Journal of Humanitarian and Applied Sciences - مجلة العلوم الإنسانية والتطبيقية
(رقم الإيداع المحلي 90-2020)
كلية الآداب والعلوم قصر خيار -جامعة المرقب

Vehicular Ad-Hoc Networks (VANETs): Foundations, Comparative Protocol Analysis and Emerging Technologies

Emadeddin A. M. Gamati

Associate Professor, Faculty of Education, Department of Computer Science Tripoli University.

e.gamati@uot.edu.ly

Omar Abdulmola Abusaeeda

Associate Professor , Faculty of Information Technology, Department of Computer Science Tripoli University

omar.abusaeeda@uot.edu.ly

Received: 3/11/2025 | Accepted:20/11/2025

Abstract

Vehicular Ad-Hoc Networks (VANETs) constitute a specialized sub-class of Mobile Ad-Hoc Networks (MANETs) tailored for high-mobility vehicular environments, and serve as a critical enabler of intelligent transportation systems (ITS). This survey presents (Al-Sultan et al., 2014) the architectural and characteristic foundations of VANETs; (Hartenstein & Laberteaux, 2010) a systematic, comparative analysis of routing and dissemination protocol classes-including recent advancements incorporating machine learning, Software-Defined Networking (SDN) and edge-computing paradigms; and (Routing Protocols…, 2023) an overview of emerging technologies shaping VANET evolution, such as federated learning, digital twins, 5G/6G V2X, and trust-based security frameworks. Through objective evaluation across metrics such as packet delivery ratio, latency, scalability, overhead and adaptability, the paper identifies current limitations and sets out a roadmap toward next-generation AI-driven, data-centric vehicular communication networks.

Keywords—VANET, V2V, V2I, V2X, ITS, SDN.

شبكات المركبات المخصصة (VANETs): الأسس، وتحليل البروتوكولات المقارن، والتقنيات الناشئة

د. عماد الدين أحمد محمد القماطي

أستاذ مشارك، جامعة طرابلس، كلية التربية، قسم علوم الحاسوب

e.gamati@uot.edu.ly

د. عمر عبد المولى أبو سعدة

أستاذ مشارك، جامعة طرابلس، كلية تقنية المعلومات، *قسم علوم الحاسوب*

omar.abusaeeda@uot.edu.ly

الملخـص

تُعدّ الشبكات المخصّصة للمركبات (VANETs) فرعًا متخصصًا من الشبكات المتنقلة ذاتية التنظيم(MANETs)، تم تصميمه خصيصًا لبيئات المركبات عالية الحركة، وتُعتبر عنصرًا أساسيًا في تمكين أنظمة النقل الذكية (ITS). يستعرض هذا البحث: (Al-Sultan et al., 2014) الأسس المعمارية والخصائص المميزة لشبكاتVANET ؛ (Hartenstein & Laberteaux, 2010) تحليلًا منهجيًا مقارنًا لفئات بروتوكولات التوجيه ونشر البيانات، بما في ذلك التطورات الحديثة التي تعتمد على تقنيات التعلّم الآلي، والشبكات المعرفة برمجيًا(SDN) ، والحوسبة الطرفية(Edge Computing) ؛ و(Routing Protocols…, 2023) عرضًا لأبرز التقنيات الناشئة التي تشكل مستقبل تطور شبكاتVANET ، مثل التعلّم الاتحادي(Federated Learning) ، والتوائم الرقمية(Digital Twins) ، وتقنيات الاتصالات 5G/6G

V2X، وأطر الأمان القائمة على الثقة. ومن خلال تقييم موضوعي وفق مؤشرات الأداء مثل معدل تسليم الحزم، وزمن التأخير، وقابلية التوسع، والعبء الزائد، والقدرة على التكيّف، يحدد البحث التحديات الحالية ويقترح خارطة طريق نحو الجيل القادم من شبكات الاتصالات الذكية للمركبات المعتمدة على الذكاء الاصطناعي والمتمحورة حول البيانات.

