International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Deep Learning based Misbehaviour Detection using Blockchain in SDN based 5G-VANET

[1]Nileema Pathak, [2]Purushottam R Patil

Submitted: 28/01/2024 **Revised**: 06/03/2024 **Accepted**: 14/03/2024

Abstract: Vehicular ad hoc network (VANETs) is fabricated by adopting the principles of ad hoc manner that embraces of group of vehicle in mobility or stationary mode connected by wireless network. Main intention of VANET is to accommodate safety and comfort in vehicular environments through information sharing. Due to highly dynamic connections and sensitive data sharing, the VANET is excessively prone to attacks and being a wireless network it is an eye-catching environment for attackers. To overcome this attack, we have proposed deep learning entrenched misbehavior detection using blockchain technology. Furthermore, to enhance the efficiency of communication and security in VANET, the software defined network is integrated with VANET known as SDVANET. In this paper, there are three phases such as quantum based authentication, dynamic clustering and hybrid misbehavior detection. Initially, the vehicles are registered and authenticated through blockchain using Quantum Key Distribution (QKD) which ensures the vehicle legitimacy. Here, the blockchain is adopted for secure communication and data storage that enhance data privacy. Following the vehicles are clustered by utilizing K-means algorithm with Leader Optimization Algorithm (i.e. Leader based K-means clustering (LKCM)) for optimal centroid selection and 5G communication is utilized, thus improves communication efficiency thereby minimizing latency. After that, hybrid misbehavior detection is accomplished in terms of data-centric and node-centric misbehavior detection. Data-centric misbehavior detection is performed by trust estimation of each vehicle in direct and indirect manner using Multi-head Attention Long Term Short Memory (MHA-LSTM). At last, we execute node-centric based misbehavior detection by determining the similarity based message verification using Fuzzy Similarity which are result in intensifying VANET security. The proposed work is conducted by OMNeT++ and several performance metrics are evaluated in terms of end-to-end delay, packet loss ratio, packet delivery ratio, transmission overhead, throughput and accuracy where the proposed outperforms the existing approaches.

Keywords: *Quantum Key Distribution, Hybrid misbehaviour detection, Similarity based message verification, Trust management, Deep learning.*

1. Introduction

A vehicular ad hoc network (VANET) includes a group of vehicles connected through a wireless network which provides support for various processes such as traffic safety, multimedia content sharing, road accidents, pedestrian warning, etc [1]. Generally, VANET includes three types of communications which are vehicle-to-infrastructure (V2I), vehicle-to-vehicle (V2V), and vehicle-to-everything (V2X) [2][3]. Due to high mobility, the communication reliability are majorly affected in VANET which is also an foremost issue. For providing ultra-low latency and high-speed internet the 5G communication is integrated into the VANET [4][5].

Unluckily, the vehicles do not support massive amount of data processing, hence the VANET used Roadside Unit (RSUs) for computing tasks, in this way, VANET improved its communication efficiency [6]. However, RSUs also have limited resources that cannot tolerate a large number of tasks, hence the edge computing servers are deployed in the VANET environment for providing additional resources and reducing latency and energy consumption in VANET [7][8]. To overcome the congestions in the traditional VANET environment, the Software Defined Network (SDN) architecture is integrated into the VANET improves the performance of the VANET environment in terms of scalability, flexibility, and management [9]. The SDN architecture has the responsibility of managing, controlling, and monitoring the network resources effectively. This integration architecture provides better solutions in terms of traffic control, congestion control, and communication efficiency [10].

However, safety is another important criterion in VANET during message broadcasting, because some dishonest vehicle participates in the network to broadcast fake information which leads to many serious issues such as traffic congestion and road accidents [11]. To resolve these issues, the authenticities of the vehicles or misbehaviors are detected by calculating the trust values based on their history information and neighbor feedback [12]. Though various misbehavior solutions are proposed by the authors in the VANET environment, still it has some research challenges. To resolve these issues both node-centric and

[1]*Computer Science and Engineering Sandip University Nasik, India*
nileemap@gmail.com
[2]*Professor, Computer Science and Engineering Sandip University Nasik, India*
purupatil7@gmail.com

data-centric misbehavior detections in combination this provides privacy, security, and quality messages [13]. However, the trust values and integrity are verified and maintained by the third party or RSUs without any security that leads to a single point of failure. Blockchain is a distributed ledger that ensures privacy and security to the environment by recording all the transaction in a hash manner that cannot compromised or hacked by anyone. All the information and trust values are collected by the RSUs and stored in the blockchain for security. The blockchain verifies all transactions and entities to enhance security.

