ARTICLE INFO
Article ID: 12-06-02-0011

doi:10.4271/12-06-02-0011

Wireless Security in Vehicular Ad Hoc Networks: A Survey

Thomas Blazek,[1] Fjolla Ademaj,[1] Stefan Marksteiner,[2,3] Peter Priller,[2] and Hans-Peter Bernhard[1,4]

[1]Silicon Austria Labs GmbH, Austria
[2]AVL List GmbH, Austria
[3]Mälardalen University, Sweden
[4]Johannes Kepler University Linz, Austria

Abstract

Vehicular communications face unique security issues in wireless communications. While new vehicles are equipped with a large set of communication technologies, product life cycles are long and software updates are not widespread. The result is a host of outdated and unpatched technologies being used on the street. This has especially severe security impacts because autonomous vehicles are pushing into the market, which will rely, at least partly, on the integrity of the provided information.

We provide an overview of the currently deployed communication systems and their security weaknesses and features to collect and compare widely used security mechanisms. In this survey, we focus on technologies that work in an ad hoc manner. This includes Long-Term Evolution mode 4 (LTE-PC5), Wireless Access in Vehicular Environments (WAVE), Intelligent Transportation Systems at 5 Gigahertz (ITS-G5), and Bluetooth. First, we detail the underlying protocols and their architectural components. Then, we list security designs and concepts, as well as the currently known security flaws and exploits.

Our overview shows the individual strengths and weaknesses of each protocol. This provides a path to interfacing separate protocols while being mindful of their respective limitations.

History

Received: 14 Jan 2022
Revised: 15 Apr 2022
Accepted: 03 Aug 2022
e-Available: 17 Aug 2022

Keywords

ITS-G5, Wi-Fi, WAVE, ITS security, Cybersecurity

Citation

Blazek, T., Ademaj, F., Marksteiner, S., Priller, P. et al., "Wireless Security in Vehicular Ad Hoc Networks: A Survey," *SAE Int. J. of CAV* 6(2):2023, doi:10.4271/12-06-02-0011.

ISSN: 2574-0741
e-ISSN: 2574-075X

1. Introduction

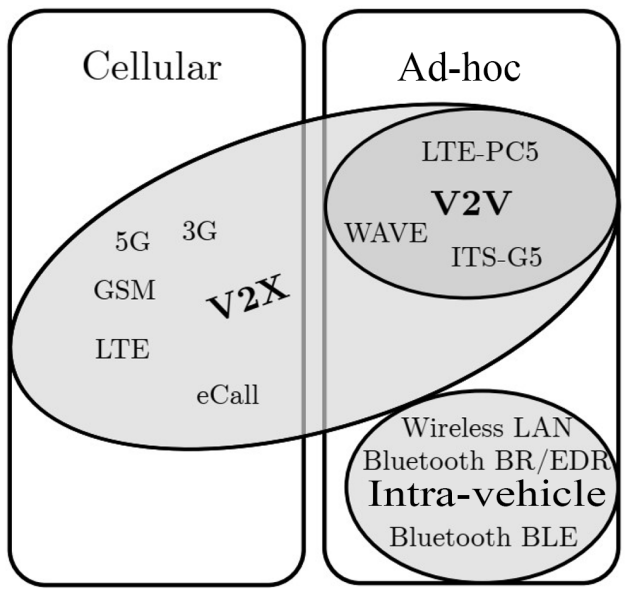
Vehicles, especially cars, are currently transitioning to Intelligent Transportation Systems (ITSs) and further Connected and Autonomous Vehicles, but there is no one clear communication protocol choice to enable this. Instead, we see a multitude of different communication standards that a car is expected to support. Within the vehicle, the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard Wireless Local Area Network (WLAN) hotspots and Bluetooth are provided for the convenience of the passengers. Such networks are referred to as intra-vehicle networks [1] and are not supposed to connect with other vehicles. Inter-vehicle networks, on the other hand, establish communications either between vehicles (Vehicle-to-Vehicle [V2V]) or between vehicles and infrastructure (Vehicle-to-Infrastructure [V2I]). Considering V2I, many cars support Long-Term Evolution (LTE) to access new data and program updates from the manufacturer (over-the-air, or OTA updates), as well as general data communications for passengers. In these networks, the backhaul infrastructure acts as a server and controls the network [2].

V2V communications are largely envisioned for road safety applications that do not want to rely on the present infrastructure. Instead, the standards provide features that allow for direct communications. Here, two competing standardization efforts attempt to provide these services. On the one hand, the IEEE provides an 802.11 version, often referred to as 802.11p, specifically for V2V communications. The Third-Generation Partnership Program (3GPP) introduced a Vehicle-to-Everything (V2X) version of LTE. Based on the Physical Layer (PHY) and Medium Access Control (MAC) of 802.11p, the European Telecommunications Standards Institute (ETSI) introduces the upper layers in Intelligent Transportation Systems at 5 Gigahertz (ITS-G5), and the IEEE defines IEEE 1609 Wireless Access in Vehicular Environments (WAVE).

The 3GPP, which standardizes LTE, also introduced a V2V ad hoc mode as part of Cellular-V2X (C-V2X), in Release 14. This mode, referred to as LTE mode 4 or LTE-PC5, provides a different PHY and MAC, but is intended as a drop-in replacement for 802.11p. Additionally, the eCall interface is a system that can issue automated emergency calls based on a GPRS (General Packet Radio Service) link. Almost every car is equipped with a Bluetooth (and maybe, additionally, a WLAN) interface for user interaction, and many cars have wireless systems for reading sensors, as well as for the key unlock. Figure 1 displays an overview of different wireless standards and their categorization in the context of this study. This extreme heterogeneity causes problems from a security perspective. The systems have fundamentally different modes of operation, systems they connect to, and topologies. This leads to radically different security concepts. Furthermore, this substantial number of different standards poses a significant danger of not keeping all the modules patched, which poses a substantial risk of open security vulnerabilities. This has been recognized by regulators and certification bodies as well. The United Nations Economic Commission for Europe (UNECE) has issued a regulation (R.155, [3]) that every vehicle manufacturer has to install a Cybersecurity Management System (CSMS) and incorporate appropriate cybersecurity engineering into their development. This applies to the full jurisdiction area of the UNECE, including Europe, Japan, and Korea, from the mid of 2022 for new type approvals and mid-2024 for all new admission, effectively preventing anybody to sell vehicles on these markets if not compliant. Such a CSMS is, among others, defined in the International Standard ISO 21434 [4] and mandates to identify and keep track of security issues, evaluate their risk, and implement proper mitigation strategies (as well as documenting the effectiveness of the latter) through the automotive development life cycle. It is therefore particularly crucial to be aware of outside interfaces that allow for access to potentially critical systems from the outside via the in-vehicle network. The most exposure is being introduced by wireless interfaces because of the lack of a physical barrier to secure the system. An especially critical type of network topology is the ad hoc network. In such a network, the car itself is the final arbiter of trust and cannot rely on an access network to ensure the trust of the communication participants. This article aims to summarize relevant ad hoc standards for vehicular communication and provide insight into their security features and weaknesses.

In Section 2, we address the types of attacks that are to be expected in an ad hoc network, as well as the security concepts we want to consider. In order to go into detail later, we describe the characteristics of the two 802.11p-based protocols, as well as LTE-PC5 and Bluetooth in Section 3. Details on the security (features as well as known attacks) of the protocols mentioned above are provided in Section 4. Section 5

FIGURE 1 Deployed technologies in vehicles and their intended communication target.



discusses the improvements, and Section 6 concludes this article.

2. Threat, Vulnerability, and Risk Analysis

Ad hoc communications have in common that the security aspects of any communication have to be governed by the communicating end nodes and cannot be supervised by a core network or central server. This can act as a direct attack vector on the computer systems of cars. This already poses a critical functional safety risk for these cyberphysical systems, and with increased autonomous driving, we expect this risk to increase further. Therefore, common security concepts are typically discussed and to which these networks must adhere. Furthermore, because of the ad hoc topology, different protocols share behavior with respect to common attack types. Hence, in this section, we summarize both the typical nomenclature and security concepts applied, as well as typical attack types and sources for specific attacks.

2.1. Security Concepts

Vehicular Ad Hoc Network (VANET) security principles have been extensively analyzed. The base requirements for secure communications are typically outlined in the CIA triad: confidentiality, integrity, and authenticity. Vehicular communications, however, must adhere to additional side constraints while fulfilling the CIA triad. These boundary conditions are often summarized as [11, 16]

1. Privacy
2. Data verification
3. Authentication
4. Availability
5. Non-repudiation
6. Real-time constraint

The first three points correspond to the classic CIA triad while points 4-6 consider safety and legal implications, respectively. Owing to safety implications and ad hoc nature, vehicular communications must be designed to ensure high local availability. In the case of road obstructions, warnings have a limited geographical relevance, but within that area, the message must be transmitted and received. Non-repudiation means that the originator of an action (e.g., sending messages) cannot be plausibly denied (e.g., it is not plausible that an advisory has sent a message that is signed using a securely distributed and stored private key). Finally, the value of safety communications is bound to their timeliness; thus, real-time constraints play a key role. This list largely mirrors the commonly used STRIDE threat model (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) introduced by Microsoft [17].

