latter, instead, the routing protocol is a priori modified to avoid such issues. This can be achieved by integrating trust mechanisms in RPL [91], [92], [93], or by exploiting the secure routing services of RPL itself. The latter solution can be done according to three possible modes [94]: (i) the default unsecured mode, where only the security mechanisms of the underlying datalink layer are applied (if any); (ii) the pre-installed secure mode, where RPL control messages are encrypted with default symmetric cryptography; and (iii) the authenticated secure mode, where the pre-installed cryptography is used by the nodes to join the network, whereas new keys are acquired during network operations. More recently, in [95] the authors leverage the well-known network coding technique over the pre-installed secure mode to obtain a novel secure mode, referred to as chained, which adds sender authenticity to RPL.

V. Secure and Low-Latency IoT at the Upper Layers

At the upper protocol levels (i.e., transport and application), the main goal is to provide end-to-end security mechanisms to provide several security services. To this end, various technologies can be employed, as highlighted in Fig. 7.

In particular, the following security services are of interest in IoT networks at upper levels of the protocol stack:

- *data confidentiality* against eavesdropping and sniffing threats;
- *user/thing authentication* against spoofing threats.
- *data integrity* against tampering threats;

In fact, such networks are prone to Distributed Denial of Service (DDoS) and Man-in-the-Middle (MitM) attacks. A comprehensive survey on this topic is given in [15].

However, the use of security mechanisms to achieve the above-mentioned services typically requires a larger computational complexity caused by the higher number of performed operations, thus leading to increased communication latency. Therefore, significant attention is given by the research community to efficient mechanisms to simultaneously achieve low latency and secure communications in IoT networks. The main approaches in the literature are the following.

1) *Lightweight cryptography*, i.e., encryption/decryption methods based on a small footprint and/or low computational complexity [28]. These schemes are employed in transport layer-supported security protocols to obtain data confidentiality and user/thing authentication. The inherent low computational complexity can empower low-latency communications.
2) *Physically Unclonable Function* (PUF), i.e., a user/thing authentication low-cost solution at the hardware level. In this case, low latency can be achieved using rapid and efficient challenge-response mechanisms.
3) *Blockchain*, i.e., a distributed ledger solution to user/thing authentication and data integrity. A blockchain can coordinate and store information about transactions from a large number of users/devices, as in IoT networks. In this case, the design of consensus algorithms for limiting the transaction delay can empower IoT-enabled applications with sensitive security and latency requirements.
4) *Certificateless communications*, i.e., a message exchange method to distribute the shared secrets needed to provide data confidentiality and user/thing authentication. Since no storing into secure and trusted third-party systems is required, this solves the so-called *key escrow* problem [96]. In this case, low latency can be achieved by properly reducing the number of exchanged messages.

Fig. 7 shows where these mechanisms are applied, i.e., which part of an IoT network employs a specific scheme. We now survey the main characteristics of these approaches that can lead to low-latency communications.

Regarding lightweight cryptography, standard cryptography methods (as in usual Web-based applications) are not always suitable in IoT scenarios, due to the resource-constrained nature of the devices that may not be able to perform the required operations. Moreover, standard cryptographic functions may require more time to process a massive amount of data. To this end, some recent interesting approaches have appeared. A first class of approaches deals with combining simple operations to achieve the desired low complexity requirement and significant savings in memory and power needs. Examples of this approach are in [97], where lightweight hashing is proposed, or in [98], where multiple symmetric key ciphers are coordinated to optimize the decryption delay, which is one of the main sources of the end-to-end latency. A similar combination approach is

pursued in [99], where a 32-bit Feistel-based block cipher is implemented in a multi-stage architecture for data protection using Radio Frequency IDentification (RFID) communications in Internet of Medical Things (IoMT) applications. The other class of approaches to lightweight secure mechanisms foresees a proper interaction with the network infrastructure, i.e., Edge and Cloud. For instance, in [100], a mechanism is proposed for industrial applications where data is stored encrypted in the Edge/Cloud and has to be retried with the so-called keyword search on demand. In [101], a multi-level lightweight security architecture is proposed, where data is split into sensitive or non-sensitive. For each class, a different block encryption method is applied, data is stored in public or private Cloud, and access is granted with different authentication levels according to the different security levels. In [102], lightweight cryptography is proposed for IIoT applications, based on pre-processing to efficiently encrypt and authenticate payload for already established secure connections, thus limiting the experienced latency. Continuing in the area of encryption, a significant and topical issue in the literature is the security of the Domain Name System (DNS) protocol. By default, DNS relies on the exchange of unencrypted queries and responses, making it vulnerable to various attacks. Consequently, the current literature focuses on the incorporation of cryptography in DNS and its adoption in various scenarios, including the IoT [103]. In this context, [104] introduces a lightweight CoAP-based version of DNS that provides security modes for encrypting name resolutions, specifically designed for IoT devices.

Regarding PUF-enabled user/thing authentication, a PUF is a physical object that for a given input and conditions (challenge) provides a physically defined digital fingerprint output (response) that serves as a unique identifier. This is a digital fingerprint that serves as a unique identity for a semiconductor device due to the physical variations that occur during the fabrication process [105]. This method is secure since the probability of replicating the exact challenge-response sequence is very low and the PUF is physically exchanged between the client and the server. However, PUF-based authentication systems may be subject to replay attacks, in which an eavesdropper can intercept the complete sequence and, then, replicate it, e.g., through machine learning algorithms. The low-latency requirement is achieved in the literature in two main ways. First, even if this technology is available in several hardware platforms, e.g., the Xilinx Zynq Ultrascale+, some research is also looking to an optimized system on chip design for IoT applications, see, e.g., [106]. PUF prototyping with the Open Connectivity Foundation (OCF) IoT platform is instead considered in [107], [108]. An alternative low-latency solution from the communication perspective is the design of optimized challenge-response mechanisms, as in [109], where an IoMT scenario is investigated with application to COVID-19 disease. In this context, PUFs are employed to authenticate users (i.e., doctors) and sensor nodes (to avoid spoofed devices in the network) by exchanging a small amount of packets between them. The application of PUFs to IoMT applications for user/thing authentication and corresponding machine learning-based attacks is well-established in the literature, as confirmed by [110], [111]. In [112], low-latency PUF is applied to user authentication in 5G IoT applications, where IoT devices pre-register their challenges which are grouped according to the group identification they belong to. To overcome replay attacks, in [113] the challenge-response exchange is split across multiple sub-packets, and data are properly pre-scrambled and padded in a way only known to the client and the server. Robustness against attacks is the primary concern in [114], where a secure and lightweight IoT device authentication scheme, featuring a two-factor mutual authentication mechanism employing PUFs, is introduced.

User authentication and data integrity employing blockchain is emerging as one of the more popular and more implemented solutions, especially in IIoT applications [115], [116]. The main literature solutions to achieve low-latency communications are based on an efficient interaction (e.g., reduced number of message exchanges per transaction) with the network infrastructure. As an example, in [117], a decentralized, secure, and robust blockchain-based authentication scheme for IoT devices in the network Edge is designed. This scheme is shown to effectively avoid standard single-side faults, due to the distributed characteristics of the architecture. Nodes' trust and data integrity for metrological traceability in a distributed measurement system is considered in [118]. The authors of [119] propose a Blockchain-based IoT platform, prioritizing low computational complexity and low latency for ensuring sensing data integrity. In [120], the latency of private blockchain for IoT applications is deeply investigated, both on small-scale (with a realistic experimental setup with Raspberry Pi 3b+ nodes) and large-scale emulated scenarios, highlighting the contribution of different network parts to the end-to-end latency.

