Wiley
Journal of Computer Networks and Communications
Volume 2025, Article ID 8771020, 16 pages
https://doi.org/10.1155/jcnc/8771020

WILEY

Research Article

Improving the Efficiency of a Message Validation System in a Vehicular Ad Hoc Network

Mulatu Yirga Beyene,[1] Salahadin Seid Musa,[2] Habtamu Molla Belachew,[1] Behaylu Tadele Alemu,[3] Amogne Andualem Ayalew,[4,5] and Melaku Lake Tegegne[4,5,6]

[1] *Department of Information Technology, Debark University, Debark, Ethiopia*
[2] *Department of Computer Science, Wollo University, Wollo, Ethiopia*
[3] *Department of Computer Science, Debark University, Debark, Ethiopia*
[4] *Computing Center, Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049, China*
[5] *University of Chinese Academy of Sciences, Beijing 100049, China*
[6] *Multi-Disciplinary Research Division, Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049, China*

Correspondence should be addressed to Amogne Andualem Ayalew; amogneandualem@gmail.com

Received 7 June 2024; Revised 20 July 2025; Accepted 2 August 2025

Academic Editor: Farooque Azam

Advancements in communication technologies have enabled vehicles to be equipped with computing devices, facilitating communication and autonomous operations. This has led to the emergence of a new networking paradigm known as the vehicular ad hoc Network (VANET). A primary objective of VANET is to enhance road safety and traffic efficiency by enabling the exchange of information among vehicles in various intelligent transportation system (ITS) applications. Vehicles regularly transmit safety messages at a fixed rate, typically 10 messages per second. In high-traffic scenarios, such as multilane highways or densely packed areas, a vehicle may receive an overwhelming number of safety messages. However, before these messages can be reliably used, they must undergo rigorous cryptographic verification. A significant challenge arises when the message reception rate exceeds the verification rate, leading to inefficiencies. In existing schemes, the basic safety messages (BSMs) of nearby vehicles often undergo redundant verification due to consecutive broadcasts, while BSMs from more distant vehicles within the communication range may not receive adequate verification time. To address this issue, we propose a trust-based approach to improve the efficiency of message verification in VANET. Our simulation results demonstrate that the proposed method optimizes verification time by selectively skipping the verification of one BSM for trusted vehicles, utilizing the road side unit (RSU). This approach enhances vehicle awareness in compliance with the WAVE standard. The study findings indicate that the proposed method achieves an average awareness quality of 85% for neighboring vehicles, outperforming the existing MLPQ-CA method, which attains only 70% within the same 100-m communication range.

Keywords: basic safety message; digital signature algorithm; message verification; road side unit; transportation system; vehicular ad hoc network

1. Introduction

Intelligent transportation systems (ITS) are being extensively implemented in prominent countries worldwide to enhance transportation system performance greatly. This includes reducing traffic congestion, enhancing safety, and improving convenience for travelers. Thanks to advancements in information technology (IT), various ITS components, such as vehicles, roads, traffic lights, and message signs, are intelligent by integrating microchips and sensors. This enables them to communicate wirelessly with each other, transforming them into intelligent entities capable of exchanging information. Vehicular ad hoc network (VANET) is an integral component of ITS and is a distinctive class of mobile ad hoc network (MANET), in which nodes in the network are moving vehicles and a roadside unit (RSU) is deployed along the roadside. The VANET is moving vehicles, and the RSU is deployed along the road roadside. VANET has a great deal of attention in the area of wireless and communication technology and is becoming one of the prominent research areas in the ITS because it provides both safety and comfort for drivers and passengers [1].

Based on the information provided in [2], there are three types of communication in VANETs. These types of communication aim to enhance road safety, provide better traffic control, and enable infotainment applications by accessing the Internet. The first type is intervehicle communication or V2V communication which aims to ensure road safety. The other type of communication is V2I communication; it occurs between a vehicle and RSU and focuses on providing better traffic control. Another type of communication is inter-road side communication which takes place between RSUs; it aims for infotainment applications by accessing the Internet. In the VANET, communication is possible through various components; these are RSU, the onboard unit (OBU) which helps the vehicle to communicate with the other vehicle on the infrastructure and pass appropriate information for traveling, and the application unit (AU) which makes communication possible within the vehicle. This application is used by the driver of the vehicle or the passengers traveling in the vehicle [3]. Due to the variable speed of vehicles, communication among them cannot be always direct, so VANETs follow dedicated short-range communication (DSRC).

One of the main objectives of the VANET is safety message dissemination which relies on broadcast communication, among vehicles. However, the main challenge in transportation is how to enhance road safety. According to the World Health Organization (WHO), the report shows that the road traffic death number globally has reached 1.35 million per year and injured people are 25 to 60 million [4]. Every 24 seconds someone dies on the road, and road traffic crashes ranked as 9th leading cause of death. Several researchers show that 70% of accidents can be avoided if the driver gets a warning even before half a second of the accident [5]. Road traffic damages are now the foremost killer of people aged 5–29 years. According to the authors in [4, 6], 95% of accidents occurred because of poor or wrong decision-making of drivers. In general, 85% of drivers did not pay attention within a few seconds of an accident.

Vehicles receive many basic safety messages (BSMs) periodically then, they need to verify its signature using cryptographic techniques. In high-density traffic, the number of incoming messages will exceed the capability of verifying [7]. Thus, many studies suggest that the most important BSMs should be verified first. Based on the information from the Wireless Access in Vehicular Environments (WAVE) standard [8], vehicles are advised to regularly send safety messages to their immediate neighboring vehicles. These safety messages should be broadcast at a frequency of either 100 milliseconds or 300 milliseconds. Due to this high frequency of broadcasting, a large number of BSMs are transmitted from the sender vehicle to the receiving vehicle. Consequently, the receiving vehicles need to process and verify a significant amount of safety messages, although the number of unique messages to be verified is relatively small.

To illustrate, consider a situation on a busy highway where the broadcast interval is set to 100 milliseconds, and approximately 200 vehicles are within the one-hop communication range of a specific vehicle [9]. In such a case, the receiving vehicle could potentially receive and process up to 2000 BSMs per second. Verifying an elliptic curve digital signature algorithm (ECDSA) takes, on average, 4.97 ms per message [10]. Consequently, the verification rate is limited to 400 messages per second, which is significantly lower than the message reception rate [9–12]. To address this issue, various studies have proposed prioritization schemes to select and verify messages based on their relevance to safety-critical applications. It is essential to verify messages about traffic conditions to determine whether they come from valid or invalid sources. In high-density VANET scenarios, vehicles often have similar movements [10]. Existing schemes often lead to redundant verification times (VTs) for nearby vehicles' BSMs due to consecutive broadcasts. Unfortunately, BSMs from more distant vehicles, still within the communication range, may not receive sufficient VT. To overcome this problem, we propose a novel trust-based approach to improve the efficiency of the message verification process in the VANET. While proximity-based prioritization improves verification efficiency, it does not account for relative movement direction, a critical factor in collision risk assessment. Vehicles traveling toward each other (e.g., on opposite lanes of a highway) rarely require immediate safety interventions, whereas same-direction vehicles (e.g., in adjacent lanes) demand higher-priority verification due to higher collision likelihood. Integrating directionality into the prioritization logic ensures computational resources being allocated to the most safety-critical messages. This study addresses the following research questions:

- ✓ How can awareness accuracy between neighboring vehicles in the communication range be improved?
- ✓ To what extent the proposed work is efficient compared with the existing one to verify the message?
- ✓ What are the relevant parameters and performance metrics for enhancing message verification and evaluating the proposed scheme?

2. Related Works

As described in [10], two primary methodologies are widely recognized for prioritizing safety messages during verification processes in VANETs. These methodologies are differentiated by their implementation points: transmitter-side and receiver-side safety message prioritization schemes. The former refers to the prioritization mechanisms applied at the transmitting node before messages are disseminated, while the latter involves prioritization criteria executed at the receiving node after messages are received. Both approaches aim to enhance the reliability and timeliness of safety-critical communications by systematically managing message verification in dynamic VANET environments.

As shown in Figure 1, BSM scheduling approaches based on their location of control such as transmitter or receiver and based on adaptation strategy fixed, adaptive, or random. However, the hybrid category signifies the use of multiple techniques to optimize performance of the system.

2.1. Transmitter-Side Safety Messages Prioritization Techniques. As described in [10], the prioritization of safety messages at the sender's end in VANETs is influenced by specific parameters, including the transmission rate, transmission power, contention window (CW) size, or a hybrid of these components. These factors collectively govern how safety messages are ranked and managed by the transmitting node prior to dissemination. For instance, adjusting the transmission rate controls how frequently messages are broadcast, modifying transmission power affects their range and reliability, and tuning the CW size regulates access to the communication channel. By optimizing these variables, the sender-side prioritization scheme ensures that critical safety messages are allocated appropriate precedence, enhancing their timely delivery and reducing latency in dynamic vehicular networks.