الكلمات المفتاحية:VANET, الاتصال V2V، الاتصال V2I، الاتصال V2X.

I. Introduction

Connected and automated vehicles, combined with advanced roadside infrastructure and pervasive sensing, are transforming modern transportation into an intelligent, cooperative ecosystem. Within this paradigm, Vehicular Ad-Hoc Networks (VANETs) enable wireless communication between vehicles (Vehicle-to-Vehicle, V2V) and between vehicles and infrastructure (Vehicle-to-Infrastructure, V2I) thereby facilitating real-time safety alerts, traffic-flow optimization, infotainment services, and cooperative autonomous driving. Unlike generic MANETs, VANETs deal with extremely high node mobility, frequent topology changes, variable node densities (ranging from sparse highways to dense urban grids), and strict latency, reliability and coverage demands.

The progression of wireless communication technologies (IEEE 802.11p, DSRC, C-V2X, 5G/6G) and increasing interest in smart mobility have driven VANET research from protocol design toward data-centric, intelligence-driven systems. This paper delivers: (i) a foundational overview of VANET architecture and characterizing features; (ii) a comparative taxonomy and evaluation of routing/dissemination protocols, including recent machine-learning/AI-enabled approaches; and (iii) a review of emerging technologies and the research agenda for future vehicular networks. The remainder of the paper is structured as follows: Section II covers architecture and characteristics; Section III presents routing protocol taxonomy and comparative analysis; Section IV discusses emerging trends and technologies; Section V offers an extended discussion of research gaps and future directions; Section VI concludes.

II. VANET Architecture and Characteristic Features

A. Architectural Layers

VANETs typically adopt a layered design comprising: (Al-Sultan et al., 2014) the **application layer**, delivering ITS services such as collision avoidance, dynamic navigation, infotainment and cooperative driving; (Hartenstein & Laberteaux, 2010) the **network/transport layer**, responsible for routing, forwarding, quality-of-service (QoS) and link management; and (Routing Protocols…, 2023) the **physical/MAC layer**, implementing wireless access technologies (e.g., IEEE 802.11p/WAVE, DSRC, C-V2X, LTE/5G) and handling channel access, interference, and link adaptation.

Key network entities include On-Board Units (OBUs) embedded in vehicles, Roadside Units (RSUs) positioned along infrastructure, Application Units (AUs) for ITS services, and backend cloud/edge controllers providing processing, storage and orchestration functionalities.

B. Communication Modes: V2V, V2I, V2X

- **V2V** (Vehicle-to-Vehicle): direct wireless links among vehicles typically using short-range communication (e.g., 802.11p).
- **V2I** (Vehicle-to-Infrastructure): vehicles exchange data with fixed RSUs or traffic control units for broader connectivity, updates and cloud access.

- **V2X** (Vehicle-to-Everything): extends beyond V2V/V2I to include Vehicle-to-Pedestrian (V2P), Vehicle-to-Network (V2N) and Vehicle-to-Device (V2D) communications, enabling integration into Internet of Vehicles (IoV) ecosystems.

C. Distinctive VANET Characteristics and Implications

VANETs differ from traditional ad-hoc networks in several respects:

- **High mobility and rapid topology changes**, resulting in short link durations and transient connectivity.
- **Variable node densities**: from sparse highway scenarios (low vehicle count) to dense urban traffic (high congestion, high interference).
- **Predictable yet constrained mobility**: vehicles move along roads, lanes and intersections, enabling mobility modelling but also imposing constraints.
- **Heterogeneous application demands**: safety messages (highest priority, stringent latency), traffic management, infotainment, which differ in QoS and routing requirements.
- **Power and resource environment**: compared to wearable or handheld nodes, vehicles can provide stable power but also face constraints in terms of cost, hardware, and ruggedness for on-board computation.

These characteristics impose challenging requirements on routing protocols (low latency, high delivery ratio, scalability), link management (frequent breakage, fragmentation) and network architectures (heterogeneous technologies, cross-layer optimizations).

