2021

5G Security Challenges and Solutions: A Review by OSI Layers

S. Sullivan
Coastal Carolina University

Alessandro Brighente
University of Padua

Sathish Kumar
Cleveland State University, s.kumar13@csuohio.edu

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 16, 2021, accepted August 5, 2021, date of publication August 16, 2021, date of current version August 27, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3105396

5G Security Challenges and Solutions: A Review by OSI Layers

S. SULLIVAN[1], ALESSANDRO BRIGHENTE[2], (Student Member, IEEE), S. A. P. KUMAR[3], (Senior Member, IEEE), AND M. CONTI[2], (Senior Member, IEEE)

[1]Department of Computing Sciences, Coastal Carolina University, Conway, SC 29528, USA
[2]Department of Mathematics, University of Padua, 35122 Padua, Italy
[3]Department of Electrical Engineering and Computer Science, Cleveland State University, Cleveland, OH 44115, USA

Corresponding author: S. A. P. Kumar (s.kumar13@csuohio.edu)

ABSTRACT The Fifth Generation of Communication Networks (5G) envisions a broader range of services compared to previous generations, supporting an increased number of use cases and applications. The broader application domain leads to increase in consumer use and, in turn, increased hacker activity. Due to this chain of events, strong and efficient security measures are required to create a secure and trusted environment for users. In this paper, we provide an objective overview of 5G security issues and the existing and newly proposed technologies designed to secure the 5G environment. We categorize security technologies using Open Systems Interconnection (OSI) layers and, for each layer, we discuss vulnerabilities, threats, security solutions, challenges, gaps and open research issues. While we discuss all seven OSI layers, the most interesting findings are in layer one, the physical layer. In fact, compared to other layers, the physical layer between the base stations and users' device presents increased opportunities for attacks such as eavesdropping and data fabrication. However, no single OSI layer can stand on its own to provide proper security. All layers in the 5G must work together, providing their own unique technology in an effort to ensure security and integrity for 5G data.

INDEX TERMS 5G technologies, security issues, security solutions, OSI layer, 5G vulnerabilities.

I. INTRODUCTION

While some still see 5G in the idea phase [1], wireless service providers such as Verizon began taking orders for their 5G Home product on October 1, 2018 in Houston, Indianapolis, Los Angeles and Sacramento [2]. 5G networking enables a major number of use cases compared to previous generations. In fact, while increasing the attainable data rate was the main driver in previous generations, in 5G this represents one among other objectives, such as ultra-low latency, ultra-dense network support, and heterogeneous quality of service support. Due to the ever-increasing demand for a networked society with unlimited access to information every time and everywhere, 5G networks employ novel architectures and technologies to overcome all the limitations imposed by previous generations [3]. Nevertheless, capacity and data rates represent one of the design objectives. In fact, new use cases such as virtual reality, augmented reality, High Definition (HD) screening, and video streaming demand high transmission rates. This is further complicated by the fact that the number of connected devices is increasing, therefore so is the demand for higher cell capacity. Some of the key targets regarding cellular environments envision peak data rates of 20 Gbps in downlink and 10 Gbps in uplink, with a connection density of 1M devices per km^2 [4]. Research predicts billons of connected sensors [5] and over 200 million devices to be deployed soon [6]. In order to cope with such requirements, technologies as massive Multiple-Input Multiple-Output (MIMO) and beamforming are considered key enablers. Furthermore, in order to avoid the limitation given by a crowded spectrum, a shift toward Millimeter Wave (mmWave) transmissions with carrier frequencies above 6 Ghz has been proposed, and significant research contributions have been devoted to its implementation [7]. As new use cases arise, end-to-end latency and reliability have drawn significant attention from the research community. Among the others, Ultra-Reliable Low-Latency Communication (URLLC) is a service envisioned for 5G network, which finds its enhancement in its extreme version [8]. Extreme URLLC envisions a network able to provide $<$ 1 ms

The associate editor coordinating the review of this manuscript and approving it for publication was Kang Chen.

latency and $1 - 10^{-9}$ reliability. This type of communication enables the use of cases such as vehicular communications and telesurgery. New network paradigms have also been proposed to guarantee the strict requirements of the Fifth Generation of Communication Networks (5G) networks. Software Defined Network (SDN) and Network Function Virtualization (NFV) are expected to provide the programmability lacking in previous cellular generations by replacing dedicated network components with programmable ones able to accommodate multiple network requirements [9]. This facilitates better user experience, as components may be adapted on the fly responding to punctual requirements. A further proposal is Infromation Centric Networking (ICN), in which content is delivered based on a pre-assigned name, replacing previous address-based routing paradigms. ICN has the advantage of reducing the distance between the user and the information, therefore providing a betterment both in terms of latency and content availability [10]. Over the life of 5G, seven trillion wireless devices are expected to be connected [11], therefore privacy and integrity are of fundamental importance in implementing diverse technologies. To protect the privacy and integrity of data traversing 5G networks, multiple layers of security using diverse technologies are required [11]–[13]. 5G will provide the underlying infrastructure that supports Cyber-Physical Systems (CPS) [5], among the others, with a particular focus on protection of devices from eavesdropping and spectrum sensing.

Existing architectures place most of their security focus above the physical layer. However, with the deployment of 5G, the physical layer will provide an attack surface with threats such as eavesdropping of communication. Physical-Layer Security (PLS) solutions have been proposed to mitigate eavesdropping, including multiple technologies and strategies such as beamforming, power control, and joint clustering [14]. Internet of Things (IoT) also represents one of the core applications of 5G, whose security importance has been discussed in literature [6]. While this work does not directly reference 5G use cases, IPsec will be an important security mechanism for the overall 5G environment [6]. Annessi *et al.* [15] discuss the importance of IPsec between the core network and the base station. Heterogeneous Network (HetNet), MIMO and mmWave are among the emerging technologies that can be exploited for security purposes [16], [17].

Due to their recent development and success, bitcoin and cryptocurrency in general, can be deemed as an important component of the 5G environment. Newegg and one US-based Subway restaurant among numerous other companies accept bitcoin payments, which is an indicator that bitcoin is becoming more accepted by the general population [18]–[20]. As such, their privacy and security issues shall be tackled along with 5G security. The work by Conti *et al.* discusses the bitcoin blockchain from the application layer [21]. The authors discuss security and privacy issues and solutions related to the blockchain and the exploited consensus protocol, such as transaction malleability and the ''SegWit'' solution [21], [22]. G. Vidan and V. Lehdonvirta also mention the bitcoin security issue of transaction malleability [23].

5G will support a highly anticipated technology, i.e., connected cars [24]. Eiza *et al.* [25] propose a protocol to addresses reliable, secure, and privacy-aware real-time video streaming. Yoo [26] reported security issues in 5G enabled vehicular networks and propose public key cryptography as a possible solution to address those issues. Hussain *et al.* [27] review the security issues in the design and implementation of VANET while integrating it with 5G.

In this paper, we provide a review of 5G security issues and security, categorized according to the Open Systems Interconnection (OSI) model layers. As shown in Table 1, the OSI model provides a protocol framework for network communication using seven distinct layers [28]. The objective of this paper is to provide an overview of 5G security technology, vulnerabilities, solutions, and challenges suitably organized according to their belonging to the communication layer. To fully understand the security issues and solutions for 5G networks we use the OSI protocol stack instead of 4-layer TCP/IP format or other layered models. OSI provides three additional layers compared to TCP/IP, namely presentation, session, data link, and physical layers. In TCP/IP instead, application, presentation and session layers are comprised in the application layer, while the network interface layer takes on the functionalities of the data link and physical layers of the seven-layered OSI approach. Therefore, considering the OSI layers allows us to provide a more detailed assessment of the security aspects. Application-driven services, such as the services automated vehicles, AR/VR, and others, are considered to be some of the major innovations in 5G system and beyond. As such, it is very important to secure the application layer. Though in practice, the presentation and session layers may be incorporated into the application and transport layers, respectively, we want to look at the security issues in the session layer and presentation layer functionalities in depth. This in-depth view allows us to look at the security issues in detail rather than looking at the application and transport layer in a shallower fashion. As we will show in section IV and section V, there are several security issues in the presentation and session layers functionalities need to be taken care of at the design stage. We should therefore consider these security issues for secure by-design 5G. Similarly, as outlined in section IX, there are several physical layer security issues for the 5G compared to other layers. It is hence important to highlight and differentiate the security issues at the physical layer and the data link layer. Moreover, as described in sections VII and VIII, several issues in the network and data link layers require immediate attention. Therefore, a more detailed survey including these additional layers will help the research community to analyze the issues in a detailed manner.

5G will impact multiple layers of the OSI model, therefore, our study categorizes each security issue by the OSI layer it lies within. Due to the increase of security threats expected with the deployment of 5G, it is important to understand what

TABLE 1. OSI layers.

OSI Layers	
Layer #	Layer Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

risks companies and individuals will face in the future, and how to mitigate them in the 5G deployment. As we later show, the organization according to OSI layers allows for a better coverage of all the security and privacy related aspects. We provide a comparison with other available surveys on the topic to show how our OSI-oriented approach allows for a better investigation of 5G security and privacy.

A. COMPARISON WITH OTHER SURVEYS

We present a review of available surveys on the subject and motivate the need for our survey. In [29], authors look at the security of technologies such as cloud, SDNhl, and NFV. In [30], authors review the security requirements of 5G applications from a technology perspective, focusing on incremental solutions such as physical layer security and lightweight encryption. In [31] authors look at the core and enabling technologies that provide 5G security, specifically looking at security monitoring and management of 5G networks. In addition, their work also evaluates the existing related security measures and baselines. The physical layer security issues were reviewed in [32], where authors surveyed security issues surrounding promising 5G technologies such as security coding and millimeter wave communications that impact the physical layer. Ferrag *et al.*, look at both 4G and 5G security issues from the authentication and privacy-preserving schemes perspective [33]. In addition to providing classification, they also provide countermeasures for issues in authentication and privacy [33]. Ahmad *et al.*, looked at the privacy and security issues of 5G enabling technologies such as SDN and NFV and recommended solutions [34]. Hussain *et al.* [35], look at the security issues, solutions, and standards arising from the integration of 5G and VANET technologies. Thus, their work does not look into 5G security issues holistically. Sriram *et al.* [36] look at the rationale of the importance of security in 5G compared to 2G/3G/4G with a focus on the security requirements, threats, and solutions. Also, they focus only on physical layer security. Choudhary *et al.* [37], look at the security of 5G mobile backhaul networks, discussing potential security threats, vulnerabilities, and key challenges. Ahmad *et al.* [38], describes 5G vulnerabilities and threats at the network and application layers and provide solutions. In addition, they also outline security issues for post-5G cellular technologies. In [39], PLS is discussed in the context of IoT and network slicing.

Table 2 shows the OSI layers covered by each referenced survey. We see that available surveys focus on the application, network, and physical layer, whereas a few focus on presentation and data-link layers, and none on the session layer. Therefore, although some surveys on 5G security are quite comprehensive, they do not fully cover the 7 OSI layers, motivating the need for our survey.

B. CONTRIBUTIONS

In our paper we focus on 5G security and, specifically, we summarize the vulnerabilities and threats, security solutions and challenges, gaps and open research issues organized by OSI layers. Each layer presents specific protocols and architectures by means of which 5G networks can meet design objectives such as increased connectivity, lower latency, and high reliability. Figure 1 shows they key technologies that we analyze in this survey, organized according to OSI layers. Among those reported in Figure 1, we find many of the key technologies that enable 5G networks. For instance, SDN has been advocated as one of the main technologies able to enhance the performance in terms of quality of service in modern and future networks. A similar reasoning is applied to ICN, which aims at shortening the distance between user and content, therefore providing lower latency and higher data availability. Among the others, also blockchain/Distributed Ledger Technology (DLT) technology has been included in this survey. Although its development was not strictly related to communications technology, it now sees application in different domains, ranging from vehicular communications, to industrial network and network management [45]–[47]. Based on our review, we state that due to increase in wireless connectivity, future researchers may benefit from focusing on physical layer security solutions in order to prevent eavesdropping and other physical channel based attacks. Furthermore, the community may also benefit from additional research on transaction malleability, due to the vulnerability within the bitcoin protocol. Our study also demonstrates that all OSI layers are important to keep the 5G environment as secure as possible. Understanding the different 5G security issues by OSI layer could help organizations focus their capital expenditure.

One of the motivations to look at the security issues in different layer is to provide perspectives to the security and network professionals and researchers on how to tackle the security in a layered approach. This will enable the in depth defense concept for the security by design. This will also allow to implement the security in a holistic manner and even if a solution in one layer cannot address the security threat, it can be addressed by the solution in a different, connected layer. Such an approach provides end-to-end network security design rather than a piece meal approach for network security against attacks. The layered approach to security can also help in addressing conflicting objectives such as security through encryption and network intelligence. By looking at the security issues in the different layers, the security and

TABLE 2. Comparison with other surveys: OSI layers covered by each survey.

Reference	Application	Presentation	Session	Transport	Network	Data-Link	Physical
[29]					x	x	
[30]	x				x		x
[31]					x		x
[32]							x
[33]					x		
[34]		x		x	x		
[35]	x				x		
[36]					x		x
[37]	x				x		x
[38]	x				x		
[39]	x			x	x		
[40]	x				x		
[41]	x			x	x		
[42]					x		
[43]							x
[44]							x
Our Survey	x	x	x	x	x	x	x

network professionals and researchers can design holistic and efficient security protocols for the 5G networks and beyond.