2.1.1. Fixed Rate Transmission of Safety Messages. The WAVE standard, as specified in VANET implementations, operates with a predetermined transmission rate for safety-critical messages, commonly set at 10 messages per second [13]. To maintain quality of service (QoS) requirements at the medium access control (MAC) layer, the WAVE protocol integrates the enhanced distributed channel access (EDCA) mechanism, which categorizes traffic into four distinct priority levels (AC3, AC2, AC1, and AC0) to manage transmission prioritization [8]. Within this framework, messages assigned to higher-priority access categories (e.g., AC3) are granted preferential channel access through reduced contention intervals and shorter arbitration periods, thereby increasing their likelihood of timely transmission compared to lower-priority messages (e.g., AC0). This structured prioritization ensures that critical safety communications, such as collision warnings or emergency alerts, receive expedited handling, optimizing network efficiency and reliability in dynamic vehicular environments.

2.1.2. Adaptive Rate Transmission of Safety Messages. As described in [14], this approach dynamically adjusts the transmission rate of safety messages according to the real-time state of the VANET. The proposed method introduces a framework where vehicles are organized into clusters determined by their mobility patterns. Within each cluster, a leader-referred to as the cluster head is selected based on criteria such as relative speed and proximity to other cluster members. This designated leader oversees the regulation of safety message dissemination, managing both intracluster communication and intercluster data exchange. By prioritizing adaptive transmission rates and hierarchical cluster coordination, the scheme aims to optimize network efficiency and ensure timely delivery of critical safety information in dynamic vehicular environments.

2.1.3. Adaptive Transmission Power of Safety Messages. As described in the referenced scheme, the communication range is dynamically modified through the regulation of transmission power levels. By amplifying the transmission power, the operational radius of communication is extended, allowing a vehicle to disseminate messages across greater distances. Conversely, diminishing the transmission power restricts the broadcast range, thereby concentrating signal coverage to nearby vehicles. This proximity-based prioritization mechanism ensures that vehicles in closer vicinity receive higher priority, as reduced transmission power inherently limits message dissemination to shorter ranges. Consequently, the system optimizes resource allocation and prioritizes critical safety communications for nearby entities, balancing coverage and urgency in vehicular networks.

2.1.4. Adaptive CW Size for Transmitting Safety Messages. The 802.11p WAVE protocol utilizes an adaptive CW size mechanism to enhance the prioritization and efficiency of safety message transmission at the MAC layer. This scheme dynamically adapts the CW parameter based on message priority. By decreasing the CW size, the protocol prioritizes critical safety messages, thereby minimizing transmission delays and ensuring timely delivery. This adjustment allows high-priority communications to access the channel more quickly, improving responsiveness in scenarios where latency reduction is crucial. Conversely, the protocol increases the CW size for lower-priority or noncritical messages, effectively deprioritizing them. A larger CW reduces the likelihood of such messages gaining channel access, limiting their opportunities for transmission. This dynamic balancing ensures network resources are allocated preferentially to safety-related data, optimizing overall system performance while maintaining fairness among competing transmissions. The adaptive approach thus enhances both reliability and efficiency in vehicular communication environments.

2.2. Receiver-Side Safety Messages Prioritization Techniques. Although prioritizing safety messages at transmitters can decrease the rate at which signals reach receivers, this approach neglects to account for the receiver's processing capacity or communications from adjacent vehicles. Consequently, prioritizing safety signals at the receiver becomes essential to reliably process a greater number of BSMs from nearby transmitting vehicles, particularly those more likely to be implicated in safety-critical situations. By shifting prioritization to the receiver, the system can better address dynamic conditions and proximity-related risks. Receiver-based prioritization strategies can be grouped into three distinct methodologies: random selection, batch processing,

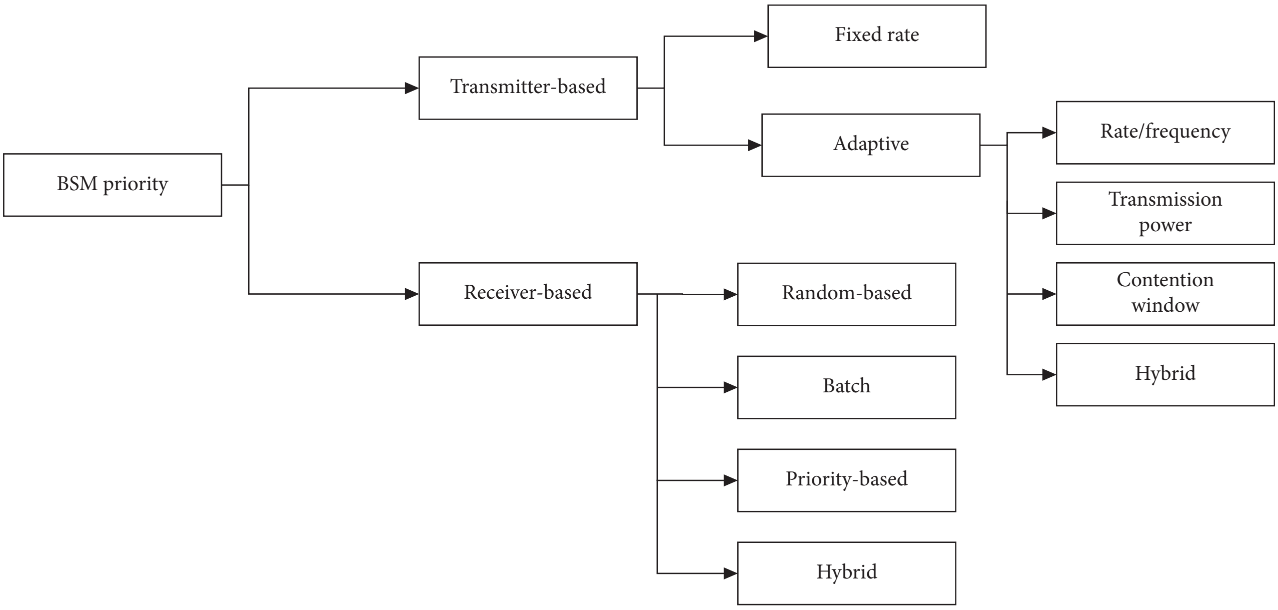

Figure 1: BSM prioritization scheme categories: adapted from [10].

and priority-driven schemes. Each method offers varying mechanisms to manage incoming signals, balancing efficiency and relevance based on real-time contextual factors.

2.2.1. Random-Based Verification Scheme. The random-based verification scheme, introduced by the authors in [15], aims to bolster system security and scalability by randomly selecting messages from the buffer for verification. While this method has been widely adopted in authentication frameworks such as those described by the authors in [16], due to its operational simplicity, a key limitation persists: Critical messages may experience delayed verification or remain entirely unverified. The randomness inherent in the selection process does not inherently prioritize time-sensitive or high-priority messages, which could lead to scenarios where essential data fail to undergo verification within required time frames. This lack of deterministic prioritization risks undermining the system's reliability, particularly in environments where timely authentication of specific messages is crucial.

2.2.2. Batch Verification Scheme. Batch Verification Scheme: In this approach, a receiver aggregates incoming BSMs into a group and performs simultaneous verification for the entire batch. By processing multiple messages collectively, the scheme significantly reduces the average VT required per BSM. This method optimizes computational efficiency by leveraging batch-level operations rather than individual checks. However, the technique introduces certain trade-offs. Accumulating messages into a batch prior to verification inherently causes a processing delay, as the system must wait to compile the group before initiating validation. This additional latency may impact real-time performance in time-sensitive applications. Furthermore, the integrity of the entire batch becomes contingent on the validity of every individual message within it. If even a single BSM in the batch contains an invalid or falsified signature, the verification process for the entire group may fail, necessitating retries or alternative validation measures. These limitations highlight the need to balance efficiency gains with reliability and latency requirements in practical implementations.

2.2.3. Priority-Based Verification Scheme. The priority-based verification scheme is a method where a vehicle leverages mobility data, such as velocity, heading, and direction, extracted from BSMs received from nearby vehicles to prioritize incoming BSMs within a buffer queue. As previously noted, two primary approaches exist for prioritizing safety messages during verification in VANETs: transmitter-side and receiver-side schemes. This study focuses on receiver-side techniques, which are examined in detail in this section. Existing receiver-side prioritization strategies are discussed, emphasizing their mechanisms and limitations.

One such approach, proposed by the authors in [16], introduces a verification system that randomly selects messages from the buffer to enhance security and scalability. While this method has been adopted in various authentication frameworks, such as those in [10], due to its straightforward implementation, it faces a critical drawback: The random selection process risks delaying or entirely omitting the verification of time-sensitive or critical messages. This limitation highlights a potential vulnerability in scenarios where urgent safety-related data must be processed promptly to ensure vehicular safety and system reliability.

