Supplementary Material

Title: Next-Generation V2x Communication And Authentication Security: Multi-Dimensional Review Of Threats And Defenses

Authors: Niranjan W, Meegammana , Harinda Fernando. Malka N. Halgamuge

Corresponding Author: Niranjan W, Meegammana , niranjan.meegammana@gmail.com

This supplementary file includes:

- **Section S1: Acronyms and Definitions**
- **Section S2: PRISMA Workflow and Inclusion Statistics**
- **Section S3: Network & Communication Layer Paper Analyses (Tables C1–C5)**
- **Section S4: Authentication & Access Control Layer Paper Analyses (Tables D1–D3)**

S1 : Acronyms and Definitions

List of Acronyms

AI – Artificial Intelligence
CNN – Convolutional Neural Network
DoS – Denial of Service
DDoS – Distributed Denial of Service
DQN – Deep Q-Network
DRL – Deep Reinforcement Learning
FPR – False Positive Rate
GAN – Generative Adversarial Network
MITM – Man-in-the-Middle
ML – Machine Learning
MIMO – Multiple-Input Multiple-Output
PQC – Post-Quantum Cryptography
QKD – Quantum Key Distribution
DRL – Reinforcement Learning
V2I – Vehicle-to-Infrastructure
V2V – Vehicle-to-Vehicle
V2X – Vehicle-to-Everything

S2: PRISMA Workflow and Extended Methodology Details

S2.1. PRISMA Workflow

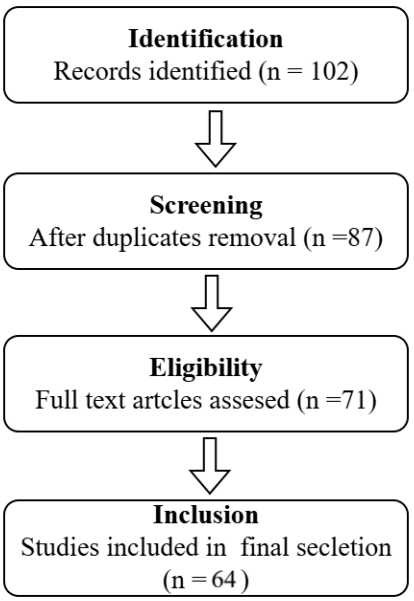

Fig S2.1 PRISMA flow diagram of study selection (Identification, Screening, Eligibility, Inclusion).

This diagram outlines the identification, screening, eligibility, and inclusion phases of the systematic review. It ensures transparency and reproducibility in selecting high-quality studies on V2X security.

S2.2 Screening Criteria

To ensure the inclusion of high-quality, peer-reviewed research, the following screening rules were applied:

- **Source type** – Only journal and conference papers were considered. Preprints, white papers, and non-peer-reviewed reports were excluded.
- **Version control** – Where multiple versions existed, the most recent peer-reviewed version was retained.
- **Duplicates** – Duplicate records were removed.
- **Topical relevance** – An NLP-assisted keyword frequency pass was conducted to prioritise papers centred on V2X cybersecurity threats and mitigations.
- **Two-stage relevance check** –
    1. **Title/abstract review** for thematic alignment.
    2. **Full-text screening** for methodological rigour, empirical validation, and tangible security contribution.

To minimise bias, two authors independently assessed eligibility. Inter-rater agreement reached **Cohen's κ = 0.87**, indicating substantial agreement.

S2.3 Eligibility Criteria

Inclusion criteria – studies were included if they:

1. Directly addressed **V2X threats/mitigations** (authentication, privacy, IDS, adversarial robustness, blockchain, PQC).
2. Proposed **novel frameworks/models** (e.g., AI/ML-based IDS, PQC schemes, hybrid architectures).

3. Provided **empirical validation** (e.g., detection rates, false positives, scalability, latency) on real-world datasets, testbeds, or prototypes.

4. Included **seminal pre-2019/2020 works** only if they were foundational (e.g., widely adopted taxonomies, cryptographic standards, or seminal models).

Exclusion criteria – studies were excluded if they:

- Lacked empirical analysis or implementation details.
- Focused solely on networking performance without a **cybersecurity perspective**.
- Offered only theoretical proposals with no modelling, PoC, or validation.
- Were redundant publications with no substantive novelty.

S2.4 Study Tier Classification

- **Tier-1 Studies** – High-impact papers with experimental validation, strong performance metrics, and realistic datasets/testbeds.
- **Tier-2 Studies** – Promising theoretical or simulation-based works with novel contributions but limited or early validation.

From an initial pool of 89 records, a total of 64 studies were included for detailed analysis after applying the above criteria.

Section S3 – Network and Communication Layer Comparative Tables (S3.I–S3.V)