C. REVIEW METHODOLOGY

There are few works in the literature discussing vulnerabilities and solutions for 5G security. In the process of reviewing existing approaches, our initial challenge was to understand what protocols are exploited at each OSI layer. This step was helpful to review several OSI layer resources that point to specific protocols, e.g., bitcoin protocol. Once created a list of protocols at each OSI layer, we proceeded by finding research works in the literature on 5G security discussing the specific protocol. From there, it is imperative to gain a basic understanding of the new 5G proposed technologies, vulnerabilities, solutions and gaps for each protocol. It is helpful if the technologies are discussed in several papers, such as in the case of HetNets. Unfortunately, that was rare. In a few cases, we identified only a single paper for a specific protocol. The end goal was to find at least one protocol per layer related to 5G that is discussed in literature, and that was achieved.

D. PAPER ORGANIZATION

The paper is organized as follows. In Section II we provide an overview of the evolution of the mobile network starting from 1G up to 5G, discussing the different security needs and vulnerabilities. In Section III to VIII we discuss respectively the application, presentation, session, transport, network, data link and physical layers. Each section is separated in three subsections: the first introducing basic concepts on the discussed layer, the second discussing its security and vulnerabilities, and the third discussing the solutions, challenges and gaps. In Section X we summarize the review of 5G security challenges and explains the recommendations for future work. Finally, in Section XI we conclude the paper with the summary of the work.

II. SECURITY THREATS EVOLUTION

Telecommunication network first appeared in the 1980s with the first generation of mobile networks (1G), and evolved during the past 40 years leading to the 5G. Starting from an analog network for voice only communications and with poor security features, it now provides ubiquitous connection for multiple types of users with enhanced security and privacy guarantees. Successive generations were introduced mitigating the vulnerabilities of the previous generations, but at the same time introducing new threat vectors due to the new employed technologies. In order to fully understand the security threats and needs of 5G we here review the technologies employed in the different generations and discuss their security vulnerabilities and features.

A. 1G SECURITY

The 1G was mainly based on analog technologies, with main and only target being voice call services [48]. However, the range was limited to single countries. The 1G networks were also knew as Advanced Mobile Phone Systems (AMPS) in USA and as Nordic Mobile Telephony (NMT) in Europe. Data network and roaming services were not part of the 1G network, and the maximum speed was limited to 2.4 Kbps. It showed a large number of shortcomings, such as insufficient capacity, poor use of spectrum, bad quality of voice calls and reckless handoff. Furthermore, it provided no security solutions allowing for call eavesdropping by unwanted listeners [49]. The security threat was further complicated by the fact that 1G networks did not allow for encryption due to their analog nature. Thanks to the clear-text nature of these communications, an attacker was also able to easily obtain not only access to the phone call, but also to other information such as the mobile identification number, or the electronic serial number. By capturing these values, an attacker was able to run impersonation attacks by cloning the phone and impersonating the subscriber. The first security measure introduced in 1G was scrambling, which allowed for prevention against eavesdropping.

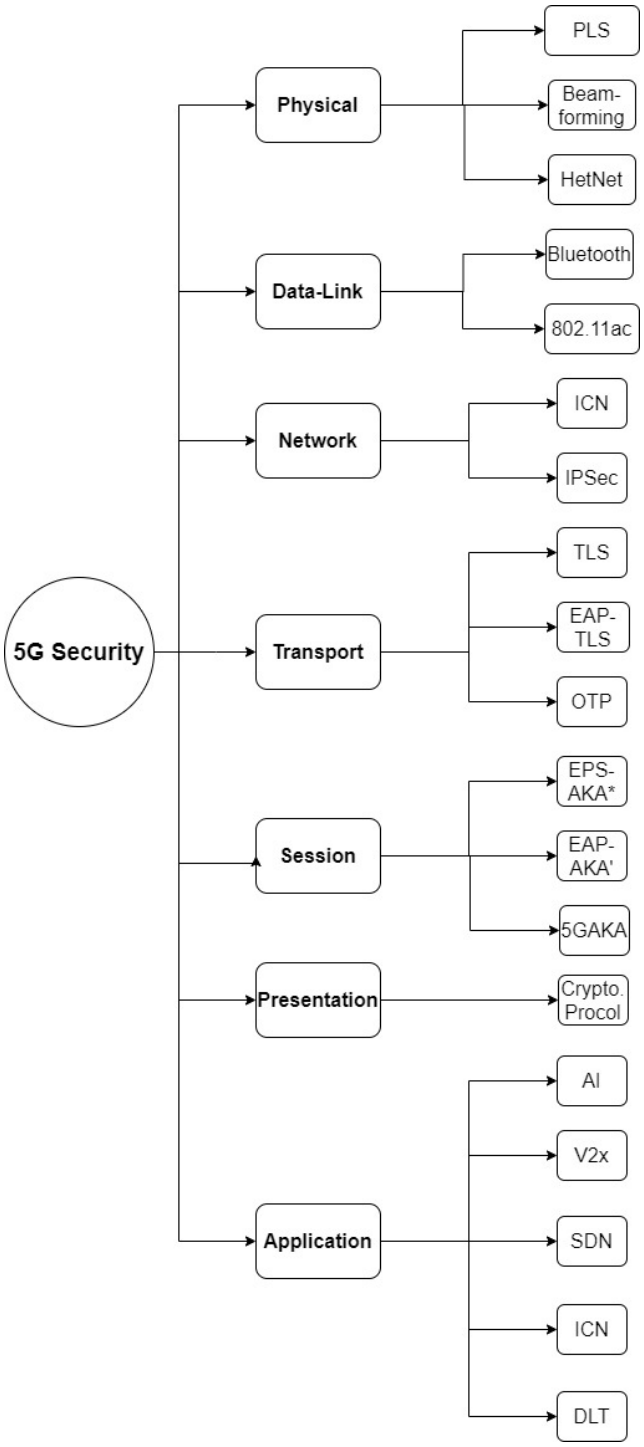


FIGURE 1. Overview of the key technologies and protocols analyzed in this survey.

B. 2G SECURITY

The second generation (2G) of mobile networks was introduced a decade after 1G, adding messaging services (via SMS) along with voice communication. 2G introduced a large number of technologies around the world, such as Code Division Multiple Access (CDMA), North America Time Division Multiple Access (NA-TDMA), Global System for Mobile Communications (GSM) and Personal Digital Cellular (PDC). Furthermore, e-mails were first supported by mobile communications [50]. 2G provided the shift from the analog to the digital world in mobile communications, and hence allowed for the introduction of a large number of security measures [31]. Authentication was first introduced in mobile communications thanks to cryptography, where secret keys were used to encrypt traffic and provide confidentiality in the communication. The identity of the subscribers was verified by introducing the Subscriber Identity Module (SIM) devices, i.e., physical devices storing a cryptovariable used in the authentication process. 2G, however, was vulnerable to multiple attacks. For instance, spamming was one of the main threat vectors, where attackers aimed at transmitting unwanted information to victim users. Furthermore, the design implementation of some of the security solutions were not properly addressed. Relevant examples are the COMP128 and A5 cryptographic algorithms [51]. Furthermore, GSM encryption was limited to the radio interface, whereas communications channels were deemed as secure and therefore not protected against eavesdroppers [51]. SMS were also vulnerable to attacks, as the roaming of messages was exposed to attackers on the Internet [31].

C. 3G SECURITY

The third generation of mobile network (3G) was introduced a decade after the 2G and brought the advantage of services based on the Internet Protocol (IP). 3G saw a significant improvement in terms of quality of service, allowing for services like global roaming and highly improved voice quality. The main technologies introduced with 3G were Wideband CDM (WCDMA), Universal Telecommunication Systems (UMTS), and High Speed Uplink/Downlink Packet Access (HSUPA/HSDPA). Shifting from 3G to the fourth generation (4G), 3.75G introduced the fundamental technologies for mobile data services such as Long-Term Evolution technology (LTE) and Fixed Worldwide Interoperability for Microwave Access (WIMAX). The security of 3G accounted for all the vulnerabilities identified in 2G and corrected them. The security architecture deployed in 3G communications was composed of five sets: i) network access security, ii) network domain security, iii) user domain security, iv) application security and v) visibility and configurability security. The design of the security features of 3G also provided higher flexibility, and the possibility for extension to mitigate new threats that may be identified after their deployment [52]. Due to the increased pool of devices involved in the network, the attack surface also increased. In fact, multiple security threats were reported targeting the operating system, the users' phone, and the computer system. Such vulnerabilities included gain of authorizations in accessing users' sensitive information, eavesdropping, and impersonation attacks. Impersonation was not only limited to the subscriber, but was also exploited to impersonate the user or the network [31]. Further attacks included man-in-the-middle,

denial of service, location update spoofing, and camping on a false base station.

D. 4G SECURITY

4G improved the existing network by including a full and reliable solution entirely based on IP. The higher data rate compared to that attained by the previous generations allowed for sharing data and multimedia ubiquitously in the network. The main technologies introduced with 4G were Multimedia Messaging Service (MMS), Digital Video Broadcasting (DVB), video chat, High Definition TV content, and mobile TV [53], [54]. 4G provided the security features needed to mitigate all the attacks identified in the previous generations, together with new cryptographic algorithms with improved key structures. The main algorithms introduced were EPS Encryption Algorithms (EEA) and EPS Integrity Algorithms (EIA), and used keys were 256-bits long (twice the length of those used in 3G) [52]. Another of the main differences compared to the previous generations is that control and user planes traffic exploited different algorithm and key sizes. Authentication was here provided by means of the Authentication and Key Agreement (AKA) protocol, whereas integrity and protection from replay attacks was guaranteed via NAS (Non-Access Stratum) and RRC (Radio Resource Control)-signaling protocol. IPSec was used to encrypt backhaul traffic [55], [56]. However, due to the connection of the cellular network with the internet network thanks to the end-to-end IP framework, 4G is vulnerable to a large number of attacks coming from the internet. All attack vectors targeting the basic functioning of the IP protocol are now a viable solution to attack the cellular network. Examples of such attacks include address spoofing, TCP SYN flood attack, TCP RST attack and hijack, Denial of Service, user ID theft, and intrusion attacks [57]. The higher computing power of mobile devices also creates new attack surfaces, as powerful attacks may also be generated from the devices in the cellular network. Furthermore, 4G supported technologies such as Wi-Fi and WIMAX, therefore inheriting all the security issues of these technologies [33].

E. 5G SECURITY

5G is creating an even more interconnected network, where devices with different capabilities and quality of service constraints need to interoperate [58]. 5G is hence also facing the ever-increasing demand of users for connection and ubiquitous access to the network. Compared to previous generations, 5G is expected to solve six challenges, namely higher capacity, higher data rate, lower end-to-end latency, massive device connectivity, reduced cost, and consistent Quality of Service. At the same time, attackers capabilities also increased compared to the previous generations. In fact, the computational power of current mobile devices allows for launching complicated attacks from inside the mobile network. Furthermore, the type of attacks and generated malwares are more efficient and effective than those faced by previous generations. This leads to attacks being driven by stronger aims compared to previous generations, including big cyber-crime rings with clear financial, political, and personal motives. This is further motivated by the fact that the mobile network is not limited to voice and video calls, but also supports a large number of other services and devices [58], creating a wide attack surface that may lead to severe disruption in the functioning of one of the interconnected networks.

Due to the larger number of services and connected devices, and despite the introduced security measure, 5G may still be vulnerable to different types of attacks. In the next sections we will discuss the identified vulnerabilities, organizing the technologies and the associated threat vectors according to the OSI model.

III. APPLICATION LAYER

The application layer (layer 7) is the layer that processes and formats data so that it can be passed to layer 6, the presentation layer [59]. Layer 7 is the closest layer to the application itself. Application based encryption is considered to be an effective security mechanism for those applications placed onto layer 7 [14]. However, the application layer does not include the applications rather the application protocols [59].

As previously discussed, 5G envisions a broader application domain compared to previous generations. In this section, we review some of the application layer services in different use cases, such as vehicular communications, ICN, blockchain/DLT, SDN, and Artificial Intelligence (AI).

- *Vehicular communications* represent, among others, one of the new use cases enabled by 5G networks. In fact, it exploits one of the core features envisioned by 5G, i.e., very low latency and ultra-reliability. By means of On-Board Equipments (OBEs), vehicles are connected to the network and exchange data with other network entities, such as other vehicles, pedestrians, and infrastructures. This allows both vehicles and other involved entities to collect and process data, such that services like autonomous driving, secure mobility management, and real time video sharing can be achieved [40]. The application layer in this context is exploited for different purposes. First, the application layer is responsible for OBEs identity. Second, it is exploited to obtain network topology, resource configuration, and other information to adjust the current network configuration. In this section, we review the security issues associated with applications for vehicular communications.
- *Blockchain and DLT* have recently drawn significant attention from the scientific community, with applications not only in the exchange of cryptocurrencies, but also for networking purposes. Bitcoin is the first introduced blockchain, providing an application layer protocol with an open-source design [21]. Bitcoin was presented in 2008, introducing the concept of a peer-to-peer electronic cash exchange [60]. The peer-to-peer exchange concept removes the traditional middle entity, such as an FDIC ensured bank. This means that the

transaction can be anonymous, free from government eyes and government taxes. Despite its controversy, Bitcoin is accepted at numerous companies, including newegg.com, a few Subway franchises and small local companies like Grass Hill Alpacas [18]–[20]. Bitcoin's ledger function is based on blockchain [61]. Anyone with access to a computer can use bitcoin. In fact, Bitcon.org walks individuals and businesses through creating a bitcoin wallet and buying bitcoin. Starting from the launch of Bitcoin, other applications, such as Hyperledger, have made use of the blockchain technology [61], [62]. While anonymity is synonymous with Bitcoin, it is not synonymous with blockchain. Among the others, blockchains find applications in networking for vehicular communications, IoT, as well as in the design of radio access networks [63], [64]. The paper by [62] explores how blockchain can be used to create secure smart homes. Since Bitcoin has clearly gained acceptance in the modern economy, we review it here in relation to 5G security.

