Accepted Manuscript

Integration of VANET and 5G Security: A review of design and implementation issues

Rasheed Hussain, Fatima Hussain, Sherali Zeadally

PII: S0167-739X(19)30690-9
DOI: https://doi.org/10.1016/j.future.2019.07.006
Reference: FUTURE 5059

To appear in: *Future Generation Computer Systems*

Received date : 15 March 2019
Revised date : 9 June 2019
Accepted date : 4 July 2019

Please cite this article as: R. Hussain, F. Hussain and S. Zeadally, Integration of VANET and 5G Security: A review of design and implementation issues, *Future Generation Computer Systems* (2019), https://doi.org/10.1016/j.future.2019.07.006

Integration of VANET and 5G Security: A Review of Design and Implementation Issues

Rasheed Hussain[a,*], Fatima Hussain[b], Sherali Zeadally[c]

[a]*Networks and Blockchain Lab, Innopolis University, Innopolis, Russia*
[b]*Royal Bank of Canada, Toronto, Canada*
[c]*College of Communication and Information, University of Kentucky, Lexington, KY 40506-0224, US*

Abstract

The commercial adaptation of Vehicular Ad hoc NETwork (VANET) to achieve secure Intelligent Transportation System (ITS) heavily depends on the security guarantees for the end-users and consumers. Current VANET security standards address most of the security challenges faced by the vehicular networks. However, with the emergence of 5th generation (5G) networks, and the demand for a range of new applications and services through vehicular networks, it is imperative to integrate 5G and vehicular networks. To achieve a seamless integration, various design and implementation issues related to 5G and VANETs must be addressed. We focus on security issues that need to be considered in order to enable the secure integration of 5G and VANETs. More precisely, we conduct in-depth study of the current security issues, solutions, and standards used in vehicular networks and then we identify the security gaps in the existing VANET security solutions. We investigate the security features of 5G networks and discuss how they can be leveraged in vehicular networks to enable a seamless and efficient integration. We also propose a security architecture for vehicular networks wherein the current VANET security standards and 5G security features coexist to support secure VANET applications. Finally, we discuss some future challenges and research directions for 5G-enabled secure

*Corresponding author
Email address: r.hussain@innopolis.ru (Rasheed Hussain)

vehicular networks.

Keywords: Architecture, Connected car, 5G VANET, Security, VANET applications

1. Introduction

Over the last couple of decades, the automotive industry has been the hotbed of technological innovation as a result of significant advances in computation, communication, and storage technologies. The main drivers behind such innovations stem from the problems faced by the transportation systems. Every year, thousands of people lose their lives and billions of dollars are spent on medical bills and insurance costs. These huge costs have led to the development of a wide range of new transportation technologies which can enable a safe and comfortable driving experience and provide additional value-added services to both drivers and passengers [1]. In this context, the Intelligent Transportation System (ITS) provides a secure and reliable driving experience by employing vehicles to communicate with each other and with the environment that includes both infrastructure and the pedestrians. In other words, ITS is achieved through Vehicular Ad hoc NETwork (VANET) where vehicles communicate with the environment through Vehicle-to-Everything (V2X) communication paradigm [2]. V2X includes Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), Vehicle-to-Cloud (V2C) communications and so on [3, 4]. VANET applications include a wide range of transportation aspects such as driving safety to traffic management, route optimization, comfort, traffic information, fleet management, automation of traffic-related functions (such as traffic lights), platooning, and entertainment such as e-advertisements, Internet on the wheels, and so on. Most of these applications leverage cooperative communication mechanisms among vehicles and with the infrastructure [5, 6]. To support these aforementioned applications, vehicles need to share their current information with their neighbors via different messages that conform to ITS standards. These messages include Cooperative

Awareness Messages (CAMs), safety messages, warning alerts, and so on. CAMs are broadcasted to the neighbors at a high frequency ranging from 100 Hz to 300 Hz depending on the current traffic situation and the underlying applications [7]. CAM includes current mobility-related and control features such as current position, speed, acceleration, azimuth, brake status, and steering angle.

1.1. VANET Applications Requirements

The various categories of VANET applications have diverse requirements such as performance, Quality of Service (QoS), security and privacy. In essence, safety-related applications exhibit stringent security requirements such as mutual authentication, authorization, integrity, resilience against attacks, non-repudiation, and trust management. From a performance perspective, such applications are sensitive to both latency and delay (i.e., they require a minimum delay and latency) because the decisions based on the information in such messages directly affect human lives [8, 9, 10]. Furthermore, these applications also require context-awareness and must be secure against security attacks. In contrast, entertainment and other value-added VANET applications and services are comparatively delay-tolerant and have less stringent security requirements. For instance, the frequently-broadcasted CAMs use relatively less-sophisticated cryptographic primitives than emergency alarm messages [11]. Other important security requirements for VANET applications include resilience against profiling where attackers use location data to profile different users based on their movements, sybil attacks where attackers create fake nodes that may cause illusion for the decision-support system of the VANET application, and so on [12, 13]. However, non-safety applications tend to be bandwidth-intensive and need more computation resources. For instance, video-on-demand, Internet-on-the-wheels, and other such services on the road need higher bandwidth and speed to be able to provide the required QoS. Many of these aforementioned applications generate a massive amount of data that needs to be gathered, processed, and then acted upon [14]. VANET uses On-Board Unit (OBU), Road-Side Unit (RSU) and back-end servers to perform these tasks.

1.2. VANET Communication Standard and Related Challenges

Since early on, VANET has been using Dedicated Short-Range Communication (DSRC) which uses 75 MHz bandwidth (in the 5.9 GHz band) [15]. There are different notions used for this standard in the United States and Europe. In the US, it is referred to as Wireless Access in Vehicular Environment (WAVE-1609) whereas it is called TC-ITS by the European Telecommunications Standards Institute (ETSI). These standards mandate a communication range of 300 meters to 1000 meters for the participating nodes. However, these are theoretical limitations whereas in the real-world scenario, the transmission range is affected by many factors such as the geometry of the surrounding objects and line-of-sight. Experimental results have revealed that the aforementioned external factors deteriorate the effective transmission range [16, 17, 18]. Therefore, the existing VANET standards are inadequate for the services and applications promised by VANET. In this context, VANET also supports other communication standards in addition to DSRC/WAVE that include, cellular (3G, LTE(A), and 5G), WiFi, Visible Light Communication (VLC), WiMax, and so on [19, 20, 21, 22]. These additional communication technologies expand the application space of the VANET and its integration with other enabling technologies such as the Internet of Things (IoT), cloud computing, and so on [23, 24, 3, 25, 26]. Despite the benefits offered by these technologies for VANET, they also open up performance and security challenges for the traditional VANET. For instance, cellular networks (3G, 4G) may solve the bandwidth problem for bandwidth-hungry VANET applications, but they adversely affect the latency. These networks also incur other overheads (such as hand-off, authentication), and cellular-specific security attacks that could jeopardize the entire VANET application space [27]. Additionally, since safety-related applications need minimum latency, cellular communications might not be suitable for emergency messages in VANET. Integration with IoT, cloud computing, and other similar technologies faces similar challenges where the inherent security challenges of these technologies are inherited in VANET [28]. Therefore, we need a holistic approach to provide high performance and strong security for

VANET applications.

To date, several research efforts have been made to address the security issues in VANET from different perspectives such as mutual authentication, authorization, defense against different attacks, secrecy, information integrity, confidentiality, conditional anonymity, availability, audibility, fairness, communication security, and so on [29, 12, 30, 31]. Attacks on VANET often focus on the vulnerabilities of these communication frameworks. Besides, extensive research has also been conducted in both traditional VANET (through DSRC/WAVE) and integrated VANET (through cellular and other technologies) [32, 2, 33, 34, 35]. Although DSRC and cellular technologies support different functional requirements of VANET applications, they have their own shortcomings. DSRC/WAVE-based communication is more reliable when the message needs to be delivered in a close proximity with tight latency requirements and optionally stringent security primitives. In contrast, cellular networks provide high network bandwidth. Furthermore, cellular networks also increase the transmission range of the VANET nodes. From the preceding discussion, we note that DSRC suffers from low bandwidth and transmission range, whereas cellular networks (3G, LTE, and LTE-A) suffer high latency which is challenge for safety and real-time applications (such as communication in autonomous cars). Additionally, security is also a crucial shortcoming in the cellular networks because of various reasons: the cellular architecture at its core is based on Internet Protocol (IP) which exposes it to the IP-based attacks such as false information injection, Distributed Denial of Service (DDoS), spoofing, and others. Furthermore, the ephemeral nature of VANET nodes also poses serious challenges for cellular communications where handover, (re)authentication and network disconnection put the security and performance of the applications at jeopardy [27]. Moreover, cellular networks not only support vehicular networks but they also help in integrating other enabling technologies with VANET. Whilst this integration increases the applicability of VANET, it also increases the attack surface for VANET. User privacy is another serious concern with the Long-Term Evolution/Long-Term Evolution Advanced (LTE/LTE-A) where attackers could launch identity-theft attacks on the cellular architecture through vulnerable Mobile Management Entity (MME). In addition to the aforementioned security issues, there are several other issues that need to be addressed while using 3G and LTE/LTE-A as communication technologies in VANET. To this end, we need a new communication paradigm in VANET that addresses scalability, flexibility for different applications, quality of service, security, connectivity, and adaptability.

Among other disruptive technologies developed during the past couple of decades, industry and academia have focused on the development of 5th Generation (5G) communication to address the shortcomings of existing communication technologies as well as meet the requirements of growing demands for high-bandwidth, low-latency, and secure applications [36]. In this context, VANET can also leverage the distinctive features of 5G along with cloud computing to handle the large amount of data generated by vehicular nodes through vehicular clouds [37]. Furthermore, the integration of VANET and IoT has also been envisioned and researched to broaden the application domain of both VANET and IoT. Since VANET applications and services exhibit different performance and security requirements, DSRC or cellular (3G and LTE/-A) alone would not be able to fulfill all the requirements seamlessly. Therefore, it is a reasonable choice for VANET to adopt 5G communication technology to maintain secure, flexible and QoS-enabled communication architecture.

1.3. Is 5G a Potential Player in VANET?

Without loss of generality, cellular networks are currently emerging as preferred choices for ITS connectivity services, at least in part, due to their global deployment and wide coverage. Specifically, the 3rd Generation Partnership Project (3GPP) standardization body has specified V2X services in the LTE network (release 14,15) and enhanced V2X (eV2X) in 5G network (release 6) [38]. 5G is the fifth-generation wireless technology and it is the latest cellular networking technology developed. It is specifically designed to achieve high data rates (up to 20 Gbps) and promises a latency of 1 ms for real-time applications [39] because the architecture supports other emerging technologies that include Heterogeneous Networks (HetNet), Network Function Virtualization (NFV) and networking slicing, massive Multiple-Input Multiple-Output (MIMO), Device-to-Device (D2D) communications, millimeter Wave (mmWave) and Software Defined Network (SDN) [40]. Empowered with these advanced technologies, 5G can achieve a higher capacity, ultra-low end-to-end latency, higher data rate, massive device connectivity and consistent Quality of Experience (QoE) provision [41].

In addition to enhanced capacity and reduced latency, network management is another salient feature of 5G technology. This network management is supported by network slicing and can have multiple virtual network connections based on the type of required service. For example, alarm messages and related security services require a fast, low latency network connection, while non-safety or multimedia application require higher capacity instead of high rate, while CAMs use only secure and data-only connections [22]. As discussed already, currently available standards for VANET (IEEE 802.11p/DSRC) have intrinsic shortcomings in terms of inefficient 5.9 GHz band utilization, short communication range, overhead/delay due centralized security and inefficient broadcast and acknowledgement protocols. Device-to-Device (D2D) communications [42], the enabler technology of 5G, addresses these shortcomings. D2D enables direct discovery of services and communication among users present in close proximity. Therefore, it can enable direct V2V and V2I communications without traversing through the cellular infrastructure and traditional cellular (i.e. uplink / downlink) communication. Hence, D2D-based vehicular broadcasting can be useful in mission critical vehicular applications because it can achieve high spectral efficiency, high data rate, low transmission power and low latency [43].

From a security perspective, 5G inherently provides flexible security benefits. Virtual Network Functions (VNFs) and SoftwareDefined Network (SDN) control are two prominent technologies that play a pivotal role in 5G-based flexible security. Therefore, 5G supports both data encryption through the user plane and network slicing which enables the adjustment of security parameters. NFV implements/deploys VNFs on cloud platforms and can be accessed from the cloud, eliminating the need for specific hardware to run different vendor-specific services and applications. Additionally SDN enables better network control by separating the network control plane from the data forwarding plane. As a result, both NFV and SDN provide dynamic and need-based security by using the characteristics of underlying networks [44]. To this end, due to SDNs unique capabilities of handling a large number of heterogeneous devices, different network conditions, better security, and network flexibility, 5G has strong potential for the commercialization of VANET.

In addition to other revolutionary features, 5G addresses the problem of accommodating a large number of nodes (such as in IoT). Furthermore, wireless network operations and applications are too closely coupled to deal with them separately. Therefore, it is imperative to focus on a communication paradigm that both complements and integrates with the existing technologies as well as fulfills different application requirements in a scalable, efficient, and heterogeneous way. In this context, 5G is a good candidate for heterogeneous scenarios. VANET is no exception and leverages not only vehicles on the road, but also other networks, such as Wireless Sensor Networks (WSN), IoT, CC, and so on. Therefore, the features of 5G can be harnessed with the above mentioned advances in computation, communication, processing and storage technologies. It can support massive number of simultaneous communication links in VANETs or among so called Internet of vehicle (IoV) [45].

1.4. Contributions of this work

As we have discussed earlier, 5G is a strong enabling communication technology for VANET applications. However, it is equally important to investigate both the requirements of VANET and the capabilities of 5G in order to support secure VANET applications. In this context, we focus on the security features of 5G and their applicability to VANET. In this paper, we investigate the role of 5G technology in VANET security. We summarize the main contributions of this paper as follows:

- We investigate the security features, requirements, and standards for vehicular networks. We also identify security weaknesses in vehicular networks and the shortcomings of the current VANET security standards.
- We present the salient security features provided by the 5G technology.
- To address the security weaknesses in current VANETs, we propose a high-level 5G-based security architecture for vehicular networks that complements the security features supported by current VANET security standards.
- We discuss future challenges and research opportunities in 5G-based security for VANETs.

The rest of the paper is organized as follows. In Section 2, we discuss the security features of 5G and Section 3 presents the VANET security which includes requirements, attacks, standards and solutions. In Section 4, we discuss the integration of the security features of 5G and VANET. We discuss future challenges and research opportunities in Section 5. Finally, we conclude the paper in Section 6.

2. 5G Security

5G is poised to be an important communication technology in today's cyber world. 5G is envisioned to serve diverse use-cases such as massive IoT applications, VANET, mobile broadband, and mission-critical applications, to name a few. This scalable and energy-efficient cellular technology has extended coverage and improved latency, and it will play a vital role in the development of future smart systems. Table 1 presents several features of 5G architecture along with enabling technologies. These technologies also diversify the threat domain of 5G technology (as shown in Figure 4 which we discuss in detail in section 2.4).