Table S3.I(a) Technical Information of Papers on DoS/DDoS Attacks

Paper	Attack Vector	Targeted Systems	Adversary Model	Impact	Methodology	Contribution	Key Findings	Limitations	Future Research Directions
Ali et al., 2024	DoS via Packet Flooding	Autonomous Vehicle Systems (AVS)	External	AV Malfunction, Potential Accidents	AI-enhanced IDS with Explainable AI (XAI)	Enhanced IDS interpretability with XAI	Improved detection accuracy with explainability	Computational complexity	Federated Learning-based IDS
Gong et al., 2024	DoS-Induced Communication Delay	Intersection Control (CAVs)	External	Delay, Risk of Collisions	Resilient Distributed Control with Lyapunov Stability	Resilient control strategy for DoS at intersections	Maintains coordination under stochastic delays	Assumes full CAV deployment	Mixed traffic resilience
Ren et al., 2024	DoS via Network Disruption	AGV Tracking Control	External	Loss of Vehicle Control	T-S Fuzzy Controller with Switching Mechanism	New controller adapting to DoS intervals	Ensures exponential stability under DoS	Complex design, fuzzy dependency	Hybrid attack integration
Liu et al., 2024	DoS on GPS Communication	AEV Lateral Control	External	Loss of Positioning Data	Observer Design + Backstepping Controller	Adaptive controller with resilience to GPS failure	Observer restores pose estimation	Real-time performance not benchmarked	Sensor redundancy strategies
Mokari et al., 2024	DoS Modeled via Time-Varying Delay	Smart Vehicle Platooning	Internal	Route Deviation, Instability	Switching System + Delay Detection	Dynamic response to time-varying DoS	Delay triggers switching to restore control	Dependent on delay threshold calibration	Real-world vehicle implementation
Razzazi et al., 2024	CAM Flooding DoS Attack	Vehicular Ad Hoc Networks (VANETs)	Insider and Outsider	Network Congestion, Data Loss	Modified Online K-Means + Outlier Detection	Improved detection with streaming buffers	Buffer-tuned clustering increases accuracy	Memory tuning needed	Hybrid anomaly detection
Liu et al., 2024	DoS Blocking GPS Signals	Lateral Control of AEVs	External	Loss of Precision Control, Pose Errors	Observer with IMU-based Estimation + Adaptive Controller	Switching control	Estimates with IMU	Requires parameter tuning	Real-world integration with noisy sensors
Xu et al., 2024	Malicious Access Requests (DoS subtype)	Access Control in CAVs	Insider	Communication Congestion, Policy Overload	Graph Reinforcement Learning with STGCN	Adaptive access policy using graph RL	GRL detects interfering access faster than DQN	Assumes ideal trust estimation	Hybrid Sybil-DoS Access Attack Detection
Scruggs et al., 2024	DoS, Replay, and Data Integrity Attacks	LSCS in EVs	External	Loss of Yaw and Sideslip Control	Neural Network-Based Threat Detection	Improve attack recognition accuracy	Underperforms compared to hybrid NN	Simulation-only validation	Hybrid MPC-Observer-NN frameworks

Lam, 2023	DoS via Routing, Replay, Jamming	CAV Network Communication	External and Insider	Vehicular Instability, Traffic Interruption	Adaptive Threat Response with Game Theory	System reconfiguration	Reconfigurable protocols	No real-time field deployment	Distributed AI for vehicle fleets

Table S3.I(b) Technical Information of Papers on DoS/DDoS Attacks

Paper	Defense Mechanisms	Detection Techniques	Attack Duration	Traffic Pattern	Attack Automation Level	Tools	Defense Adaptability	Security Objectives
Ali et al., 2024	ML-based IDS, LIME (XAI)	Local Interpretable Model	Short-term	Flooding	Fully Automated	Python, LIME, SVM	Moderate	Cn, In, Av, Au, Ac, Pr
Gong et al., 2024	Polytopic Overapproximation and Control Synthesis	Delay Feedback Monitoring	Intermittent	Delay Injection	Semi-Automated	MATLAB	High	Cn, In, Av, Au, Ac, Pr
Ren et al., 2024	Switching Controller, Lyapunov Stability	State Monitoring, Switching Logic	Variable	Disruption (Non-periodic)	Semi-Automated	CarSim, MATLAB/Simulink	High	Cn, In, Av, Ac, Pr
Liu et al., 2024	State Observer (IMU), Adaptive Control	Switching Based on Attack Activity	Intermittent	GPS Blocking	Automated	MATLAB	High	Cn, In, Av, Au, Ac
Mokari et al., 2024	Resilient Control Strategy, Detection Algorithm	Incremental Counters	Variable	Time-varying Delays	Semi-Automated	Matlab	High	Cn, In, Av, Au, Ac, Pr
Razzazi et al., 2024	Unsupervised Clustering	1-SVM, LOF, IF, EE	Short-term	Flooding	Automated	Python, Clustering Libraries	Moderate	Cn, In, Av, Ac
Liu et al., 2024	Switching Controller, IMU Observer, Backstepping	State Observer Monitoring	Intermittent	Signal Drop	Automated	Matlab/Simulink	Moderate	Cn, In, Av, Au, Ac
Xu et al., 2024	VPolicy-GRL	Trust Graph Dynamics	Persistent	High-Frequency Requests	Fully Automated	PyTorch, STGCN, DQN	High	Cn, In, Av, Au, Ac, Pr
Scruggs et al., 2024	FNN and Observer Comparison	Residual Monitoring (Observer vs NN)	Short-term	Mixed	Fully Automated	MATLAB, Simulink, FNN	Moderate	In, Av
Lam, 2023	Context-aware Two-Tier Defense	Behavioral and Structural Monitoring	Variable	Composite Jamming	Semi-Automated	Simulation, Game Theory, AI Modules	High	Cn, In, Av, Au, Ac, Pr

Table S3.I(c) Performance Data of Papers on DoS/DDoS Attacks

Paper	Detection Rate	FPR	Scalability of Attack	Scalability of Defense	Experimental Validation	Response Time	Energy Consumption Impact	Communication Overhead	Datasets Used
Ali et al., 2024	High	Moderate	High	Moderate	Yes	Fast	Moderate	Medium	UNSW-NB15 (DoS features)
Gong et al., 2024	-	-	Moderate	High	Yes	Moderate	Low	Low	Simulated Intersection Scenario
Ren et al., 2024	-	-	Moderate	High	Yes	Medium	Moderate	Medium	Simulated
Liu et al., 2024	-	-	High	High	Yes	Fast	Low	Low	Simulated AEV

									Scenarios
Mokari et al., 2024	-	-	High	High	Yes	Variable	Moderate	Moderate	Simulated Vehicle Network
Razzazi et al., 2024	High	Low	High	High	Yes	Fast	Low	Medium	21 VANET datasets
Liu et al., 2024	-	-	High	Moderate	Yes	Moderate	Low	Low	Simulated GPS/IMU
Xu et al., 2024	High	Low	High	High	Yes	Fast	Low	Medium	Simulated Access Requests
Scruggs et al., 2024	High	-	High	Moderate	Yes	Fast	Low	Low	MATLAB Vehicle Sim
Lam, 2023	High	Low	High	High	Yes	Fast	Moderate	High	Synthetic CAV Communication