- *ICN* has been proposed as a novel approach in 5G networks to shift from a user-centric paradigm to a data-centric one. The idea is to enable in-network caching and replication by having data independent from location, application, storage, and means of transportation. Therefore, each data/content is assigned a specific name, and is retrieved without knowing the physical location of the content provider. This provides a significant shift compared to IP based networks, allowing for a significant reduction in network traffic and communications delay. Among the others, ICN has been proposed as an implementation at the application layer [65]. Also, ICN plays an important role in the IoT context. In fact, since devices such as smart sensors and meters are becoming increasingly powerful, they start to act like users, and therefore have specific requirements at the application layer [66]. ICN is used in this context to provide higher network throughput and smaller transmission delays.
- *SDN* enables a more flexible network management compared to the traditional architectures. A global view of the network is maintained at the SDN software-based controllers, which receive requests from the different applications and provide them with resources to guarantee the required quality of service. At the application layer, SDN involves network components to provide abstraction and supervision for a proper network configuration at any time, as well as orchestration and resource allocation [67].
- *AI* is now largely adopted as a solution in different domains and all those applications in which classical methods for function parametrization or estimation are not viable. In its supervised implementation, AI exploits previously collected data to train a proper model, and successively takes decisions on newly generated data. AI is widely diffused in the wireless domain, finding applications such as channel estimation, fault recovery, and resource allocation [68]. We here focus on the challenges and security issues posed by the application of AI at the application layer.

A. VULNERABILITIES AND THREATS

As new kinds of services and paradigms are implemented at the application layer, the associated security and privacy threats pose a significant challenge for their successful deployment. Figure 2 summarizes the security and privacy threats at the application layer.

1) VEHICULAR NETWORKS

We discussed in the previous section how OBEs are in charge of dealing with the identities of each vehicle. This represents a privacy threat, because if an OBE is using the same identity in multiple broadcast messages, it is possible for an attacker to track the movements of the vehicle and hence compromise its privacy. Furthermore, application layer identities managed by OBEs should be protected from eavesdropping [40]. Since OBEs are also in charge of adjustments to the network topology based on the collected information [69], attacks from the users or central control may cause issues. Examples of associated threats are given by unencrypted transmission, information leakage, and resource depletion. Regarding the novel services guaranteed by 5G to vehicular communications, authors in [25] propose a protocol for video exchange based on the application layer. However, this protocol was deemed as non-secure by [26]. In fact, the protocol is vulnerable to several attacks, such as impersonation, forged video upload, and lack of proper separation between authorities. Therefore, it is essential to have a clear overview of all the application components, and to foresee all possible leverages that could undermine security and privacy.

2) BLOCKCHAIN

Among blockchain-based currencies, Bitcoin is the most widely used cryptocurrency thus far [21]. According to [21], Distributed Denial of Service (DDoS) represents a threat toward the Bitcoin protocol. DDoS attacks are capable of causing security breaches to Bitcoin currency exchanges, mining pools, and eWallets [21]. Therefore, the same issues can be reflected into the network application of the blockchain technology. For instance, in vehicular applications, a DDoS attack may cause the vehicle disconnection from the infrastructure, causing major damages to both the vehicle and the people in it. Transaction malleability has been pointed out as a cause for security issues [21], [23]. Blockchain uses cryptography to secure the peer-to-peer transaction [70]. Cryptography can be vulnerable if the wrong type of algorithm is used. For example, there is SHA-256 and double SHA-256. Among these two algorithms, double SHA-256 is the less vulnerable because it is not susceptible to length extension attacks [70]. Additional vulnerabilities to blockchain are replay attacks, sybil attacks, impersonation attacks, and man-in-the-middle attacks [70]. Another major

threat is given by the consensus protocol. In particular, 51% attack represents one of the major attacks, in which the majority of the mining power in the network is controlled by a single entity. In this case, this entity may control transactions preventing some of them to be concluded. This also allows the attacker to undermine the possibility of other users getting reward for mining a transaction, therefore monopolizing the reward associated with mining. Furthermore, this would allow the attacker to perform a double spend, in which the same asset is spent twice in the network due to the fact that the attacker gets to mine a transaction at the required time creating a fork in the network [21]. In an initial deployment state, where the network is populated by a small number of devices, the 51% attack represents a concrete threat for the consensus. Therefore, blockchain application designs shall consider all the significant threats highlighted in literature before obtaining a successful deployment.

3) INFORMATION-CENTRIC NETWORKING

Privacy represents one of the major problems in ICN. In fact, data is associated with names that reveal significant information to a passive eavesdropper. Names in ICN serve both as identifier and locator of data, allowing attackers to infer the identity of the provider based on the content. In a watchlist attack, a malicious user is able to build a predefined list of content names to monitor. The attacker then performs a real-time filtering to delete the request or the content itself based on the users' requests. Therefore the attacker is able to censor a content, or to perform a Denial of Service (DoS) attack toward a user accessing the content in the watchlist. Furthermore, the attacker is able to monitor a large number of requests for a certain content, hence jeopardizing the privacy of the users searching for that content [71]. ICN names are user-generated content that is recorded into the routing table. This implies that it is possible for a malicious user to act on the application layer to run a resource exhaustion attack. The very same freedom given by name spaces can also be used by producer applications to advertise any desired namespace [72]. A further threat is given by the possibility of an attacker being able to breach the signer's key. In fact, an attacker retrieving a certain content also has access to the singer's public key and signature. This can be used with the content itself to determine the signer's key [71].

4) SOFTWARE DEFINED NETWORK

The application layer of SDN architectures is vulnerable to multiple attacks, given by surfaces such as malicious or bugged applications and weak authorization or authentication [73]. For instance, third-party and control applications may be compromised if not equipped with proper authority restrictions. This may imply the execution of shut down or disconnect commands with the attacker gaining privileges over those applications. A further threat at the application layer is given by the installation of malicious applications on top of the controller. Such malicious applications can be exploited to manipulate and control packet handlers, by means of packet discard, reordering and disrupting proper packet forwarding. Furthermore, the same applications can be used to infer information about users' activities by means of packet sniffing. Another threat surface is given by the northbound interface, which connects the application plane with the control plane. In case of vulnerable protocols, Application Program Interfaces (APIs), or those without a proper encryption, sensitive information may be exposed to attackers, showing the information exchanged between the controller and the target application [73]. The SDN application layer is also vulnerable toward DoS attacks and their distributed version [74].

5) ARTIFICIAL INTELLIGENCE

One of the most critical threats toward AI is given by *adversarial learning*. The attacker aims at injecting malicious data inside the learning model, such that training is performed based on malformed/corrupted data. Considering, for instance, classification problem, the goal of adversarial learning is to inject malicious data such that classification no longer return the correct output. The assumption here is that the attacker is able to infer information from the legitimately trained classifier, such that an adversarial dataset can be built [75]. Therefore, an application leaking this kind of information or that can be queried from an external actor is sensitive to adversarial learning attacks. These two scenarios also arise a threat toward the privacy of users. In fact, if the training set is based on costumers' behavior or sensitive information, by querying the learning model, it is possible for an attacker to gather statistical information regarding users or to perform model inversion [76].

B. SECURITY SOLUTIONS, CHALLENGES AND GAPS

In vehicular networks, OBEs should carefully manage communication between different layers in order to notify changes in identities at the different layers. From an application layer perspective, OBE identity shall be protected from eavesdropping. A new protocol [25], is specific to 5G enabled vehicular networks and addresses reliable, secure and privacy-aware real-time video. In [26], authors analyzes and provides additional security solutions to that proposed in [25]. In order to solve for impersonation attack and forged video upload, public key cryptography is proposed as possible solution.

Transaction malleability has been resolved with ''segwit'' [21], which is implemented as a soft fork change in bitcoin's transaction format [22]. Conti *et al.* [21] conclude that for Bitcoin's continued success, it is important that the Bitcoin network scale easily as it grows in popularity and use. Currently, Bitcoin protocol can complete approximately seven transactions per second compared to Visa, which can complete approximately 2000 transactions per second [23]. The outstanding question is whether new security risks will arise while proposing a modified Bitcoin protocol to support greater transactions per second. Bitcoin protocol uses a hash functions such as SHA-256, so it will be important for the

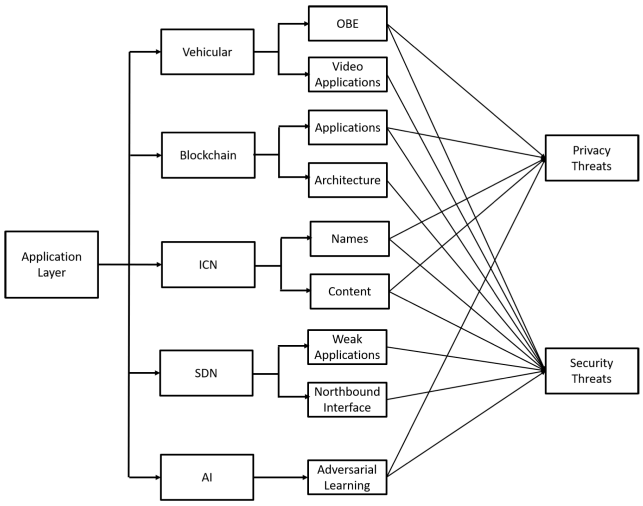


FIGURE 2. Security and privacy threats at the application layer.

Bitcoin protocol to be modified to work with stronger hashing algorithms as they are developed [21]. Several blockchain vulnerabilities can be addressed via Lightning Network and Smart Contract (LNSC) [70], [77]. The LNSC is expected to resolve replay attack, impersonation attack and man-in-the-middle attack [70] due to the lightning network's trading management system and the smart contract's general-purpose computations [77]. The sybil attack, which makes use of several fake identities controlled by a single lead fake identity, can be avoided by using TrustChain [70].

In SDN environments, DoS and its distributed version at the application layer pose a significant threat. Therefore, detection and mitigation of such attacks represents one of the core features for security. Machine learning can be exploited for this purpose [74]. However, has previously discussed, machine learning is vulnerable to adversarial attacks.

In ICN, data aggregation represents a significant threat towards users' privacy. Therefore, solutions such as the one proposed by authors in [78] need to be included to guarantee arbitrary data aggregation while preserving users' privacy.

In AI-based applications, adversarial learning poses one of the major threats. Therefore, a secure system needs to prevent malicious data to be injected in the learning phase. Different solutions for robust classification and anomaly detection have been proposed [79].

IV. PRESENTATION LAYER

The presentation layer formats the file so that the destination computer understands how to open and present it, including decompression and decryption of files [59], [80]. While encryption will continue to play an important role in 5G networks, research points to encryption via applications rather than at the presentation layer [14]. Vulnerabilities in layer six can be due to weaknesses in the implementation of the presentation layer functions [81]. Figure 3 summarizes the security and vulnerability threats at the presentation layer.

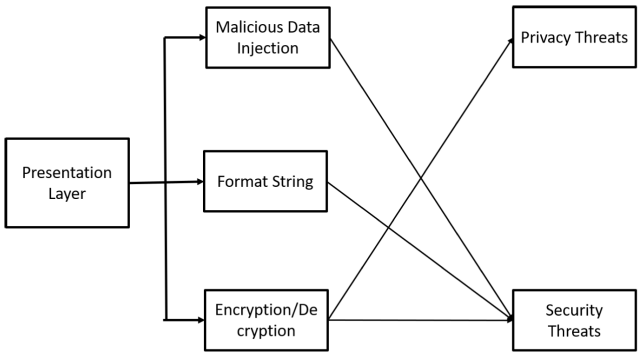


FIGURE 3. Security and privacy threats at the presentation layer.

A. VULNERABILITIES AND THREATS

The insertion of malicious data into files, web pages and applications is a common practice today. More than twenty years ago, Handel *et al.* [82] reported the possibility of hiding data in the presentation layer by using multimedia components. In recent years, social media applications such as YouTube, Facebook and TikTok have become very popular and are hence widely used. According to Pew Research Center, social media usage for adults has increased from five percent in 2005 to 72% in 2021 [83]. The increase in social media usage is caused, in turn, by the opportunity to insert malicious data into all forms of files used by these platforms, including audio and video. Attackers can insert illegal input into presentation-layer facilities in order to cause issues such as buffer overflows [81]. Inserting illegal input into multimedia files is an easy task for an attacker, as these files tend to be large in size [82]. Format string vulnerabilities can cause a program to crash, provide attackers access control to the program, and cause bad information to be displayed on the output stream [81]. Lastly, since instructions for encryption and decryption are provided at the presentation layer, this opens up vulnerabilities related to cryptography that can be exploited by the attackers to compromise the confidentiality requirements [81].

B. SECURITY SOLUTIONS, CHALLENGES AND GAPS

To proactively address the vulnerabilities at the presentation layer, Reed [81] advises thoroughly checking input resulting from the interaction of layers seven and five. This points to the need to provide security at all OSI layers, with each layer working together to guarantee the most secure network possible. Short-cuts in implementation plans that skip over a multi-layer security assessment may end up being disastrous. In addition, it is important to carefully review cryptography protocols periodically, considering the past issues arising with previously released crypto-solutions [81]. This is needed to ensure that not only the existing vulnerabilities and security issues are taken care of, but also to make sure that the emerging threats are proactively addressed before they result in an issue. In addition, the security solutions should diligently validate the input to create a clear delineation from the user input data to the data generated by the program, such that

the user input is safe to be used [81]. Any redesign to the presentation layer to resolve security concerns is expected to create additional opportunities for exploitation [82]. Hackers will hence maintain the ability to insert illegal input and take advantage of the format string vulnerabilities in 5G networks as well, if this is not properly mitigated.