Table 1: 5G Features, corresponding design principles and enabling technologies

5G features	Enabling technologies/design principles
Improved data rate	• Massive MIMO and enhanced air interface and multiple access techniques • Provision of optical transmission/switching • Device-to-Device (D2D) communication • Use of high frequency spectrum • Separation of control and data plane • Small cell area network
Reduced latency	• Optical transmission/switching • Device to device (D2D) communication • Caching and prefetching techniques • Innovative air interface hardware and protocol stack. Shorter Time Intervals (STI)
Enhanced QoS provision	Use an intelligent agent to manage QoE, routing, mobility and resource allocation. Redesign NAS protocols, services and service complexity.

Massive number of concurrent connections	• Local offload (e.g., D2D, enhanced local area) • Caching/prefetching • Advanced multiple access techniques and better air interfaces • NFV and SDN cloud • Maximizing energy efficiency at various points at network
Capacity and coverage improvement	• Optimum spectrum management by employing pooling, aggregation and so on • Separation of control and data plane • Small cell area networks • Massive MIMO techniques and inclusion of new air interface • Optical switching increases capacity requirements in various network locations in backbone and backhaul/fronthaul • Device to device (D2D) communication
Better security control	• Security at physical layer • Security control • Per user and per application security • Security management

Next, we discuss the specific 5G security architecture with a special emphasis on the supported security features and potential security challenges [46, 47, 48].

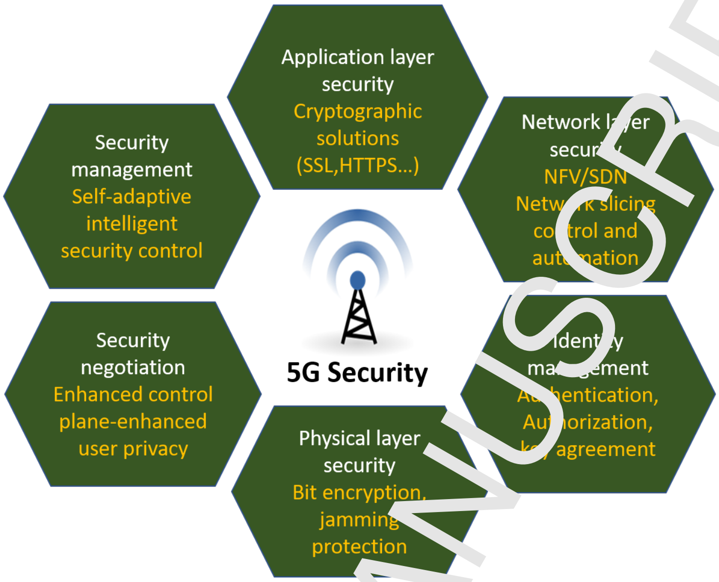

Figure 1: 5G Security Architecture

2.1. 5G Security Architecture

We discuss the 5G security architecture at various layers [49, 50, 51, 40] in this section. Figure 1 presents a high-level overview of 5G security architecture.

2.1.1. Physical layer security provision

Information security and data confidentiality are essential requirements for any communication technology and the same is true for 5G technology. Physical Layer Security (PLS) is a promising solution for information security due to its competitive user-centric benefits and flexible security provision. PLS provides keyless secure signal design and transmission by exploiting channel characteristics and by using simple signal processing techniques, PLS avoids the use of compute-intensive cryptographic techniques and encryption/decryption methods. Therefore, it is well suited for the heterogeneous nature of 5G users and devices (e.g., IoT devices) which are typically low-power and have low computational capabilities. 5G networks are also distributed and decentralized in nature, characterized by dynamic changes in topology due 5G devices joining/leaving the network. In this case, if cryptographic techniques are used, key distribution and management become a challenge. Above all, 5G technology promises to provide diverse services with versatile security requirements. For instance, sensitive online payment applications require sophisticated security in contrast to simple Voice over IP (VoIP) services. Simple encryption/decryption techniques cannot provide varying level of service-oriented security. Rather, they only provide binary-featured security (fully protected or fully exposed if the secret key is exposed) [52]. However, most of the future 5G-enabled communication is expected to be among low-cost machine-type devices with limited computing and processing capabilities. Thus, existing PLS techniques cannot be directly utilized. Therefore, there is need for innovative PLS solutions to match the unique features (versatile QoS requirement) of 5G networks. Moreover, current PLS techniques consider only link level properties such as fading and noise and hardly take into consideration network level properties including feedback, cooperation and cognition [53].

In this context, various Low-Density Parity-Check (LDPC) codes, polar and lattice codes are used for secure data transmission and are recommended for 5G networks. Moreover, technologies such as massive MIMO and millimeter Wave (mmWave) constitute the foundation for 5G and provide secure communication at the physical layer. Massive MIMO provides high spectral and power efficiency by using arrays of antennas. Transmit power is considerably reduced in these MIMO systems, resulting in reduced Signal to Noise Ratio (SNR) at the eavesdropper's channel. These systems use Artificial Noise (AN)-based data transmission which further degrades the signal received by eavesdropper.

mmWave is another enabling technology for 5G wherein high frequency signals are used for high directional and secure transmission. These high frequency signals increase free space path losses and only eavesdroppers in close proximity are able to overhear the signal. Thus it decreases the probability of overhearing signals by the remote eavesdroppers. mmWaves are highly directional and considerably reduce SNR received by eavesdropper thereby making it difficult to extract useful information from the received signal [54].

2.1.2. Network slicing

Network slicing is used to support virtual networks over the same physical infrastructure to enable flexibility and QoS provision for smart applications in 5G networks. NFV, SDN, cloud-RAN with centralization and virtualization processes are key enablers for network slicing. Network services are virtualized in contrast to the traditional systems wherein dedicated and proprietary hardware is reserved for each network. NFV and SDN are complementary technologies where NFV moves functions and services to a virtual environment and SDN uses/makes policies for the automation and control of these virtual networks. Additionally, multi-tenancy is supported by NFV and SDN where the infrastructure is accessed through virtual network slices on an on-demand basis. Various network functions such as firewall, routing and load balancing are available through Virtual Machines (VMs).

These network slices are independent and autonomous in nature. Therefore security configuration and policies can be implemented on each virtual network according to the functional requirements of the network. These policies can include access control, authentication and authorization in individual slices as well as mutual authentication among various virtual networks when network functions are shared by more than one slice [55]. Moreover, SDN and NFV also provide SECurity as a Service (SECaaS) and incorporate security Virtualized Network Functions (VNFs) for various network slices. These functions not only provide optimal resource sharing but also enable service-oriented agreements and policies. These features also provide predictive auto-scaling function along with the monitoring and flow control mechanisms.

2.1.3. Application layer security features

In essence, 5G complements the security mechanisms applied at the application layer. Normally the application layer security is transparent to the lower layers; however, in case of 5G, we need to exchange the context information of the application among different entities for better security provision. Arfaoui et al. [50] introduced the terms stratum and security realm in their 5G architecture where stratum refers to the collection of protocols, functions and data that are related to similar services and the security realm defines the security needs of these strata. At the application layer, the existing security mechanisms such as HTTPS and Secure Sockets Layer (SSL) are used. However, the applications may need additional provisions for security which include mutual authentication, auditing, billing, and so on. Therefore, the 5G architecture incorporates the context of the application at the application layer as well to know the security requirements of the application and provide the required level of security.

2.1.4. Security management using SDN

SDN is a key technology that enables flexible and re-configurable network management in 5G networks. The SDN architecture is divided into three planes: application, control and infrastructure [56] as shown in Fig. 2. We can see that various network functions such as network management, network interface management and QoS management can be achieved using software-based applications. Similarly, security management functions are implemented as an application in the SDN application plane. The decoupling between network security functions and vendor's hardware can be achieved in SDN. Flexible security management operations in SDN do not require modifying the firmware of various types of hardware used for security functions.

The SDN architecture can provide reactive as well as proactive security monitoring, analysis and the implementation of security policies. Due to the centralized nature of SDN, the global view of the network facilitates instant threat identification, state and flow analysis followed by policy updates and network flows modification (if required). This automation addresses any inconsistencies in configuration and policy conflicts across the network.

The combined features of NFV and SDN further enhance the flexible security management in 5G such that the network security function can be placed and programmed in real-time at any network entity without altering the underlying hardware configuration. For instance, if an intrusion detection security function

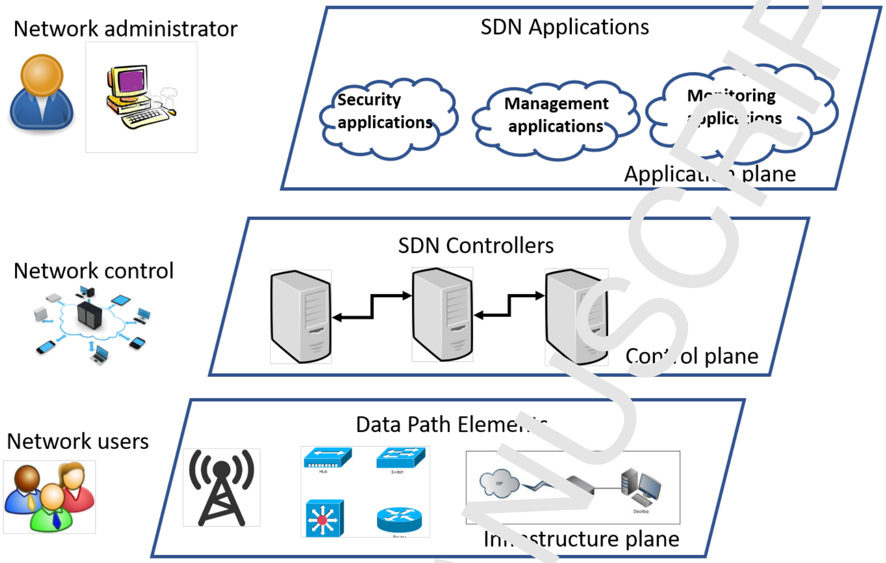

Figure 2: SDN Planes

implemented as an application, all the packets can be checked at the application plane and then forwarded through the control plane to the data forwarding plane. After performance analysis at the application plane, these packets are either dropped (if corrupted) or forwarded to a specific port (depending on the network policy). Advanced security analysis can be performed by adding a security middle-box at the port performing the forwarding functions. Furthermore, SDN enables 5G to implement Software-Defined Security (SDS). Similarly, NFV also provides security services such as trusted computing and remote verification for virtual environments that are leveraged by 5G. Moreover, a chain of trust is also established between communicating entities in NFV. Both NFV and SDN offer virtual security service functions for monitoring the network slices and correlate relevant data and events for detecting anomalies [57]. These network security functions are abstracted when needed and are delivered as a service. Security as a service can be applied to any application area and is a strong use case of 5G technology. In a nutshell, 5G provides security both through its core architecture and through enabling technologies.

2.1.5. *Security negotiations*

Security negotiation is an important element of the 5G security architecture due to the large number of heterogeneous devices in 5G. The 5G architecture differs from the legacy 3G and 4G in the way security is negotiated between the user and the network. The one-size-fits-all approach is not applicable in 5G because of the large number of applications with their own unique security requirements. Thus 5G uses network slicing for each application as we have mentioned earlier. 5G is more flexible than 3G or 4G for security negotiation. One example scenario could be IoT, where traditional cryptographic algorithms might not work and more optimized, lightweight, and energy-efficient algorithms must be used.

2.1.6. *Data security*

Data confidentiality is one of the important aspects in the 5G security architecture. Data confidentiality is concerned with allowing data access only to legitimate users who have the required access rights for the particular data. Similarly, privacy is also essential in 5G because a lot of data is shared among nodes which could be used to find patterns (e.g., in the case of VANET, the mobility information) that are linkable to individual users [39, 58]. To mitigate attacks against data security, encryption is the traditional mechanism to secure data against different attacks. It is also worth mentioning that applications implement their own data security mechanisms at upper layers but these mechanisms may not withstand the attacks (such as jamming and eavesdropping) at lower layers. 5G offers strong PLS mechanisms that can mitigate such attacks [59, 53].

2.2. *Security Enhancement and Features*

5G enables flexible inter and intra-networking among various network entities. It provides a service-based architecture such that one network function can provide services to another network function. Next, we discuss some of the features (not supported in previous 3G and 4G cellular generations) that make 5G well suited for today's smart systems including ITS [60, 61].

2.2.1. Network slicing security

The 5G network provides end-to-end security for logical networks which includes access network security, core network security, terminal security and sliced network management security. The significance of network slices is best illustrated by comparing applications with different requirements. A network of sensors for example, requires the capability to capture data from a large number of devices. In this case, the need for capacity and mobility is not significant. Media distribution in vehicular networks on the other hand, is challenged by large network bandwidth requirements which can be eased through distributed caching. Similarly, critical safety-related information exchange in VANET requires low latency, reliability, authentication, and other important security guarantees.

2.2.2. Separation of control and user plane

The Control and Data Separation Architecture (CDSA) is a key design feature in 5G. The control plane functions are deployed on the edge or cloud platforms as a software while the data plane functions are deployed on high speed hardware devices (network connections, interfaces etc.). These functions not only support flexible scaling of control functions but also optimize packet forwarding and switching tasks for traffic which varies in terms of the amount, type, velocity, and arrival pattern. The common data plane is used by various logical networks (NFV) and provides ease of service provisioning and management. This separation of planes is further complemented by the use of SDN which separates control action enforcement elements and control decision entities. CDSA and SDN are two different concepts complementing each other. While the control plane in CSDA also includes decision making entities along with network and control signaling used for service requested/provided by/to the devices. This includes connection establishment and maintenance commands,

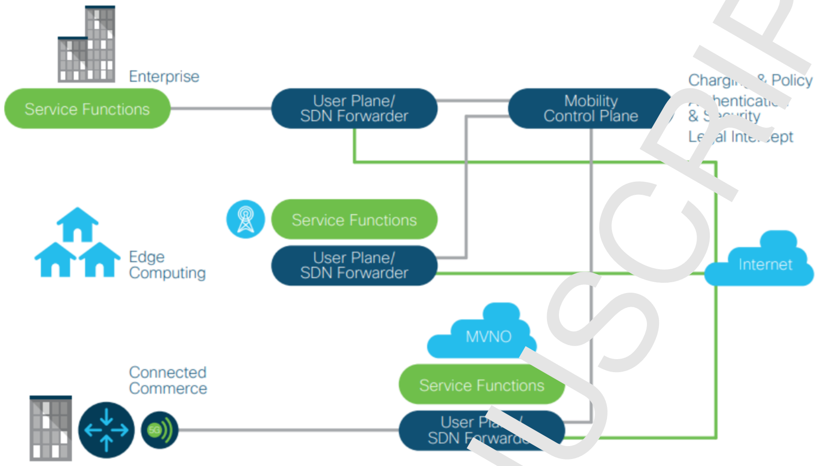

Figure 3: Control and Data Planes [62]

scheduling and channel access information to support seamless data transmission. Figure 3 illustrates the concept of separation of control and data planes.