Table S3.II(a) General Information of Papers on MitM Attacks

Paper	Targeted System	Adversary Model	Communication Channel Targeted	Real-Time Capability	Attack Vector	Methodology
Huo et al., 2025	V2X Messaging	Passive Listener	V2X	Yes	Replay	Timestamp-based hash chaining
Chen et al., 2024	CAV Perception and Control	External Adaptive Agent	V2V, V2I	Yes	False Data Injection (FDI)	Hybrid estimation (NN + physics) with DRL-based controller
Scruggs et al., 2024	EV LSCS	Simulated internal node	In-vehicle	Yes	Replay, FDI, DoS	Residual-based detection with neural observer
Nazat and Abdallah, 2023	Autonomous Platoons, RSUs	Internal/External Hybrid	V2X, V2V	Yes	Impersonation, Injection	Dual-tier detection with LSTM and platoon monitoring
Gothwal et al., 2023	AV Wi-Fi	External MITM Wi-Fi Attacker	Wi-Fi	Yes	ARP Spoofing	Physical test using Ettercap
Chung et al., 2023	V2X Communication	Passive traffic manipulator	V2V, V2I	Yes	Message modification, delay, drop	Behavior Monitoring using BM-DEVS
Kumar et al., 2023	VANET	Insider with credentials	V2V	Yes	Replay of BSM	ML-based BSM classifier

Table S3.II(b) Technical Information of Papers on MitM Attacks

Paper	Defense Mechanisms	Detection Techniques	Encryption Bypass Techniques	Message Integrity Violation	Attack Duration	Tools	Future Directions	Security Objectives
Huo et al., 2025	Hash chain, RSU time sync	Message timestamp hash	Replay injection	Yes	Event-triggered	Protocol testing	Integration with RSU networks	In, Av
Chen et al., 2024	Model-predictive controller (MPC),	Reward-optimized observation usage	Sensor-level injection	Observation spoofing	Intermittent	Simulation, DRL framework	Real-world deployment with cross-validation	In, Av

	DRL							
Scruggs et al., 2024	NN + MPC + PID	Error threshold banding	Internal command spoof	Yes	Short-term bursts	MATLAB, Simulink	Field testing in EV	In, Av
Nazat and Abdallah, 2023	Signature validation, RSU trust channel	Forecast voting (LSTM-based)	Key spoofing	Yes	Dynamic	Python, LSTM, Simulation	Hardware deployment of RSU intelligence	In, Av
Gothwal et al., 2023	VPN, WPA2 encryption	Packet sniffing analysis	ARP spoof, SSL strip	Yes	Continuous	Ettercap, Wireshark, Raspberry Pi	Multi-platform protocol testing	In, Av
Chung et al., 2023	Context-aware traffic info validation	Behavior comparison	Replay-based	Yes	Scenario-dependent	BM-DEVS, Simulation engine	Dynamic model fusion with real-time analytics	In, Av
Kumar et al., 2023	Feature-based BSM validation	Supervised ML model	Signed replay	Yes	Event-triggered	Python, ML	Real-world RSU deployment	In, Av

Table S3.II(c) Performance Data of Papers on MitM Attacks

Paper	Impact	Detection Rate	FPR	Scalability of Attack	Scalability of Defense	Experimental Validation	Datasets Used	Contribution	Key Findings	Limitations
Huo et al., 2025	Routing disruption, stale data injection	High	Low	Moderate	High	Yes (simulated)	Hash simulation	Efficient anti-replay scheme	Lightweight and scalable	Time sync dependency
Chen et al., 2024	Trajectory deviation, unsafe maneuvering	High	Low	Moderate	High	Yes ((simulated)	Custom driving simulator	Hybrid secure control with adaptive detection	Control-aware filtering reduces FDI impact	Lacks real-world validation
Scruggs et al., 2024	Trajectory manipulation, yaw instability	High	Low	High	High	Yes (simulated)	Simulated lateral data	NN-based control security	Better than physics-only methods	Simulation-only validation
Nazat and Abdallah, 2023	Network hijack, behavior anomalies	High	Low	High	High	Yes (simulated)	Synthetic traffic scenarios	Layered MitM + anomaly detection framework	Combining RSU-level learning with vehicle input boosts accuracy	Latency sensitivity, trust assumptions
Gothwal et al., 2023	Session hijack, message spoofing	High	N/A	Moderate	Moderate	Yes (real-world)	None	Empirical attack demonstration	VPN mitigates MITM effectively on Wi-Fi	Niche network layer use-case
Chung et al., 2023	Route misguidance, misinformed planning	Moderate	Moderate	High	Moderate	Yes (simulated)	Behavior-based simulation	BM-DEVS model for context-aware defense	Detection varies by traffic complexity	Hard to calibrate across diverse scenarios
Kumar et al., 2023	False congestion/emergency	Very High (>90%)	Low	High	High	Yes (simulated)	VeReMi extension	Replay-specific ML framework	ML > crypto-only detection	Sender ID overfit risk

Table S3.III(a) General Information of Papers on Jamming Attacks

Paper	Attack Vector	Targeted System	Jamming Type	Attack Location	Channel Used	Impact	Adversary Model

von Hünerbein, 2024	GNSS Signal Jamming and Spoofing	GPS/GNSS Navigation	Continuous Wave Interference	Harbours, Industrial Areas	GNSS Bands	Loss of Navigation Accuracy	Passive Spoofers, Intentional Jammers
Alam et al., 2024	DSRC Jamming	VANETs, CAV Communication	Omnidirectional Jamming	Urban DSRC Zones	DSRC, WAVE	Total network disruption, beacon loss	Multiple Dynamic Jammers
Lohan et al., 2024	AI-enabled Jamming and Interference	5G/6G Vehicular Networks	Sensing-based, Reactive, Sweep	Various 5GB Deployment Scenarios	Various (mmWave, THz, DSRC)	SNR degradation, transmission failure	Smart AI-enabled Jammers
Yao et al., 2023	Joint Jamming and Eavesdropping	V2V in CAV Networks	Reactive Smart Jamming	Urban CAV Scenarios	5.9 GHz	Reduced Secrecy Rate, Data Throughput	Dynamic, Smart Jammer
da Silva et al., 2023	Radio Jamming	V2X - DNPW and IMA Use Cases	Drone-based Interference	Real Urban Map (Simulated)	DSRC CH 172	V2X Packet Loss, Safety Failure	External RF Jammer
Zhou et al., 2023	Malicious Signal Jamming	Wireless Comms (Vehicular/IoT)	Dynamic and Continuous	Simulated Wireless Channels	Multi-band Wireless Channels	Communication failure, latency spikes	Adaptive Malicious Jammers
Yao et al., 2023	Smart Jamming and Eavesdropping	Autonomous Vehicle Networks	Adaptive DRL-Based	CAV Networks	V2V Channels	QoS degradation, secrecy leakage	Unknown Smart Attackers