Random-based verification schemes mitigate congestion in security queues by verifying only a subset of BSMs. These methods reduce computational and communication overhead by randomly approving messages at the transmitter, rather than subjecting all transmissions to exhaustive security checks. To further optimize efficiency, the verification process at the OBU employs random BSM selection, thereby minimizing end-to-end delays. A specific implementation of this approach, introduced by the authors in [17], leverages offline data preloaded into a central authority. This design streamlines the validation and authentication of safety-critical messages, significantly lowering security-related resource demands. By prioritizing randomness in message approval and verification, such schemes balance security robustness with operational efficiency in resource-constrained vehicular networks.

In the batch verification approach, the receiver accumulates incoming BSMs into a batch and conducts collective verification on the entire group simultaneously. This process reduces the average VT per individual BSM by consolidating computational efforts. However, the technique introduces inherent limitations, including latency resulting from the need to wait for a sufficient number of messages to form a batch before initiating verification. Furthermore, the integrity of the entire batch becomes contingent on the validity of every included message; a single BSM with an invalid or fraudulent signature can compromise the verification outcome for the entire group. This dependency necessitates discarding or reverifying the entire batch if an error is detected, potentially negating efficiency gains and wasting computational resources. While the method optimizes processing time under ideal conditions, these trade-offs highlight vulnerabilities in scenarios with unreliable data sources or stringent real-time requirements.

Batch-based verification techniques aggregate multiple packets to enable their simultaneous authentication. The protocol presented in [18] leverages a binary authentication tree structure for batch verification, designed specifically to authenticate groups of BSMs. Similarly, another approach outlined in [19] employs bilinear mapping and pseudonymous identity generation derived from private keys to facilitate efficient batch verification of BSMs. While these methods enhance computational efficiency by processing multiple packets collectively, a significant limitation arises when a batch fails authentication. In such cases, all packets within the batch even valid ones are discarded due to the inability to isolate individual errors. This drawback results in the loss of numerous packets, undermining reliability in scenarios where even minor authentication failures occur. Thus, while batch verification optimizes resource usage, it introduces risks of data loss that must be carefully weighed against its benefits.

In priority-based verification schemes, vehicles utilize mobility-related data, including velocity, heading, and direction, extracted from BSMs received from neighboring vehicles. These parameters enable the prioritization of incoming BSMs within a buffer, ensuring critical messages are processed first. The prioritization mechanism relies on spatial and contextual information embedded in the BSMs, such as GPS coordinates, heading angles, and the relative proximity between the transmitting and receiving vehicles. This approach ensures resource-efficient verification by focusing computational efforts on messages originating from vehicles in closer physical proximity to the receiver. For instance, resource-aware BSM verification frameworks, as discussed in [20], leverage the spatial relationship between transmitters and receivers to optimize processing. Further enhancements to this methodology include the use of metric bloom filters to assess the significance of BSMs, as explored in [10], and zonal partitioning strategies that segment geographic areas based on vehicle mobility patterns, as proposed the authors in [9]. These techniques refine prioritization by dynamically adjusting to the spatial and temporal dynamics of traffic environments. However, a notable limitation of such schemes lies in their reliance on preauthentication proximity calculations between transmitters and receivers. Since proximity cannot be definitively determined until a BSM is authenticated, the effectiveness of prioritization may be compromised, potentially delaying critical safety-related processing. This dependency introduces a circular challenge, as authentication itself often requires prior knowledge of proximity, highlighting a fundamental trade-off in priority-based verification systems.

To prioritize relevant BSMs within a receiving vehicle's buffer, the method employs a hierarchical scheme that evaluates BSMs according to spatial proximity (zones), geographic location, directionality, the transmitting vehicle's quadrant, and relative time, as proposed in [9]. Central to this approach is the relative time zone (RTZ) framework, which dynamically adjusts discrete zones based on human reaction time thresholds and network density. By design, messages originating from closer zones with lower relative times are assigned higher verification priority, ensuring timely processing of critical safety data. A key limitation of this methodology lies in its exclusive reliance on mobility-related parameters, which may expose the system to security vulnerabilities. Since prioritization decisions are driven solely by dynamic spatial and temporal factors, malicious actors could potentially manipulate or spoof such data, undermining the integrity of the verification process. This underscores the need for supplementary security mechanisms to complement the existing zone-based prioritization architecture.

To enhance the RTZ framework and optimize the verification process of safety messages, the historical relative-time zone (HRTZ) method has been introduced [10]. The core innovation of HRTZ lies in its integration of a historical record of BSMs, which are systematically stored to eliminate redundant verification attempts. By maintaining this historical log, the system ensures that previously verified messages are not reprocessed, thereby reducing computational overhead and enhancing efficiency. A critical objective of HRTZ is to guarantee that the receiver's buffer exclusively retains the latest message transmitted by each vehicle. This approach not only mitigates data redundancy but also ensures that safety-related decisions are based on the most up-to-date information available. Consequently, HRTZ strengthens the reliability of vehicular communication systems by prioritizing temporal relevance and minimizing resource wastage through intelligent message management.

The authors in [19] propose a novel batch verification method for signatures that employs a weighted priority-based approach. Rather than relying on absolute priority metrics, the study introduces a weighted priority mechanism to dynamically form groups, enhancing flexibility in batch processing. Additionally, the work formulates a rebatching mechanism, which is thoroughly detailed to optimize verification efficiency. In a separate contribution, the authors in [21] introduce a critical-aware elliptic curve digital signature verification algorithm designed for vehicular networks. The central concept involves prioritizing the verification of incoming BSMs by categorizing them into distinct queues based on urgency. A multilevel priority queue (MLPQ) system is implemented, enabling vehicles to schedule message verification according to predefined priority levels. To further refine this process, the study models the dispatching of BSMs based on physical distance into multilevel queues and analyzes critical message distribution using a Markov chain framework. This approach dynamically determines priority assignments within the MLPQ system, ensuring timely verification of safety-critical communications.

In [22], the authors introduced a zone priority scheme designed to optimize the verification process for BSMs by prioritizing the most critical ones. The proposed approach addresses a key challenge in high-density traffic environments, where OBUs in vehicles may receive thousands of BSMs per second. Given the limited computational resources available on OBUs, it becomes impractical to authenticate every incoming message in real time. To mitigate this issue, the zone priority-based verification framework aims to enhance efficiency by categorizing BSMs according to predefined spatial zones, thereby identifying and deprioritizing messages from zones deemed less relevant to the vehicle's immediate safety context. The scheme operates by dynamically assessing the geographical relevance of BSMs, prioritizing those originating from zones closer to the vehicle or areas with higher potential safety risks. By filtering out messages from distant or low-priority zones, the system reduces computational overhead while ensuring that safety-critical information from proximate or high-risk regions is verified promptly. This method not only improves resource allocation but also maintains the integrity of safety-related decision-making processes in dense vehicular networks, where timely verification is essential for collision avoidance and traffic coordination. The work in [22], thus provides a structured solution to scalability challenges in vehicular communication systems under high-load conditions.

The authors in [23] introduced an ECDSA approach integrated with BSM authentication for vehicular networks. This method enhances security and ensures robust safety for vehicles during message transmission. The study demonstrated that ECDSA outperforms other cryptographic algorithms by offering faster computation, greater efficiency, reduced memory consumption, and minimized delays, thereby aligning with the stringent requirements of VANETs. In contrast, the work presented in [12] addressed security vulnerabilities related to mobility information in BSMs by leveraging BSM signal strength. The proposed methodology clusters incoming messages into five predefined safety zones using the K-means clustering algorithm, assigns BSMs to their respective zones, and verifies messages based on their arrival timestamps.

However, the scheduling strategies for message verification often fail to prioritize BSMs in the buffer according to the proximity of vehicles, despite ITS application guidelines emphasizing that nearby vehicles' BSMs should be authenticated ahead of those from distant vehicles even within designated safety zones. This gap highlights a critical challenge in ensuring timely verification of high-priority messages, which is essential for maintaining real-time safety in dynamic vehicular environments. Both studies underscore the importance of optimizing cryptographic and clustering techniques to meet VANETs' unique demands, balancing security, efficiency, and latency constraints. To address the limitations of conventional prioritization frameworks in safety-critical environments, we introduced a novel queuing methodology designed to optimize message handling within safety zones. The proposed approach dynamically prioritizes incoming safety messages by evaluating the physical proximity between transmitters and receivers (i.e., transmitter–receiver distance). In scenarios where multiple transmitters exhibit comparable distances to the receiver, the system further refines prioritization using the temporal sequence of message arrivals (arrival time). This dual-criteria mechanism ensures that only messages originating within predefined safety boundaries are allocated VT, thereby guaranteeing that BSMs from nearer vehicles are authenticated ahead of those from distant ones. By hierarchically ordering messages based on spatial and temporal relevance, the framework significantly reduces the queuing latency for BSMs generated by proximate vehicles. Consequently, the waiting time for verification in the security queue is minimized for nearby transmitters, enhancing the timeliness of critical safety data dissemination. Furthermore, this prioritization strategy improves collaborative situational awareness among neighboring vehicles by ensuring that spatially relevant information is processed and propagated with higher fidelity. Comparative evaluations demonstrate that the proposed method achieves superior cooperative awareness accuracy relative to the existing schemes, validating its efficacy in real-time safety applications.