In [121], blockchain technology is integrated with SDN to keep nodes' authentication in IIoT applications. In [122], blockchain is considered to achieve a novel contextual access token method.

Finally, regarding certificateless communications, the research has recently focused on reducing the potentially high message overhead, large computational complexity, and relatively large energy consumption, which are in contrast with IoT requirements. In particular, work in the literature differs for the specific message exchange strategy. As an example, in [123] a lightweight certificateless solution is proposed with reduced overhead, latency, and energy consumption. The rationale behind this protocol is to use two pairs of messages, one for exchanging the cryptography materials and the other to verify the authenticity of the remote party and to establish a unique session key. The effectiveness of this approach is proved on IEEE 802.15.4-compliant networks.

The considered approaches and the corresponding categories are summarized in Table V.

The above analysis has shown that several techniques exist to simultaneously provide security and low latency at the upper layers of IoT scenarios. However, as mentioned in Section II-C, QUIC has recently emerged as one of the protagonists in this area; therefore, we now describe in Section VI in more detail its application to IoT scenarios.

TABLE V
CATEGORIZATION OF APPLICATION-LAYER METHODS FOR SECURE AND LOW-LATENCY IOT NETWORKS

Topic	Data confidentiality	User/thing authentication	Data Integrity
Lightweight cryptography	[28], [97]–[102] [104]	[101], [102] [104]	–
PUF	–	[106]–[114]	–
Blockchain	–	[115]–[122]	[115]–[119] [122]
Certificateless communications	[96], [123]	[123]	–

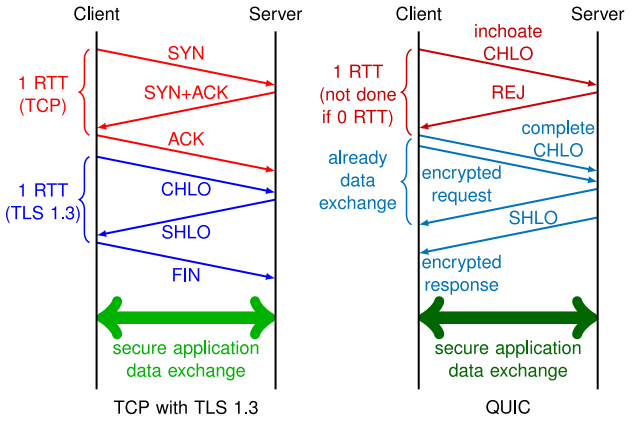

Fig. 8. Protocol message passing for connection establishment and data exchange with TCP+TLS and QUIC.

VI. A RECENT SOLUTION AT THE UPPER LAYERS: INTEGRATING QUIC WITH THE IOT

As already mentioned, typical IoT applications leverage very lightweight protocols to achieve reduced complexity and latency, such as UDP, MQTT, and CoAP. However, when security requirements should be met, such protocols need to be integrated, at the transport layer, with Transmission Control Protocol (TCP) and Transport Layer Security (TLS). However, TCP is based on the well-known 3-way handshaking, so that terminals can exchange data only after 1 Round Trip Time (RTT). To establish a secure connection, TLS 1.2 further takes 2 RTTs, whereas TLS 1.3 takes 1 RTT, leading to an overall TLS/TCP handshake of 3 and 2 RTTs, respectively. Afterward, secure data exchange can occur. This procedure is summarized on the left-hand side of Fig. 8, where the protocol message passing for connection establishment and data exchange with TCP+TLS is shown, where ClientHelLO (CHLO) and ServerHelLO (SHLO) packets are used for key exchange based on standard Diffie-Hellman algorithm.

To reduce this delay, a possible alternative is given by QUIC, which uses UDP as the underlying transport protocol and can establish secure communication in 1 RTT by combining its operations with those of TLS 1.3. In particular, as depicted on the right-hand side of Fig. 8, with QUIC the client initializes the communications with an inchoate CHLO message used to inform the server it wants to communicate with. At this point, in the 1-RTT procedure, the server sends a REJect (REJ) packet to send the ticket needed to authenticate with the client. At this point, the client initializes the key exchange procedure (based on the Diffie-Hellman algorithm) with a complete CHLO and the server responds with a SHLO. In this phase, data can already be exchanged by means of pre-shared keys which are then replaced by the final ones once the complete CHLO-SHLO occurs.

This latency can be further reduced to 0 RTT if the endpoints previously established a communication, so that data can be sent before a new handshake is repeated in 0-RTT packets [43]. In this version, the client skips the preliminary inchoate CHLO and uses the ticket received with the REJ packet during the previous 1-RTT to start authenticating with the server and exchanging data preliminary encrypted with the pre-shared keys. At this point, the complete CHLO-SHLO is performed and the message exchange proceeds as in the previous case.

Finally, since QUIC is based on UDP, it can alleviate typical TPC issues, such as head-of-line blocking and connection migration.

The above-described QUIC solution for secure and low latency at the transport layer is a de facto standard in Web-based scenarios [124], [125], [126]. However, it has been recently considered as a promising solution also for secure and low-latency communications in IoT networks.[2]

An increasing body of literature explores protocols commonly employed in IoT applications, incorporating QUIC at the transport layer to leverage the advantages outlined above. For instance, the authors of [128] present a QUIC-based implementation of MQTT implemented using the GO language. Through extensive experiments conducted on various wired and wireless communication scenarios, the authors demonstrate outstanding results in terms of security and communication latency. A similar experimental methodology is employed in [129], where a practical testbed was created to evaluate the performance of this MQTT version, even under non-ideal channel conditions. Performance evaluation with experimental testbeds may not offer a complete perspective due to dependencies on scenario setup, specific network conditions and device capabilities, impacting the reproducibility of results. To overcome this limitation, many studies are opting for network simulators such as ns-3, thus finding a proper trade-off. This approach is pursued in [130], where the authors use ns-3 to simulate a hybrid scenario. In this configuration, communications between the Cloud and the gateway are protected with standard TLS, while QUIC is used for communications between the gateway and IoT devices. The results not only validate the suitability of QUIC-based MQTT for IoT scenarios, but also demonstrate better performance than the standard version. These results are also confirmed in other works using the same experimental methodology, i.e., in [131], [132].

Originally designed for Web-based applications, the QUIC protocol demonstrates its adaptability not only to the publisher/subscriber model but also, in particular, to the client/server model. In recent studies, researchers have

[2]Note that unfortunately no standard implementation of QUIC exists and several solutions, based on different programming languages, are online available [127].

explored the use of Hypertext Transfer Protocol Version 3 (HTTP/3) with QUIC in IoT scenarios as an alternative to traditional protocols. In [133], the authors compare HTTP/3 and MQTT over QUIC using a testbed consisting of Raspberry Pi Zero devices, evaluating their performance under different network conditions and with different message payloads. Similarly, the work proposed in [134] compares the performance of HTTP-based transactions using QUIC with MQTT and CoAP, highlighting the potential offered by this protocol in lossy and disruptive environments. The literature widely recognizes the advantages of QUIC in terms of communication latency. Consequently, several studies have chosen to examine this protocol using alternative metrics. In [135], the analysis of HTTP/3 focuses on resource consumption, while [136] places more emphasis on security aspects. Moreover, the investigation in [137] focuses on the multipath QUIC extension combined with HTTP/3 to improve the throughput performance of this protocol.

