World Journal of Engineering Research and Technology
WJERT
www.wjert.org SJIF Impact Factor: 7.029

SECURITY CHALLENGES IN CONNECTED AUTONOMOUS VEHICLES: A CASE STUDY OF HD MAP TRANSMISSION

Mohammed Sharfuddin*

MS in Computer Sciences, Campbellsville University, KY, USA.

Article Received on 11/03/2025 **Article Revised on 01/04/2025** **Article Accepted on 20/04/2025**

***Corresponding Author**
Mohammed Sharfuddin
MS in Computer Sciences,
Campbellsville University,
KY, USA.

ABSTRACT

Connected autonomous vehicles (CAVs) depend heavily on high-definition (HD) maps for safe navigation. As these maps are frequently transmitted between cloud servers, infrastructure, and vehicles, ensuring their secure delivery is critical. This paper explores key security challenges associated with HD map transmission in CAVs, including data integrity, confidentiality, and real- time authentication. We present a case study of a simulated HD map transmission pipeline, identify common vulnerabilities, and propose mitigation strategies using cryptographic techniques and secure vehicular networking protocols. Our findings underscore the importance of end-to-end security for maintaining safety and trust in autonomous transportation systems.

1. INTRODUCTION

High-definition maps serve as a foundational layer for autonomous driving, offering centimeter-level details of road layouts, lane markings, and traffic infrastructure. Unlike traditional navigation maps, HD maps are used for vehicle localization, obstacle prediction, and trajectory planning [1][2]. In a connected autonomous vehicle (CAV) ecosystem, these maps are often updated and transmitted over vehicle-to-everything (V2X) networks. This transmission can occur in real- time from infrastructure (e.g., RSUs), from cloud servers over 5G, or between vehicles. These interactions introduce significant cybersecurity challenges. This paper analyzes the security risks specific to HD map transmission and presents a framework for safeguarding CAVs from potential attacks like map spoofing, man-in-the-middle (MitM), and data tampering. A simulated case study illustrates real-world vulnerabilities and recommended countermeasures.

2. Background and Related Work

CAV security has been studied across several dimensions—network, software, hardware, and data integrity. However, HD maps remain a relatively unexplored vector of attack. V2.

Communication Security: Research highlights vulnerabilities in DSRC and C-V2X protocols, including jamming, spoofing, and message injection.[3][4]

HD Map Sensitivity: HD maps contain precise location data, making them attractive targets for adversaries seeking to misguide AVs.[5]

Cryptographic Methods: Techniques like digital signatures, hash verification, and secure key management offer potential solutions but can introduce latency and scalability challenges.[6-10]

Our work builds on these studies by focusing specifically on the security of HD map transmission channels.

3. Threat Model and Case Study

3.1 Threat Model

We consider an attacker capable of

Intercepting HD map data in transit (MitM). Injecting false map data (spoofing).

Tampering with map integrity (e.g., modifying lane geometry). Launching replay attacks using old map data.

