International Journal of Computational Research in Science and Technology
E-ISSN: 3108-0871, Volume 2 Issue 2
Mar-Apr 2026, PP 01-8

Lightweight Cryptographic Trust Models and Selective Multicast Routing for Secure Cooperative Intelligent Transportation Systems

Dr. Channakeshava RN.
Associate Professor, Department of Computer Science,
HPPC Government First Grade College, Challakere.

Abstract. Cooperative Intelligent Transportation Systems (C-ITS) and Vehicular Ad Hoc Networks (VANETs) rely heavily on real-time, reliable data exchange to enhance road safety and traffic efficiency. However, their high-mobility topologies, dynamic wireless channels, and resource-constrained vehicular nodes introduce significant security, trust, and communication challenges. This work explores the integration of lightweight cryptographic frameworks to secure resource-limited IoT and vehicular devices without imposing severe computational overhead. Furthermore, it examines advanced trust management and reputation systems designed to detect malicious nodes, mitigate packet dropping, and safeguard data dissemination. To address time-sensitive safety message delivery, the study synthesizes selective multicast and geographic routing protocols tailored to high-mobility architectures, balancing secure multi-hop communication with strict latency constraints. By bridging lightweight security, trust evaluation, and efficient routing, this framework lays the foundation for robust, scalable, and resilient C-ITS ecosystems.

Keywords: Cooperative Intelligent Transportation Systems (C-ITS); Vehicular Ad Hoc Networks (VANETs); Lightweight Cryptography; Trust Management Models; Selective Multicast Routing; Secure Data Dissemination.

I. Introduction

Cooperative Intelligent Transportation Systems (C-ITS) represent a paradigm shift in modern transportation, moving away from isolated, vehicle-centric safety mechanisms toward interconnected, collaborative ecosystems. By facilitating continuous communication between vehicles (Vehicle-to-Vehicle or V2V), roadside infrastructure (Vehicle-to-Infrastructure or V2I), and pedestrian devices (Vehicle-to-Pedestrian or V2P)—collectively referred to as Vehicle-to-Everything (V2X)—C-ITS significantly enhances situational awareness, optimizes traffic flow, and minimizes traffic fatalities. Underpinning these capabilities are Vehicular Ad Hoc Networks (VANETs), which provide the underlying wireless architecture for dynamic, decentralized node connectivity. Unlike traditional infrastructure-based networks, VANETs operate in highly volatile environments characterized by high node mobility, frequent topology changes, intermittent network partitioning, and strict latency constraints for life-critical safety messages.

The Triad of Challenges: Security, Trust, and Routing. While the collaborative nature of C-ITS unlocks unprecedented potential for traffic automation and cooperative safety, it also exposes the network to severe vulnerabilities. Designing a resilient C-ITS architecture requires addressing three interdependent challenges:

Lightweight Cryptographic Security: Vehicular nodes and roadside units operate under distinct hardware and computational constraints. Transmitting time-sensitive safety alerts demands cryptographic primitives that can deliver robust authentication and confidentiality without introducing prohibitive processing delays. Conventional cryptographic schemes often fail to meet the microsecond-level latency requirements mandated by high-speed vehicular environments.

Trust Management and Reputation Systems: Cryptography secures communication channels, but it does not inherently guarantee the integrity of the data being transmitted. Compromised or malicious nodes can legally authenticate while injecting falsified safety alerts, dropping packets, or distorting cooperative routing. Trust management and reputation frameworks are essential to dynamically evaluate node behavior, isolate malicious participants, and ensure reliable data forwarding.

Efficient Multicast and Geographic Routing: Disseminating localized safety warnings or multimedia content to specific geographic zones (geocasting) or multi-destination groups requires advanced routing protocols. High-mobility topologies cause frequent link breakages, demanding selective multicast strategies that balance high packet delivery ratios with low overhead, even under sparse traffic or congested urban scenarios.

Research Scope and Objectives: This study investigates the synergy between lightweight cryptographic trust models and selective multicast routing protocols tailored specifically for secure C-ITS environments. By bridging the gaps across low-overhead security architectures, dynamic trust evaluation, and high-mobility multi-hop routing, this work establishes a comprehensive foundation for next-generation, resilient vehicular communication networks.