Recently, the integration of other commonly used IoT protocols with QUIC was investigated. In [138], a QUIC-based CoAP version is presented. With respect to other works, in this case, the seamless integration was facilitated by the native UDP support of this application protocol. Similarly, the work proposed in [139] evaluates CoAP over QUIC in an IoT testbed, demonstrating the performance improvement achieved over the standard version. In the study presented in [140], the WebSocket over QUIC protocol is examined, showing its promising performance for IoT applications. In addition, the paper introduces a scheme for session ticket reuse within small-to-medium clusters of IoT devices, with the objective of further minimizing intra-network communication latency. The works [141], [142] propose to integrate QUIC and Advanced Message Queuing Protocol (AMQP) 1.0 to improve the performance of IoT communications in various situations, from simple WiFi and 4G/LTE scenarios to satellite communications.

A different approach from previous studies is that of [143], where the authors explore the possibility of deploying QUIC directly on resource-constrained IoT devices. The investigation focuses on Quant QUIC and the evaluation focuses on several metrics including memory, computation, storage, and energy requirements.

In Table VI, a comparison between the above-discussed works dealing with QUIC in IoT scenarios is presented. The main highlighted characteristics are the considered implementation, the type of work (i.e., simulation-based or experimental), and the application protocol using QUIC as the underlying transport protocol. We believe that it is critical to emphasize these two methodological attributes, as they significantly influence the reproducibility of the results of the work done. These aspects help researchers in the field, enabling them to identify valid research that can then be compared with their QUIC-based proposals.

In summary, leveraging the QUIC protocol presents both significant advantages and disadvantages. On the positive side, QUIC brings notable features for IoT applications, including low latency, TLS1.3 integration for security, adaptability to dynamic network conditions, resilience through path switching, and efficient resolution of head-of-line blocking issues, improving data transmission. However, challenges include potential limited support due to its recent standardization in 2021, leading to interoperability issues, and possible obstacles in certain network environments where firewalls and middleboxes may block or impede traffic.

TABLE VI
COMPARATIVE ANALYSIS OF PAPERS DEALING WITH QUIC-BASED APPROACHES FOR IOT

Paper	Implementation	Type of work	Appl. protocol
[128]	GO	Experimental	MQTT
[129]	GO	Experimental	MQTT
[130]	GO & ns-3	Simulation	MQTT
[131], [132]	GO & ns-3	Simulation	MQTT
[133]	GO	Experimental	HTTP/3 & MQTT
[134]	C	Sim./Exp.	HTTP/3
[135]	GO	Simulation	HTTP/3
[136]	Python	Simulation	HTTP/3
[137]	ns-3	Simulation	HTTP/3
[138]	VPS+	Simulation	CoAP
[139]	GO	Experimental	CoAP
[140]	Python	Experimental	WebSocket
[141], [142]	GO	Experimental	AMQP
[143]	Quant	Experimental	built-in Quant

As a final remark, it is worth mentioning that other transport layer solutions exist as alternatives to QUIC. In particular, one may resort to the specific optimization of the TLS protocol for resource-constrained devices. A standardized solution is given by Datagram Transport Layer Security (DTLS), a datagram-based equivalent of TLS. In this field, an interesting approach is provided in [144], where the authors propose a lightweight version of TLS, referred to as iTLS. The key idea is to dynamically generate secret keys before receiving a server response, allowing clients to send the encrypted data without additional RTT. The protocol is fully compatible with TLS 1.3 and can be easily converted to a DTLS version traffic. Results show that traffic overhead and latency can be reduced by approximately 60%, especially in harsh wireless environments.

VII. CONCLUDING REMARKS

In this paper, we have provided a systematic review of state-of-the-art solutions for providing fast and secure communications in IoT scenarios. In particular, we have focused our analysis on looking at different levels of the protocol stack and categorizing the different approaches to solve the problem according to the specific level they belong to.

Access Layer — At the network access layer, it arises that the two issues of latency and security are treated most of the time separately. Latency is often taken as a constraint that is imposed together with others, e.g., complexity and reliability especially when focusing on URLLC services. While imposing these constraints, the proposed works aim at *optimizing key parameters* such as the transmission rate, the transmission power, the spreading factor, and the retransmission parameters when ARQ/HARQ techniques are adopted. Another way to pave the way to low-latency IoT communications is to enhance the medium access, in particular by *compressing packets* or *optimizing the resource allocation*. The network access functionalities are often supported by the Fog/Edge/MEC

resources whose involvement may affect the latency. For this reason, great attention has also been devoted to the *allocation of tasks and sub-tasks* into which these are properly dived to different levels of the network. Finally, security is separately obtained by *resorting to physical layer techniques* or *securing the resource allocation strategy*. On the other hand, some joint effort between security and low-latency is performed in the realm of using Fog/Edge/MEC resources, that require proper trust management. At this level, the *integration of physical layer security* together with *optimized transmission and medium access parameters*, and Fog/Edge/MEC capabilities represent an interesting future direction for the research community.

Network Layer — At the network level, secure and low-latency routing can be applied using different technologies depending on the considered network part. In this case as well, the two requirements (security and low latency) are typically considered separately. Within the IoT network, the *definition of proper topologies* and *scheduling* is the utmost solution to limit the end-to-end delay in data delivery. However, the definition of such topologies poses crucial security issues that lead to significant research activity on the management of trust relationships among the nodes in the network. When IP-based routing is used, the use of RPL is mostly investigated in the literature, with its *optimization in message exchange* towards low latency or security. Finally, at the network level, the *availability of Fog/Edge/MEC capabilities* is exploited, similarly to the network access layer, to limit the latency. At the network level, an interesting future research direction for the community would be the design of RPL-based schemes that jointly take into account security and low latency requirements.

Upper Layers — At upper levels, i.e., transport and application, different security mechanisms can be applied to inherently guarantee various security services. Since security and low latency are in contrast to each other, all the surveyed mechanisms have, therefore, the common goal to limit the latency, yet guarantee the desired security services. In this survey, we have in particular analyzed four technologies and categorized them according to the specific class of security services they want to achieve. First, the use of *lightweight cryptography*, possibly together with PUF-based key exchange (based on challenge-response methods), can be used for low-latency and low-complexity data confidentiality and integrity, as well as authentication. Moreover, data integrity can be also guaranteed through the application of *Blockchain technologies*, whose latency may be limited by designing specific and optimized per transaction message exchange. Finally, *certificateless communications* are exploited to achieve data confidentiality and authentication and further reduction of the end-to-end latency by resorting to proper message exchange with reduced overhead.

Joint Secure and Low-Latency — We have finally investigated the possible use of integrated solutions to design fast secure network protocols that minimize connection establishment between different devices. In particular, we have focused on the recently appeared use of the *QUIC transport layer protocol* in conjunction with lightweight application layer protocols, such as MQTT, CoAP, or HTTP/3. Since QUIC provides low-latency connection establishment as in TLS 1.3, but uses UDP as the underlying protocol instead of TCP, it can be regarded as a promising solution to the problem of secure low-latency communications. The adoption of QUIC-based communication protocols to a large variety of IoT services in next-generation 6G-enabled networks would represent a key direction for the research community.

REFERENCES

[1] Z. Zhang et al., "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sep. 2019, doi: 10.1109/MVT.2019.2921208.

[2] "Redefine connectivity by building a network to support the Internet of Things," Cisco Syst. Inc., San Jose, CA, USA, White Paper, 2019.

[3] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[4] D. C. Nguyen et al., "6G Internet of Things: A comprehensive survey," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 359–383, Jan. 2022, doi: 10.1109/JIOT.2021.3103320.