V. SESSION LAYER

The session layer is used for application-to-application communications. This layer opens the communication connection, keeps it open while data is transferred, then closes it once the transfer is complete [59]. Session layer provides three security services: authentication, authorization and session restoration [84]. Examples of layer 5 protocols are Password Authentication Protocol (PAP), Remote Procedure Call (RPC) and NetBIOS [84]. Furthermore, an authentication framework that is widely used in wireless networks is Extensible Authentication Protocol (EAP) [59]. EAP framework provides the flexibility for authentication protocols to fit the specific need of an individual environment [59], [85], [86]. Abdrabou *et al.* indicate that in 4G environments, EAP-AKA is modified to support LTE and named Evolved Packet System Authentication and Key Agreement (EPS-AKA) [59]. For 5G networks, authentication is supported by 5G AKA and EAP-AKA', which is the 5G version of EPS-AKA [87]. 5G-AKA and EAP-AKA' are important for secure 5G networking, as they address several vulnerabilities in 4G authentication while being used to authenticate the nodes. Furthermore, they also support the Universal Mobile Telecommunications System (UMTS) [59]. Figure 4 summarizes the security and vulnerability threats at the session layer.

A. VULNERABILITIES AND THREATS

PAP is not very secure, as its credentials are sent in plaintext [59]. This allows an attacker to run sniffing and man-in-the-middle attacks [59]. Systems sometimes are built to use PAP as the last attempt to attaining authentication if other, more robust, authentication protocols do not work [59]. RPC fails to provide secure authentication [59], opening up the possibility of malicious activity. NetBIOS can be set up to permit shared resources in Windows environments [59]. Accordingly, this vulnerability can be used to discover information about various machines on a Windows NT network [88]. EAP as a stand-alone framework does not have security vulnerabilities. However, its variants may be non-secure [89]. An implementation vulnerability for the variant EAP-GSS and LEAP is a dictionary attack, which uses common words in a brute-force attempt to break the code [89]. EAP can use PAP and therefore may be vulnerable to threats associated with PAP [89]. EPS-AKA vulnerabilities include disclosure of the user identity, man-in-the-middle attacks and DoS attacks [90], [91].

B. SECURITY SOLUTIONS, CHALLENGES AND GAPS

To aid with the PAP plaintext vulnerability, administrators can build the system to support the Challenge Handshake Authentication Protocol (CHAP) [59]. To circumvent the NetBIOS vulnerability, the administrator can disable the system's null session ability using a very strong local admin passwords, and negate shared access to the root of the hard drive [92]. Secure RPC (SRPC) resolves the weak authentication associated with RPC [59]. Security challenges continue to exist with the EAP framework and its associated variants, such as EPS. Examples of such vulnerabilities include: disclosure of the user identity, man-in-the-middle attacks, and DoS attacks. 5G-AKA and EAP-AKA' provide solutions to some of the existing authentication issues in 4G and earlier generations [87]. Some of the key differences between 5G-AKA and EAP-AKA' are given by the operational flow and the exploited key derivation functions. Abdrabou and El-Wanis [86] propose the Simple Password Exponential Key Exchange (SPEKE) as a solution for the vulnerabilities. Another work by David Lanzenberger shows the vulnerabilities associated with EAP-AKA' and EPS-AKA*, the 5G successor to EPS-AKA. Lanzenberger's research concluded that EAP-AKA' has stricter guarantees with the drawback of a messaging overhead compared to EPS-AKA*. However, Lanzenberger's thesis proves EPS-AKA* has stronger authentication properties. Per analysis of Basin *et al.*, 5G-AKA is affected by several weaknesses, including session key agreement, unlinkability against active attacker and implicit authentication [87].

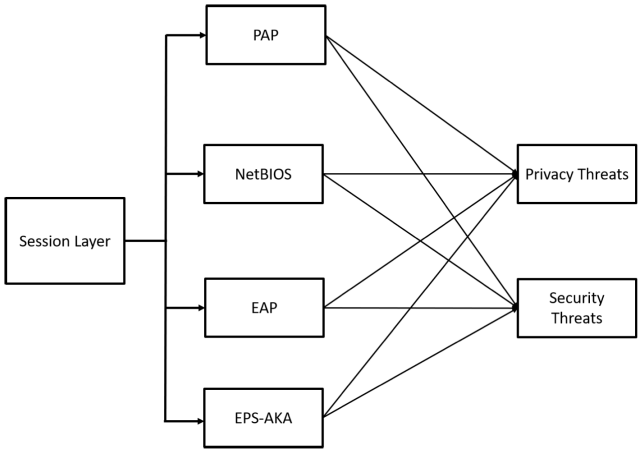


FIGURE 4. Security and privacy threats at the session layer.

VI. TRANSPORT LAYER

The transport layer has been referred to as the heart of the OSI model, as it is used for computer-to-computer communications [59]. Just like the session layer, it opens communications, keeps them open and closes them once complete [59]. SDN is one of the enabling technologies for the transport layer in 5G networks [93], [94]. It is believed that as 5G is adopted on a mainstream basis, the SDN will to play an important role to get the most out of 5G. As similar to software and hardware, SDN and 5G will dovetail each other. This section reviews transport layer information as it relates

to the 5G/SDN combo. Figure 5 summarizes the security and vulnerability threats at the session layer.

A. VULNERABILITIES AND THREATS

Transport Layer Security (TLS) from the SDN perspective is seen as vulnerable to DoS attacks, rule modification, and malicious rule insertion [94]. While SDN can improve the functionality of the 5G network, it does pose security challenges. Some of the vulnerabilities associated with SDN are:

- Weak authentication for the applications and users can lead to spoofing attacks;
- Weak authorization can also lead to man-in-the-middle and unauthorized access related attacks.

Security vulnerabilities and challenges for SDN are possible in different planes such as Application (for example, applications that abuse SDN control messages), Control (for example, manipulation of system variables), Interface (Man in the Middle attacks) and Data (Side channel attacks) [59]. In case of the application or user requesting a service from the 5G network, before routing information is created for packet traversal, a proper authorization is required for the accountability purposes. Lack of encryption standards can lead to eavesdropping or spoofing related attacks [95]. As SDN supports centralized control, it is an easy target for DoS attacks, and exposure of important APIs to the intruder. To implement DDoS attacks, the TCP or UDP SYN messages will be used to flood the host [95]. As a result of the DDoS attacks, the controller is made unavailable to serve other nodes in order to make routing decisions, thereby reducing the performance of the SDN networks. Due to its centralized nature, the controller represents a potential bottleneck and enables the adversaries to sniff the controller traffic [34]. The transport layer protocol proposed for 5G is open transport protocol (OTP) [96]. In OTP, TCP modifications and adaptations to retransmit the lost or damaged TCP segments over the wireless link are proposed as solution for 5G networks. As per our review, the vulnerabilities, threats and security challenges are not studied in detail. With respect to EAP-TLS, Zhang *et al.* point out several design flaws. For instance, 5G networks and subscribers cannot agree on the mutual identification and master key after the successful termination of the session, due to the ambiguities in the specified standards [97].

B. SECURITY SOLUTIONS, CHALLENGES AND GAPS

Security should be pre-built into the SDN architecture, and delivered as a service in order to provide privacy and integrity to connected resources [94], [98]. This is made possible by using an architecture with two communication channels, i.e., the control and data channels. The control channel transports only the control data between the control and data planes. On the other hand, the user communication data is transported only through the data channel [98]. As technology morphs and improves to release new solutions in areas such as SDN, security should be considered. Building the security into SDN will aid in defending against attacks at the transport layer [94], and in turn will defend against attacks towards the overall 5G architecture. This is achieved by designing components to secure the SDN controller, protecting the flow layer of the SDN, and hardening interfaces such as application programming interfaces and communication channels [94].

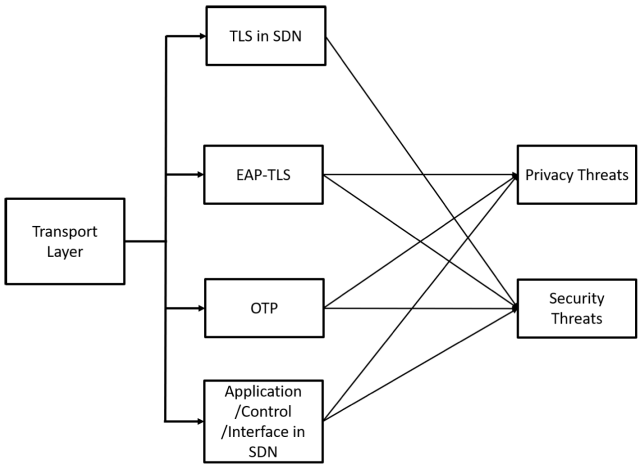


FIGURE 5. Security and privacy threats at the transport layer.

Since SDN inherently provides the logical centralized control, it supports robust security monitoring and protection. It also enables rapid deployment of security policies, that may not be easily possible in traditional security approaches. The SDN approach by Ahmed *et al.* has the potential to provide security protection not only from a virtualized environment perspective, but also from a physical environment perspective [34]. To address the issues in EAP-TLS, Zhang *et al.* approached the solution in a formal manner. However, their approach has some limitations due to their assumption of perfect cryptography, which may not hold in practical implementations [97]. There are several open issues that need attention in securing SDN. For example, network virtualization in SDN is vulnerable to multiple issues such as rewrite problems, spoofing attacks, implementation of action isolation, and DoS attacks etc. [94]. In the future, these security challenges at the transport layer need to be addressed by the security community to ensure the security of 5G.

VII. NETWORK LAYER

The network layer instructs packet routing. This layer supports adding information as to where, how, and when packet routing happens in order to prevent congestion. With 5G networking, security will need to be implemented in multiple OSI model layers to ensure the protection of data. ICN plays an important role at the network layer as well, as it has been proposed as a new paradigm to tackle the inefficiencies and architectural problem of existing networks. The network layer of ICN assigns a unique name to each content, which is later used for routing over the network. Different from IP-based

routing, content requests search for the closest available copy regardless of the destination machine's address.

This section investigates the security issues of both traditional IP-based content routing and ICN. In the former architecture, we investigate the use of IPsec to achieve security at the network layer. Figure 6 summarizes the security and vulnerability threats at the network layer.

A. VULNERABILITIES AND THREATS

Breaking the IPSec is generally considered not feasible [15]. However, IPSec alone cannot provide security for 5G networking. It must work in conjunction with other successful security protocols in other layers of the OSI model to ensure security [15].

Apart from generic threats like DoS, other threats from the network layer perspective include man-in-the-middle attack, IP Spoofing, injection, eavesdropping, packet sniffing, and Gateway attacks represent a significant threat. Due to the new technologies in 5G, specialized threats such as virtualization and multi-edge computing, edge node overload, and abusing of edge open APIs need to be taken into consideration [99]. One of the innovations that is proposed in 5G network standard is network slicing, which has unique security challenges. For example, if an adversary gets access to one slice, they can conduct attacks on other network slices, resulting in security threats toward confidentiality, integrity and availability. Specifically, if an adversary is able to tamper the network slice selection data, unauthorized devices or the adversaries may use such information to connect to a particular network slice and consume resources [100]. Network Function Virtualization Infrastructure, which is part of 5G network, has several potential threats and vulnerabilities, such as the potential infection of Virtual Machine (VM) images by the attacker. These infections, in turn, result in data leakage, DoS attacks, performance degradation of other VMs, and hijacking of the components of the compromised hypervisor [41].

Although ICN may prevent attacks to the IP-based internet architecture such as DoS, it is still vulnerable to different types of attacks [101]. In fact, resource exhaustion, publisher unavailability, and route depletion pose threats toward the availability of the content. For instance, considering stateful routing, routers need to keep record of requested/received packets per interface until the request is consumed. This mechanism is vulnerable to DoS attacks, in which the attacker aims at disrupting forward services or overloading network traffic by issuing an excessive number of requests. Requests flooding can also be exploited to jeopardize the publisher's availability. In fact, by sending an excessive number of requests for the same content publisher, the publisher's availability is undermined and the related content unreachable. In route depletion attacks, saturation is exploited at the routing table, filling it with malicious content belonging to different domains. This jeopardizes the correct forward of content requests to publishers or to available cached data copies. Furthermore, delay in the replies or lack of replies may also be exploited by an attacker to disrupt users' services [102].

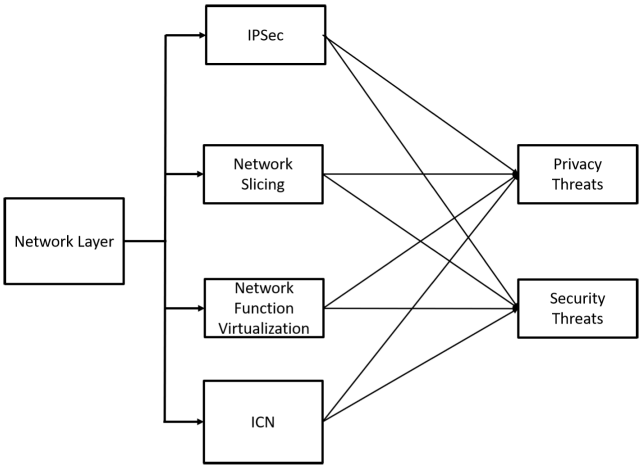


FIGURE 6. Security and privacy threats at the network layer.

