JOURNAL OF SOFT COMPUTING AND DATA MINING
e-ISSN: 2716-621X

JSCDM

Vol. 6 No. 2 (2025) 370-386
https://publisher.uthm.edu.my/ojs/index.php/jscdm

AI-Driven Secure Emergency Message Dissemination in 5G-Enabled VANETs Using LSTM-Based Intrusion Detection and CP-ABE Encryption

Maath A. Albeyar[1]*, Ikram Smaoui[2], Hassene Mnif[2], Sameer Alani[3]

[1] *National School of Electronics and Telecommunications, University of Sfax, TUNISIA*
[2] *National School of Electronics and Telecommunications, Laboratory of Electronics and Technologies of Information (LETI), ENIS, University of Sfax, Sfax, TUNISIA*
[3] *Electronic Computer Center, University of Anbar, IRAQ*

*Corresponding Author: maath.albeyar@enetcom.u-sfax.tn
DOI: https://doi.org/10.30880/jscdm.2025.06.03.023

Article Info

Received: 1 September 2025
Accepted: 24 November 2025
Available online: 30 December 2025

Keywords

Vehicular Ad Hoc Networks (VANETs), Intrusion Detection System (IDS), Long Short-Term Memory (LSTM), Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Edge-DENM, 5G security, privacy preservation

Abstract

The number of vehicles has expanded rapidly due to advances in automobile technology and global population growth, resulting in an increase in the frequency of traffic accidents. Wireless Vehicle-to-Vehicle (V2V) connections are used by event-driven safety applications to alert drivers to potentially dangerous situations. For emergency vehicles to respond to urgent emergency services, there must be uninterrupted traffic on the roads. Even a small delay in an emergency journey time can be costly and potentially result in lost lives. To overcome this limitation in this research, we designed an AI-driven emergency message dissemination framework for "Vehicular Ad hoc Networks (VANETs)" with 5G, for the efficient, secure, and privacy-preserving communication of messages at critical times. Using time-series data analysis, an AI-based Intrusion Detection System (IDS) that uses Long Short-Term Memory (LSTM) networks classifies emergency messages through recognizing abnormalities and false warnings. To ensure secure emergency message dissemination in the VANET environment, this research proposes a Multi-Authority Ciphertext-Policy Attribute-Based Encryption (MA-CP-ABE). Priority-based scheduling leverages are the Edge-DENM Prioritization Algorithm, which categorizes emergency messages based on urgency levels to prevent delays in high-risk scenarios. The proposed approach ensures secure, scalable, and privacy-preserving emergency communication, improving overall VANET performance by dynamically adapting to traffic conditions and vehicle mobility.

1. Introduction

The growing population is a primary reason for the increase in road traffic. Given the high volume of traffic, the situation is extremely difficult for the traffic control authority [1]. As per the World Health Organization's 2018 "Global Road Safety Status Report," road accidents contribute to the deaths of 1.35 million people each year [6, 7]. Traffic accidents are also the leading cause of fatalities and injuries worldwide. To minimize road traffic crashes, "Intelligent Transportation Systems (ITS)" and VANET generally aim to improve human health and welfare. The event-driven safety apps use wireless Vehicle-to-Vehicle (V2V) connections to warn drivers of potentially

hazardous circumstances. Security and privacy issues are paramount within VANETs. Nodes may be compromised due to the open communication medium they use, and a variety of attacks are possible, such as Sybil attacks, data privacy violations or breaches, and message tampering [8, 9].

To establish these issues and position countermeasures such as public key infrastructure, Intrusion Detection System (IDS), and encryption methods to protect messages in VANETs. The emergence of 5G technology will present opportunities to address the potentially significant limitations of VANET readiness and will offer higher data rates, enhanced connectivity, and reduced latency, features that exceed those offered by previous generations of wireless networks [10].

The introduction of Artificial Intelligence (AI) algorithms helps in enhancing the broadcasting of emergency messaging. As an illustration, machine learning algorithms can predict traffic patterns and identify potential dangers, and thus, pre-emptive warnings can be issued to a particular driver [13, 14]. However, there are still inherent challenges in the VANET environment, such as security threats. Consequently, one must have an elaborate framework that incorporates an AI IDS, secure encryption, and scheduling priorities for broadcasting emergency messages in 5G VANETs, ensuring security, efficiency, and privacy safeguards. This research will provide a framework for leveraging AI and 5G to enhance emergency communication in VANETs.

The attempts to ensure the 5G network of VANET have suffered significant setbacks in the past due to limitations of detection accuracy and security issues. Other metrics, such as precision, recall, and F1-score, will be used to effectively test the detection quality of the proposed IDS, ensuring low false positives and low false negatives. The following are the main aspects that are likely to lead to data security and privacy vulnerabilities: False message detection: Current detection methods do not guarantee that false messages are correctly detected in the VANET environment. In this manner, the system would risk being exposed to a security threat without detection.

The VANET communication system is vulnerable to security issues. Malicious or self-serving nodes exploit such vulnerabilities to manipulate normal behaviour during the routing of emergency messages, thereby compromising the network's reliability in their own selfish interests. Challenges with priority-based scheduling: Selfish nodes or malicious vehicles in VANETs disrupt the routing of emergency messages by assigning priority to their own communications or introducing fake data, resulting in delays, resource misuse, and disruption of system integrity. These obstacles hinder the timely and safe distribution of high-priority alerts, which endangers road safety.

The main purpose and scope of the study are to develop an AI-based emergency message dissemination model for 5G Vehicular Ad hoc Networks (VANETs) to effectively communicate important messages safely and without infringing privacy in times of emergency. It employs AI to make the most of message dissemination, minimizing delays, limiting interference, and enhancing data security and privacy under high-mobility conditions.

1. By implementing an intrusion detection-based LSTM classification algorithm to improve the false message detection accuracy.
2. The utilization of CP-ABE in this method enhances the security of the emergency message during dissemination in the VANET environment.
3. Edge-DENM Prioritization Algorithm is used to categorize the messages based on their priority level.

The remainder of the present study will be organized as follows: Section 2 will outline a survey of prior publications, highlighting gaps in the research. Section 3 describes the main issue with the current methods of approach. Section 4 gives the study methodology of the proposed model, the corresponding pseudocode, mathematical representations, and diagrams. The implementation details, the experimental findings, and a comparison of the proposed and existing methods are provided in Section 5. Section 6 discusses the end of the ducts referred to in the content.

2. Literature Survey

In this section, the use of AI in vehicular ad hoc 5G networks has been outlined in terms of delivering emergency messages in terms of security and privacy-based distribution. Additionally, this section highlights the research gap found in earlier studies.

The authors of [17] propose a secure edge-computing-assisted video-reporting service for 5G-capable vehicle networks. Edge nodes finish the message categorization and verification in the suggested approach. Additionally, to facilitate local video report uploads and downloads and to reduce the time required to store repeated accident reports in the cloud, these nodes forward the first received report message for the same accident to the authorized official vehicles. According to security research, the proposed plan meets several requirements for automotive networks and is secure under the random oracle model. Nevertheless, the proposed approach performs better as the suggested method finishes video categorization at the edge node.

The authors in [21] describe a method for routing Emergency Messages geographically based on trusted nodes. They emphasize the importance of measuring the reliability of nodes and connections. To minimize the

risk of link interruption, the link signal-to-noise ratio and actual transmission cost are measured to assess the link quality between nodes. Along with the node value, this value is used to calculate the trustworthiness of nodes and to eliminate any nodes that are susceptible to malice in the network. By using these algorithms, this paper detected and avoided false communications and fake nodes, with the main aim of identifying and stopping fraudulent vehicle nodes and their corresponding messages [22]. The false node detection and prevention algorithms analyze the node's profile once the mesh structure is identified.