Table S3.III. Technical Information of Papers on Jamming Attacks

Paper	Methodology	Defense Mechanisms	Detection Techniques	Tools	Mitigation Complexity	Future Directions	Contribution	Security Objectives
von Hünerbein, 2024	Real-Time Signal Monitoring (GIDAS)	GIDAS Detection, Snapshot Logging	Spectrum Analysis, Snapshot Storage	GIDAS System	Low	Integrate mitigation with detection systems	Operational monitoring tool for AV signal health	Av
Alam et al., 2024	Centroid Localization, Graham Scan Hull	Bloom Filter Blocking	Localization + Area Mapping	NS-3, SUMO	Moderate	Real-world deployment and filter optimization	Presents full jamming detection, localization, and prevention pipeline	Av
Lohan et al., 2024	Survey-based Review of ML Techniques	AI/ML (DL, RL, FL, Meta-L)	Classification, Regression, Signal Analytics	Not applicable (Survey)	High	Adaptive learning models for dynamic interference	Survey of AI-based jamming/anti-jamming for B5G vehicular networks	Av
Yao et al., 2023	Hierarchical DQN + Kalman Filter	Distributed Kalman Filter, Deep RL	Channel Monitoring, Secrecy Rate Optimization	MATLAB, Simulation	High	Lightweight RL	First DRL-based joint anti-jamming and anti-eavesdropping scheme for AVs	Cn, Av,
da Silva et al., 2023	Simulation with Capon Beamforming	Antenna Array, Beamforming	SNR/SNIR Evaluation	Simu5G, Veins, OpenStreetMap	Moderate	Evaluate NLOS and mixed-mode traffic	Validated antenna-based mitigation for 3GPP use cases	Cn, Av
Zhou et al., 2023	Imitation Learning-based Spectrum Decision	Expert Strategy + Imitation Learning Neural Networks	Imitation of historical expert strategy	Custom simulation setup	Moderate	Expand to real-world jamming scenarios	Introduces IL into anti-jamming decisions with high adaptability	Av
Yao et al., 2023	Hierarchical DQN for Power/Channel Control	Deep Reinforcement Learning, DKF	DRL-Optimized Decision Making	DRL Framework, Kalman Filters	High	Hybrid detection for jamming-eavesdropping	Secure V2V via hierarchical DRL against joint threats	Av

Table S3.III(c) Performance Data of Papers on Jamming Attacks

Paper	Disruption Level	Experimental Validation	Detection Rate	FPR	Datasets Used	Key Findings	Limitations
von Hünerbein, 2024	High	Yes	Real-time interference alerts	Low	Field Data	Monitoring GNSS quality enhances AV safety	Does not prevent jamming only detects
Alam et al., 2024	Communication Loss	Yes	96.03%	0.86%	Synthetic Mobility Dataset	Mapping enhances proactive jammer blocking	Limited jammer types simulated
Lohan et al., 2024	Dynamic and Adaptive	No (Survey)	Varies by approach	Not quantified	Various Literature-based	Comprehensive taxonomy and future roadmap for AI anti-jamming	Lacks experimental validation
Yao et al., 2023	High	Yes	Not explicitly quantified	Not explicitly mentioned	Synthetic Data	Hierarchical DQN boosts secrecy and communication rate	High computational complexity, lack of real-world test
Yao et al., 2023	Severe	Yes	Improved over baselines	Not clearly reported	Synthetic	DRL models outperform static approaches	Needs scalable real-time implementation
da Silva et al., 2023	Critical	Yes	Gain of 9.66 dB	Not applicable	Custom Simulation Data	Beamforming reduces jamming drastically	Only LOS scenarios tested
Zhou et al., 2023	High	Yes	Higher than RL and DQN	Low (qualitative)	Expert-generated Simulations	Outperforms RL/DQN with better convergence and adaptability	Lacks large-scale field testing

Table S3.IV(a) General Information of Papers on Eavesdropping Attack

Paper	Attack Vector	Targeted System	Adversary Model	Impact	Methodology	Contribution	Key Findings	Limitations	Future Research Directions
Zhao et al., 2024	Eavesdropping on V2I	V2I Backscatter Links	Passive Listener	Confidentiality and Privacy Violation	Power control algorithms	Optimization-based approach	Joint resource allocation to enhance secrecy	Focused on physical layer only	Extend to multi-antenna systems
Tao and Hu, 2024	Eavesdropping and Packet Drop	Sensor-State Estimation Link	External	State Disclosure via Channel Leakage	Paillier Cryptosystem + Round-Robin	Encryption-aware estimator with bandwidth constraints	Maintains accuracy under eavesdropping	Latency from encryption	Real-time encrypted estimation
Stavdas et al., 2024	Quantum Eavesdropping	V2I Links via RSU and BS	Quantum Passive	Key Leakage, Identity Spoofing	QKD with Software-Defined Network	Integrated QKD with SDN for V2I	Effective detection and mitigation of eavesdropping	LoS dependency of FSO links	Resilient quantum routing protocols
Ayaz et al., 2023	Eavesdropping / Impersonation	V2X / C-V2X	Passive eavesdropper	Leakage of vehicle ID, impersonation	Radio Frequency Fingerprinting	Use of inherent RF hardware features	RFF can prevent identity spoofing	Depends on environmental	Combine RFF with machine

					(RFF)			factors	learning
Yao et al., 2023	Smart Jamming + Eavesdropping	V2V Transmission Channels	Adaptive External Eavesdropper	QoS Disruption, Secrecy Rate Loss	Distributed Kalman Filtering + DRL	Real-time DRL-based power/channel optimization	Enhanced secrecy and communication rate	Requires training and calibration	Cooperative anti-eavesdropping methods