Content caching exhibits vulnerabilities undermining content integrity and availability. Examples of attacks toward caching include cache snooping, pollution and poisoning [101]. In cache snooping, the attacker obtains sensitive information regarding a user or a group of users, therefore undermining their privacy. This may be obtained by gaining access to lists of cached content and by monitoring its content, or the time difference between replies from publisher or nearby caches. The gain obtained by caching may be disrupted by means of cache pollution. In fact, if an attacker populates a cache with useless content, the routing algorithm needs to search content in remote points in the network. Cache poisoning also exploits the injection of malicious data in caches. In this case, however, the attacker's goal is to distribute fake content in the network [103].

B. SECURITY SOLUTIONS, CHALLENGES AND GAPS

For the segment between the Broadcast Multicast - Service Center and Evolved Node Base station, IPSec can provide authenticity, integrity, and confidentiality over a unicast link [15]. Implementation of IPSec at the network layer will be fundamental in providing confidentiality, integrity, data-origin authentication, and protection against replay attacks for each individual packet [6], [104]. Unfortunately, IPSec cannot extend all the way to the User Equipment (UE). We will discuss different security measures in the Physical layer section to provide base station to UE security solutions. Saleem *et al.* propose in [99] bio-inspired techniques to address several types of network attacks. However, the authors have not implemented and evaluated their approach [99]. While some solutions have been proposed for network slicing, there are several limitations and gaps that need to be addressed. Machine learning-based solutions have been proposed to address the security threats in network layer. However, the experimentation has not been conducted in a realistic scenario, so the proposed solutions cannot be deemed as reliable in real-world scenarios [105], [106].

For a successful deployment of ICN, security solutions should provide content integrity and availability, authenticity, certified content provenance, and ensure users' privacy [71]. In order to prevent the aforementioned DoS attacks to content routing, hash functions on pending request tables have been proposed as a countermeasure. Content caching attacks may instead be prevented by means of signature verification, and by monitoring caches' content. Although different solutions have been proposed for content routing [107]–[109] and caching attacks [110]–[112], still mobility and scalability represent a significant challenge. Furthermore, centralization shall be avoided, in order to prevent a single point of failure being a target for the attacker. Figure 7 summarizes the security and vulnerability threats at the data link layer.

VIII. DATA LINK LAYER

The data link layer supports the integrity of the point-to-point transmission. It determines what type of technology and protocol is being used, so data can be successfully transferred to the physical layer [59]. The 5G protocols consists of a user plane (UP) and a control plane (CP). The UP layer refers to the Data Link Layer. This layer is made up of four different sublayers: service data adaptation protocol, packet data convergence protocol, radio link control, and medium access control [113]. In 5G, flexibility is one important security requirement that needs to be considered. For example, some applications would require end-to-end security rather than relying on the security functionality provided by the core network. For those applications, that require end to end security, the applications would require security considerations in data link layer [114]

Wireless point-to-point protocol transmission examples are IEEE 802.11 and Bluetooth. The standard 802.11, also known as WiFi, is the original wireless local area network standard protocol which has since been improved to 802.11ac, with a transfer max rate of 1.3 gigabytes per second [59], [113]. Bluetooth, on the other hand, has a max rate of three megabytes per second and a much smaller range of connectivity of 10 meters [59]. In this section we discuss the vulnerabilities and solutions for IEEE 802.11 and Bluetooth.

A. VULNERABILITIES AND THREATS

The Access Stratum (AS) that is associated with the UP traffic is vulnerable to multiple threats, and further protection is required. This, in turn, results in customer data and communication flow being intercepted between the user equipment and centralized server by the rogue base stations. Possible solutions include Integrity Protection security algorithms [115]. Sybil attack also represent a threat in this context, where the attacker replicates and manages more than one identity on a single device [116].

In 2015, C. Kolias *et al.* released a study on IEEE 802.11 security protocols. WEP, WPA and WPA2 were studied to identify vulnerabilities relating to 5G networking. The study concluded that easily obtainable penetration tools are effective and good enough to break IEEE 802.11 security [113]. For example, CloudCracker is capable of evaluating 300 million WPA passwords in 20 minutes, and therefore potentially cracking a WiFi password in a reasonable time frame [113]. Bluetooth is a high-risk protocol in public areas because of the ease of transferring data to a close range [59]. Bluejacking and Bluesnarfing are two types of attacks that, when a user accepts an unsolicited message, result in personal information leakage [59]. Attacks in the mobile edge computing environment is possible in this layer through DDoS type of attacks [115].

The routing process, i.e., delivery of the packet from the sender to the transmitter in a multi-hop network, may be vulnerable to different types of attack. In particular, blackhole attacks are the most impactive ones. In a blackhole attack the attacker, upon receiving a packet to forward in the routing process, eliminates the packet therefore preventing it from reaching the intended receiver [117], [118]. A different version of this attack is grayhole attack, with the main difference that the attacker does not systematically drop packets. Instead, packets are dropped in a random fashion [119]. Although grayhole attacks may have lower impact in the overall network, they are also more difficult to be identified, as random drops may be due to malfunctioning of devices. Another variant of this attack is given by the sinkhole attack, where a node advertises itself as the best route in the network, such that packets are pass through it and are redirected to the sink node and hence discarded [120].

In a fog environment, IoT devices are vulnerable to multiple treats at the data link layer. In fact, due to their limited power resources and to the huge number of connected devices, they provide multiple attack surfaces [121]. Example of such attacks are DoS, and replay attacks, where a data packet is captured by the attacker and retransmitted in later sessions to impersonate the victim node. Furthermore, these devices are vulnerable to sybil attacks, where malicious node generates a fake virtual node to exploit resources from the network.

B. SECURITY SOLUTIONS, CHALLENGES AND GAPS

Some of the attacks at the data link layer could be prevented by end-to-end security encryption protocols such as SSL [115]. Threat intelligence solutions using machine learning and artificial intelligence can also be applied to mitigate threats at the user plane level. For example, device type and behavior profile can be detected to identify and mitigate botnets, malware, DDoS attacks etc. Augmented protection approaches using extensible authentication protocol (EAP) may help the core network to authenticate the devices the secondary protection at this layer [115].

Authors in [113] suggest two solutions for WiFi security, 1) updating the firmware on Access Points, and 2) deploying Machine Learning-based Intrusion Detection Systems. In [116] authors suggest the use of Received Singal Strength (RSS) to identify and exclude intruders that duplicated a node identity in 802.11 ad hoc based networks. The study in [113] indicates that updating the firmware may be impractical.

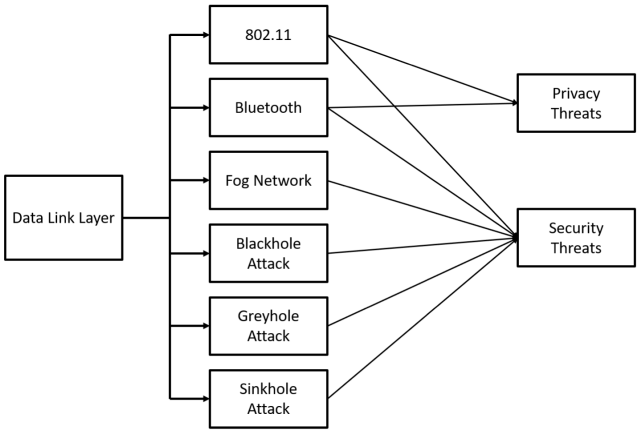


FIGURE 7. Security and privacy threats at the data link layer.

With respect to the machine learning-based solution, the slow convergence of the learning algorithms is an issue for their application in Intrusion Detection System, and should be taken into consideration. This is particularly critical when mitigating real-time attacks. Real time solutions for machine learning-based intrusion detection systems represent a fundamental component of 5G network. A possible solution is proposed by authors in [122], where a light gradient boosting machine is used as detection algorithm. A deep learning based approach is proposed by authors in [123], where an autoencoder network is trained to recognize four different type of attacks. Although most of the intrusion detection systems is based on machine learning techniques [124], non machine learning-based solutions can be exploited to mitigate the aforementioned shortcomings. For instance, the energy consumption of nodes and a suitable blacklist can be exploited in conjunction with connected dominating sets [125]. A different approach for intrusion detection considers also the location of the devices, where a null space-based homomorphic MAC scheme can be deployed to guarantee efficient detection in terms of computational complexity and communication overhead [126]. Cause effect relationship an also be exploited for intrusion detection. In particular, a code book based approach can be exploited to associate keys to alerts to facilitate the alert correlation process [127]. However, significant research efforts are still needed to provide general real-time intrusion detection systems. As a third-party security measure, a Virtual Private Network (VPN), can provide an additional layer of security by acting as a container for the 802.11 network [113]. Bluetooth can be secured by simply making the device undiscoverable when in public areas [59]. In regards to the DDoS types of attacks, a combination of caching, anti-DDoS technologies can mitigate the DDoS attacks [115]. One of the important challenges for security solution at this layer is balancing latency and power requirements as the high-speed encryption and integrity requirements would mean high power consumption, which is again a limitation in the mobile environment [115]. To address the Sybil and replication attacks, techniques such as building trusted certification solution for infrastructure-less domain. In addition, the techniques such as resource (radio, storage and computational) testing and position verification, to counter identity replication and spoofing [116].

Different solutions have been proposed in literature to mitigate blackhole, grayhole, and sinkhole attacks. The joint identification of blackhole and grayhole attacks has been proposed by authors in [125], and a preamble TDMA solution is proposed to mitigate the effect of such attacks. Authors in [119] propose a system based on trust levels assigned to node. Data is periodically collected from network's nodes to verify both the data authenticity and consequently assign a trust level. A solution based on count based detection scheme has been proposed by authors in [120] to mitigate sinkhole attacks. Each node in the network needs to report its hop count to the base station, which keeps track of the values reported by each node to detect possible sinkhole attacks.

Solutions for fog computing and IoT devices include authorization, cryptography, collision detection and error correcting codes [121].

IX. PHYSICAL LAYER

The physical layer, also known as layer one, deals with voltage values, which in turn are converted to digital signals, and transmitted by a physical electrical or optical port [59]. The core of the 5G infrastructure will remain connected with physical fiber cable, but the edge of the 5G infrastructure - the segment closest to the UE - will be predominately wireless [14], [16], [128]. Three progressive 5G technologies are within the wireless segment: HetNet, massive MIMO, and mmWave [128], [129]. The term HetNet refers to a network in which different cell types and access technologies coexist, playing a fundamental role in the expansion of the 5G network. Massive MIMO envisions the deployment of a larger number of antennas compared to previous antennas technology. mmWave instead envisions the shift towards higher transmission frequencies. Therefore, MIMO and mmWave refer to more physical related aspects. Since wireless signals are transmitted through the air, hackers have opportunities to to intercept and interfere with the wireless segment [128]. In this section, we discuss the physical layer security and threats in 5G networks. Figure 8 summarizes the security and vulnerability threats at the physical layer.

A. VULNERABILITIES AND THREATS

Due to the transmission of wireless signals in free space, attackers can obtain private information from oscillations in the observed power [14]. Eavesdropping enables the attacker to obtain cipher text. Merely obtaining the cipher text does not mean the attacker can read it. However, if a large number of cipher texts is captured, it is easier to infer the security scheme applied at the upper OSI layers, and opening the gate for private information to be stolen [14]. Data fabrication and privacy violation attacks exploit physical layer vulnerabilities during wireless transmissions [5]. Signal amplification

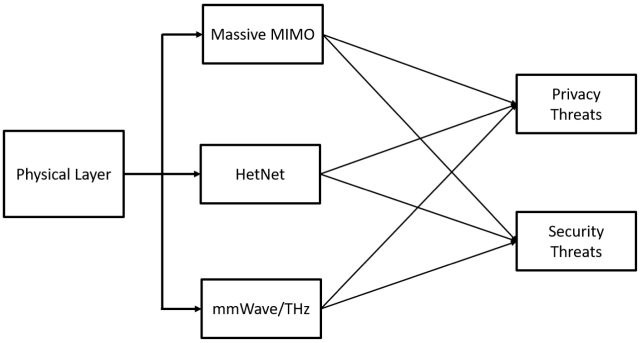


FIGURE 8. Security and privacy threats at the physical layer.

attacks currently exist in 4G networks and are expected to increase on 5G. A signal amplification attack can be performed by botnets using various infected devices within a single cell area [42], [43]. The increase in ports on mobile devices opens the possibility of attacks through multiple forms of connectivity [42]. Ports can be physical and logical. Mobile devices are especially vulnerable to logical port attacks, as each mobile app may present the opportunity for an attacker to take advantage of an open port in the individual app. According to the University of Michigan, open ports can be used to obtain private information [130]. As each user adds a new app to their mobile device, the vulnerabilities increase.

One of the security issues concerning heterogeneous network is how to define an access authentication method that can adapt to various network structures [131]. Also, due to the open nature of the wireless channel of 5G heterogeneous networks, the wireless communication system is more vulnerable to imitation, theft, and other external attacks that needs attention and security by design. Due to the complex nature and higher requirements for 5G networks, the resulting wireless communication network system is complex and highly modular. Hence, if one module is under attack, the entire wireless communication network system security is jeopardized.

