Advances in Engineering Innovation Vol.16 Issue 2 EWA Publishing
Available Online: 17 March 2025 DOI: 10.54254/2977-3903/2025.21619

Automotive DoIP Cybersecurity analysis

Ning Xu[1], Feng Luo[1]*

[1]School of Automotive Studies, Tongji University, Shanghai, China

*Corresponding Author. Email: 1141701105@qq.com

Abstract. The paradigm shifts from a closed system to an always-on and fully connected vehicle leads to a largely increased risk to the automotive in-vehicle domain. Thereby, important automotive-specific protocols, which must be protected from a security point of view. This paper focuses on security aspects of Automotive Ethernet to address security challenges of the DoIP. First, it starts with an overview description of DoIP. Then, based on an exemplary in-vehicle network architecture, diagnostic via automotive ethernet by using DoIP are analyzed under security aspects with the help of Microsoft's threat model. We identify the assets and attack surface of DoIP End Nodes and DoIP data flow, and risk assessment is carried out for DoIP data flow. Finally, the DoIP Cybersecurity goals and risk treatments are proposed to tackle the identified DoIP attacks.

Keywords: Automotive Ethernet, DoIP, Cybersecurity

1. Introduction

Nowadays modern cars are desired to read out diagnostic data from anywhere via remote diagnostics and due to the ever-increasing number of ECUs and their increasing complexity, the software update packages are becoming larger, in some cases several gigabytes. This is no longer feasible with conventional bus systems such as Controller Area Network (CAN) [1]. Automotive Ethernet has been identified as a suitable solution to address the novel bandwidth requirements of automotive industry's application, such as on-board diagnostics over DoIP [2]. As one of the external interfaces, DoIP is inevitably prone to malicious attacks, which could lead to unauthorized software upgrades and data acquisition from vehicles. Cybersecurity and privacy issues have become increasingly paramount with the evolution of Intelligent Connected Vehicles (ICVs), Cyber-attacks have become more sophisticated and frequent [3]. Protection against external attacks is very important where DoIP is concerned.

2. Background

Diagnostics over Internet Protocol (DoIP) uses Ethernet as the physical and data link layer by the International Organization for Standardization (ISO) [4]. ISO 13400 [4] is the specification of the DoIP standard, which will foster the usage of the Internet Protocol (IP) for diagnosis and the usage of Automotive Ethernet as a replacement for CAN for reprogramming and diagnosing automotive applications [2]. Figure 1 illustrates an overview of vehicle diagnostic communication framework.

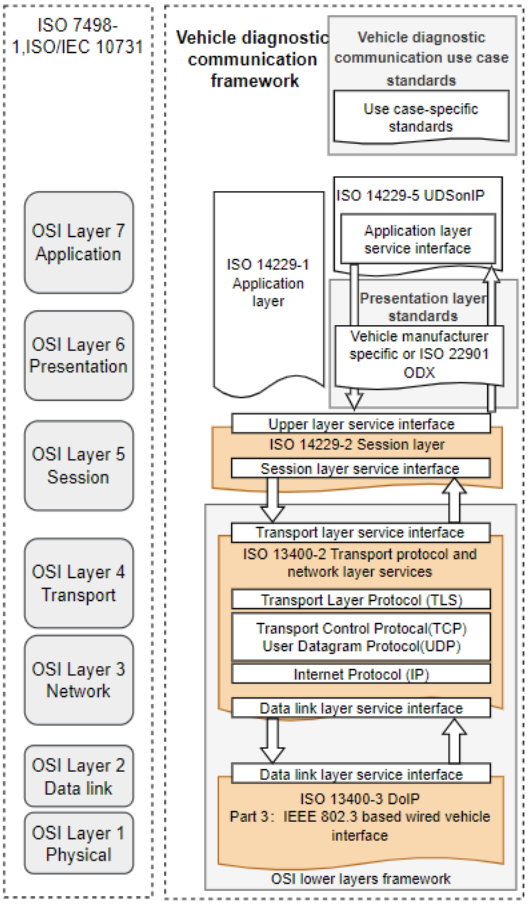

Figure 1. DoIP document reference according to OSI model

The protocols used by DoIP include DHCP, ARP, NDP, ICMP, IP, TCP and UDP. UDP is used for transmission of status or configuration information. TCP enables transmission of actual diagnostic packets via a fixed communication channel. The DoIP message structure is shown in Figure 2:

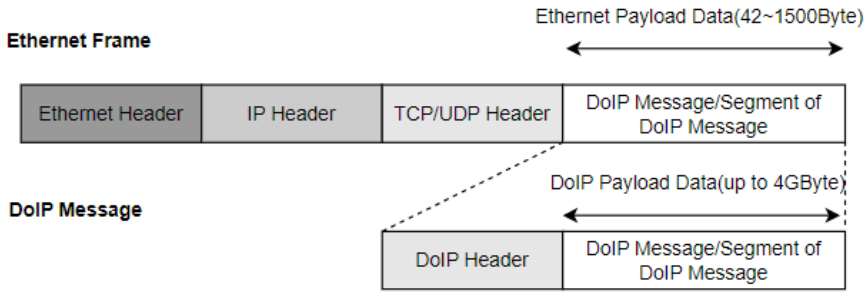

Figure 2. DoIP message structure

A DoIP server typically is a part of an ECU and it responds to requests by a client entity. The client typically is an off-board tester but can also be an on-board test device. A vehicle can have multiple DoIP entities and there are several possible network configurations that DoIP can work in. The options are (1) to directly connect external test equipment to a vehicle via dedicated physically separate wiring, (2) a network connection between one vehicle and one test device, (3) the connection of multiple vehicles and one tester, or (4) one vehicle connected to more than one tester [4].

In general, the DoIP communication sequence between a client and a server entity consists of three phases:

1) DoIP vehicle identification based on UDP,
2) DoIP routing activation based on TCP, and
3) DoIP diagnostic messages based on TCP.

3. Threat analysis of DoIP

3.1. Exemplary E/E architecture

The conclusion should elaborate on the key points of the research results, analyze the conclusions drawn from the results, and explain their significance for future research or practice. All sections such as patents, appendices, funding projects, and acknowledgments should be placed after the conclusion and before the references.

An exemplary in-vehicle E/E architecture as shown in Figure 3. The OBD-II is connected to the Central Gateway, which has an integrated switch for the isolation of the in-vehicle network and the out-vehicle network. The ADAS Domain Controller Unit (ADCU) is connected to the central gateway through Ethernet. DoIP use case are analyzed under security aspects based on this architecture.

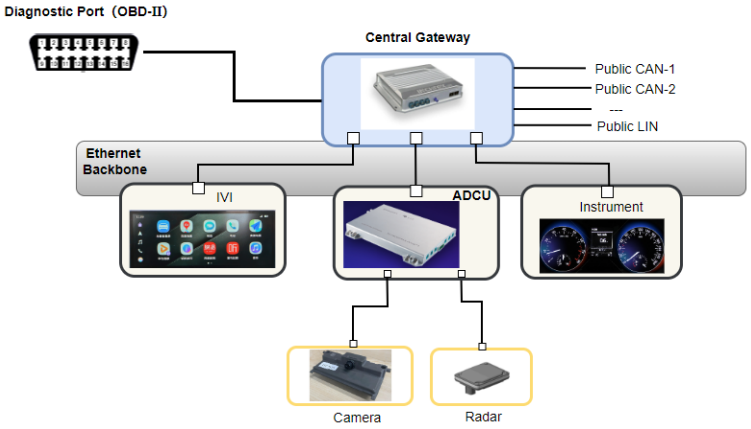

Figure 3. In-vehicle E/E architecture

Figure 4 shows the topology of the DoIP process with the help of Microsoft's threat model tool. An Ethernet Tester is connected via ODB-II to the automotive Ethernet network. First, the Ethernet tester has to obtain an IP address from the DoIP Central Gateway. This is done using DHCP. Communications then begin with vehicle identification and routing activation between the Tester and the Central Gateway. This is followed by subsequent diagnostic requests and responses among the Ethernet Tester, Central Gateway, ADCU.