1.1 Motivation & Objectives

The main aim of this research is to detect misbehaviors with high accuracy and less latency in SDN based 5G-VANET environment using blockchain and deep learning techniques. This research also addresses high energy consumption, inefficient network management, and decentralized security for VANET. The major objective of this is to detect misbehaviors in SDN based 5G-VANET environment. The other sub-objectives of this research are listed as follows,

- To increase security authentication was performed for vehicles, RSUs, and pedestrians which protect against external and position falsification attacks
- To reduce energy consumption and increase communication efficiency clustering is performed in SDN based 5G-VANET environment
- To improve scalability, and management hierarchical controllers are placed in an environment that provides robust control management
- To improve security data-centric and node-centric misbehaviors are detected by deep learning techniques with high training speed and accuracy

1.2 Research Contributions

The foremost contribution of this research is to misbehaviors with high accuracy and less latency in SDN based 5G-VANET environment. The major contributions of this research are elucidated as follows,

- Ensuring vehicle legitimacy through quantum based authentication by blockchain where to enhance security QKD is utilized for key generation. In which a key is generated and transmitted through quantum channel that amplifies tamper proof. Furthermore, the legitimate vehicles are only allowed into the network and vehicle credentials are securely store in blockchain.
- Security enhancement is achieved by proposing hybrid misbehavior detection which detects the misbehaviour in terms of data centric and node centric categories. Here, the data centric misbehavior detection is executed by trust estimation of vehicles using MHA-LSTM and node centric misbehavior detection by similarity based message verification using fuzzy similarity.
- For decoupling of control and data plane, the SDN is integrated with VANET, while combining these network the SDN improves the VANET efficiency and misbehavior detection performance thus aids to security strengthen. Overall the proposed SDVANET enhance network security thereby improving communication among vehicles.

1.3 Paper Organization

This paper is further arranged into several sections which are defined as follows, Section II represents the state-of-art and its research limitations. Section III describes the major problems that are faced on misbehavior detection in VANET. Section IV demonstrates the proposed MHA-LSTM Model research methodology which enfolds of pseudocode, mathematical equations and algorithm workflows. Section V illustrates the simulation setup and comparison results of the simulation results and summary of proposed work. Section VI concludes the proposed MHA-LSTM Model.

2. Literature Survey

A misbehavior detection system using machine learning approaches to detect position falsification attacks in VANET was proposed [16]. This research considered speed, position, distance, and angle of arrival for identified position falsification attacks. The distance was calculated based on RSSI between receiver and sender. Here, two machine learning algorithms (kNN and random forest) were proposed to extract the features from the safety messages for identifying position falsification attacks. Based on the extracted features, classification was done by a generalized linear model. The comparison result demonstrated that the proposed work achieved superior performance in terms of classification accuracy and computation time. Deep learning approach for misbehavior detection in intelligent transportation systems was proposed [17]. The proposed system used both single-stage and multi-stage classifiers namely Convolutional Neural Network (CNN) and Long Short-Term Machine (LSTM) to perform classification which is run into the edge server. The RSU collects the information and send it to the edge server for misbehavior detection. The experimental result demonstrates that the proposed work achieved better performance in terms of f-score and prediction time. Here, LSTM and CNN are used for misbehavior detection which leads to high complexity because of generating unwanted convolutional layers and unnecessary calculation in CNN and LSTM respectively. A machine learning based misbehavior detection in VANET was introduced in this

research [18]. The proposed work identified both external and internal attacks by evaluating the reputation score of the vehicles. The reputation certificate was provided by the access point and it was verified by using a private key which are stored in the reputation server. Here, Dempster Shafer theory was used for feedback combination, based on the result of feedback reputation was updated in the server. If the node is identified as malicious then the revocation process was performed to increase security. The comparison results show that the proposed work achieved superior performance in term of accuracy. Here, machine algorithm learning algorithm was proposed for misbehavior detection, however, it takes much time for training that leads to high latency which reduces the efficiency of the work. Misbehavior detection using an ensemble learning algorithm was enabled for VANET [19]. The proposed work used random forest algorithm for performing local intrusion detection. The proposed work includes four processes such as individual intrusion classification, neighbor intrusion classification, misbehavior evaluation, and collaborative intrusion classification. Initially, unwanted and incomplete data were removed from the collected data to increase detection accuracy. Based on the collected information the random forest classifies the intrusions. After that, the neighbor's misbehaviors were evaluated using local data. Finally, the collaborative intrusion was detected by calculating the weight values of the tested sample which classified the vehicle into normal or intruder. Here, random forest algorithm was used for misbehavior detection, however generates large amount of sub trees that leads to high complexity and latency which reduces the performance of misbehavior detection.