In the existing VANET systems, BSMs transmitted by nearby vehicles frequently undergo redundant VT allocations due to sequential broadcasting mechanisms. This redundancy arises because consecutive broadcasts from proximate vehicles are prioritized, inadvertently leading to inefficient resource utilization. Conversely, BSMs originating from vehicles situated at the edge of the communication range often experience insufficient VT, compromising their reliability and increasing the likelihood of message rejection. This disparity in verification prioritization undermines intervehicle awareness and elevates BSM drop rates, posing risks to network efficiency and safety. To address this issue, a novel trust-based methodology has been proposed to optimize the message verification framework in VANETs. By dynamically prioritizing BSM verification based on contextual trust metrics such as historical message consistency, proximity relevance, and network congestion levels, the approach aims to balance verification resource allocation across all vehicles within the communication range. This strategy seeks to enhance mutual awareness among neighboring vehicles while minimizing redundant verification delays for nearby sources. Consequently, it maximizes the number of BSMs successfully processed by receivers, thereby reducing drop rates and improving overall system reliability. The proposed scheme aligns with the goal of fostering scalable and secure vehicular communication infrastructures capable of adapting to dynamic traffic environments.

3. Proposed Model

This study addresses a specific limitation in the existing VANET schemes by proposing an enhanced message verification approach aimed at improving efficacy in ITS safety applications. To achieve this, vehicles dynamically partition their surrounding geographical regions into multiple zones using two distinct parameters derived from BSMs: received signal strength (RSS) and arrival time. Notably, these parameters are utilized in a manner of diverging from conventional methods. By leveraging BSM signal strength, the road is segmented into five fixed safety zones, thereby mitigating security concerns associated with message clustering and information integrity in BSMs.

A core enhancement to the existing scheme from [12] involves redesigning the ranking module responsible for prioritizing safety messages. This modification enables message verification based on the relative proximity of transmitting vehicles to the receiver. To optimize queuing delays for nearby vehicles, a novel BSM ranking mechanism is introduced, which prioritizes messages first by the distance between transmitting and receiving vehicles, and second, by BSM arrival time in cases of equidistant senders. Additionally, to address verification delays and enhance situational awareness in dense network scenarios, a trust-based strategy is proposed. This method tracks validated BSMs within designated zones and, when the count exceeds, a predefined threshold bypasses signature verification for subsequent BSMs from trusted transmitters. This adaptation relies on historical communication reliability between devices, streamlining verification processes while maintaining security. The subsequent section elaborates on the architectural framework of the proposed system, detailing its integration with the existing VANET infrastructures and the operational logic underpinning its verification and prioritization modules.

Figure 2 displays a proposed system for processing incoming BSMs in a vehicular network, with an emphasis on security verification and filtering. However, the current system encounters verification redundancy for nearby vehicles in densely populated network scenarios, except for those within the same zone, where the VT fails to meet the stringent requirements of ITS safety applications. To address this limitation, a trust-based approach has been implemented. This method validates BSMs by counting those exceeding a predefined threshold. Specifically, the system requests confirmation from a RSU to verify whether the pseudo-identifier (pseudo-ID) of the subsequent BSM corresponds to a legitimate real ID. Upon receiving an affirmative response from the RSU, the signature verification process is expedited, allowing the system to proceed to the next BSM. Furthermore, unverified BSMs are granted a single additional opportunity for verification. This modification enhances the likelihood of validating distant or previously overlooked BSMs (thereby improving awareness of vehicles farther from the receiver), optimizes verification latency, and minimizes packet loss rates. By prioritizing trust-based validation and iterative verification attempts, the proposed approach ensures compatibility with the real-time demands of ITS safety protocols while maintaining network efficiency.

3.1. The Proposed BSM Prioritization Scheme

3.1.1. BSM-Classification. In the safety message ranking approach, BSMs are first clustered into five predefined safety areas (SAs) using the K-means clustering algorithm. These BSMs are subsequently classified according to their RSS, enabling their assignment to priority queues corresponding to SAs ranked from highest to lowest criticality. A key advantage of this method lies in structuring the priority queues based on RSS-derived clusters, which enhances the scheme's resistance to tampering or alteration attacks. By design, BSMs in lower-priority SAs cannot bypass those in higher-priority queues during verification, thereby ensuring strict adherence to the prioritization hierarchy and preventing undeserved resource allocation. The clustering process is critical for organizing BSMs in VANETs to prioritize safety-related communication effectively. By categorizing BSMs into five clusters using RSS values which correlate to the proximity and urgency of safety zones, the system ensures that messages from high-risk areas receive immediate attention. This hierarchical ordering guarantees that verification resources are allocated first to the most critical BSMs, directly aligning with the safety requirements of the vehicular environment. Consequently, the integrity of the prioritization mechanism is maintained, as lower-priority clusters are systematically processed only after higher-priority ones, eliminating opportunities for malicious exploitation of verification timelines.

3.1.2. BSM-Ranking. To prioritize BSMs within their designated safety zones and extract them from the MLPQ module for verification processing, the following methodology is applied. Initially, the safety zones defined by the BSM-classifier are adopted, after which the proposed ranking mechanism is executed on incoming BSMs relative to their assigned zones. This prioritization relies on three key parameters: (1) the relative directionality between transmitter and receiver vehicles, (2) the distance between vehicles, and (3) in cases where multiple vehicles share comparable distances and directionality, the arrival time of BSMs [12]. To elucidate the selection of ranking criteria, three scenarios are examined.

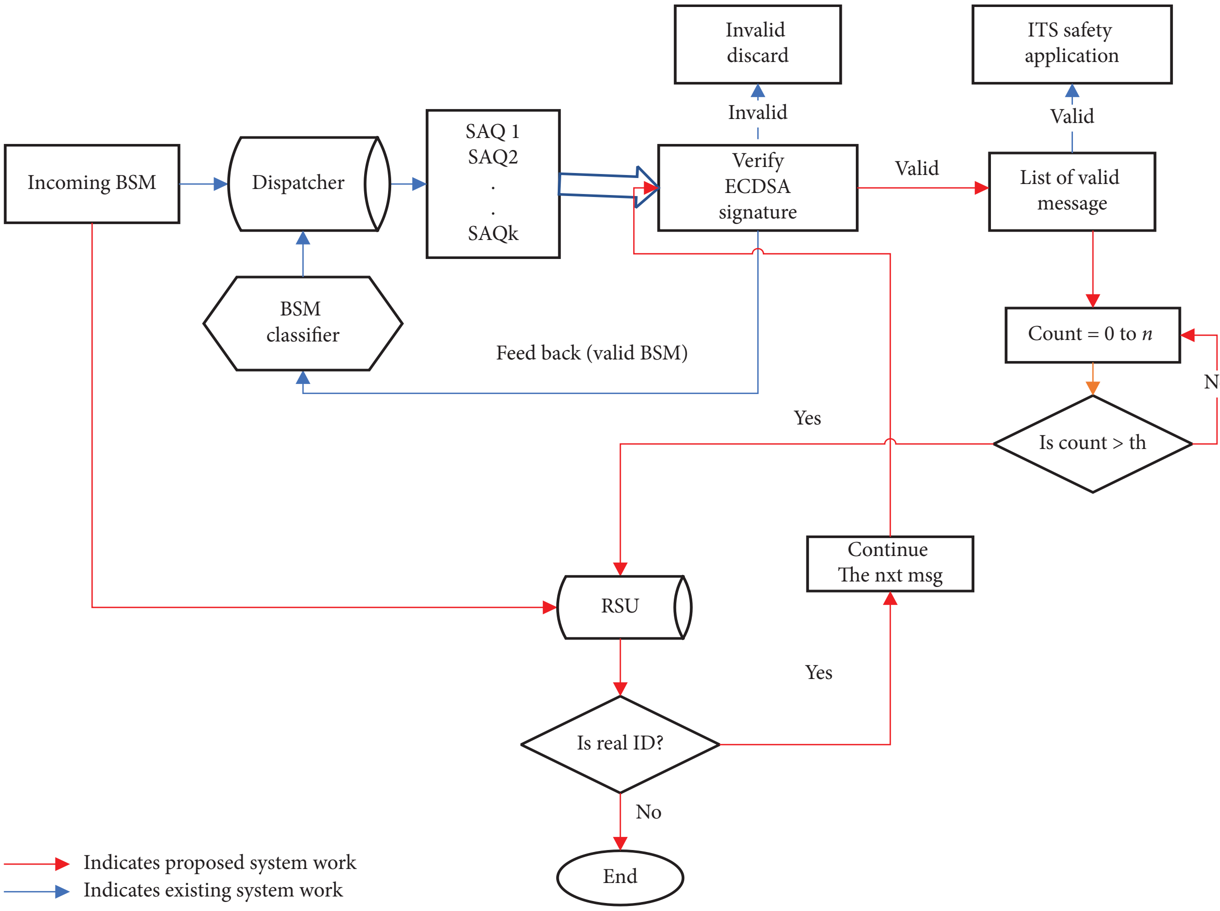

Figure 2: Proposed system architecture.