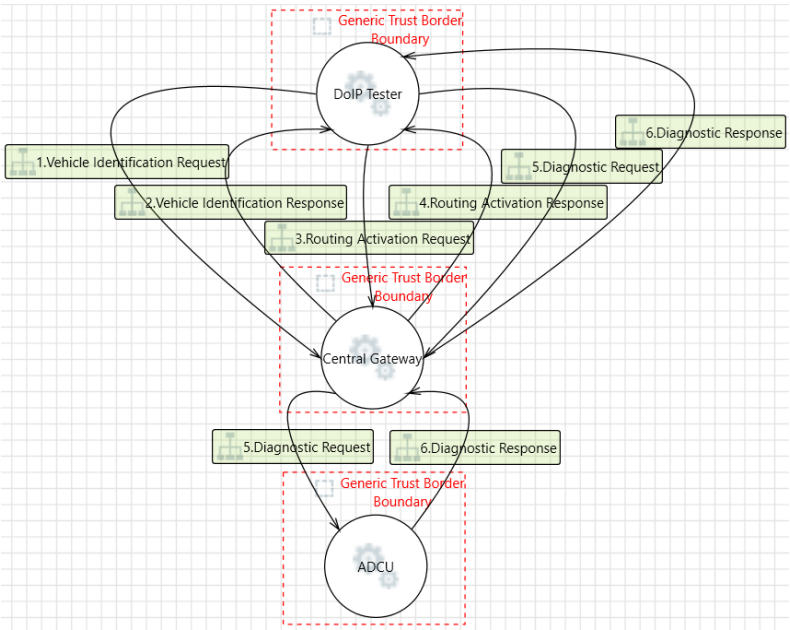

Figure 4. A DoIP topology

ADCU which can be accessed under two paradigms -Locked Switch and Transparent Switch. A Locked Switch state is usually the default state in Central Gateway. In this state, the switch enforces VLAN separation, which allows the tester to communicate only with the Central Gateway, the DoIP tester has no direct access to the ADCU. Once the tester is authenticated, the Central Gateway can reconfigure the switch to a Transparent Switch state. This removes Central Gateway as a bottleneck, allowing the tester direct access to the ADCU. In this case, Central Gateway is only acting as a switch between the Tester and the ADCU.

3.2. Assets identification

Based on DoIP topology, the assets and security attributes are identified. The result is shown in Table 1.

Table 1. DoIP topology assets

Assets			Security Attributes					
ID	Name	Description	Authenticity	Integrity	Non-repudiation	Confidentiality	Availability	Authorization
GW	Central Gateway	The Central Gateway coordinates communication between OBD-II and ADCU. The switch is embeded in it.	X	X	X	X	X	X
ADCU	ADAS Domain Control Unit	This module is responsible for the ADAS system	X	X	X	X	X	X
OBD-GW-DF	Vehicle Identification Request	OBD-II sends Vehicle Identification Request (UDP) to Central Gateway		X			X	
GW-OBD-DF	Vehicle Identification Response	Central Gateway responds with Vehicle Announcement Message (UDP), contains VIN, Central Gateway address etc.		X		X	X	
GW-ADCU-DF	Diagnostic Request/Response	Request/ Response for diagnostic data diagnostics functions		X		X	X	

3.3. Identification of threats and attacks

There are some attack surfaces among Automotive Ethernet among different OSI layers are identified with reference to the STRIDE [5] threat identification method. The various threat categories and attack surface for DoIP End Nodes (GW/ADCU) are analyzed in Table 2.

Table 2. Threat and attacks for DoIP end nodes

Security Attributes	Threat Model	Attack Surface
Authentication	Spoofing	-ARP-based MitM-Attack -ARP Cache Poisoning -IP Address Spoofing -MAC Address Spoofing [6]
Integrity	Tampering	-IP Replay Attack -ARP-based MitM-Attack
Non-Repudiation	Repudiation	-ARP-based MitM-Attack
Confidentiality	Information disclosure	-TCP Packet Sniffing -ARP Cache Poisoning
Availability	Denial of Service	-VLAN Multicast Brute-Force Attack -ICMP Flooding -DoIP Header Magnification Attack [7] -ARP Jamming -ICMP Smurf Attack -DoIP Header NACK Storm [8] -TCP Fragmentation Attack -TCP LAND Attack -UDP Flooding -UDP Fragmentation Attack
Authorization	Elevation of privilege	-TCP Session Hijacking -IP Address Spoofing -MAC Address Spoofing

The various threat categories and attacks for DoIP Data Flow (OBD-GW-DF, GW- OBD-DF, GW-ADCU-DF, ADCU-GW-DF) are analyzed in Table 3.

Table 3. Threats and attacks for DoIP data flow

Security Attributes	Threat Model	Attack Surface
Integrity	Tampering	-IP Replay Attack -ARP-based MitM-Attack
Confidentiality	Information disclosure	-TCP Packet Sniffing -ARP Cache Poisoning -VLAN Double Tagging
Availability	Denial of Service	-VLAN Multicast Brute-Force Attack -ICMP Flooding -DoIP Header Magnification Attack -ICMP Smurf Attack -DoIP Header NACK Storm -TCP Fragmentation Attack -TCP LAND Attack -UDP Flooding -UDP Fragmentation Attack

4. Risk assessment of DoIP data flow

In this part, the risk value and risk treatment are determined by referring to the ISO/SAE 21434 [9]. According to ISO/SAE 21434, for each threat scenario the risk value shall be determined from the impact of the associated damage scenarios and attack feasibility of the associated attack paths. Impact rating for damage scenarios involving safety, financial, operational and privacy damage. Attack feasibility is defined in ISO/IEC 18045 as a measure of the effort to be expended in attacking an item or component, expressed in terms of an attacker's expertise and resources. Attack potential relies on five core parameters: elapsed time (ET), specialist expertise (SE), knowledge of the item or component (KoIC), window of opportunity (WoO), and equipment (Eq).