The study in [26] presents a proof-trustworthiness-based, intelligent, secure message-dissemination scheme for VANETs based on blockchain and deep learning methods. This work guarantees the authenticity, integrity, and safe distribution of information in the most ever-changing vehicular settings.

In other papers [8, 9, 11, 12], the authors introduce authentication and privacy-preserving protocols adapted to VANETs that address protection against Sybil attacks, unauthorized access, and data breaches. These researchers emphasize the need for lightweight yet strong authentication systems capable of operating in the constrained vehicular environment with high security assurance.

Overall, earlier research has sought to address security and privacy in VANETs by combining intrusion detection, secure dissemination, authentication, and trust-based models. However, existing solutions often suffer from limited scalability, high computational overhead, or insufficient detection accuracy. There remains a need for an integrated framework that leverages AI-driven IDS, attribute-based encryption, and prioritization mechanisms to ensure both secure and efficient emergency message dissemination in 5G-enabled VANETs. Table 1 summarizes related work on security and privacy in VANETs.

Table 1 *Summary of related works on VANET security and privacy*

Reference	Focus Area	Contribution	Limitation
[17]	Edge-assisted secure video reporting	Categorization and verification at edge nodes to reduce redundancy	Does not address EN proximity limitations
[21, 22]	Trust and false node detection	Trust-based routing, prevention of fraudulent nodes/messages	Computational complexity in large networks
[26]	Blockchain & deep learning trust model	Proof-of-trustworthiness for secure message dissemination	Overhead in dynamic vehicular environments
[8, 9, 11, 12]	Authentication & privacy protocols	Defense against Sybil attacks, data breaches, and unauthorized access	Scalability and lightweight operation remain issues

3. Proposed Method

The proposed solution, grounded in AI strategies, may enhance the security and privacy of emergency message dissemination in 5G VANET environments. The general architecture of the offered method is illustrated in Figure 1.

- Data collection and pre-processing
- AI-based Emergency message classification
- Secure Emergency Message Dissemination
- Priority-based scheduling

3.1 Data Collection and Pre-Processing

The vehicular communication data, collected by vehicles and RSUs, is first gathered and pre-processed to enhance accuracy and consistency. Redundant and noisy data are filtered, and data normalization and filtering are performed to preserve key features. This translates to the quality of the inputs to AI models, ensuring they can effectively perform pattern analysis and anomaly detection in later stages.

3.2 AI-based Emergency Message Classification

VANETs are a fast communication network between roadside units (RSUs) and vehicles in order to enhance road safety as well as traffic management. Nonetheless, it is essential to introduce the authenticity and reliability of emergency messages to prevent unjustified panic and waste of resources. To overcome this, we will propose an IDS using a Long Short-Term Memory (LSTM)-based deep learning model to classify emergency messages. The overall architecture of the proposed method is depicted in Figure 1.

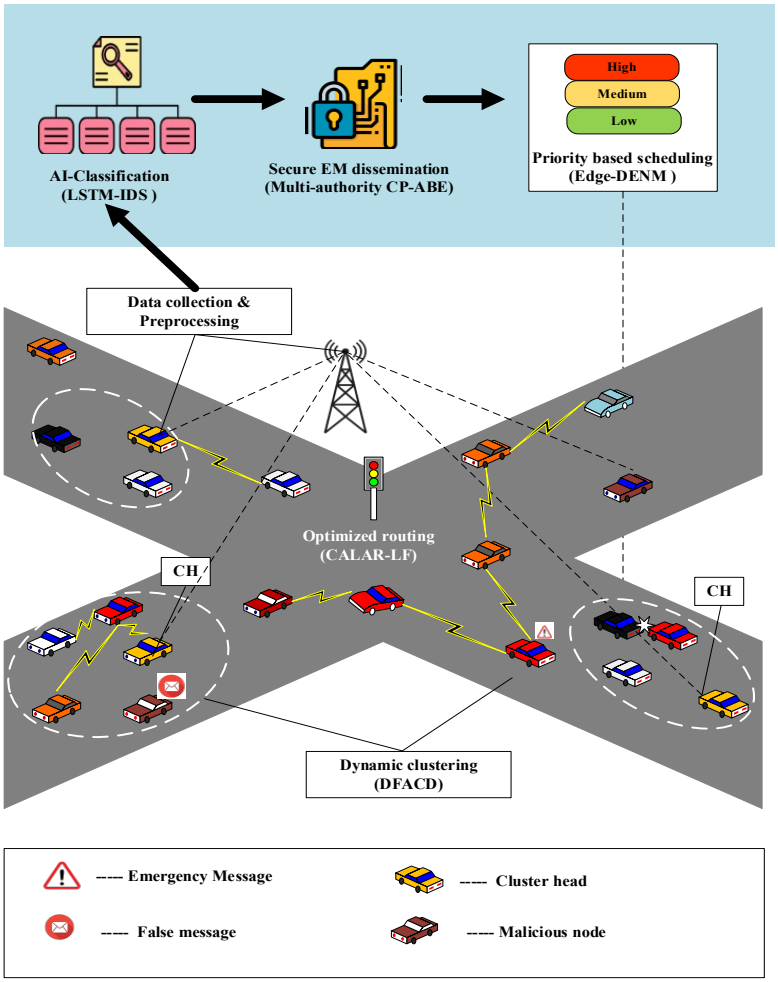

Fig. 1 *Overall architecture of the proposed method*

The LSTM-based IDS uses time-series vehicular communications messages to distinguish between emergency and non-emergency messages, such as false alerts. The LSTM network treats streams of vehicle communication as sequences of varying durations. This enables the LSTM model to capture long-range temporal correlations to distinguish between real messages, messages indicating emergencies, behaviors, and patterns, and malicious messages. The four fundamental components process each sequence of messages: the forget gate, the input gate, the candidate cell state, and the output gate. The LSTM network has been used to effectively learn sequential correlations of vehicular communication, differentiating normal and anomalous patterns. This would provide a high detection rate with few false positives, thereby enhancing the reliability of emergency message dissemination in VANETs [27]-[30].

Let $A = \{a_1, a_2, \dots, a_t\}$ represents a time series of vehicle communication information, indicating the input feature vector of time. The following equation defines the LSTM network and comprises memory cells that explicitly preserve long-term dependencies.

Forget gate: Determines how much of the previous information to retain or discard.

$$f_t = \sigma\left(w_f \cdot [h_{t-1}, a_t] + b_f\right) \tag{1}$$

Here, f_t represents the forget gate activation at the time step t, w_f denotes the weight matrix, h_{t-1} represents the previous hidden state, $a_t$is the current input, and b_f is the bias term. The sigmoid activation function σ ensures values are between 0 and 1, regulating memory retention.

Input gate: Regulates the addition of new information to the memory cell.

$$i_t = \sigma(w_i \cdot [h_{t-1}, a_t] + b_i) \tag{2}$$

$$\widetilde{c_t} = \tan h(w_c \cdot [h_{t-1}, a_t] + b_c) \tag{3}$$

The input gate i_t determines which new information is relevant, whereas $\widetilde{c_t}$ represents the candidate cell state computed via the hyperbolic tangent activation function, which enables values between -1 and 1 for better information representation.