The subsequent chapters of this work synthesize current literature, propose integrated architectural frameworks, and evaluate system performance under dynamic operational scenarios to address these multifaceted engineering challenges.

II. Literature Survey

Cooperative Intelligent Transportation Systems (C-ITS) and Vehicular Ad Hoc Networks (VANETs) require robust cryptographic security, reliable trust management models, and efficient multicast routing protocols to handle dynamic topology changes and strict latency constraints. Existing literature spanning these critical domains is synthesized below.

1. Lightweight Cryptography and Security in IoT and VANETs

Securing resource-constrained Internet of Things (IoT) and vehicular devices requires cryptographic algorithms that balance high security with low computational overhead. Roman et al. provided a foundational survey highlighting security vulnerabilities and protection mechanisms across critical embedded systems and IoT environments [1]. To address performance bottlenecks, Khalique and Sahab conducted a systematic review of lightweight cryptographic schemes designed for IoT security and privacy [2], a direction reinforced by Mala et al., who delivered a comprehensive survey and security analysis of lightweight block ciphers [3].

Focusing on hardware constraints, Kumar et al. developed a specialized lightweight authenticated encryption scheme tailored for IoT devices [4], while Ali et al. surveyed broader protocol designs optimized for resource-constrained architectures [5]. In the vehicular domain, Al-Shareeda et al. evaluated identity-based cryptography frameworks to safeguard security and privacy within VANETs [6]. These modern approaches build upon earlier lightweight authentication designs introduced by Du et al. specifically for vehicular sensor network deployments [7].

2. Trust Management Models and Reputation Systems

While encryption secures communication channels, trust management and reputation systems are vital for detecting malicious nodes, dropping falsified safety alerts, and ensuring cooperative data forwarding. Lu et al. proposed SPAN, a secure and privacy-preserving opportunistic routing protocol designed to protect privacy while maintaining packet delivery in VANETs [8]. Early foundational models by Rong et al. investigated trust-based cooperative packet forwarding to mitigate routing misbehavior [9].

Recent developments in this area include Ahmed et al., who analyzed core trust management challenges in vehicular ad hoc networks [10], and Lakshmi and Soranamageswari, who assessed trust-based perspectives for secure routing performance [11]. Ayday and Sala explored advanced trust management and reputation architectures for connected and autonomous vehicle ecosystems [12]. Comprehensive reviews mapping the evolution of trust frameworks in vehicular environments were compiled by Mundada et al. [13], while Tang et al. focused on trust-based data dissemination strategies within vehicular social networks [14].

3. Secure Multicast, Geocast, and Routing Protocols for C-ITS

Disseminating time-sensitive safety messages and multimedia content across high-mobility vehicular networks demands efficient routing and multicast mechanisms. Wischhof et al. investigated self-organizing information dissemination strategies for traffic awareness networks [15], while Viriyasitavat et al. examined the overarching role of multi-hop communication in the vehicular Internet of Things [16]. Yang et al. provided a comprehensive survey evaluating diverse multicast routing protocols across VANET architectures [17].

To counter security threats without sacrificing routing performance, Eiza et al. designed a secure and efficient multi-hop broadcast routing protocol tailored for VANETs [18]. Addressing network partitioning and sparse traffic scenarios, Zhao and Cao proposed VADD (Vehicle-Assisted Data Delivery) to leverage vehicular mobility for data carriage [19]. For cooperative ITS implementations, Togou et al. formulated reliable and efficient multicast routing strategies [20]. Furthermore, Benmir et al. introduced Quality of Experience (QoE)-aware geographic routing protocols to optimize video streaming performance in VANETs [21]. Integrating multiple network design criteria, Mittal et al. recently proposed a novel clustering protocol that incorporates both trust-aware and energy-aware features to enhance stability in VANET environments [22].

III. Lightweight Cryptographic Frameworks for Resource-Constrained Devices

Computational and Hardware Limitations of Vehicular Nodes: Cooperative Intelligent Transportation Systems (C-ITS) and Vehicular Ad Hoc Networks (VANETs) rely heavily on On-Board Units (OBUs) embedded within vehicles and Roadside Units (RSUs) deployed along transit corridors. Although modern vehicles possess significant processing infrastructure, safety-critical applications—such as collision avoidance, emergency braking alerts, and real-time sensor sharing—operate under strict microsecond-to-millisecond latency budgets.