B. SECURITY SOLUTIONS, CHALLENGES AND GAPS

Atat *et al.* and Gao *et al.* provide three possible solutions to eavesdropping: power control, beamforming, and clustering [5], [14]. Power control relies on detecting the wire-tappers and adjusting the transmission power. By making changes to the transmission power, the eavesdropper will not be able to access the private information [14]. Beamforming also involves identifying attackers by using transmission power. Beamforming and power control can be used together, but the algorithm implementing such a solution has not been perfected yet [14]. Clustering involves grouping users together to keep out the hacker [5], [14]. Clustering must work hand in hand with a method to identify the hackers, such that they can be isolated from a non-hacker group [14]. It is also suggested by authors in [5] that Device to Device (D2D) communication can help in defending against eavesdropping, data fabrication, and policy violations by defining a specific spatial transmission region that guarantees a minimum secrecy rate. PLS is a new network security solution that entails the use of noise, interference and fading to decrease the ability for intruders to capture readable data [132]. Yang *et al.* [128] state that degrading signal reception can be exploited as a security mechanism to prevent intruders from obtaining confidential information. Furthermore, they also show the benefits of a decreased computational complexity with respect to higher layers cryptography [128]. Reduced power consumption and artificial noise insertion in massive MIMO systems are effective in averting eavesdropping attacks [128]. As for devices' ports, a suggested workplace solution is to scan all employees' phones for viruses or scan employees' phones randomly [42].

A PLS solution against eavesdroppers has been proposed by authors in [133]. Authors propose a jamming solution to design secure routing paths in multi-hop decentralized IoT, showing good performance against an increasing number of eavesdroppers. A further solution for secure routing has been proposed by authors in [134], where authors propose a jamming mechanism with optimized transmit power to efficiently deliver the content while preserving data security. In the MIMO context, different PLS solutions based on artificial noise have been proposed. A viable solution is represented by the introduction of an Imaginary Receiver (IR), and the precoding matrix is generated targeting the IR. This solution provides the advantage that the imaginary receiver does not feedback its channel response hence preventing eavesdropping of the precoder matrix [135]. Artificial noise can also be designed to lie in the null subspace of the receiver channel while being present in all other channels [136], [137]. Artificial noise is also used in intelligent transportation systems. For instance, it can be exploited to guarantee a secure communication while offloading part of the data from increased network quality of service [138]. Furthermore, multiple vehicles can be exploited to cooperatively generate noise schemes to secure the communication [139].

mmWave has limitations, which can be turned into benefits. mmWave is deemed to have built-in security and privacy due to limited transmission area, inability to penetrate solid materials, and the narrow beam widths [140]. By using mmWave in private or public office buildings, it is possible to prevent leakage of information outside the building. Tang *et al.* propose PLS enhancements for authentication, secret key distribution, and secure communication perspective to defend against security attacks in 5G networks [141].

Alquhayz *et al.* implemented a policy-based security management system to ensure that end-user devices cannot be used as weapons or tools of attack. They evaluated the proposed framework by implementing it using threat models such as IP spoofing and man-in-the-middle (MITM) attacks [142]. However, the framework is limited by a methodology that gives isolated end-user devices their privileges back [142]. Zhou *et al.* noted that sharing of large-scale spectrum in 5G heterogeneous networks leads

to many security and privacy challenges [143]. To address these issues, they developed a privacy-preserving, incentive-compatible, and spectrum-efficient framework that is based on blockchain. In this framework, they built a smart contract, which allows the users to sign a contract with the base station for spectrum sharing and receive dedicated payments based on their contributions. In addition, they also built the framework to support the details of secure spectrum sharing and consensus-based incentive mechanism design [143]. The proposed solution is limited due to performance degradation issues, which can be improved further by learning through historical observations such as user behavior, load profiles and traffic distribution. The solution also did not consider multiple service providers or multiple base stations. The hash algorithms that aid the proof of work has vulnerabilities, and they need to be addressed [143]. Lv *et al.* implemented a deep learning solution to solve the security issues of the 5G heterogeneous network from the physical layer perspective [131]. In addition, they also surveyed and presented the existing security issues in 5G heterogeneous networks. The proposed method only handles the issues at the physical layer and not the other layers, such as network layer. According to Lv *et al.*, the security problems in the network layer will need to be discussed in future works.

Anum *et al.* surveyed and presented the physical layer security issues of massive MIMO-enabled Heterogeneous networks [144]. They also provided an insight into the secrecy outage and secrecy rates of the users when their security is breached by attackers. Anum *et al.* observed that a trade-off exists between the optimal coverage and the secrecy in the network, and further work needs to be done to optimize the coverage and ensure security. Wu *et al.* utilized the intrinsic randomness of the transmission channel to guarantee the security in the physical layer challenged by the heterogeneous networks [32]. They also outlined several challenges that need to be handled as a part of future work. For example, most works for physical layer security in heterogeneous networks focus on analyzing the security performance of the networks [32]. Since multiple users have access to multiple tiers, a possible research strategy is to investigate how to properly schedule these users access to different network ties to better safeguard multi-tier communications.

As reflected above, many works in the literature have focused on 5G security at the physical layer [44], [145]. It can be concluded that PLS is the key framework for 5G security, as it contributes to secure 5G at every layer of the OSI model. However, due to the lack of direction as to which standards will eventually be implemented in the 5G environment, it is difficult to determine which protective measures are worth further investigation. This uncertainty is not uncommon in technology, and multiple standards are likely to be heavily financed and researched. Since it has not been determined if one single 5G technology, such as HetNets, will win out over another, it is difficult to focus on one set of security issues. For example, Ciena mentions the use of heterogeneous networks [16], while Verizon implements its 5G network through small cell technology and mmWave bands [2]. The scale of the 5G network could impact the ability of security solutions to work [14], so HetNets, MIMO, mmWave, and D2D, can be used depending on the scale of the solution.

X. SUMMARY OF 5G SECURITY CONCERNS AND RECOMMENDATIONS FOR FUTURE WORK

In this paper, we showed that security concerns are still present at each layer of the OSI model in 5G. Table 3 provides a summary of the identified vulnerabilities, solutions and challenges organized according to the OSI model. The table begins with the Application layer and ends with the Physical layer. In some cases, limited or null published information was found regarding a specific solution or challenge. We indicate these situations by a ''not found'' comment. Based on our review, following are future 5G security research:

- Application Layer: scalability represents one of the major threats to safe identity management in vehicular networks. While including blockchain technology in different components of the network, increasing the amount of transactions that the application layer bitcoin protocol can handle per second represents one of the main targets. Considering this improvement in the transaction rate, researchers should also take care of the arising security concerns connected with it. All new network paradigms, such as SDN and ICN, may contribute to increase the quality of the network in different aspects. Still, data availability and user privacy need to be fully investigated before their successful deployment. AI may further contribute to a better network experience both from designers' and users' perspectives. However, significant threats are posed on user's privacy and data integrity.
- Presentation Layer: researchers should look at the system for periodical review and update of the cryptographic protocols to address data hiding and illegal input into presentation layer protocols.
- Session Layer: researchers should pay particular attention to sniffing and man-in-the-middle attacks. In addition, the EPS-AKA protocol should be enhanced by looking into the key agreement from the home network's user equipment with respect to serving network identification issues.
- Transport Layer: before SDN matures and 5G is generally deployed, it will be beneficial to pre-build SDN security into the infrastructure.
- Network Layer: researchers should look at the ways IPSec can be extended for 5G security to provide confidentiality and integrity against replay attacks all the way to the user equipment level. When considering ICN, researchers should focus on the scalability of the network. Furthermore, mobility poses a major challenge for a secure deployment of ICN.
- Data Link Layer: researchers should improve the learning speed of machine learning based Intrusion Detection System (IDS) to ensure the feasibility of protecting

TABLE 3. Summary of 5G security concerns and solutions by OSI layers.

5G Security Concerns by OSI Layers				
Layer #	Layer Name	Vulnerability and Threats	Solution, *proposed	Challenge
7	Application	A. DDoS - bitcoin protocol [21] B. Transaction Malleability - bitcoin protocol [21] C. Forged video upload connected car [26]	A. Not found B. SegWit [21] C. Public Key Cryptography* [26]	A & B: Bitcoin protocol has a lower limit on transactions per second. If the protocol is modified to support greater numbers of transactions per second, stronger hash functions will also need to be incorporated [23] C. Proposed solution that requires additional evaluation [21]
6	Presentation	A. Hiding data in presentation layer using multimedia components [82] B. Illegal input into presentation layer facilities causing buffer overflows [81] C. Format string vulnerabilities [81]	A, B, C. Thoroughly check input and output from layers 7 and 7 [81] A, B, C. Review of cryptography protocols periodically [81]	A, B, C. There are no recent research papers found on the security of the presentation layer
5	Session	A. Sniffing and man-in-the- middle attacks due to PAP credentials in plaintext [59] B. NetBIOS permitting resource sharing on Windows NT [88] C. Disclosure of user identify, DoS, and man-in- the-middle attacks with EPA-AKA [90], [91]	A. Not found B. Admin to disable system's null session ability and use strong admin passwords [92] C. EPS-AKA & SPEKE* [86]	A & B. Not found C. EAP-AKA' has stricter guarantees but exchanges more messages than EPS-AKA*. EPS-AKA* has stronger authentication properties but has a gap in that it did not achieve key agreement for the home network with the user equipment on the identity of the serving network [146]
4	Transport	A. DoS attacks, rule modification, and malicious rule insertion at the southbound interface of SDN [94]	A. Pre-build security into SDN architecture [94], [98]	A. Security should be considered in the SDN architecture but a solution on how this can be done was not found [94]
3	Network	A. Confidentiality, integrity, and replay attacks [6], [104]	A. IPsec [15]	A. IPSec cannot extend all the way to the user equipment (UE). Security measures at other layers of OSI are required [6], [104]
2	Data Link	A. Penetration tools available to break IEEE 802.1 [113]	A. Update firmware on access points, Machine Learning IDS*, RSS* [113]	A. Updating firmware may be impractical, MLIDS may have low learning speeds, RSS is vulnerable to noise interference [113], [116]
1	Physical	A. Release of private info from power leakage in wireless signal [14] B. Eavesdropping [14] C. Data fabrication [5] D. Signal amplification [42], [43] E. Increase of ports to attack [42]	A & B. Power control, beamforming, and clustering [5], [14] B & C. Define spatial transmission region, use of D2D communications, use of PLS [5] D. Not found. E. Scan for viruses [42]	A, B, C, D, E. It will be imperative to narrow down the 5G physical layer technologies in an attempt to capture the best technology with the strongest security solutions versus continuing research on multiple technologies

against real-time attacks. Furthermore, researchers should look at the noise interference issues in the RSS.

- Physical Layer: due to the numerous emerging technologies dealing with the physical layer of 5G, it could be beneficial to narrow down the list of employed technologies to a small list in order to capture the best solution, instead of deeply investigating multiple technologies. Also, since signaling amplification is a known issue in 4G, 5G solutions should consider it as a possible threat to mitigate.

XI. CONCLUSION

5G technology is expected to connect billions of sensors [5] and millions of devices [6]. There is a financial spend and gain associated with these deployments that will impact the world. Due to this significant impact, resolving security issues is an important task for 5G companies, investors, researchers and individuals. The expected quantity of connected devices naturally expands the opportunity for hackers to exploit networking at several layers of the OSI layer model. While application-based encryption secures the application itself, it is not sufficient to provide security for data traversing 5G mobile networks due to power leakage in wireless signaling [14]. 5G networks will require a different approach from cryptographic techniques, with the viable solutions in the domain of PLS [17], [128]. Our study reflects the high research interest in securing 5G at the physical layer. Security mechanisms such as noise interference, beamforming and degrading signal reception are introduced in order to protect data from threats such as eavesdropping and data fabrication. In addition to the physical layer findings, we identified security issues at the application layer with bitcoin protocol and in connected cars. At the network layer, we point out the importance of IPsec along with a penetration

tool vulnerability with 802.11 at the data link layer. There are known existing vulnerabilities and attacks at the session layer, such as disclosure of user identify, DoS and man-in-the-middle attacks with EPA-AKA and EPS-AKA. There is an immediate opportunity for research at the session layer to solve for the vulnerabilities, along with the opportunity to secure emerging technologies like SDN. Organizations and researchers can prepare for 5G by investing in areas where vulnerabilities exist, and by ensuring emerging technologies complement the existing security in all layers of the OSI model.

REFERENCES

[1] Z. Kotulski, T. W. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, T. Osko, and J.-P. Wary, "Towards constructive approach to end-to-end slice isolation in 5G networks," *EURASIP J. Inf. Secur.*, vol. 2018, no. 1, Dec. 2018.

[2] Verizon. (2019). *5G is Here*. [Online]. Available: https://www.verizon.com/about/news/5G-here

[3] A. Gupta and E. R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[4] A. Dogra, R. K. Jha, and S. Jain, "A survey on beyond 5G network with the advent of 6G: Architecture and emerging technologies," *IEEE Access*, vol. 9, pp. 67512–67547, 2021.

[5] R. Atat, L. Liu, H. Chen, J. Wu, H. Li, and Y. Yi, "Enabling cyber-physical communication in 5G cellular networks: Challenges, spatial spectrum sensing, and cyber-security," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 1, pp. 49–54, 2017.

[6] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in Internet of Things: Challenges, solutions and future directions," in *Proc. 49th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2016, pp. 5772–5781.

[7] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, 2013.

[8] J. Park, S. Samarakoon, H. Shiri, M. K. Abdel-Aziz, T. Nishio, A. Elgabli, and M. Bennis, "Extreme URLLC: Vision, challenges, and key enablers," 2020, *arXiv:2001.09683*. [Online]. Available: http://arxiv.org/abs/2001.09683

[9] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Comput. Netw.*, vol. 167, Feb. 2020, Art. no. 106984.

[10] O. Serhane, K. Yahyaoui, B. Nour, and H. Moungla, "A survey of ICN content naming and in-network caching in 5G and beyond networks," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4081–4104, Mar. 2021.

[11] P. Pirinen, "A brief overview of 5G research activities," in *Proc. 1st Int. Conf. 5G Ubiquitous Connectivity*, 2014, pp. 17–22.

[12] R. Jover and V. Marojevic, "Security and protocol exploit analysis of the 5G specifications," *IEEE Access*, vol. 7, pp. 24936–24956, 2019.