In this paper [20], the author performed misbehavior detection using machine learning algorithm. This research mainly concentrated on position falsification attack detection. Initially, all the vehicles register their entity during registration and get a secret key for authentication. The safety messages were broadcast by the vehicles and the RSU access the information and combined the information if it is received from the same sender. From the collected information features (i.e., RSSI, position, and speed) are extracted for classification. Here, four algorithms were proposed for classification such as random forest, naïve bayes, decision tree, and k nearest neighbor. Here, misbehaviors are detected based on RSSI, position, and speed which are not enough for misbehavior detection that leads to poor accuracy in misbehavior detection. A data centric misbehavior detection using machine learning approach for internet of vehicles offered in another research [21]. The proposed machine learning algorithms extracted the features such as distance, direction, position, and velocity from the ground truth data. After completing feature selection, the proposed initiate the plausibility checks using machine learning models. Here, two types of plausibility checks were performed such as location plausibility and movement plausibility. The experimental results demonstrate that the proposed work achieved good performance in terms of precision, and recall. Author in [22], proposed reinforcement learning based trust management in software defined VANET environment. The proposed work provided a secure communication between the vehicle nodes. For that purpose, both direct and indirect trust values of the node were evaluated based on packet forwarding ratio. Here, Deep Q-learning algorithm was used to optimize the ETX values by considering delivery ratio and trust feature for secure link communication. In that way, this research detected the optimal link with high quality communication that reduces misbehaviors. Here, Q-learning algorithm was proposed for detecting the optimal links in the environment, however, it leads to high latency due to slow convergence that reduces the efficiency of the process. A local trust management system for detecting fake trust nodes using blockchain in VANET was introduced [23]. The proposed work includes the entities like RSU, primary server, vehicles, and blockchain. Initially, the trust values of the node were evaluated from the neighbor nodes and RSU which was updated in the primary server. Here, three types of trust were evaluated for a vehicle such as detection trust, reference trust, and transmission trust which are updated in the blockchain for enhancing security. Based on this trust value the fake trust nodes were detected in this research. Here, RSU evaluates the trust values of the vehicles which have a limited number of resources; hence it leads to high latency and overload due to a massive number of vehicles entered into the network.

Situation awareness with machine learning approach for misbehavior detection in VANET was proposed [24]. The main contribution of this research was situation aware misbehavior detection. In this work, reserachers have implemented their work using publicly available dataset and several types of ML models for performing accurate misbehavior detection. Furthermore, the trust management system was enabled for enhancing VANET security. An improved robust misbehavior detection scheme (iRMDS) scheme was proposed [25]. Here, the proposed scheme is replaced with statistics-based detection threshold. Initially, this research proposed Neuro-Kalman based robust misbehavior detection which consists of three phases. At first, the independent features were extracted from signal properties and combined with context information. Then, the Kalman filter was designed for extracting consistent patterns in context information for 9individual vehicle. At last, Artificial neural network (ANN) algorithm was combined with Kalman filter to detect the malicious pattern. Lightweight false BSM detection scheme (FBDS) was proposed [26]. The proposed work was leveraged by hyper-parameter tuning in ensemble random forest (Ens,RF) algorithm for accurate classification. Here, the hyper-parameter values were selected robustly that reduces

the classification error by utilizing randomized search cross-validation (RSCV) which ensures reliability and robust estimation. Based on fine-tuned parameter false BSM was detected using Ens.RF. An adaptive real-time malicious detection framework was proposed in VANET using ML [27]. Here, the real-time malicious node detection problem was resolved. Furthermore, the multi-layer classifier was proposed in distributed manner for malicious node detection by considering significant parameters where the random forest and gradient boosting based tree algorithm achieved high accuracy thereby enhancing security in VANET.

3. Problem Statement

A secure method for misbehavior detection in VANET was proposed [28]. This work includes three entities such as vehicles, local authority has the responsibility of collecting the trust values and feedback from the vehicles, and trusted authority (TA) has the responsibility of managing the reputation score of pseudonyms and certificates. This research considered pseudonyms and trust values during registration by TA, in which the trust values and feedback are encrypted and send and broadcast to prevent attackers. The major problems of this research were illustrated below,

- Here, all the information was stored in a trusted authority that leads to a single point of failure that reduces the throughput, in addition, it is not suitable for real-time application because the latency and complexity increases when the number of vehicles increased due to its limited computation capability.
- Here, a classical encryption mechanism was used for encrypting the feedback that leads to poor security due to sharing the encryption keys through unsecured connection that may misuse by the malicious third parties.

Blockchain based trust management for behavior analysis in VANET was introduced [29]. The proposed work includes three layers as VANET layer- vehicles were collected the information from RSU or other vehicles, edge-assisted blockchain layer- the duplication of RSU was stored in the blockchain to overcome a single point of failure issue, and certificate authority layer provided the secret key and certificates for RSU to ensure its security. Here, trust values were calculated by using hidden Markov model by considering history information. The crucial drawbacks of this research were described below,

- Here, vehicle trust values were evaluated based on historical information which was not enough to calculate optimal trust value that led to misclassification; hence it reduces accuracy of behavior analysis.
- Behavior analysis was done by certificate authority layer which leads to poor network management due to a lack of centralized controller that reduces scalability, flexibility and robustness.
- Here, only node centric misbehavior was detected by evaluating trust values, not concentrated on data centric misbehavior detection which is also important to detect misbehaviors in the network, because the attackers may inject or modify the information during broadcasting leads to poor security.