2.2. Attack Types

Multiple papers have proposed taxonomies for attacks found in vehicular communications [10, 18, 19]. In Table 1 we present an overview of the most prominent attacks grouped into attack types. We now explain these types and how they pertain to VANET communications.

2.2.1. Routing-Based Attacks A malicious node in the routing process can perform a variety of attacks on packets before it forwards them to a network. However, the highly dynamic nature of VANETs limits the impact of attack possibilities. Many crucial communications are one-hop broadcasts. Furthermore, a network cannot guarantee to have stable multihop connections for prolonged periods. Overall, V2X communications see few critical multihop use cases, and intravehicle communications do not. Hence, attacking routing is of limited interest. However, owing to ad hoc routing protocols, it is, in principle, easily done.

2.2.2. Denial of Service Denial-of-service attacks are among the easiest attacks to conduct and unfortunately, in the VANET setting, potentially highly effective. Due to the real-time requirements of safety communications, simple denial of service can have deeply damaging effects.

2.2.3. Impersonation Impersonating another vehicle is potentially an extremely dangerous attack. Vehicles communicate critical information such as position and speed, as well as emergency maneuver information. During a successful impersonation attack, a vehicle can be tricked into performing emergency maneuvers, which can have real-world consequences. However, impersonation attacks are difficult to conduct owing to the VANET system that incorporates strong authenticity measures.

2.2.4. Data Manipulation Data manipulation attacks fall under the same point of view as impersonation attacks. The integrity of the data has a uniquely high importance, and

TABLE 1 Types of attacks relevant to VANET communications.

Attack types	Example attacks
Routing-based attacks	Wormhole, Blackhole, Greyhole, Isolation attacks [5, 6]
Denial of Service	Message exhaustion, Message flooding, Jamming [7, 8]
Impersonation	Replay attacks, Source spoofing, Masquerade [9]
Data manipulation	Data injection, False information dissemination, Location spoofing, Ranging manipulation [10, 11]
GPS attacks	GPS jamming, GPS spoofing [12]
Reputation tampering	Sybil attacks [13], Message distortion [14]
Passive attacks	Eavesdropping [15]
Active attacks	Attacks breaking a cipher or hash algorithm

any attack that can violate the integrity is extremely dangerous. Conversely, owing to the employed integrity measures, it is also difficult to conduct such events.

2.2.5. Global Positioning System Attacks The Global Positioning System (GPS) is an essential component of cars and is also an integral part of VANET communication. Spoofing or jamming the GPS signal is a dangerous prospect and has been studied extensively [12]. Here, additional systems must be used to validate the GPS information as the system itself is currently not tamper-proof. Typically, sensors and VANET communication are used to identify the veracity of the GPS data [20, 21].

2.2.6. Reputation Tampering Ad hoc networks often rely on reputation concepts. Information from a node is disregarded if its reputation is extremely low. This is used to mitigate the fact that malicious nodes cannot be kept out of the system by a centralized authority. Tampering with the reputation of a node means that this node is likely to be disregarded. While tampering with the reputation can be problematic because it may be simple to conduct, the impact is limited. VANETs are designed with the expectation that communication will not always be possible; hence, not communicating is a problem with limited impact.

2.2.7. Passive Attacks Eavesdropping is not a major priority in V2X communications. Most packets are broadcast and are open to read. Intra-vehicle communications can be impacted and should be aware of eavesdropping. However, this requires a vehicle driving in proximity for a prolonged time, owing to the limited reach of intra-vehicle networks.

2.2.8. Cryptographic Attacks Most of the standardized cryptographic ciphers and hashing algorithms used in the discussed protocols are regarded as safe for today's state of the art [22], except for SAFER/SAFER+ (Secure And Fast Encryption Routine) in the older Bluetooth version (see Section 4.4.1). Some standardized curves used in Elliptic Curve Cryptography (ECC) have been repeatedly criticized for their opaque seed choice and some other suboptimal design decisions (this, however, applies to all standardized ECC curves) [23]. In addition, some curves (e.g., NIST and Brainpool) were numerously suspected to be compromised by a government agency through backdoors; however, there was no clear evidence that would withstand thorough analysis that this is actually the case [24].

3. Ad Hoc Communication Standards

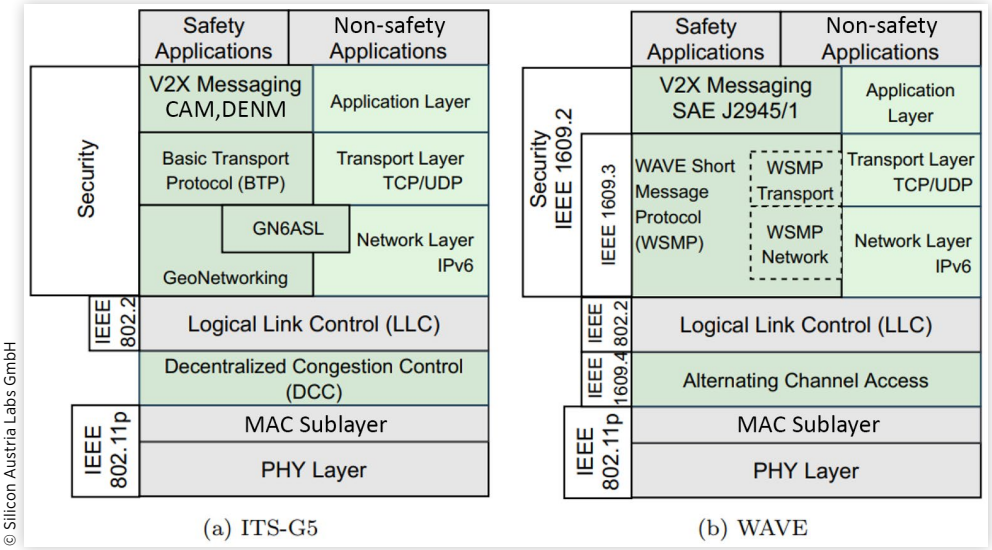
While ad hoc communication standards share some aspects in their nature, other aspects are extremely dependent on the chosen implementation, scope, and security measures of the given standard. To better present the resulting diversity in behavior, we will now give a brief overview of the relevant layers of the considered communication protocols. This allows better side-by-side comparison of the protocol stacks. Furthermore, it presents a compiled reference on where security is implemented in which protocol, and the systems with which it is integrated. We will present short descriptions of the PHY, which defines how bits are mapped to physical waveforms that are transmitted and received, and MAC, which controls when and how the communication medium is accessed. Furthermore, we give brief insights into the most relevant communication aspects and message formats for this review.

3.1. ITS-G5 and WAVE

The ITS-G5 and WAVE standards refer to a dedicated non-voice short-range communication between vehicles themselves, as well as vehicles and roadside infrastructure. The two main components are the onboard equipment installed on the dashboard of the vehicle and roadside equipment installed alongside the road. The two standards are issued by two different standardization bodies and have a common architecture mainly on the PHY and partly on the MAC layer while being different in the upper layers. We describe the main characteristics and emphasize the differences between the two standards.

3.1.1. ITS-G5 The ITS-G5 standard, developed by ETSI, is specified in [25]. It operates in the 5.9 GHz frequency band with 10 MHz channels. The PHY utilizes the half-clocked Orthogonal Frequency-Division Multiplexing (OFDM) multicarrier transmission scheme as outlined in [26] and uses the existing IEEE 802.11p standard. The data link layer consists of two sublayers: MAC and Logical Link Control (LLC). The MAC sublayer, which is responsible for scheduling, utilizes the existing IEEE 802.11p as indicated in Figure 2(a). As an extension to the MAC layer (upper MAC sublayer), the standard features the Decentralized Congestion Control (DCC) to dynamically adapt to the channel conditions, that is, by adjusting the transmit power, the sensitivity of the radio to determine whether a channel is considered idle or busy, the modulation data rate, etc. In ITS-G5, DCC support is mandatory and requires special functionalities on the MAC, network, and transport layers [25]. The LLC functionality is specified according to IEEE 802.2 [27]. The LLC header of 2 bytes has the same functionality as that of WAVE. It differs in the fact that it enables differentiation between Internet Protocol (IP) and GeoNetworking services. The GeoNetworking protocol is a routing protocol for multihop communication defined in the network layer that uses geographical position information for packet transport. It provides services to upper protocol entities, that is, the transport protocol, such as Basic Transport Protocol (BTP) and the GeoNetworking to IPv6 Adaptation Sub-Layer (GN6ASL), and is specified in more detail in [28]. In the facilities layer, corresponding to the session, information, and application layer of the Open Systems Interconnection (OSI) model, application-related

FIGURE 2 Protocol architecture of ITS-G5 and WAVE denoting the differences between the two standards.