III. Routing and Data Dissemination Protocols: Comparative Analysis

A. Taxonomy of Protocol Classes

Routing and dissemination methods in VANETs can be broadly categorized into:

1. **Topology-based protocols** (e.g., AODV, DSR) which maintain routes via link state or distance-vector mechanisms but tend to struggle in high-mobility VANETs. In these protocols, routes are discovered on demand or maintained proactively through periodic control messages. While they are conceptually simple and well understood from MANET literature, frequent topology changes in vehicular environments cause route breaks, leading to high control overhead and increased end-to-end delay, especially in dense or fast-moving scenarios.

2. **Position/Geographic-based protocols** (e.g., GPSR, GPCR) leveraging location (via GPS) to make forwarding decisions, thus better suited to vehicular mobility patterns. Nodes forward packets greedily toward the geographic position of the destination or an intermediate anchor, avoiding the need for global route discovery. These schemes scale well with node density and mobility, but they rely on accurate positioning and may suffer from local maxima (void problem) in sparse road segments or obstructed urban canyons.

3. **Cluster/Hybrid protocols** that combine clustering of vehicles (to improve stability) with geographic information and topology awareness, aiming to balance overhead and resilience. Vehicles are grouped into clusters, each managed by a cluster head responsible for intra- and inter-cluster communication. This structure reduces routing state and isolates local dynamics, but cluster formation and maintenance introduce extra signaling and may become complex under rapidly changing densities and speeds.

4. **Broadcast/Geocast and safety dissemination strategies** designed specifically for safety message propagation with low latency (e.g., multi-hop broadcast with reliability guarantees). These protocols focus on efficient dissemination of periodic beacons and event-driven alerts to vehicles inside a geographical region of interest. Techniques such as probabilistic rebroadcast, suppression timers, and direction-aware forwarding are used to mitigate broadcast storms while preserving high reachability for time-critical safety notifications.
5. **Intelligent/Adaptive protocols** leveraging machine learning (ML), deep learning (DL), reinforcement learning (RL) or SDN control to dynamically adapt routing/forwarding rules to context (vehicle density, mobility, link quality). Such schemes can learn optimal forwarding decisions, predict link lifetime, or reconfigure paths using global network views provided by SDN controllers. Although they offer improved performance and robustness, they require training data, computational resources, and careful design to meet real-time constraints in highly dynamic vehicular environments.

B. Comparative Metrics and Evaluation Criteria

Key metrics for comparing protocols include:

- Packet Delivery Ratio (PDR)
- End-to-End Delay (latency)
- Routing/Forwarding Overhead
- Link Stability / Route-Repair Frequency
- Scalability (node count, vehicle density)
- Adaptability to mobility and topology variation
- Suitability for different application types (safety vs. infotainment)

C. Recent Developments and Enhancements

Position-based protocols remain dominant due to their scalability in dynamic environments, but recent enhancements have incorporated link-lifetime awareness, trajectory prediction and connectivity duration estimation. For instance, advanced protocols integrate ML-based link estimation or mobility prediction to improve forwarding decisions (HaghighiFard & Coleri, 2024; Yigit et al., 2024; "Lightweight machine learning model to detect VANET attacks," 2024). Hybrid and cluster-based approaches are increasingly used in dense urban deployments, where vehicle clusters and RSU coordination reduce route breakage and delay.

Intelligent routing protocols (e.g., ANN-based secure routing ("Lightweight machine learning model to detect VANET attacks," 2024)) have been proposed to mitigate malicious nodes, dynamically predict best paths and incorporate security/trust metrics. These reflect a shift toward context-aware and adaptive vehicular networks.