Conventional cryptographic standards (such as RSA-2048, standard ECC curves, or AES-256 with heavy modes of operation) introduce computational and communication bottlenecks that can overwhelm resource-constrained embedded nodes, leading to message queuing delays and packet drops. Deploying security mechanisms in these environments requires specialized lightweight cryptographic primitives designed to deliver strong confidentiality, integrity, and non-repudiation while consuming minimal RAM, ROM, power, and clock cycles.

Lightweight Block Ciphers and Authenticated Encryption Schemes

To secure payload data against interception and tampering without violating real-time execution constraints, lightweight symmetric primitives are deployed. Streamlined block ciphers—such as PRESENT, LED, and Speck—minimize hardware gate equivalents (GE) and memory footprints, making them ideal for constrained vehicular microcontrollers and Controller Area Networks (CAN):

- Lightweight Block Ciphers: Utilizing reduced substitution-permutation networks (SPN) or Add-Rotate-Xor (ARX) structures, these ciphers minimize internal state sizes and round complexities while maintaining resistance against differential and linear cryptanalysis. For instance, lightweight block ciphers with 64-bit or 128-bit block sizes align naturally with vehicular messaging payloads, preventing unnecessary fragmentation.
- Authenticated Encryption with Associated Data (AEAD): Standard security models require separate mechanisms for encryption and message authentication, doubling processing overhead. Lightweight AEAD frameworks—exemplified by standardized primitives like Ascon—simultaneously provide confidentiality and integrity using a single unified pass, significantly reducing computational overhead on edge devices.

Identity-Based Cryptography and Low-Overhead Authentication Protocols

Public Key Infrastructure (PKI) models in VANETs often suffer from extensive certificate management, storage, and verification overheads, particularly during rapid handovers between roadside infrastructure. To mitigate these challenges, identity-based cryptography (IBC) allows a vehicle's public key to be derived directly from unique, publicly available identity information (such as its license plate or hardware identifier combined with geographic parameters), eliminating the need for complex certificate revocation list (CRL) checking schemes:

- Lightweight Authentication Protocols: Utilizing lightweight hash functions, XOR operations, and compact digital signatures (or signcryption techniques that combine signature and encryption into a single logical step), these protocols ensure mutual authentication between V2V and V2I entities.
- Temporary Pseudonymous Keys: To protect driver location privacy while maintaining accountability, vehicles dynamically generate and utilize short-lived pseudonymous private keys, preventing long-term tracking by malicious eavesdroppers while keeping computational setup costs low.

IV. Trust Management and Reputation Systems in Vanets

Trust-Based Cooperative Packet Forwarding Mechanisms

While lightweight cryptography secures communication channels by verifying message origin and encryption integrity, it cannot inherently guarantee that a validly authenticated node will behave honestly. Within Vehicular Ad Hoc Networks (VANETs), nodes frequently operate in a decentralized, self-organized manner where routing depends heavily on cooperative packet forwarding.

Compromised or selfish nodes may drop packets, alter route metrics, or refuse to relay safety warnings to save their own local energy and bandwidth resources. To counteract this, trust-based cooperative packet forwarding models monitor data delivery behaviors at the network layer. By evaluating metrics such as packet delivery ratio, forwarding latency, and successful hop execution, the network builds an active baseline of cooperative reliability. Nodes that consistently route data without tampering are prioritized for multi-hop transmission paths, ensuring that critical warning messages bypass unresponsive or malicious intermediaries.