Table S3.IV(b) Technical Information of Papers on Eavesdropping Attack

Paper	Defense Mechanisms	Detection Techniques	Encryption Method	Attack Complexity	Tools	Countermeasure Adaptability	Security Objectives
Zhao et al., 2024	Resource allocation and power control	Not explicit	None	Low	Simulation tools	Channel conditions and vehicular dynamics	Cn, In, Av
Tao and Hu, 2024	Secure Estimator via Public-Key Encryption	None (Prevention-Focused)	Paillier Public-Key	Moderate	Mathematical Proofs, Paillier Encryption	High	Cn
Stavdas et al., 2024	Device Private Networks (DPN), DAU, ZAP	QKD Interference Detection	Quantum Key Distribution (QKD)	High	Quantum Hardware, SDN	High	Cn
Ayaz et al., 2023	Physical-layer authentication with REF	Classification of RF features	Not encryption-based	Moderate	RF fingerprint extraction, signal processing, ML	Moderate	Cn, In, Au
Yao et al., 2023	Hierarchical DQN Strategy	Secrecy Rate Assessment	Adaptive Secrecy Rate Control	High	Python, DRL, Kalman Filter	High	Cn

Table S3.IV(c) Performance Data of Papers on Eavesdropping Attack

Paper	Detection Rate	False Positive Rate (FPR)	Scalability of Attack	Scalability of Defense	Experimental Validation	Real-Time Impact	Data Sensitivity Level	Datasets Used
Zhao et al., 2024	-	-	High	Moderate	Yes	High	Medium	Simulated Model
Tao and Hu, 2024	N/A	N/A	Moderate	High	Yes	Moderate	Very High	Simulated Sensor Data
Stavdas et al., 2024	High	Low	Low	High	Yes	Moderate	Very High	Urban V2I Simulation
Ayaz et al., 2023	High (>90%)	Low	Limited	Moderate	Yes	High	High	Proprietary RF signal datasets
Yao et al., 2023	Superior to Classical Models	Low	High	High	Yes	High	High	Simulated Dynamic Channels

Table S3.V(a) General Information of Papers on V2X Secure Communication Protocols

Paper	Methodology	Security Protocol	Communication Channel	Attack Vector	Threat Model	Security Objectives
Iordache et al., 2024	Blockchain-secured AV communication	Blockchain with Byzantine Fault Tolerance (BFT), smart contracts	V2V, V2I, VANETs	Sybil attacks, data tampering, DoS	External spoofers, malicious vehicles, rogue RSUs	In, Au,Ac

Jin et al., 2024	BeHarmony Blockchain-IoV Communication	BeMutual, BeDNS	V2X (inter and intra-vehicle)	Sybil, spoofing, impersonation	Malicious RSUs, unauthorized peer entities	Cn, In, Au, Ac
Hussain et al., 2024	Ethereum-Based IoV Security Framework	Ethereum blockchain with PoW/PoS	V2V, V2I	Spoofing, unauthorized access	Unauthorized node access, message injection	In, Au, Ac
Lv et al., 2024	Safe Multi-Agent Reinforcement Learning	Safe MARL architecture with authentication filters	Wireless V2X	Spoofing, adversarial message injection	Spoofing attackers with fake observations	Au
Vybornova, 2024	Secure V2V Protocol with Physical Layer Security	Hybrid TLS with visible light and ultrasonic channels	V2V, V2X	Message tampering, location spoofing	External adversaries, spoofers	Cn, In, Au
Giaccaglini, 2024	PKI-based V2X Message Security	IEEE 1609.2, ECDSA	VANETs	Message tampering, impersonation, eavesdropping	External eavesdroppers, rogue vehicles	Cn, In, Au
Kumar, 2024	RSFVC: Biometric-ECC Framework for VCN	ECC + Biometric + AVISPA verification	Vehicular Cloud Network (VCN)	Replay, impersonation, MITM	External and insider attackers	Au, Pr
Meijers et al., 2022	Blockchain-enabled V2X Communication	Distributed Ledger with Consensus	V2V, V2I, IoT	Data tampering, message deletion, Sybil attacks	Malicious nodes, compromised sensors	In, Ac
Jasim et al., 2022	4G/5G Encryption Protocol Evaluation	AES, ZUC, SNOW 3G	Cellular V2X (C-V2X)	Cryptanalysis, brute-force key guessing	Generic adversaries, cipher breakers	Cn, In

Table S3.V(b) Technical Information of Papers on V2X Secure Communication Protocols

Paper	Authentication Method	Encryption Technique	Key Management Strategy	Trust Model	Message Integrity Mechanism	Replay Protection	Intrusion Detection
Iordache et al., 2024	Blockchain identity verification, smart contracts	Blockchain-native cryptography	Decentralized, smart contract-based	Decentralized consensus (BFT)	Immutable blockchain ledger	Blockchain timestamping	No
Jin et al., 2024	Decentralized domain identity via BeDNS	Blockchain-native, unspecified	Distributed identity-based	Smart contract and legal contract fusion	Hash-based blockchain entries	Contract-layer authentication	No
Hussain et al., 2024	Smart contract and wallet identity	SHA-256	Wallet-based cryptographic keys	Public permissionless blockchain	Transaction immutability	Blockchain timestamps	No
Lv et al., 2024	Message filtering and sharing reputation	None – relies on reputation validation	Implicit – based on agent behavior	Reputation-based multi-agent policy	Message authentication filters	Temporal comparison in MARL	Yes
Vybornova, 2024	Secrecy capacity-based clustering	Hybrid key agreement (physical + TLS)	Intra-cluster key exchange	Base station led security clusters	Encrypted signatures + cluster validation	Session-specific keying	No
Giaccaglini, 2024	Digital certificates via PKI	ECDSA, ECC	PKI certificate management	Hierarchical (PKI trust chain)	Digital signatures	Session freshness validation	Yes
Kumar, 2024	Three-factor (ID, password, biometrics)	Elliptic Curve Cryptography	Biometric-derived session keys	Mutual authentication with BAN logic	ECC + hash verifications	Session freshness tokens	Yes
Meijers et al., 2022	Smart contract-based ID verification	Cryptographic hashing (SHA)	Peer-verified identity and ledger consensus	Decentralized via blockchain nodes	Immutable blockchain ledger	Consensus-timed block inclusion	No