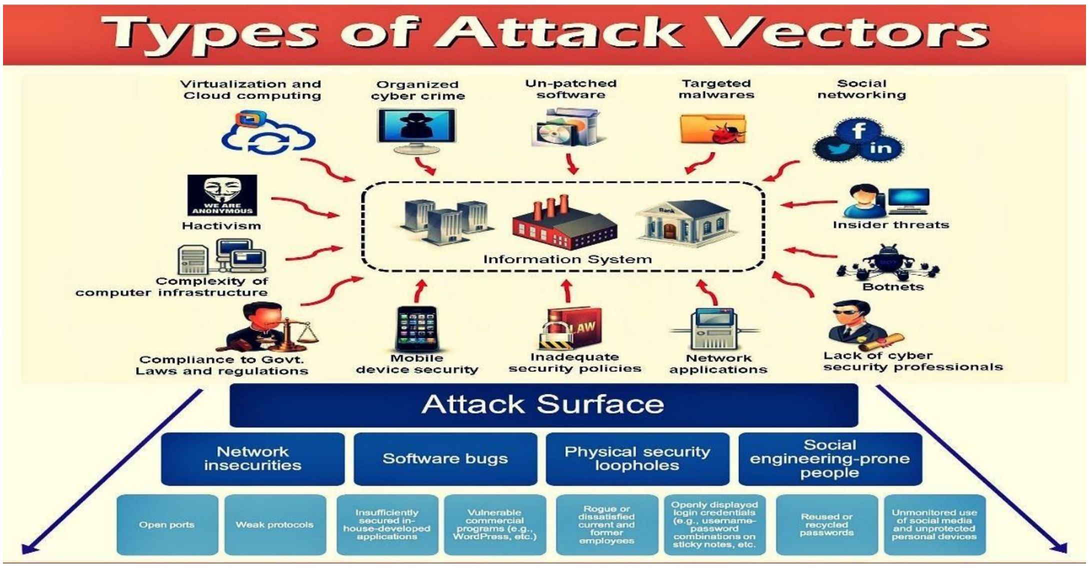
Types of Attack Vectors
Virtualization and Cloud computing
Organized cyber crime
Un-patched software
Targeted malwares
Social networking
Hactivism
Insider threats
Information System
Complexity of computer infrastructure
Botnets
Compliance to Govt. Laws and regulations
Mobile device security
Inadequate security policies
Network applications
Lack of cyber security professionals
Attack Surface
Network insecurities
Software bugs
Physical security loopholes
Social engineering-prone people
Open ports
Weak protocols
Insufficiently secured in-house-developed applications
Vulnerable commercial programs (e.g., WordPress, etc.)
Rogue or dissatisfied current and former employees
Openly displayed login credentials (e.g., username-password combinations on sticky notes, etc.
Reused or recycled passwords
Unmonitored use of social media and unprotected personal devices

Figure 1: Attack Vectors During HD Map Transmission.

3.2 Case Study Setup

We simulated an AV network where HD map data is transmitted from a roadside unit (RSU) to an AV using a basic C-V2X protocol stack.

Key observations included

No encryption by default: HD map packets were visible to packet sniffers.

No hash validation: The receiving AV could not verify if the map data had been tampered with.

Susceptibility to replay: A previously recorded map segment could be re-transmitted to confuse AV localization.

4. Security Mechanisms and Evaluation

4.1 Proposed Solutions

We evaluated several defense mechanisms

Digital Signatures (ECDSA): Ensures map origin and authenticity.

SHA-256 Hashing: Validates map segment integrity.

Timestamping & Nonces: Prevents replay attacks.

TLS over V2X: Encrypts map data in transit.

4.2 Performance and Overhead

Table 1: Security Method Evaluation.

Mechanism	Latency (ms)	Overhead (%)	Effectiveness
ECDSA Signature	4.5	+12%	High

SHA-256 Hash Check	2.1	+5%	High
TLS Tunnel (C-V2X)	8.3	+20%	Very High
Timestamp Validation	<1	+2%	Moderate

While TLS provides comprehensive protection, its overhead may not be suitable for time-critical transmissions. A hybrid solution using hashes and signatures offers a balance between performance and security.

5. Real-World Incidents and Simulations

A simulated attack showed that:

AVs receiving fake map data adjusted speed limits or rerouted unexpectedly. Overridden lane geometry led to lateral control errors.

Lack of timestamp validation allowed replayed construction zones to persist beyond their closure.