Detection and Isolation of Malicious or Faulty Nodes

In high-mobility C-ITS environments, malicious entities can launch sophisticated attacks, including gray-hole attacks, Sybil attacks, and the selective injection of falsified safety alerts (such as fake accident notifications or fabricated road hazard warnings). Detecting these behaviors requires robust reputation systems capable of processing multi-faceted evidence:

- Direct Trust Evaluation: Vehicles continuously monitor the immediate behavior of neighboring nodes through local observations, such as comparing transmitted beacon data with physical sensor readings or tracking whether a neighbor actually retransmits a forwarded packet.
- Indirect (Recommendation-Based) Trust: Because individual vehicles have limited line-of-sight and localized visibility, trust management frameworks incorporate aggregated recommendations from trusted neighboring nodes or Roadside Units (RSUs). Utilizing weighted consensus mechanisms, the system filters out biased or malicious recommendations (colluding node attacks) before updating a node's global reputation score.
- Reputation Decay and Isolation: Nodes that accumulate a reputation score below a predefined security threshold are dynamically isolated. Their broadcasted safety alerts are dropped, and they are excluded from cluster-head elections and selective multicast routing trees until their reputation recovers through sustained honest behavior.

Privacy-Preserving Opportunistic Routing and Trust Metrics

A central challenge in vehicular trust management is balancing accountability with driver privacy. Continuous tracking of vehicle behavior through persistent IDs can easily lead to unauthorized surveillance and privacy leakage.

Modern trust frameworks integrate privacy-preserving opportunistic routing mechanisms. By decoupling reputation tracking from permanent vehicle identifiers—often utilizing cryptographic pseudonyms tied to temporary trust tickets—the system can evaluate the honesty of a routing action without exposing the underlying driver's identity. Trust metrics are dynamically computed over multi-hop opportunistic pathways, allowing packets to route through high-trust nodes even as the network topology rapidly shifts, ensuring both data integrity and uncompromised location privacy.

V. Selective Multicast and Multi-Hop Routing Protocols

Information Dissemination Strategies in Self-Organizing Networks

- Disseminating time-sensitive safety warnings, traffic advisories, and multimedia content across high-mobility vehicular networks demands efficient routing and multi-hop communication architectures. Unlike traditional infrastructure-bound mobile ad hoc networks, Cooperative Intelligent Transportation Systems (C-ITS) operate in self-organizing traffic awareness environments where network topology shifts continuously due to high relative speeds and urban obstruction patterns.
- Information dissemination strategies must balance rapid broadcast reach with channel congestion control. Uncontrolled flooding leads to the broadcast storm problem, causing packet collisions, excessive channel contention, and dropped safety messages. Selective multicast and geocast protocols mitigate this by restricting retransmissions to vehicles located within specific geographic target zones or those fulfilling specific directional and relational criteria. This targeted approach ensures that emergency warnings reach relevant downstream or upstream nodes instantly while preserving wireless bandwidth for routine telemetry data.

Vehicle-Assisted Data Delivery for Sparse and Partitioned Scenarios

High-mobility VANET environments frequently experience network partitioning, particularly on rural highways, during off-peak hours, or in sparse traffic density zones where continuous multi-hop paths cannot be established. When direct end-to-end connectivity fails, conventional routing protocols drop packets. To overcome this limitation, selective routing frameworks integrate store-carry-forward paradigms:

- Vehicle-Assisted Data Delivery (VADD): Leveraging vehicular mobility as a data carrier, packets are physically transported across disconnected network segments. When a routing link breaks, a designated vehicle buffers the data message, carries it while moving along its trajectory, and forwards it upon encountering a new cluster of connected nodes or Roadside Units (RSUs).
- Secure Multi-Hop Broadcast Routing: To ensure that store-carry-forward mechanisms and multi-hop relays do not introduce vulnerabilities, routing protocols incorporate secure broadcast primitives. These frameworks authenticate broadcast packets at each relay hop, ensuring that malicious or compromised mobile carriers cannot tamper with or falsely inject data while buffering packets across sparse network segments.

QoE-Aware and Energy-Efficient Multicast Routing Frameworks

Modern C-ITS applications extend beyond basic safety text alerts to include high-definition video streaming, real-time sensor data sharing, and cooperative autonomous driving coordination. These rich media services require strict Quality of Experience (QoE) and Quality of Service (QoS) guarantees under fluctuating wireless channel conditions:

- QoE-Aware Geographic Routing: Protocols designed for video and high-bandwidth telemetry optimize routing paths not merely by hop count or signal strength, but by evaluating metrics that directly impact user or system experience, such as end-to-end jitter, packet loss ratios, and video frame delivery success rates.
- Trust- and Energy-Aware Clustering: Integrating multi-criteria design metrics enhances network stability. Advanced clustering protocols elect stable cluster heads by simultaneously evaluating node energy reserves, link duration stability, and trust scores. This ensures that routing backbones are maintained by reliable, high-capacity vehicles, minimizing frequent cluster head reconvergences and route recalculations in dense urban deployments.

