Agent-Based Secure Route Switching and QoS Management in VANETs Using the Wiedemann Car-Following Prediction Model

Ma'en S. Saleh
Engineering Faculty, Tafila Technical University, Tafila, Jordan
Email: maen@ttu.edu.jo (M.S.S.)

Manuscript received July 5, 2025; revised August 15, 2025; accepted August 17, 2025

***Abstract*—In Vehicular Ad-Hoc Networks (VANETs), ensuring robust security alongside high Quality-of-Service (QoS) is essential due to the network's dynamic topology and limited infrastructure, which can impact safety and comfort applications. This paper presents an agent-based, security-aware multi-path route switching protocol designed to enhance QoS in VANETs. The protocol integrates a secure route-connectivity prediction agent, leveraging the Wiedemann car-following model, with a flexible QoS agent that intelligently selects and switches among secure multi-path routes from source to destination. Unlike traditional methods, the QoS agent employs multiple adaptive switching strategies—including Least Path Switching (LPS), Least Path Switching with Minimum Delay (LPSMD), and Least Disconnection Delay (LDD)—to maintain route stability and optimize performance. To secure communication, vehicular nodes utilize a hybrid key agreement mechanism combining Diffie-Hellman and Short Authentication String (SAS) protocols executed over Wi-Fi direct out-of-band channels. Extensive simulations in a heterogeneous VANET environment assess the protocol under varying conditions such as node density, average vehicle speed, data collection intervals, and the prevalence of Man-In-the-Middle Attacks (MITMAs). The results show that secure protocol variants significantly improve packet delivery ratios, especially under adversarial and high-mobility conditions, while incurring only modest increases in end-to-end delay due to security overhead. Performance trends remain consistent across scenarios, with LDD-based strategies achieving the best results in both secure and non-secure modes. These outcomes confirm the proposed protocol's effectiveness in enhancing both security and QoS in real-time VANET environments.**

***Index Terms*—agents, connectivity prediction, path switching, routing, security, Vehicular Ad-Hoc Networks (VANETs)**

I. Introduction

Intelligent Transportation Systems (ITS) have become a cornerstone of modern smart city initiatives, aiming to improve traffic safety, reduce congestion, and enhance passenger comfort. Within this domain, Vehicular ad Hoc Networks (VANETs) have emerged as a pivotal technology enabling vehicles, roadside infrastructure, and pedestrians to communicate dynamically. By leveraging Dedicated Short-Range Communication (DSRC), Wi-Fi direct, and other wireless technologies, VANETs foster a connected and cooperative transportation environment that supports applications ranging from collision avoidance to real-time traffic management and infotainment [1–3]. Fig. 1 illustrates a typical intelligent transportation scenario integrating Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Infrastructure (I2I) communication components.

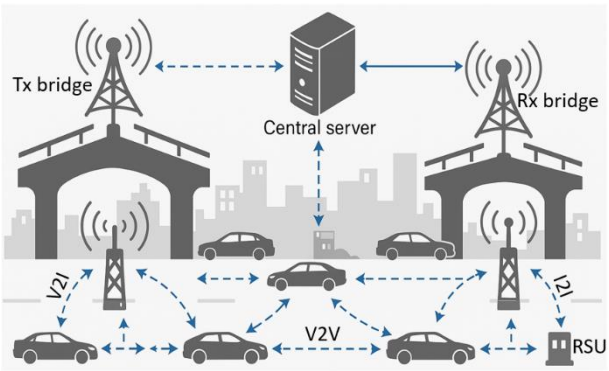

Fig. 1. Intelligent transportation system.

In practice, VANET deployment faces significant challenges primarily due to the network's inherent characteristics such as high node mobility, frequently changing network topologies, and constrained communication resources [4]. Moreover, the broadcast nature of vehicular communications introduces substantial security risks, including Man-In-the-Middle Attacks (MITMAs), spoofing, and Denial-of-Service (DoS) attacks, which can compromise data integrity, privacy, and overall road safety [5, 6]. These challenges necessitate security mechanisms that are robust, lightweight, and adaptable to highly dynamic environments.

Routing protocols in VANETs must deliver messages reliably and timely despite these conditions. Traditional routing schemes often fall short when faced with frequent link breakages and security threats. Consequently, secure multipath route switching protocols capable of predicting link stability and reacting swiftly to changes are crucial for maintaining Quality-of-Service (QoS) [4, 7]. Predictive models, such as the Wiedemann car-following model, provide effective tools for estimating vehicle behaviour and link connectivity, enabling smarter and more resilient route selection strategies that reduce latency and disconnections [7].

doi: 10.18178/ijeetc.14.6.341-353

Agent-based systems have increasingly been integrated into VANET architectures, embedding autonomous software agents within vehicles and Roadside Units (RSUs) to manage routing, security, and QoS dynamically. This decentralized approach enhances scalability, resilience, and real-time responsiveness [8].

Recent research also explores machine learning techniques to optimize routing and threat detection; however, such methods may impose heavy computational overhead or require centralized infrastructure, limiting their suitability for distributed, real-time VANET environments [9].

This paper proposes a novel security-based multi-path route switching protocol that integrates secure connectivity prediction, lightweight cryptographic security, and advanced QoS optimization to address the unique challenges of VANETs. The main contributions are as follows:

1) Introducing a multi-path route switching protocol that combines secure connectivity prediction, lightweight cryptographic mechanisms, and QoS optimization tailored for VANETs.
2) Utilizing the Wiedemann Car-Following Model to generate and update multi-path connectivity reports via RSU feedback, enabling rapid adaptation to dynamic network changes.
3) Implementing strong security protocols using Diffie-Hellman and short authentication string key agreements over Wi-Fi Direct out-of-band communication to safeguard against MITMA and related attacks.
4) Applying multiple QoS-based switching criteria: least number of path-switching (LPS), least number of path-switching with minimum delay (LPSMD), and least-disconnection-delay (LDD) to enhance communication stability and performance.
5) Integrating agent-based decision-making frameworks within vehicles and RSUs to enable collaborative and autonomous management of routing and security under real-time constraints.

Extensive simulations demonstrate that the proposed protocol significantly enhances secure data delivery rates while maintaining low end-to-end packet delays across a wide range of network conditions, including varying vehicle speeds, node densities, and MITMA attack prevalence. These results validate the protocol's effectiveness in providing a secure and efficient VANET environment, thereby contributing to safer and more reliable intelligent transportation systems.

The remainder of the paper is organized as follows: Section II reviews related work in secure routing, mobility modelling, and agent-based VANET systems. Section III describes the agent-based system modelling and design. Section IV details the functional agents of the server agent. Section V presents the methodology used in this work. Section VI presents the simulation setup and performance evaluation. Finally, Section VII concludes the paper and outlines directions for future research.

II. Related Work

Reliable and secure data transmission in VANETs has garnered significant attention, especially in the context of multipath routing protocols designed to ensure both network performance and QoS. Multipath routing improves communication reliability by offering alternative paths, which is vital in dynamic vehicular environments to maintain safety and service continuity [10]. Reddy *et al*. [11] proposed a trust-enabled secure routing protocol for VANETs that evaluates node reliability through multiple trust metrics, including direct, indirect, and situational trust. This approach dynamically adapts routing decisions to network conditions, improving security and enhancing performance metrics such as latency, packet delivery ratio, and throughput. An *et al*. [12] proposed a deep-learning-based secure routing protocol designed to detect and avoid blackhole attacks in VANETs by dynamically adapting routing decisions, enhancing security and network performance, although challenges remain in reducing control overhead in highly dynamic scenarios. Jubair *et al*. [13] developed a hybrid cryptographic routing protocol integrating Advanced Encryption Standard (AES) and Elliptic Curve Cryptosystems (ECC) with QoS-aware cluster head selection, significantly enhancing security and network performance by improving throughput, reducing delay, and minimizing routing overhead in VANETs. Addressing security threats such as blackhole attacks remains a priority in VANET research. Ramamoorthy [14] proposed an enhanced location-aided ant colony routing protocol that integrates secure group-based key management to improve data confidentiality and routing efficiency in VANETs, demonstrating strong performance in throughput, packet delivery, and latency. Pandey *et al*. [15] developed a PKI (public key infrastructure)-based multipath routing protocol that enhances VANET security by mitigating blackhole and wormhole attacks through reliable dual-path selection. Privacy preservation has also become increasingly essential. Zhao *et al*. [16] introduced a secure location-based routing protocol utilizing order-revealing encryption to balance location privacy and routing efficiency. Razzaque *et al*. [17] proposed a secure and efficient RSU-assisted routing protocol for VANETs that improves route reliability and mitigates routing attacks, resulting in higher packet delivery rates and enhanced network security. Cluster-based routing plays a crucial role in enhancing VANET performance. Kumar and Kuila [18] proposed a particle swarm optimization-based clustering scheme that optimizes cluster head selection and cluster formation, improving cluster stability, communication efficiency, and overall network scalability in dynamic vehicular environments. Furthermore, Silva *et al*. [19] introduced CMAF, a context- and mobility-aware forwarding model based on Named Data Networking (NDN) and Extended KALMAN Filters (EKF), which enhances data delivery and adaptability in urban vehicular environments.