2.2.3. Diversified and scalable identity management

5G supports the provisioning the management of various devices under the same user ID. For instance, for an IoT Body Area Network (BAN) wherein a user wants to manage various wearable IoT devices (that may be embedded inside the body, implanted, or wearable on the body in a fixed position), 5G enables flexible management of all wearable devices within a specific scope (e.g., network access service attribute). The user identity across various devices is inter-related and authorization, identification and management of these devices is done through a single identity. In another example, an in-vehicle network uses different devices that communicate with each other and with the core vehicular network, 5G can flexibly manage these devices through identity management and provide the necessary security provisions.

Artificial Intelligence (AI) based proactive approaches along with the traditional and manual security methods have been proposed for proactive threat analysis and response. For example, Machine Learning (ML) and AI techniques are being explored for malicious code and anomaly detection in code and network traffic [63, 64]. ML is being used for collaboration among multiple security functions which include vulnerability scanning, malicious code detection, security hardening for automated security, monitoring, and agile security management.

2.2.4. Addition of new functions and identities

The 5G security architecture incorporates the following functions (which were not present in previous cellular generations, i.e. 3G and 4G (LTE/-A) [65, 49, 61]:

- The Security Anchor Function (SEAF) is co-located with the authentication management function and is used to generate primary authentication and the unified anchor key, known as KSEAF, which is used for user authentication across various points in the network.

  The AUthentication Server Function (AUSF) is provided by Extensible Authentication Protocol (EAP) server and takes requests from SEAF connect and interacts with the authentication processing function.

- The Authentication Credential Repository (ACRP) and the Processing Function (ARPF) is collocated with the Unified Data Management (UDM) and is used to keep long term security credentials such as keys. These functions apply cryptographic algorithms on the security credentials and create authentication vectors.

- The Security Context Management Function (SCMF) is co-located with SEAF and derives access network specific keys by retrieving other keys from SEAF.

- The Security Policy Control Function (SPCF) is used to provide security policies to various network entities such as SMF and AMF. This policy design might include the authentication function, key length, confidentiality, and integrity protection rules.

2.3. Security Services Provided in 5G

5G offers security services in 2 stages, i.e. through the architecture and through enabling technologies [40, 66, 67] such as SDN and NFV. Through its core architecture, 5G offers services such as authentication, confidentiality, data integrity, and availability. The authentication service is provided between the User Equipment (UE)[1] and the 5G network entities such as Mobility Management Entity (MME) and other service providers. This is the main difference between the traditional cellular networks (3G and 4G) and 5G. However, the frequent handover, efficient and ultra-fast authentication mechanisms are still subject to further research in 5G. Similarly, confidentiality and data security is also provided by 5G. As we have mentioned earlier, 5G focuses on the lower communication layers that are prone to notorious attacks and need to be protected against such attacks. The data integrity service is inherited by 5G from the upper layers and is not provided additionally by 5G. However, the information related to data integrity is protected at the lower layers through the 5G architecture. 5G also mitigates attacks such as DoS and jamming at the lower communication layers through Direct-Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS).

2.4. Threat Landscape 5G

5G is envisioned as a promising technology for serving multiple sectors including social networks, society, public safety, industries, interconnecting infrastructures and IoT applications. 5G is under higher threats and attacks than previous generations (3G and 4G), starting from physical layer to application layers spanning network interfaces, cloud RAN and user management. The 5G platform introduces the most sophisticated, persistent (ability to evolve), complex (mix of various attack vectors), obfuscatory (spanning across multiple layers) and evasive (ability to disguise) threats in the future technological world [66]. The threat landscape of 5G is wide because of the following reasons:

[1] In this paper, we use the terms 'UE', 'smart device', and 'user' interchangeably.

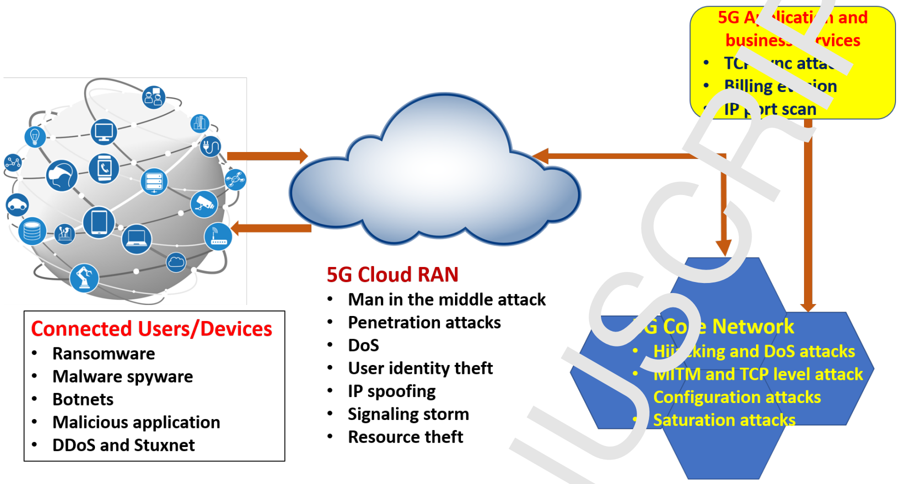

Figure 4: 5G Threat Landscape

- 5G is envisioned to support new use-cases and smart applications, in which most of the computing and storage related functions are carried out at the network's edge (to reduce latency) and therefore, a considerable change in network structure is expected.
- All the networking functions have changed from physical to virtual implementations. These functions and related virtual services are distributed across and are accessible from the edge and cloud.
- 5G has a flexible software-based access and networking architecture comprising technologies such as SDN, Software-Define Access (SDA) and Software-Defined Radio (SDR).

Figure 4 and Table 2 further illustrate the threats in various domains/modules.

Table 2: 5G Threat Landscape

5G Domains	Threat analysis

5G core network security	• Critical infrastructure and service attacks • DDoS on centralized control elements • TCP Level attacks on the communication between SDN controller and the application • Saturation attacks on SDN controller and switches • Configuration attacks on SDN (virtual) switches and routers • Signaling attacks on 5G core elements • Man-in-the-Middle (MITM) targeting the SDN controllers communication • Hijacking attacks targeting the SDN controller and hypervisors
5G cloud RAN security	• Penetration attacks on virtual resources and clouds • DoS for controlling elements • User identity theft from user information database • Timing attack

End user/device Threats	• User identity theft (User information databases affected) • Advanced malware • Firmware hacks • Device tampering • Spyware • DDoS • IoT botnets due to IoT/mobile devices(receiving and transmitting to a remote system) can lead to active and passive attacks • Semantic information and boundary attacks on subscriber location
Business application threats	• TCP sync attack • Billing evasion • IP port scan • Download unauthorized applications which are not verified and checked can be potential source of threat • Insecure application can leak un-encrypted sensitive personal/sensitive data

2.4.1. 5G core network security threats

SDN and NFV network slicing simplify the network management by separating and programming various logical planes and virtualizing various network functions. However, it opens up doors for a plethora of security challenges in various network slices and may cause mis-configuration of NFVs. Furthermore, inter-federated conflicts among SDN controllers can jeopardize the entire 5G network. Furthermore, due to the centralized network control, the SDN controller is under potential saturation attacks and can make SDN controller a bottleneck for the entire network. In addition to this, with the separation of traffic flows in the data and the control planes by using SDN controller, control information is a visible entity and is prone to DoS attacks. A DoS attack can affect user and management planes, signaling planes as well as logical and physical resources. Thus a very strong authentication and authorization mechanism is required to avoid the misuse of control planes through APIs and critical applications [40]. We would expect a rise in signaling-based threats because of the inclusion of IP protocols in user and control planes. These signaling threats can affect authentication and attached/detached devices, device location updates and bearer activation [56].

2.4.2. 5G cloud RAN security threats

Cloud and edge computing enable virtualization of resources and infrastructure. However, they lead to potential security threats for storage, processing, and scheduling of data. It includes data misplacement (loss or leakage), insider attacks, abuse and nefarious use of cloud/edge, anonymous access due to insecure APIs and network interfaces, and DoS attack [68, 69].

Intrusion into distributed clouds adversely affects the availability and confidentiality of cloud resources and can jeopardize the integrity of data and security of network infrastructures. Traditional access control involves authorizing users to access data/network resources as well as monitoring/recording access attempts by unauthorized users. These are based on only user identity and do not support flexible control of various domains and policies, and dynamic activation of access privileges. Furthermore, cloud RAN is prone to various threats such as DoS, man-in-the-middle, malicious node problems, and inconsistent security policies [70].

2.4.3. End user and device threats

In 5G technology, the security of user plane is not completely matured as there is no specialized cryptographic mechanism available for end device protection, security of the user applications, operating systems and data security. These devices are prone to eavesdropping, (D)DoS, botnets and Spyware. (D)DoS attack can target battery, memory, sensors, actuators and even radio links of these devices/users [40]. Cryptographic methods are used to protect user/devices depending on the strength and computing capability of the end devices. Since most of these devices are low-power and have limited computational capabilities, therefore they cannot execute complex algorithms.

3. VANET Security: Requirements, Threats, Attacks, and Standards

The features of connected car technology enjoyed by consumers are numerous. However, these features expose VANET to unprecedented security threats ranging from typical network attacks to sophisticated malware and hacking [12]. These attacks can have dire consequences for both service providers (in the form of loss in business) and for consumers (human lives could be endangered). Apart from these consequences, the commercialization of connected car technology is also, at least in part, impeded by the security issues faced by this technology. To date, extensive research has been carried out both by industry and academia to develop efficient, scalable and viable security solutions for VANET[2]. Nevertheless, the increasing number of smart services introduced in vehicles open up new security threats, such as hacker attacks, intrusion, and physical abuse. It is also important to mention that there are mainly two types of communications involved in VANET, inter-vehicle communication where vehicular nodes are connected to other entities (including vehicles, pedestrians, and management entities) and intra-vehicle communication where different components of the car are connected through a network and to the Internet. These types of

[2] In this paper, we use the terms 'VANET' and 'connected car' interchangeably.

communications increase the risk for remote access attacks and data manipulation attacks on VANET applications. Recent studies have shown that in-vehicle network through Controller Area Network (CAN) is vulnerable to serious attacks where an attacker, by exploiting the vulnerabilities in diagnostic applications, can take the control of a car remotely [71]. In this context, the fact that current VANET use existing networking infrastructure (which is prone to plethora of attacks) put a question mark on its adaptation in the consumers as well as industry. In this section, we present the security requirements of VANET applications and services and different security attacks that are possible on VANET. We also describe current standards for VANET that deal with different security aspects of VANET and then we identify the security weaknesses in VANET.

3.1. Security Requirements in VANET

The safety-related applications of VANET require efficient and reliable security mechanisms to mitigate different attacks. The messages exchanged in such applications must not be altered, forged, and/or abused by the attackers because the compromise of such messages could create life-threatening consequences for both drivers and passengers [29]. In the literature, few papers identify different security requirements of VANET [29, 12, 15, 31, 72]. Table 3 summarizes the major security requirements in VANET and its breeds with their implications on the network. If these security requirements are not met, they can have different implications that include financial, operational, safety, and privacy.

Table 3: Security Requirements in VANET

Security Requirement	**Communication Paradigm**	**Impact**
Authentication	V2X	• Operational • Privacy

Continued on next page

Table 3 – continued from previous page

Data confidentiality and liability	• In-vehicle • V2X	• Financial • Privacy
Key distribution	V2I	• Operational • Safety • Privacy
Trust management	V2V	• Safety • Privacy
Misbehavior	• V2V • V2I	• Safety • Financial
Availability	V2X	• Operational • Financial • Safety
Integrity	V2X	• Operational • Financial • Safety
Access control	• V2I • V2V	• Financial • Safety • Operational

Continued on next page

Table 3 – continued from previous page

Privacy	• V2V • V2P • V2C	• Financial • Safety
Location privacy	• V2V • V2C	• Financial • Safety
Flexibility	• V2I • V2C	• Operational • Safety

3.2. Security Threats and Attacks in VANET

Attackers can be broadly divided into two categories, insiders and outsiders [73]. Insiders are the benign and authenticated VANET users whereas outsiders are the entities that are not authenticated and do not have legal access to the network. In principle, insider attackers pose more serious threats because they have legitimate access to most of the network resources. The attackers' behavior is also an important element to consider in VANET. The motives behind the attack could vary and may include monetary, fun, and other malicious reasons. Furthermore, the attackers also differ in their scope and strategy. The scope could be either local or global whereas the strategy could be either active or passive. In this subsection, we present some of the security threats and attack in VANET. Common threats to VANET include: bogus information, impersonation, illusion, eavesdropping, profiling, message suspension, and tampering. Other sophisticated threats include malware, DDoS, location theft, and so on. In the following sections, we discuss different categories of attacks on VANET and present a summary of these attacks in Table 4.

3.2.1. *Intra-vehicular attacks*

Vehicular nodes in VANET are hosts to large number of sensors and Electronic/Engine Control Units (ECUs). These sensors communicate with each other, central control unit, and with the external entities such as passengers or other hand-held devices forming an in-vehicle network. Recent researches have shown that in-vehicle networks are prone to serious cyber attacks that could not only disrupt the normal function of a vehicle but could also endanger human lives. Vehicular nodes also use in-vehicle infotainment (information and entertainment) system which is connected to the external devices such as smartphone through Bluetooth technology. On one hand, such infotainment system provides the drivers and/or passengers with more added value services, but on the other hand increases vulnerability to cyber attacks. Moreover, the external links to the vehicular node are also used for diagnostics (wired through On-Board Diagnostics - OBD and wireless through Bluetooth and WiFi). These external links to vehicular nodes can lure the attackers to launch cyber attacks on the car. For instance, rouge android applications, bugs in the Bluetooth software and other enabling technologies could be used to target the CAN. Woo et al. carried out a practical attack on CAN bus of a high-end car [71]. They used malicious diagnostic application from smartphone to control the entire vehicle. They also proposed a secure version of the security protocol and a new security architecture for CAN bus to mitigate such attacks [74]. However, the security issues of CAN bus are still prevalent.

Global Positioning System (GPS) is also an essential component for vehicular nodes in VANET and it is used to navigate the vehicle and share location information with other entities. Sharing wrong location information could have catastrophic consequences for the transportation safety (both in case of connected and autonomous cars [75]). Furthermore, the conventional GPS systems are prone to spoofing and jamming attacks and therefore need special attention for VANET and autonomous cars [76]. Thus, VANET nodes must incorporate detection mechanisms against such attacks.

3.2.2. Inter-vehicular attacks

VANET nodes (which communicate based on the existing communication standards) are prone to different security attacks. Here, we discuss different security attacks on VANET.