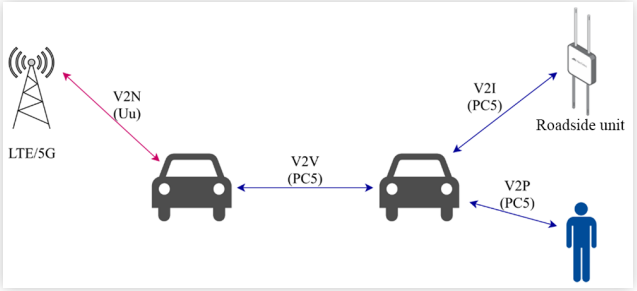
functionalities are defined such as cooperative awareness, static and interactive local hazard warnings, advertised services, and multicast services. For instance, ETSI defines the Cooperative Awareness Message (CAM) in ETSI EN 302 637-2 [29]. Via CAMs, a vehicle periodically reports critical vehicle safety state information and traffic efficiency by broadcasting it to any possible receiver. Another important message type is Distributed Environmental Notification Message (DENM), specified in ETSI EN 302 637-3 [30], which sends safety information in a specified geographical region. In contrast to a CAM, an application must trigger a DENM transmission. The security entity is specified in [31] and contains security functionalities related to the communication protocol stack. Such functionalities include firewall and intrusion management, authentication, authorization and profile management, and encryption and certificate management, among others.

3.1.2. WAVE Like ITS-G5, WAVE operates within the 5.9 GHz frequency band with 10 MHz channels and utilizes the half-clocked OFDM multi-carrier transmission scheme. Compared to IEEE 802.11a, which uses a full-clocked mode with 20 MHz bandwidth, the carrier spacing is reduced by half in 802.11p and the symbol length is doubled, thus making the signal more robust to fading and Doppler shifts that occur both more frequently and intensely in vehicular environments [32]. The PHY layer and MAC sublayer (lower MAC) are adopted from IEEE 802.11p. In addition to the MAC based on 802.11p, there is a MAC sublayer extension based on IEEE 1609.4, which defines a management extension for multi-channel operation, known as the Alternating Channel Access (ACA) method. In contrast to ITS-G5, which dynamically adapts to the channel conditions via the DCC mechanism, in WAVE the ACA divides the channel time into equal intervals alternating between the control and service channels. During the control channel interval, safety-related and system control data exchange occurs; whereas in the service channel interval, IP-based services are transmitted. The remaining part of OSI layer 2, LLC, is based on the IEEE 802.2 standard. In addition to default IP and Transmission Control Protocol (TCP)/User Datagram Protocol (UDP), the network and transport layer protocols incorporate the WAVE Short-Message Protocol (WSMP) defined in the IEEE standard 1609.3. WSMP is specifically designed for vehicular communication. The facilities layer is defined in SAE J2735 [33] whereas SAE J2945/1 [34] specifies the Basic Safety Message (BSM). The BSM can be seen as an equivalent to the CAM in ITS-G5. Security services are covered by IEEE 1609.2, defining secure message formats, processing, and methods to secure application messages.

3.2. LTE-PC5

The C-V2X communication, specified in 3GPP Release 14, supports two interfaces: the legacy LTE air interface also known as Uu and the ProSe Communication Reference Point 5 (PC5) also known as LTE mode 4. While the first mode is based on the conventional cellular communication interface, it can be used to establish V2X communications [35]. However, at least for establishing the connection, it relies on an eNodeB to assign resources [15]. The latter provides the possibility of a direct connection between two devices (V2V, V2I and Vehicle-to-Person [V2P]) via a sidelink, as shown in Figure 3. The LTE mode 4 communication on the PC5 interface operates on the 5.9 GHz frequency band regardless of the presence of a cellular network (both in-coverage and out-of-coverage area). It utilizes Single-Carrier Frequency-Division Multiple Access with 10 MHz and 20 MHz channels. Both PHY and MAC layer mechanisms follow the 3GPP standard with

FIGURE 3 V2X communication interfaces in the LTE/5G cellular network.



mechanisms such as transport blocks that carry data over Physical Sidelink Shared Channels and control information over Physical Sidelink Control Channel. In the network layer, LTE-PC5 employs IEEE 1609.3 and ETSI TC ITS [36]. For the facilities layer, LTE-PC5 allows full flexibility to utilize the mechanisms from either ETSI, SAE, or IEEE.

3.3. WLAN

The WLAN is a family of wireless network protocols based on the IEEE 802.11 family of standards [26] which operate in the unlicensed Industrial, Scientific, and Medical (ISM) spectrum of 2.4 GHz and 5 GHz. The WLAN encompasses various versions (e.g., IEEE 802.11a/b/g/n/ac/ax) with capabilities from lower to higher data rates and with various communication ranges indoors and outdoors. The IEEE 802.11 family employs Carrier-Sense Multiple Access with Collision Avoidance scheme before the transmission of each frame. The modulation scheme varies between protocol types, 802.11b employs Direct Sequence Spread Spectrum and 802.11a/g/n/ac uses OFDM. As the family of 802.11 continues to develop, with new protocols, the latest version of IEEE 802.11ax also known as Wi-Fi 6 is foreseen to be adopted in the automotive sector. A data market report from ABI Research forecasts that 70% of the Wi-Fi chipsets shipped into automotive applications will be Wi-Fi 6 by 2024 [37]. Wi-Fi 6 operates at 2.4 GHz and 5 GHz, and its extension Wi-Fi 6E operates in the 6 GHz range. It supports greater spectral efficiency than previous versions and allows for more simultaneous clients and faster access for the same number of clients. One of the main applications of Wi-Fi 6 in the automotive industry is in infotainment systems, especially as backseat infotainment systems are becoming more common across new vehicle models.

3.4. Bluetooth

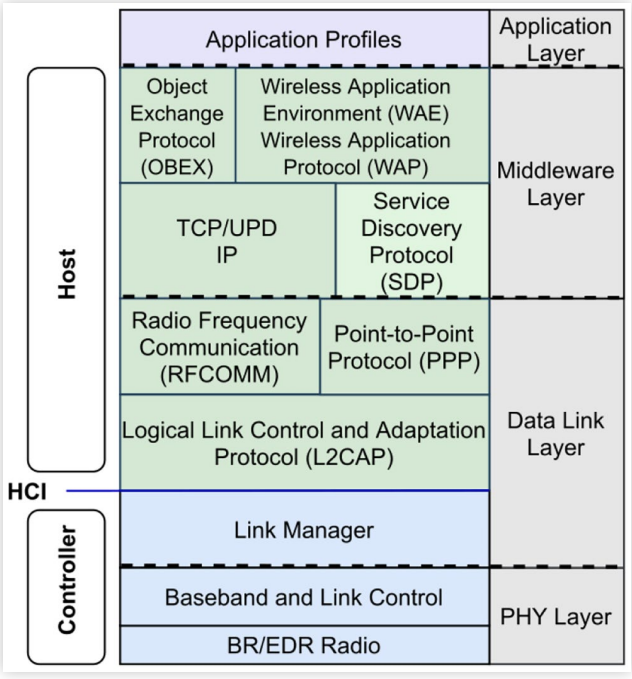
Bluetooth wireless technology is a short-range communication system operating in the unlicensed 2.4 GHz ISM band. The low-cost deployment, low power consumption, and robustness are among the key features that have made Bluetooth technology incredibly attractive for use in many applications in the automotive domain. The Bluetooth protocol stack is defined by the Bluetooth Special Interest Group (SIG) in the core specification [38]. The core specification defines two forms of Bluetooth wireless technologies: Basic Rate/Enhanced Data Rate (BR/EDR) and Bluetooth Low Energy (BLE). The BR provides a data rate of 721.2 kbps, and its extended version EDR reaches 2.1 Mbps. The BLE system includes features that enable low-energy consumption and can also support lower data rates than the BR/EDR, depending on the use case.

According to the core specification, the Bluetooth core system consists of a controller, host, and application profile. The controller component consists of the lower layers of the protocol stack (PHY and part of the Data Link Layer). The host component encompasses the core Bluetooth protocols (Bluetooth stack and the high-level layers of the Bluetooth architecture). The Host Controller Interface is responsible for inter-communications between the controller and host components.