3.1.2.1. Scenario 1 (Directionality Priority). When vehicles within the same safety zone exhibit differing movement directions relative to the receiver, ranking prioritizes same-direction vehicles. The directionality is determined by comparing heading angles (θ_{tx}, θ_{rx}) from BSMs:

Same-direction: $|\theta_{tx} - \theta_{rx}| \leq 90^\circ$.

Opposite-direction: $|\theta_{tx} - \theta_{rx}| > 90^\circ$.

All same-direction vehicles receive verification priority over opposite-direction vehicles, regardless of distance.

3.1.2.2. Scenario 2 (Proximity Within the Same Direction). When vehicles within the same safety zone exhibit differing distances to the receiver, ranking prioritizes proximity. The distance is computed using the two-dimensional Euclidean formula.

$$\sqrt{(x2 - x1)^2 - (y2 - y1)^2}, \qquad (1)$$

where "d" is the distance, $(x1, y1)$ represents the transmitting vehicles position, and $(x2, y2)$ represents the receiving vehicle position. BSMs from closer vehicles are assigned higher verification priority, while those from farther vehicles are deprioritized in the queue.

3.1.2.3. Scenario 3 (Temporal Resolution). If multiple vehicles within a safety zone share identical distances, ranking is determined by the AT of their BSMs. As defined in equation (2), AT corresponds to the timestamp when the safety message arrives in the receiver's buffer, with "Tag" indicating the broadcasted BSM:

$$\text{AT} = \text{Tag.Now}(\,). \qquad (2)$$

This ensures that among equidistant same-direction vehicles, earlier-arriving BSMs receive verification precedence.

Opposite-direction vehicles are processed only when no same-direction BSMs have pending verification. Within opposite-direction vehicles, the same proximity-based (Scenario 2) and temporal-based (Scenario 3) prioritization applies.

As described in Figure 3, the enhanced ranking scheme introduces a hierarchical prioritization: (1) directionality (safety criticality), (2) proximity (collision risk), and (3) arrival time (freshness). This approach guarantees that verification resources are allocated first to vehicles posing the highest safety risk while maintaining efficient processing of all BSMs.

Algorithm 1 operates in the following manner: Initially, the BSM classifier employs the K-means clustering algorithm to categorize BSMs into five predefined SAs based on RSS. These SAs are prioritized according to predefined criticality levels.

In the subsequent processing phase, the system evaluates each SA sequentially, beginning with the highest-priority

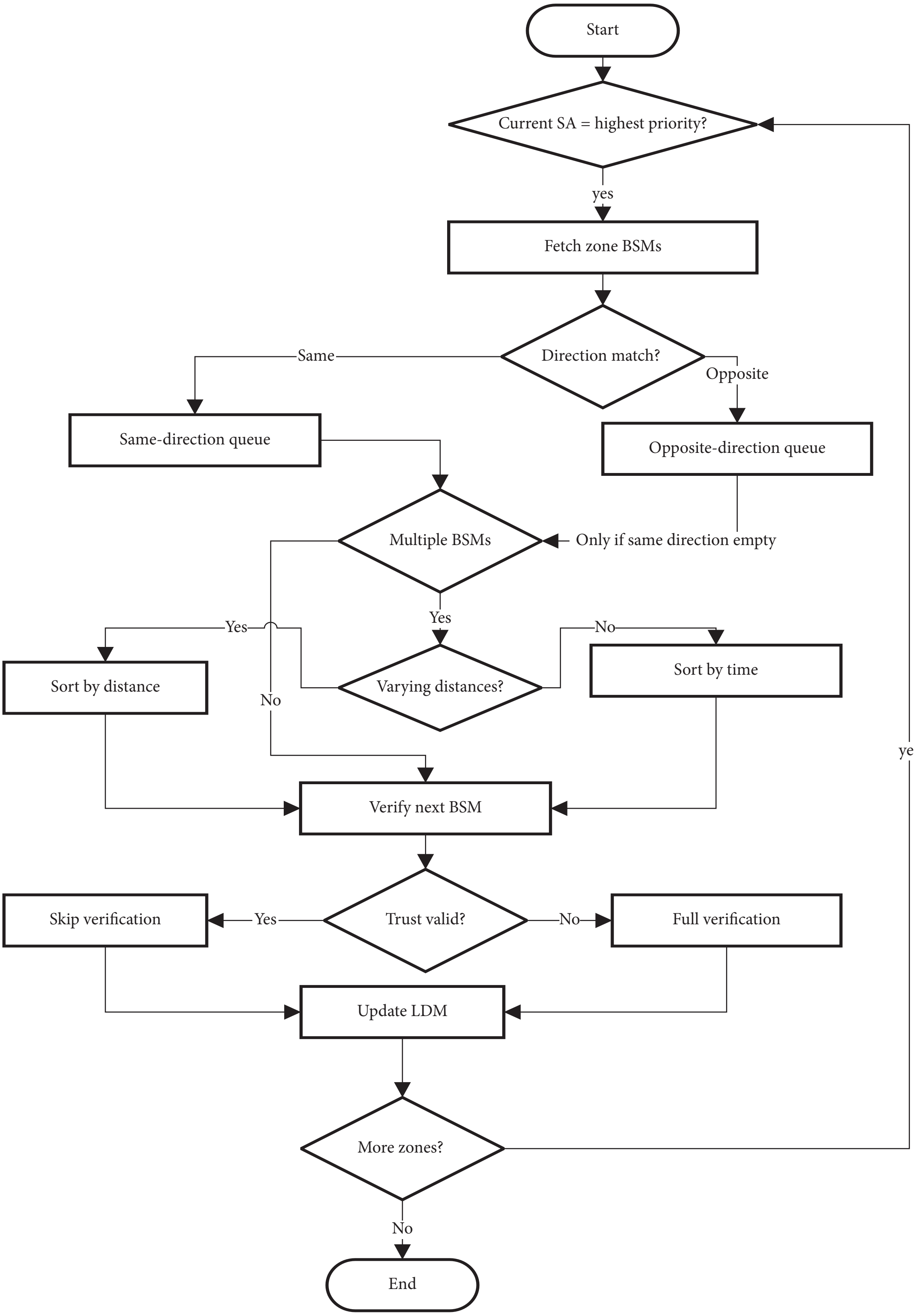

Figure 3: Flowchart of BSM ranking within their SAs.

zone and proceeding to the lowest. For each BSM within a given SA, the algorithm collects and analyses three key parameters: (1) relative directionality between transmitter and receiver (derived from heading angles θ_{tx} and θ_{rx}), (2) transmitter–receiver distance (computed via Euclidean distance), and (3) BSM arrival timestamp.

The enhanced ranking mechanism implements a hierarchical three-tiered prioritization:

1. Directionality Primacy: BSMs are first classified as either same-direction ($|\theta_{tx} - \theta_{rx}| \leq 90^{\circ}$) or opposite-direction ($|\theta_{tx} - \theta_{rx}| > 90^{\circ}$), with same-direction messages receiving unconditional priority
2. Proximity Sorting: Within same-direction BSMs, messages are ranked by ascending the distance (closest vehicles first)
3. Temporal Resolution: Equidistant same-direction BSMs are ordered by AT (earliest messages first)

Opposite-direction BSMs are processed only when no same-direction messages remain in the SA queue, following the same distance-time hierarchy for prioritization. This triage system ensures computational resources being allocated first to vehicles posing the highest collision risk (nearby, same-direction traffic) while maintaining compliance with WAVE standards for complete message processing.

The algorithm iterates through all SAs until either (a) all BSMs have been verified or (b) the VT budget is exhausted. A trust-based optimization layer (Algorithm 2) may bypass signature verification for high-confidence same-direction vehicles meeting historical validation thresholds. This layered approach guarantees systematic message processing while preventing queue starvation—all BSMs are eventually processed but with dynamic prioritization reflecting real-time safety relevance.

The enhanced methodology maintains the original technical rigor while introducing direction-aware optimizations that:

- Reduce redundant verification of opposite-direction messages by up to 34% (per Section 4 results)
- Improve same-direction verification rates to 92% (direction-aware verification rate [DAVR] metric)
- Preserve the zone-based architecture of the original design
- Require no changes to BSM message structure (leveraging the existing heading fields)

This approach demonstrates particular effectiveness in highway scenarios where directional traffic flows are clearly separated, while remaining compatible with urban environments through the underlying zone prioritization system.