A trust management method for providing security to the SDN based VANET environment was proposed [30]. This research calculated two types of trust values such as subjective trust and role base trust. To enhance the accuracy of trustworthiness this research evaluates the similarity by verifying the trust value get from the RSU and neighbors using cosine similarity. In this way, this research identified the attacks in the environment. The major issues faced in this research are defined as,

- Here, only node centric misbehavior was detected by evaluating the trust values, however, it does not enough for optimal misbehavior detection, because the malicious users may change the information of the authenticated nodes that leads to poor security.
- Here, trust management was done by RSU which was not suitable for real time environment, because of its limited resources that lead to high latency and overhead during attack detection.
- All the transactions are stored in a centralized server without providing any security which leads to poor security because the attackers may compromise and misuse the information by hacking centralized server.

Author in [31], proposed a misbehavior detection system for detecting malicious nodes in VANET environment. Here, the fuzzy algorithm was used for detecting misbehavior by considering the context of the vehicles. It used enhanced Kalman filter for performed context acquisition from vehicles. After that, the contexts were shared between the vehicles using adaptive broadcasting rate strategy. Here, fuzzy algorithm was used to construct the context reference, and calculate the context score. Based on context score and reference information, classification was done by fuzzy classifier which classifies the vehicles as rogue or benign. The vital problems of this research are narrated as below,

- Here, fuzzy algorithm was used for evaluating the context reference and score, however, it generated predefined threshold value which leads to misdetection that increases high false alarm rate.

- Here, context references were collected by RSU which leads to high overload during large amount of context collection that increase high latency during node classification which reduces the efficiency of the work.
- In this research, context was collected from individual vehicles which leads to high energy consumption and latency which reduces the performance of misbehavior detection because of the resource constraint nature of VANET environment.
- Here, misbehavior detection was performed to increase security, however, it takes much more time for detecting the same misbehaviors entered in this research because performing again all the processes listed in this research leads to high complexity.

Research Solution: To encounter these issues, we have proposed deep learning based misbehaviour detection by utilizing blockchain. Initially, the vehicles legitimacy are ensured by quantum authentication using QKD, where the legitimate vehicles are authenticated by blockchain. Furthermore, to enhance security, the key is transmitted through quantum channel. Following that, we have executed dynamic clustering using LCKM (Leader Based k-means Clustering), to optimal centroid selection we have utilized LBO thus enhance communication. Here, we have also integrated SDN network for enhancing VANET efficiency. Moreover, the hybrid misbehaviour detection is executed to improve security. Data centric misbehaviour detection is implemented by trust estimation and behaviour classification utilizing MHA-LSTM At last, similarity base message verification for node centric misbehaviour detection is accomplished using fuzzy similarity.

4. Proposed Work

The main goal of this research is to detect misbehaviors in SDN based 5G-VANET environment using blockchain and other artificial intelligence methodologies. By performing misbehavior detection and revocation this research achieved high security, throughput, and less false alarm rate. Here, SDN is integrated to VANET environment for management of traffic control and resources which increase the flexibility of the network. Edge computing is integrated to reduce latency and energy efficient management. For communication, we have used 5G technology which increases high throughput and less transmission latency. The proposed work includes entities namely Global SDN controller (Cloud server), local SDN controller (Edge server), RSU, Vehicles, pedestrians, 5G Base station, and blockchain. Here, vehicle to everything (V2X) communication is performed in SDN based 5G-VANET. Fig 1 represents the overall architecture of proposed work. The major consecutive phases of this research are listed as follows,

- Quantum Authentication
- Dynamic Clustering
- Misbehavior Detection and Revocation