3.4.1. Bluetooth BR/EDR

The architecture of the Bluetooth BR/EDR is shown in Figure 4. The PHY layer defines the requirements of the Bluetooth transceiver that utilizes the Frequency-Hopping Spread Spectrum (FHSS) technique. In total there are 79 Bluetooth channels with a 1 MHz bandwidth each. In the modulation technique, Bluetooth BR utilizes Gaussian Frequency-Shift Keying (GFSK) whereas EDR applies Differential Phase-Shift Keying (DPSK). The Baseband and Link Control sublayer enables the PHY radio link between different Bluetooth devices, where channel processing and timing are performed by the Baseband whereas the channel access control is managed by the Link Control part. In the Data Link Layer, the Link Manager sublayer is respon-

FIGURE 4 Protocol architecture of Bluetooth BR/EDR.

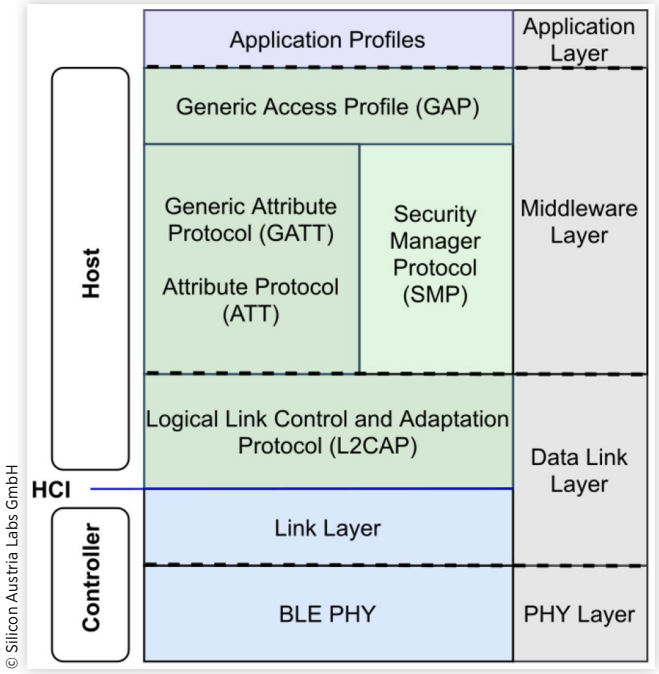


sible for the link setup and configuration. Here the security functions such as authentication and encryption are established. Further, the Logical Link Control and Adaptation Protocol (L2CAP) provides channel abstraction such as segmentation and reassembly and multiplexing/de-multiplexing of multiple channels over a shared logical link. This protocol ensures a compact structure of the lower layers adapting to higher-layer protocols and vice versa. In addition, Bluetooth BR/EDR uses Radio Frequency Communication (RFCOMM), which provides transport capabilities for higher layers that use a serial interface as a transport mechanism (it substitutes the RS-232 cable transmission). Apart from the core protocols, Bluetooth BR/EDR includes protocols adopted from other standards such as Point-to-Point Protocol (PPP) responsible for transporting IP datagrams over point-to-pint connections [39]. In the Middleware layer comprising network, transport, and session layer functions, the BR/EDR uses adopted protocols such as TCP, UDP, IP, and Service Discovery Protocol (SDP) (providing means for applications to discover which services are available and with what characteristics [38]). Another adopted protocol is Object Exchange (OBEX), which is a compact binary protocol enabling a wide range of devices to exchange data in a simple and spontaneous manner [40]. Furthermore, BR/EDR adopts the Wireless Application Environment (WAE) and Wireless Application Protocol (WAP) that provide functions such as remote control and data fetching and build application gateways that function as interfaces with other applications. The Application Profile is on top of the Bluetooth BR/EDR. The Bluetooth core specification [38] enables vendors to define proprietary profiles for use cases that are not defined by SIG.

3.4.2. Bluetooth BLE

The protocol architecture of Bluetooth BLE is shown in Figure 5. The BLE PHY operating frequency band is divided into 40 channels with a bandwidth of 2 MHz. Three channels are used as primary advertising channels, while 37 are general-purpose channels. Similar to Bluetooth BR, BLE utilizes the GFSK modulation and FHSS techniques. Various data rates can be supported depending on the version of the BLE. In the case of BLE version 5.1, this means coded transmission with 125 kbps or 500 kbps and uncoded transmission with 2 Mbps. Devices compliant with version 4.x support a data rate of 1 Mbps. In the Data Link Layer, the Link Layer interfaces directly with the BLE PHY and manages the link state of the BLE radio to define the role of a device as master, slave, advertiser, or scanner. The L2CAP, which is part of the host in the BLE stack, is responsible for channel abstraction and data encapsulation. In the Middleware layer, protocols are defined such as Security Manager Protocol (SMP), Attribute Protocol (ATT), Generic Attribute Protocol (GATT), and Generic Access Profile (GAP). The SMP implements security functions between devices, whereas the ATT provides a method to communicate small amounts of data over a fixed L2CAP channel as well as determine services and other capabilities of other devices. The GATT profile is built on top of the ATT and establishes common operations and a framework for the data transported and stored by the ATT.

FIGURE 5 Protocol architecture of Bluetooth BLE.



GATT defines two roles: server and client. GATT is used for profile service discovery in BLE devices and describes the hierarchy of services, characteristics, and attributes used in a server/client attribute [38]. The GAP profile represents the base functionality common to all Bluetooth devices such as modes and access procedures used by the transport layer and application profiles [38]. GAP services include device discovery, connection modes, security, authentication, association models, and service discovery. In the Application Profiles layer, similar to the Bluetooth BR/EDR, the Bluetooth core specification [38] enables vendors to define proprietary profiles for use cases that are not defined by SIG profiles.

4. Security Measures and Known Weaknesses

In this section, we consider how security issues are addressed by the standards presented in the previous section. Furthermore, we consider known weaknesses and exploits. We also want to point out that cars have an exceptionally long deployment time, and software and firmware upgrades are unfortunately not guaranteed, especially for older models. Hence, we will consider relevant exploits that may theoretically already be fixed as many cars will still use unpatched versions.

4.1. ITS-G5 and WAVE

In Europe, the ITS-G5 standard defines the security infrastructure [26]. However, the standard leaves certain questions

open, such as requirements on GPS accuracy and the chosen encryption. Here, the private Car-to-Car Communication Consortium (C2C-CC) provides the Basic Systems Profile [41], which consists of agreed-upon parameter sets that complement the ETSI standard. In the USA, the specification of 802.11-based systems was conducted by the IEEE 1609 standard family, also referred to as WAVE [42].

4.1.1. Security Features To account for the highly dynamic nature of the network and the lack of central authorities that moderate access, both ITS-G5 and IEEE WAVE refrain from employing security features at the MAC or PHY layer. Instead, basic communication features are unsecured, and security features are moved in their entirety to the application layer. The backbone of ITS-G5 and WAVE security features is built on a Public Key Infrastructure (PKI) [43, 44, 45]. This PKI is the building block for all privacy, data verification, and authentication issues. Hence, particular care must be taken to ensure that the PKI is implemented correctly and guarded against attacks. Owing to the extreme availability requirements, no checks are conducted on the PHY or MAC layer. Instead, authenticity and integrity are fully relayed to the application layer. This implies that non-reputation measures are important. Based on this asymmetric infrastructure, the algorithms of choice for authentication and encryption are Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Integrated Encryption Scheme (ECIES) [46]. In case symmetric channels are required, the standard supports Hash-based Message Authentication Code using the Secure Hash Algorithm (HMAC-SHA)-256 for authentication and Advanced Encryption Standard in Counter mode with Cipher Block Chaining Message Authentication Code (AES-CCM) mode for encryption. These are used, for example, in the authorization process before a public key can be announced to the PKI. However, AES-CCM is also used in multicast messages, where the symmetric key is communicated to all targets via ECIES encryption. Then multicast messages are transmitted using AES-CCM [46]. The security header and certificate formats of ITS-G5 are based on IEEE 1609.2 (and the .1 amendment) [47]. This standard supports the ECDSA on the NIST-P256 curve or the Brainpool-P256 and Brainpool-P384 curves as signature algorithms [48].

4.1.2. Known Attacks Currently, there are studies on simulating different attacks on ITS-G5 systems including jamming, replay, falsification, and congestion attacks [47]. A 2019 red team test found that an attacker was able to replay any type of message on a channel, which would enable faking traffic light signals, pedestrians' presence, speed limits, and signals from roadside units and other vehicles [50]. Moreover, studies demonstrated the successful application of Sybil attacks on 802.11p-based platooning settings [51].

4.2. LTE-PC5

4.2.1. Security Features LTE-PC5 is currently considered an alternative PHY/MAC for both WAVE and ITS-G5. As security features are defined purely at the application level, the security considerations are equivalent. In Release 14, it is declared for the pure V2V sidelink mode, termed PC5, that network-based security measures are not feasible, whereas application layer measures similar to WAVE or ITS-G5 satisfy the security requirements and are therefore out of the scope of that standard [52]. This is similarly explicated in [53], where the security and privacy protection for the PC5-based communication shall be defined by other Standards Development Organizations. Furthermore, [52] lists safety concept requirements without providing implementation details. In general, a 2019 survey paper found that the PC5 interface has fewer security services in place than 802.11p-based networks (e.g., no encryption prescribed) [54]. For a brief critique of these stipulations and their reasoning, see Section 5.3.