D. Comparative Table Summary

Protocol Class	Strengths	Weaknesses	Best-Use Scenario
Topology-based	Well-understood, simple implementation	High overhead, fragile under high mobility	Low/moderate mobility environments
Position/Geographic	Low overhead, adapted to mobility	Requires accurate location; void problem in sparse areas	High mobility, highway scenarios

Protocol Class	Strengths	Weaknesses	Best-Use Scenario
Cluster/Hybrid	Better stability, mitigates fragmentation	Cluster maintenance overhead, complexity	Dense urban traffic, platooning
Intelligent/Adaptive	Adaptive to context, predictive routing	Requires data, computation, introduces complexity	Next-gen intelligent vehicular networks

Table 1: Routing and Data Dissemination Protocols Comparison

E. Critical Analysis and Comparative Insights

The comparative synthesis reveals an ongoing paradigm shift from topology-dependent to **context-adaptive** and **AI-enabled** routing. Geographic protocols, though efficient in dynamic mobility, underperform in sparse or obstructed regions. Cluster-based designs enhance stability in dense traffic but incur coordination overhead and energy consumption.

Machine-learning-based methods, including reinforcement learning and deep neural routing models, demonstrate improved predictive performance by leveraging historical mobility patterns (Yigit et al., 2024; "Ensuring security and privacy in VANET: A comprehensive survey," 2024). SDN-controlled VANETs further decouple data and control planes, enabling flexible traffic management but introducing single-point vulnerabilities and controller latency ("Security challenges in Internet of Vehicles (IoV) for ITS: A survey," 2025).

Critically, **no routing protocol achieves optimal performance across all VANET scenarios**. Instead, the effectiveness depends on contextual parameters—node density, link quality, mobility pattern, and application priority. The field’s direction points toward **cross-layer, edge-assisted, and data-driven integration**, combining the resilience of geographic routing with the adaptability of intelligent models to support real-time ITS requirements.

IV. Emerging Technologies and Trend Analysis

A. Software-Defined Networking (SDN) and Network Slicing for VANETs

The application of SDN in VANETs facilitates centralized control, dynamic resource allocation and rapid routing adaptation. SDN-based vehicular networks permit controllers to adjust forwarding decisions based on current traffic and network state. Recent work highlights that SDN-VANET architectures improve capacity and responsiveness, though they raise questions about scalability, reliability of controllers and latency in disseminating control information (Abu Maria et al., 2024).

B. Edge/Fog Computing and Data-Centric Architectures

As vehicles and infrastructure generate massive sensor data, VANETs are transitioning toward data-centric models. Edge and fog computing close to RSUs process data locally, reducing cloud latency and network load. Recent analysis ("Survey of multicast routing protocols for vehicular ad hoc networks," 2024) of clustering, energy-efficient routing and IoT integration in VANETs shows that distributed data analytics significantly benefit traffic safety and ambient monitoring. The integration of Wireless Sensor Networks (WSNs), IoT devices and VANETs is increasingly common.

C. Federated Learning and AI-Driven Routing

Federated learning—where vehicles/edge nodes locally train models and share updates rather than raw data—supports privacy-conscious, distributed intelligence. A hierarchical federated learning approach in multi-hop cluster-based VANETs demonstrated enhanced convergence and accuracy under non-IID vehicular data distributions (HaghighiFard & Coleri, 2024). AI counterpart routing models (ANN, RL, DRL) are being applied for path prediction, mobility forecasting and anomaly detection (HaghighiFard & Coleri, 2024), ("Lightweight machine learning model to detect VANET attacks," 2024).

D. Digital Twin and Cyber-Twin Frameworks

Digital twin architectures build real-time virtual replicas of vehicles or RSUs for monitoring, simulation and security - enabling proactive anomaly detection and resource management. The “Cyber-Twin” framework for VANET attack detection shows how real-time modelling can enhance network security and adaptability (Yigit et al., 2024).

E. Next-Generation Communications: 5G/6G, Terahertz and VLC

Emerging communication technologies such as 6G, terahertz (THz) links and visible-light communication (VLC) hold the promise of ultra-low latency (<1 ms), ultra-reliable low-latency communications (URLLC) and very high node densities. VANETs must adapt to support V2X across multiple spectra and heterogeneous link technologies, enabling IoV frameworks. Recent comprehensive work ("Survey of multicast routing protocols for vehicular ad hoc networks," 2024) underscores developments in energy-efficient routing, 802.11p channel utilization and remote monitoring.