Cell state update: Combines past and new information to update the memory cell.

$$c_t = f_t \cdot c_{t-1} + i_t \cdot \widetilde{c_t} \tag{4}$$

This equation updates the current cell state c_t by incorporating the previous cell state c_{t-1} (modulated by the forget gate) and the new candidate state c_t (modulated by the input gate). This ensures the model retains relevant long-term dependencies.

Output gate: Computes the hidden state, which determines the classification result.

$$O_t = \sigma\left(w_O \cdot [h_{t-1}, a_t] + b_O\right) \tag{5}$$

$$h_t = O_t \cdot \tan h(c_t) \tag{6}$$

The output gate O_t regulates what part of the updated cell state c_t contributes to the hidden state h_t, which is used in further computations and message classification.

Final classification: The final hidden state is passed through a fully connected layer with a SoftMax activation function to classify the message as an emergency ($y = 1$) or non-emergency $\hat{y} = 0$:

$$\hat{y} = softmax\left(w_y \cdot h_t + b_y\right) \tag{7}$$

The softmax function ensures that the output probabilities sum to 1, facilitating classification. Loss function: To train the LSTM model, we minimize the cross-entropy loss function.

$$L = -\sum_{i=1}^{n} y_i \log(\hat{y}_1) \tag{8}$$

This loss function computes the difference between predicted probabilities and actual labels to influence the optimization process [31, 32]. The pseudocode of the LSTM-based emergency message classification is shown in Algorithm 1.

Algorithm 1: LSTM-based emergency message classification

Begin
Initialize LSTM model parameters
  For each training iteration:
    For each sequence in the dataset:
      Compute forget gate: $f_t = \sigma\left(w_f \cdot [h_{t-1}, a_t] + b_f\right)$
      Compute input gate: $i_t = \sigma(w_i \cdot [h_{t-1}, a_t] + b_i)$
      Compute candidate cell state: $\widetilde{c_t} = \tan h(w_c \cdot [h_{t-1}, a_t] + b_c)$
      Update cell state: $c_t = f_t \cdot c_{t-1} + i_t \cdot \widetilde{c_t}$
      Compute output gate: $O_t = \sigma\left(w_O \cdot [h_{t-1}, a_t] + b_O\right)$
      Compute hidden state: $h_t = O_t \cdot \tan h(c_t)$
      Compute final classification: $\hat{y} = softmax\left(w_y \cdot h_t + b_y\right)$
      Compute loss: $L = -\sum_{i=1}^{n} y_i \log(\hat{y}_1)$
      Backpropagate and update parameters
    End for
  End for
End

The LSTM model had been trained on sequential vehicular datasets, where the representation of each sample corresponded to a temporal window of DENM and CAM messages. As a preparatory step before training, data normalization, sequence padding, and noise filtering were performed to ensure uniformity of embeddings across different traffic-density levels. Throughout training, the model developed the ability to differentiate real emergency patterns characterized by a progressively increasing tempo over time from false, malicious, or fraudulent alerts that exhibit sudden or temporal signature inconsistencies. Depending on changes in vehicular density, hyperparameters, including the learning rate, dropout ratio, batch size, and number of hidden units, were tuned to achieve the best model performance. The LSTM-based IDS effectively separates genuine emergency alerts

from false messages, improving the security and quality of message transmission in 5G-enabled VANETs. The presented strategy guarantees proper identification of anomalies, prioritization of actual emergencies, and minimization of false positives.

3.3 Secure Emergency Message Dissemination

The architecture of the Multi-Authority Ciphertext-Policy Attribute-Based Encryption (MA-CP-ABE) algorithm is shown in Figure 2. To ensure safe dissemination of emergency messages in the VANET environment, this study presents a so-called MA-CP-ABE. This improved encryption system can provide a more adaptable and safer means of sending emergency messages. In this way, only a combination of attributes will obtain emergency messages. Each attribute is assigned a set of keys to users, and various authorities generate keys for their respective attribute sets. Communications are encrypted and can be deciphered only by users whose attribute sets match the policy, because access controls affect the encryption process. The approach offers scale and flexibility of access control through the separation of attribute management roles. The protocol also minimizes the burden of calculations for users and ensures efficient, secure communication by outsourcing decryption to proxy servers.

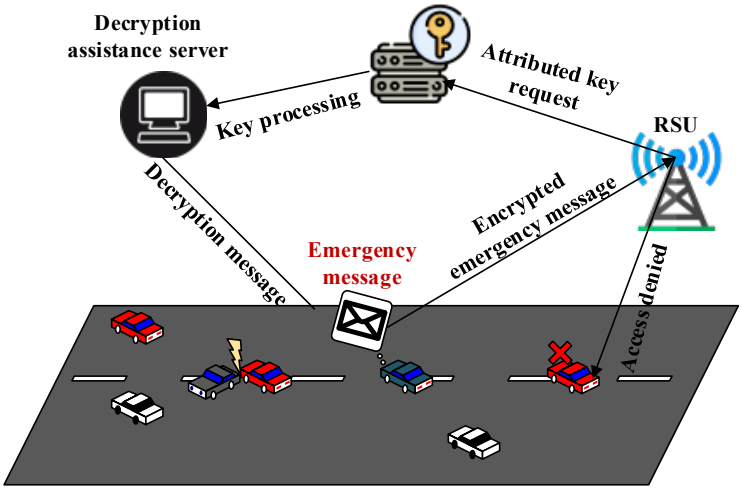

Fig. 2 *Multi-Authority Ciphertext-Policy Attribute-Based Encryption (MA-CP-ABE)*

3.4 System Initialization

To secure message transmission of emergency messages in a VANET setup, we recommend a MA-CP-ABE scheme. The scheme also includes various attribute authorities (AAs), a trusted third party (TTP), and vehicle users (i.e., with computing power). Each authority manages a collection of attributes, and the decryption capability of an emergency message is determined by the attributes attached to the user. This increases scalability, security, and flexible access control.

The system initialization entails the setup phase, where a bilinear pairing function is established for two cyclic groups $\mathcal{G}_1$ and $\mathcal{G}_2$ of prime order:

$$e: \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2 \tag{9}$$

Here, e is defined to be a bilinear pairing function. In particular, in cryptography and notably in ABE, this pairing function is crucially a part of the key generation and encryption computations. The function e takes two inputs from the group $\mathcal{G}_1$ and produces an output in the target group $\mathcal{G}_2$, while satisfying certain bilinear properties that enable secure computation in encryption systems.

A generator G is selected for $\mathcal{G}_1$, and public parameters $\mathcal{p}_P$ are established as:

$$\mathcal{p}_P = \mathcal{G}_1, \mathcal{G}_2, e, G, u_1, \ldots, u_n \tag{10}$$

where $u_1, \ldots, u_n$ is the components that correlate with certain attributes in the system. These settings provide the key management and encryption technique.

A master secret key (α_K) and related public key ($\mathbb{P}_K$) are established by each attribute authority $\mathring{A}_K$. The public key is computed as:

$$\mathbb{P}_K = e(G, G)^{\alpha_K} \tag{11}$$

These authorities are expected to implement attribute-based keys for users and control access policies to maintain secure communications. Once the user is registered and keys are generated, each vehicle user $\mathfrak{U}_i$ is registered with a list of attributes under various authorities. Every attribute to which a user has access has a private key, which is issued by the appropriate authority. We define the secret key as:

$$\mathcal{S}_{K_{\mathfrak{U}_i}} = \left(G^{\alpha_K} u_\beta^{\rho_K}\right) \tag{12}$$

where u_β denotes the attribute-based parameter, while (ρ_K) echoes the previously introduced random blinding factor, serving as an additional disguise for the key.