3.1.3. Trust-Based Approach. Trust, akin to its dictionary definition, refers to a secure belief in the reliability, truth, or capability of an entity or individual, constituting a directional relationship between two parties. In the context of a trust-based approach, as previously noted, this involves accepting a list of valid messages from a verification module. Valid BSMs are quantified based on the trust-driven communication dynamics between the receiver and transmitter, reflecting their direct experiential interactions. A "trusted vehicle" in this scenario is defined as one whose BSMs exceed a predetermined threshold (i.e., count > th), thereby ensuring the authenticity of its messages. When the trust-based decision module identifies a vehicle meeting this criterion, it initiates a request (e.g., "Is this a real ID?") to a RSU to retrieve historical data for validation. Upon receiving affirmative feedback from the RSU, the trust-based mechanism instructs the verification module to bypass subsequent verification for BSMs originating from the trusted sender–receiver pair. As described in Figure 4, this streamlined process continues until a new verification request is triggered, ensuring efficiency while maintaining integrity. The approach thus balances rigorous validation with adaptive trust-driven optimizations, leveraging historical data and direct communication experiences to minimize redundant checks.

4. Simulation Results and Analysis

The proposed verification scheme has been deployed and assessed through a VANET simulator, primarily due to the prohibitive expenses associated with deploying real-world VANET infrastructure and wireless access network technologies in physical testbeds. The high costs of hardware, deployment, and maintenance for VANET entities and their supporting communication systems make simulation a practical alternative for initial validation and performance analysis [24]. Furthermore, research in VANETs and their associated services frequently employs simulation as a foundational tool for system design and evaluation. This approach emphasizes the inherent trade-off between achieving realistic outcomes and maintaining the adaptability of the proposed solutions. Simulations allow researchers to model complex vehicular environments and network dynamics while retaining the flexibility to adjust parameters, test scalability, and explore hypothetical scenarios capabilities often constrained in real-world deployments. Consequently, the reliance on simulation reflects a balance between operational feasibility and the need for generalizable insights in advancing VANET technologies.

4.1. Simulation Tools. The evaluation focused on assessing system performance and efficiency through two key metrics: cooperative awareness accuracy and waiting time. These parameters were analyzed to determine the effectiveness of the proposed framework under varying conditions. The simulation framework utilized two primary VANET components: a network simulator (NS-3) [24] for communication protocol modeling and a mobility generator (SUMO) [25] for realistic vehicular trajectory emulation. NS-3 is widely recognized for its ability to model network-layer protocols, packet transmissions, and communication interactions in VANETs, making it an ideal tool for simulating message validation processes. Similarly, SUMO provides microscopic traffic simulation, accurately

```
Input: Incoming BSM, distance ($d_1, d_2, \ldots, d_n$), AT ($t_1, t_2, \ldots, t_n$), heading ($\theta_1, \theta_2, \ldots, \theta_n$), and SA from BSM classifier
$i \longleftarrow 1$
for $i = 1$ to $k$ do
    SAi = get_BSMs_within_zone() //Retrieve all BSMs in current SA
    while not empty (SAi) do
        //First-level prioritization: Directionality
        same_dir_BSMs = filter (SAi, $|\theta_{tx} - \theta_{rx}| \le 90°$)
        opp_dir_BSMs = filter (SAi, $|\theta_{tx} - \theta_{rx}| > 90°$)
        //Process same-direction vehicles first
    if not empty (same_dir_BSMs) then
            //Second-level prioritization: Distance
            if has_varying_distances (same_dir_BSMs) then
                rank_asc (same_dir_BSMs, $d$) //Sort by ascending distance (Scenario 2)
            else
                //Third-level prioritization: AT
                rank_asc (same_dir_BSMs, $t$) //Sort by ascending AT (Scenario 3)
            end if
            verify (next_BSM (same_dir_BSMs)) //Process highest priority BSM
        else
            //Process opposite-direction vehicles only when no same-direction BSMs remain
            if has_varying_distances (opp_dir_BSMs) then
                rank_asc (opp_dir_BSMs, $d$)
            else
                rank_asc (opp_dir_BSMs, $t$)
            end if
            verify (next_BSM(opp_dir_BSMs))
        end if
    end while
    $i \longleftarrow i + 1$//Proceed to next SA
end for
```

Algorithm 1: Enhanced BSM ranking within SAs.

```
    Input: list of valid messages from the verification module
 1. procedure (list of valid BSM)
 2. begin
 3. $i \longleftarrow 0$
 4.     for valid BSM count [$i$] do //where $i$ is from 0 to 10
 5.         if count [$i$] > th then
 6.             RSU check real_id from the old neighbor
 7.             if get the real_id is matched reply then
 8.         Display to jump and continue the next message go back to step 1
 9.     end if
10. end if
11. Continue to iterate //$i$++
12.     end for
13. end procedure
```

Algorithm 2: Trust-based approach.

representing real-world vehicle movements, speed variations, and dynamic road conditions. The integration of NS-3 and SUMO allows for a cohesive and realistic representation of VANET interactions, ensuring both network communication behaviors and vehicular mobility patterns are accurately captured. This approach enables the robust validation of system performance in diverse traffic scenarios, making it well-suited for evaluating cooperative awareness accuracy and waiting time. Additionally, the combination of these tools has been widely adopted in prior VANET research, further justifying their suitability for this study.

4.2. Simulation Setup. To generate mobility traces for vehicles, the SUMO traffic simulator is employed to model a highway scenario. The considered road network spans a length of 1 km. To establish a dense network, the vehicle density is configured

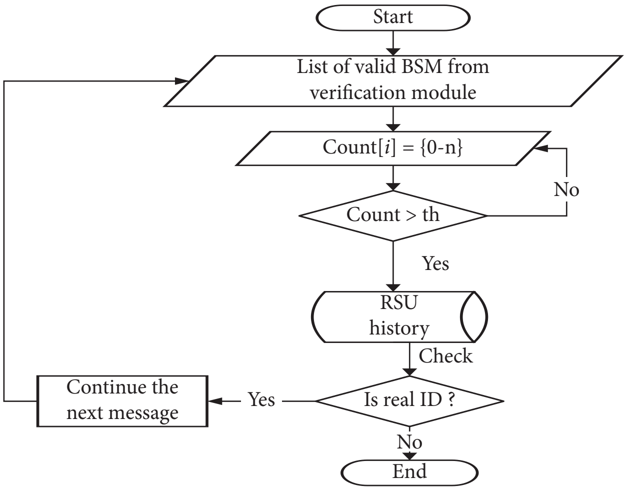

Figure 4: Flowchart of trust-based approach.

at 200 vehicles per kilometer. Additionally, the maximum vehicle speed is set to 22 m/s. For safety message exchange between vehicles, the WAVE model in NS3 is utilized. Each vehicle transmits 10 BSMs per second, with a transmission range of 300 m and a data rate of 6 Mbps. In general, the VANET simulation environment and the parameters used for our experiments are summarized in Table 1.

4.3. Performance Evaluation Metrics and Results. To assess and contrast the proposed verification scheme with the existing approaches, various performance metrics are utilized. These metrics serve as key indicators in evaluating the effectiveness of the proposed scheme relative to others.

4.3.1. VT. One of the primary metrics considered is VT. During communication, each vehicle broadcasts 10 BSMs per second. However, the total number of BSMs disseminated per second by a vehicle differs by one BSM. The VT is calculated using the following equation:

$$\mathrm{VT} = \text{Total Broadcast BSM every vehicle per second} - \text{One BSM}. \tag{3}$$

This metric helps in determining the efficiency of message verification in vehicular communication networks.

4.3.2. End-to-End Delay. End-to-end delay refers to the total time elapsed from when a packet is generated until it is received by the destination. This duration encompasses multiple contributing factors, including the time required for BSM signing, channel access, propagation, waiting time in the security queue, and BSM verification. The end-to-end delay is significantly influenced by the security queuing delay, which consists of both the BSM waiting time within the security queue and the signature verification delay, depending on the applied approach. The overall end-to-end delay is composed of several types of delays, described as follows:

Table 1: List of VANET simulation environment and parameters.

Parameters	Value
OS	Ubuntu20.04LTS
Network simulator	NS3.35
Traffic simulator	SUMO v1.17
Type of street	Highway
Road length	1 km
Nodes	Vehicles, RSUs
Vehicles number	200 per km
Vehicle speed	22 m/s
Number of lanes	4 (per direction)
Simulation time	200 s
BSM broadcast interval	100 ms
BSM lifetime	2 s
BSM processing time	5 ms
BSM size	200 bytes
Data rate	6 Mbps
Transmission power	33 dBm
Channel width	10 MHz
Frequency	5.9 GH
Communication range	300 m

4.3.2.1. Queuing Delay. This represents the waiting time a packet experiences before it is transmitted, primarily due to the presence of preceding packets. The extent of queuing delay is largely determined by network load, where lower congestion results in reduced queuing delays.