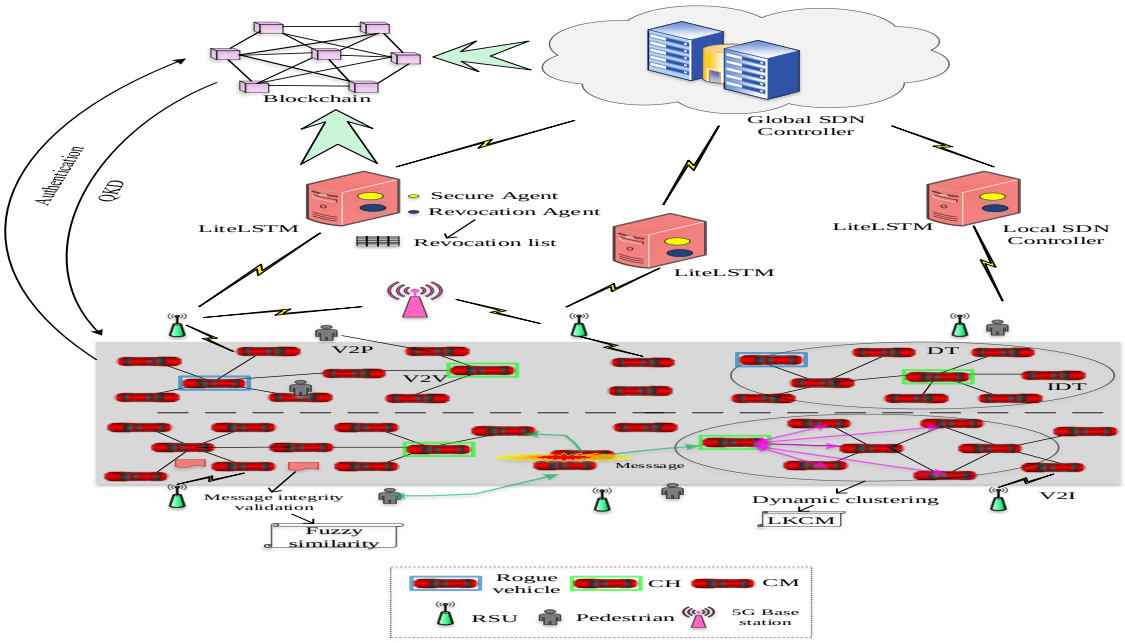

Fig.1 Overall Proposed Architecture of MHA-LSTM Model

4.1 Quantum Authentication

Initially, all the vehicles, pedestrians and RSU register their entities to the blockchain for ensuring legitimacy, in which the vehicle registers with their credentials as ID, password, location, and PUF values to the blockchain. RSU register their ID and location, and pedestrians register their ID and password. After completed registration, the blockchain generates a secret key for authentication using

Quantum Key Distribution (QKD). In this method, the secret keys are shared between known parties through a quantum channel rather than a classic channel that cannot hack by attackers.

Initially, to construct from quantum secure one-way function there are few steps where are following below for key generation,

Definition: A one-time signature (OTS) scheme is described as tuple $(EGen, Sign, Ver)$ including the polynomial time algorithm:

- $(vk, sk) \leftarrow EGen_k(1^\sigma)$: This is a polynomial time algorithm that, on given input 1^σwhich is security parameter, generates two bit strings of output vk and sk.
- $\beta \leftarrow Sign(sk, cre)$: An algorithm when given input as signing key sk and credentials cre , generates β as output signature.
- $\{0.1\} \leftarrow Ver(vk, cre, \beta)$: An algorithm when given input as verification key vk, return the bit defining accept or reject.
- *Generation:* $Gen_k(1^\sigma)$: At first, the two key pairs are generated:

$$(sk_0, vk_0) \leftarrow EGen_k(1^\sigma) \quad (1)$$

$$(sk_1, vk_1) \leftarrow EGen_k(1^\sigma) \quad (2)$$

- Determine,

$$\beta_0 \leftarrow Sign(sk_0, 0) \text{ and } \beta_1 \leftarrow Sign(sk_1, 1)$$

- Illustrating the state,

$$|\mathfrak{B}\rangle = \frac{|0,0,\beta_0\rangle + |1,1,\beta_1\rangle}{\sqrt{2}} \quad (3)$$

Where this state is effectively potential by assembling the key pair and the bits of signatures into the register of auxiliary, controlled on first qubit value. Then, measure the first qubit using Hadamard basis to acquire a bit $f_0 \in \{0,1\}$. Fix the quantum part in public key þ which is stated as unmeasured registers, then set the classical part of public key and the key of classical secret to,

$$pk = (vk_0, vk_1) \text{ and } sk = (\beta_0, \beta_1, f_0) \quad (4)$$

return,

$$(þ, pk, sk) \quad (5)$$

- *Encryption:* Enc$(þ, pk, cre)$

Here, project þ onto the subspace of acceptable signature of 0 and 1, below vk_0 and vk_1 respectively. Moreover, exactly, describe by $\sum_0 and \sum_1 the$ fix of validating signature on 0 and 1, below vk_0 and vk_1 respectively and consider the projector,

$$\prod = \sum_{\beta \in \sum_0,} |0, \beta\rangle \langle 0, \beta| + \sum_{\beta \in \sum_1,} |1, \beta\rangle\langle 1, \beta| \quad (6)$$

- Measure the state of residual in Hadamard basis, to acquire bit strings (f_1, f_2), where we defined by $f_1 \in \{0,1\}$ the first of measurement outcome and $f_2$are the remaining. Then, return as classical ciphertext,

$$c_t = (cre \oplus f_1, f_2) \quad (7)$$

- *Decryption:* $Dec(sk, c_t)$:
- Examine $c_t = (c_t 1, c_t 2)$, where $c_t 1 \in \{0,1\}$ is one bit and return,

$$cre = f_0 \oplus c_t 1 \oplus c_t 2 \cdot (\beta_0 \oplus \beta_1) \quad (8)$$

In this way, this proposed research provides better security to the participants. Additionally, we have overcome the position falsification attacks due to storing the position information of the vehicles, RSU, and pedestrians into the blockchain using QKD.