F. Security, Privacy and Trust Mechanisms

Increasing vehicular connectivity enlarges the attack surface: spoofing, Sybil, DoS, and routing attacks are prevalent. The latest survey on VANET security and privacy ("Ensuring security and privacy in VANET: A comprehensive survey," 2024), ("Security challenges in Internet of Vehicles (IoV) for ITS: A survey," 2025) shows a shift toward lightweight ML-based intrusion detection, trust-based clustering ("Design of CSKAS-VANET model for stable clustering and secure communication," 2024), and hybrid blockchain/AI frameworks. The challenge remains designing real-time, low-overhead security mechanisms compatible with high mobility and dynamic topology.

V. Extended Discussion: Research Gaps, Objective Comparisons and Future Directions

A. Objective Comparison of Thematic Dimensions

1. **Scalability in High-Density Environments**
   - Many existing protocols perform well in simulations at moderate densities but degrade under ultra-dense urban scenarios.
   - How do machine-learning based routing methods scale when thousands of vehicles are present?

- Data-centric designs and edge/fog architectures can relieve centralized bottlenecks, but their deployment cost and coordination mechanisms require further study.

2. **Latency and Reliability under URLLC Requirements**
   - Safety applications demand < 50 ms latency, high delivery ratio (> 99 %). Classic protocols often cannot guarantee this under mobility and load.
   - Emerging 6G/THz/VLC links promise ultra-low latency; protocol frameworks must be adapted accordingly.

3. **Heterogeneous Link and Technology Interoperability**
   - In practice, vehicles may support DSRC, C-V2X, 5G/6G and even VLC simultaneously. Protocols must operate across multiple link types.
   - Few works convincingly integrate multi-radio, multi-standard environments into routing and dissemination frameworks.

4. **Adaptivity and Intelligence vs. Overhead and Complexity**
   - AI/ML based routing protocols demonstrate improved performance (e.g., predictive forwarding, link-lifetime estimation), but introduce overhead (training, computation, data collection).
   - The trade-off between improved PDR/latency and overhead/resource consumption is under-explored in real-world vehicular settings.
   - Security, Trust and Privacy in Highly Dynamic Contexts
   - Surveys ("Ensuring security and privacy in VANET: A comprehensive survey," 2024), ("Security challenges in Internet of Vehicles (IoV) for ITS: A survey," 2025) highlight attack taxonomies and defense mechanisms; yet, few integrate security design with routing, protocol stacks and real-time constraints.
   - Trust-based clustering ("Design of CSKAS-VANET model for stable clustering and secure communication," 2024) and lightweight ML intrusion detection ("Lightweight machine learning model to detect VANET attacks," 2024) are promising, but their additional latency overhead and vehicular compatibility remain open questions.

5. **Data Governance, Ethics and Deployment Realities**
   - With federated learning and data-centric VANETs, issues of data privacy, ownership, liability and ethics arise.
   - Real deployment (city-scale, multi-vendor infrastructure) remains a research gap—simulation dominates literature.

B. Future Roadmap and Open Research Challenges

- **Towards 6G-Enabled Cognitive VANETs**: The next generation vehicular networks will merge ultra-reliable low-latency communications, edge intelligence, and AI-driven decision-making. Research should target fully integrated architectures (radio, edge, cloud, AI) with end-to-end QoS guarantees.
- **Cross-Layer, Context-Aware Protocols**: Protocols must blend link, network, application and mobility layers, incorporating real-time traffic conditions, predicted trajectories and QoS context.
- **Lightweight, Real-Time AI/ML for Vehicular Environments**: Models suitable for vehicle/edge hardware, fast convergence under mobility, minimal overhead and high accuracy are required.