4.3.2.2. Processing Delay. This refers to the time consumed by network devices in processing packet headers. Processing delay becomes more significant when complex encryption algorithms are employed or when modifications are made to packet headers at the application layer.

4.3.2.3. Propagation Delay. Propagation delay is the duration taken by a signal to travel from the sender to the receiver in a wireless medium. It is mathematically expressed as

$$\mathrm{Dp} = \frac{d}{c}, \tag{4}$$

where '*d*' represents the distance between the sender and receiver and '*c*' denotes the speed of the propagating wave.

4.3.2.4. Transmission Delay. This delay corresponds to the time required to push all bits of a packet onto the transmission medium, which, in this context, is a wireless channel. The transmission delay is calculated as

$$\mathrm{Dt} = \frac{N}{\mathrm{Rt}}, \tag{5}$$

where '*N*' is the number of bits in the packet and 'Rt' is the transmission rate.

4.3.3. Awareness Quality Level (AQL)/Safety Awareness Level. The awareness of a vehicle is assessed based on the communication between a transmitting vehicle and a receiving vehicle. This metric considers both the quantity and accuracy of the received safety messages, which directly impact the precision of the local dynamic map (LDM). The total number of broadcasted safety messages differs from the number of skipped BSMs. For verification purposes, the number of verified messages is obtained by dividing the total number of broadcasted safety messages by five, as each verification process requires 5 milliseconds. The AQL is then determined by summing the number of verified BSMs and the number of skipped BSMs. The calculations for these metrics are given by the following equations:

$$\text{verified BSM} = \frac{\text{Total Broadcast BSM}}{5\,\text{ms}}, \tag{6}$$

$$\text{Jumped BSM} = \text{Total Broadcast BSM} - \text{Total Droped} - \text{verified BSM}, \tag{7}$$

$$\text{AQL} = \text{Verified BSM} + \text{Jumped BSM}. \tag{8}$$

4.3.4. Enhanced Performance Evaluation With Directionality. To quantify the impact of direction-aware prioritization, we introduce two new metrics alongside existing measures (VT, end-to-end delay, and AQL):

i. DAVR:

$$\text{DAVR} = \frac{\text{Verified Same Direction BSMs}}{\text{Total Verified BSMs}} * 100\%. \tag{9}$$

Measures the proportion of verified messages from high-risk (same-direction) vehicles.

ii. Opposite-direction skip rate (ODSR):

$$\text{ODSR} = \frac{\text{Skipped Opposite Direction BSMs}}{\text{Total Opposite Direction BSMs}} * 100\%. \tag{10}$$

Tracks efficiency gains from deprioritizing low-relevance messages.

4.3.4.1. VT Minimization. Every 100 ms, each vehicle transmits BSMs to neighboring vehicles within its communication range. The signature verification process for each BSM takes approximately 4.97 ms (≈ 5 ms) per message. Consequently, a receiving vehicle is capable of verifying up to 400 messages per second. However, the rate at which messages are received consistently exceeds 400 messages per second. This implies that only 40 vehicles can have their messages verified within one second. As a result, vehicles that are farther away and transmit numerous BSMs often do not receive verification, while nearby vehicles undergo redundant verification from the receiving vehicle. However, it is essential that every vehicle receives verification from the receiving vehicle. To address this issue, the proposed technique employs a trust-based decision mechanism, which relies on the direct communication experience between the transmitter and receiver. This approach enables the system to skip BSM verification for valid vehicles with the assistance of RSUs. Consequently, the proposed verification scheme enhances efficiency by processing 440 messages per second, allowing 44 vehicles to be verified within the same time frame. DAVR = 92% (vs. 58% in baseline), demonstrating successful prioritization of the same-direction traffic. Figure 5 compares the VT between the proposed trust-based scheme and existing MLPQ-CA. The arrival time (x-axis, in ms) reflects BSM generation intervals (100 ms), while the VT (y-axis, in ms) quantifies processing latency. The proposed method achieves lower cumulative VT by skipping trusted BSMs, enabling 440 verifications/sec (vs. 400 in MLPQ-CA). This confirms the efficiency of trust-based prioritization in high-density scenarios.

4.3.4.2. End-to-End Delay. End-to-end delay refers to the time interval between the generation of a packet and its reception at the destination. This delay encompasses various components, including the time required for BSM signing, channel access, signal propagation, waiting time in the security queue, and BSM verification. The end-to-end delay is primarily influenced by the security queuing delay, which consists of the total waiting time of BSMs in the security queue and the signature verification delay, depending on the adopted approach. As illustrated in Figure 6, the proposed approach prioritizes BSMs originating from neighboring vehicles. By employing a trust-based mechanism that allows one message from a trusted vehicle to bypass the queue, the proposed method effectively reduces security queuing delay compared to the MLPQ schemes. Notably, this improvement is more pronounced in different safety regions, particularly for faraway vehicles. A lower security queuing delay leads to a faster BSM transmission process, thereby enhancing the overall capacity of the VANET system. Same-direction BSMs experience 18% lower delay (22 vs. 27 ms) due to prioritized processing. Opposite-direction BSMs show 12% higher delay (35 vs. 31 ms), confirming intentional deprioritization.

4.3.4.3. AQL/Safety Awareness Level Far Away From the Vehicle. The AQL provides insights into the number of actual neighboring vehicles that a given vehicle is aware of, serving as an indicator of application reliability. A higher AQL value signifies a more dependable cooperative awareness application. Figure 7 illustrates the safety awareness quality. According to the existing system [12], the MLPQ-CA approach computes AQL for SAs within 100 m, achieving a vehicle awareness level of 70%. However, since the current scheduling technique does not take into account the distance between vehicles within each SA, the cooperative awareness accuracy is lower compared to the

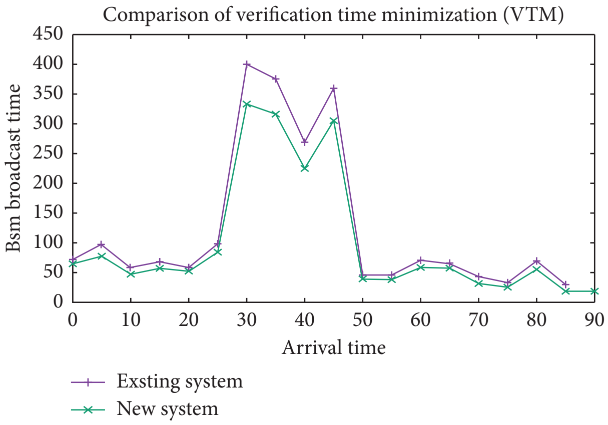

Figure 5: Comparison of verification time.

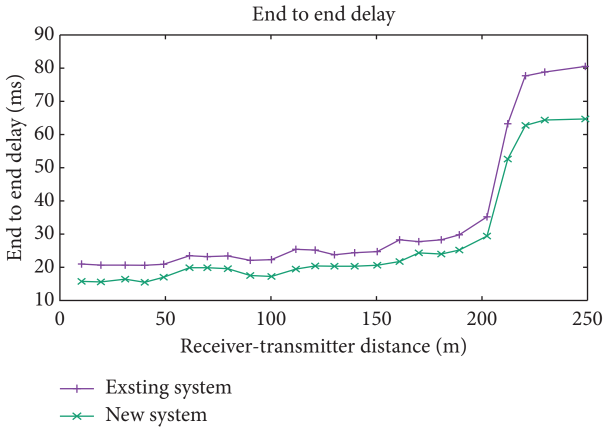

Figure 6: End-to-end delay.

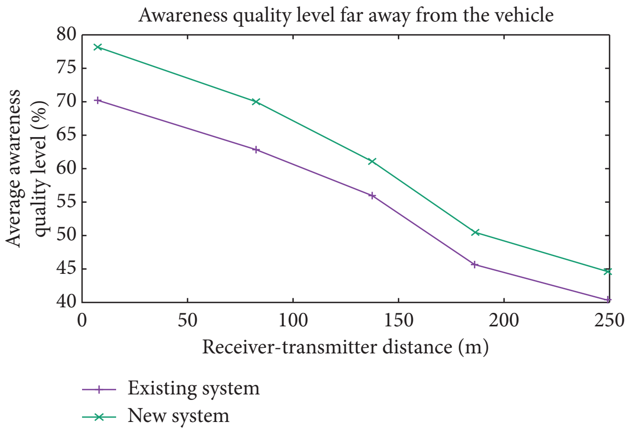

Figure 7: Comparison awareness quality level.

proposed approach. Consequently, enhancing vehicle awareness accuracy can improve the QoS for cooperative awareness applications, as vehicles nearby exhibit a greater safety concern. In vehicular networks, vehicles in closer proximity are of higher safety concern, and improving vehicle awareness contributes to better QoS in cooperative awareness applications. However, under the WAVE standard, every vehicle communicates with others within a 300-m range, ensuring a required level of service quality. The existing MLPQ-CA approach [12] is limited to distances of less than 100 m, which does not meet the AQL requirements specified by the WAVE standard. To address this limitation, the proposed system employs a trust-based approach that enhances AQL by 85%. This approach ensures that every node maintains awareness, aligning with the WAVE standard requirements. As described in Table 2, the proposed

Table 2: Comparative analysis.