The key distribution hierarchy will ensure that emergency messages are decrypted by authorized users who meet the established access conditions. This initialisation step provides a means of preventing unauthorised access to emergency messages without restricting dynamic, secure key management by multiple authorities.

3.5 Data Encryption

The encryption scheme will ensure that emergency messages are encrypted safely using an access policy before they are sent. In this case, the data owner encrypts an emergency message $\mathcal{M}$ with an encryption key K and encrypts it using an MA-CP-ABE scheme, so that the emergency data is revealed only to authorized users.

The encryption process is launched by the random selection of a secret ζ and the formation of an access structure (A_P, B_0), when it is known that A_P is a policy on access, and u_0 describes the attribute on each row of A_P. A random vector is chosen as:

$$\mathbb{W} = (\zeta, b_2, \dots, b_n) \in Z_{PN}^n \tag{13}$$

The notation PN is a prime number, ζ is the encryption exponent, and $b_2, \dots, b_n$ distributes the encryption exponent over attributes. We calculate for each row μ_j in A_P:

$$\mu_j = \mathbb{W} \cdot V_j \tag{14}$$

The vector that represents the j -th row of the matrix is denoted by V_j. A random number $\delta \in Z_{PN}$ is introduced for additional security. The ciphertext generation $\mathfrak{C}$ is performed as follows:

$$\mathfrak{C} = K \cdot \prod_{K \in \mathbb{S}_{\mathring{A}}} e(G, G)^{\alpha_K \zeta} \tag{15}$$

$$\mathfrak{C}' = G^{\zeta}, \quad \mathfrak{C}'' = G^{\delta} \tag{16}$$

The term $\mathbb{S}_{\mathring{A}}$ represents the subset of attribute authorities that are responsible for encrypting the message under the given access policy. For each attribute j, the attribute-specific ciphertext component is generated as:

$$\mathfrak{C}_j = G^{w\mu_j} \cdot \left(G^{t_{B_0(j)}} u_{B_0(j)}\right)^{\alpha_K(-\delta)} \tag{17}$$

Where $B_0(j)$ maps attributes to access structure elements. Thus, the final ciphertext is structured as:

$$\mathfrak{C}_T = \left(\mathfrak{C}, \mathfrak{C}', \mathfrak{C}'', \{\mathfrak{C}_j\}_{j \in [1,n]}\right) \tag{18}$$

This encrypted message ensures that only users with attributes that match the policy can decrypt the symmetric key and retrieve the emergency message. The improved MA-CP-ABE encryption offers a more flexible and efficient system for emergency message dissemination, ensuring secure and scalable access control and minimizing the computational overhead of proxy-based decryption systems.

3.6 Key Generation

After the system is initialized and encrypted, the attribute authorities provide the authorized users with private decryption keys. The Key Generation phase ensures that users receive an attribute-based secret key, allowing them to decrypt messages only if they meet the predefined access policy.

For each user $\mathfrak{U}_i$, possessing an attribute set $\mathbb{S}_i$, the corresponding secret key components are computed as:

$$\mathcal{S}_{K_{\mathfrak{U}_i}} = \left(G^{\alpha_K} u_\beta^{\rho_K}\right)^{\mathfrak{r}_i} \tag{19}$$

where $\mathfrak{r}_i$ is a random secret assigned to each user to add another layer of security. Each attribute authority independently generates attribute-specific keys for every user $\mathfrak{U}_i$, ensuring that decryption is possible only when the user holds the correct combination of attributes. The secret key for each attribute Q_γ is computed as:

$$Q_\gamma = G^{\lambda_\gamma} \cdot \left(G^{\tau_\gamma} u_\gamma\right)\Gamma_K \tag{20}$$

where, λ_γ is a secret component associated with the attribute, τ_γ introduces an additional blinding factor, and Γ_K is a security-enhancing random parameter.

Thus, the final user-specific decryption key is structured as:

$$\mathcal{S}_{K_{\mathfrak{U}_i}} = \left(Q_\gamma\right)_{\gamma \,\epsilon\, \mathbb{S}_i} \tag{21}$$

This key will allow the user to do decryption if and only if its attributes meet the encryption policy. Multiple authorities and randomization help increase security and provide fine-grained access control for emergency message dissemination in VANETs.

3.7 Data Decryption

To decrypt the encrypted emergency message, the user possessing the correct attribute set computes:

$$\mathcal{M} = \mathfrak{C} \cdot \left(\prod_{j \epsilon \mathbb{S}_i} e\left(\mathfrak{C}_j, \mathcal{S}_{K_{\mathfrak{U}_i}}\right)\right)^{-1} \tag{22}$$

where $\mathcal{S}_i$ is the set of attributes that the user possesses. If the user holds the required attributes per the access policy, decryption succeeds, and the original message is retrieved.

3.8 Attribute Revocation

In cases where an attribute is compromised or a user loses access rights, the attribute revocation mechanism is triggered. The system updates the attribute keys using a time-based or dynamic revocation strategy. The revoked attribute key is updated as:

$$\mathbb{P}_{K_\gamma}{}' = \mathbb{P}_{K_\gamma} \cdot G^{\Delta_\gamma} \tag{23}$$

where Δ_γ is a revocation parameter that ensures previous keyholders cannot decrypt messages encrypted under the updated access policy. Users who still hold valid attributes receive updated keys:

$$\mathcal{S}_{K\mathfrak{U}_i}{}' = \mathcal{S}_{K_{\mathfrak{U}_i}} \cdot G^{\Delta_\gamma} \tag{24}$$

This approach will ensure that revoked users cannot decrypt future emergency messages and that authorized users can still communicate safely within the VANET framework.

3.9 Priority-based Scheduling

The urgency of emergency messages exchanged over VANETs is prioritized by implementing the Edge-Decentralized Environmental Notification Messages (DENM) Prioritization Algorithm. The urgency of the messages is considered, and once they have been arranged into various priority levels, they are presented to the communication channel accordingly. Therefore, messages associated with accidents or hazardous situations receive priority over the rest. This implies that despite the presence of malicious or selfish nodes that pervert the network, vital messages are received and sent in a timely manner. Upon re-evaluation of priorities and paths, the algorithm efficiently eliminates transmission delays, delivering emergency messages to individuals in the minimum possible time.

The prioritization score $\mathbb{P}_m$ of an emergency message m is calculated based on multiple factors:

$$\mathbb{P}_m = w_1 SE_m + w_2 \Re_m + w_3 t_m + w_4 D_m \tag{25}$$

where SE_m represents the severity of the emergency, $\Re_m$ denotes the relevance to nearby vehicles, t_m captures the time sensitivity, and D_m is the distance from the event location. The weight factors are assigned to each parameter to determine the overall priority of the message. The message arrival rate is given by:

$$\lambda_m = \frac{n_m}{t} \tag{26}$$

where n_m is the number of incoming messages within a given time t, allowing the system to determine traffic congestion levels. The total transmission delay is computed as:

$$Dl_{total} = t_q + t_p \tag{27}$$

where t_q represents the queuing delay due to network congestion, and t_p is the propagation delay that depends on distance.