[13] R. F. Olimid and G. Nencioni, "5G network slicing: A security overview," *IEEE Access*, vol. 8, pp. 99999–100009, 2020.

[14] Y. Gao, S. Hu, W. Tang, Y. Li, Y. Sun, D. Huang, S. Cheng, and X. Li, "Physical layer security in 5G based large scale social networks: Opportunities and challenges," *IEEE Access*, vol. 6, pp. 26350–26357, 2018.

[15] R. Annessi, J. Fabini, and T. Zseby, "To trust or not to trust: Data origin authentication for group communication in 5G networks," in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, pp. 1–7.

[16] B. Lavallee. (2016). *Why 5G Will Change Everything About the Network*. [Online]. Available: https://www.ciena.com/insights/articles/Why-5G-Will-Change-Everything-About-The-Network_prx.html

[17] N.-P. Nguyen, T. Q. Duong, H. Q. Ngo, Z. Hadzi-Velkov, and L. Shu, "Secure 5G wireless communications: A joint relay selection and wireless power transfer approach," *IEEE Access*, vol. 4, pp. 3349–3359, 2016.

[18] J. Chokun. (2018). *Who Accepts Bitcoins as Payment? List of Companies, Stores, Shops*. [Online]. Available: https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins

[19] Newegg. *Bitcoin Accepted*. [Online]. Available: https://promotions.newegg.com/nepro/16-6277/index.html

[20] Kryptomoney. (2017). *Subway Accepts Bitcoin as Payment*. [Online]. Available: https://kryptomoney.com/subway-accepts-bitcoins-in-payment

[21] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[22] D. Mechkaroska, V. Dimitrova, and A. Popovska-Mitrovikj, "Analysis of the possibilities for improvement of BlockChain technology," in *Proc. 26th Telecommun. Forum (TELFOR)*, Nov. 2018, pp. 1–4.

[23] G. Vidan and V. Lehdonvirta, "Mine the gap: Bitcoin and the maintenance of trustlessness," *New Media Soc.*, vol. 21, no. 1, pp. 42–59, Jul. 2018, doi: 10.1177/1461444818786220.

[24] D. Kaushik and A. Gupta, "Ultra-secure transmissions for 5G-V2X communications," *Mater. Today, Proc.*, Jan. 2021.

[25] H. Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7868–7881, Mar. 2016.

[26] S. G. Yoo, "5G-VRSec: Secure video reporting service in 5G enabled vehicular networks," *Wireless Commun. Mobile Comput.*, vol. 2017, pp. 1–22, Jan. 2017.

[27] R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G security: A review of design and implementation issues," *Future Gener. Comput. Syst.*, vol. 101, pp. 842–864, Dec. 2019.

[28] G. Bora, S. Bora, S. Singh, and S. M. Arsalan, "OSI reference model: An overview," *Int. J. Comput. Trends Technol.*, vol. 7, no. 4, pp. 214–218, Jan. 2014.

[29] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[30] X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu, and M. Yi, "Overview of 5G security technology," *Sci. China Inf. Sci.*, vol. 61, no. 8, pp. 1–25, 2018.

[31] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.

[32] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[33] M. A. Ferrag, L. Maglars, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *J. Netw. Comput. Appl.*, vol. 101, pp. 55–82, Jan. 2018.

[34] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Sep. 2017, pp. 193–199.

[35] R. Hussain, F. Hussain, and S. Zeadally, "Integration of VANET and 5G security: A review of design and implementation issues," *Future Gener. Comput. Syst.*, vol. 101, pp. 843–864, Dec. 2019.

[36] P. P. Sriram, H.-C. Wang, H. G. Jami, and K. Srinivasan, "5G security: Concepts and challenges," in *5G Enabled Secure Wireless Networks*. Springer, 2019, pp. 1–43.

[37] G. Choudhary, J. Kim, and V. Sharma, "Security of 5G-mobile backhaul networks: A survey," 2019, *arXiv:1906.11427*. [Online]. Available: http://arxiv.org/abs/1906.11427

[38] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[39] X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu, and M. Yi, "Overview of 5G security technology," *Sci. China Inf. Sci.*, vol. 61, no. 8, pp. 1–25, 2018.

[40] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar. 2020.

[41] S. Zhang, Y. Wang, and W. Zhou, "Towards secure 5G networks: A survey," *Comput. Netw.*, vol. 162, Oct. 2019, Art. no. 106871.

[42] G. Mantas, N. Komninos, J. Rodriuez, E. Logota, and H. Marques, "Security for 5G communications," Tech. Rep., 2015, pp. 207–220.

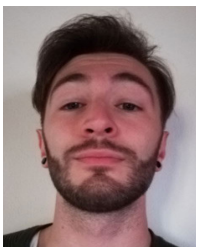
[43] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.

[44] J. Sánchez, L. Urquiza-Aguiar, M. Paredes, and D. Osorio, "Survey on physical layer security for 5G wireless networks," *Ann. Telecommun.*, vol. 76, no. 3, pp. 1–20, 2020.
[45] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.
[46] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
[47] Y. Lu, "Blockchain: A survey on functions, applications and open issues," *J. Ind. Integr. Manage.*, vol. 3, no. 4, Dec. 2018, Art. no. 1850015.
[48] P. Lapsley, "The history of phone phreaking," in *Exploding the Phone*. Grove Press, 2011, pp. 1–448.
[49] K. R. Santhi, V. K. Srivastava, G. SenthilKumaran, and A. Butare, "Goals of true broad band's wireless next wave (4G-5G)," in *Proc. IEEE 58th Veh. Technol. Conf. (VTC-Fall)*, vol. 4, Oct. 2003, pp. 2317–2321.
[50] T. Halonen, J. Romero, and J. Melero, *GSM, GPRS and EDGE Performance: Evolution Towards 3G/UMTS*. Hoboken, NJ, USA: Wiley, 2004.
[51] S. Gindraux, "From 2G to 3G: A guide to mobile security," in *Proc. 3rd Int. Conf. 3G Mobile Commun. Technol.* Edison, NJ, USA: IET, 2002, pp. 308–311.
[52] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
[53] S. Sesia, I. Toufik, and M. Baker, *LTE—The UMTS Long Term Evolution: From Theory to Practice*. Hoboken, NJ, USA: Wiley, 2011.
[54] B. Furht and S. A. Ahson, *Long Term Evolution: 3GPP LTE Radio and Cellular Technology*. Boca Raton, FL, USA: CRC Press, 2016.
[55] Y. E. H. El Idrissi, N. Zahid, and M. Jedra, "Security analysis of 3GPP (LTE)—WLAN interworking and a new local authentication method based on EAP-AKA," in *Proc. 1st Int. Conf. Future Gener. Commun. Technol.*, 2012, pp. 137–142.
[56] M. Liyanage and A. Gurtov, "Secured VPN models for LTE backhaul networks," in *Proc. IEEE Veh. Technol. Conf. (VTC Fall)*, Sep. 2012, pp. 1–5.
[57] M. Liyanage, M. Ylianttila, and A. Gurtov, "A case study on security issues in LTE backhaul and core networks," in *Case Studies in Secure Computing: Achievements and Trends*, vol. 1. Boca Raton, FL, USA: CRC Press, p. 167, Aug. 2014.
[58] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli, "5G evolution: A view on 5G cellular technology beyond 3GPP release 15," *IEEE Access*, vol. 7, pp. 127639–127651, 2019.
[59] S. Harris and F. Maymi, "Cissp exam guide," Tech. Rep., 2016, pp. 483–1083.
[60] M. Rahouti, K. Xiong, and N. Ghani, "Bitcoin concepts, threats, and machine-learning security solutions," *IEEE Access*, vol. 6, pp. 67189–67205, 2018, doi: 10.1109/ACCESS.2018.2874539.
[61] M. Lucas. (2017). *The Difference Between Bitcoin and Blockchain for Business*. https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-bitcoin-and-blockchain-for-business/
[62] M. Moniruzzamana, S. Khezra, A. Yassineb, and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges," *Comput. Electr. Eng.*, vol. 83, May 2020, Art. no. 106585.
[63] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102693.
[64] X. Ling, J. Wang, Y. Le, Z. Ding, and X. Gao, "Blockchain radio access network beyond 5G," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 160–168, Dec. 2020.
[65] R. Ullah, M. A. U. Rehman, M. A. Naeem, B.-S. Kim, and S. Mastorakis, "ICN with edge for 5G: Exploiting in-network caching in ICN-based edge computing for 5G networks," *Future Gener. Comput. Syst.*, vol. 111, pp. 159–174, Oct. 2020.
[66] M. Huang, A. Liu, N. N. Xiong, T. Wang, and A. V. Vasilakos, "An effective service-oriented networking management architecture for 5G-enabled Internet of Things," *Comput. Netw.*, vol. 173, May 2020, Art. no. 107208.
[67] N. Psaromanolakis, A. Ropodi, P. Fragkogiannis, K. Tsagkaris, L. A. Neto, A. El Ankouri, M. Wang, G. Simon, and P. Chanclou, "Software defined networking in a converged 5G fiber-wireless network," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2020, pp. 225–230.
[68] R. Shafin, L. Liu, V. Chandrasekhar, H. Chen, J. Reed, and J. Zhang, "Artificial intelligence-enabled cellular networks: A critical path to beyond-5G and 6G," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 212–217, Apr. 2020.
[69] S. Wan, R. Gu, T. Umer, K. Salah, and X. Xu, "Toward offloading internet of vehicles applications in 5G networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4151–4159, Jul. 2021.
[70] D. Dasgupta, J. M. Shrein, and K. D. Gupta, "A survey of blockchain from security perspective," *J. Banking Financial Technol.*, vol. 3, no. 1, pp. 1–17, Apr. 2019, doi: 10.1007/s42786-018-00002-6.
[71] E. G. AbdAllah, H. S. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1441–1454, 3rd Quart., 2015.
[72] E. Ngai, B. Ohlman, G. Tsudik, E. Uzun, M. Wählisch, and C. A. Wood, "Can we make a cake and eat it too? A discussion of ICN security and privacy," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 47, no. 1, pp. 49–54, Jan. 2017.
[73] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, "Security in SDN: A comprehensive survey," *J. Netw. Comput. Appl.*, vol. 159, Jun. 2020, Art. no. 102595.
[74] C. Benzaïd, M. Boukhalfa, and T. Taleb, "Robust self-protection against application-layer (D)DoS attacks in SDN environment," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, May 2020, pp. 1–6.
[75] D. Lowd and C. Meek, "Adversarial learning," in *Proc. 11th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2005, pp. 641–647.
[76] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 3–18.
[77] K. Wang, Y. Zhang, S. Guo, M. Dong, R. Q. Hu, and L. He, "IEEE access special section editorial: The Internet of Energy: Architectures, cyber security, and applications," *IEEE Access*, vol. 6, pp. 79272–79275, 2018.
[78] C. Xu, L. Zhang, L. Zhu, C. Zhang, X. Du, M. Guizani, and K. Sharif, "Aggregate in my way: Privacy-preserving data aggregation without trusted authority in ICN," *Future Gener. Comput. Syst.*, vol. 111, pp. 107–116, Oct. 2020.
[79] D. J. Miller, Z. Xiang, and G. Kesidis, "Adversarial learning targeting deep neural network classification: A comprehensive review of defenses against attacks," *Proc. IEEE*, vol. 108, no. 3, pp. 402–433, Mar. 2020.
[80] A. F. Behrouz and C. Sophia, "Data communications and networking," *Forouzan With Sophia Chung Fegan*, 2007.
[81] D. Reed, "Applying the OSI seven layer network model to information security," *SANS GIAC GSEC Practical Assignment*, p. 8, Nov. 2003.
[82] T. Handel, G. Theodore, and T. Maxwell, "Hiding data in the OSI network model," in *Proc. Int. Workshop Inf. Hiding*, 1996, pp. 23–28.
[83] Pew Research Center. *Social Media Fact Sheet*. [Online]. Available: https://www.pewresearch.org/internet/fact-sheet/social-media/
[84] W. F. Emmons and A. S. Chandler, "OSI session layer: Services and protocols," *Proc. IEEE*, vol. 71, no. 12, pp. 1397–1400, Dec. 1983.
[85] S. Sotillo, "Extensible authentication protocol (EAP) security issues," Dept. Technol. Syst., East Carolina Univ., Greenville, NC, USA, Tech. Rep., Nov. 2007, pp. 1–6.
[86] M. A. Abdrabou and A. El-Wanis, "Security enhancement for LTE authentication protocol (EPS-AKA)," in *Proc. Int. Conf. Aerosp. Sci. Aviation Technol.*, vol. 16, May 2015, pp. 1–23.
[87] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2018, pp. 1383–1396.
[88] E. Schultz. (2000). *The Windows NT Network Environment*. [Online]. Available: http://www.informit.com/articles/article.aspx?p=130690&seqNum=11
[89] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput. Secur.*, vol. 105, Jun. 2021, Art. no. 102248.
[90] M. A. Abdrabou, A. D. E. Elbayoumy, and E. A. El-Wanis, "LTE authentication protocol (EPS-AKA) weaknesses solution," in *Proc. IEEE 7th Int. Conf. Intell. Comput. Inf. Syst. (ICICIS)*, Dec. 2015, pp. 434–441.
[91] H. Ghorbani, M. S. Mohammadzadeh, and M. H. Ahmadzadegan, "DDoS attacks on the IoT network with the emergence of 5G," in *Proc. Int. Conf. Technol. Entrepreneurship-Virtual (ICTE-V)*, Apr. 2020, pp. 1–5.
[92] T. Olzak. (2007). *The Problem With Netbios*. [Online]. Available: https://www.techrepublic.com/blog/it-security/the-problem-with-netbios