[5] H. Kagermann, J. Helbig, A. Hellinger, and W. Wahlster, *Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0: Securing the Future of German Manufacturing Industry; Final Report of the Industrie 4.0 Working Group*. Berlin, Germany: Forschungsunion, 2013.

[6] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on Industrial Internet of Things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018, doi: 10.1109/ACCESS.2018.2884906.

[7] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014, doi: 10.1109/TII.2014.2300753.

[8] C. Paniagua and J. Delsing, "Industrial frameworks for Internet of Things: A survey," *IEEE Syst. J.*, vol. 15, no. 1, pp. 1149–1159, Mar. 2021, doi: 10.1109/JSYST.2020.2993323.

[9] (Samsung Res., Suwon-si, South Korea). *6G: The Next Hyper Connected Experience for All*. Dec. 2020. [Online]. Available: https://cdn.codeground.org/nsr/downloads/researchareas/6G

[10] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

[11] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 281–291, Aug. 2020, doi: 10.1016/j.dcan.2020.07.003.

[12] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, "A survey of blockchain and artificial intelligence for 6G wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2494–2528, 4th Quart., 2023, doi: 10.1109/COMST.2023.3315374.

[13] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of Things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020, doi: 10.1109/ACCESS.2020.2970118.

[14] A. Hussain et al., "A resource-efficient hybrid proxy mobile IPv6 extension for next-generation IoT networks," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2095–2103, Feb. 2023, doi: 10.1109/JIOT.2021.3058982.

[15] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606–1616, Apr. 2019, doi: 10.1109/JIOT.2018.2847733.

[16] E. L. C. Macedo et al., "On the security aspects of Internet of Things: A systematic literature review," *J. Commun. Net.*, vol. 21, no. 5, pp. 444–457, Oct. 2019, doi: 10.1109/JCN.2019.000048.

[17] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for Internet of Things, Industrial Internet of Things, and cyber-physical systems," *IEEE Commun. Surveys Tut.*, vol. 23, no. 4, pp. 2351–2383, 4th Quart., 2021, doi: 10.1109/COMST.2021.3106669.

[18] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors*, vol. 20, no. 13, p. 3625, 2020, doi: 10.3390/s20133625.

[19] H. Xiong, T. Yao, H. Wang, J. Feng, and S. Yu, "A survey of public-key encryption with search functionality for cloud-assisted IoT," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 401–418, Jan. 2022, doi: 10.1109/JIOT.2021.3109440.

[20] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edge-computing-assisted Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4004–4022, Mar. 2021, doi: 10.1109/JIOT.2020.3015432.

[21] L. Babun, K. Denney, Z. B. Celik, P. McDaniel, and A. S. Uluagac, "A survey on IoT platforms: Communication, security, and privacy perspectives," *Comput. Netw.*, vol. 192, Jun. 2021, Art. no. 108040, doi: 10.1016/j.comnet.2021.108040.

[22] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of Industrial Internet of Things security: Requirements and fog computing opportunities," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2489–2520, 4th Quart., 2020, doi: 10.1109/COMST.2020.3011208.

[23] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2300–2317, Feb. 2021, doi: 10.1109/JIOT.2020.3025916.

[24] Z. Liao, X. Pang, J. Zhang, B. Xiong, and J. Wang, "Blockchain on security and forensics management in edge computing for IoT: A comprehensive survey," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 2, pp. 1159–1175, Jun. 2022, doi: 10.1109/TNSM.2021.3122147.

[25] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey," *IEEE Access*, vol. 8, pp. 167123–167163, 2020, doi: 10.1109/ACCESS.2020.3022661.

[26] A. A. Cook, G. Misirli, and Z. Fan, "Anomaly detection for IoT time-series data: A survey," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6481–6494, Jul. 2020, doi: 10.1109/JIOT.2019.2958185.

[27] B. Jiang, J. Li, G. Yue, and H. Song, "Differential privacy for Industrial Internet of Things: Opportunities, applications, and challenges," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10430–10451, Jul. 2021, doi: 10.1109/JIOT.2021.3057419.

[28] M. N. Khan, A. Rao, and S. Camtepe, "Lightweight cryptographic protocols for IoT-constrained devices: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4132–4156, Mar. 2021, doi: 10.1109/JIOT.2020.3026493.

[29] A. Uprety and D. B. Rawat, "Reinforcement learning for IoT security: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8693–8706, Jun. 2021, doi: 10.1109/JIOT.2020.3040957.

[30] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 8, pp. 3779–3795, Aug. 2023, doi: 10.1109/TNNLS.2021.3121870.

[31] A. Masaracchia et al., "UAV-enabled ultra-reliable low-latency communications for 6G: A comprehensive survey," *IEEE Access*, vol. 9, pp. 137338–137352, 2021, doi: 10.1109/ACCESS.2021.3117902.

[32] M. Alsabah et al., "6G wireless communications networks: A comprehensive survey," *IEEE Access*, vol. 9, pp. 148191–148243, 2021, doi: 10.1109/ACCESS.2021.3124812.

[33] M. A. Siddiqi, H. Yu, and J. Joung, "5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices," *Electronics*, vol. 8, no. 9, p. 981, 2019, doi: 10.3390/electronics8090981.

[34] M. Gupta, R. K. Jha, and S. Jain, "Tactile based intelligence touch technology in IoT configured WCN in B5G/6G-A survey," *IEEE Access*, vol. 11, pp. 30639–30689, 2023, doi: 10.1109/ACCESS.2022.3148473.

[35] D. Lopez-Perez et al., "A survey on 5G radio access network energy efficiency: Massive MIMO, lean carrier design, sleep modes, and machine learning," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 653–697, 1st Quart., 2022, doi: 10.1109/COMST.2022.3142532.

[36] K. Jiang, H. Zhou, X. Chen, and H. Zhang, "Mobile edge computing for ultra-reliable and low-latency communications," *IEEE Commun. Stand. Mag.*, vol. 5, no. 2, pp. 68–75, Jun. 2021, doi: 10.1109/MCOMSTD.001.2000045.

[37] A. Sarah, G. Nencioni, and M. M. I. Khan, "Resource allocation in multi-access edge computing for 5G-and-beyond networks," *Comput. Netw.*, vol. 227, May 2023, Art. no. 109720, doi: 10.1016/j.comnet.2023.109720.

[38] A. Salh et al., "A survey on deep learning for ultra-reliable and low-latency communications challenges on 6G wireless systems," *IEEE Access*, vol. 9, pp. 55098–55131, 2021, doi: 10.1109/ACCESS.2021.3069707.

[39] Z. Ma, M. Xiao, Y. Xiao, Z. Pang, H. V. Poor, and B. Vucetic, "High-reliability and low-latency wireless communication for Internet of Things: Challenges, fundamentals, and enabling technologies," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7946–7970, Oct. 2019, doi: 10.1109/JIOT.2019.2907245.

[40] A. Shahraki, A. Taherkordi, O. Haugen, and F. Eliassen, "A survey and future directions on clustering: From WSNs to IoT and modern networking paradigms," *IEEE Trans. Netw. Service Manag.*, vol. 18, no. 2, pp. 2242–2274, Jun. 2021, doi: 10.1109/TNSM.2020.3035315.

[41] A. K. Mishra, O. Singh, A. Kumar, and D. Puthal, "Hybrid mode of operations for RPL in IoT: A systematic survey," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 3, pp. 3574–3586, Sep. 2022, doi: 10.1109/TNSM.2022.3159241.