Jasim et al., 2022	Protocol-layer dependent	AES-128/192/256, SNOW 3G, ZUC	Static/dynamic key usage per standard	3GPP and LTE cryptographic compliance	Block cipher modes (CBC, CTR)	IV management and timestamps	No

Table S3.V(c) Performance Data of Papers on V2X Secure Communication Protocols

Citation	Experimental Validation	Dataset Used	Tools/Frameworks	Latency Impact	Scalability	Real-time Capability	Limitations	Future Work
Iordache et al., 2024	Yes – simulated environment	Synthetic AV communication logs	CARLA simulator, smart contracts	Moderate	High (edge-cloud integration)	Yes	High computational load, edge dependence	Integrate real-world vehicular testbeds
Jin et al., 2024	Yes – simulation of RSU cases	Synthetic RSU availability scenarios	BeMutual, BeDNS, Ethereum	Low	High	Yes	Smart contract limitations, legal interpretability	Integrate cross-jurisdictional compliance automation
Hussain et al., 2024	Yes – Ethereum simulation	Vehicle registration logs	Remix IDE, Metamask, Ethereum	Moderate (due to Ethereum consensus)	Moderate	Limited	Ethereum gas costs, transaction delays	Evaluate newer blockchains (e.g., Polkadot)
Lv et al., 2024	Yes – UAV swarm simulations	Simulated jamming and video transmission logs	Neural MARL, Raspberry Pi UAVs	Low	High	Yes	Dependent on agent cooperation and computation	Generalize for diverse communication conditions
Vybornova, 2024	Literature synthesis and protocol proposal	None (conceptual model)	N/A	Low	Moderate	Yes	No implementation, lacks empirical validation	Prototype hybrid VLC-acoustic V2V network
Kumar, 2024	Yes – AVISPA and BAN logic	Simulated protocol traffic	AVISPA tool, ECC library	Low	High	Yes	Complex biometric setup	Biometric efficiency optimization
Giaccaglini, 2024	Yes – ms-van3t and OScar frameworks	Simulated vehicular messages and GPS logs	ProVerif, OScar, ms-van3t	Negligible	High	Yes	Pseudonym handling and user privacy	Enhance privacy management in PKI
Meijers et al., 2022	Conceptual and simulated	N/A (theoretical architecture)	Not specified	Moderate	High	Limited	Performance trade-offs, privacy leakage risks	Scalable architectures for V2X-specific demands
Jasim et al., 2022	Yes – algorithmic analysis	Encryption performance benchmarks	Cryptanalysis methods	Low to Moderate	High	Yes	No application-layer scenarios	Application in IoV and AV environments

Section S4 – Authentication and Access Control Comparative Tables (S4.I - S4.III)

Table S4.1(a) General Information of Papers on Authentication Security

Paper	Methodology	Authentication	Authentication Domain	Protocol Type	Trust Model	Security Objectives
Qiu et al., 2024	Learning-based authentication via GAN	Generative Adversarial Framework (GAF)	V2X	Signal classification via ML	Adaptive authentication logic	Au

Du et al., 2024	Anonymous V2V Identity Authentication Protocol (EAIA)	Elliptic Curve Cryptography (ECC)	V2V	Lightweight mutual authentication	No central authority in-session	Au
Cui et al., 2024	Cross-domain Authentication with Trust Scoring	Edge server-based key management	V2X , Edge, TA	Multi-step credential exchange	Edge + TA mutual scoring	Au
Chen et al., 2024	RFF-based LTE-V2X Authentication	Radio Frequency Fingerprinting	C-V2X	Channel estimation + fingerprint extraction	RFF integrity and uniqueness	Au
Lin and Jhuang, 2024	Blockchain-based Certificateless AKA Protocol	CL-AKA with smart contract keys	V2V	Certificateless auth + key exchange	Decentralized blockchain KGC	Au, Ac
Xu et al., 2024	Post-Quantum Platoon Authentication	Signal-based ICA-VSSI + QC-MDPC	V2X platoon	Initial Access Authentication (IAA)	Centralized + physical-layer verification	Cn, Au
Li et al., 2023	Digital Twin-based Authentication	Digital twin-assisted handover auth	5G-V2X	Proactive handover auth	Zero Trust with digital twin agents	Au
Anderson et al., 2023	Zero-Trust Architecture (ZTA)	Continuous authentication	IVN	ZTA control + policy enforcement	Zero Trust (never trust, always verify)	Au
Cui et al., 2023	Anonymous Authentication and Group Key Agreement	V2X-GKA (Group Key Agreement)	C-V2X	Session key + pseudonym auth	TA centralized trust	Au, Pr
Suo and Sarma, 2022	Two-Factor Authentication Scheme	NLOS + LOS challenge-response	RSU and Vehicle	Certificate-based challenge-response	Whitelisting approach	Au

Table S4.1(b) Technical Information of Papers on Authentication Security

Paper	Cryptographic Techniques	Key Management	Identity Protection	Attack Resistance	Session Management	Mutual Authentication	Multi-factor Support
Qiu et al., 2024	DCGAN, enhanced CNN	ML-based classification	Channel attribute-based signal enhancement	Spoofing and impersonation	Implicit via continuous classification	Yes	Single factor (signal patterns)
Du et al., 2024	ECC, pseudo-identity, session key agreement	pseudonyms, local session keys	Anonymous identity exchange	Yes - impersonation, key exposure, replay	Temporary session key generation	Yes	No
Cui et al., 2024	Elliptic Curve Key Agreement	TA-controlled hierarchical trust	Trust and pseudonym evaluation	Yes - BAN logic proof	Session keys per domain handoff	Yes	Behavioral scoring + keying
Chen et al., 2024	None (physical-layer security)	Implicit via RFF	RFF uniqueness	Yes - spoofing	None (continuous auth)	Yes	No
Lin and Jhuang, 2024	Certificateless crypto, blockchain	Smart contract decentralized KGC	Certificateless ID, blockchain audit	Yes - session-state, forging	eCK-secure session keys	Yes	No
Xu et al., 2024	QC-MDPC, ICA-VSSI signal filtering	Quantum walk-based dynamic private keys	Pseudonyms + PHY preamble	Yes - quantum-secure, jamming	Bit-level BPSK modulated data	Yes	Yes (signal + quantum cryptography)
Li et al., 2023	ECC, bilinear maps	Digital twin-initiated key negotiation	Pseudonyms, encrypted channels	Yes - Replay, MITM, forging	Session key via DT pre-negotiation	Yes	Yes (Digital twin + ECC)
Anderson et al., 2023	TLS, encryption keys	Pre-configured during	Device fingerprinting	Yes - CAN injection,	Dynamic context-aware auth	Yes	Yes (contextual + ID)