In the vehicle identification phase, no authentication is provided, which is why it is possible for attackers to send false information as a response. The attacker does not even have to establish a TCP connection for this, since this phase runs via UDP. They can respond to requests with their own IP address and pretend to be a vehicle. Also lacking any integrity protection, all fields

in the response can be changed by an attacker. Attackers may disrupt the vehicle discovery function, preventing the diagnostic tool from connecting to legitimate vehicles. The detailed TARA for vehicle identification are shown in Table 4 and Table 5.

Table 4. Impact analysis of vehicle identification

Damage Scenario of vehicle identification request/response	Safety	Financial	Operation	Privacy	Impact Rating
An attacker impersonates a legitimate vehicle or floods the network with spoofed discovery requests, preventing the diagnostic tool from correctly identifying legitimate vehicles or connecting to malicious devices.	The diagnostic tool may connect to a malicious device, bypassing or disabling vehicle safety features.	Unauthorized access to the vehicle may lead to increased recall or repair costs.	The diagnostic tool cannot discover legitimate vehicles, affecting production line or after-sales service efficiency.	Vehicle identity information may be leaked, violating user privacy.	Major

Table 5. Attack feasibility rating for vehicle identification

STRIDE	Threat Scenario	ET	SE	KoIC	WoO	Eq	Attack Feasibility
Spoofing	An attacker impersonates a legitimate vehicle and responds to the diagnostic tool's discovery request.	⩽ 1week	Proficient	Restricted information	Easy	Specialized	High
Denial of Service	An attacker floods the network with spoofed discovery requests, exhausting vehicle or network resources.	⩽ 1day	Proficient	Restricted information	Easy	Specialized	High

For spoofing of vehicle identification, it requires time to analyze DoIP protocol and craft spoofed responses (1–5 days), it requires knowledge of DoIP protocol (ISO 13400), network packet crafting, and basic automotive diagnostics. The attacker needs familiarity with Wireshark or Scapy for traffic analysis and spoofing. The attacker needs understanding of DoIP discovery mechanisms (UDP broadcast, Vehicle Identification Request/Response) and knowledge of vehicle identifiers (e.g., VIN, EID) and how they are formatted in DoIP messages. DoIP discovery uses unencrypted UDP broadcasts, making spoofing straightforward. Low-cost tools such as standard computers, Network Interface Card (NIC), and open-source tools (e.g., Scapy, Kali Linux) can be used to perform attack activity. The attack feasibility for vehicle identification spoofing is high.

For DOS of vehicle identification, minimal (hours to days) to set up tools and generate spoofed requests and immediate impact once the attack is launched (seconds to minutes). It requires basic networking skills to craft and send UDP packets. The attacker needs familiarity with DoIP protocol structure (optional for simple flooding attacks). The attacker only requires knowledge of DoIP's use of UDP port 13400 for discovery messages and doesn't need to understand vehicle identifiers (e.g., VIN, EID) or protocol specifics. Legacy DoIP implementations lack rate-limiting or authentication for discovery requests. UDP's connectionless nature allows easy spoofing of source IP addresses. Low-Cost Tools such as standard computers with network access and open-source tools can perform attack activity. The attack feasibility for vehicle identification DOS is high.

The overall risk assessment results for DoIP Data Flow are shown in Table 6. By implementing appropriate measures, the security risks in the DoIP communication process can be effectively reduced, ensuring the safety and reliability of the vehicle diagnostic system.

Table 6. Risk assessment of DoIP data flow

Asset	Threat scenario	Impact Rating	Attack Feasibility	Risk Value	Risk Treatment
DoIP Data Flow-Vehicle Identification Request/Response	An attacker impersonates a legitimate vehicle and responds to the diagnostic tool's discovery request.	Major	High	4	Reduce
	An attacker floods the network with spoofed discovery requests, exhausting vehicle or network resources.	Major	High	4	Reduce

5. Security goal definition and security mechanisms recommendation

From the assets identification and attack path analysis and risk assessment, various security goals that require protection have been identified in Table 7.