[42] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

[43] "QUIC: A UDP-based multiplexed and secure transport," Internet Eng. Task Force, RFC 9000, 2022. [Online]. Available: https://datatracker.ietf.org/doc/rfc9000/

[44] H. B. Celebi, A. Pitarokoilis, and M. Skoglund, "A multi-objective optimization framework for URLLC with decoding complexity constraints," *IEEE Trans. Wireless Commun.*, vol. 21, no. 4, pp. 2786–2798, Apr. 2022, doi: 10.1109/TWC.2021.3115983.

[45] J. Zhao and W.-P. Zhu, "Power allocation and scaling law analysis for secured and energy efficient URLLC IoT networks," *Phys. Commun.*, vol. 45, Apr. 2021, Art. no. 101293, doi: 10.1016/j.phycom.2021.101293.

[46] N. Saqib, K. F. Haque, K. Yelamarthi, P. Yanambaka, and A. Abdelgawad, "D2D-LoRa latency analysis: An indoor application perspective," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, New Orleans, LA, USA, 2021, pp. 29–34, doi: 10.1109/WF-IoT51360.2021.9595324.

[47] Q. He, Y. Zhu, P. Zheng, Y. Hu, and A. Schmeink, "Multi-device low-latency IoT networks with blind retransmissions in the finite blocklength regime," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12782–12795, Dec. 2021, doi: 10.1109/TVT.2021.3120145.

[48] M. Shehab, H. Alves, E. A. Jorswieck, E. Dosti, and M. Latva-Aho, "Effective energy efficiency of ultrareliable low-latency communication," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11135–11149, Jul. 2021, doi: 10.1109/JIOT.2021.3052965.

[49] J.-B. Seo, W. T. Toor, and H. Jin, "Analysis of two-step random access procedure for cellular ultra-reliable low latency communications," *IEEE Access*, vol. 9, pp. 5972–5985, 2021, doi: 10.1109/ACCESS.2020.3048824.

[50] C. Michaelides, T. Adame, and B. Bellalta, "ECTS: Enhanced centralized TSCH scheduling with packet aggregation for Industrial IoT," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2021, pp. 40–45, doi: 10.1109/CSCN53733.2021.9686162.

[51] M. Rady, Q. Lampin, D. Barthel, and T. Watteyne, "g6TiSCH: Generalized 6TiSCH for agile multi-PHY wireless networking," *IEEE Access*, vol. 9, pp. 84465–84479, 2021, doi: 10.1109/ACCESS.2021.3085967.

[52] H. Yang, Z. Xiong, J. Zhao, D. Niyato, C. Yuen, and R. Deng, "Deep reinforcement learning based massive access management for ultra-reliable low-latency communications," *IEEE Trans. Wireless Commun.*, vol. 20, no. 5, pp. 2977–2990, May 2021, doi: 10.1109/TWC.2020.3046262.

[53] Y. Tanaka, P. Minet, M. Vucinic, X. Vilajosana, and T. Watteyne, "YSF: A 6TiSCH scheduling function minimizing latency of data gathering in IIoT," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8607–8615, Jun. 2022, doi: 10.1109/JIOT.2021.3118017.

[54] M. R. Amini and M. W. Baidas, "Performance analysis of grant-free random-access NOMA in URLL IoT networks," *IEEE Access*, vol. 9, pp. 105974–105988, 2021, doi: 10.1109/ACCESS.2021.3097553.

[55] R. Karem, M. Ahmed, and F. Newagy, "Resource allocation in uplink NOMA-IoT based UAV for URLLC applications," *Sensors*, vol. 22, no. 4, p. 1566, 2022, doi: 10.3390/s22041566.

[56] M. Feng, M. Krunz, and W. Zhang, "Joint task partitioning and user association for latency minimization in mobile edge computing networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 8108–8121, Aug. 2021, doi: 10.1109/TVT.2021.3091458.

[57] Z. Sun, Y. Mo, and C. Yu, "Graph reinforcement learning based task offloading for multi-access edge computing," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3138–3150, Feb. 2023, doi: 10.1109/JIOT.2021.3123822.

[58] C. Feng and H.-M. Wang, "Secure short-packet communications at the physical layer for 5G and beyond," *IEEE Commun. Stand. Mag.*, vol. 5, no. 3, pp. 96–102, Sep. 2021, doi: 10.1109/MCOMSTD.121.2100028.

[59] S. A. Haider, M. N. Adil, and M. Zhao, "Optimization of secure wireless communications for IoT networks in the presence of eavesdroppers," *Comput. Commun.*, vol. 154, pp. 119–128, Mar. 2020, doi: 10.1016/j.comcom.2020.02.027.

[60] D. Efstathiou, "Flexible physical-layer security for 5G wireless devices," in *Proc. IEEE Int. Mediterr. Conf. Commun. Netw. (MeditCom)*, Athens, Greece, 2021, pp. 342–347, doi: 10.1109/MeditCom49071.2021.9647558.

[61] Z. Ji et al., "Physical-layer-based secure communications for static and low-latency Industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 18392–18405, Oct. 2022, doi: 10.1109/JIOT.2022.3160508.

[62] Y. He, G. Han, M. Xu, and M. Martinez-Garcia, "A pseudo-packet scheduling algorithm for protecting source location privacy in the Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9999–10009, Jun. 2022, doi: 10.1109/JIOT.2021.3117957.

[63] H. Dai, C. Zhang, J. Luo, C. Li, and B. Wang, "QoE-driven resource allocation for secure URLLC in 6G-enabled IoT networks," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2021, pp. 1–5, doi: 10.1109/WCSP52459.2021.9613597.

[64] J. Zhang, T. Li, Z. Ying, and J. Ma, "Trust-based secure multi-cloud collaboration framework in cloud-fog-assisted IoT," *IEEE Trans. Cloud Comput.*, vol. 11, no. 2, pp. 1546–1561, Apr.–Jun. 2023, doi: 10.1109/TCC.2022.3147226.

[65] T. Kumar, M. Ylianttia, and E. Harjula, "Securing edge services for future smart healthcare and Industrial IoT applications," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp.*, Budapest, Hungary, 2022, pp. 1–6, doi: 10.1109/NOMS54207.2022.9789900.

[66] B. Kharel, O. L. A. Lopez, N. H. Mahmood, H. Alves, and M. Latva-Aho, "Fog-RAN enabled multi-connectivity and multi-cell scheduling framework for ultra-reliable low latency communication," *IEEE Access*, vol. 10, pp. 7059–7072, 2022, doi: 10.1109/ACCESS.2022.3142430.

[67] Y. Zhang, Q. Ren, K. Song, Y. Liu, T. Zhang, and Y. Qian, "An energy efficient multi-level secure routing protocol in IoT networks," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10539–10553, Jul. 2022, doi: 10.1109/JIOT.2021.3121529.

[68] M. Adil et al., "enhanced-AODV: A robust three phase priority-based traffic load balancing scheme for Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14426–14437, Aug. 2022, doi: 10.1109/JIOT.2021.3072984.

[69] R. V. Prasad, V. S. Rao, C. Sarkar, and I. Niemegeers, "ReNEW: A practical module for reliable routing in networks of energy-harvesting wireless sensors," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1558–1569, Sep. 2021, doi: 10.1109/TGCN.2021.3094771.

[70] "RPL: IPv6 routing protocol for low-power and lossy networks," Internet Res. Task Force, RFC 6550, 2012. [Online]. Available: https://datatracker.ietf.org/doc/rfc6550/

[71] B. Safaei et al., "Impacts of mobility models on RPL-based mobile IoT infrastructures: An evaluative comparison and survey," *IEEE Access*, vol. 8, pp. 167779–167829, 2020, doi: 10.1109/ACCESS.2020.3022793.