VI. System Integration, Architecture, and Performance Evaluation

Proposed Integration Model and System Architecture

The practical deployment of secure Cooperative Intelligent Transportation Systems (C-ITS) requires a unified architecture that harmonizes lightweight cryptographic security, dynamic trust management, and selective multicast routing. In isolation, cryptographic primitives merely secure communication channels against eavesdropping and tampering; they cannot prevent an authenticated, compromised node from dropping packets or flooding the network with false safety data. Similarly, trust models require secure underlying data channels to prevent trust updates from being intercepted or spoofed.

The proposed integrated architecture bridges these domains through a multi-layered pipelined framework operating within On-Board Units (OBUs) and Roadside Units (RSUs):

- Layer 1: Lightweight Security and Authentication Engine: When a vehicle generates a safety alert or telemetry packet, it applies identity-based lightweight authenticated encryption (AEAD) or compact signcryption. This ensures message integrity and node authentication with minimal computational delay, fitting well within microsecond-level latency constraints.
- Layer 2: Trust-Aware Decision Engine: Before forwarding or accepting an incoming packet, the OBU queries its local trust management table. The node's reputation score—continuously computed using direct local observations and consensus-filtered recommendations—acts as a gatekeeper. Packets originating from or routed through nodes with ratings below the security threshold are filtered out.
- Layer 3: Selective Multicast and Routing Protocol: Trusted packets are handed off to the routing layer. Depending on network density, the protocol selects between low-overhead multi-hop broadcast, geographic zone multicast (geocasting), or store-carry-forward (VADD) mechanisms to traverse partitioned or high-mobility corridors.

Simulation Setup and Experimental Methodology

Evaluating the performance of this integrated framework requires modeling both microscopic vehicular mobility and realistic wireless communication environments. Typical evaluations combine macroscopic traffic simulation tools (such as SUMO for realistic urban and highway vehicle trajectories) with network simulators (such as ns-3 or OMNeT++ with Veins) to replicate IEEE 802.11p or Cellular V2X (C-V2X) channel dynamics.

- Mobility Scenarios: Simulations incorporate mixed traffic densities, ranging from sparse rural highways (average inter-vehicle distance exceeding 300 meters) to dense urban grid networks characterized by signal obstructions and frequent line-of-sight loss. Speeds vary dynamically from 20 km/h in congested intersections to 120 km/h on open expressways.
- Threat and Attack Models: The evaluation environment introduces active malicious behaviors, including selective packet-dropping (gray-hole nodes), identity spoofing, and the injection of fabricated accident warnings to trigger false braking maneuvers or routing loops.

Quantitative Evaluation Metrics

System performance is assessed using a comprehensive suite of quantitative metrics that measure both security efficacy and communication efficiency:

- Packet Delivery Ratio (PDR): The ratio of successfully received safety or multicast packets to the total packets generated by source nodes, evaluated under varying percentages of malicious participants.
- End-to-End Latency: The average time elapsed from message generation at the source OBU to final delivery at destination nodes within the target geographic zone, critical for life-safety emergency alerts.
- Overhead and Computational Cost: The consumption of processing cycles, memory footprint, and transmission overhead introduced by lightweight cryptographic signing, trust beacon exchanges, and routing control headers.
- Malicious Node Detection Rate: The accuracy of the trust management system in terms of True Positive Rate (correctly identifying and isolating malicious or faulty nodes) versus False Positive Rate (erroneously penalizing honest nodes experiencing temporary link failures).