Building on these foundations, Saleh [20] proposed a security-based multipath route switching protocol employing the Wiedemann car-following model. This model enables accurate path connectivity predictions and

dynamic route switching to optimize QoS. By integrating robust cryptographic protocols and out-of-band Wi-Fi Direct communication, this approach effectively counters man-in-the-middle attacks while maintaining network performance.

Recent advances increasingly integrate Artificial Intelligence (AI) and decentralized frameworks. Ali and Ali [21] proposed an energy-efficient routing protocol using real-time traffic information to adaptively optimize route selection, reducing travel latency and improving overall network performance in vehicular environments. Chellapandi *et al*. [22] presented a comprehensive survey of federated learning techniques tailored for connected and automated vehicles, emphasizing privacy preservation, decentralized training, and communication efficiency key considerations for secure routing in VANETs.

Agent-based systems continue to gain prominence in VANETs for their ability to support adaptive routing and secure traffic management. Recently, Xu and Wang [23] proposed Secure and Reliable Opportunistic Routing (SROR) protocol that is an agent-based routing protocol for VANETs which leverages deep reinforcement learning agents to optimize relay selection based on metrics like relative velocity and connectivity, enhancing packet delivery, reducing delay, and improving security. Zhang *et al*. [24] proposed a blockchain-based multi-path mobile access point selection strategy for secure 5G VANETs, leveraging decentralized ledger technology to enhance route reliability and incorporate trust-based attack detection mechanisms, thereby improving communication security and reducing delays in highly dynamic vehicular environments. Ali *et al*. [25] proposed an enhanced QoS routing protocol for unmanned ground vehicles using the Ant Colony Optimization (ACO) approach. Their method optimizes routing paths to ensure safe and efficient navigation in dynamic environments, improving throughput and reducing delays in VANET communications. Meanwhile, Ezumalai and Santhakumar [26] proposed a cluster-oriented intelligent secure routing protocol for VANETs that enhances communication robustness and security by leveraging clustering techniques to improve the reliability and safety of data transmission in dynamic vehicular environments.

Lightweight cryptography remains vital for resource-constrained vehicles. Sang *et al*. [27] proposed a privacy-Preserving Authentication Scheme with On-Chain Certificate Management (PACM) for VANETs. Their approach enhances security and privacy by leveraging blockchain technology to manage certificates, ensuring efficient and secure authentication in vehicular networks. Similarly, Lin [28] evaluated the unforgeability of a privacy-preserving aggregation-authentication scheme for fog-cloud based VANETs, demonstrating its strong resistance to forgery and ensuring robust data integrity in vehicular safety systems. Enhanced mobility modelling continues to improve routing resilience. Abdollahzade and Kazemi [29] developed an evolving car-following model that dynamically updates its structure and parameters via time-variant local linear models, enhancing adaptability and accuracy in modeling diverse vehicle dynamics. This complements Saleh's [20] use of the Wiedemann car-following model for adaptive multipath switching.

SDN integration offers centralized control and flexible routing. Assafra *et al*. [30] proposed a privacy-preserving and security-managed VANET architecture based on the SDN paradigm, enhancing resilience and confidentiality through centralized control and adaptive policy enforcement. Alaya and Sellami [31] developed a secure SDN-based VANET architecture that integrates heterogeneous access technologies under centralized control, enabling dynamic controller placement and robust confidentiality, integrity, and authentication in highly mobile environments.

Privacy-preserving mechanisms beyond routing are also vital. Saini *et al.* [32] introduced TMAPS, a trust-based mutual authentication and privacy scheme embedded in VANET routing, ensuring secure data forwarding, privacy preservation, and resistance to impersonation and Sybil attacks with minimal overhead. Wang *et al*. [33] developed ARPLR, an all-round and highly privacy-preserving location-based routing scheme for VANETs that ensures strong privacy protection while maintaining efficient and reliable communication in dynamic vehicular environments.

Emerging communication technologies further influence VANET routing. Quy *et al*. [34] proposed an efficient routing algorithm for self-organizing networks in 5G-based intelligent transportation systems, enhancing network adaptability and communication performance in highly dynamic vehicular environments. Chithaluru *et al*. [35] proposed an energy-efficient routing scheme for real-time WSN-VANETs, reducing power consumption while ensuring reliable data delivery.

Multi-agent reinforcement learning has been applied for decentralized routing. Lu *et al*. [36] proposed MARVEL, a multi-agent reinforcement learning approach for VANETs that minimizes communication delay by optimizing routing decisions in dynamic vehicular networks. Nakayima *et al*. [37] combined software-defined and delay-tolerant networking with deep reinforcement learning to enhance VANET security and reliability, improving network adaptability and resilience in dynamic vehicular environments.

Trust and reputation systems play a growing role in VANET security. Baccari *et al*. [38] proposed a secure, trust-aware cross-layer routing protocol for VANETs that enhances data integrity and trust management to improve network security and performance in highly dynamic vehicular environments. Salim *et al*. [39] proposed SOMACA, a swarm optimization-based, mobility-aware clustering approach for the Internet of Vehicles, enhancing cluster stability and network efficiency in dynamic vehicular environments.

To jointly improve QoS and security, Maliya *et al*. [40] provided an overview of safety-focused information routing protocols in VANETs, highlighting techniques that enhance secure and reliable communication for improved vehicular safety. Garai *et al*. [41] proposed an enhanced digital certificate-based authentication approach for QoS-aware VANETs, improving security and service quality by

ensuring reliable vehicle identity verification. Finally, Al-Mekhlafi *et al*. [42] presented a comprehensive taxonomy and systematic review of vehicular environment in network simulation models (VEINS) for VANETs, emphasizing the integration of blockchain, AI, secure routing, and safety mechanisms to enhance vehicular network security and performance.

III. Agent-Based System Modelling and Design

To effectively address the dynamic, distributed, and security-critical environment of VANETs, the proposed system uses an agent-based architecture [43, 44]. In this setup, each intelligent system component is modeled as an autonomous agent with clear objectives, localized decision-making capabilities, and the ability to collaborate with other agents to meet the overall system goals. This modular approach significantly enhances scalability, flexibility, and robustness essential qualities for managing the complexities inherent in VANETs. The overall system architecture, based on agent interactions, is illustrated in Fig. 2.

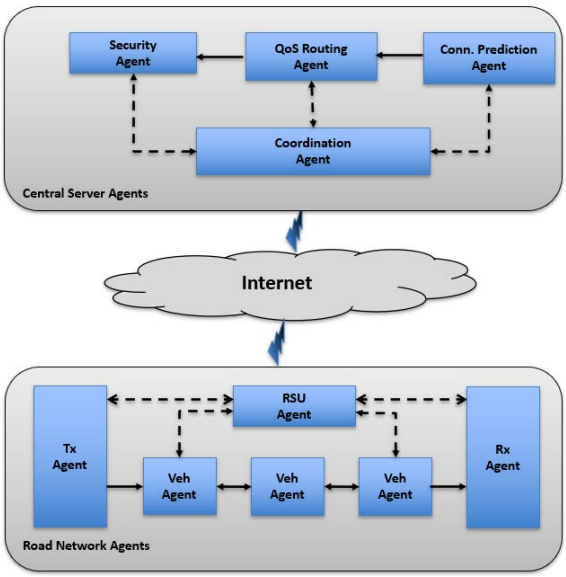

Fig. 2. Agent-based system architecture.

A. Road Network Agents

The road network is represented as a collection of cooperative zone agents, each corresponding to a virtual path zone (VPZ) along the predetermined end-to-end route. These agents include:

1) Transmitter Agent (TxAgent)

Located at the source vehicle, this agent initiates communication by sending periodic real-time traffic flows embedded with QoS requirements such as throughput and delay constraints. The TxAgent coordinates with its associated RSU Agent to request and maintain optimal routing paths.

2) Receiver Agent (RxAgent)

Situated at the destination vehicle, it acts as the terminal endpoint for the data flow. The RxAgent manages incoming traffic reception and supports acknowledgment and route feedback mechanisms as needed.