The queuing delay is formulated as:

$$t_q = \frac{\mathbb{L}_m}{T_{rate_m}} \tag{28}$$

where $\mathbb{L}_m$ is the message length and T_{rate_m} resembles the transmission rate, determining how fast a message can be processed. The propagation delay is given by:

$$t_p = \frac{D_m}{\mathbb{v}_m} \tag{29}$$

where D_m denotes the physical distance between sender and receiver, and $\mathbb{v}_m$ is the signal propagation speed. To evaluate the urgency of message transmission, the priority index $\mathcal{P}_{in_m}$ is computed as:

$$\mathcal{P}_{in_m} = \frac{\mathbb{P}_m}{Dl_m} \tag{30}$$

This ensures that messages with high urgency and low delay receive priority access to network resources. The available bandwidth for transmission BW_A is determined as:

$$BW_A = BW_{total} - \sum_{i=1}^{n} BW_i \tag{31}$$

where BW_{total} refers to the total bandwidth and BW_i is the bandwidth utilized by current transmissions. Messages are either transmitted right away or held in a queue for subsequent transmission. If a channel is available, message assignment is conducted as follows:

$$\mathbb{C}_m = \begin{cases} Assigned, & if\ BW_A > \mathbb{C}_m \\ Qucued, & otherwise \end{cases} \tag{32}$$

Messages are either transmitted right away or held in a queue for subsequent transmission. The optimal scheduling decision rule OP_{sh} is given by:

$$OP_{sh} = \min_m (Dl_m | \mathbb{P}_m > \mathbb{P}_{th}) \tag{33}$$

Making sure that only messages that surpass a defined priority level of $\mathbb{P}_{th}$ will be sent out first. The probability of a message dropping due to congestion is given by:

$$PN_{Congestion} = e^{-\psi_m t} \tag{34}$$

Let ψ_m equal the rate at which your system is servicing requests. Thus, compute the probability of a message being sent successfully:

$$P_{SU} = 1 - PN_{Congestion} \tag{35}$$

The scheduling mechanism will ensure that emergency messages arrive at their intended destinations with minimal latency and will regulate the network's congestion state, making it more efficient for ordinary message delivery in VANETs. In a real-world implementation scenario, the suggested structure could operate within the scope of a 5G-enabled VANET, in which RSUs equipped with real-time, LSTM-based message-validation edge-light

servers relay only authorized messages to proximal vehicles. To manage on-vehicle computational load, CP-ABE encryption could be performed at the edge or a proxy. RSU's DENM scheduling module is a priority queue. This arrangement complements existing smart-city ITS deployments with no structural modifications required, only the usual RSU-OBU exchanges.

4. Experimental Results

The primary goal of this study is to establish an AI-based communication framework for emergency messages in VANETs that uses 5G to transmit messages efficiently, securely, and privately during emergencies. Artificial intelligence optimizes the communication process, reduces delays and interference, and strengthens the security and privacy of communications in a high-mobility environment.

4.1 Simulation Setup

The VANETs emergency message dissemination scheme, which was secured, was designed and implemented using OMNeT 4.6 as the primary network simulation tool and SUMO-0.19.0 as the traffic simulation tool. The whole simulation was done on Windows 11 (64-bit). The network case consists of 50 vehicles and 2 Road Side Units, which simulate an intelligent transport system. The vehicle-to-RSU connection used to gather real-time data for emergency event classification was via communication. The system specification setup is as given in Table 2.

Table 2 *System specification*

Hardware specifications	Storage	500 GB SSD
	RAM	16 GB
Software specifications	Simulation tools	OMNET++ 4.6, SUMO-0.19.0
	Processor	Intel Core i7
	OS	Windows 11 – (64-bit)

4.2 Model Accuracy

In emergency message distribution, model accuracy is highly important not only for suitable message classification but also for limiting false alarms and action determination in uncertain traffic states. The suggested model is also relative to the number of vehicles allocated to its networks. Thus, the increased density will cause congestion, obstruction, interruptions, and packet collisions. The model accuracy ($A_{ccuracy}$) is computed as:

$$A_{ccuracy} = \frac{(True\ positive + True\ negative)}{True\ positive + True\ negative + False\ positive + False\ negative} \tag{36}$$

The classification accuracy of emergency messages is also a key performance factor that directly influences the reliability and credibility of the entire communication framework. As the experimental findings reveal, the proposed LSTM-based IDS exhibits a consistently high classification accuracy across all considered vehicle-density conditions. The initial accuracy of the proposed method with 5 vehicles was 94% and decreased to 76% with maximum density (50 vehicles), with a steady 9-20% performance advantage over competitive strategies. Such a downward trend is indicative of the practicality of machine learning systems operating in increasingly complex, interacting network scenarios, as depicted in Table 3.

Table 3 *Number of vehicles vs. model accuracy (%)*

Number of Vehicles	Model Accuracy (%)			
	Proposed	MCB-HCC	TBGR	LAMD
5	94	85	80	75
10	92	83	78	72
15	90	81	76	70
20	88	79	74	68
25	86	77	72	66
30	84	75	70	64
35	82	73	68	62
40	80	71	66	60
45	78	69	64	58
50	76	67	62	56

J. of Soft Computing and Data Mining Vol. 6 No. 3 (2025) p. 370-386

The greater the vehicle density, the more difficult situations the LSTM classifier would need to handle, such as high background noise, high packet collisions, and more intricate interference patterns that inherently degrade classification precision. The high-performance level is based on the multiple architectural solutions in the presented framework. The LSTM network's capacity to learn long-term temporal correlations in vehicle communication patterns enables it to identify the real emergency signature over the false-alarm pattern, unlike traditional rule-based or threshold-based detectors used by rival algorithms. The time-series analysis method enables the system to capture the evolutionary nature of emergencies: genuine emergencies tend to exhibit a temporal pattern in their communication signatures. Moreover, the LSTM architecture has an adaptive learning capability that allows it to continuously refine classification parameters in response to observed traffic patterns and environmental conditions. This dynamic adaptive scheme ensures that the system remains robust as network conditions change, unlike traditional static classification schemes, which gradually degrade under changing operating conditions. The continuous performance difference with MCB-HCC (9% improvement), TBGR (14-16% improvement), and LAMD (17-20% improvement) indicates the efficiency of the AI-based methodology compared to traditional clustering-, trust-, and location-based detection processes. The increasing performance gap at higher vehicle densities (9% to 20% better than competitors) demonstrates that the suggested approach scales better, as it does not deteriorate performance as much as traditional approaches do under harsh high-density vehicle conditions. Figure 3 shows the relation between the number of vehicles and model accuracy.

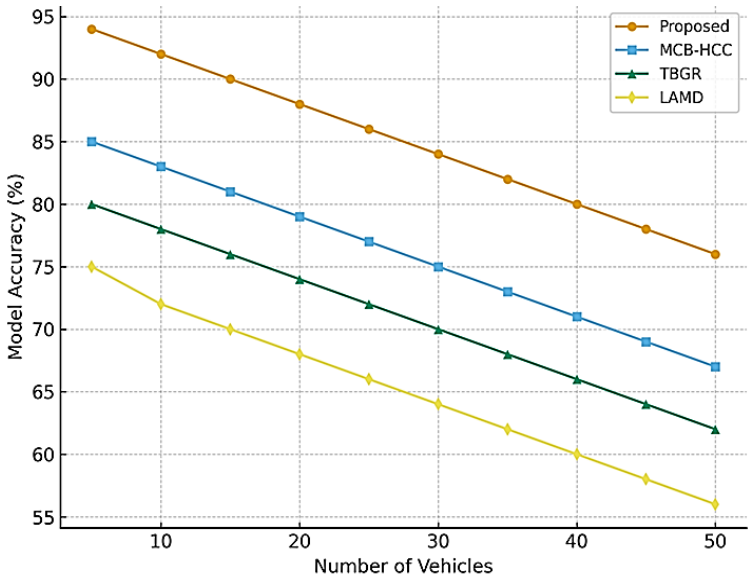

Fig. 3 *Number of vehicles vs. model accuracy (%)*

4.3 Precision Analysis

Precision is the percentage of messages marked as malicious that are actually malicious. In VANET emergency message dissemination, sensitivity is very precise, so the IDS will not issue unnecessary alarms by incorrectly labeling valid emergency alerts as attacks. This is vital because false alarms may delay the provision of safety-critical information to vehicles. The precision performance of the suggested IDS and existing approaches is provided in Table 4 and Figure 4, respectively. Precision indicates how well the system can accurately categorize malicious messages without creating false alarms. The proposed IDS attains a precision of more than 94% at all vehicular densities, whilst being much more precise than the baseline methods (MCB-HCC, TBGR, LAMD, and EEMDS) by around 8-12 percentage points. This implies that the suggested structure is highly efficient at reducing false alerts, which is essential in VANET emergencies, where the unwarranted blocking of legitimate messages may slow the delivery of life-saving information.