[72] N. H. M. Yusoff, N. A. Zakaria, A. Sikora, and E. J. Sebastian, "6LoWPAN protocol in fixed environment: A performance assessment analysis," in *Proc. IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl. (IDAACS)*, vol. 2, 2019, pp. 1142–1147, doi: 10.1109/IDAACS.2019.8924283.

[73] N. H. M. Yusoff, N. A. Zakaria, A. Sikora, and E. J. Sebastian, "HRPL protocol for 6LoWPAN smart home system: A performance assessment analysis," in *Proc. IEEE Int. Symp. Smart Wireless Syst. (IDAACS-SWS)*, Dortmund, Germany, 2020, pp. 1–5, doi: 10.1109/IDAACS-SWS50031.2020.9297079.

[74] K. A. Darabkh, M. Al-Akhras, and A. Khalifeh, "Improving routing protocol for low-power and lossy networks over IoT enviroment," in *Proc. Wireless Opt. Commun. Conf. (WOCC)*, Taipei, Taiwan, 2021, pp. 31–35, doi: 10.1109/WOCC53213.2021.9603069.

[75] X. Guo, H. Lin, Z. Li, and M. Peng, "Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6242–6251, Jul. 2020, doi: 10.1109/JIOT.2019.2960033.

[76] R. K. Das, N. Ahmed, F. H. Pohrmen, A. K. Maji, and G. Saha, "6LE-SDN: An edge-based software-defined network for Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7725–7733, Aug. 2020, doi: 10.1109/JIOT.2020.2990936.

[77] S. U. R. Malik, T. Kanwal, S. U. Khan, H. Malik, and H. Pervaiz, "A user-centric QoS-aware multi-path service provisioning in mobile edge computing," *IEEE Access*, vol. 9, pp. 56020–56030, 2021, doi: 10.1109/ACCESS.2021.3070104.

[78] V. Karagiannis, P. A. Frangoudis, S. Dustdar, and S. Schulte, "Context-aware routing in fog computing systems," *IEEE Trans. Cloud Comput.*, vol. 11, no. 1, pp. 532–549, Jan.–Mar. 2023, doi: 10.1109/TCC.2021.3102996.

[79] K. Alatoun, K. Matrouk, M. A. Mohammed, J. Nedoma, R. Martinek, and P. Zmij, "A novel low-latency and energy-efficient task scheduling framework for Internet of Medical Things in an edge fog cloud system," *Sensors*, vol. 22, no. 14, p. 5327, 2022, doi: 10.3390/s22145327.

[80] A. Sheikh, S. Kumar, and A. Ambhaikar, "A secure trust-based routing framework for improving the QoS of Internet of Things based networks," in *Proc. Int. Conf. Comput. Commun. Technol. (ICCCT)*, 2021, pp. 149–154, doi: 10.1109/ICCCT53315.2021.9711865.

[81] R.-H. Hsu, H.-S. Fan, and L.-C. Wang, "SGD^2: Secure group-based device-to-device communications with fine-grained access control for IoT in 5G," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Fukushima, Japan, 2021, pp. 1–8, doi: 10.1109/DSC49826.2021.9346250.

[82] R. Gupta, N. K. Jadav, A. Nair, S. Tanwar, and H. Shahinzadeh, "Blockchain and AI-based secure onion routing framework for data dissemination in IoT environment underlying 6G networks," in *Proc. Int. Conf. Smart Cities, Internet Things Appl. (SCIoT)*, Mashad, Iran, 2022, pp. 1–6, doi: 10.1109/SCIoT56583.2022.9953671.

[83] A. Gupta and T. Sasikala, "Secure routing protocols for MANET-enabled IoT," in *Proc. IEEE Int. Conf. Mobile Net. Wireless Commun. (ICMNWC)*, 2021, pp. 1–4, doi: 10.1109/ICMNWC52512.2021.9688553.

[84] X. Li, H. Qi, and J. Wu, "Node social nature detection OSN routing scheme based on IoT system," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 14048–14059, Aug. 2022, doi: 10.1109/JIOT.2022.3145379.

[85] A. Kore and S. Patil, "Reliable and secure data transmission in smart Healthcare application of Internet of Things," in *Proc. IEEE Bombay Sect. Signat. Conf. (IBSSC)*, 2021, pp. 1–6, doi: 10.1109/IBSSC53889.2021.9673462.

[86] B. Tasneem and M. Wahid, "A review of secure routing challenges in low power and lossy networks," in *Proc. Int. Conf. Commun. Techn. (ComTech)*, 2021, pp. 120–125, doi: 10.1109/ComTech52583.2021.9616966.

[87] S. S. Ambarkar and N. Shekokar, "Impact analysis of RPL attacks on 6LoWPAN based Internet of Things network," in *Proc. IEEE Int. Conf. Electron., Comput. Commun. Tech. (CONECCT)*, 2021, pp. 1–5, doi: 10.1109/CONECCT52877.2021.9622711.

[88] S. Karmakar, J. Sengupta, and S. D. Bit, "LEADER: Low overhead rank attack detection for securing RPL based IoT," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, 2021, pp. 429–437, doi: 10.1109/COMSNETS51098.2021.9352937.

[89] A. S. Baghani, S. Rahimpour, and M. Khabbazian, "The DAO induction attack against the RPL-based Internet of Things," in *Proc. Int. Conf. Softw., Telecommun. Comput. Net. (SoftCOM)*, 2020, pp. 1–5, doi: 10.23919/SoftCOM50211.2020.9238224.

[90] I. Wadhaj, B. Ghaleb, C. Thomson, A. Al-Dubai, and W. J. Buchanan, "Mitigation mechanisms against the DAO attack on the routing protocol for low power and lossy networks (RPL)," *IEEE Access*, vol. 8, pp. 43665–43675, 2020, doi: 10.1109/ACCESS.2020.2977476.

[91] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. Humayun, A. O. Ibrahim, and A. Abdelmaboud, "A trust-based model for secure routing against RPL attacks in Internet of Things," *Sensors*, vol. 22, no. 18, p. 7052, 2022, doi: 10.3390/s22187052.

[92] M. Abid, S. N. Bahloul, and S. Hamlili, "Trust-based approach to secure low-power and lossy networks routing protocol," in *Proc. Int. Conf. Netw. Adv. Syst. (ICNAS)*, 2021, pp. 1–6, doi: 10.1109/ICNAS53565.2021.9628947.

[93] X. Sun, "Research on the secure routing mechanism for software defined Internet of Things based on IPv6," in *Proc. Int. Conf. Intell. Comput., Autom. Appl. (ICAA)*, 2021, pp. 714–718, doi: 10.1109/ICAA53760.2021.00129.

[94] A. Raoof, A. Matrawy, and C.-H. Lung, "Enhancing routing security in IoT: Performance evaluation of RPL's secure mode under attacks," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11536–11546, Dec. 2020, doi: 10.1109/JIOT.2020.3022276.

[95] A. Raoof, C.-H. Lung, and A. Matrawy, "Securing RPL using network coding: The chained secure mode (CSM)," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 4888–4898, Apr. 2022, doi: 10.1109/JIOT.2021.3109109.

[96] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Taipei, Taiwan, 2003, pp. 452–473.

[97] Z. A. Al-Odat, E. M. Al-Qtiemat, and S. U. Khan, "An efficient lightweight cryptography hash function for big data and IoT applications," in *Proc. IEEE Cloud Summit*, Harrisburg, PA, USA, 2020, pp. 66–71, doi: 10.1109/IEEECloudSummit48914.2020.00016.