4.2.2. Known Attacks Owed to the similarities with WAVE and ITS-G5, the threats and possible attacks are similar. This includes fake nodes and false information, as well as jamming and replay attacks [55]. This is aggravated by providing fewer security services as stated above (e.g., the lack of encryption allows for eavesdropping attacks). This can only be prevented by application layer security measures, which offload attack protection from the standard and, thus, make the standard per se (i.e., without proprietary vendor measures on the application layer) insecure.

With Release 16 and the advent of 5G New Radio, the 5G standard changed the strategy and started to provide in-house implementation details for PC5 security that allow the use of the 5G encryption and integrity algorithms [56, 57].

4.3. WLAN

The WLAN is deployed in some cars as part of the In-Vehicle Infotainment System [58]. WLAN provides a variety of security protocols. Of these, open uses, no authentication, and Wired Equivalent Privacy and Wireless Protected Access (WPA) are considered unsafe to well-known attacks. WPA2 is currently the most widely used configuration [59], and WPA3 was released in 2018. This is supposed to update the wireless security protocols to modern standards. Since WPA2 was released in 2004 and older standards are not recommended, we will focus on WPA2 and WPA3. Both versions define enterprise and personal security options, but for the intra-car use case, we universally expect personal solutions.

4.3.1. Security Features WPA2 uses AES-CCM for both authentication and encryption. For key exchange, WPA2-personal operates based on a Preshared Key (PSK) which is known by anyone trying to connect to the network. As an alternative, Wi-Fi Protected Setup (WPS) provides an alternative key distribution similar to Bluetooth pairing that works either on a shared PIN or a push-button solution.

WPA3 replaced the PSK solution with Simultaneous Authentication of Equals (SAE). This enhancement addresses the weaknesses of the PSK implementation. Otherwise, WPA3-personal parameters do not change from their

WPA2-personal settings. However, it does impose stronger encryption in the enterprise configuration.

4.3.2. Known Attacks WPS is known to have a weak design inviting brute-force attacks, as demonstrated by Stefan Viehböck in 2011. It has since been recommended to be deactivated and is not recommended for use in WPA3 [60, 61].

The Key Reinstallation AttaCK (KRACK) allows to attack the four-way handshake to force nonce resets via key reinstallation, allowing the circumvention of the security provided by the nonce. FragAttacks allow the forging of encrypted frames based on weaknesses in the fragmentation/aggregation functionality WLAN [62]. PSKs that are too short are vulnerable to hash-comparison attacks [63]. Basing the pairing on a password also incurs all weaknesses typically associated with passwords: the default password may not be set device by device, allowing attackers to learn default passwords per model, and changed passwords often do not follow security recommendations [64].

In a vehicular setting, research is mostly ongoing, with some analysis of spoofing and jamming effects [65]. However, in 2017, WLAN was used as a vector to attack Tesla's CAN bus, proving a severe elevation of privilege exploit [66].

4.4. Bluetooth BR/EDR

Bluetooth has fundamentally different approaches to security compared to ITS-G5 and WAVE. The goal of Bluetooth is to primarily allow an easy point-to-point setup with limited network capabilities. The pairing relies on active user interaction to ensure that only legitimate devices are allowed unless another communication channel is already established. As this pairing has to work with different types of devices that have varying amounts of Input/Output capabilities, different connection types with different associated security features are defined.

4.4.1. Security Features As for cryptographic protection measures, Bluetooth versions up to 4.0 use the E0 cipher for encryption, which is not Federal Information Processing Standard approved [67] and also has a known attack [68]. Authentication occurs using the E1 cipher. Both ciphers are based on the SAFER/SAFER+. With version 4.1, the standard switched to the AES-CCM, which is an authenticated encryption scheme that is deemed to be secure [69], while the standalone authentication and integrity checking without encryption runs via an HMAC-SHA-256, which is now called secure connections.

More critically seen was, however, the pairing mechanism. This was also based on SAFER+ and yielded some practical attacks, which allow for determining the exchanged symmetric key (link key) that is protecting the logical Bluetooth channel [70]. Therefore, it has been replaced in version 2.1 with an elliptic curve Diffie-Hellman-Merkle key exchange on curve P-192; while beginning with 4.1 (secure connections), it switched to the P-256 curve [38]. The complete set used in secure connections is recommendable for near-term applications [69]. The SAFER+ is, however, used in the legacy mode for backward compatibility. This circumstance allows for executing version downgrade attacks (e.g., the BIAS attack as described below), which force the communicating parties to switch to a less secure negotiation method. The Bluetooth overall security, therefore, depends strongly on the type of pairing used and the Bluetooth version in use. Even within the versions, the build dates of devices are important because of the inability to update most Internet of Things (IoT) devices. Hence, particular care must be taken if devices connect to a car via Bluetooth in what privileges they gain in the process.

4.4.2. Known Attacks The mandated versatility of the pairing process opens the door to a multitude of attacks on the pairing mechanism and the resulting strength.

The KNOB Attack exploits a weakness in the allowed encryption key length [71]. Although this attack is difficult to conduct maliciously, it provoked an interesting reaction from the Bluetooth SIG. When Bluetooth 5.0 was released, all standards down to 4.2 were issued errata that fixed the KNOB attack. Even though this seems to be positive on the surface, it is problematic. Bluetooth is largely deployed in devices that will not receive updates. Therefore, patching protocol 4.2 gives the impression that 4.2 is secure, while most devices released with 4.2 are vulnerable. The BIAS attack acts to impersonate one node of a pairing (CVE-2020-10135) [72]. The pairing-key derivation is attacked in [73], called BLURtooth (CVE-2020-15802). One of the most infamous sets of attacks on Bluetooth over the last few years has been BlueBorne. This set allows for a variety of attacks including information disclosure, man-in-the-middle, and remote code execution. It works on Android, Apple Systems, Linux, and Windows and includes the following vulnerabilities: CVE-2017-0781, CVE-2017-0782, CVE-2017-0783, CVE-2017-0785, CVE-2017-8628, CVE-2017-14315, CVE-2017-1000250, CVE-2017-1000251 [74]. Another critical vulnerability, called BlueFrag (CVE-2020-0022), with similar effects was discovered in the Android Bluetooth stack in early 2020 [75]. Attacks targeting certain chipsets (CVE-2019-13916, CVE-2019-11516, CVE-2019-18614) used in a variety of popular mobile phones (e.g., Apple iPhones, Samsung Galaxy, and the Fitbit Ionic smartwatch) were discovered in 2019. One adjunct vulnerability (CVE-2019-15063) also affects the WLAN system, owing to the combination of the same chipset [76].

4.5. Bluetooth Low Energy

BLE security concepts follow those of BR/EDR. A point-to-point pairing is established through user interaction. However, while BLE is now part of the Bluetooth standard, it originated from a different protocol called Wibree, devised by Nokia in 2006. Therefore, it was not originally derived from Bluetooth. This allows BLE to avoid some design weaknesses that are inherent to the BR/EDR design. Hence, fewer open issues are known with regard to BLE.

4.5.1. Security Features This distinctive design results in a different choice of cryptographic protection measures: from the beginning BLE has been using AES-CCM as an encryption cipher and used it (as the CCM mode is an authenticated encryption mode) for authentication as well, instead of using a dedicated algorithm. This means that unencrypted traffic is also not authenticated and integrity checked (the NULL cipher is not defined for encryption in BLE). Prior to version 4.2, BLE also used a proprietary key exchange scheme, which was broken [77]. Therefore, it switched to an Elliptic Curve Diffie-Hellman Scheme. In addition, the basic issues with BR/EDR hold also for BLE. The security of BLE depends also on the pairing type and the build date of the devices.

4.5.2. Known Attacks Despite the similarities with BR/EDR, from the abovementioned weaknesses in the standard, only BLURtooth affects BLE. However, both BR/EDR and BLE are also affected by implementation weaknesses of the given standards, for example, CVE-2020-10134, CVE-2017-8628, CVE-2017-14315, CVE-2017-1000250, CVE-2017-1000251, and CVE-2018-5383.

4.6. Susceptibility to STRIDE

Table 2 shows an assessment of the analyzed standards susceptibility to the separate groups of threats covered in STRIDE. This subsection provides reasoning for this assessment.

4.6.1. Spoofing of Identity Bluetooth-based standards rely on pairing and bonding processes to establish an identity. Therefore, spoofing the identity is accomplished by impersonating a device in an established pairing. This is mostly dependent on the vulnerabilities of the authentication algorithm. Hence, we consider outdated standards to be highly endangered. For modern standards, this depends on the exact protocol version and the patch level. Thus, the likelihood of successful spoofing is low to medium. The inter-vehicle networks (ITS-G5, WAVE, PC5) base authenticity services on PKIs, which make spoofing exceedingly difficult when state-of-the-art methods (cryptographic algorithms, deployment methods, etc.) are used as the standards suggest.