3) Vehicular Agents (VehAgents)

Representing intermediate vehicles forwarding data along the route, each VehAgent maintains a dynamic profile including mobility parameters such as velocity, acceleration, and position. VehAgents engage in both Vehicle-to-RSU (V2R) and V2V communication, cooperating to facilitate secure, hop-by-hop data forwarding while continuously updating their status and responding to RSU queries.

4) RSU agents

Overseeing specific virtual road segments, RSU Agents maintain local registries of active VehAgents within their coverage areas. Acting as gateways between the vehicular network and the central server, RSU Agents collect and forward vehicle state information to the coordination agent. They also manage route updates and disseminate instructions to local VehAgents and the TxAgent to ensure synchronized operation.

B. Central Server Agents

At the system core, centralized but modular intelligent agents hosted on a central server oversee system-wide control and coordination:

1) Coordination agent

Serving as the primary interface between RSU Agents and other central agents, it manages incoming requests from RSUs, orchestrates the execution of prediction and routing agents, and distributes routing decisions and updates back to RSUs and the TxAgent.

2) Connectivity prediction agent

Leveraging location prediction based on the Wiedemann car-following model, this agent analyses vehicle behaviour to forecast connectivity status across all potential paths [7, 45]. It evaluates the likelihood of link disconnections caused by vehicle mobility or malicious activity. The agent periodically updates connectivity reports at fixed intervals and integrates security alerts from RSUs to reclassify path trustworthiness.

3) QoS routing agent

Utilizing updated connectivity reports, this agent assesses multiple routing options against predefined QoS constraints. It applies advanced criteria, including LDD, LPS, and LPSMD to select the most reliable and efficient route [7]. The selected path is then relayed to the coordination agent for dissemination to RSUs and the TxAgent.

4) Security agent

A key part of this architecture is the security agent, which protects routing from malicious VehAgents by allowing only authenticated nodes to forward data. It includes an authentication agent that secures associations between vehicles; a malicious behavior detection agent that identifies compromised nodes; an alert and response agent that informs the RSU and coordination agent to blacklist unsafe paths; and a key management agent that handles secure key distribution. The security agent uses cryptographic methods like Diffie-Hellman key exchange and Short Authentication String (SAS) validation for lightweight mutual authentication. Details of the protocol and verification are provided in the methodology section [1, 20].

C. Communication and Agent Interactions

Agent communication follows a structured protocol to ensure coordinated and efficient system operation. Initially, the TxAgent requests an optimal route via its associated RSU agent. RSU agents continuously monitor vehicle states and forward pertinent data to the coordination agent. The connectivity prediction agent processes this information, combining it with mobility predictions and security assessments to evaluate real-time connectivity for all candidate routes. The QoS routing agent selects the optimal path based on reliability, stability, and security metrics. This decision is communicated back through the coordination agent to RSU agents and the TxAgent, establishing the data transmission route. The system supports dynamic adaptation; upon detecting connectivity changes or malicious behaviour, RSU or vehicular agents notify the coordination agent to trigger a new prediction-routing cycle, thereby maintaining secure and high-quality communication.

D. Agent Autonomy and Cooperation

Each agent operates autonomously with the ability to respond promptly to real-time network changes or security threats. Agents proactively initiate communication and updates to ensure continuous QoS compliance, minimizing the need for centralized supervision. Furthermore, agents demonstrate social abilities by exchanging information, notifying peers of state changes, and coordinating routing decisions in a distributed manner. Adaptability is also fundamental; agents modify behaviour based on evolving mobility patterns, network topology fluctuations, and detected security incidents. This blend of reactivity, proactivity, cooperation, and adaptability empowers the system to effectively manage VANET challenges, delivering robust, secure, and efficient communication services.

E. Scalability, Robustness, and Extensibility

The agent-based design inherently supports scalability and robustness—key attributes for VANETs characterized by highly dynamic topologies and variable vehicle densities [8, 23]. Autonomous agents can be seamlessly added or removed as vehicles enter or leave the network, without compromising overall system stability. This modularity also facilitates fault tolerance; failure or compromise of individual agents can be isolated and mitigated locally, preventing cascading effects. Moreover, the architecture is future proof, enabling straightforward integration of new agent types to address emerging challenges such as enhanced security mechanisms, advanced traffic analytics, or cooperative autonomous driving [10, 34]. This extensibility ensures the system evolves in parallel with advances in VANET technologies and applications.

In summary, the proposed agent-based architecture provides a scalable, adaptive, and security-focused framework for managing complex VANETs. Through a coordinated network of autonomous agents from mobility-aware Veh. Agents to intelligent Coordination and Routing Agents. it ensures service continuity, route optimization, and real-time responsiveness. The introduction of the specialized security agent further fortifies the design, enabling proactive authentication and route protection mechanisms. Together, these agents cooperate to deliver secure, reliable, and efficient vehicular communication, even under dynamic network conditions and adversarial threats.

IV. Functional Agents of the Server Agent

To address the high dynamism and heterogeneity of VANETs, the server agent hosts a set of intelligent agents, each responsible for a core functionality: location prediction, QoS assessment, and security enforcement.

These agents operate collaboratively to support real-time routing decisions, maintain secure multipath communication, and optimize vehicular data exchange under rapidly changing network conditions.

At the centre of this collaborative framework is the coordination agent, which orchestrates interactions among all functional agents. It ensures seamless integration of predictions, routing evaluations, and trust assessments, maintaining a consistent global view of the network state. By coordinating the domain-specific logic of each agent—from mobility forecasting and QoS evaluation to proactive threat detection—the system forms a distributed decision-making engine that enhances scalability, resilience, and real-time responsiveness.

A. Security Agent

Under the coordination agent's supervision, the security agent protects communication paths by detecting malicious nodes and establishing trust among vehicles. It employs a lightweight, distributed security association protocol over a secure Wi-Fi direct out-of-band channel, reducing risks of eavesdropping and spoofing. This protocol extends the model from our previous work [20], enhancing real-time coordination and adaptive threat response within the integrated server agent framework. The security mechanism comprises a two-phase mutual verification process:

1) Diffie-Hellman key agreement

This protocol forms the initial step in the security association to establish shared cryptographic parameters securely [20]. Each vehicular node generates its public key using the Diffie-Hellman protocol with agreed-upon parameters: a large prime modulus n, a base g, and a private key k. The public key P is computed as:

$$P = g^k \bmod n \tag{1}$$

2) Short Authentication String (SAS) commitment

Following public key generation, the node creates a commitment value C by hashing a concatenated message M which includes the public key P and a randomly generated, non-shared string r:

$$M = P \oplus r \tag{2}$$

$$C = H(M, k) \tag{3}$$

where H is a cryptographic hash function, and this commitment scheme is used for peer validation and mutual authentication, mitigating MITMAs [20]. When a trusted

neighbouring node (j) receives this commitment from node i, it extracts the string r_i from the appended message and compares it to its locally generated string r_j. If the two strings differ, the sender is flagged as malicious, and the incident is reported to the nearest RSU. The RSU then informs the Secure Route Connectivity Prediction agent, prompting a security reassessment with a different adjacent node [20].

If the strings match, mutual trust is established. Both nodes independently compute a shared symmetric key K_{ij} without exchanging it over the network. Given the public key of the peer node j, denoted P_j, and the private key of the current node i, denoted k_i, then the shared key is derived as:

$$K_{ij} = P_j^{k_i} \bmod n \tag{4}$$

This end-to-end authentication and session key generation process ensures secure data transmission between verified vehicular nodes [20]. The security agent's continuous threat monitoring and adaptive re-authentication capabilities dynamically isolate untrusted nodes and maintain trusted communication chains all coordinated centrally by the coordination agent.

B. Location Prediction Agent

The location prediction agent, embedded within the server agent architecture and coordinated by the central coordination agent, is responsible for anticipating vehicular mobility patterns to support proactive multipath route discovery and switching. To achieve accurate and dynamic predictions in fast-changing traffic environments, this agent leverages the Wiedemann car-following model—a psychophysical driver behaviour framework adopted from our earlier work [7].

The Wiedemann model simulates a vehicle's motion based on its relative position and speed with respect to the nearest leading vehicle in the same lane. It defines four distinct driving regimes based on calibrated behavioral thresholds: Free, Closing, Following, and Emergency. Each regime governs the expected acceleration or deceleration behavior that a driver should exhibit to ensure safe and efficient movement [7].