Dissemination of wrong information . One of the most common attacks is the dissemination of fake and/or wrong information to misguide other vehicles. This attack is usually launched by insider attackers and can be the result of a Sybil attack [77] or any other attack that leads to identity-theft. This attack could also lead to framing attack where benign nodes are framed with wrong information shared in the network on behalf of the victim node.

Sybil attack . Sybil attack is also referred to as illusion attack where the attacker both generates fake identities and uses others identities to create illusions for the network and influence the network in decision-making [78, 79, 80, 13]. Such illusion can result in severe consequences for the applications that take majority-based decisions. Furthermore, it can also disrupt the traffic information application. In short, Sybil attacks can cause almost all kinds of other attacks [13]. Strong authentication and revocation mechanisms might impede the intensity of the Sybil attack, however, different flavors of Sybil attack make it harder to safeguard the network.

Jamming attack. In jamming attacks, the attackers interfere the communication among entities through jamming the signals. For VANET applications, availability is a primary concern and it will be adversely affected in the presence of jamming attacks. It is also worth mentioning that jamming attack is relatively easy to launch in VANET because it does not need sophisticated mechanisms such as keys compromise and so on.

Profilation. It is an attack on the privacy of the VANET users where the spatio-temporal information shared by the benign VANET nodes is exploited to construct movement profiles against the users [11]. For instance, CAMs are broadcasted in the order of milliseconds and contain fine-grained location and other information. The attackers use this information to construct movement profiles against individual users. To mitigate this attack, pseudonyms have been used in the literature [81]. However, it has been found that using different pseudonyms for communication by the same nodes may still be linkable to each other and to a specific node [82, 83].

DDoS . Distributed DoS is launched by attackers by flooding the network with a huge volume of irrelevant information. This kind of attack could be either launched individually by the attacker or by colluding with other nodes. The main reason behind DDoS is to render the VANET unavailable. In the face of such attack, critical warning messages would not reach the nodes and may cause deadly consequences for the benign nodes [84].

Replay attacks . Data freshness is essential in VANET. In the replay attacks, the attacker reuses the old data at a different point in time. The effect of this attack is similar to the bogus information dissemination. This could also be as a result of identity-theft and other attacks such as Sybil attack. Usually replay attacks are also used to obtain cryptographic keys of the victim node(s) [85].

Tampering with hardware . Unlike other attacks, the attackers tamper with physical hardware to get hands on the cryptographic material from On-Board Unit (OBU) or RSU [86]. With sophisticated attackers, tampering attacks are possible in VANET; however, tamper-resistant or tamper-proof hardware can be used to mitigate such attacks. Apart from RSU and OBU, sensors and other devices in vehicle are also prone to such attacks.

Malware . Depending on the intention of the attacker, spam messages are sprayed into the network to consume network resources and compromise the normal functions of the device. The victim node can then be used as a bot by the attacker to use it as a launching pad for other attacks in the network [87, 88]. Mitigation of such an attack is challenging in VANET (specially in V2V) communication due to the absence of the necessary infrastructure.

3.2.3. *Integrated attacks*

In addition to the aforementioned attacks, there are attacks that could be launched directly on the primary VANET infrastructure or through integrated technologies such as cloud computing [89, 90], IoT [91], and Software-Defined Network (SDN) [92]. These infrastructures could be leveraged to launch notorious attacks such as DDoS, false information injection, impersonation and so on [93] on VANET. Vehicular cloud is the extension of traditional VANET to expand its service and application space. However, this extension brings new security challenges to the core VANET such as data breaches through cloud, Application Programming Interface (API) vulnerabilities, escalation of privileges and so on [89, 93]. Similarly, leveraging IoT through vehicular networks also exposes VANET to attacks that originally target IoT devices. The resource constraints of IoT devices can be easily exploited by the attackers and then through a series of attacks such as bug exploitation and vulnerabilities in software, the attackers could control VANET. In case of SDN, the conceptual decoupling of data and control poses challenges for vehicular nodes in VANET by exposing them to various software-driven attacks such as API security, implementation bugs and so on. In short, the contemporary services provided by the above-mentioned enabling technologies pose security challenges to the existing VANET and therefore these challenges must be addressed before the integration of enabling technologies with traditional VANET.

Table 4: Security attacks in VANET

Attack type	**Purpose**	**Target communication type**

Continued on next page

Table 4 – continued from previous page

Intra-vehicle attacks	• Attack on CAN bus • Control the car remotely • Inject malicious code • Malicious application-based access	In-vehicle network
Wrong information injection	• Mislead other vehicles • Clear the road for the attacker • Monetary purpose	• In-car network • V2V • V2P
Sybil attack	• Create illusion through non-existent nodes • Create fake nodes • Launch other attacks • Adversely affect decision-based applications	V2V
Jamming attack	• Affect availability • Disrupt resource utilization • Affect VANET application	• V2V • V2I • V2P

Continued on next page

Table 4 – continued from previous page

Profilation	• Abuse privacy • Spy on targeted users for commercial purpose • Target users with advertisements of interest	V2V
DDoS	• Drain the resources of vehicles and service provider(s) • Adversely affect the service availability • Disrupt the QoS of VANET application • Monetary purposes (for ransom)	• V2V • V2I
Replay	• Impersonation • Inject bogus information • Steal user identity • Launch sybil attack	• V2V • V2I • V2P
Tampering	• Physical access to hardware • Launch physical attacks • Steal cryptographic material • Inject malware	• In-car network (diagnostics, CAN) • V2I

Continued on next page

Table 4 – continued from previous page

Malware	• Take control of the vehicle • Steal cryptographic information • Use the vehicle as a bot • Perform profiling • Monetary purposes	• In-car communication network • V2V
Integrated attacks	• Attacks through the cloud computing architecture • Attacks through IoT • Attacks through SDN • Attacks through APIs	• V2I • V2C

3.3. VANET Security Standard

Security is going to be the cornerstone for VANET commercialization in addition to consumer satisfaction and adaptation in the society. Therefore, it is important to discuss the state of the current standards and in the context of this work with a focus on VANET security. There are two main families of standards, Institute of Electrical and Electronic Engineers (IEEE) standards that are mainly used in United States and ETSI standards are used in (almost) all of the European countries. There have been extensive efforts from both standardization bodies to ensure security services in VANET in order to fulfill different security requirements. To be more precise, in Europe the Working Group 5 of ETSI (ETSI-TC-WG5) and in the US the IEEE 1609.2 working group have drafted (and have been constantly updating) the security standards for ITS [[illegible]4]. In this section, we discuss the standardization efforts from both ETSI and IEEE. IEEE 1609 family defines, among other parts, the security mechanism for vehicular networks through IEEE 1609.2 standard in the upper layers of the network whereas IEEE 802.11p is used for the lower layers. The latest version of 1609.2 standard is the updated version of 1609.2-2006 and is known as 1609.2-2016 [95].

IEEE 1609.2 provides 3 basic security services, message formats for security-related messages used by WAVE-enabled devices (for instance OBUs), security of management messages and the security of application messages. This standard takes into account the safety-application requirement (timeliness and minimum overhead). As we mentioned before, this standard provides security at both lower and upper layers. The security at lower layers is provided through WAVE Internet Security Services (WISS) and to the upper layers it is referred to as WAVE Higher Layer Security Services (WHLSS). The internal security services are related to the security functions that are applied to the data coming from upper layers to the lower layers. These services are related to the data itself and define Secure Data Service (SDS). SDS defines the procedures for securing the Protocol Data Unit (PDU) by encrypting and adding security envelope to the original PDU. Furthermore, WISS also manages the certificates that are used at the upper layers. On the other hand, WHLSS provides the revocation service through Certificate Revocation List (CRL). The CRLs are validated by CRL Verification Entity (CRLVE). It is important to mention that certificate distribution is also essential and a peer-to-peer certificate distribution in defined by WHLSS.

IEEE 1609.2 defines the general framework of the security-related messages and methods. It is worth explaining the standardized message set, the data structures used in these messages, and data elements. In this context, the Society of Automotive Engineers (SAE) defined a standard SAE J2735[3]. SAE J2735 defines the overall structure of the message, data structures elements, and frames used in these messages for V2X communication. SAE J2735 defines 17 Messages, 156 Data Frames, 230 Data Elements, and 58 external references for

[3] https://www.sae.org/standards/content/j2735_200911/

data element definition[4]. The common messages include basic safety message, intersection collision avoidance, emergency vehicle alert and so on.

At a higher level, vehicles and vehicular networks are part of the Cyber Physical System (CPS). Therefore, the cybersecurity of V2X communication framework must take into account the security lifecycle of the CPS. In this context, SAE J3061[5] defines a detailed security framework to address cybersecurity issues in V2X communication [96]. The framework defined in SAE J3061 can be tailored according to specific application requirements and supports cybersecurity by design. It is also worth mentioning that SAE J3061 is designed in compliance with the functional safety standard for the automotive industry (ISO 26262).

Next, we discuss the existing security standards defined by ETSI in Europe. ETSI TC ITS WG5 has defined a series of standards to address different security challenges in the vehicular network environment.

3.3.1. ETSI TS 102 723-8 V1.1.1 (2016-04)[6]

This standard defines the interface between the security entity and intermediate upper layers (network and transport layer). The security services defined by this standard include confidentiality, authentication and integrity, identity management, and additional services that include logging all the security events, permissions management, and encapsulating/decapsulating of messages. Identity management includes multiple pseudonyms and a strategy for the process of pseudonym change.

[4]https://www.transportation.institute.ufl.edu/wp-content/uploads/2017/04/HNTB-SAE-Standards.pdf

[5]https://www.sae.org/standards/content/j3061/

[6]https://www.etsi.org/deliver/etsi_ts/102700_102799/10272308/01.01.01_60/ts_10272308v010101p.pdf

3.3.2. *ETSI TS 102 731 V1.1.1 (2010-09)*[7]

In the TS-102-731 standard, ETSI defines a generic secure and privacy-preserving communication mechanism among entities in ITS. In other words, this standard provides the security architecture for the ITS. It focuses on the credential management for enrollment and registration to use ITS services, identity management for privacy preservation and anonymity, data integrity protection, authentication and authorization. Since this standard deals with the functional aspects of the ITS, therefore, information flow and functional entity identification are also covered.

3.3.3. *ETSI TR 102 893 V1.2.1 (2017-03)*[8]

This standard provides threat, vulnerability and risk analysis in the context of communication among ITS nodes. The standard focuses on the 5.9 GHz radio (which is the primary hardware radio used for ITS communication) communication. It considers all types of communications (V2X) and applications in VANET. The standard focuses on the identification and understanding of the threats and identify the risks.

3.3.4. *ETSI TS 102 940 V1.3.1 (2018-04)*[9]

This standard focuses on the security architecture of vehicular communications. It uses the standard ETSI TS 102 731 as baseline and defines relationships among the participating entities. At the functional level, this standard defines security mechanisms in terms of the security for shared information. It also defines the guidelines for trust establishment among different entities. Furthermore, this standard defines the Public Key Infrastructure (PKI) processes for providing cryptographic security in ITS.

---

[7] https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf

[8] https://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.02.01_60/tr_102893v010201p.pdf

[9] https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf

3.3.5. ETSI TS 102 941 V1.2.1 (2018-05)[10]

The standard defines trust establishment, management, and privacy preservation mechanisms. It is based on the services that are already defined in *ETSI TS 102 731* and *ETSI TS 102 940* (discussed above). More precisely, this standard defines the procedures for trust establishment among communicating entities and privacy preservation in ITS. The standard also defines the necessary cryptographic primitives for the aforementioned services and identity management. The hierarchy of the authority is important to establish and manage trust among entities, therefore this standard defines the authority hierarchy in ITS. The standard also defines and complements the privacy attributes for the nodes in ITS that include anonymity, the use of pseudonyms, unlinkability, and unobservability in all kinds of messages.

3.3.6. ETSI TS 102 942 V1.1.1 (2012-06)[11]

Access control is an essential component of authentication and security. This standard defines the authentication and authorization mechanisms for proper access control in ITS. The authentication and authorization depend on the requirements of the ITS application. The authentication mechanism is different for different kinds of messages in ITS. For instance, CAMs and other safety-related messages have different requirements of authentication and authorization. More precisely, CAMs are broadcasted and access is granted to all benign ITS users whereas authorized emergency vehicles or public buses may have special rights (depending on national legislation). Similarly, the authorization and access rights for other kinds of messages are defined in this standard.

[10]https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.02.01_60/ts_102941v010201p.pdf

[11]https://www.etsi.org/deliver/etsi_ts/102900_102999/102942/01.01.01_60/ts_102942v010101p.pdf

3.3.7. ETSI TS 102 943 V1.1.1 (2012-06)[12]

This standard defines the confidentiality services in ITS. The standard takes into account the confidentiality required for the communication among different stations based on the security requirements. It is worth noting that different applications have different requirements for confidentiality. For instance, CAMs do not need any confidentiality and similarly static local hazard warning do also not need confidentiality. On the other hand, signaling data needs confidentiality to prevent its modification. The standard also defines confidentiality services at different layers (up to the network layer) and the methods/tools/techniques to achieve these services.

3.3.8. ETSI TS 103 097 V1.3.1 (2017-10)[13]

For all the security services mentioned so far, it is important to define the secure data structures. These data structures include header and certificate formats. This standard defines the header and certificate formats for security services. This standard like IEEE Std 1609.2, defines the headers format in Abstract Syntax Notation 1 (ASN.1) and it is required to be encoded in the Canonical Octet Encoding Rules (COER). This document is similar to the IEEE standard for the cross-environment operations.

3.3.9. ETSI TS 103 096 (1,2,3) V1.4.1 (2018-08)[14][15][16]

These three documents define the specifications for ITS security in different ways. The first part of this standard defines the specifications for protocol

[12] https://www.etsi.org/deliver/etsi_ts/102900_102999/102943/01.01.01_60/ts_102943v010101p.pdf

[13] https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf

[14] https://www.etsi.org/deliver/etsi_ts/103000_103099/10309601/01.04.01_60/ts_10309601v010401p.pdf

[15] https://www.etsi.org/deliver/etsi_ts/103000_103099/10309602/01.04.01_60/ts_10309602v010401p.pdf

[16] https://www.etsi.org/deliver/etsi_ts/103000_103099/10309603/01.04.01_60/ts_10309603v010401p.pdf

implementation in ITS. The second part defines the goals of the tests and defines the test suite. These definitions are in accordance with the ETSI TS 103 097. The third part of this standard provides the Abstract Test Suite (ATS) for security in ITS according to the 097 standard document.

3.3.10. ETSI TR 103 061-6 V1.1.1 (2015-09)[17]

This document presents the validation report of the above-mentioned standard (*ETSI TS 103 096-1(2,3)*) as a result of different tests such as validation of the GeoNetworking conformance test. More precisely, this standard describes the security code validation of the above standards. Two prototype implementations of the above-mentioned standards carried out by the industry, are considered for conformance tests.