6. Secure HD Map Distribution Architecture

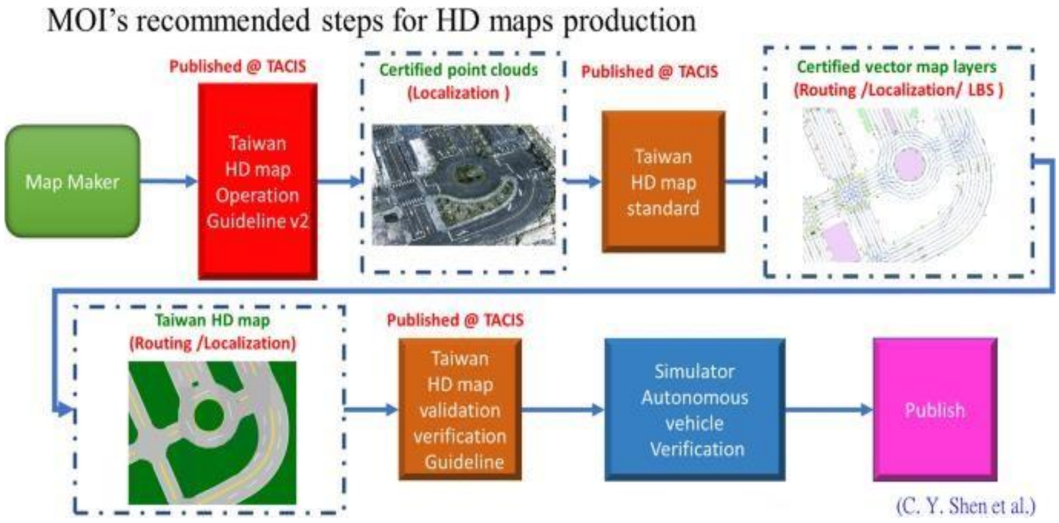
MOI's recommended steps for HD maps production
Published @ TACIS
Certified point clouds (Localization)
Published @ TACIS
Certified vector map layers (Routing /Localization/ LBS)
Map Maker
Taiwan HD map Operation Guideline v2
Taiwan HD map standard
Taiwan HD map (Routing /Localization)
Published @ TACIS
Taiwan HD map validation verification Guideline
Simulator Autonomous vehicle Verification
Publish
(C. Y. Shen et al.)

Figure 2: Proposed Secure HD Map Delivery System.

Components

Edge Map Servers: Cache encrypted and signed map segments.

Cloud Controller: Manages key revocation and signing authority.

Vehicle Trust Module: Verifies digital signatures, hashes, and timestamps before ingesting map data.

Table 2: Comparison of HD Map Security Protocols.

Protocol	Integrity	Confidentiality	Replay Protection	Latency (ms)
None (Baseline)	Low	None	None	~1
ECDSA + Hash	High	None	High	~4
TLS + Timestamp	High	High	High	~8

7. DISCUSSION

Our study highlights how the security of HD map transmission is both critical and vulnerable. A manipulated map can lead to incorrect localization or planning decisions, potentially endangering passengers.

Security systems must also consider

Key distribution in mobile networks.

Real-time performance for low-latency applications.

Scalability, especially in urban environments with dense AV traffic.

Future solutions may involve edge-based security gateways, zero-trust architectures, and blockchain for verifiable map updates.

8. CONCLUSION

This paper investigated the cyber security challenges associated with HD map transmission in CAVs. Through a threat model and simulation, we demonstrated common vulnerabilities and evaluated practical security mechanisms. Securing HD maps is essential to maintaining trust and safety in autonomous driving ecosystems, and our results offer actionable guidance for deploying secure, scalable AV networks.

9. REFERENCES

1. Z. Chen et al., "HD Map Generation for Autonomous Driving," IEEE Access, 2021.
2. C. Zhang et al., "High Definition Map for Self Driving Vehicles," IEEE Access, 2020.
3. R. Lu et al., "Connected Vehicles and Security: Challenges and Solutions," IEEE Internet of Things Journal, 2019.
4. A. Rouf et al., "Security and Privacy Vulnerabilities of In-Car Wireless Networks," NDSS, 2010.
5. S. Saponara et al., "Cybersecurity for Autonomous Vehicles: Review and Research Challenges," Electronics, 2020.
6. K. Zhang et al., "Security and Privacy in Smart Cities: Challenges and Opportunities," IEEE Communications Magazine, 2017.

7. M. Amoozadeh et al., "Security Vulnerabilities of Connected Vehicle Streams and Impact on Automated Driving," IEEE Comm. Mag., 2016.
8. ETSI TS 102 940, "Security Architecture and Management for Intelligent Transport Systems (ITS)," 2021.
9. A. Perrig et al., "Efficient Authentication and Signing of Multicast Streams Over Lossy Channels," IEEE S&P, 2000.
10. IEEE 1609.2, "Security Services for WAVE", 2020.