4.2 Dynamic Clustering

The authenticated vehicles are considered for clustering which reduces latency and energy consumption during communication. Here, clustering is done by RSU which acts as switch which maintains a OpenFlow of the network. Here, Leader based K-Means Clustering (LKCM) is proposed for performing dynamic clustering. For clustering, the proposed algorithm considered location, direction, RSSI, and distance. Fig 2 represents LCKM based clustering. The k-means initially selects the number of clusters $ƙ_n$ and the objective is to rearrange a set of vehicles υ with $1 \le j \le N$, into $ƙ_n$ clusters. For that, the k-means arbitrarily choose $ƙ_n$ points x_i with $1 \le i \le ƙ_n$ of vehicle in the vehicle set as centroids, where individual centroid belongs to cluster $\mathcal{C}$. After that, the algorithm allocates individual point in the environment to nearest centroid. This process is incorporated based on objective function, which evaluates the addition of entire squared distance in cluster where the evaluation is determined using objective function as follows,

$$avgmin_c = \sum_{i=1}^{ƙ_n} \sum_{x_j \in \mathcal{C}_i} d(x_j, \mathcal{u}_i) + avgmin_c \sum_{i=1}^{ƙ_n} \sum_{x_j \in \mathcal{C}_i} |x_j - \mathcal{u}_i|^2 \quad (9)$$

where $d(x_j, \mathcal{u}_i) = |x_j - \mathcal{u}_i|^2$ represents the distance among the point and cluster centroid. x_j denotes the position of point and $\mathcal{u}_i$ is the centroid position with $i = 1,2, \dots, ƙ_n$. The major challenge in K-Means s is initial cluster selection which increases poor local optimum due to selecting random centers. To overcome this issue, we proposed Leader-based Optimization algorithm (LBO) which selects the optimal cluster centroids rather than random selection which increases high convergence and low latency in clustering. Here, the vehicle populations are

identical to other population-based algorithms which can be mathematically modeled utilizing matrix as,

$$\upsilon = \begin{bmatrix} \upsilon_1 \\ \vdots \\ \upsilon_i \\ \vdots \\ \upsilon_N \end{bmatrix}_{N\times m} = \begin{bmatrix} \upsilon_{1,1} & \cdots & \upsilon_{1,j} & \cdots & \upsilon_{1,m} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ \upsilon_{i,1} & \cdots & \upsilon_{i,j} & \cdots & \upsilon_{i,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \upsilon_{N,1} & \cdots & \upsilon_{N,j} & \cdots & \upsilon_{N\times m} \end{bmatrix}_{N\times m} \quad (10)$$

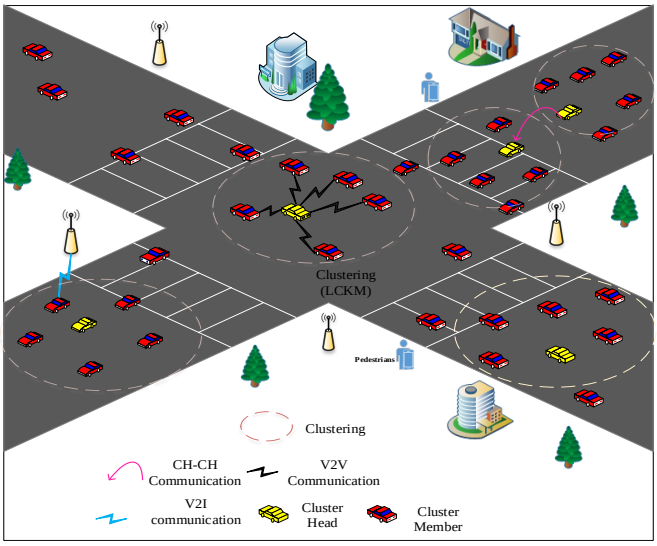

Fig.2 LCKM based Clustering

where υ_i is the ith candidate solution, $x_{i,j}$ is the value of j th variable computed by i th candidate solution, N represents the size of vehicle population and m is the number of problem variables. The position of individual member $\upsilon_i, i = 1,2,\dots,N,$

of the population υ is firstly initialized arbitrarily by contemplating the restraints of the problem variables entrenched on following equation,

$$x_{i,j} = \ell b_j + r \cdot (\mathcal{u}b_j - \ell b_j), j = 1,2,\dots,m \quad (11)$$

where r denotes the random number from interval $[0,1]$, ℓb_j and $\mathcal{u}b_j$ are the lower bound and upper bound of the jth problem variables. The objective function of problem is estimated based on individual candidate solutions calculated by vehicle members υ, that is specified in below equation by utilizing a vector as,