Table 7. Security goals

ID	Security Goal
SG1	Protection of Central Gateway
SG2	Protection of ADCU
SG3	Protection the integrity and availability of Vehicle Identification Request/Response

In general, the risk treatment methods for securing DoIP communications were considered from a network view. Thus, Transport Layer Security (TLS) is recommended on transport layer to protect all lower level and higher level protocols (higher level protocols are encapsulated in low level protocols). TLS has already widely adopted that are used by numerous websites and applications to facilitate privacy and data security for Internet communication. It uses a client-server handshake mechanism to establish an encrypted and secure connection and to ensure authenticity of communication. During set up, the devices exchange encryption capabilities followed by authentication of either server or client or both (mutual) using digital certificates. Then a session key exchange process is done in which both the parties agree on a key to encrypt the data to be transferred over this session.

Furthermore, it is important to point out that a trust boundary is created by selecting a security mechanism. For example, all lower-level protocols must be trusted, and they might not be protected by selecting a security mechanism on OSI layer 4 (e.g., TLS). So, it is recommended to combine multiple security mechanisms to ensure integrity, availability, authenticity, confidentiality etc. of all DoIP connections.

In addition, as Central Gateway can implement security mechanisms, network Segregation and VLAN can be implemented by Switch in Central Gateway. A VLAN tag is inserted between the Ethernet Header and the data. This tag provides unique identification for all Ethernet messages of a VLAN. The VLAN tag is added or removed at the switch. This makes it possible to achieve a clear and efficient separation of data traffic involving external devices (e.g., diagnostic test devices) and purely internal communication. Firewalls also can be used for access control. That means, what kind of DoIP messages are allowed to be sent to the other ECUs for diagnostic purposes. It allows for better security. From network topology aspects, defense, monitoring, isolation and reactive security controls (IDS, IPS) are also necessary to prevent, detect, limit, and/or stop attacks.

6. Conclusion

The focus of this paper is to address security challenges in Automotive DoIP use case. The assets and threat analysis are listed based on exemplary E/E architecture and Ethernet attack surface, the risk assessment is also performed for DoIP data flow. Various security goals and risk treatments are refined to protect the DoIP end nodes and data flow. From a network view, SSL/TLS is a suggested method. Besides, network segmentation and VLAN configuration can also be considered in Central Gateway.

References

[1] Wachter, P., & Kleber, S. (2022). Analysis of the DoIP Protocol for Security Vulnerabilities. *Proceedings of the 6th ACM Computer Science in Cars Symposium*, Article 9. Association for Computing Machinery, Ingolstadt, Germany.

[2] ISO. (2022). Road vehicles — Unified diagnostic services (UDS) — Part 5: Unified diagnostic services on Internet Protocol implementation (UDSonIP), pp. 1-26.

[3] Luo, F., Wang, J., Li, Z., & Zhang, X. (2024). Vulnerability analysis of DoIP implementation based on model learning. *SAE Technical Paper 2024-01-2807*.

[4] ISO. (2019). BS ISO 13400-2. Road vehicles. Diagnostic communication over Internet Protocol (DoIP). Part 2. Transport protocol and network layer services, pp. 1-94.

[5] Microsoft. (2002). The STRIDE threat model. Commerce Server 2002. Retrieved from https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

[6] Matsubayashi, M., Koyama, T., Okano, Y., Tanaka, M., Miyajima, A., Oshima, Y., Ukai, S., Wakatsuki, T., Sugashima, T., & Nakamura, T. (2021). Attacks Against UDS on DoIP by Exploiting Diagnostic Communications and Their Countermeasures. *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. https://doi.org/10.1109/VTC2021-Spring51267.2021.9448963

[7] Lauser, & Krauß, T. (2023). Formal Security Analysis of Vehicle Diagnostic Protocols. *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 1-11. https://doi.org/10.1145/3600160.3600184

[8] Lindberg, J. (2011). Security Analysis of Vehicle Diagnostics using DoIP (Master's thesis, Chalmers University of Technology). Retrieved from https://odr.chalmers.se/items/9d6c756c-1d74-48c2-957f-fea957462dc2

[9] ISO/SAE. (2021). ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering [International standard]. International Organization for Standardization; SAE International. Retrieved from https://cdn.standards.iteh.ai/samples/70918/9c85ee86ba1945fe845ac38711773665/ISO-SAE-21434-2021.pdf