To determine the current regime of the following (subject) vehicle, the agent computes six threshold parameters following the modelling Eqs. (1) to (6) in [7]) which include:

- AX: Minimum average stopped headway,
- ABX: Minimum average moving headway,
- SDV: Starting deceleration threshold due to a slower leading vehicle,
- CLDV: Deceleration trigger when the follower is faster than the leader,
- OPDV: Trigger for reacting to increasing inter-vehicle distance over time,
- SDX: Maximum distance boundary of the following regime.

These thresholds are calculated using system parameters such as inter-vehicle headway, relative speed, and driver calibration factors. The behavioral boundaries across these regimes are visually depicted in Fig. 3, while all relevant calibration parameters used for threshold evaluation are listed in Table I of [7].

Once the subject vehicle's regime is identified, the agent estimates its expected acceleration using the regime-specific logic, which was defined Eqs. in (7) to (11) of [7]. The corresponding behaviors are:

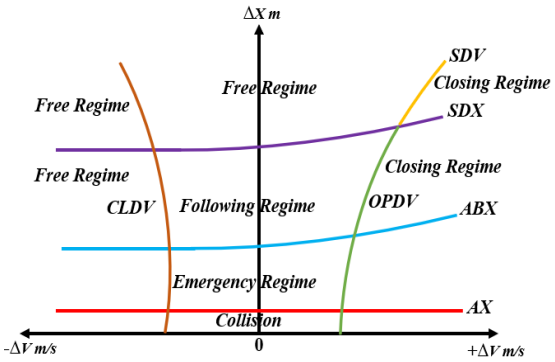

Fig. 3. Wiedemann model driving regimes.

- In the Free Regime, the vehicle accelerates toward its desired speed.
- In the Closing Regime, it decelerates to match a slower leading vehicle.
- In the Following Regime, minor speed adjustments applied to maintain a stable gap.
- In the Emergency Regime, it performs sharp deceleration to avoid potential collisions.

After evaluating the expected acceleration, the agent then computes the expected velocity v_{exp} and expected distance d_{exp} that the subject vehicle will travel in the next discrete time step using the following equations adapted from [7]:

$$v_{\text{exp}} = v_{\text{cur}} + (a_{\text{exp}}\Delta t) \tag{5}$$

$$d_{\text{exp}} = (v_{\text{cur}}\Delta t) + (0.5a_{\text{exp}}\Delta t^2) \tag{6}$$

where v_{exp} is the predicted velocity of the subject vehicle, d_{exp} is the predicted distance it will travel in the next-time interval, v_{cur} is the current velocity, a_{exp} is the expected acceleration based on regime, and Δt is the time step used in the simulation.

The behavioral coefficients and acceleration calibration values used in these calculations are specified in Table II of [7]. By computing these motion parameters, the agent predicts the subject vehicle's next location, which is then forwarded to the server agent's route coordination engine. This allows for timely route evaluations and adaptive multipath switching based not only on current topological data but also on proactive motion forecasting.

This predictive mechanism significantly enhances the resilience, stability, and responsiveness of multipath routing under high-mobility and variable-connectivity conditions, ensuring more efficient route maintenance and timely recovery from link disruptions.

C. QoS Routing Agent

The QoS Routing agent, situated within the server agent architecture and governed by the central coordination

agent, is tasked with generating adaptive multipath routing schedules that fulfil the application-specific QoS requirements of the source vehicle. These requirements—such as throughput, end-to-end delay, and packet loss ratio—are initially received from the source application through the primary RSU and forwarded via the coordination agent. To construct QoS-compliant routes, the agent integrates two key inputs:

1) Connectivity predictions from the Prediction Agent, which forecasts the availability of multiple paths over time based on real-time vehicular mobility trends and link stability estimates.
2) QoS constraints received from the source node, including a key threshold (Φ), which represents the playout buffer time for delay-sensitive applications such as real-time video streaming.

Using this information, the QoS Routing agent evaluates which paths can satisfy the application's QoS requirements during each discrete time interval. When no single path can maintain the desired performance throughout the entire transmission session, the agent constructs a time-dependent multipath routing schedule. This schedule determines which path should be used at each point in time and dynamically switches between paths as needed to preserve QoS compliance. To optimize such decisions, the QoS Routing agent supports three multipath route-switching strategies originally proposed in our earlier work [7]:

- Least Disconnection Delay: Prioritizes the selection of routes that minimize total disconnection duration while staying within the delay bound.
- Least Path Switching: Minimizes the number of path switches by maintaining a stable route if it satisfies the QoS constraints.
- Least Path Switching with Minimum Delay: A hybrid strategy that first minimizes the number of switches and then, among those options, selects the route with the least disconnection delay.

Once the routing schedule is determined, the agent forwards it to the coordination agent, which relays it to the primary RSU. The RSU then communicates the routing instructions to the source vehicle, which follows the schedule to guide its real-time transmission.

By incorporating proactive connectivity forecasting and adaptive routing logic, the QoS Routing agent enables reliable, delay-aware, and context-sensitive communication across dynamically changing vehicular topologies. Its integration with the Prediction Agent and coordination agent ensures tight coupling between mobility trends and route planning, significantly enhancing the stability and performance of multipath routing under real-world VANET conditions [7].

V. Methodology

This methodology builds upon our earlier security-based multipath route-switching protocol [20], evolving it into a real-time agent-based framework that jointly addresses QoS, security, and dynamic connectivity within VANETs. The proposed design enables each system component—vehicles, RSUs, and the central server—to operate autonomously via intelligent agents while remaining coordinated through secure communication protocols and predictive analytics.

When a source vehicle initiates a transmission session, its Transmitter Agent (TxAgent) issues a route request embedded with the application's QoS constraints to the nearest RSU. This RSU forwards the request to the coordination agent, hosted on a centralized server. The coordination agent then orchestrates secure route discovery through three core system agents: the security agent, the Location Prediction Agent, and the QoS Routing Agent.

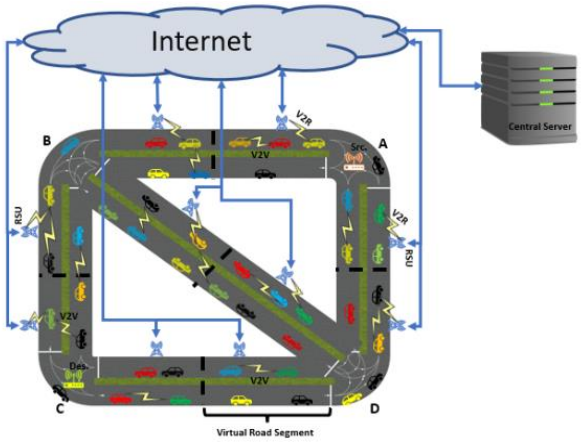

Fig. 4. Case study scenario of the intelligent transportation system—VANET setup with transmitter at A, receiver at C, and four predefined multi-hop paths [7].

The scenario under investigation (illustrated in Fig. 4) involves a transmitter and receiver communicating over a vehicular network with four predefined candidate paths connecting them. The transmitter is located at node A, and the receiver is at node C. The four alternative multi-hop paths between them are: P1 (A → B → C), P2 (A → B → D → C), P3 (A → D → C), and P4 (A → D → B → C). These paths traverse different sets of vehicular nodes, road segments, and virtual zones across forward and backward lanes.

The security agent authenticates participating vehicles using a hybrid two-phase protocol combining Diffie–Hellman key exchange and SAS-based verification, performed over secure Wi-Fi Direct out-of-band communication channels. This prevents in-band eavesdropping or spoofing. Vehicles failing this authentication are excluded from route planning.

After establishing a secure forwarding node set, the Location Prediction Agent forecasts short-term connectivity using the Wiedemann Car-Following Model, which considers vehicle spacing, acceleration, and behavioral regimes. The connectivity for each candidate path is evaluated over a 5-second prediction window T=5s, divided into 1-second intervals. The system deems a path connected during an interval if it contains at least one authenticated vehicle in the relevant forward or backward virtual zone.

Fig. 5 presents a sample connectivity analysis for path P1 (A → B → C), showing that it is connected during [t_1,

t_2] and [t_3, t_4], but disconnected during [t_2, t_3] and [t_4, t_6] due to an empty zone. The complete connectivity analysis across all paths (P1–P4) is shown in Fig. 6, forming a basis for secure QoS-driven path switching.