Table 4 *Precision of proposed IDS vs. baselines*

Vehicles	Proposed IDS	MCB-HCC	TBGR	LAMD	EEMDS
50	94.2	85.0	82.1	79.4	81.6
100	94.6	85.8	82.9	80.1	82.0
200	95.0	86.3	83.6	80.5	82.5
300	95.4	86.9	84.2	81.0	82.9
500	95.7	87.2	84.7	81.5	83.4

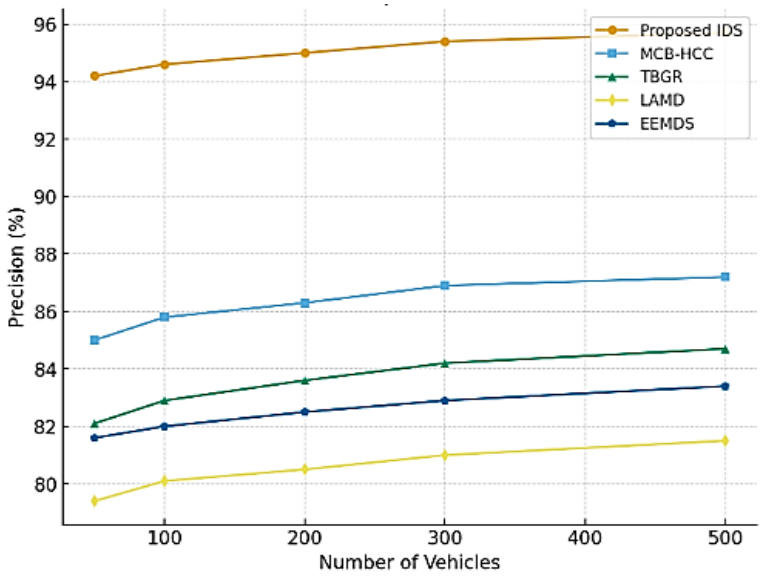

Fig. 4 *Precision (%) of proposed IDS vs. baselines*

4.4 Recall Analysis

Recall, also referred to as sensitivity or detection rate, is the percentage of real malicious messages correctly recognized by the IDS. High recall is a requirement in VANETs, since false negatives (missed attacks) may enable the spread of false data about an emergency, which can potentially endanger road safety. Figure 5 and Table 5 depict the IDS's recall performance, which quantifies its ability to recall malicious emergency messages. The proposed system has a recall of over 92.5% at low densities and over 95% at higher densities. Compared with the baseline schemes, the schemes stand in the 76-84% range. Such findings confirm that the IDS proposed catches almost every malicious activity, which contributes to a reduction of false negatives. This is essential in the case of VANETs, where undetected false messages can jeopardize road safety and emergency response organizations.

Table 5 *Recall of proposed IDS vs. baselines*

Vehicle	Proposed IDS	MCB-HCC	TBGR	LAMD	EEMDS
50	92.5	82.0	79.0	76.0	78.2
100	93.8	82.7	80.0	76.5	78.5
200	94.2	83.5	80.8	77.2	79.1
300	94.8	84.1	81.4	77.9	79.6
500	95.1	84.8	82.0	78.6	80.2

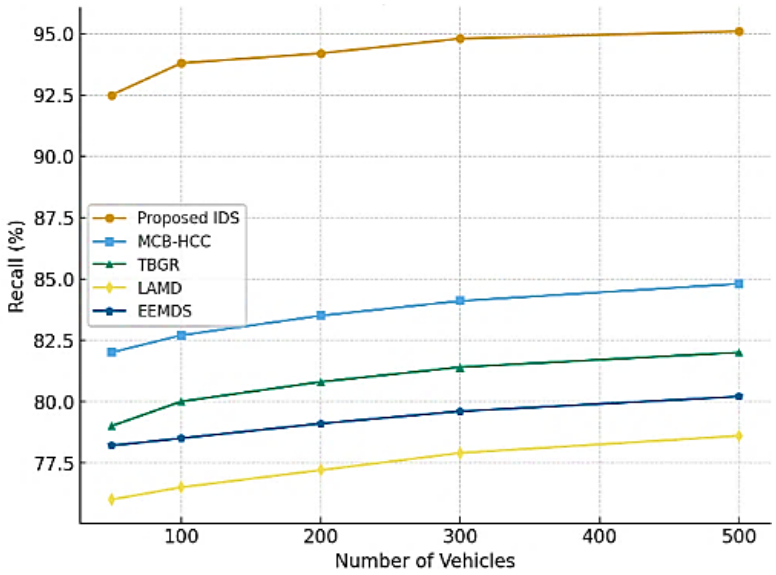

Fig. 5 *Recall (%) of proposed IDS vs. baselines*

4.5 F1-Score Analysis

The F1-Score represents the harmonic mean of recall and precision, which is a single measure of detection quality. F1 is highly applicable to VANET system settings because it can provide both low false positives and low false negatives. Table 6 and Figure 6 display the F1-score, a combination of precision and recall into one indicator of detection quality. The proposed IDS has an F1-score of 93.3% to 95.4% in all cases, which is 10 to 13% higher than the baselines. The consistency of the F1-score at different traffic densities is an indication of the strength of the proposed system. This demonstrates that the architecture consistently detects malicious messages and is resistant to false alarms, and thus fits well within massive VANET implementations in dynamic 5G settings.

Table 6 *F1-Score of proposed IDS vs. baselines*

Vehicles	Proposed IDS	MCB-HCC	TBGR	LAMD	EEMDS
50	93.3	84.7	82.1	79.4	81.6
100	94.2	85.5	82.9	80.1	82.0
200	94.6	86.2	83.6	80.5	82.5
300	95.1	86.7	84.2	81.0	82.9
500	95.4	87.1	84.7	81.5	83.4