3.3.11. ETSI TS 122 185 V15.0.0 (2018-07)[18] *and 3GPP TS 22.185 V14.4.0 (2018-06)*[19]

This document focuses on the service requirements of ITS through LTE. The document describes the 3rd Generation Partnership Project (3GPP) support for V2X communication through LTE. In addition to application requirements such as latency, reliability, message size, and frequency, this document defines the security requirements that include authentication, authorization, integrity protection, and privacy protection through pseudonymity. The standard also describes the 3GPP network support for authentication and authorization between the Mobile Network Operator (MNO) and the User Equipment (UE) to support different V2X applications.

[17] https://www.etsi.org/deliver/etsi_tr/103000_103099/10306106/01.01.01_60/tr_10306106v010101p.pdf

[18] https://www.etsi.org/deliver/etsi_ts/122100_122199/122185/14.03.00_60/ts_122185v140300p.pdf

[19] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2989

3.3.12. *ETSI TS 133 185 V15.0.0 (2018-07)*[20] *and 3GPP TS 33.185 V14.1.0 (2017-09)*[21]

These two documents define the security aspects of V2X in an LTE environment. It is worth mentioning that the documents mention 5G, but in the standard, there is no mention for 5G per se. This standard specifies the security architecture, security requirements for different network entities and the solutions provided as a result of those requirements. In this specification, application data security requirements are specified where the integrity and confidentiality (depending on the applications) of the data exchanged among V2X entities and the V2X system must be protected and resilient to replays. Furthermore, the privacy of the entities must also be protected whenever necessary.

3.3.13. *ETSI TS 122 186 V15.4.0 (2018-10)*[22]

This standard specifies the service requirements for V2X through Evolved Packet System (EPS) and 5G. In order to support V2X services through 5G, the document outlines the enhancements needed in 3GPP. The standard focuses on the transport layer support for safety and non-safety V2X applications. Among other requirements, this standard specifies the application-specific requirements for different applications such as platooning, advanced driving, extended sensors, and remote driving. This standard does not particularly focus on security. However, the future versions of this standard are expected to take security and privacy in 5G into account as well.

[20] https://www.etsi.org/deliver/etsi_ts/133100_133199/133185/14.00.00_60/ts_133185v140000p.pdf

[21] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3141

[22] https://www.etsi.org/deliver/etsi_ts/122100_122199/122186/15.03.00_60/ts_122186v150300p.pdf

3.3.14. ETSI TS 123 285 V15.1.0 (2018-07)[23]

This standard describes the enhancements to the architecture of the cellular system (LTE-/A) to support V2X services. These enhancements are based on the standard TS 22.185 (ETSI TS 122 185) as described above. The standard focuses on V2X communication over (LTE-V2X) PC5 and Uu interfaces. The architecture includes a roaming architecture over these interfaces with the specification of all functional entities that support V2X communications. Furthermore, the authentication and authorization provisioning procedures are defined for different network entities. The standard focuses on the upper layer security provisions for V2X services as well as identity management. It also specifies different options for RSU deployment and communication with RSUs with different interfaces.

3.3.15. ETSI TS 102 867 V1.1.1 (2012-06)[24]

This document is a compatibility effort by ETSI and specifies the use of IEEE 1609.2 standard in the ITS. This standard focuses on the subset of standards defined in TS 102 731 that contains security services. This document is also important because it identifies the security services that are not defined in IEEE 1609.2. For instance, this standard identifies that security association, confidentiality service for some messages, replay protection services, plausibility protection, and remote management are not supported by IEEE 1609.2.

Table 5 presents a summary of the standards presented above.

Table 5: VANET security standards

Standard	**Security aspects focused**	**Current status**
		Continued on next page

[23] https://www.etsi.org/deliver/etsi_ts/123200_123299/123285/15.01.00_60/ts_123285v150100p.pdf

[24] https://ia601007.us.archive.org/33/items/etsi_ts_102_867_v01.01.01/ts_102867v010101p.pdf

Table 5 – continued from previous page

IEEE 1609.2	• Message formats • Security of management messages • Security of application messages	Latest active version 1609.2-2016
SAE J2735	• Structure of the messages • Data structures • Data frames	Revised: 2009-11-19 (J2735_200911)
SAE J3061	• Security framework for ITS • Cybersecurity by design • Compliant with ISO 26262	Latest active version: J3061_201601
ETSI TS 102 723-8	• Interface between security entity, network, and transport layer • Confidentiality • Authentication and integrity • Identity management • Logging security events • Permissions management • Encapsulation/ decapsulation	V1.1.1 (2016-04), published

Continued on next page

Table 5 – continued from previous page

ETSI TS 102 731	• Security and privacy of communication among entities • Credential management • Identity management and anonymity • Data integrity protection • Authentication and authorization • Functional entity identification	V1.1.1 (2010-09), published
ETSI TR 102 893	• Threat identification and analysis • Risk analysis • Vulnerability analysis	V1.2.1 (2017-03), published (*update in preparation*)

Continued on next page

Table 5 – continued from previous page

ETSI TS 102 940	• Security architecture • Relationship among entities • Security for shared information • Guidelines for trust establishment • Public Key Infrastructure (PKI) definition	V1.3.1 (2018-04), published
ETSI TS 102 941	• Trust establishment and management • Privacy preservation mechanisms • Cryptographic primitives for trust establishment and management	V1.2.1 (2018-05), published
ETSI TS 102 942	• Access control • Authentication and authorization • Access rights definition	V1.1.1 (2012-06), published

Continued on next page

Table 5 – continued from previous page

ETSI TS 102 943	• Confidentiality services • Confidentiality at different layers (up to the network layer) • Definition of tools/methods/techniques to achieve confidentiality	V1.1.1 (2012-06)
ETSI TS 103 097	• Secure data structures • Headers and certificates format in ASN.1	V1.3.1 (2017-10), published (*update in preparation*)
ETSI TS 103 096-1(,2,3)	• Specifications for protocol implementation • Purpose of the tests and test suite • Abstract Test Suite (ATS) for security in ITS	V1.4.1 (2018-08), published
ETSI TR 103 061-6	• Validation report of *TS 103 07* and *TS 103 096*	V1.1.1 (2015-09), published
ETSI TS 122 185	• Service requirements of ITS through LTE • Security requirements of ITS • Network support for authentication and authorization	V15.0.0 (2018-07), published

Continued on next page

Table 5 – continued from previous page

ETSI TS 133 185	• Security aspects of V2X through LTE and 5G • Security structure and requirements for network entities • Application data security • Privacy preservation	V15.0.0 (2018-07), published
ETSI TS 122 186	• Service requirements of V2X through EPS • Enhancements needed in 3GPP • Transport layer support for safety and non-safety applications	V15.4.0 (2018-10), published
ETSI TS 123 285	• Enhancements to cellular architecture to support V2X • V2X communication over PC5 and Uu interfaces • Upper layer security for V2X services	V15.1.0 (2018-07), published
ETSI TS 102 867	• Compatibility of ETSI ITS and IEEE 1609.2 • Security services that are not mentioned in 1609.2	V1.1.1 (2012-06), published

Continued on next page

Table 5 – continued from previous page

3.4. Existing Security Inadequacies in VANET

In the previous section, we discussed the existing standardization efforts in the context of VANET security. Both ETSI and SAE have documented the standards focusing on different security aspects of VANET. However, it is important to mention that the current standards do not encompass the entire scope of the security requirements in VANET. More precisely, the existing standards mandate the use of cryptographic approaches for the security primitives such as authentication, authorization, integrity, trust, and privacy at the upper layers. Most of the current standards focus on the applications and services. It is also worth mentioning that the existing standards are based on both short-range (DSRC/WAVE) and long range (3G/LTE-(A)) communication mechanisms. There are still security gaps which are not fully addressed by the aforementioned standards. For instance, the existing standards focus on the core security requirements such as confidentiality, integrity, identity management, and authentication in cellular network-driven VANET. However, these standards do not take into account the attacks that are launched on cellular networks through IP-based backbone. These attacks include false data injection, data modification, IP spoofing, DDoS, and so on. The authentication becomes even more complex in the case of cellular network due to frequent handovers and mobility. Research results have demonstrated that in case of roaming, the users have to transmit their network identity in cleartext to the Mobile Management Entity (MME) which jeopardizes user privacy. Other attacks are discussed in more detail in [27].

Another important gap in the existing standards is the lack of focus on security at the lower layers (link and physical) [97]. From the core network perspective, lower layers are important for security provisioning in the network. Therefore, VANET needs security both at upper and lower layers. Some attacks such as jamming, channel distortion, and other lower layer attacks have not been extensively explored in VANET and the current VANET security standards do not address these issues. Furthermore, the proliferation of VANET services through clouds, IoT, SDN, blockchain and other enabling technologies also require new research directions in the security area. More precisely, the integration of new technologies with VANET will increase the challenges faced by existing VANET. For instance, enchanced VANET will also need efficient security management and control where context-aware per-user security provisions will be needed. Such fine-grained security control is not provided by the existing security solutions in VANET.

In this context, both enhancements to the old security solutions and new emerging solutions are necessary. New security standards along with communication paradigms are needed to address the security issues at the lower layers. To this end, 5G fills this gap by meeting the performance requirements of VANET applications, integration with different enabling technologies and enhancing security both at lower and upper layers with better management and control of the security services.

4. Seamless Integration of VANET and 5G Security

As we have mentioned before, VANET offers both safety applications and various value-added services. The distinction among these types of applications is important to invoke necessary functions such as security, performance, quality of service and so on. Some of these applications need higher bandwidth and low latency, whereas others need sophisticated security (more details are provided in the next subsections). Due to the enhanced applications' and services' landscape of vehicular networks and the inclusion of enabling technologies, the need for new communication technologies is essential. Without loss of generality, this paper focuses on the 5G communication technology and its security features offered to VANETs. However, it is equally important for the security features of the new communication paradigm(s) to co-exist with existing VANET security solutions and harness their benefits.

In the previous sections, we covered the background of the VANET security in detail and discussed the existing established security standards as well as the gaps that have not been filled yet. We also discussed the security features of the 5G, security architecture of 5G, enhanced security features of 5G and the threat landscape of 5G. In this section, we propose a high-level architecture for the integration of 5G security in VANETs. Next, we discuss the integrated security architecture of VANET and 5G, including context-aware extended security features introduced by 5G.

4.1. High Level Integrated Security Architecture

Figure 5 illustrates our proposed security architecture of VANET with 5G. The figure includes both the current security features offered by VANET standards at different layers and the security features (offered by 5G). We model the vehicular communication network into two broad layers, the upper layer that includes network and application, and lower layer where physical communication occurs. In the current VANET security standards, the upper layers provide security solutions that meet security requirements such as confidentiality, identity management, non-repudiation, routing, and privacy. At the application layer, current security standards support techniques such as HTTPS, SSL, TLS, standard cryptographic primitives, and PKI.

These techniques, at least to some extent, fulfill the security requirements of normal VANET applications. However, in the wake of new services such as real-time services on the road, enhanced security features and better security control and management are needed. Furthermore, in the case of large number of users, per user service provisions would require service providers to implement flexible security mechanisms. On the other hand, different users may have different security requirements for the same application. Such flexibility is not offered by the current security standards in VANET. In the network layer, current security standards support identity management, secure routing, interface security, and network support for security services. However, the heterogeneity of VANET and the integration of other enabling technologies such as IoT and

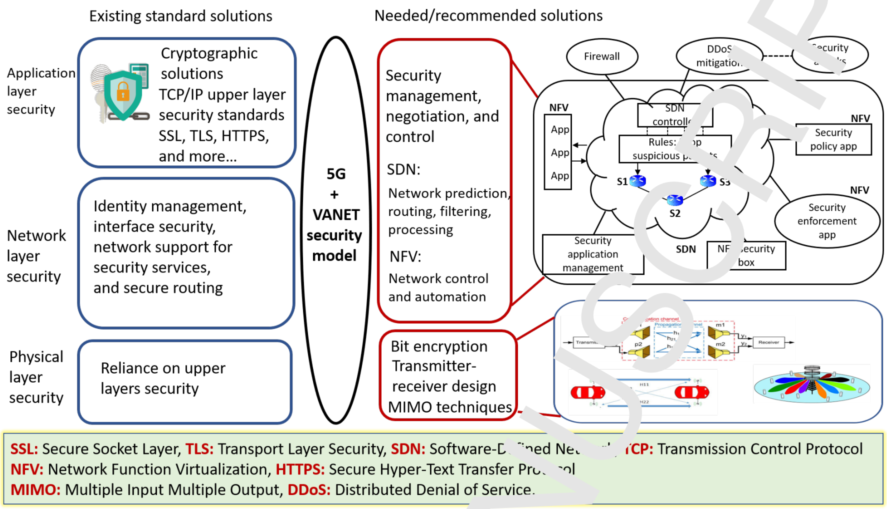

Figure 5: High level security architecture of 5G-enabled VANET

cloud computing need enhanced security, control, and management mechanisms to deal with the large number of users, versatile network infrastructures and communication paradigms.

In a nutshell, despite current security solutions, the management, control, agile provision and negotiation of security services that are essential for vehicular networks are missing in the current VANET security standards. Similarly, the decoupling of data and control planes enables flexible security management at network level which is also missing in the current standards. 5G offers these features through enabling technologies such as SDN and NFV, and can co-exist with the existing VANET security solutions. In essence, the security mechanisms are decoupled from the physical resources and are not associated with specific section of a network, therefore common security mechanisms can be applied to any network unit [98]. These virtualized security solutions are also helpful to meet the challenge of variation in traffic load and dynamically scale the security resources, accordingly. This provision of network programmability will also support on-demand, dynamic and flexible security policy adjustment according to the change in the network topology, size and attack type. Furthermore, due to flow-based policy enforcement, suspicious and infected flows can be isolated from rest of the network and can be prevented from back haul devices to restrict the propagation of security malfunction and network disruption. For instance, malicious traffic generated by a wireless edge for mobile-based DDoS attacks can be dropped easily without allowing it to reach the core network switches. In addition, sophisticated physical layer security measures are missing in the current VANET security standards whereas 5G along with its enabling technologies such as MIMO and Filter-Bank Multi-Carrier (FBMC) can address this limitation. Security at the physical layer is essential in VANET. 5G supports and implements security at the physical layer through different techniques such as secure channel design, MIMO techniques, and so on as shown in Fig. 5. Last but not the least, the context of VANET applications is important in defining the required security solutions and management, and 5G is expected to incorporate context-awareness for specific VANET scenarios or use-cases. The co-existence of current VANET security solutions and 5G security will need the context of application. In the following section, we describe the contexts specific to various applications in 5G-enabled VANET.