[98] S. Oh, S. Park, and H. Kim, "Patterned cipher block for low-latency secure communication," *IEEE Access*, vol. 8, pp. 44632–44642, 2020, doi: 10.1109/ACCESS.2020.2977953.

[99] B. Aboushosha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed, and M. M. Dessouky, "SLIM: A lightweight block cipher for Internet of Health Things," *IEEE Access*, vol. 8, pp. 203747–203757, 2020, doi: 10.1109/ACCESS.2020.3036589.

[100] W. Wang, P. Xu, D. Liu, L. T. Yang, and Z. Yan, "Lightweighted secure searching over public-key ciphertexts for edge-cloud-assisted Industrial IoT devices," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4221–4230, Jun. 2020, doi: 10.1109/TII.2019.2950295.

[101] S. Atiewi et al., "Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography," *IEEE Access*, vol. 8, pp. 113498–113511, 2020, doi: 10.1109/ACCESS.2020.3002815.

[102] J. Hiller, M. Henze, M. Serror, E. Wagner, J. N. Richter, and K. Wehrle, "Secure low latency communication for constrained Industrial IoT scenarios," in *Proc. 43rd IEEE Conf. Local Comput. Netw. (LCN)*, 2018, pp. 614–622, doi: 10.1109/LCN.2018.8638027.

[103] M. Lyu, H. H. Gharakheili, and V. Sivaraman, "A survey on DNS encryption: Current development, malware misuse, and inference techniques," *ACM Comput. Surv.*, vol. 55, no. 8, pp. 1–28, Aug. 2023, doi: 10.1145/3547331.

[104] M. S. Lenders, C. Amsüss, C. Gündogan, M. Nawrocki, T. C. Schmidt, and M. Wählisch, "Securing name resolution in the IoT: DNS over CoAP," in *Proc. Int. Conf. Emerg. Netw. Exp. Technol. (CoNEXT)*, 2021, pp. 1–25, doi: 10.1145/3609423.

[105] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf. (DAC)*, 2007, pp. 9–14.

[106] B. Lee, I.-G. Lee, and M. Kim, "Design and implementation of secure cryptographic system on chip for Internet of Things," *IEEE Access*, vol. 10, pp. 18730–18742, 2022, doi: 10.1109/ACCESS.2022.3151430.

[107] B. Kim, S. Yoon, and Y. Kang, "PUF-based IoT device authentication scheme on IoT open platform," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, 2021, pp. 1873–1875, doi: 10.1109/ICTC52510.2021.9620848.

[108] S. Yoon, B. Kim, K. Kim, and Y. Kang, "Enhancing IoT security with PUF-based authentication scheme," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, 2022, pp. 2319–2321, doi: 10.1109/ICTC55196.2022.9952899.

[109] M. Masud et al., "A lightweight and robust secure key establishment protocol for Internet of Medical Things in COVID-19 patients care," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15694–15703, Nov. 2021, doi: 10.1109/JIOT.2020.3047662.

[110] S. Shamshad, M. F. Ayub, K. Mahmood, M. Rana, A. Shafiq, and J. J. P. C. Rodrigues, "An identity-based authentication protocol for the telecare medical information system (TMIS) using a physically unclonable function," *IEEE Syst. J.*, vol. 16, no. 3, pp. 4831–4838, Sep. 2022, doi: 10.1109/JSYST.2021.3118014.

[111] P. Gope, O. Millwood, and B. Sikdar, "A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for Internet of Medical Things," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 1971–1980, Mar. 2022, doi: 10.1109/TII.2021.3096048.

[112] X. Ren, J. Cao, M. Ma, H. Li, and Y. Zhang, "A novel PUF-based group authentication and data transmission scheme for NB-IoT in 3GPP 5G networks," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3642–3656, Mar. 2022, doi: 10.1109/JIOT.2021.3098224.

[113] M. Ebrahimabadi, M. Younis, and N. Karimi, "A PUF-based modeling-attack resilient authentication protocol for IoT devices," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3684–3703, Mar. 2022, doi: 10.1109/JIOT.2021.3098496.

[114] A. Mostafa, S. J. Lee, and Y. K. Peker, "Physical unclonable function and hashing are all you need to mutually authenticate IoT devices," *MDPI Sens.*, vol. 20, no. 16, p. 4361, 2020, doi: 10.3390/s20164361.

[115] T. Alladi, V. Chamola, R. M. Parizi, and K.-K. R. Choo, "Blockchain applications for industry 4.0 and Industrial IoT: A review," *IEEE Access*, vol. 7, pp. 176935–176951, 2019, doi: 10.1109/ACCESS.2019.2956748.

[116] H. H. Pajooh, S. Demidenko, S. Aslam, and M. Harris, "Blockchain and 6G-enabled IoT," *Inventions*, vol. 7, no. 4, p. 109, 2022, doi: 10.3390/inventions7040109.

[117] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-based decentralized authentication modeling scheme in edge and IoT environment," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2116–2123, Feb. 2021, doi: 10.1109/JIOT.2020.3037733.

[118] L. D. Santis, V. Paciello, and A. Pietrosanto, "Blockchain-based infrastructure to enable trust in IoT environment," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, 2020, pp. 1–6, doi: 10.1109/I2MTC43012.2020.9128817.

[119] L. Hang and D.-H. Kim, "Design and implementation of an integrated IoT blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, p. 2228, 2019, doi: 10.3390/s19102228.

[120] X. Chen, K. Nguyen, and H. Sekiya, "On the latency performance in private blockchain networks," *IEEE Internet Things J.*, vol. 9, no. 19, pp. 19246–19259, Oct. 2022, doi: 10.1109/JIOT.2022.3165666.

[121] S. Asaithambi et al., "An energy-efficient and blockchain-integrated software defined network for the Industrial Internet of Things," *Sensors*, vol. 22, no. 20, p. 7917, 2022, doi: 10.3390/s22207917.

[122] T. Sylla, L. Mendiboure, M. A. Chalouf, and F. Krief, "Blockchain-based context-aware authorization management as a service in IoT," *Sensors*, vol. 21, no. 22, p. 7656, 2021, doi: 10.3390/s21227656.

[123] P. Tedeschi, S. Sciancalepore, A. Eliyan, and R. Di Pietro, "LiKe: Lightweight certificateless key agreement for secure IoT communications," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 621–638, Jan. 2020, doi: 10.1109/JIOT.2019.2953549.

[124] M. Polese, F. Chiariotti, E. Bonetto, F. Rigotto, A. Zanella, and M. Zorzi, "A survey on recent advances in transport layer protocols," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3584–3608, 4th Quart., 2019, doi: 10.1109/COMST.2019.2932905.

[125] T. Shreedhar, R. Panda, S. Podanev, and V. Bajpai, "Evaluating QUIC performance over web, cloud storage, and video workloads," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 2, pp. 1366–1381, Jun. 2022, doi: 10.1109/TNSM.2021.3134562.

[126] Y. A. Joarder and C. Fung, "A survey on the security issues of QUIC," in *Proc. Cyber Secur. Netw. Conf. (CSNet)*, 2022, pp. 1–8, doi: 10.1109/CSNet56116.2022.9955622.

[127] "QUIC implementations." Accessed: Apr. 10, 2024. [Online]. Available: https://github.com/quicwg/_newline_ttbase-drafts/wiki/Implementations

[128] P. Kumar and B. Dezfouli, "Implementation and analysis of QUIC for MQTT," *Comput. Netw.*, vol. 150, no. 26, pp. 28–45, Feb. 2019, doi: 10.1016/j.comnet.2018.12.012.