4.6.2. Tampering Even though all discussed standards provide the possibility for multihop communications, the main use case for all of them is one-hop transmission, or even broadcast. In such a use case, tampering is not a major risk. In addition, all modern standards use state-of-the-art encryption and integrity algorithms. Outdated standards are considered to exhibit medium risk owing to their outdated algorithms.

4.6.3. Repudiation ITS-G5, WAVE, and LTE-PC5 are used to share sensitive roadside data, such as position and speed. This data is used again as input in a cyberphysical system and, as such, requires an elevated level of trust. Therefore, non-repudiation is of the highest importance. Even though this should be mitigated by the PKI and signing the communication, there is no guarantee the cryptographic signatures will be analyzed. Hence, we consider this an elevated risk. For Bluetooth (BT) and BLE, while the basic likelihood of successful repudiation is similar, the use case is ordinarily not system-critical inter-vehicle communications. Therefore, the risk is principally only medium, however, because of the relatively easy spoofing and tampering, which makes denying of communications very plausible for older versions, which again yields a high-risk rating.

4.6.4. Information Disclosure We consider the risk of disclosing information to be of medium severity for the use case. On the one hand, an ad hoc network must be designed around the concept of minimizing information disclosure threats. On the other hand, an information breach can be especially critical because of the sensitive nature of the involved data. BT less than 4.1 is considered to display a substantial risk as the encryption algorithm used, and more importantly, the vulnerable pairing is not considered state of the art, which makes the older BT versions prone to eavesdropping. The same applies to older BLE versions because of their broken key exchange scheme (see Subsections 4.4.1 and 4.5.1). The V2V standards work mostly with broadcast messages, which carry no hidden information, so eavesdropping is not of interest. However, they convey a considerable amount of data about the vehicles, and as such, we consider the disclosed information to be relevant enough to put the risk at medium.

TABLE 2 Susceptibility to the STRIDE model.

Protocol	Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
BT < 2.1	High	Medium	High	High	Low	Medium
BT < 4.1	Medium	Medium	High	High	Low	Medium
BT ≥ 4.1	Low to medium	Low	Medium	Medium	Low	Low to medium
BLE < 4.2	High	Medium	High	High	Low	Medium
BLE ≥ 4.2	Low to medium	Low	Medium	Medium	Low	Low to medium
WLAN	Low to medium	Low	Medium	High	Low	High
ITS-G5	Low	Low	High	Medium	High	Low
WAVE	Low	Low	High	Medium	High	Low
LTE-PC5	Low	Low	High	Medium	High	Low

4.6.5. Denial of Service In an ad hoc wireless setting, denial of service is most easily conducted by jamming the channel access. The inter-vehicle standards ITS-G5, WAVE, and LTE-PC5 are especially susceptible to this attack since their communication range is expected to extend over 100 m [78]. As the Bluetooth variants are predominantly used for in-vehicle usage with low transmit powers and shielding by the car, denial of service is of low impact.

4.6.6. Elevation of Privilege The elevation of privilege is of no large concern for ITS-G5, WAVE, and LTE-PC5, as the standards do not grant access but rather only exist for information exchange. The Bluetooth standards carry a higher risk. However, this risk is mitigated by the required Bluetooth handshake and limited communication range. Still, it is worth mentioning that there are a couple of attacks on different BT/BLE stack implementations that allow for privilege execution by executing a remote code (see Subsections 4.4.2 and 4.5.2).

5. Discussion

Vehicular communications over the past 15 years have demonstrated that we cannot expect one comprehensive standard to encompass all use cases. Instead, we will have to work with heterogeneous communication systems and the issues these entail. The most likely outcome is a state like the current one where one vehicle will be equipped with a multitude of different standards. All these standards have different concepts and partially rely on different security building blocks. Table 3 provides an overview of the cryptographic security measures of the discussed protocols.

Further, these standards may provide different security levels and have different goals, strengths, and weaknesses. Most importantly, due to the ever-increasing connectedness of the IoT, they will interact and exchange data. Therefore, we must envision vehicular communication systems as systems that are built of fundamentally heterogeneous networks. This requires three approaches to enable security and safety in such a setup:

1. Clear requirements and specifications of subsystem capabilities
2. Application layer security concepts that consider and abstract the limitations of the underlying subsystem
3. Security concepts still defined on the network layer

Only when combining those aspects can we expect the overall system to avoid risks. In the following section, we discuss each of these aspects.

5.1. Requirements and Specifications of Subsystem Capabilities

Any subsystem must be able to clearly report what security measures it provides and what requirements it must satisfy. For example, conventional Bluetooth is designed to only allow the pairing of authorized equipment. It does so by requiring either human interaction or a sidelink. Conversely, ITS-G5 and WAVE do not have such requirements, and they also do not distinguish between authorized and unauthorized users for connection establishment. When every subsystem accurately reports its capabilities and what it requires from cooperating protocols, the application layer may decide whether those protocols provide compatible security features and are able to interoperate. Of note here is that the strengths and weaknesses of protocols and their versions can be relied upon. Hence, backporting errata to older protocol versions, as done with the KNOB attack in Bluetooth 4.2, must be considered problematic. In IoT applications, we cannot expect devices to receive patches post manufacturing. Hence, a device can only be checked for

TABLE 3 Cryptographic protection measures per protocol.

Protocol	Authentication/integrity algorithm	Length	Encryption	Length	Replay protection	Key exchange
BT < 2.1	E1(SAFER+)	8+	E0(SAFER)	8+	Counter with nonce	E2 (SAFER+)
BT < 4.1	E1(SAFER+)	8+	E0(SAFER)	8+	Counter with nonce	P-192 ECDH HMAC-SHA-256
BT ≥ 4.1	HMAC-SHA-256	128	AES-CCM	128	Counter with nonce	P-256 ECDH HMAC-SHA-256
BLE < 4.2	AES-CCM	128	AES-CCM	128	Counter with nonce	Proprietary
BLE ≥ 4.2	AES-CCM	128	AES-CCM	128	Counter with nonce	P-256 ECDH
WLAN WPA2	AES-CCM	128	AES-CCM	128	Counter with nonce	HMAC-SHA1 with PSK or WPS
WLAN WPA3	AES-CCM	384	AES-CCM	128	Counter with nonce	HMAC-SHA1 with SAE
ITS-G5	ECDSA/HMAC-SHA-256	128	ECIES/AES-CCM	128	Counter with nonce	P-256 ECDH
WAVE	ECDSA/HMAC-SHA-256	128	ECIES/AES-CCM	128	Counter with nonce	P-256 ECDH
LTE-PC5	Declared to be out of scope by the standard, ITS-G5 or WAVE equivalent application security recommended					

standard compliance at manufacture, and the standard version must reflect this practical inability to update.

5.2. Application Layer Security Concepts

WAVE, ITS-G5, and LTE-PC5 provide a glimpse of how to address heterogeneity in networks. The key mechanisms for evaluating the security concepts are placed at the application layer. This layer may implement security measures independently of the underlying radio access, such as the PKI. For example, multiple publications have suggested that blockchain-based technologies can be leveraged here to ensure trust [79]. However, the decision is made, this layer can define both security measures that are completely agnostic of the radio access, as well as trust zones for various levels of associated risk. Then, zones can enable and disable communication standards depending on the risk attached to a given zone. For instance, infotainment systems may be lenient with the allowed communication protocols, while communications related to autonomous driving will be very restrictive in allowing communications.

5.3. Network Layer Security Concepts

Despite these points, there is reasoning for applying security services at the network layer (i.e., in the respective VANET protocol itself). If the most used V2X (i.e., LTE-PC5, WAVE, and ITS-G5) protocols impose authentication and integrity checking on the network layer, the impact on an enhanced overall security would be significant. In particular, the reasoning of LTE-PC5 to set security out of scope because the communication partners of a VANET are not known a priori dissents from widely proliferated Internet architectures where the setting is the same, but security is still imposed. A use case for security on the network layer is ensuring general authenticity, integrity, and non-repudiation (in the sense of transparency) for any ad hoc messages (e.g., CAMs and DENMs). ITS-G5 and WAVE describe a PKI that allows for cryptographic protection of such messages. If the respective signature keys are strictly bound to a vehicle (as described in the ITS-G5 standard), the sender of a critical message can be clearly identified (assuming an intact certificate chain), making it exceedingly difficult to issue fake messages if V2X communication partners only accept secure messages. If there were bogus messages sent from a legitimate device, they would be traceable. However, this would require some sort of authorization body to function as a higher certificate authority and vendors to function as subordinates issuing certificates to their own devices. Furthermore, as with any PKI, this requires secure key storage and certificate management (issuing, updating, revoking). The benefit would be that any communication is already secured, not having to rely on security to be implemented separately by different vendors on the application layer.