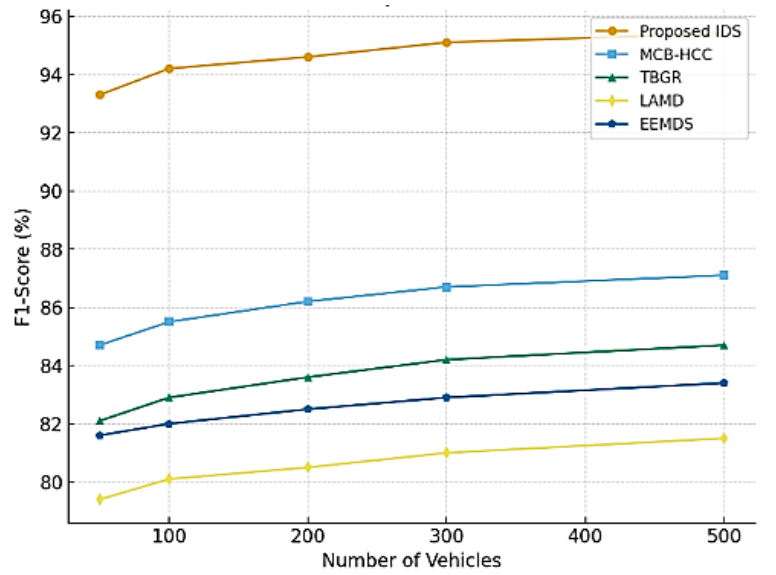

Fig. 6 *F1-score of proposed IDS vs. baselines*

4.6 False Positive Rate vs. True Positive Rate

An essential parameter for assessing the reliability of the emergency message broadcast system in VANETs is the False Positive Rate (FPR) relative to the True Positive Rate (TPR). Greater TPR values indicate better detection of legitimate emergency messages, and lower FPR values indicate reduced misclassification of normal messages as emergency messages. The results for the FPR and TRP of the proposed IDS versus the baseline are shown in Table 7 and Figure 7.

Table 7 *False positive rate (%) Vs. true positive rate (%)*

X-axis (False Positive rate %)	Y-axis True Positive rate (%)			
	Proposed	MCB-HCC	TBGR	EEMDS
5	78	65	65	55
10	85	72	72	63
15	89	78	78	69
20	92	83	83	74
25	94	87	87	78
30	95	90	90	81
40	97	93	93	85
50	98	95	95	88

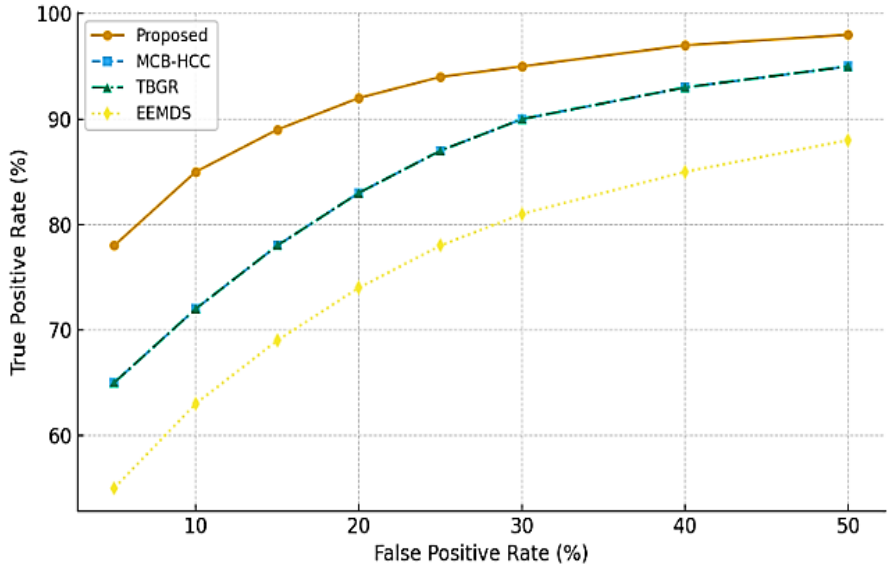

Fig. 7 *False positive rate vs. true positive rate (%)*

The correlation between the TPR and the FPR provides important information about the reliability of the emergency detection system's classification, which is the primary trade-off between detector sensitivity and the generation of false alarms. The proposed technique shows better detection performance across all analysed FPR limits, with 85% TPR at 10% FPR and a scaling of 98% TPR at 50% FPR. This performance is a steady improvement to competing approaches, with improvements of 13-22 percentage points in TPR at similar FPR levels. The excellent TPR-FPR performance is due to the LSTM network's advanced pattern recognition, which enables a more discriminative separation between genuine emergency patterns and false-alarm signatures. The time-series analysis method ensures that the system can account for the temporal dynamics of emergencies, as real emergencies tend to follow characteristic development patterns that can be distinguished from random anomalies or intentional false alarms. The LSTM architecture's adaptive learning mechanism enables continuous improvement of detection thresholds based on the encountered traffic patterns and the nature of false alarms. Such dynamic optimization guarantees the system a constant optimal sensitivity during false-alarm reduction, outperforming competing methods that use a static threshold. There are far-reaching practical implications of the obtained detection performance in emergency response systems. The fact that the TPR values are very high (85-98%) indicates that the risk of missing life-threatening incidents is minimized.

At the same time, the regulated FPR rates prevent resource waste and user fatigue caused by too many false alarms. The excellent performance in the middle of an FPR (94% TPR at 25% FPR) is indicative of the system's real-world applicability, since the ability to maintain high emergency detection rates and reduce false alarms is essential to user acceptance and effective emergency service. Nevertheless, the LSTM-based IDS has a very high

TPR, but the FPR is also high (up to 50%). Additional classification threshold or ensemble model tuning is needed to lower false positives before it is put into practice.

5. Conclusion

The work proposes a novel AI-driven design of privacy-preserving and secure dissemination of emergency messages in VANETs as part of 5G deployment. The system combines AI-based IDS with LSTM networks, CP-ABE, and priority scheduling of efficient emergency message delivery in VANETs. After an extensive assessment relative to benchmarks MCB-HCC, TBGR, LAMD, and EEMDS, balanced scores were achieved. The analysis has shown that the suggested IDS consistently achieved high precision, recall, and F1 Score, indicating that the system could reduce false alarms while identifying nearly all malicious messages. Such a balance is paramount in the emergency message dissemination in VANET, where false positives and false negatives may pose a threat to road safety. Overall, this study presents a scalable, secure, and privacy-preserving emergency communication system designed for dynamic VANET settings. The proposed solution is a promising approach for future ITS because it significantly enhances the security of emergency message dissemination through intelligent IDS, encryption, and scheduling strategies. The proposed IDS demonstrates superior performance relative to MCB-HCC, TBGR, LAMD, and EEMDS owing to the temporal learning within the LSTM network. Traditional approaches often consider static attributes such as geographical location, trust thresholds, or the state of the cluster, making them quite vulnerable to noise and packet-drop collisions. Unlike traditional approaches, LSTM considers the messages over time, allowing the detection of small deviations in message streams associated with default alerts or fabricated emergencies. Accordingly, the IDS exhibits high precision and recall scores despite increasing the message density.

Data Availability Statement:

The datasets produced and assessed in the course of the current study can be obtained from the respective author upon reasonable request. The simulation scenarios and parameter files (OMNeT++ and SUMO settings) can be made available on request under research and educational use.

Acknowledgments

The authors gratefully acknowledge the Electronic Computer Center at the University of Anbar for providing computational resources and technical support.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design:*** *Maath A. Albeyar, Ikram Smaoui;* ***data collection:*** *Ikram Smaoui;* ***analysis and interpretation of results:*** *Maath A. Albeyar, Ikram Smaoui, Hassene Mnif;* ***draft manuscript preparation:*** *Ikram Smaoui, Sameer Alani. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] Kaur, R., Doss, R., & Pan, L. (2024). The route based emergency message dissemination scheme using multihop wireless network for VANETs. Telecommunication Systems, 87(4), 1183-1199.

[2] Dodia, A., Kumar, S., Rani, R., Pippal, S. K., & Meduri, P. (2023). EVATL: A novel framework for emergency vehicle communication with adaptive traffic lights for smart cities. IET Smart Cities, 5(4), 254-268.