- **Multi-Standard, Multi-Link Interoperability**: Routing and dissemination frameworks must transparently handle transitions between DSRC, C-V2X, 5G NR, VLC and THz links, with handoff and coexistence management.
- **Security and Trust as First-Class Elements**: Security must be baked into architecture (not bolted on). Trust models, intrusion detection, privacy mechanisms should be integrated with routing and control planes.
- **Data Governance, Ethical Frameworks and Deployment Studies**: Research must move from simulation to real-world pilots, addressing legal, ethical and business-model aspects of vehicular data, edge/cloud partnerships and multi-stakeholder cooperation.
- **Sustainable and Resource-Efficient Designs**: Considering energy consumption (especially for edge/RSU deployments), green communications, and efficient hardware utilization remains a gap.

C. Limitations of Current Study

This survey is constrained by the pace of published literature and focuses primarily on routing/dissemination and emerging technologies-less on commercial deployment, regulatory and business-model issues. Furthermore, full quantitative meta-analysis (e.g., numerical benchmarking across many studies) lies outside its scope.

VI. Conclusion

This survey has traced the architectural foundations of VANETs, provided a comparative protocol analysis including the latest intelligent and adaptive approaches, and reviewed emerging technologies shaping the vehicular network future—such as SDN, edge/fog computing, federated learning and digital-twin frameworks. The evolution of VANETs is shifting from pure communication systems toward data-centric, intelligence-enabled vehicular ecosystems embedded within smart cities and IoV frameworks. To fully realize this vision, research must address scalability, heterogeneity, latency, security, resource efficiency and cross-layer integration in dynamic vehicular settings. The roadmap outlined herein aims to guide the next generation of VANET research and deployment.

References

1. Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). A comprehensive survey on vehicular ad hoc network. Journal of Network and Computer Applications, 37, 380–392.
2. Hartenstein, H., & Laberteaux, K. P. (2010). VANET: Vehicular applications and inter-networking technologies. John Wiley & Sons.
3. Routing protocols in vehicular ad hoc networks (VANETs): A comprehensive survey. (2023). Computer Communications.
4. Asituha, A. (2023). Privacy and security issues surrounding vehicular Ad-hoc networks (VANET). World Journal of Advanced Research and Review, 20(3), 1449–1479.
5. Nasir, R., Ashraf, H., & Jhanjhi, N. Z. (2023, December). Secure authentication mechanism for cluster based vehicular adhoc network (VANET): A survey. arXiv:2312.12925.

6. HaghighiFard, M. S., & Coleri, S. (2024, January). Hierarchical federated learning in multi-hop cluster-based VANETs. arXiv:2401.10361.

7. Yigit, Y., Panitsas, I, Maglaras, L., Tassiulas, L., & Canberk, B. (2024, January). Cyber-Twin: Digital twin-boosted autonomous attack detection for vehicular ad-hoc networks. arXiv:2401.14005.

8. A comprehensive review of recent developments in VANET for traffic, safety & remote monitoring applications. (2024). Journal of Network and Systems Management, 32, Article 73.

9. Ensuring security and privacy in VANET: A comprehensive survey. (2024). Mathematical Problems in Engineering, Article 1818079.

10. Security challenges in Internet of Vehicles (IoV) for ITS: A survey. (2025). TST Transactions, Article 9010083.

11. Abu Maria, K., El-Dalahmeh, A., Abu Maria, E., & El-Dalahmeh, M. (2024). VANETs built on SDN: Emerging trends in technology and modeling. Journal of Electrical Systems, 20(3), 7023–7040.

12. Survey of multicast routing protocols for vehicular ad hoc networks. (2024). International Journal of Fuzzy Mathematics & Optimization.

13. Lightweight machine learning model to detect VANET attacks. (2024). Vehicular Communications, 16(6), Article 324.

14. Design of CSKAS-VANET model for stable clustering and secure communication. (2024). Frontiers in Computer Science, 4, Article 1384515.