$$\mathbb{G} = \begin{bmatrix} \mathbb{G}_1 \\ \vdots \\ \mathbb{G}_i \\ \vdots \\ \mathbb{G}_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} \mathbb{G}(\upsilon_1) \\ \vdots \\ \mathbb{G}(\upsilon_i) \\ \vdots \\ \mathbb{G}(\upsilon_N) \end{bmatrix}_{N\times 1} \quad (12)$$

where $\mathbb{G}$ defines the vector of objective functions and $\mathbb{G}_i$ represents the delivered value of objective function from the i th candidate solution. LBO embrace of significant indicator in performance which is taken by updating and changing process of position in search space are known as exploration. The proposed optimization utilizes optimal centroid C_{op} leader to renovate the vehicle

Pseudocode : LCKM based Clustering

Input: υ

Determine optimal centroid

Output: vehicle clustered

Begin

Initialize k

For

Select number of clusters $\mathfrak{k}_n$

Generate objective function (9)

// Employ LBO for centroid selection

For

Initialize υ population (10)

Estimate $\mathbb{G}$ (12)

Generate candidate solution (13)

Estimate participate coefficient (14)-(16)

Select C_{op} (17)

Update new position (18)

End

Form $\mathfrak{k}_n$

End

members and C_{op} is generated for individual member of vehicle at every iteration. The C_{op} is selected based on the data points assigned to the cluster. Furthermore, the quality of individual member of vehicle in presenting the candidate solution can be determined as,

$$q_i = \frac{\mathbb{G}_i - \mathbb{G}_{worst}}{\sum_{j=1}^{N}(\mathbb{G}_j - \mathbb{G}_{worst})}, i \in \{1,2,\dots,N\} \quad (13)$$

where $\mathbb{G}_{worst}$ denotes the vehicle that accommodates repulsive value for objection function. Then, utilizing the aforementioned equation, the coefficient of participation for each vehicle are evaluated as three equations,

$$\wp C_i = \frac{q_i}{q_i + q_{best} + q_h} \quad (14)$$

$$\wp C_{best} = \frac{q_{best}}{q_i + q_{best} + q_h} \quad (15)$$

$$\wp C_h = \frac{q_h}{q_i + q_{best} + q_h} \quad (16)$$

where $i, h \in \{1,2,\dots,N\}, h \neq i$, q_i describes the quality of ith candidate solution, $\mathbb{G}_{worst}$ is the objective function value of repulsive candidate solution, $\wp C_i, \wp C_{best}, \wp C_h$ are the participation coefficients of ith vehicle the best member and the hth member respectively in generating C_{op}. Once the participation coefficients are

determined, the C_{op} is computed for each cluster of population as,

$$\mathsf{C}_{op,i} = \wp C_i \cdot v_i + \wp C_{best} \cdot v_{best} + \wp C_h \cdot v_h \quad (17)$$

where $\mathsf{C}_{op,i}$ is the optimal cluster centroid for the ith member and v_h represents the arbitrarily choosen vehicle member that index h is the row number to this member in the matrix of vehicle population. The new position for individual member of vehicle population in search phase across the C_{op} guidance is determined as,

$$x_{i,j}^{new,\wp 1} = \begin{cases} x_{i,j} + r \cdot \left(\mathsf{C}_{op_{i,j}} + I.x_{i,j}\right), & \mathbb{G}_{\mathsf{C}_{op,i}} < \mathbb{G}_i; \\ x_{i,j} + r \cdot \left(x_{i,j} - \mathsf{C}_{op_{i,j}}\right), & else \end{cases} \quad (18)$$

$$v_i = \begin{cases} v_i^{new,\wp 1}, & \mathbb{G}^{new,\wp 1} < \mathbb{G}_i \\ v_i, & else \end{cases} \quad (19)$$

where $v_i^{new,\wp 1}$ defines the new position of the ith member, $x_{i,j}^{new,\wp 1}$ illustrates its j th dimension, $\mathbb{G}^{new,\wp 1}$ defines the objective function value of LBO, Idenotes the integer that is choosen arbitrarily from the set $\{1,2\}$ and $\mathbb{G}_{\mathsf{C}_{op,i}}$ is the objective function value acquired from optimal centroid C_{op} of the i th member. After completing clustering, Cluster Head (CH) is selected by considering link stability, node degree, and distance. In this way, this research reduces energy consumption and latency during communication.