4.2. Context awareness

The proliferation of new VANET applications and services along with the integration with other enabling technologies require context-aware QoS and security provisions that are flexible on a per-user, per-application, and per-service basis. In this case, the context of the application is of paramount importance because based on the context, the required security provision will be invoked. Context information on one hand guarantees the relevant security primitives and on the other hand improves the QoS by invoking the appropriate security functions which match the capabilities of the underlying technology. For instance, when vehicular network needs information from IoT or cloud, the authentication scheme needed for both technologies may be different, wherein sophisticated authentication with IoT nodes may not work well and instead lightweight

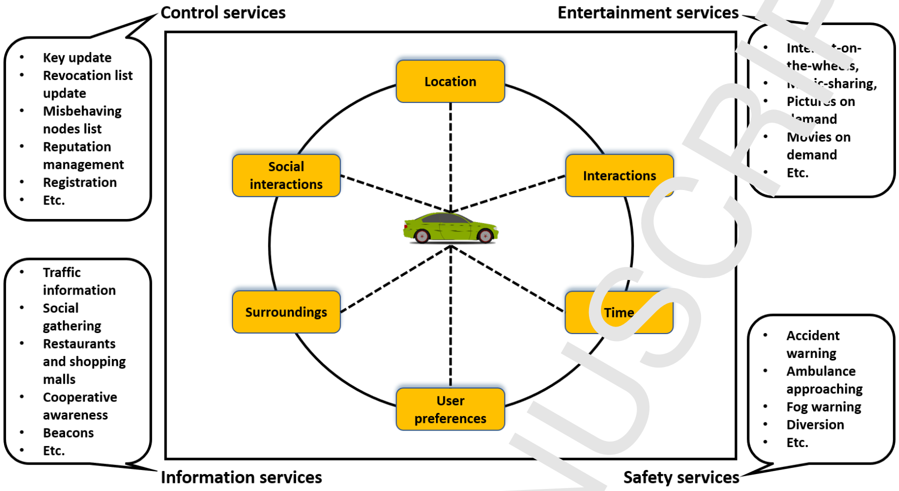

Figure 6: Contexts and their use-cases in integrated 5G-VANET

authentication mechanism would be preferred. We divide the context into 4 use-cases namely information, entertainment, control, and safety for which context is important when security provision is needed. Figure 6 illustrates the context and security requirements for various types of VANET applications.

4.2.1. Information exchange services

In the case of information exchange, VANET nodes request information from and share information (such as mobility information) not only among vehicular nodes but also with the surroundings. When the information is shared in close proximity, both DSRC and PC5 interfaces of 5G could be used when the security provisions are different and must be invoked accordingly. On the other hand, sharing information among multiple hops spanning large distances may use cellular (5G) or DSRC over multiple hops. This again needs clear context information from the application about the performance and security requirements. Similarly, smart advertisements could be shared among vehicular nodes that require security assurances. Other applications and services which need information exchange include sharing weather information, traffic information at specific locations, restaurant, shopping mall information and so on. In these applications, although the characteristics of the applications are different, the context is important for security provisions which can be efficiently achieved with 5G networking.

4.2.2. Entertainment services

VANET also offers entertainment applications such as Internet-on-the-wheels, music-sharing, pictures on demand [99], online social networking, and other content sharing services. These applications require unique security and network provisions such as strong authentication, privacy, and higher bandwidth. Content sharing services usually need higher bandwidth and low latency with better access control whereas online social networking needs flexible privacy provisions for different users with location privacy. The contribution by different users to such applications also require efficient and secure incentives mechanisms where user privacy is essential [83]. Furthermore, applications such as streaming video through home-network, controlling home appliances through vehicular networks and other such services need better management of security with respect to the context of the application. In such use-cases, 5G is well suited to utilize the existing resources and provide the required security using both the infrastructure and enabling technologies.

4.2.3. Safety services

Context is equally important for safety-related applications and services in VANET. Most of the safety applications in VANET require a minimum latency and high integrity. However, even within these requirements, based on the context of application, the priority could be different for different types of messages such as when there is an accident ahead, an ambulance approaching, fog, diversion, and so on. Therefore, to use the correct communication technology along with appropriate security provisions, knowledge of the applications context becomes essential. Hence, the context determines for the underlying communication mechanism the correct security function to invoke. The context for these use-cases require the coexistence of heterogeneous communication paradigms such as 5G and DSRC.

4.2.4. Control services

In addition to the data associated with entertainment and safety services offered by VANET applications, a lot of control information is also exchanged among different vehicular nodes and the management entities. For instance, in the case of traditional VANET applications, the delivery of cryptographic material and other security-sensitive information such as the list of revoked certificates/nodes, misbehaving vehicles, change of services, and so on, are also shared with the vehicles on the road through some communication infrastructure. These control services have stringent security requirements in terms of confidentiality, integrity, and non-repudiation. One use-case of such scenario could be the cluster head selection in the case of platooning. Therefore, context is essential for the communication mechanisms to invoke the right security functions at the right time for the right user. As discussed earlier, for VANET applications to work efficiently, we need to incorporate a context-aware mechanism where different communication paradigms (both cellular and DSRC/WAVE) can coexist. The context of the application could provide a better insight to the communication paradigm as well as necessary security primitives needed.

5. Future Challenges and Research Opportunities

To achieve secure 5G-based VANET applications/services, we need to increase investors interests in the commercialization of VANET, and consumers to utilize VANET services in their daily lives. Furthermore, with the proliferation of 5G-based VANET, consumers will be able to utilize the CPS ecosystem that includes smart home, health-care, transportation, smart office, and so on. The security services provided by 5G to the VANET are promising and solve various issues not previously addressed by traditional VANET security standards. However, the introduction of 5G to VANET also brings new challenges which need to be addressed before the commercial roll out of the 5G-based

VANET. In this section, we highlight and discuss some of the future challenges and research opportunities of 5G and VANET security.

5.1. Optimum Economic Model

Vehicular nodes in VANET produce large amount of data as a result of communication with other nodes and their surroundings. Using a cellular network such as 5G for such communication will not be free of cost and consumers may have to subscribe for the data plans. Furthermore, from the service providers' perspective, Return on Investment (RoI) should also be taken into account. Hardware cost is also an important factor and therefore service providers will need to come up with a concrete economic model that is attractive for the consumers. It is important because it will directly affect the proliferation of such integration and the interest of consumers. The possible choices for the consumers could be adapted from current business models such as pay-as-you-go, pay-as-you-use, pay-per-service, and so on. On the other hand, the processing and storage are also important issues that need to be considered by the service providers. Acceptable security and privacy guarantees to the consumers are also essential.

5.2. Handover Management

Mobility is the pinnacle of VANET and the current implementations of VANET exploit the dense deployment of RSUs. In the case of 5G, owing to the cellular network architecture, frequent handovers among different network entities (e.g., Base Transceiver Station (BTSs)) and different service providers are common. Depending on the type of VANET application and context, security-related information such as cryptographic keys, identities, and certificates might also need to be migrated to the new cells for authentication, confidentiality and other necessary security functions. Therefore, we need to design efficient handover management mechanisms. One possible solution could be the concept of umbrella cells used in 5G where one large cell manages small micro-cells and covers large area to accommodate node mobility. For high-speed nodes such as vehicles and connected rail, the connection might be managed by the umbrella cell to avoid frequent hand-overs. However, the security management at the umbrella cell is still subject to further investigation.

Authentication among different entities is also critical for most of the VANET applications and specially for safety-critical applications. With the integration of 5G into VANET, other enabling technologies such as SDN, cloud computing, and NFV will have to re(design) efficient, secure, seamless, and context-aware authentication mechanisms. To be more precise, the authentication among vehicular nodes and between a vehicular node and an IoT device is different, and therefore context-switching is essential. More research is needed in this area. One of the possible solutions could be Single Sign-On (SSO) authentication mechanism that is already implemented by many technologies. Another traditional solution could leverage Flat Distributed Cloud (FDC) that uses a cloud architecture, where the network is divided into clusters managed by the umbrella cells. This approach could be used for vehicular authentication in the context of 5G; however, more research is needed to evaluate such approaches. Furthermore, the storage and communication of the security-related information and its management is also subject to further research.

5.3. Identity Management and Privacy

Most of the VANET services need accurate location information and the user identity. However, user and location privacy is the prime concern of the consumers. For user identity, the current VANET security standards recommend the use of temporary identities (pseudonyms) and other cryptographic primitives whereas mix-zones and silence periods are used for location privacy [100, 101]. Furthermore, location-based encryption is also used for location privacy [25]. On the other hand, in case of cellular networks, a dedicated hardware-based identity Subscriber Identification Module (SIM) is issued to each subscriber for user identification. The user privacy with such hardware-based identity management must be further investigated to preserve user and location privacy. It is also worth mentioning that identity management is supported by 5G where more than one device could correspond to the single subscriber (which will come handy in case of IoT and in-care network); however, the privacy requirements and solutions must be further investigated. Some existing solutions like [81] and [102] could be tailored for the VANET applications with 5G communication paradigm. More precisely, Petit et al. [81] extensively surveyed the pseudnoym-based solutions for privacy preservation in VANET. The pseudonym-exchange mechanisms can be tailored for privacy preservation in 5G based VANET. Furthermore, as proposed in [102], identity-based conditional privacy preservation techniques can be tailored for the integrated 5G-based VANET.

5.4. Security Management of Enabling Technologies

Through 5G, the network control is virtualized and softwarized, which enables easy and efficient network management. However, it also provides opportunities to attackers for launching network attacks by exploiting vulnerabilities. Traditional hardware-based solutions for security issues are viable and currently well-adapted. Therefore, the change in paradigm to software-based network control may adversely affect the network security. The security of software-based network control through SDN in 5G should be further investigated, as human lives are at stake while using a VANET safety application. Furthermore, identity security, privacy, and other security requirements must also be taken into account as a result of such softwarization. Malicious applications, DDoS attacks, and other access control vulnerabilities could have severe consequences on the VANET applications and therefore must be further investigated from the integration standpoint of VANET and 5G. Other attacks include saturation attack on the network controller and exploitation of malicious Application Programming Interfaces (APIs). Additionally, the configuration errors in SDN and NFV could lead to negative consequences in mobile networks and VANET which could affect the auditability, security provisions, and other important functionalities of VANET. Furthermore, NFV is also vulnerable to DoS and other virtualization and side-channel attacks and hypervisor hijacking [103]. In order to realize the 5G-driven secure VANET, the security threats inherited from enabling technologies must be investigated and addressed.

5.5. Trust Management

The scale of information shared among different VANET entities is huge. All the applications and services offered by the VANET and the enabling technologies through 5G rely on the exchange of trustworthy information. Therefore, both entity and content trust should be guaranteed. In traditional VANET, various techniques are used to establish and manage trust among different network entities using both the cryptographic and non-cryptographic techniques. However, with the inclusion of new types of services such as cloud services, IoT services, SDN, and so on, traditional trust establishment techniques might not work. Therefore, new trust and reputation management schemes must be investigated. The large number of sources of information and their heterogeneity create more challenges for establishing trust in VANET while using 5G networking. Secure data transmission over 5G-enabled VANET has been researched and cryptographic solutions have been proposed in the literature [104, 105, 106]. For instance, Eiza et al. [104] proposed a system model for secure video transmission in 5G-enabled VANET. However establishing trust among different entities is a challenge and legacy solutions such as recommendation, social, and other trust establishment techniques might not work. It is also important to note that context also plays a vital role in trust establishment (entity and content trust) because different contexts of applications may have different security requirements. Therefore, efficient and adaptive trust mechanisms need to be developed for 5G-enabled VANET.

5.6. Efficiency, Flexibility, and Agility

Security solutions for VANET applications realized through 5G networking should be both efficient and flexible. From an efficiency perspective, cryptographic approaches are often both storage and compute-intensive which will adversely affect VANET applications. Furthermore, the integration of other enabling technologies will create various challenges such as the need for optimized security solutions in resource-constrained devices [107]. Flexibility is also important when multiple applications have different security requirements and each application and service must be secured according to their requirements. The ultra-low latency promise of 5G increases the range of new and exciting services for VANET. However, security solutions must be designed and optimized accordingly to achieve the ultra-low latency objective in addition to guaranteed promised security. One solution is to reduce the signalling overhead in 5G [108, 109]. Therefore, more investigation is needed in this area. Safety-critical applications of VANET need ultra-low latency which makes 5G a suitable candidate, but lightweight and efficient cryptographic solutions are needed to meet the requirement of low latency [100]. A possible solution for improving the efficiency could involve efficient control plane design where the control plane is placed near to the core. From an agility standpoint, security resource provisioning would depend on both the type and context of the application. Therefore, security management mechanisms must be agile to meet the varying demands of different applications and services. More investigation is needed in this context.

5.7. Flash Traffic Management

Vehicular nodes generate huge amounts of data as a result of communication within the vehicle, with peer vehicles, and with their surrounding infrastructure. This data contains mobility traces, control data, personalized data, and so on. The volume and velocity of such data advocates for using big data techniques for the realization of VANET applications. For instance, each vehicle in VANET shares cooperative awareness messages in the order of milliseconds. Therefore, in case of dense traffic, a lot of data would be generated by the neighboring nodes. Furthermore, this data could also be used by other services such as IoT, e-health, traffic management, and so on. 5G-enabled VANET must have efficient mechanisms to handle and manage such huge amounts of data and make sure that all the security requirements such as access control, access rights, integrity, privacy and similar requirements are met for each consumer. Furthermore, these mechanisms must be efficient so that the QoS requirements of different applications are met. Optimized big data techniques and in-network caching could be used to deal with the large amount of network data generated. However, more research is needed in this area in the future.

6. Conclusion

Efficient, viable, robust, and adaptive security solutions will pave the way for commercial vehicular network applications. To date, promising research results have been produced both by academia through publications, and by industry through practical experiments. However, before the commercialization of vehicular networks, advances in communication technologies such as emergence of 5th generation network (5G) have spurred even more interest in ITS. The demand for new and exciting real-time applications through vehicular networks and the integration with other enabling technologies such as cloud computing and IoT will need a communication paradigm that meets the requirements of the new applications. In this context, 5G is a strong candidate and has been studied by both academia and industry to integrate with VANET. In this paper, we studied VANET security focusing specifically on requirements, solutions, and current standards, and we pointed out existing deficiencies in VANET security solutions. We also presented the security features offered by 5G and their adequacy in vehicular networks. We proposed a high-level security architecture that integrates both VANET and 5G so that we can reap the benefits of both. Finally we also identified the challenges and future research directions for 5G-enabled vehicular networks. We summarize our conclusions as follows:

a. Current VANET security standards focus on the upper layers of the communication model and there is lack of security solutions at the lower layers.

b. Security at the lower layers of communication in VANET is equally important to mitigate attacks such as jamming and eavesdropping. More precisely, security at the physical layer should also be provided in addition to security at the application and network layers.

c. Merging VANET with other enabling technologies such as IoT, cloud computing, and social networks is essential to support the new services in VANET and therefore VANET security must be enhanced to address the resulting security challenges.

d. 5G is a strong candidate for VANET but 5G alone is not a silver bullet that will solve all the problems of VANET.

e. The security solutions provided by 5G and the existing VANET security solutions should coexist to achieve secure VANET applications. The security services provided by 5G at the physical layer and the management and control functions at the upper layer should be combined with the current security standards of VANET.

f. The research community should focus on a holistic security approach to enable a 5G-enabled VANET.

We believe that this work will serve as steppingstone for further research in the direction of 5G-enabled vehicular networks.