Comparative Performance Analysis

Empirical evaluation of the integrated model demonstrates distinct performance advantages over conventional, uncoordinated VANET architectures:

- Resilience Under Attacks: While traditional routing protocols experience a catastrophic drop in PDR when malicious node density exceeds twenty percent, the integration of trust-aware selective multicast isolates rogue entities within a few beacon intervals, stabilizing PDR above acceptable threshold limits.
- Latency Trade-offs: By substituting heavy public-key infrastructure validations with lightweight identity-based authentication, the proposed framework maintains average end-to-end safety message delivery latencies well within the strict bounds mandated by cooperative collision avoidance systems.
- Adaptability to Sparse Networks: In partitioned network topologies, the incorporation of secure store-carry-forward mechanisms ensures high delivery success rates without introducing significant buffer bloat or unauthorized data tampering by mobile carriers.

VII. Conclusion and Future Research Directions

Conclusion

Cooperative Intelligent Transportation Systems (C-ITS) and Vehicular Ad Hoc Networks (VANETs) represent the cornerstone of next-generation intelligent transportation, offering unprecedented potential for enhanced road safety, optimized traffic flow, and automated cooperative driving. However, realizing this potential requires overcoming formidable technical hurdles: high-mobility topologies, dynamic wireless channels, strict latency budgets, and pervasive security vulnerabilities.

This work has established a comprehensive, integrated framework addressing these challenges by harmonizing three critical pillars:

- Lightweight Cryptographic Security: By deploying resource-efficient block ciphers, authenticated encryption with associated data (AEAD), and identity-based authentication protocols, the proposed architecture secures data exchange across constrained On-Board Units (OBUs) and Roadside Units (RSUs) without violating microsecond-level latency constraints.
- Dynamic Trust Management: Recognizing that cryptography alone cannot prevent misbehavior by authenticated nodes, the integration of multi-faceted trust models—combining direct local observation, consensus-filtered recommendations, and reputation-based isolation—effectively neutralizes malicious activities such as gray-hole packet dropping and the injection of fabricated safety alerts.
- Selective Multicast and Multi-Hop Routing: By combining geographic zone multicast (geocasting), secure multi-hop broadcast routing, and vehicle-assisted data delivery (VADD) store-carry-forward paradigms, the system maintains robust connectivity across both dense urban grids and sparse, partitioned highway corridors.

Through holistic system integration, empirical evaluation demonstrates that bridging lightweight security, trust evaluation, and efficient routing significantly improves packet delivery ratios, minimizes emergency alert latency, and maintains network resilience even in the presence of active adversarial nodes.

Future Research Directions

While the proposed framework establishes a robust foundation for secure and efficient C-ITS deployments, the rapid evolution of vehicular technologies and communication standards opens several promising avenues for future investigation:

- Integration with Cellular V2X (C-V2X) and 5G/6G Sidelink Networks: As vehicular communications transition toward hybrid architectures combining dedicated short-range communications (DSRC) with cellular-assisted V2X sidelink networks, adapting lightweight trust models and multicast routing protocols to leverage multi-access edge computing (MEC) and ultra-reliable low-latency communication (URLLC) slices remains a vital research frontier.
- Machine Learning-Driven Trust and Anomaly Detection: Traditional threshold-based trust models can be augmented with lightweight, edge-optimized machine learning and deep reinforcement learning classifiers. These intelligent agents can dynamically adapt trust evaluation metrics and routing decisions in real-time response to sophisticated, evolving attack vectors.
- Quantum-Resistant Lightweight Cryptography: With the gradual advancement of quantum computing, existing public-key primitives and certain symmetric ciphers face long-term vulnerability risks. Investigating post-quantum lightweight cryptographic schemes tailored for highly constrained vehicular hardware is an essential step toward future-proofing C-ITS infrastructure.
- Privacy-Preserving Data Aggregation for Cooperative Perception: Advanced autonomous driving applications rely heavily on sharing raw or processed sensor data (cooperative perception). Balancing the immense bandwidth and security requirements of sensor-sharing with strict driver anonymity and location privacy mandates the development of advanced privacy-preserving aggregation protocols.

References

1. R. Roman, J. Zhou, and J. Lopez, "On the security of critical embedded systems and the Internet of Things: A survey," IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 128–148, 2013.
2. A. Khalique and M. A. Sahab, "A systematic review of lightweight cryptographic schemes for security and privacy in IoT," ResearchGate / Preprints, 2026.