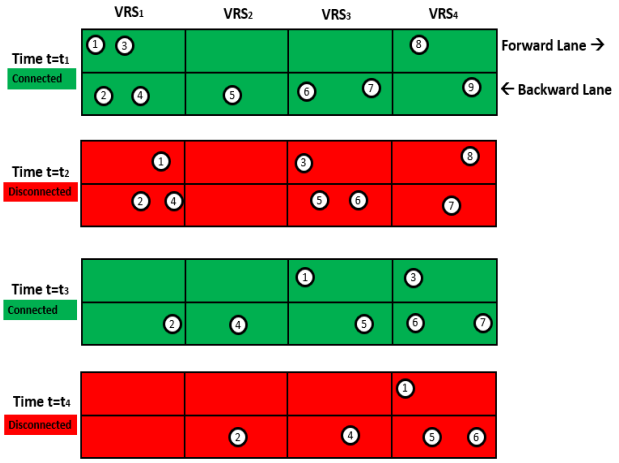

Fig. 5. Path connectivity prediction for P1: A → B → C; *T*=5s — Connectivity evaluation using 1-second snapshots [20].

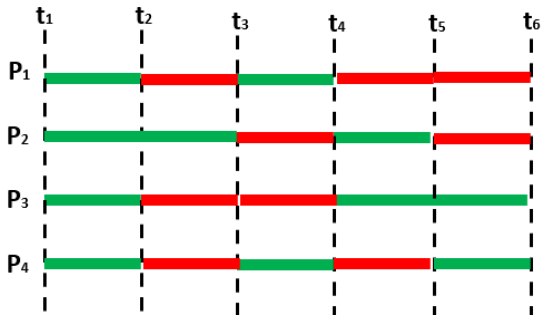

Fig. 6. Path-connectivity report for P1–P4; *T*=5s, interval = 1s — compiled by the location prediction agent and sent to the QoS routing agent [20].

At this stage, the QoS Routing Agent applies secure least disconnection delay (S-LDD), which minimizes cumulative expected disconnect time. It schedules P2 from [t_1, t_3], switches to either P1 or P4 during [t_3, t_4], and finally to P3 from [t_4, t_6].

If a MITMA attack is detected—for example, involving node 4 which lies on P1 and P2—the security agent flags it and updates the coordination agent. This prompts the Location Prediction Agent to regenerate a connectivity report excluding node 4. As shown in Fig. 7 and Fig. 8, P1 becomes completely disconnected and P2 partially degraded. Under these conditions, the updated S-LDD schedule selects P2 from [t_2, t_3], P4 from [t_3, t_4], and P3 from [t_4, t_6].

If instead the system applies secure least path switching (S-LPS), it chooses the route with the fewest number of switches that satisfies the QoS constraint, meaning the path's total disconnection duration remains within the application's playout buffer tolerance and thus the path is still stable and reliable. So, the choice here to switch to either P2, P3 or P4 since in all paths the disconnection is 2-time units which is within the QoS constraints (i.e. $\Phi \leq$ 2-times units).

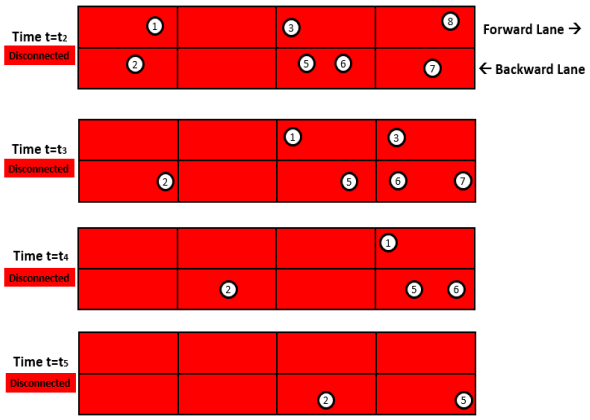

Fig. 7. Updated path-connectivity report (Node 4 neglected)- result of security-triggered reevaluation of available paths [20].

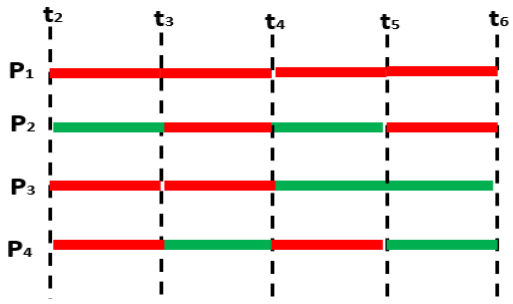

Fig. 8. Connectivity impact of malicious node removal — P1 is removed; P2 is weakened due to node 4 exclusion [20].

The Secure Least Path Switching with Minimum Delay (S-LPSMD) strategy selects the same route as S-LPS (i.e. P2, P3 or P4). This choice is justified both by minimizing switches and ensuring lower total disconnection delay compared to alternatives. In our scenario all paths exhibit equal disconnection delays, and all satisfy the QoS requirements.

To ensure that any switching strategy still satisfies application QoS, the agent evaluates the allowable disconnection tolerance, which is application dependent. For example, in video streaming, the playout buffer size defines the threshold above which the receiver would experience disruption. To enforce this constraint, a route (or a switching combination) is considered valid only if:

$$\sum_{i=1}^{n} \Delta t_{\text{disc}}(i) \leq \Phi \tag{7}$$

where $\Delta t_{disc}(i)$ is the disconnection duration during the ith time interval, Φ is the maximum tolerable delay (e.g., Φ = 2 s, representing 2 time-units).

Finally, the total expected availability window (T) for any secure route is calculated using:

$$T = \psi Q \lambda^{-1} \tag{8}$$

where ψ: is the path density factor (node clustering), Q is the number of authenticated forwarding nodes, λ is the average path disconnection rate from mobility estimation.

The system repeats this evaluation at each prediction window T, or when triggered by a security alert (e.g., MITMA detection). If no route combination satisfies the QoS condition in Eq. (7), the transmitter is prompted to either relax its QoS requirement or defer transmission.

VI. Simulation and Results

This section presents an extensive evaluation of the proposed secure, agent-based multipath route switching protocols in a realistic heterogeneous Vehicular Ad-hoc Network (VANET) environment. Simulations were performed using the QualNet simulator, an advanced extension of the discrete-event Global Mobile Information System Simulator (GloMoSim), which integrates the Wiedemann car-following model to realistically emulate vehicle mobility dynamics.

The performance of the original protocols—LDD, LPSMD, and LPS—and their secure variants—S-LDD, S-LPSMD, and S-LPS—is compared. The secure protocols employ a hybrid key agreement mechanism that combines Diffie-Hellman and Short Authentication String (SAS) methods executed over Wi-Fi Direct out-of-band channels, as proposed in our prior conference work [20].

Two main Network Performance Metrics (NPMs) are analyzed: the average end-to-end packet delay and the packet delivery ratio Packet Delivery Ratio (PDR). Each subsection investigates the effect of a specific network parameter on these metrics, with six protocol variants plotted per figure to clearly illustrate the performance trends.

A. System Parameters

The simulation environment is configured to emulate realistic VANET conditions, consistent with the setup described in our previous work [7]. Vehicles operate within a 1000 m² area and communicate over a 200-meter transmission range using a 2 Mbps MAC data rate. Packet flows are generated at a rate of 100 packets per second, with each packet sized at 512 bytes and a bulk data size of 1 KB, as summarized in Table III of our previous work [7].

Vehicle mobility follows the Wiedemann car-following model, calibrated with parameters like safety gaps, acceleration response, and reaction time to realistically simulate urban traffic. Assumptions on vehicular nodes and virtual road segments are listed in Table IV, and calibration factors for the Wiedemann model are detailed in Table V of our previous work [7].

The simulation topology includes four multipath routes connecting the source vehicle at (1000, 1000) and the destination vehicle at (0, 0), passing through four intersections, with four virtual segments between each intersection pair. A central prediction update interval T governs the frequency at which vehicle state information—such as position, speed, and acceleration—is refreshed, directly influencing route connectivity estimation and QoS-based path decisions.

The simulation of secure protocol variants includes randomly generated cryptographic parameters—Diffie-Hellman modulus, base, and private keys to support the hybrid key agreement protocol used for authentication over Wi-Fi direct out-of-band channels.

B. Effect of Vehicular Node Density

To investigate the effect of vehicular node density N, simulations vary N from 10 to 100 nodes in increments of 10, with vehicle speed fixed at 40 m/s and T =1 s.

As shown in Fig. 9, average end-to-end packet delay increases with higher node density due to more extensive routing overhead and longer multi-hop paths. Among all protocols, the LDD variant achieves the lowest delay by favoring longer, more stable routes that reduce route rediscoveries. Secure protocols introduce additional delay overhead due to cryptographic operations; however, S-LDD outperforms other secure variants (S-LPSMD and S-LPS), mirroring the non-secure protocol order.