[129] S. Jeddou, F. Fernández, L. Diez, A. Baina, N. Abdallah, and R. Aguero, "Delay and energy consumption of MQTT over QUIC: An empirical characterization using commercial-off-the-shelf devices," *Sensors*, vol. 22, no. 10, p. 3694, May 2022, doi: 10.3390/s22103694.

[130] A. Alqattaa, D. Loebenberger, and L. Moeges, "Analyzing the latency of QUIC over an IoT gateway," in *Proc. IEEE Int. Conf. Omni-Layer Intell. Syst. (COINS)*, 2022, pp. 1–6, doi: 10.1109/COINS54846.2022.9854951.

[131] F. Fernandez, M. Zverev, P. Garrido, J. R. Juarez, J. Bilbao, and R. Aguero, "And QUIC meets IoT: Performance assessment of MQTT over QUIC," in *Proc. Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, 2020, pp. 1–6, doi: 10.1109/WiMob50308.2020.9253384.

[132] F. Fernandez, M. Zverev, P. Garrido, J. R. Juarez, J. Bilbao, and R. Aguero, "Even lower latency in IIoT: Evaluation of QUIC in industrial IoT scenarios," *Sensors*, vol. 21, no. 17, p. 5737, Aug. 2021, doi: 10.3390/s21175737.

[133] D. Saif and A. Matrawy, "An experimental investigation of tuning QUIC-based publish-subscribe architectures in IoT," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 4924–4933, Feb. 2024, doi: 10.1109/JIOT.2023.3302160.

[134] E. Liri, P. K. Singh, A. B. Rabiah, K. Kar, K. Makhijani, and K. K. Ramakrishnan, "Robustness of IoT application protocols to network impairments," in *Proc. IEEE Int. Symp. Local Metrop. Area Netw. (LANMAN)*, 2018, pp. 97–103, doi: 10.1109/LANMAN.2018.8475048.
[135] D. Saif and A. Matrawy, "A pure HTTP/3 alternative to MQTT-over-QUIC in resource-constrained IoT," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2021, pp. 36–39, doi: 10.1109/CSCN53733.2021.9686113.
[136] J. Dizdarevic and A. Jukan, "Experimental benchmarking of HTTP/QUIC protocol in IoT cloud/edge continuum," in *Proc. IEEE Intern. Conf. Commun. (ICC)*, 2021, pp. 1–6, doi: 10.1109/ICC42927.2021.9500675.
[137] M. H. Firmansyah, J.-H. Jung, and S.-J. Koh, "Proxy-based adaptive transmission of MP-QUIC in Internet-of-Things environment," *Electron.*, vol. 10, no. 17, p. 2175, Sep. 2021, doi: 10.3390/electronics10172175.
[138] R. Herrero, "Analysis of QUIC transported CoAP," *SN Comput. Sci.*, vol. 2, no. 2, p. 62, Apr. 2021, doi: 10.1007/s42979-021-00468-0.
[139] J.-H. Jung, H.-B. Nam, D.-K. Choi, and S.-J. Koh, "Use of QUIC for CoAP transport in IoT networks," *Internet Things*, vol. 24, Dec. 2023, Art. no. 100905, doi: 10.1016/j.iot.2023.100905.
[140] G. Pettorru and M. Martalò, "QUIC and WebSocket for secure and low-latency IoT communications: An experimental analysis," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2023, pp. 628–633, doi: 10.1109/ICC45041.2023.10279305.
[141] F. Iqbal, M. Gohar, H. Alquhayz, S.-J. Koh, and J.-G. Choi, "Performance evaluation of AMQP over QUIC in the Internet-of-Thing networks," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 4, pp. 1–9, Apr. 2023, doi: 10.1016/j.jksuci.2023.02.018.
[142] F. Iqbal, M. Gohar, H. Karamti, W. Karamti, S.-J. Koh, and J.-G. Choi, "Use of QUIC for AMQP in IoT networks," *Comput. Netw.*, vol. 225, Apr. 2023, Art. no. 109640, doi: 10.1016/j.comnet.2023.109640.
[143] L. Eggert, "Towards securing the Internet of Things with QUIC," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2020, pp. 1–6. [Online]. Available: https://easychair.org/publications/preprint/68D2
[144] P. Li, J. Su, and X. Wang, "iTLS: Lightweight transport-layer security protocol for IoT with minimal latency and perfect forward secrecy," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6828–6841, Aug. 2020, doi: 10.1109/JIOT.2020.2988126.

Marco Martalò (Senior Member, IEEE) received the Ph.D. degree in information technologies from the University of Parma, Italy, in 2009. From 2012 to 2017, he was an Assistant Professor with E-Campus University, Italy, and also a Research Associate with the University of Parma until 2020. Since 2020, he has been an Associate Professor of Telecommunications with the University of Cagliari, Italy, where he is a part of the Networks for Humans (Net4U) Laboratory. He is also a member of the Research Unit of Cagliari at the Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT). He has coauthored the book *Sensor Networks with IEEE 802.15.4 Systems: Distributed Processing, MAC, and Connectivity*. As of April 2024, he authored more than 90 publications and his H-index is equal to 14 (according to Scopus). He is also the inventor of two Italian patents (one of them with international extension). His research interests are in the design of communication and signal processing algorithms for wireless systems and networks, as well as the security aspects of them. He serves on the technical program committee of major international conferences and he is an Associate Editor of the IEEE ACCESS.

Giovanni Pettorru received the B.Sc. degree in electrical and electronic engineering in Cagliari in 2020, with the thesis "Implementation of a parking occupancy detection system based on magnetometer sensor" and the master's degree in Internet engineering from the University of Cagliari in 2022, by discussing the thesis "Secure and Low-Latency Communications Based on WebSocket and QUIC in the Internet of Things Scenario." He is currently pursuing the Ph.D. degree with the Department of Electrical and Electronic Engineering (DIEE), University of Cagliari. He is part of the Networks for Humans (Net4U) Laboratory and member of the Research Unit of Cagliari at the Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT). His research interests include network protocols and network security. He is a member of IEEE as a graduate student. He achieved an Award at the IEEE ComSoc Three Minute Thesis Competition during the ICC 2023 Event. Additionally, he served as a PC Member at the AQ-IoT 2023 Conference.

Luigi Atzori (Senior Member, IEEE) received the Ph.D. degree in 2000. He is a Professor of Telecommunications with the University of Cagliari, where he leads the activities of the Net4U Laboratory (Network for Humans) with around 20 affiliated researchers. He is a member of the Research Unit of Cagliari at the Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT). Since 2018, he has been the Coordinator of the master's degree course in internet technology engineering with the University of Cagliari. His works on the IoT and the social IoT have received a great impact with more than 20K citations. His interests also fall in the area of Quality of Experience (QoE), with particular application to the management of services and resources in new generation networks for multimedia communications. Lately, he also applies the study of QoE to IoT services. His research interests fall in the area of Internet of Things (IoT), with particular reference to the design of effective algorithms for the realization of social networks among connected devices to develop the Social IoT paradigm. He serves regularly as referee for several international and national funding programs, in the organizing committee of international conferences, and as an associate and a guest editor in several international journals (*Ad Hoc Networks*, IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY, and *IEEE Communications Magazine*). He is a Co-Founder of two spinoffs in the areas of IoT solutions for people mobility.

Open Access funding provided by "Università degli Studi di Cagliari" within the CRUI CARE Agreement