		manufacturing		spoofing	sessions		
Cui et al., 2023	ECDLP, DBDH, ECC	TA-certified dynamic pseudonyms	Pseudonyms + session key rotation	Yes - eavesdropping, forging	Secure dynamic group key updates	Yes	Yes (cert + behavior)
Suo and Sarma, 2022	Digital certificates, PKI	Pre-installed certs from TA	LOS physical verification	Yes -Replay, MITM, spoofing	Ephemeral challenge-response sessions	Yes	Yes (LOS + certs)

Table S4.1(c) Performance Data of Papers on Authentication Security

Paper	Experimental Validation	Dataset Used	Tools	Latency	Scalability	Real-time Capability	Limitations	Future Work
Qiu et al., 2024	Yes	NIST automotive	GAN, CNN	Low	Moderate	Yes	Signal noise	Robust training
Du et al., 2024	Yes	Protocol simulation	Scyther	47.07 μs	High	Yes	No RSU fallback support	Generalizing to more dynamic V2X cases
Cui et al., 2024	Yes	Simulated IoV (NS3)	NS3, BAN logic	Low	Moderate	Yes	Edge-heavy overhead	Lightweight trust propagation methods
Chen et al., 2024	Yes (LTE-V2X lab trials)	LTE-V2X signal testbed	LS estimation, denoising	Low	High	Yes	High mobility noise sensitivity	Broader mobility and spectrum support
Lin and Jhuang, 2024	Yes (simulation and comparison)	None (simulated scenarios)	Blockchain, ECC, eCK model	Low	High	Yes	Simulation-based, no real deployment	Real-world deployment
Xu et al., 2024	Yes (BER, system failure rate)	Simulated platoon environments	Signal separation, QC-MDPC	Low	High	Yes	Complex Quantum requirement	Quantum resistance for 5G/6G
Li et al., 2023	Yes	Simulated 5G-V2X scenarios	Custom simulator, ECC tools	Very low	High	Yes	Cloud dependency	Lightweight DT optimization
Anderson et al., 2023	Yes	CAN bus simulator	ZT controller, policy manager	0.155 ms	Moderate	Yes	Static policy structure	Adaptive policy control
Cui et al., 2023	Yes	Simulated V2X group interaction	Group crypto framework	Low	High	Yes	Heavy TA dependency	TA decentralization, protocol tuning
Suo and Sarma, 2022	Yes	LOS/NLOS vehicular trials	Simulation tools, NLOS/LOS metrics	High	Moderate	Low	Communication bottleneck via LOS	Lightweight LOS tech, implicit certs

Table S4.1I(a) General Information of Papers on Sybil attack

Paper	Attack Vector	Targeted System	Adversary Model	Impact	Contribution	Key Findings	Limitations
Xu et al., 2024	Malicious access by Sybil identities	Access control in CAVs	Distributed Sybil attackers	Policy manipulation, unauthorized access	Novel trust-based access control using GRL for Sybil detection	GRL improves detection accuracy	Simulated scenarios, not real-world tested
Morton,	Multiple fake	VANET trust and GPS	Malicious entities with	Traffic misguidance,	Decentralized Sybil detection	Low latency Sybil	Simulation only, real-world

2024	identity generation	verification	spoofed identity clusters	network congestion	without central authority	detection	variability not tested
Zhu et al., 2024	Beacon packet manipulation	Vehicular communication trust layer	Malicious vehicles controlling Sybil beacons	False neighbor creation, traffic state spoofing	Simultaneous Sybil detection and traceability	Real-time traceability for resilience	RSU dependency
Tulay and Koksal, 2024	Identity spoofing via wireless signal	VANETs at intersections	Single vehicle with multiple identities	Network control, congestion manipulation	Hardware-free Sybil detection via CSI clustering	Effective under real word conditions	Performance in multipaths
Du et al., 2024	Sybil disruption in localization	Multi-vehicle source localization	Unbounded Sybil attackers	Localization errors, convergence failure	Gradient-free localization under Sybil attacks	Achieves source convergence	No real-world deployment yet
Rajendra et al., 2024	Multiple identity generation	VANET trajectory tracking	Vehicles with multiple OBUs	Traffic manipulation, consensus disruption	VDF-based tamper-proof trajectory Sybil detection	Improves over timestamp-only systems	Dependency on beaconing frequency
Noman and Atkison, 2023	Sybil attack and packet injection	VANET communication layers	Malicious spoofing tools	Traffic manipulation, message falsification	Unified detection and mitigation scheme	Trusted CA and key distribution	Performance cost