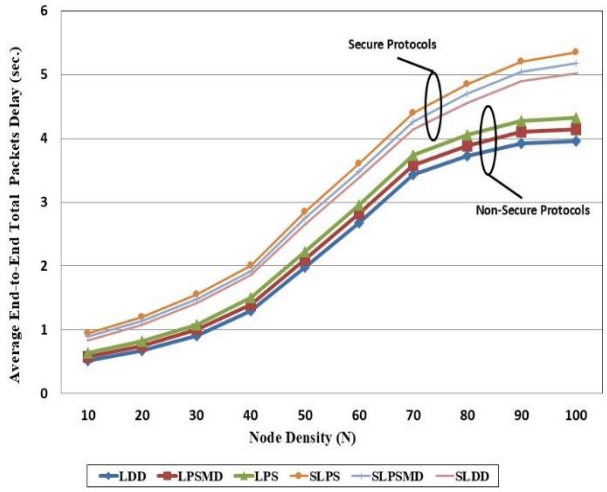

Fig. 9. Average end-to-end packet delay versus vehicular node density for secure and non-secure protocols.

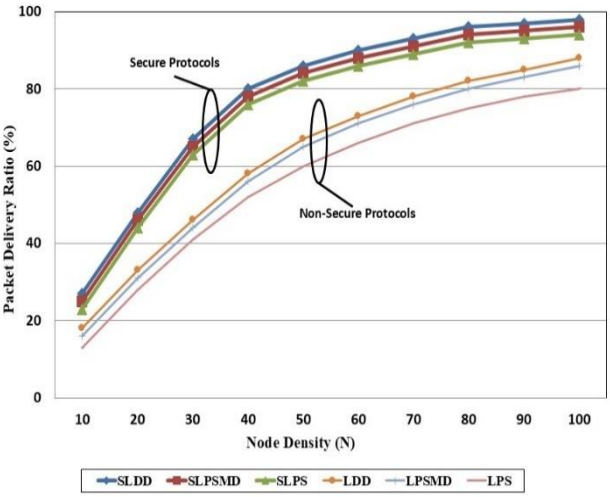

Fig. 10. Packet delivery ratio versus vehicular node density for secure and non-secure protocols.

In Fig. 10, packet delivery ratio improves with increasing node density as connectivity strengthens, and path disconnections reduce. Secure protocols consistently achieve higher delivery ratios than their non-secure counterparts by effectively excluding malicious nodes. The ranking remains LDD > LPSMD > LPS for both secure and non-secure versions.

Discussion: Increasing node density creates a trade-off where routing overhead and delays rise, but improved connectivity enhances packet delivery. Security mechanisms add modest delay overhead but significantly increase delivery reliability.

C. Effect of Average Vehicle Speed

Simulations vary average vehicle speed v between 20 m/s and 65 m/s with 60 nodes and T=1 s. Fig. 11 illustrates that end-to-end delay grows as speed increases due to frequent route failures caused by rapidly changing network topology. LDD remains the most delay-efficient protocol by selecting longer-lived paths. Secure protocols add delay overhead, yet S-LDD still performs best among them.

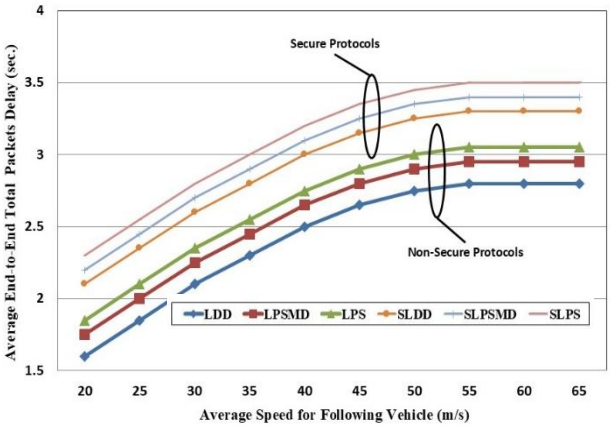

Fig. 11. Average end-to-end packet delay versus average vehicle speed for secure and non-secure protocols.

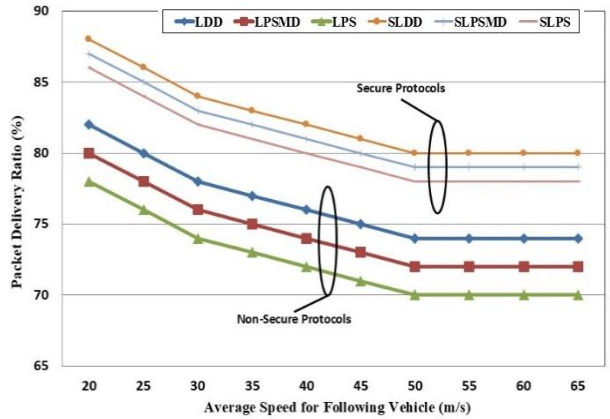

Fig. 12. Packet delivery ratio versus average vehicle speed for secure and non-secure protocols.

Fig. 12 shows a decreasing packet delivery ratio at higher speeds due to path instability. Secure protocols maintain a clear delivery advantage by identifying and avoiding compromised or unstable nodes, with S-LDD leading.

Discussion: Higher mobility challenges routing stability, but secure, adaptive protocols mitigate delivery degradation, balancing delay overhead with security benefits.

D. Effect of Prediction Update Interval (T)

The prediction update interval T is varied from 1 to 10 s, holding node count at 60 and speed at 40 m/s.

In Fig. 13, end-to-end delay increases as T grows, since stale vehicle data reduce route prediction accuracy, leading to more frequent rediscovery. LDD and S-LDD maintain the lowest delays due to their path selection strategies.

To quantify the increase in end-to-end delay over time, we define the relative delay growth (RDG) metric:

$$\mathrm{RDG}[i] = \left(\frac{\mathrm{Delay}[i]-\mathrm{Delay}[1]}{\mathrm{Delay}[1]}\right) \times 100\% \qquad (9)$$

where Delay[1] is the minimum delay recorded at T = 1 s, and Delay[i] is the delay later interval $T = i$. A higher RDG value indicates a greater degradation in delay performance compared to the baseline. Fig. 14 depicts packet delivery ratio decreasing with larger T, reflecting the reduced accuracy of vehicle state predictions. To evaluate the change in packet delivery ratio across time intervals, we introduce the relative delivery drop (RDD) metric:

$$\mathrm{RDD}[i] = \left(\frac{\mathrm{Delivery}[1]-\mathrm{Delivery}[i]}{\mathrm{Delivery}[1]}\right) \times 100\% \qquad (10)$$

where Delivery[1] represents the maximum delivery ratio observed at T = 1 s, and Delivery[i] is the ratio later interval $T = i$. Higher RDD values indicate a greater decline in reliability compared to the optimal state.

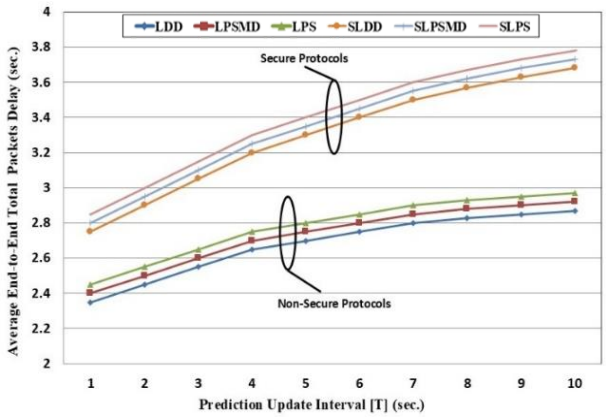

Fig. 13. Average end-to-end packet delay versus prediction update interval T for secure and non-secure protocols.

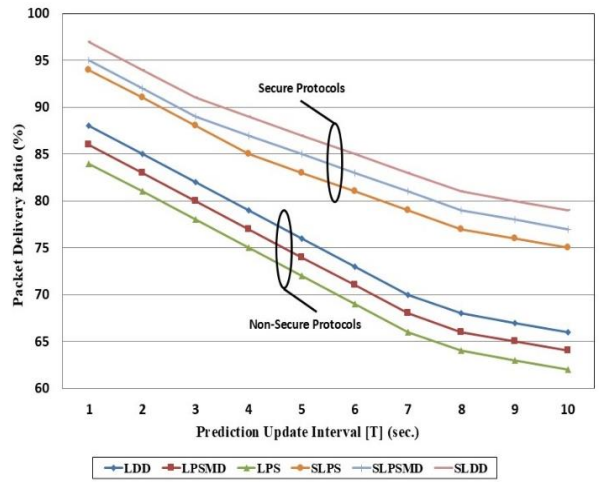

Fig. 14. Packet delivery ratio versus prediction update interval T for secure and non-secure protocols.