6. Conclusions

Vehicular communications are a highly vulnerable set of technologies because of their exceptionally long product life cycles, heterogeneous network topologies, and substantial risk involved with unauthorized access. In this study, we demonstrate the strengths and weaknesses of the currently deployed standards in vehicles. While technology is steadily progressing, it is unlikely that the number of deployed protocols will be reduced. Therefore, security concepts are required that can correctly adapt to this situation.

We hope that technologies such as 5G will be able to further provide modular security solutions that can be linked with ITS-G5 and WAVE, instead of purely competing solutions that lead to further proliferation. Similarly, at the application layer, trust concepts must be established that grant technologies power proportional to the security that can be provided. To facilitate this process, this article summarizes the currently deployed ad hoc network standards with their security-relevant features. We especially focused on the currently known exploits and systematic strengths and weaknesses of the respective standards.

Contact Information

Thomas Blazek
Scientist
Silicon Austria Labs GmbH
Science Park 4 Altenberger Straße 66c
A 4040 Linz, Austria
M: +43 664 9639434
Thomas.Blazek@silicon-austria.com

References

1. Tuohy, S., Glavin, M., Hughes, C., Jones, E. et al., "Intra-Vehicle Networks: A Review," *IEEE Trans. Intell. Transp. Syst.* 16, no. 2 (2015): 534-545, doi:10.1109/TITS.2014.2320605.
2. Lai, C., Lu, R., Zheng, D., and Shen, X., "Security and Privacy Challenges in 5G-Enabled Vehicular Networks," *IEEE Netw.* 34, no. 2 (2020): 37-45, doi:10.1109/MNET.001.1900220.
3. United Nations Economic and Social Council—Economic Commission for Europe, "UN Regulation on Uniform Provisions Concerning the Approval of Vehicles With Regard to Cyber Security and of Their Cybersecurity Management Systems," ECE/TRANS/WP.29/2020/79, Brussels, 2020.
4. International Organization for Standardization and Society of Automotive Engineers, "Road Vehicles—Cybersecurity Engineering," ISO/SAE Standard 21434, 2020.
5. Safi, S.M., Movaghar, A., and Mohammadizadeh, M., "A Novel Approach for Avoiding Wormhole Attacks in

VANET," in *2009 Second International Workshop on Computer Science and Engineering*, Qingdao, China, October 2009, vol. 2, 160-165, doi:10.1109/WCSE.2009.787.

6. Grimaldo, J. and Martí, R., "Performance Comparison of Routing Protocols in VANETs under Black Hole Attack in Panama City," in *2018 International Conference on Electronics, Communications and Computers (CONIELECOMP)*, Cholula, Mexico, February 2018, 126-132, doi:10.1109/CONIELECOMP.2018.8327187.
7. Puñal, O., Aguiar, A., and Gross, J., "In VANETs We Trust? Characterizing RF Jamming in Vehicular Networks," in *Proceedings of the Ninth ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications*, New York, 2012, 83-92, doi:10.1145/2307888.2307903.
8. Azogu, I.K., Ferreira, M.T., Larcom, J.A., and Liu, H., "A New Anti-jamming Strategy for VANET Metrics-Directed Security Defense," in *2013 IEEE Globecom Workshops (GC Wkshps)*, Atlanta, GA, December 2013, 1344-1349, doi:10.1109/GLOCOMW.2013.6825181.
9. Hasrouny, H., Samhat, A.E., Bassil, C., and Laouiti, A., "VANet Security Challenges and Solutions: A Survey," *Veh. Commun.* 7 (2017): 7-20, doi:10.1016/j.vehcom.2017.01.002.
10. Ratasuk, R., Prasad, A., Li, Z., Ghosh, A. et al., "Recent Advancements in M2M Communications in 4G Networks and Evolution towards 5G," in *2015 18th International Conference on Intelligence in Next Generation Networks*, Paris, France, 2015, 52-57, doi:10.1109/ICIN.2015.7073806.
11. Al-kahtani, M.S., "Survey on Security Attacks in Vehicular Ad Hoc Networks (VANETs)," in *2012 6th International Conference on Signal Processing and Communication Systems*, December 2012, 1-9, doi:10.1109/ICSPCS.2012.6507953.
12. Bittl, S., Gonzalez, A.A., Myrtus, M., Beckmann, H. et al., "Emerging Attacks on VANET Security Based on GPS Time Spoofing," in *2015 IEEE Conference on Communications and Network Security (CNS)*, Florence, Italy, September 2015, 344-352, doi:10.1109/CNS.2015.7346845.
13. Iwendi, C., Uddin, M., Ansere, J.A., Nkurunziza, P. et al., "On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique," *IEEE Access* 6 (2018): 47258-47267, doi:10.1109/ACCESS.2018.2864111.
14. Emara, K., "Safety-Aware Location Privacy in VANET: Evaluation and Comparison," *IEEE Trans. Veh. Technol.* 66, no. 12 (2017): 10718-10731, doi:10.1109/TVT.2017.2736885.
15. Engoulou, R.G., Bellaïche, M., Pierre, S., and Quintero, A., "VANET Security Surveys," *Comput. Commun.* 44 (2014): 1-13, doi:10.1016/j.comcom.2014.02.020.
16. Raya, M. and Hubaux, J.-P., "The Security of Vehicular Ad Hoc Networks," *SASN '05: Proceedings of the 3rd ACM Workshop on Security of ad hoc and Sensor Networks, November*, (2005): 11-21, https://doi.org/10.1145/1102219.1102223.
17. Kohnfelder, L. and Garg, P., "The Threats to Our Products," vol. 33, Microsoft Interface Microsoft Corp., 1999.
18. Thing, V.L.L. and Wu, J., "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Chengdu, China, December 2016, 164-170, doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.
19. Loukas, G., Karapistoli, E., Panaousis, E., Sarigiannidis, P. et al., "A Taxonomy and Survey of Cyber-Physical Intrusion Detection Approaches for Vehicles," *Ad Hoc Netw.* 84 (2019): 124-147, doi:10.1016/j.adhoc.2018.10.002.
20. Lim, K., Tuladhar, K.M., and Kim, H., "Detecting Location Spoofing Using ADAS Sensors in VANETs," in *2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Las Vegas, NV, January 2019, 1-4, doi:10.1109/CCNC.2019.8651763.
21. Milaat, F.A. and Liu, H., "Decentralized Detection of GPS Spoofing in Vehicular Ad Hoc Networks," *IEEE Commun. Lett.* 22, no. 6 (2018): 1256-1259, doi:10.1109/LCOMM.2018.2814983.
22. Barker, E. and Roginsky, A., "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths (Revision 1)," SP 800-131A, National Institute of Standards and Technology, 2015.
23. Bernstein, D.J. and Lange, T., "SafeCurves: Choosing Safe Curves for Elliptic-Curve Cryptography," 2017, accessed 19 August 2022, https://safecurves.cr.yp.to.
24. Koblitz, N. and Menezes, A., "A Riddle Wrapped in an Enigma," *IEEE Secur. Priv.* 14, no. 6 (2016): 34-42, doi:10.1109/MSP.2016.120.
25. European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); ITS-G5 Access Layer Specification for Intelligent Transport Systems Operating in the 5 GHz Frequency Band," European Standard EN 302 663 v1.3.1, 2020.
26. Institute of Electrical and Electronical Engineers, "Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Standard 802.11-2016, 2020.
27. Institute of Electrical and Electronics Engineers, International Organization for Standardization, and International Electrical Commission, "Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 2: Logical Link Control," IEEE/ISO/IEC Standard 8802-2-1998, Institute of Electrical and Electronical Engineers, 2009.
28. European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture," Technical Specification 102 636 v1.1.1, 2020.
29. European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," European Standard EN 302 637-2 v1.3.2, 2014.