Acknowledgments

We thank the anonymous reviewers for their useful comments which helped us to improve the organization, content, and presentation of this paper.

References

[1] J. Guerrero-Ibáñez, S. Zeadally, J. Contreras-Castillo, Sensor technologies for intelligent transportation systems, Sensors (Basel) 18 (4). doi:10.3390/s18041212.

[2] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, H. Zedan, A comprehensive survey on vehicular ad hoc network, Journal of Network and Computer Applications 37 (2014) 380 – 392. doi:https://doi.org/10.1016/j.jnca.2013.02.036.

URL http://www.sciencedirect.com/science/article/pii/S108480451300074X

[3] M. Whaiduzzaman, M. Sookhak, A. Gani, R. Buyya, A survey on vehicular cloud computing, Journal of Network and Computer Applications 40 (2014) 325–344.

[4] R. Hussain, Z. Rezaeifar, H. Oh, A paradigm shift from vehicular ad hoc networks to vanet-based clouds, Wireless Personal Communications 83 (2) (2015) 1131–1158.

[5] Y. Toor, P. Muhlethaler, A. Laouiti, A. D. L. Fortelle, Vehicle ad hoc networks: applications and related technical issues, IEEE Communications Surveys Tutorials 10 (3) (2008) 74–88. doi:10.1109/COMST.2008.4625806.

[6] E. Schoch, F. Kargl, M. Weber, T. Leinmuller, Communication patterns in vanets, IEEE Communications Magazine 46 (11) (2008) 119–125. doi:10.1109/MCOM.2008.4689254.

[7] R. Hussain, Z. Rezaeifar, D. Kim, A. O. Tokuta, H. Oh, On secure, privacy-aware, and efficient beacon broadcasting among one-hop neighbors in vanets, in: 2014 IEEE Military Communications Conference, 2014, pp. 1427–1432. doi:10.1109/MILCOM.2014.236.

[8] K. A. Hafeez, L. Zhao, B. Ma, J. W. Mark, Performance analysis and enhancement of the dsrc for vanet's safety applications, IEEE Transactions on Vehicular Technology 62 (7) (2013) 3069–3083. doi:10.1109/TVT.2013.2251374.

[9] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. Mini, A. A. Loureiro, Data communication in vanets: Protocols, applications and challenges, Ad Hoc Networks 44 (2016) 90 – 103. doi:https://doi.org/10.1016/j.adhoc.2016.02.017.

URL http://www.sciencedirect.com/science/article/pii/S1570870516300580

[10] M. A. Javed, E. B. Hamida, On the interrelation of security, qos, and safety in cooperative its, IEEE Transactions on Intelligent Transportation Systems 18 (7) (2017) 1943–1957. doi:10.1109/TITS.2016.2614580.

[11] R. Hussain, S. Kim, H. Oh, Towards privacy aware pseudonymless strategy for avoiding profile generation in vanet, in: H. Y. Youm, M. Yung (Eds.), Information Security Applications, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009, pp. 268–280.

[12] J. T. Isaac, S. Zeadally, J. S. Camara, Security attacks and solutions for vehicular ad hoc networks, IET Communications 4 (7) (2010) 894–903. doi:10.1049/iet-com.2009.0191.

[13] R. Hussain, H. Oh, On secure and privacy-aware sybil attack detection in vehicular communications, Wireless Personal Communications 77 (4) (2014) 2649–2673. doi:10.1007/s11277-014-1659-5.
URL https://doi.org/10.1007/s11277-014-1659-5

[14] J. Contreras-Castillo, S. Zeadally, J. A. Guerrero Ibaez, Solving vehicularad hocnetwork challenges with big data solutions, IET Networks 5 (4) (2016) 81–84. doi:10.1049/iet-net.2016.0001.

[15] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (vanets): status, results, andchallenges, Telecommunication Systems 50 (4) (2012) 217–241. doi:10.1007/s11235-010-9400-5.
URL https://doi.org/10.1007/s11235-010-9400-5

[16] R. Meireles, M. Boban, P. Steenkiste, O. Tonguz, J. Barros, Experimental study on the impact of vehicular obstructions in vanets, in: 2010 IEEE Vehicular Networking Conference, 2010, pp. 338–345. doi:10.1109/VNC.2010.5698233.

[17] M. Boban, R. Meireles, J. Barros, O. Tonguz, P. Steenkiste, Exploiting the height of vehicles in vehicular communication, in: 2011 IEEE Vehicular Networking Conference (VNC), 2011, pp. 163–170. `doi:10.1109/VNC.2011.6117138`.

[18] M. Boban, T. T. V. Vinhoza, M. Ferreira, J. Barros, O. K. Tonguz, Impact of vehicles as obstacles in vehicular ad hoc networks, IEEE Journal on Selected Areas in Communications 29 (1) (2011) 15–28. `doi:10.1109/JSAC.2011.110103`.

[19] K. Dar, M. Bakhouya, J. Gaber, M. Wack, P. Lorenz, Wireless communication technologies for its applications [topics in automotive networking], IEEE Communications Magazine 48 (5) (2010) 156–162. `doi:10.1109/MCOM.2010.5458377`.

[20] A. Cailean, B. Cagneau, L. Chassagne, V. Popa, M. Dimian, A survey on the usage of dsrc and vlc in communication-based vehicle safety applications, in: 2014 IEEE 21st Symposium on Communications and Vehicular Technology in the Benelux (SCVT), 2014, pp. 69–74. `doi:10.1109/SCVT.2014.7046710`.

[21] F. Hussain, H. Farahneh, X. Fernando, A. Ferworn, Vlc enabled foglets assisted road asset reporting, in: 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), 2017, pp. 1–6. `doi:10.1109/VTCSpring.2017.8108636`.

[22] S. A. A. Shah, E. Ahmed, M. Imran, S. Zeadally, 5g for vehicular communications, IEEE Communications Magazine 56 (1) (2018) 111–117. `doi:10.1109/MCOM.2018.1700467`.

[23] R. Hussain, F. Abbas, J. Son, H. Eun, H. Oh, Privacy-aware route tracing and revocation games in vanet-based clouds, in: 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 730–735. `doi:10.1109/WiMOB.2013.6673437`.

[24] W. He, G. Yan, L. D. Xu, Developing vehicular data cloud services in the iot environment, IEEE Transactions on Industrial Informatics 10 (2) (2014) 1587–1595. doi:10.1109/TII.2014.2299233.

[25] R. Hussain, Z. Rezaeifar, Y.-H. Lee, H. Oh, Secure and privacy-aware traffic information as a service in vanet-based clouds, Pervasive and Mobile Computing 24 (2015) 194 – 209, special Issue on Secure Ubiquitous Computing. doi:http://dx.doi.org/10.1016/j.pmcj.2015.07.007.
URL http://www.sciencedirect.com/science/article/pii/S1574119215001455

[26] A. Boukerche, R. E. D. Grande, Vehicular cloud computing: Architectures, applications, and mobility, Computer Networks 135 (2018) 171 – 189. doi:https://doi.org/10.1016/j.comnet.2018.01.004.
URL http://www.sciencedirect.com/science/article/pii/S1389128618300057

[27] J. Cao, M. Ma, H. Li, Y. Zhang, Z. Luo, A survey on security aspects for lte and lte-a networks, IEEE Communications Surveys Tutorials 16 (1) (2014) 283–302. doi:10.1109/SURV.2013.041513.00174.

[28] J. A. Guerrero-ibanez, S. Zeadally, J. Contreras-Castillo, Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies, IEEE Wireless Communications 22 (6) (2015) 122–128. doi:10.1109/MWC.2015.7368833.

[29] F. Qu, Z. Wu, F. Y. Wang, W. Cho, A security and privacy review of vanets, IEEE Transactions on Intelligent Transportation Systems 16 (6) (2015) 2985–2996. doi:10.1109/TITS.2015.2439292.

[30] Z. Lu, G. Qu, Z. Liu, A survey on recent advances in vehicular network security, trust, and privacy, IEEE Transactions on Intelligent Transportation Systems 20 (2) (2019) 760–776. doi:10.1109/TITS.2018.2818888.

[31] H. Hasrouny, A. E. Samhat, C. Bassil, A. Laouiti, Vanet security challenges and solutions: A survey, Vehicular Communications 7 (2017) 7 – 20. doi:https://doi.org/10.1016/j.vehcom.2017.01.002. URL http://www.sciencedirect.com/science/article/pii/S2214209616301231

[32] H. Hartenstein, L. P. Laberteaux, A tutorial survey on vehicular ad hoc networks, IEEE Communications Magazine 46 (6) (2008) 164–171. doi:10.1109/MCOM.2008.4539481.

[33] G. Araniti, C. Campolo, M. Condoluci, A. Iera, A. Molinaro, Lte for vehicular networking: a survey, IEEE Communications Magazine 51 (5) (2013) 148–157. doi:10.1109/MCOM.2013.6515060.

[34] S. Chen, J. Hu, Y. Shi, L. Zhao, Lte-v: A td-lte-based v2x solution for future vehicular network, IEEE Internet of Things Journal 3 (6) (2016) 997–1005. doi:10.1109/JIOT.2016.2611605.

[35] W. Lobato Junior, J. Costa, D. Rosario, E. Cerqueira, L. A. Villas, A comparative analysis of dsrc and vlc for video dissemination in platoon of vehicles, in: 2018 IEEE 10th Latin-American Conference on Communications (LATINCOM), 2018, pp. 1–6. doi:10.1109/LATINCOM.2018.8613247.

[36] M. Agiwal, A. Roy, N. Saxena, Next generation 5g wireless networks: A comprehensive survey, IEEE Communications Surveys Tutorials 18 (3) (2016) 1617–1655. doi:10.1109/COMST.2016.2532458.

[37] T. Mekki, I. Jabri, A. Rachedi, M. ben Jemaa, Vehicular cloud networks: Challenges, architectures, and future directions, Vehicular Communications 9 (2017) 268 – 280. doi:https://doi.org/10.1016/j.vehcom.2016.11.009. URL http://www.sciencedirect.com/science/article/pii/S2214209616300559

[38] M. et al., Survey on existing authentication issues for cellular-assisted V2X communication, Elsevier Journal on Vehicular Communication (12) (2018) 50–65.

[39] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, H. Janicke, Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes, Journal of Network and Computer Applications 101 (2018) 55 – 82. doi:https://doi.org/10.1016/j.jnca.2017.10.017.
URL http://www.sciencedirect.com/science/article/pii/S1084804517303521

[40] D. Fang, R. Qingyang, Security for 5G Mobile Wireless Networks, IEEE Access 6 (2018) 4850–4874.

[41] D. et al., The Internet of Vehicles based on 5G Communications, IEEE Conference on Internet of Things (2016) 445–448.

[42] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, M. A. Javed, A survey of device-to-device communications: Research issues and challenges, IEEE Communications Surveys Tutorials 20 (3) (2018) 2133–2168. doi:10.1109/COMST.2018.2828120.

[43] M. et al., Reliable vehicular broadcast using 5g device-to-device communication, IFIP Wireless and Mobile Networking Conference (WMNC) (2017) 1–8.

[44] S. Y. Ahmad, Liyanage, Gurtov, Design principles for 5g security, in: A Comprehensive Guide to 5G Security, Wiley, 2018, pp. 75–95.

[45] J. Contreras-Castillo, S. Zeadally, J. A. Guerrero-Ibaez, Internet of vehicles: Architecture, protocols, and security, IEEE Internet of Things Journal 5 (5) (2018) 3701–3709. doi:10.1109/JIOT.2017.2690902.

[46] D. S. W. K. A. B. P. Agyapong, M. Iwamura, Design considerations for a 5G network architecture, IEEE Communication Magazine 52 (11) (2014) 65–75.

[47] A. Gupta, R. K. Jha, A survey of 5g network: Architecture and emerging technologies, IEEE Access 3 (2015) 1206–1232. doi:10.1109/ACCESS.2015.2461602.

[48] A. K. Jain, R. Acharya, S. Jakhar, T. Mishra, Fifth generation (5g) wireless technology revolution in telecommunication, in: 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 1867–1872. doi:10.1109/ICICCT.2018.8473011.

[49] G. T. 33.401, 3gpp system architecture evolution (sae); security architecture, 2017.

[50] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Flix, F. Klaedtke, P. K. Nakarmi, M. Nslund, P. OHanlon, J. Papay, J. Suomalainen, M. Surridge, J. Wary, A. Zahariev, A security architecture for 5g networks, IEEE Access 6 (2018) 22466–22479. doi:10.1109/ACCESS.2018.2827419.

[51] M. S. Siddiqui, E. Escalona, E. Trouva, M. A. Kourtis, D. Kritharidis, K. Katsaros, S. Spirou, C. Canales, M. Lorenzo, Policy based virtualised security architecture for sdn/nfv enabled 5g access networks, in: 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2016, pp. 44–49. doi:10.1109/NFV-SDN.2016.7919474.

[52] L. Sun, Q. Du, Physical layer security with its applications in 5g networks: A review, China Communications 14 (12) (2017) 1–14. doi:10.1109/CC.2017.8246328.

[53] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, X. Gao, A survey of physical layer security techniques for 5g wireless networks and challenges ahead, IEEE Journal on Selected Areas in Communications 36 (4) (2018) 679–695. doi:10.1109/JSAC.2018.2825560.

[54] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, M. D. Renzo, Safeguarding 5g wireless communication networks using physical layer security, IEEE Communications Magazine 53 (4) (2015) 20–27. doi:10.1109/MCOM.2015.7081071.

[55] I. Farris, T. Taleb, Y. Khettab, J. Song, a survey on emerging sdn and nfv security mechanisms for iot systems, in: IEEE Communication Surveys and Tutorials, 2018, pp. 1–26.

[56] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, M. Ylianttila, A Comprehensive Guide to 5G Security, 1st Edition, Wiley Publishing, 2018.

[57] I. Adam, J. Ping, Framework for security event management in 5g, in: Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018, ACM, New York, NY, USA, 2018, pp. 51:1–51:7. doi:10.1145/3230833.3233254.
URL http://doi.acm.org/10.1145/3230833.3233254

[58] D. Liao, H. Li, G. Sun, M. Zhang, V. Chang, Location and trajectory privacy preservation in 5g-enabled vehicle social network services, Journal of Network and Computer Applications 110 (2018) 108 – 118. doi:https://doi.org/10.1016/j.jnca.2018.02.002.
URL http://www.sciencedirect.com/science/article/pii/S1084804518300390

[59] D. Kapetanovic, G. Zheng, F. Rusek, Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks, CoRR abs/1504.07154. arXiv:1504.07154.
URL http://arxiv.org/abs/1504.07154

[60] X. Zhang, A. Kunz, S. Schrder, Overview of 5g security in 3gpp, in: 2017 IEEE Conference on Standards for Communications and Networking (CSCN), 2017, pp. 181–186. doi:10.1109/CSCN.2017.8088619.

[61] G. S. Architecture, https://www-file.huawei.com/, 2017.

[62] M. Geller, P. Nair, 5G Security Innovation with Cisco, Tech. rep., Cisco (01 2018).