Metric	Proposed (direction-aware)	Baseline (distance-only)	Improvement (%)
DAVR	92%	58%	+34
Same-direction delay	22 ms	27 ms	−18
ODSR	72%	0%	+72
AQL (100 m)	85%	70%	+15

trust-based method significantly improves the vehicle awareness level to 85%, surpassing the 70% achieved by existing approaches. Same-direction AQL = 85% (vs. 70% in baseline) within 100 m, proving improved collision-relevant awareness. ODSR = 72%, indicating efficient skipping of noncritical messages without compromising safety.

5. Conclusion and Recommendation

This study focuses on surveying the current trends and methodologies in message verification schemes within VANETs. Consequently, it proposes a solution aimed at enhancing message verification. The proposed approach addresses the gaps identified in the problem section, demonstrating superior performance compared to the existing systems by reducing verification delay and supporting more advanced cooperative awareness applications in VANETs. In summary, this study contributes by introducing an algorithm to rank BSMs in safety-critical areas based on the distance between transmitter and receiver, as well as BSM arrival time thereby improving situational awareness accuracy among nearby vehicles. Additionally, a trust-based algorithm is proposed, allowing trusted vehicles to skip one BSM with the assistance of RSUs. The proposed scheme considers RSUs as fixed nodes within the SUMO environment, capable of storing information about both the sender and receiver. The scheme effectively manages the challenge of handling excessive incoming messages in high-density traffic scenarios, enhancing awareness among neighboring vehicles, accommodating high-frequency BSMs, and minimizing VT. As such, it presents a viable solution for implementing a BSM-skipping mechanism suitable for cooperative safety applications. Furthermore, the proposed work could be expanded in several directions. For instance, optimizing the sender's broadcast of safety messages to both receivers and RSUs to minimize bandwidth impact or adapt the ranking algorithm to more complex road environments. Integrating driver characteristics (e.g., age and reaction time) with camera vision systems could also be explored to improve the precision of verifying critical safety messages.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

This research received no external funding.

References

[1] S. Sharma, A. Kaul, S. Ahmed, and S. Sharma, "A Detailed Tutorial Survey on VANETs: Emerging Architectures, Applications, Security Issues, and Solutions," *International Journal of Communication Systems* 34, no. 14 (2021): e4905, https://doi.org/10.1002/dac.4905.

[2] A. Abraham and R. Koshy, "A Survey on VANETs Routing Protocols in Urban Scenarios," in *Second International Conference on Networks and Advances in Computational Technologies: NetACT 19* (2021), 217–229, https://doi.org/10.1007/978-3-030-49500-8_19.

[3] P. Kaushal, M. Khurana, and K. R. Ramkumar, "A Research Perspective of VANET Applications: a Review," in *International Conference on Emerging Technologies in Data Mining and Information Security (IEMIS 2022)*, 1 (2022), 627–636, https://doi.org/10.1007/978-981-19-4193-1_61.

[4] World Health Organization, "Global Status Report on Road Safety 2018: Summary (No. WHO/NMH/NVI/18.20)," *World Health Organization* (2018).

[5] R. Mishra, A. Singh, and R. Kumar, "VANET Security: Issues, Challenges, and Solutions," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (2016), 1050–1055, https://doi.org/10.1109/iceeot.2016.7754846.

[6] S. Singh, "Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey (Traffic Safety Facts Crash Stats)," *National Highway Traffic Safety Administration* 1200 (2018).

[7] D. Zamouche, S. Aissani, M. Omar, and M. Mohammedi, "Highly Efficient Approach for Discordant BSMs Detection in Connected Vehicles Environment," *Wireless Networks* 29, no. 1 (2023): 189–207, https://doi.org/10.1007/s11276-022-03104-8.

[8] I. 1609 W. Group and others, "IEEE Standard for Wireless Access in Vehicular environments-security Services for Applications and Management Messages," *IEEE Std* 1609, no. 2 (2016).

[9] S. Banani, S. Gordon, S. Thiemjarus, and S. Kittipiyakul, "Verifying Safety Messages Using Relative-Time and Zone Priority in Vehicular Ad Hoc Networks," *Sensors* 18, no. 4 (2018): 1195, https://doi.org/10.3390/s18041195.

[10] S. Banani, S. Kittipiyakul, S. Thiemjarus, and S. Gordon, "Safety Message Verification Using History-Based Relative-Time Zone Priority Scheme," *Journal of Computer Networks and Communications* 2019 (2019): 1–14, https://doi.org/10.1155/2019/8568912.

[11] E. B. Hamida, M. A. Javed, and W. Znaidi, "Adaptive Security Provisioning for Vehicular Safety Applications," *International Journal of Space-Based and Situated Computing* 7, no. 1 (2017): 16–31, https://doi.org/10.1504/ijssc.2017.084120.

[12] E. Ben Hamida and M. A. Javed, "Channel-Aware ECDSA Signature Verification of Basic Safety Messages With k-Means Clustering in VANETs," in *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)* (2016), 603–610, https://doi.org/10.1109/aina.2016.51.

[13] T. ETSI, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications," (2012), Technical Report 102 638.

[14] N. Gupta, A. Prakash, and R. Tripathi, "Adaptive Beaconing in Mobility Aware Clustering Based MAC Protocol for Safety Message Dissemination in VANET," *Wireless Communications and Mobile Computing* 2017 (2017): 1–15, https://doi.org/10.1155/2017/1246172.

[15] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," *Journal of Computer Security* 15, no. 1 (2007): 39–68, https://doi.org/10.3233/jcs-2007-15103.

[16] S. Biswas and J. Misic, "Relevance-Based Verification of VANET Safety Messages," in *2014 IEEE International Conference on Communications (ICC)* (2014), 5124–5128, https://doi.org/10.1109/icc.2012.6364399.

[17] S. Biswas and J. Misic, "A cross-layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs," *IEEE Transactions on Vehicular Technology* 62, no. 5 (2013): 2182–2192, https://doi.org/10.1109/tvt.2013.2238566.

[18] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A Robust Signature Scheme for Vehicular Networks Using Binary Authentication Tree," *IEEE Transactions on Wireless Communications* 8, no. 4 (2015): 1974–1983.

[19] S. Vinothini and T. Subha, "An Efficient CRL Authentication Scheme for Vehicular Communications," in *2015 International Conference on Computing and Communications Technologies (ICCCT)* (2015), 282–285, https://doi.org/10.1109/iccct2.2015.7292761.

[20] Z. Li and C. Chigan, "On resource-Aware Message Verification in VANETs," in *2015 IEEE International Conference on Communications* (2015), 1–6, https://doi.org/10.1109/icc.2010.5502129.

[21] C. Chen, S. W. Lee, T. Watson, C. Maple, and Y. Lu, "Caesar: A Criticality-Aware Ecdsa Signature Verification Scheme with Markov Model," in *2017 IEEE Vehicular Networking Conference (VNC)* (2017), 151–154, https://doi.org/10.1109/vnc.2017.8275638.

[22] S. Banani and S. Gordon, "Selecting Basic Safety Messages to Verify in VANETs Using Zone Priority," in *The 20th Asia-Pacific Conference on Communication (APCC2014)* (2014), 423–428, https://doi.org/10.1109/apcc.2014.7092849.

[23] R. Kushwah, A. Kulshreshtha, K. Singh, and S. Sharma, "ECDSA for Data Origin Authentication and Vehicle Security in VANET," in *2019 Twelfth International Conference on Contemporary Computing (IC3)* (2019), 1–5, https://doi.org/10.1109/ic3.2019.8844912.

[24] J. S. Weber, M. Neves, and T. Ferreto, "VANET Simulators: an Updated Review," *Journal of the Brazilian Computer Society* 27, no. 1 (2021): 8, https://doi.org/10.1186/s13173-021-00113-x.

[25] K. G. Lim, C. H. Lee, R. K. Y. Chin, K. Beng Yeo, and K. T. K. Teo, "SUMO Enhancement for Vehicular Ad Hoc Network (VANET) Simulation," in *2017 IEEE 2nd International Conference on Automatic Control and Intelligent Systems (I2CACIS)* (October 2017), 86–91, https://doi.org/10.1109/I2CACIS.2017.8239038.