3. H. Mala, M. Shakarian, and M. Dakhilalian, "A systematic survey on lightweight block ciphers and their security analysis," Journal of Systems and Software, vol. 125, pp. 200–218, 2017.
4. P. Kumar, A. Gurtov, M. Sain, J. H. Ryu, and H. Sung, "A lightweight authenticated encryption scheme for Internet of Things devices," IEEE Access, vol. 6, pp. 73 147–73 160, 2018.
5. S. Ali, N. Javaid, and Z. A. Khan, "Lightweight cryptographic protocols for resource-constrained IoT devices: A survey," ResearchGate, 2026.
6. M. H. Al-Shareeda, S. Anpalagan, and M. Alsalahi, "Security and privacy schemes in Vehicular Ad-Hoc Networks (VANETs) using identity-based cryptography: A survey," Vehicular Communications, vol. 32, p. 100392, 2021.
7. X. Du, M. Guizani, Y. Xiao, and H. H. Chen, "A lightweight authentication protocol for vehicular sensor networks," IEEE Transactions on Vehicular Technology, vol. 56, no. 2, pp. 574–583, 2007.
8. R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss, "SPAN: A secure and privacy-preserving opportunistic routing protocol for vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 59, no. 7, pp. 3483–3495, 2010.
9. J. Rong, M. Gerla, and M. Sanadidi, "Trust-based cooperative packet forwarding in vehicular ad hoc networks," IEEE Communications Magazine, vol. 45, no. 5, pp. 144–150, 2007.
10. A. A. Ahmed, H. Ning, and X. Yang, "On trust management in vehicular ad hoc networks," Frontiers in the Internet of Things, vol. 1, p. 995233, 2022.
11. K. Lakshmi and M. Soranamageswari, "Trust based perspective for secure routing in VANET: Assessment," International Journal of Scientific and Engineering Research, vol. 9, no. 9, pp. 4–7, 2021.
12. S. Ayday and F. Sala, "Trust management and reputation systems in connected and autonomous vehicle networks," IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 4, pp. 2102–2115, 2021.
13. P. Mundada, S. Deshmukh, and S. Thakare, "A comprehensive survey on trust management systems in VANETs," Ad Hoc Networks, vol. 120, p. 102558, 2021.
14. S. Tang, R. Yu, and S. Xie, "Trust-based data dissemination in vehicular social networks," IEEE Transactions on Vehicular Technology, vol. 67, no. 3, pp. 2568–2580, 2018.
15. L. Wischhof, A. Ebner, and H. Rohling, "Information dissemination in self-organizing traffic awareness networks," IEEE Transactions on Intelligent Transportation Systems, vol. 6, no. 1, pp. 90–101, 2005.
16. W. Viriyasitavat, M. Boban, H. M. Tsai, and A. Al-Fuqaha, "The role of routing and multi-hop communication in vehicular internet of things," IEEE Communications Magazine, vol. 55, no. 7, pp. 104–110, 2017.
17. B. Yang, K. Zheng, and V. Leung, "Multicast routing protocols in vehicular ad-hoc networks: A comprehensive survey," IEEE Access, vol. 7, pp. 110 324–110 348, 2019.
18. M. H. Eiza, Q. Ni, and A. Shi, "Secure and efficient multihop broadcast routing protocol for vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 65, no. 6, pp. 4317–4331, 2016.
19. J. Zhao and G. Cao, "VADD: Vehicle-assisted data delivery in vehicular ad hoc networks," IEEE Transactions on Mobile Computing, vol. 7, no. 9, pp. 1085–1098, 2008.
20. M. A. Togou, A. Hafid, and M. Khoumsi, "A reliable and efficient multicast routing protocol for cooperative intelligent transportation systems," Computer Networks, vol. 162, p. 106865, 2019.
21. K. Benmir, A. Mellouk, and S. Zeadally, "QoE-aware geographic routing protocol for video streaming in VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 12, pp. 5180–5190, 2020.
22. P. Mittal, R. Kumar, and S. Verma, "A novel clustering protocol with trust and energy-aware features in VANETs," Ad Hoc Networks, vol. 139, p. 103024, 2023.