Secure protocols consistently outperform non-secure ones in delivery while incurring additional delays, underscoring the trade-off between security and latency.

Discussion: Timely vehicle state updates critically influence routing performance. Secure adaptive routing remains robust even with less frequent updates.

E. Effect of MITMA Density

Malicious nodes vary from 5% to 30% of total vehicles, increasing in 5% increments ($N = \{5, 10, 15, 20, 25, 30\}$). Simulations use a vehicle speed of 40 m/s and a data collection interval of 1 s. As shown in Fig. 15, average end-to-end delay rises sharply with higher MITMA density due to frequent route disruptions and rediscovery. Secure protocols mitigate this by detecting and excluding malicious nodes but incur additional cryptographic overhead.

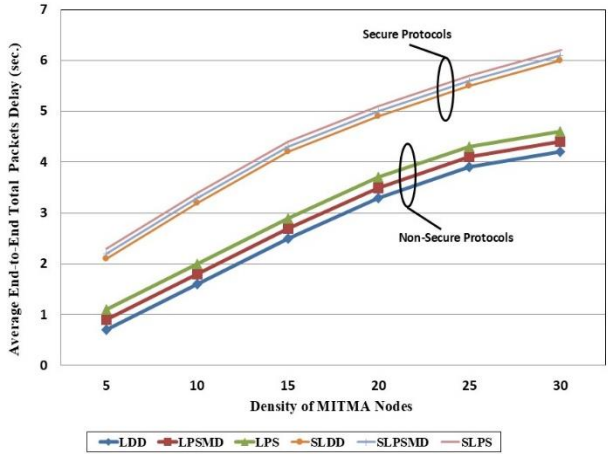

Fig. 15. Average end-to-end packet delay versus MITMA density for secure and non-secure protocols.

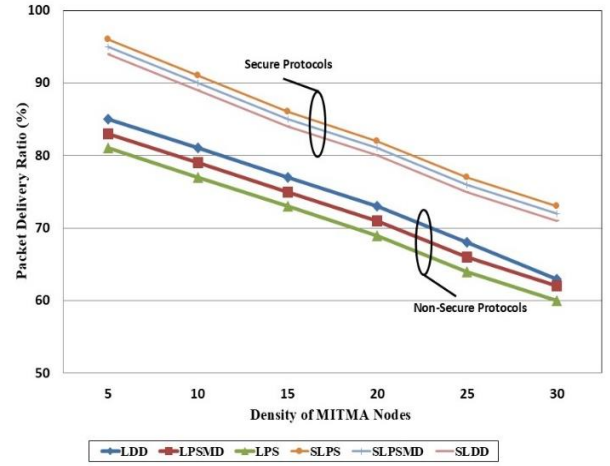

Fig. 16. Packet delivery ratio versus MITMA density for secure and non-secure protocols.

Among the secure strategies, S-LDD achieves the lowest average delay, demonstrating its efficiency in maintaining performance under attack. Fig. 16 shows a substantial improvement in PDR for secure protocols compared to their non-secure counterparts. Notably, S-LDD significantly outperforms all other approaches, highlighting its robustness in hostile network conditions.

Discussion: The integration of security mechanisms significantly enhances network resilience in the presence of active attacks. While this comes with a trade-off in the form of increased packet delay, the resulting protection against malicious behaviour and improved reliability—especially under high attack densities—underscore the importance of adopting secure routing protocols in VANET environments.

In summary, simulation results show that secure multi-path route switching protocols consistently improve packet delivery ratios across all scenarios, especially under high mobility and adversarial conditions, though with increased end-to-end delay due to security overhead. Protocol performance ranking remains stable, with LDD outperforming LPSMD and LPS, mirrored by their secure counterparts. These findings confirm and extend our previous work [7, 20], demonstrating that integrating security significantly enhances VANET reliability without severely impacting delay.

VII. Conclusion and Future Work

This paper presented a secure, agent-based multi-path route switching protocol for VANETs combining predictive connectivity modeling via the Wiedemann car-following model, adaptive QoS-driven strategies (LDD, LPSMD, LPS), and lightweight cryptographic authentication using Diffie-Hellman and SAS over Wi-Fi Direct out-of-band channels. Simulations with QualNet showed that secure variants (S-LDD, S-LPSMD, S-LPS) consistently improved packet delivery ratios across diverse and adversarial conditions, with only moderate increases in end-to-end delay. LDD protocols outperformed LPSMD and LPS, confirming the efficacy of predictive, QoS-aware routing. These results demonstrate that integrating security into VANET routing is feasible without significant performance trade-offs. For real-world deployment, the protocol assumes RSUs have sufficient processing power for cryptographic operations and coordination. Lightweight cryptography and out-of-band Wi-Fi Direct communication minimize overhead, but reliable RSU connectivity and controlled vehicle density are essential to avoid resource strain. Future work will focus on optimizing RSU task distribution and communication scheduling, while enhancing scalability and resilience through machine learning, RSU-edge collaboration, real-world testing, and adaptive security mechanisms. Future work will focus on enhancing scalability and intelligence through machine learning-based prediction, RSU-edge collaboration, real-world trace validation, and dynamic trust and cryptographic adaptation under evolving attack models.

Conflict of Interest

The author declares no conflict of interest.

References

[1] M. Saleh, L. Dong, A. Aljaafreh, and N. Al-Oudat, "Secure location-aided routing protocols with Wi-Fi direct for vehicular ad hoc networks," *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, no. 1, pp. 11–17, 2020.

[2] M. Saleh, "Secure Tilted-Rectangular-Shaped Request Zone Location-Aided Routing protocol (STRS-RZLAR) for vehicular ad hoc networks," *Procedia Comput. Sci.*, vol. 160, pp. 248–253, Nov. 2019.

[3] M. Saleh, "Secure optimized request zone location-aided routing protocols with Wi-Fi direct for vehicular ad hoc networks," *J. Commun.*, vol. 17, no. 3, pp. 156–166, 2022.

[4] A. Dutta, L. M. S. Campoverde, and F. De Rango, "A comprehensive review of recent developments in VANET for traffic, safety & remote monitoring applications," *J. Netw. Syst. Manage.*, vol. 32, 73, Aug. 2024.

[5] T. K. Venkatasamy, M. J. Hossen, R. Gopi, and N. H. Binti A. Aziz, "Intrusion detection system for V2X communication in VANET networks using machine learning-based cryptographic protocols," *Sci. Rep.*, vol. 14, 31780, Dec. 2024.

[6] T. Chatterjee, R. Karmakar, G. Kaddoum, S. Chattopadhyay, and S. Chakraborty, "A survey of VANET/V2X routing from the perspective of non-learning- and learning-based approaches," *IEEE Access*, vol. 10, pp. 23022–23050, 2022.

[7] M. Saleh, "Position-based multipath route switching protocol for intelligent VANETs using Wiedemann car-following model," *Int. J. Electr. Electron. Eng. Telecommun.*, vol. 12, no. 1, pp. 22–34, 2023.

[8] N. M. Quy, V. K. Quy, A. Chehri, and D. M. Linh, "A novel multi-agents-based clustering algorithm for VANETs in 5G networks," *Wireless Networks*, vol. 30, no. 3, pp. 1509–1524, Mar. 2024.

[9] K. Kandali, L. Bennis, O. E. Bannay, and H. Bennis, "An intelligent machine learning based routing scheme for VANET," *IEEE Access*, vol. 10, pp. 74318–74333, 2022.

[10] A. F. Gunes and I. Abasikeles-Turgut, "Recent topology-based routing approaches in VANETs: A review," *Balkan Journal of Electrical & Computer Engineering*, vol. 11, no. 3, pp. 976–997, Jul. 2023.

[11] M. V. K. Reddy, G. K. Kumar, P. V. Terlapu, D. Jayaram, and S. Samreen, "Trust enabled secure routing in vehicular ad hoc networks," *International Arab Journal of Information Technology*, vol. 22, no. 3, pp. 592–613, May 2023.

[12] A. Amalia, Y. Pramitarini, R. H. Y. Perdana *et al*., "A deep-learning-based secure routing protocol to avoid blackhole attacks in VANETs," *Sensors*, vol. 23, no. 19, art no. 8224, 2023.

[13] M. A. Jubair, M. S. Abd Latiff, A. M. H. Al-Zaidi, M. A. Saeed, and M. A. Mohamed, "A QoS aware cluster head selection and hybrid cryptography routing protocol for enhancing efficiency and security of VANETs," *IEEE Access*, vol. 10, pp. 124792–124804, 2022.