[63] C. Jiang, H. Zhang, Y. Ren, Z. Han, K. Chen, L. Hanzo, Machine learning paradigms for next-generation wireless networks, IEEE Wireless Communications 24 (2) (2017) 98–105. doi:10.1109/MWC.2016.1500356WC.

[64] J. Li, Machine learning-based ids for software-defined 5g network, IET Networks 7 (2018) 53–60(7).
URL https://digital-library.theiet.org/content/journals/10.1049/iet-net.2017.0212

[65] G. T. 33.899, "study on the security aspects of the next generation system", Vol. 1.1.1.0, 2017.

[66] P. Schneider, G. Horn, Towards 5g security, in: 2015 IEEE Trustcom/BigDataSE/ISPA, Vol. 1, 2015, pp. 1165–1170. doi:10.1109/Trustcom.2015.499.

[67] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, Overview of 5g security challenges and solutions, IEEE Communications Standards Magazine 2 (1) (2018) 36–43. doi:10.1109/MCOMSTD.2018.1700063.

[68] I. Stojmenovic, S. Wen, X. Huang, H. Luan, An overview of fog computing and its security issues, Concurrency and Computation: Practice and Experience 28 (10) 2991–3005. arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.3485, doi:10.1002/cpe.3485.

URL https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.3485

[69] M. A. Khan, A survey of security issues for cloud computing, Journal of Network and Computer Applications 71 (2016) 11 – 29. doi:https://doi.org/10.1016/j.jnca.2016.05.010.
URL http://www.sciencedirect.com/science/article/pii/S1084804516301060

[70] F. Tian, P. Zhang, Z. Yan, A survey on c-ran security, IEEE Access 5 (2017) 13372–13386. doi:10.1109/ACCESS.2017.2717852.

[71] S. Woo, H. J. Jo, D. H. Lee, A practical wireless attack on the connected car and security protocol for in-vehicle can, IEEE Transactions on Intelligent Transportation Systems 16 (2) (2015) 993–1006. doi:10.1109/TITS.2014.2351612.

[72] V. H. Le, J. den Hartog, N. Zannone, Security and privacy for innovative automotive applications: A survey, Computer Communications 132 (2018) 17 – 41. doi:https://doi.org/10.1016/j.comcom.2018.09.010.
URL http://www.sciencedirect.com/science/article/pii/S014036641731174X

[73] M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks, J. Comput. Secur. 15 (1) (2007) 39–68.
URL http://dl.acm.org/citation.cfm?id=1370616.1370618

[74] S. Woo, H. J. Jo, I. S. Kim, D. H. Lee, A practical security architecture for in-vehicle can-fd, IEEE Transactions on Intelligent Transportation Systems 17 (8) (2016) 2248–2261. doi:10.1109/TITS.2016.2519464.

[75] R. Hussain, S. Zeadally, Autonomous cars: Research results, issues and future challenges, IEEE Communications Surveys Tutorials (2018) 1–1doi:10.1109/COMST.2018.2869360.

[76] S. Bittl, A. A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer, B. Eissfeller, Emerging attacks on vanet security based on gps time spoofing, in: 2015 IEEE Conference on Communications and Network Security (CNS), 2015, pp. 344–352. doi:10.1109/CNS.2015.7346845.

[77] R. Hussain, H. Oh, S. Kim, Antisybil: Standing against sybil attacks in privacy-preserved vanet, in: 2012 International Conference on Connected Vehicles and Expo (ICCVE), 2012, pp. 108–113. doi:10.1109/ICCVE.2012.27.

[78] T. Zhou, R. R. Choudhury, P. Ning, K. Chakrabarty, P2dap sybil attacks detection in vehicular ad hoc networks, IEEE Journal on Selected Areas in Communications 29 (3) (2011) 582–594. doi:10.1109/JSAC.2011.110308.

[79] S. Chang, Y. Qi, H. Zhu, J. Zhao, X. Shen, Footprint: Detecting sybil attacks in urban vehicular networks, IEEE Transactions on Parallel and Distributed Systems 23 (6) (2012) 1103–1114. doi:10.1109/TPDS.2011.263.

[80] R. Hussain, S. Kim, H. Oh, Privacy-aware vanet security: Putting data-centric misbehavior and sybil attack detection schemes into practice, in: D. H. Lee, M. Yung (Eds.), Information Security Applications, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 296–311.

[81] J. Petit, F. Schaub, M. Feiri, F. Kargl, Pseudonym schemes in vehicular networks: A survey, IEEE Communications Surveys Tutorials 17 (1) (2015) 228–255. doi:10.1109/COMST.2014.2345420.

[82] B. Wiedersheim, Z. Ma, F. Kargl, P. Papadimitratos, Privacy in inter-vehicular networks: Why simple pseudonym change is not enough, in: 2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS), 2010, pp. 176–183. doi:10.1109/WONS.2010.5437115.

[83] R. Hussain, D. Kim, J. Son, J. Lee, C. A. Kerrache, A. Benslimane, H. Oh, Secure and privacy-aware incentives-based witness service in social internet of vehicles clouds, IEEE Internet of Things Journal 5 (4) (2018) 2441–2448. doi:10.1109/JIOT.2018.2847249.

[84] K. D. Thilak, A. Amuthan, Cellular automata-based improved ant colony-based optimization algorithm for mitigating ddos attacks in vanets, Future Generation Computer Systems 82 (2018) 304 – 314. doi:https://doi.org/10.1016/j.future.2017.11.043.
URL http://www.sciencedirect.com/science/article/pii/S0167739X1732215X

[85] F. Sakiz, S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: vanets and iov, Ad Hoc Networks 61 (2017) 33 – 50. doi:https://doi.org/10.1016/j.adhoc.2017.03.006.
URL http://www.sciencedirect.com/science/article/pii/S1570870517300562

[86] N. Vanitha, G. Padmavathi, A study on various cyber-attacks and their classification in uav assisted vehicular ad-hoc networks, in: G. Ganapathi, A. Subramaniam, M. Graña, S. Balusamy, R. Natarajan, P. Ramanathan (Eds.), Computational Intelligence, Cyber Security and Computational Models. Models and Techniques for Intelligent Systems and Automation, Springer Singapore, Singapore, 2018, pp. 124–131.

[87] M. T. Garip, P. Reiher, M. Gerla, Ghost: Concealing vehicular botnet communication in the vanet control channel, in: 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), 2016, pp. 1–6. doi:10.1109/IWCMC.2016.7577024.

[88] M. T. Garip, P. Reiher, M. Gerla, Botveillance: A vehicular botnet surveillance attack against pseudonymous systems in vanets, in: 2018 11th IFIP

Wireless and Mobile Networking Conference (WMNC), 2018, pp. 1–8. doi:10.23919/WMNC.2018.8480909.

[89] G. Yan, D. Wen, S. Olariu, M. C. Weigle, Security challenges in vehicular cloud computing, IEEE Transactions on Intelligent Transportation Systems 14 (1) (2013) 284–294. doi:10.1109/TITS.2012.2211870.

[90] H. Li, R. Lu, J. Misic, M. Mahmoud, Security and privacy of connected vehicular cloud computing, IEEE Network 32 (3) (2018) 4–6. doi:10.1109/MNET.2018.8370870.

[91] J. Joy, M. Gerla, Internet of vehicles and autonomous connected car - privacy and security issues, in: 2017 26th International Conference on Computer Communication and Networks (ICCCN), 2017, pp. 1–9. doi:10.1109/ICCCN.2017.8038391.

[92] A. Di Maio, M. R. Palattella, R. Soua, L. Lamorte, X. Vilajosana, J. Alonso-Zarate, T. Engel, Enabling sdn in vanets: What is the impact on security?, Sensors 16 (12). doi:10.3390/s16122077.
URL http://www.mdpi.com/1424-8220/16/12/2077

[93] F. Ahmad, M. Kazim, A. Adnane, A. Awad, Vehicular cloud networks: Architecture, applications and security issues, in: 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), 2015, pp. 571–576. doi:10.1109/UCC.2015.101.

[94] E. B. Hamida, H. Noura, W. Znaidi, Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures, Electronics 4 (3) (2015) 380–423. doi:10.3390/electronics4030380.
URL http://www.mdpi.com/2079-9292/4/3/380

[95] Ieee standard for wireless access in vehicular environments–security services for applications and management messages, IEEE Std 1609.2-

2016 (Revision of IEEE Std 1609.2-2013) (2016) 1–240doi:10.1109/IEEESTD.2016.7426684.

[96] C. Schmittner, Z. Ma, C. Reyes, O. Dillinger, P. Puschner, Using sae j3061 for automotive security requirement engineering, in: A. Skavhaug, J. Guiochet, E. Schoitsch, F. Bitsch (Eds.), Computer Safety, Reliability, and Security, Springer International Publishing, Cham, 2016, pp. 157–170.

[97] Y. O. Basciftci, F. Chen, J. Weston, R. Burton, C. E. Koksal, How vulnerable is vehicular communication to physical layer jamming attacks?, in: 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), 2015, pp. 1–5. doi:10.1109/VTCFall.2015.7390968.

[98] M. Liyanage, A. B. Abro, M. Ylianttila, A. Gurtov, Opportunities and challenges of software-defined mobile networks in network security, IEEE Security Privacy 14 (4) (2016) 34–44. doi:10.1109/MSP.2016.82.

[99] M. Gerla, J. Weng, G. Pau, Pics-on-wheels: Photo surveillance in the vehicular cloud, in: 2013 International Conference on Computing, Networking and Communications (ICNC), 2013, pp. 1123–1127. doi:10.1109/ICCNC.2013.6504250.

[100] A. Zhang, L. Wang, X. Ye, X. Lin, Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems, IEEE Transactions on Information Forensics and Security 12 (3) (2017) 662–675. doi:10.1109/TIFS.2016.2631950.

[101] L. Buttyan, T. Holczer, A. Weimerskirch, W. Whyte, Slow: A practical pseudonym changing scheme for location privacy in vanets, in: 2009 IEEE Vehicular Networking Conference (VNC), 2009, pp. 1–8. doi:10.1109/VNC.2009.5416380.

[102] D. He, S. Zeadally, B. Xu, X. Huang, An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc net-

works, IEEE Transactions on Information Forensics and Security 10 (12) (2015) 2681–2691. doi:10.1109/TIFS.2015.2473820.

[103] A. van Cleeff, W. Pieters, R. J. Wieringa, Security implications of virtualization: A literature study, in: 2009 International Conference on Computational Science and Engineering, Vol. 3, 2009, pp. 353–358. doi:10.1109/CSE.2009.267.

[104] M. H. Eiza, Q. Ni, Q. Shi, Secure and privacy-aware cloud-assisted video reporting service in 5g-enabled vehicular networks, IEEE Transactions on Vehicular Technology 65 (10) (2016) 7868–7881. doi:10.1109/TVT.2016.2541862.

[105] K. Mershad, H. Artail, A framework for secure and efficient data acquisition in vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 62 (2) (2013) 536–551. doi:10.1109/TVT.2012.2226613.

[106] X. Feng, L. Wang, S2pd: A selective sharing scheme for privacy data in vehicular social networks, IEEE Access 6 (2018) 55139–55148. doi:10.1109/ACCESS.2018.2872789.

[107] K. Boakye-Boateng, E. Kuada, E. Antwi-Boasiako, E. Djaba, Encryption protocol for resource-constrained devices in fog-based iot using one-time pads, IEEE Internet of Things Journal (2019) 1–1doi:10.1109/JIOT.2019.2893172.

[108] P. Andres-Maldonado, P. Ameigeiras, J. Prados-Garzon, J. J. Ramos-Munoz, J. M. Lopez-Soler, Reduced m2m signaling communications in 3gpp lte and future 5g cellular networks, in: 2016 Wireless Days (WD), 2016, pp. 1–3. doi:10.1109/WD.2016.7461499.

[109] R. Jin, X. Zhong, S. Zhou, The access procedure design for low latency in 5g cellular network, in: 2016 IEEE Globecom Workshops (GC Wkshps), 2016, pp. 1–6. doi:10.1109/GLOCOMW.2016.7849058.

ACCEPTED MANUSCRIPT

The authors do not have any conflict of interest.

Rasheed Hussain received his B.S. Engineering degree in Computer Software Engineering from University of Engineering and Technology, Peshawar, Pakistan in 2007, MS and PhD degrees in Computer Science and Engineering from Hanyang University, South Korea in 2010 and 2015, respectively. He worked as a Postdoctoral Fellow at Hanyang University, South Korea from March 2015 to August 2015. He also worked as a guest researcher and consultant at University of Amsterdam (UvA) from September 2015 till May 2016. He worked as Assistant Professor at Innopolis University, Innopolis Russia from June 2016 till December 2018. Currently he is an Associate Professor and Head of the MS program in Secure System and Network Engineering (SNE) at Innopolis University, Russia. He is also the Head of Networks and Blockchain Lab at Innopolis University. He serves as editorial board member for various journals including IEEE Access, IEEE Internet Initiative, Internet Technology Letters, Wiley, and serves as reviewer for most of the IEEE transactions, Springer and Elsevier Journals. He also serves as technical program committee member of various conferences such as IEEE VTC, IEEE VNC, IEEE Globecom, IEEE ICCVE, and so on. He is a certified trainer for Instructional Skills Workshop (ISW). Furthermore, he is also ACM Distinguished Speaker. His research interests include Information Security and Privacy and particularly security and privacy issues in Vehicular Ad Hoc NETworks (VANETs), vehicular clouds, and vehicular social networking, applied cryptography, Internet of Things, Content-Centric Networking (CCN), cloud computing, and blockchain. Currently he is working on carpooling and blockchain technologies for resource-constrained environments.

Fatima Hussain is working as Security Analyst in security service squad. She is leading the development and promotion of a new API and API platform learning curriculum, along with assisting API security duties. Her background includes a number of distinguished professorships at Ryerson University and the University of Guelph, where she has been awarded for her research, teaching and course development accomplishments within Wireless Telecommunications, Internet of Things Networks, and Machine Learning. She has long list of research publications in top tire conferences and journals. She is an associate editor for various IEEE Newsletters (IEEE Ethics and Policy, IEEE Future Initiative, IEEE WIE (Toronto section)). She also holds a Doctorate, a Master of Engineering, a Master of Science, and a Bachelor of Science degree, all in Electrical & Computer Engineering, along with professional engineer (P.Eng) license (in progress).

Sherali Zeadally is an associate professor in the College of Communication and Information at the University of Kentucky. He received his bachelor degree in Computer Science from the University of Cambridge, England, and his doctoral degree in Computer Science from the University of Buckingham, England. He is a Fellow of the British Computer Society and a Fellow of the Institution of Engineering Technology, England.

Rasheed Hussain

Fatima Hussain

Sherali Zeadally

Highlights

- Security issues in vehicular networks
- Inadequacy of current Vehicular Ad hoc NETwork (VANET) security solutions
- Security features of 5G network
- Integration of VANET and 5G security
- Future challenges in 5G-based VANET security