[3] Albeyar, M. A., Smaoui, I., Mnif, H., & Alani, S. (2024). Proposed supercluster-based UMBBFS routing protocol for emergency message dissemination in edge-RSU for 5G VANET. Computers, 13(8), 208.

[4] Guesmia, S., Djahel, S., & Semchedine, F. (2023). A new delay-based broadcast suppression mechanism for efficient emergency messages dissemination in CAVs environment. Ad Hoc Networks, 149, 103242.

[5] Ahmed, A., & Iqbal, M. M. (2024). SDN-based emergency message dissemination protocol for IoV-Fog networks. Telecommunication Systems, 85(2), 225-235.

[6] Shah, M. A., Zeeshan Khan, F., Abbas, G., Abbas, Z. H., Ali, J., Aljameel, S. S., ... & Aslam, N. (2022). Optimal path routing protocol for warning messages dissemination for highway VANET. Sensors, 22(18), 6839.

[7] Figueiredo, A., Rito, P., Luís, M., & Sargento, S. (2023). Mobility sensing and V2X communication for emergency services. Mobile Networks and Applications, 28(3), 1126-1141.

[8] Saad, M. A., Alhamdane, H. J., Ali, S. A. H., Hashim, M. M., & Hasan, B. (2020). Total energy consumption analysis in wireless mobile ad hoc network with varying mobile nodes. *Indonesian Journal of Electrical Engineering and Computer Science*, *20*(3), 1397-1405.

[9] Al-Heety, O. S., Zakaria, Z., Abu-Khadrah, A., Ismail, M., Shakir, M. M., Alani, S., & Alsariera, H. (2025). Traffic Congestion Control with Emergency Awareness and Optimized Communication Infrastructure using Reinforcement Learning and Non-Dominated Sorting Genetic Algorithm. *IEEE Access*.

[10] Zoghlami, C., Kacimi, R., & Dhaou, R. (2023). 5G-enabled V2X communications for vulnerable road users safety applications: A review. Wireless Networks, 29(3), 1237-1267.

[11] Zhang, C., Lin, X., Lu, R., & Ho, P. H. (2008). *RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks*. In *IEEE International Conference on Communications (ICC)*, pp. 1451–1457.

[12] Chim, T. W., Yiu, S. M., Hui, L. C. K., & Li, V. O. K. (2011). *SPECS: Secure and privacy enhancing communications schemes for VANETs*. Ad Hoc Networks, 9(2), 189–203.

[13] Alani, S., Zakaria, Z., & Hamdi, M. M. (2019). A study review on mobile ad-hoc network: Characteristics, applications, challenges and routing protocols classification. *International Journal of Advanced Science and Technology*, *28*(1), 394-405.

[14] Sánchez, L. C., Gómez, J., & Parra, O. J. S. (2025). The evolution of VANET: A review of emerging trends in artificial intelligence and software-defined networks. IEEE Access.

[15] Barmpounakis, S., Maroulis, N., Koursioumpas, N., Kousaridas, A., Kalamari, A., Kontopoulos, P., & Alonistioti, N. (2022). AI-driven, QoS prediction for V2X communications in beyond 5G systems. Computer Networks, 217, 109341.

[16] Bilal, M., Munir, E. U., & Ullah, A. (2023). BEMD: Beacon-oriented Emergency Message Dissemination scheme for highways. Ad Hoc Networks, 142, 103095.

[17] Liu, J., Wan, J., Jia, D., Zeng, B., Li, D., Hsu, C. H., & Song, H. (2017). *High-efficiency urban traffic management in edge computing-assisted 5G vehicular networks*. IEEE Transactions on Vehicular Technology, 68(5), 4192–4203.

[18] Ali, R., Liu, R., Nayyar, A., Waris, I., Li, L., & Shah, M. A. (2023). Intelligent driver model-based vehicular ad hoc network communication in real-time using 5G new radio wireless networks. IEEE Access, 11, 4956-4971.

[19] Rizwan, S., Husnain, G., Aadil, F., Ali, F., & Lim, S. (2023). Mobile Edge-based Information-Centric Network for emergency messages dissemination in Internet of Vehicles: A Deep Learning Approach. IEEE Access, 11, 62574-62590.

[20] Hemmati, A., & Zarei, M. (2024). UFC3: UAV-Aided Fog Computing Based Congestion Control Strategy for Emergency Message Dissemination in 5G Internet of Vehicles. Automotive Innovation, 7(3), 456-472.

[21] Rawat, D. B., & Popescu, D. C. (2015). *Enhanced trust-based routing protocol to secure vehicular ad hoc networks*. In *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, pp. 1–5.

[22] Gazdar, T., Rachedi, A., Benslimane, A., & Belghith, A. (2015). *A distributed and adaptive trust-based approach for securing communications in vehicular ad hoc networks*. IEEE Transactions on Vehicular.

[23] Firdissa, N., Gemeda, K. A., Mishra, S., Rathee, D. S., Singh, R. S., & Darejew, T. (2025). Disseminating a Fair Emergency Message With V2V Communication Technology in VANET. Security and Communication Networks, 2025(1), 8882649.

[24] Lim, J., Pyun, D., Choi, D., Bok, K., & Yoo, J. (2023). Efficient Dissemination of Safety Messages in Vehicle Ad Hoc Network Environments. Applied Sciences, 13(11), 6391.

[25] Hassan, N., Fernando, X., & Woungang, I. (2023, December). An Emergency Message Routing Protocol for Improved Congestion Management in Hybrid RF/VLC VANETs. In Telecom (Vol. 5, No. 1, pp. 21-47). MDPI.

[26] Ghaleb, F. A., Ali, W., Al-Rimy, B. A. S., & Malebary, S. J. (2023). Intelligent proof-of-trustworthiness-based secure safety message dissemination scheme for vehicular ad hoc networks using blockchain and deep learning techniques. Mathematics, 11(7), 1704.

[27] Alowish, M., Shiraishi, Y., Mohri, M., & Morii, M. (2021). Three layered architecture for driver behavior analysis and personalized assistance with alert message dissemination in 5G envisioned Fog-IoCV. Future Internet, 14(1).

[28] Ullah, S., Abbas, G., Waqas, M., Abbas, Z. H., & Halim, Z. (2023). Multi-hop emergency message dissemination through optimal cooperative forwarder in grid-based 5G-VANETs. Journal of Ambient Intelligence and Humanized Computing, 14(4), 4461-4476.

[29] Nauman, A., Iqbal, A., Khurshaid, T., & Kim, S. W. (2024). Multi-Layered Unsupervised Learning Driven by Signal-to-Noise Ratio-Based Relaying for Vehicular Ad Hoc Network-Supported Intelligent Transport System in eHealth Monitoring. Sensors, 24(20), 6548.

[30] ul Hassan, M., Al-Awady, A. A., Ali, A., Sifatullah, Akram, M., Iqbal, M. M., ... & Abdelrahman Ali, Y. A. (2024). ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV. Sensors, 24(3), 818.

[31] Chakroun, R., Abdellatif, S., & Villemur, T. (2022). LAMD: Location-based Alert Message Dissemination scheme for emerging infrastructure-based vehicular networks. Internet of Things, 19, 100510.

[32] Ullah, S., Abbas, G., Waqas, M., Abbas, Z. H., Tu, S., & Hameed, I. A. (2021). EEMDS: An effective emergency message dissemination scheme for urban VANETs. Sensors, 21(5), 1588.