Table S4.1I(b) Technical Information of Papers on Sybil attack

Paper	Methodology	Defense Mechanisms	Detection Techniques	Tools	Future Directions	Targeted Channel	Security Objectives
Xu et al., 2024	Graph Reinforcement Learning	Trust-based access control	Trust evaluation via spatio-temporal graphs	DQN, STGCN, GNN frameworks	Real-world deployment and hybrid trust models	CAV Access Interfaces	Cn, In, Ac
Morton, 2024	TASER framework and directional antennas	Cumulative trust scoring and GPS verification	Trust evaluation + directional GPS validation	OMNeT++, SUMO, VEINS, TraCI	Adapt to real-world mixed traffic	V2V, GPS	In, Au, Ac
Zhu et al., 2024	Edge success probability via beacon key validation	RSU-coordinated identity challenge protocol	Graph-based neighbor analysis	Custom beacon protocol, RSU modules	Reduce RSU reliance, extend to platoons	Beacon channels (V2V, RSU)	In, Au, Ac
Tulay and Koksal, 2024	Signal clustering	Spatio-temporal signal analysis	K-means clustering on CSI	DSRC radios, urban ray-tracer	Integration with RSU and AI methods	V2V, V2I	In, Ac
Du et al., 2024	Trust-based resilient localization algorithm	Stochastic inter-agent trust model	Trust-weighted observations	Mathematical modeling, simulation	Deployable control protocols	Inter-vehicle	In, Au, Ac
Rajendra et al., 2024	Trajectory analysis Delay Functions	VDF chain with V2V + V2I interactions	Sybil trajectory similarity + interaction proof	VDF, RSUs, simulation environment	Real-world integration + lower latency VDFs	V2V, V2I	In, Au,Ac
Noman and Atkison, 2023	Attack and mitigation strategies	Radar verification, time stamping, trusted CA	Certificate-based trust validation	Radar systems, timestamping modules	Efficient cross-attack detection integration	V2V, V2I	In, Ac

Table S4.1I(c) Performance Data of Papers on Sybil attack

Paper	Detection Rate	FPR	Scalability of Attack	Scalability of Defense	Validation	Technique	Dataset	Real-Time Interference	Integrity Violation	Attack Duration	Encryption Bypass Techniques
Xu et al., 2024	Higher true rejection rate than DQN	-	High	Moderate	Yes	Simulated trust interaction graphs	Simulated	Yes	Yes	Persistent	Identity spoofing
Morton, 2024	High accuracy 30% malicious nodes	Low	Moderate	High	Yes	SUMO, OMNeT++, VEINS	Simulated	Yes	Yes	Short bursts	None
Zhu et al., 2024	98.11% (Sybil), 96.38%	Low	High	Moderate	Yes	Simulated CAV scenarios	Simulated	Yes	Yes	Persistent	Beacon spoofing
Tulay and Koksal, 2024	98% (real-world)	Low	Moderate	High	Yes	DSRC + ray-tracing sim data	Real-world, Simulated	Yes	Yes	Short to medium	Bypass via signal spoofing
Du et al., 2024	Precise convergence	-	High	High	Yes	Simulated data	Simulated	Yes	Yes	Persistent	Trust model circumvents need
Rajendra et al., 2024	High	Low	High	High	Yes	Simulated traffic + beacon data	Simulated	Yes	Yes	Sustained	Impersonation via OBU spoofing
Noman and Atkison, 2023	High	-	High	Moderate	No	-	N/A	Yes	Yes	Ongoing	Certificate spoofing, packet timing manipulation

Table S4.1II(a) General Information of Papers on Misbehavior Detection

Paper	Methodology	Misbehavior Type	Detection Approach	Detection Domain	Attack Vectors Covered	Anomaly vs Rule-based
Hu et al., 2025	LLM-based AV safety	NDD traffic sign, motion forgery	LLM-based analysis (LoRA, Adapters)	Perception + message validation	Image forgery, motion falsification	Anomaly-based
Campos et al., 2024	FL for misbehavior detection	Position spoofing and more (VeReMi)	MLP + FL with Fed+ and FedAvg	Distributed vehicular ML	Position falsification, spoofing	Anomaly-based
Abdullahi et al., 2024	Stacked meta-learning for robust MBS	DoS, Sybil, replay, speed/position falsification	Probabilistic models + CNN-LSTM meta learner	Cooperative driving V2X	Multiple (replay, Sybil, falsification)	Hybrid
Alladi et al., 2023	DL-based intrusion detection	18 types including DoS, replay, disruptive attacks	Deep Learning (CNN, LSTM)	Edge computing via RSUs	Position, speed falsification, DoS, replay	Anomaly-based
Kamel et al., 2020	Simulation Framework	Position spoofing, message inconsistency, various vehicular faults	Modular MBD simulation environment	Network and semantics-level V2X	Message tampering, delay, spoofing	Hybrid

Table S4.1II(b) General Information of Papers on Misbehavior Detection

Paper	Feature Type	Detection Algorithm	Trust Model	Communication Layer Monitored	Security Objectives

Hu et al., 2025	Traffic signs, motion data	LLMs with adapter	Hierarchical	Application	In
Campos et al., 2024	Position, velocity data	MLP, Fed+, FedAvg	Collaborative FL nodes	Network	In, Au, Ac, Pr
Abdullahi et al., 2024	BSMs, message semantics	Probabilistic + CNN-LSTM	RSU-localized validation	Application/Network	In
Alladi et al., 2023	Time-series vehicular communication data	DL Classification Engines (DLCEs)	Edge-trusted validation	Network/Transport	In
Kamel et al., 2020	V2X message semantics and vehicle kinematics	Plausibility checks, behavioral analysis, ML integration	Evidence-based with Misbehavior Authority (MA)	Application and network	In, Av

Table S4.1II(c) Performance Data ion of Papers on Misbehavior Detection

Paper	Validation	Dataset Used	Simulation/Testbed	Tools	Limitations	Future Work
Hu et al., 2025	Yes	Simulated traffic data	LLM model comparisons	ChatGPT, LLaMA, Gemini	High computational cost	Edge deployment
Campos et al., 2024	Yes	VeReMi + SMOTE-Tomek	Flower framework	MLP, Fed+ algorithm	Scalability not tested	Mobility-aware FL validation
Abdullahi et al., 2024	Yes	Vehicular dataset	Not specified	CNN, LSTM, probabilistic models	Overhead in inference	Dynamic traffic adaptation
Alladi et al., 2023	Yes	VeReMi Extension	Jetson Nano, Raspberry Pi	TensorFlow, Python DL	Not all attacks detected	Refining DL classification
Kamel et al., 2020	Yes	VeReMi	F2MD on VEINS, SUMO	OMNeT++, SUMO, VEINS	Simulation results only	Real-world validation