[14] R. Ramamoorthy, "An enhanced location-aided ant colony routing for secure communication in vehicular ad hoc networks," *Human-Centric Intelligent Systems*, vol. 4, pp. 25–52, Jan. 2024.

[15] P. K. Pandey, V. Kansal, and A. Swaroop, "PKI-based secure multipath routing for Unmanned Military Vehicles (UMV) in VANETs," *Wireless Networks*, vol. 30, no. 2, pp. 595–615, 2024.

[16] Y. Zhao, L. Yang, and D. He, "Location privacy-preserving routing using order-revealing encryption in VANETs," *IEEE Access*, vol. 11, pp. 77990–78001, 2023.

[17] M. A. Razzaque, M. T. Iqbal, and K. Muhammad, "Secure and efficient RSU-assisted routing protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 4, pp. 3632–3642, Apr. 2022.

[18] S. Kumar and P. Kuila, "Particle swarm optimization-based efficient cluster formation in vehicular networks," in *Proc. Int. Conf. on Signal, Image Processing, Communication and Automation (SIPCOV)*, Atlantis Press, pp. 279–288, Oct. 2024.

[19] E. T. da Silva, J. Macedo, and A. Costa, "CMAF: Context- and mobility-aware forwarding model for V-NDN," *Electronics*, vol. 13, no. 12, 2394, Dec. 2024.

[20] M. Saleh, "Security-based multipath route switching protocol for quality-of-service enhancement in VANETs using Wiedemann car-following model," in *Proc. IEEE Int. Conf. Enabling Technol.: Infrastruct. for Collaborative Enterprises (WETICE)*, 2023. doi: 10.1109/WETICE57085.2023.10477782.

[21] Z. H. Ali and H. A. Ali, "Energy-efficient routing protocol on public roads using real-time traffic information," *Telecommun. Syst.*, vol. 82, pp. 465–486, Mar. 2023.

[22] V. P. Chellapandi, L. Yuan, C. G. Brinton, S. H. Zak, and Z. Wang, "Federated learning for connected and automated vehicles: A survey of existing approaches and challenges," *IEEE Trans. Intell. Veh.*, vol. 9, no. 1, pp. 119–141, Jan. 2024.

[23] H. Xu and Y. Wang, "SROR: A secure and reliable opportunistic routing for VANETs," *Vehicles*, vol. 6, no. 4, pp. 1730–1751, 2024.

[24] Z. Zhang, W. Guo, L. Li, and D. Li, "Blockchain-based multi-path mobile access point selection for secure 5G VANETs," arXiv preprint arXiv:2411.03371, Nov. 2024.

[25] A. M. Ali, M. A. Ngadi, R. Sham, and I. I. Al_Barazanchi, "Enhanced QoS routing protocol for an unmanned ground vehicle, based on the ACO approach," *Sensors*, vol. 23, no. 3, 1431, Mar. 2023.

[26] R. Ezumalai and D. Santhakumar, "Cluster-oriented intelligent secure routing protocol design for strengthened communication in vehicular ad hoc networks," in *Proc. 2025 International Conf. on Advanced Computing Technologies*, Sivalasi, India, 2025. doi: 10.1109/ICoACT63339.2025.11004793

[27] G. Sang, J. Chen, Y. Liu, H. Wu, Y. Zhou and S. Jiang, "PACM: Privacy-preserving authentication scheme with on-chain certificate management for VANETs," *IEEE Trans. on Network and Service Management*, vol. 20, no. 1, pp. 216–228, Mar. 2023.

[28] X.-J. Lin, "On the unforgeability of "privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based VANET," *IEEE Trans. on Information Forensics and Security*, vol. 19, pp. 10371–10372, Jun. 2024.

[29] M. Abdollahzade and R. Kazemi, "An intelligent evolving car-following model," *IEEE Access*, vol. 11, pp. 506–516, 2023.

[30] K. Assafra, B. Alaya, and M. Abid, "Privacy preservation and security management in VANET based to Software Defined Network," in *Proc. 2022 IEEE Wireless Communications and Networking Conference*, Austin, USA, 2022, pp. 96–101.

[31] B. Alaya and L. Sellami, "Toward the design of an efficient and secure system based on the software-defined network paradigm for vehicular networks," *IEEE Access*, vol. 11, pp. 43333–43348, 2023.

[32] K. Saini, K. Namdev and K. Rai, "TMAPS: A Trust-based Mutual Authentication and Privacy in VANET," in *Proc. 2022 3rd International Conference for Emerging Technology (INCET)*, 2022. doi: 10.1109/INCET54531.2022.9824952

[33] Y. Wang, X. Li, X. Zhang, X. Liu and J. Weng, "ARPLR: An all-round and highly privacy-preserving location-based routing scheme for VANETs," *IEEE Trans. on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16558–16575, Sept. 2022.

[34] V. K. Quy, A. Chehri, N. M. Quy, V.-H. Nguyen and N. T. Ban, "An efficient routing algorithm for self-organizing networks in 5G-based intelligent transportation systems," *IEEE Trans. on Consumer Electronics*, vol. 70, no. 1, pp. 1757–1765, Feb. 2024.

[35] P. Chithaluru, R. Uyyala, A. Singh *et al*., "A lightweight energy-efficient routing scheme for real-time WSN-VANET-based applications," *IEEE Trans. on Consumer Electronics*, vol. 70, no. 1, pp. 3820–3826, Feb. 2024.

[36] C. Lu, Z. Wang, W. Ding, G. Li, S. Liu and L. Cheng, "MARVEL: Multi-agent reinforcement learning for VANET delay minimization," *China Communications*, vol. 18, no. 6, pp. 1–11, Jun. 2021.

[37] O. Nakayima, M. I. Soliman, K. Ueda and S. A. E. Mohamed, "Combining software-defined and delay-tolerant networking concepts with deep reinforcement learning technology to enhance vehicular networks," *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 721–736, Mar. 2024.

[38] S. Baccari, M. Hadded, H. Touati and P. Muhlethaler, "A secure trust-aware cross-layer routing protocol for vehicular ad hoc networks," *Journal of Cyber Security and Mobility*, vol. 10, no. 2, pp. 377–402, May 2021.

[39] A. Salim, A. M. Khedr, B. Alwasel, W. Osamy and A. Aziz, "SOMACA: A new swarm optimization-based and mobility-aware clustering approach for the internet of vehicles," *IEEE Access*, vol. 11, pp. 46487–46503, 2023.

[40] R. M. Maliya, K. Patel, R. Shanmugam and D. Khaitan, "An overview of safety using information routing protocol in vehicular ad hoc network," in *Proc. 2023 IEEE 11th Region 10 Humanitarian Technology Conference (R10-HTC)*, Rajkot, India, 2023, pp. 760–765.

[41] M. Garai, M. Sliti, M. Mrabet, N. Boudriga and L. B. Ammar, "Authentication in QoS aware VANET: An approach based on enhanced digital certificates," *IEEE Access*, vol. 12, pp. 124452–124477, 2024.

[42] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, B. A. Mohammed *et al*., "Integrating safety in VANETs: A taxonomy and systematic review of VEINS models," *IEEE Access*, vol. 12, pp. 148935–148960, 2024.

[43] J. Redondo, N. Aslam, J. Zhang and Z. Yuan, "Multi-agent assessment with QoS enhancement for HD map updates in a vehicular network and multi-service environment," *IEEE Trans. on Network Science and Engineering*, vol. 12, no. 2, pp. 738–749, 2025.

[44] R. M. A. Latif, M. Jamil, J. He, and M. Farhan, "A novel

authentication and communication protocol for urban traffic monitoring in VANETs based on cluster management," *Systems*, vol. 11, no. 7, 322, Jul. 2023.

[45] A. Chaudhari, K. K. Srinivasan, B. R. Chilukuri *et al*., "Calibrating Wiedemann-99 model parameters to trajectory data of mixed vehicular traffic," *J. Transp. Res. Rec.*, vol. 2676, no. 1, pp. 718–735, 2022.

Ma'en S. Saleh received his Ph.D. degree in electrical and computer engineering from Western Michigan University in 2012. He joined the Faculty of Tafila Technical University as an assistant professor of ECE in 2012. He joined the ECE Department at Baylor University, TX in 2016 as a postdoctoral researcher. He was promoted to professor in 2023. In 2024, he joined the Department of Computer Science & Software Engineering at the University of Detroit Mercy. His research interests include real-time scheduling for packet switched networks, security in VANETs, simulating real-time networks, real-time agent-based systems, and QoS for heterogeneous networks.