30. European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specification of Decentralized Environmental Notification Basic Service," European Standard EN 302 637-3 v1.2.1, 2014.
31. European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Communications Architecture," European Standard EN 302 665 v1.1.1, 2010.
32. Mecklenbräuker, C.F. et al., "Vehicular Channel Characterization and Its Implications for Wireless System Design and Performance," *Proc. IEEE* 99, no. 7 (2011): 1189-1212, doi:10.1109/JPROC.2010.2101990.
33. Society of Automotive Engineers, "Dedicated Short Range Communications (DSRC) Message Set Dictionary," SAE Standard J2735, 2009.
34. Society of Automotive Engineers, "On-Board System Requirements for V2V Safety Communications," SAE Standard J2945/1, 2016.
35. Yang, M.J., Lim, S.Y., Park, H.J., and Park, N.H., "Solving the Data Overload: Device-to-Device Bearer Control Architecture for Cellular Data Offloading," *IEEE Veh. Technol. Mag.* 8, no. 1 (2013): 31-39.
36. European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocols," European Standard EN 302 636-5-1 v2.2.0, 2019.
37. ABI Research, "Wireless Connectivity Technology Segmentation and Addressable Markets," MD-WCMT-186, ABI Research, 2021.
38. Bluetooth SIG, "Bluetooth Specification," Core Specification v5.2, Bluetooth SIG, 2019.
39. Simpson, W. (Ed.), "The Point-to-Point Protocol (PPP)," RFC 1661, RFC Editor/Internet Engineering Task Force, 1994.
40. Infrared Data Association (IrDA), "IrDA Object Exchange Protocol OBEX," Core Specification v1.3, Infrared Data Association (IrDA), 2003.
41. C.-2-C. C. Consortium and Others, "C2C-CC Basic System Profile," Rel, 2017.
42. IEEE Vehicular Technology Society, "IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages," 2013.
43. Monteuuis, J.P. et al., "Securing PKI Requests for C-ITS Systems," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, Vancouver, BC, Canada, July 2017, 1-8, doi:10.1109/ICCCN.2017.8038492.
44. Fernandes, B., Rufino, J., Alam, M., and Ferreira, J., "Implementation and Analysis of IEEE and ETSI Security Standards for Vehicular Communications," *Mob. Netw. Appl.* 23, no. 3 (2018): 469-478, doi:10.1007/s11036-018-1019-x.
45. Festag, A., "Cooperative Intelligent Transport Systems Standards in Europe," *IEEE Commun Mag* 52, no. 12 (2014): 166-172, doi:10.1109/MCOM.2014.6979970.
46. European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," Technical Specification 102 941, 2012.
47. European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats," Technical Specification 103 097, 2017.
48. Institute of Electrical and Electronical Engineers, "Wireless Access in Vehicular Environments (WAVE)-Certificate Management Interfaces for End Entities," IEEE Standard 1609.2.1, 2020.
49. Cassou-Mounat, J., Labiod, H., and Khatoun, R., "Simulation of Cyberattacks in ITS-G5 Systems," in *Communication Technologies for Vehicles*, Cham, 2020, 3-14.
50. Di Massa, V. and Foni, S., "Improving ITS-G5 Cybersecurity Features Starting from Hacking IEEE 802.11p V2X Communications through Low-Cost SDR Devices," in *Electronic Components and Systems for Automotive Applications*, Cham, 2019, 275-284.
51. Boeira, F., Barcellos, M.P., de Freitas, E.P., Vinel, A. et al., "On the Impact of Sybil Attacks in Cooperative Driving Scenarios," in *2017 IFIP Networking Conference (IFIP Networking) and Workshops*, Stockholm, Sweden, 2017, 1-2, doi:10.23919/IFIPNetworking.2017.8264890.
52. European Telecommunications Standards Institute, "LTE; 5G; Security Aspect for LTE Support of Vehicle-to-Everything (V2X) Services," Technical Specification 133 185, 2017.
53. European Telecommunications Standards Institute, "Universal Mobile Telecommunications System (UMTS); LTE; Architecture Enhancements for V2X Services," Technical Specification 123 285, 2012.
54. Alnasser, A., Sun, H., and Jiang, J., "Cyber Security Challenges and Solutions for V2X Communications: A Survey," *Comput. Netw.* 151 (2019): 52-67, doi:10.1016/j.comnet.2018.12.018.
55. Marojevic, V., "C-v2x Security Requirements and Procedures: Survey and Research Directions," 2018.
56. European Telecommunications Standards Institute, "LTE; 5G; Security Aspects of 3GPP Support for Advanced Vehicle-to-Everything (V2X) Services," Technical Specification 133 536, 2020.
57. European Telecommunications Standards Institute, "5G; Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services," Technical Specification 133 287, 2020.
58. Luo, Q. and Liu, J., "Wireless Telematics Systems in Emerging Intelligent and Connected Vehicles: Threats and Solutions," *IEEE Wirel. Commun.* 25, no. 6 (2018): 113-119, doi:10.1109/MWC.2018.1700364.
59. Dobrilovic, D., Stojanov, Z., Jäger, S., and Rajnai, Z., "A Method for Comparing and Analyzing Wireless Security Situations in Two Capital Cities," *Acta Polytech. Hung.* 13, no. 6 (2016): 67-86.

60. Zisiadis, D., Kopsidas, S., Varalis, A., and Tassiulas, L., "Enhancing WPS Security," in *2012 IFIP Wireless Days*, Ireland, 2012, 1-3, doi:10.1109/WD.2012.6402836.

61. Viehböck, S., "Brute Forcing Wi-Fi Protected Setup," Wi-Fi Prot. Setup, vol. 9, 2011.

62. Vanhoef, M., "Fragment and Forge: Breaking Wi-Fi through Frame Aggregation and Fragmentation," 2021.

63. Berghel, H. and Uecker, J., "WiFi Attack Vectors," *Commun. ACM* 48, no. 8 (2005): 21-28, doi:10.1145/1076211.1076229.

64. Van Heerden, R.P. and Vorster, J., "Statistical Analysis of Large Passwords Lists, Used to Optimize Brute Force Attacks," 2009.

65. El-Rewini, Z., Sadatsharan, K., Selvaraj, D.F., Plathottam, S.J. et al., "Cybersecurity Challenges in Vehicular Communications," *Veh. Commun.* 23 (2020): 100214, doi:https://doi.org/10.1016/j.vehcom.2019.100214.

66. Nie, S., Liu, L., and Du, Y., "Free-Fall: Hacking Tesla from Wireless to Can Bus," *Brief. Black Hat USA* 25 (2017): 1-16.

67. Padgette, J. et al., "Guide to Bluetooth Security (Revision 2)," SP 800-121, National Institute of Standards and Technology, 2017.

68. Lu, Y., Meier, W., and Vaudenay, S., "The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption," in *Advances in Cryptology—CRYPTO 2005*, Berlin, Heidelberg, 2005, 97-117.

69. Smart, N.P. et al., "Algorithms, Key Sizes and Parameters Report—2014," TP-05-14-084-EN-N, European Union Agency for Network and Information Security, 2014, accessed 19 August 2022, https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014.

70. Jakobsson, M. and Wetzel, S., "Security Weaknesses in Bluetooth," in *Topics in Cryptology—CT-RSA 2001*, Berlin/Heidelberg, 2001, 176-191.

71. Antonioli, D., Tippenhauer, N.O., and Rasmussen, K.B., "The KNOB Is Broken: Exploiting Low Entropy in the Encryption Key Negotiation of Bluetooth BR/EDR," in *28th USENIX Security Symposium (USENIX Security 19)*, Santa Clara, CA, August 2019, 1047-1061.

72. Antonioli, D., Tippenhauer, N.O., and Rasmussen, K., "BIAS: Bluetooth Impersonation AttackS," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, New York, 2020, 549-562.

73. Antonioli, D., Tippenhauer, N.O., Rasmussen, K., and Payer, M., "BLURtooth: Exploiting Cross-Transport Key Derivation in Bluetooth Classic and Bluetooth Low Energy," 2020.

74. Seri, B. and Vishnepolsky, G., "Blueborne—The Dangers of Bluetooth Implementations: Unveiling Zero Day Vulnerabilities and Security Flaws in Modern Bluetooth Stacks," Armis Inc., 2017.

75. Ruge, J., "CVE-2020-0022 an Android 8.0-9.0 Bluetooth Zero-Click RCE—BlueFrag," 2020, accessed 19 August 2022, https://insinuator.net/2020/04/cve-2020-0022-an-android-8-0-9-0-bluetooth-zero-click-rce-bluefrag/.

76. Ruge, J., Classen, J., Gringoli, F., and Hollick, M., "Frankenstein: Advanced Wireless Fuzzing to Exploit New Bluetooth Escalation Targets," in *29th USENIX Security Symposium (USENIX Security 20)*, Berkeley, CA, August 2020, 19-36, https://www.usenix.org/conference/usenixsecurity20/presentation/ruge.

77. Ryan, M., "Bluetooth: With Low Energy Comes Low Security," Washington, DC, August 2013, accessed 19 August 2022, https://www.usenix.org/conference/woot13/workshop-program/presentation/ryan.

78. Cecchini, G., Bazzi, A., Masini, B.M., and Zanella, A., "Performance Comparison between IEEE 802.11p and LTE-V2V In-Coverage and Out-of-Coverage for Cooperative Awareness," in *2017 IEEE Vehicular Networking Conference (VNC)*, Torino, Italy, 2017, 109-114, doi:10.1109/VNC.2017.8275637.

79. Didouh, A., Lopez, A.B., El Hillali, Y., Rivenq, A. et al., "Eve, You Shall Not Get Access! A Cyber-Physical Blockchain Architecture for Electronic Toll Collection Security," in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, Rhodes, Greece, 2020, 1-7.