[93] M. Knight. (2017). *5G+SDN: When Worlds Collide*. [Online]. Available: https://about.att.com/innovationblog/when_worlds_collide
[94] A. Akhunzada, A. Gani, N. B. Anuar, A. Abdelaziz, M. K. Khan, A. Hayat, and S. Khan, "Secure and dependable software defined networks," *J. Netw. Comput. Appl.*, vol. 61, pp. 199–221, Feb. 2016.
[95] J. Yao, Z. Han, M. Sohail, and L. Wang, "A robust security architecture for SDN-based 5G networks," *Future Internet*, vol. 11, no. 4, p. 85, Mar. 2019.
[96] A. Gohil, H. Modi, and S. K. Patel, "5G technology of mobile communication: A survey," in *Proc. Int. Conf. Intell. Syst. Signal Process. (ISSP)*, Mar. 2013, pp. 288–292.
[97] J. Zhang, L. Yang, W. Cao, and Q. Wang, "Formal analysis of 5G EAP-TLS authentication protocol using proverif," *IEEE Access*, vol. 8, pp. 23674–23688, 2020.
[98] M. Liyanage, I. Ahmed, M. Ylianttila, J. L. Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, E. M. De Oca, A. Valtierra, and C. Jimenez, "Security for future software defined mobile networks," in *Proc. 9th Int. Conf. Next Gener. Mobile Appl., Services Technol.*, Sep. 2015, pp. 256–264.
[99] K. Saleem, G. M. Alabduljabbar, N. Alrowais, J. Al-Muhtadi, M. Imran, and J. J. P. C. Rodrigues, "Bio-inspired network security for 5G-enabled IoT applications," *IEEE Access*, vol. 8, pp. 229152–229160, 2020.
[100] X. Zhang, A. Kunz, and S. Schröder, "Overview of 5G security in 3GPP," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Sep. 2017, pp. 181–186.
[101] E. Mannes and C. Maziero, "Naming content on the network layer: A security analysis of the information-centric network model," *ACM Comput. Surveys*, vol. 52, no. 3, pp. 1–28, Jul. 2019.
[102] M. Wählisch, T. C. Schmidt, and M. Vahlenkamp, "Lessons from the past: Why data-driven states harm future information-centric networking," in *Proc. IFIP Netw. Conf.*, 2013, pp. 1–9.
[103] N. Fotiou, G. F. Marias, and G. C. Polyzos, "Towards a secure rendezvous network for future publish/subscribe architectures," in *Proc. Future Internet Symp.* Berlin, Germany: Springer, 2010, pp. 49–56.
[104] M. Jinsong and M. Yamin, "5G network and security," in *Proc. 7th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, 2020, pp. 249–254.
[105] J. Li, Z. Zhao, and R. Li, "Machine learning-based IDS for software-defined 5G network," *IET Netw.*, vol. 7, no. 2, pp. 53–60, Mar. 2017.
[106] N. Haider, M. Z. Baig, and M. Imran, "Artificial intelligence and machine learning in 5G network security: Opportunities, advantages, and future research trends," 2020, *arXiv:2007.04490*. [Online]. Available: http://arxiv.org/abs/2007.04490
[107] J. Burke, P. Gasti, N. Nathan, and G. Tsudik, "Secure sensing over named data networking," in *Proc. IEEE 13th Int. Symp. Netw. Comput. Appl.*, Aug. 2014, pp. 175–180.
[108] H. Dai, Y. Wang, J. Fan, and B. Liu, "Mitigate DDoS attacks in NDN by interest traceback," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2013, pp. 381–386.
[109] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS and DDoS in named data networking," in *Proc. 22nd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2013, pp. 1–7.
[110] M. Conti, P. Gasti, and M. Teoli, "A lightweight mechanism for detection of cache pollution attacks in named data networking," *Elsevier Comput. Netw.*, vol. 57, no. 16, pp. 3178–3191, 2013.
[111] S. DiBenedetto and C. Papadopoulos, "Mitigating poisoned content with forwarding strategy," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2016, pp. 164–169.
[112] N. Ntuli and S. Han, "Detecting router cache snooping in named data networking," in *Proc. Int. Conf. ICT Converg. (ICTC)*, Oct. 2012, pp. 714–718.
[113] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 184–208, 1st. Quart., 2016.
[114] P. Schneider and G. Horn, "Towards 5G security," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 1165–1170.
[115] 5G Americas. (2020). *Security Considerations for the 5G Era. A 5G Americas White Paper*. https://www.5gamericas.orgwp-contentuploads202007Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf
[116] M. Faisal, S. Abbas, and H. U. Rahman, "Identity attack detection system for 802.11-based ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 128, Dec. 2018.
[117] G. Li, Z. Yan, and Y. Fu, "A study and simulation research of blackhole attack on mobile AdHoc network," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, May 2018, pp. 1–6.
[118] K. H. Mohammadani, K. A. Memon, I. Memon, N. N. Hussaini, and H. Fazal, "Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 5, May 2020, Art. no. 155014772092162.
[119] S. Huang, Z. Zeng, K. Ota, M. Dong, T. Wang, and N. N. Xiong, "An intelligent collaboration trust interconnections system for mobile information control in ubiquitous 5G networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 1, pp. 347–365, Jan. 2021.
[120] L. C. Sejaphala and M. Velempini, "The design of a defense mechanism to mitigate sinkhole attack in software defined wireless sensor cognitive radio networks," *Wireless Pers. Commun.*, vol. 113, no. 2, pp. 977–993, Jul. 2020.
[121] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, "Fog computing security challenges and future directions [energy and security]," *IEEE Consum. Electron. Mag.*, vol. 8, no. 3, pp. 92–96, May 2019.
[122] D. Jin, Y. Lu, J. Qin, Z. Cheng, and Z. Mao, "SwiftIDS: Real-time intrusion detection system based on LightGBM and parallel intrusion detection mechanism," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 101984.
[123] M. Lin, B. Zhao, and Q. Xin, "ERID: A deep learning-based approach towards efficient real-time intrusion detection for IoT," in *Proc. IEEE 8th Int. Conf. Commun. Netw. (ComNet)*, Oct. 2020, pp. 1–7.
[124] A. A. Salih and A. M. Abdulazeez, "Evaluation of classification algorithms for intrusion detection system: A review," *J. Soft Comput. Data Mining*, vol. 2, no. 1, pp. 31–40, Apr. 2021.
[125] Z. A. Zardari, J. He, N. Zhu, K. Mohammadani, M. Pathan, M. Hussain, and M. Memon, "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs," *Future Internet*, vol. 11, no. 3, p. 61, Mar. 2019.
[126] R. Parsamehr, G. Mantas, J. Rodriguez, and J.-F. Martinez-Ortega, "IDLP: An efficient intrusion detection and location-aware prevention mechanism for network coding-enabled mobile small cells," *IEEE Access*, vol. 8, pp. 43863–43875, 2020.
[127] E. Mahdavi, A. Fanian, and F. Amini, "A real-time alert correlation method based on code-books for intrusion detection systems," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101661.
[128] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[129] A. Gupta, R. K. Jha, and S. Jain, "Attack modeling and intrusion detection system for 5G wireless communication network," *Int. J. Commun. Syst.*, vol. 30, no. 10, p. e3237, Jul. 2017.
[130] M. Riggins. (2017). *Mobile Device Security: Defend Your Ports!* [Online]. Available: https://inspiredelearning.com/blog/open-ports/
[131] Z. Lv, A. K. Singh, and J. Li, "Deep learning for security problems in 5G heterogeneous networks," *IEEE Netw.*, vol. 35, no. 2, pp. 67–73, Mar. 2021.
[132] L. Sun, K. Tourki, Y. Hou, and L. Wei, "Safeguarding 5G networks through physical layer security technologies," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–2, Sep. 2018.
[133] Y. Xu, J. Liu, Y. Shen, J. Liu, X. Jiang, and T. Taleb, "Incentive jamming-based secure routing in decentralized Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 3000–3013, Feb. 2021.
[134] Y. Xu, J. Liu, Y. Shen, X. Jiang, Y. Ji, and N. Shiratori, "QoS-aware secure routing design for wireless networks with selfish jammers," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 4902–4916, Aug. 2021.
[135] Y. Tanigawa, Y. Kozai, and T. Saba, "A physical layer security scheme employing imaginary receiver for multiuser MIMO-OFDM systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.
[136] M. Ahmed and L. Bai, "Space time block coding aided physical layer security in Gaussian MIMO channels," in *Proc. 14th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Jan. 2017, pp. 805–808.
[137] Y. Liu, H.-H. Chen, and L. Wang, "Secrecy capacity analysis of artificial noisy MIMO channels—An approach based on ordered eigenvalues of Wishart matrices," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 617–630, Nov. 2016.
[138] Y. Liu, W. Wang, H.-H. Chen, F. Lyu, L. Wang, W. Meng, and X. Shen, "Physical layer security assisted computation offloading in intelligently connected vehicle networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, pp. 3555–3570, Jun. 2021.

[139] X. Luo, Y. Liu, H.-H. Chen, and Q. Guo, "Physical layer security in intelligently connected vehicle networks," *IEEE Netw.*, vol. 34, no. 5, pp. 232–239, Sep. 2020.
[140] L. Wei, R. Q. Hu, Y. Qian, and G. Wu, "Key elements to enable millimeter wave communications for 5G wireless systems," *IEEE Wireless Commun.*, vol. 21, no. 6, pp. 136–143, Dec. 2014.
[141] J. Tang, H. Wen, K. Zeng, R.-F. Liao, F. Pan, and L. Hu, "Light-weight physical layer enhanced security schemes for 5G wireless networks," *IEEE Netw.*, vol. 33, no. 5, pp. 126–133, Sep. 2019.
[142] H. Alquhayz, N. Alalwan, A. I. Alzahrani, A. H. Al-Bayatti, and M. S. Sharif, "Policy-based security management system for 5G heterogeneous networks," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–14, Nov. 2019.
[143] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks," *IEEE Netw.*, vol. 34, no. 1, pp. 24–31, Jan. 2020.
[144] A. Umer and S. A. Hassan, "Physical layer security in 5G hybrid heterogeneous networks," in *5G Enabled Secure Wireless Networks*. Springer, 2019, pp. 103–121.
[145] M. Shakiba-Herfeha, A. Chorti, and H. V. Poor, "Physical layer security: Authentication, integrity, and confidentiality," in *Physical Layer Security*. Cham, Switzerland: Springer, 2021, pp. 129–150.
[146] D. Lanzenberger. (2017). *Formal Analysis of 5G Protocols*. [Online]. Available: https://www.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/information-security-group-dam/research/software/5G_lanzenberger.pdf

S. SULLIVAN received the master's degree in information systems technology from Coastal Carolina University, in 2020. She is currently a Senior Telecom Engineer with Windstream Communications, where her current work focuses on applying data analytics and business intelligence to the equipment lifecycle management of telecom equipment. She is also the Leader and a Women Member of Windstream Employee Resource Group, whose mission is to support women professionally and personally. Her research interests include 5G technology, network security, cyber security, diversity, and inclusion.



ALESSANDRO BRIGHENTE (Student Member, IEEE) received the Ph.D. degree in information engineering from the University of Padua, in February 2021. From June 2019 to November 2019, he was a Visiting Researcher at Nokia Bell Labs, Stuttgart. He is currently a Postdoctoral Researcher with the SPRITZ Research Group, University of Padua. He is involved in European projects (Ontochain) and company projects (IOTA) with the University of Padua. His current research interests include security and privacy in cyber-physical systems, UAV communications, vehicular networks, blockchain/distributed ledger technology, and physical layer security.

S. A. P. KUMAR (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the University of Louisville, KY, USA, in 2007. He is currently an Associate Professor of computer science with the Department of Electrical Engineering and Computer Science, Cleveland State University, Cleveland, OH, USA. He is also the Co-Director of Cleveland State University TECH Hub, an interdisciplinary center related to technology. He is directing the Intelligent Secure Cyber-Systems Analytics and Applications Research (ISCAR) Laboratory, Cleveland State University. He has published more than 50 technical articles in international journals and conference proceedings. His current research interests include cybersecurity, machine learning, big data analytics, and secure distributed systems and their applications.

M. CONTI (Senior Member, IEEE) received the Ph.D. degree from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Postdoctoral Researcher with Vrije Universiteit Amsterdam, The Netherlands. In 2011, he joined as an Assistant Professor with the University of Padua, where he became an Associate Professor, in 2015, and a Full Professor, in 2018. He has been a Visiting Researcher with GMU, UCLA, UCI, TU Darmstadt, UF, and FIU. He is currently a Full Professor with the University of Padua, Italy. He is also affiliated with TU Delft and the University of Washington, Seattle. His research is funded by companies, including Cisco, Intel, and Huawei. His main research interests include the area of security and privacy. In this area, he has published more than 400 papers in topmost international peer-reviewed journals and conferences. He is a fellow of the Young Academy of Europe. He is a Senior Member of the ACM and a member of the Blockchain Expert Panel of the Government of Italy. He has been awarded with a Marie Curie Fellowship, by the European Commission, in 2012, and a Fellowship by the German DAAD, in 2013. He was the Program Chair of TRUST 2015, ICISS 2016, WiSec 2017, and ACNS 2020, and the General Chair of SecureComm 2012, SACMAT 2013, CANS 2021, and ACNS 2022. He is an Area Editor-in-Chief of IEEE Communications Surveys & Tutorials, and has been an Associate Editor of several journals, including IEEE Communications Surveys & Tutorials, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, and IEEE Transactions on Network and Service Management.