4.3 Hybrid Misbehavior Detection and Revocation

In V2X environment the vehicles and pedestrians broadcast the information to another vehicle or RSU. The message includes information about the event like road, accidents, traffic, speed limit and event location, event timestamp. The messages may send by vehicles, RSU and pedestrians in the environment. During message broadcasting, the attackers may hack and broadcast false messages that increase high traffic and other serious issues. To overcome these problems, we perform both node centric and data centric misbehavior detection. Here, misbehavior detection is performed in the edge server which incorporates with the local SDN server to perform network management. It includes two agents such as revocation agent and a secure agent, in which the revocation agent maintains the revocation list of the environment and the secure agent performs misbehavior detection. The revocation list is stored in the blockchain to increase security. The cloud server includes a global SDN controller which maintains and managed the local SDN controllers.

(a) Node centric misbehavior detection

The trust values of the vehicles are calculated to identify misdetection. Here, we have calculated both direct and indirect trust for the vehicles. Direct trust (D_{tru}) calculated based on history, packet delivery ratio, and throughput. Indirect trust (ID_{tru}) is calculated from neighbor vehicle and RSU by considering feedback, and success rate. Fig 3 denotes workflow of MHA-LSTM based misbehavior detection. Based on the direct and indirect trust, we perform misbehavior detection using Multi-head attention based LSTM (MHA-LSTM) which classifies the node into normal or rouge.

Here, the attention based LSTM was proposed to reduce the complexity. To capture the features effectively, we develop two-channel module for feature extraction. In the first channel, we utilized multi-level attention to extract the features based on direct and indirect trust. We can remark an attention mechanism phase as query mapping and pairs of key-value to output. A query attention function and key is employed to determine the weight of individual value, then the output is calculated as weighted sum of values. For multi-head attention, we utilize the trust estimation $Tru_E = \{D_{tru}, ID_{tru}\}$ to initialize the query $\mathcal{Q}$, value ύ and key Ƙ. Given query matrix $\mathcal{Q}$, ύ and Ƙ, the attention of scaled dot-product is estimated by the following equation,

$$Attention\ (\mathcal{Q}, \mathrm{K}, ύ) = softmax\left(\frac{\mathcal{Q}\mathrm{K}^T}{\sqrt{(\mathfrak{q}_k)}}\right) ύ \quad (20)$$

$$head_i = Attention\left(w_i^{\mathcal{Q}}\mathcal{Q}, w_i^{\mathrm{K}}\mathrm{K}, w_i^{ύ} ύ\right) \quad (21)$$

$$Z = w^m[head_1 \oplus \cdots \oplus head_r] \quad (22)$$

where $w_i^{\mathcal{Q}}$, w_i^{K}, $w_i^{ύ} \in \mathbb{R}^{\mathfrak{q}^k/r * \mathfrak{q}^k}$ represent the projection matrices, $w^m \in \mathbb{R}^{\mathfrak{q}^k * \mathfrak{q}^k}$ describes the mapping parameter from space of input to representation, r represents the number of attention heads, $\mathfrak{q}^k$ denotes the dimension of trust vectors and $\oplus$ is the connection operator. In second channel, we integrate recurrent neural networks of LSTM with attention mechanism. Here, the significant features are extracted for misbehavior detection. The LSTM embrace of two sub-networks for capturing left and right sequence context, which are known as forward and backward layer. We consider the trust estimation $Tru_E = \{D_{tru}, ID_{tru}\}$ as input, at time step $\mathfrak{t}$ the LSTM units are illustrated as follows,

$$i_{\mathfrak{t}} = \delta(w_i \mathfrak{w}_{\mathfrak{t}} + \varphi_i h_{\mathfrak{t}-1} + \mathfrak{b}_i) \quad (23)$$

$$\mathfrak{f}_{\mathfrak{t}} = \delta\left(w_{\mathfrak{f}} \mathfrak{w}_{\mathfrak{t}} + \varphi_{\mathfrak{f}} h_{\mathfrak{t}-1} + \mathfrak{b}_{\mathfrak{f}}\right) \quad (24)$$

$$\mathfrak{o}_{\mathfrak{t}} = \delta(w_{\mathfrak{o}} \mathfrak{w}_{\mathfrak{t}} + \varphi_{\mathfrak{o}} h_{\mathfrak{t}-1} + \mathfrak{b}_{\mathfrak{o}}) \quad (25)$$

$$\tilde{\mathfrak{c}}_{\mathfrak{t}} = tan\ h(w_{\mathfrak{c}} \mathfrak{w}_{\mathfrak{t}} + \varphi_{\mathfrak{c}} h_{\mathfrak{t}-1} + \mathfrak{b}_{\mathfrak{c}}) \quad (26)$$

$$\mathfrak{c}_{\mathfrak{t}} = \mathfrak{f}_{\mathfrak{t}} \odot \mathfrak{c}_{\mathfrak{t}-1} + i_{\mathfrak{t}} \odot \tilde{\mathfrak{c}}_{\mathfrak{t}} \quad (27)$$

$$h_{\mathfrak{t}} = \mathfrak{o}_{\mathfrak{t}} \odot tan\ h(\mathfrak{c}_{\mathfrak{t}}) \quad (28)$$

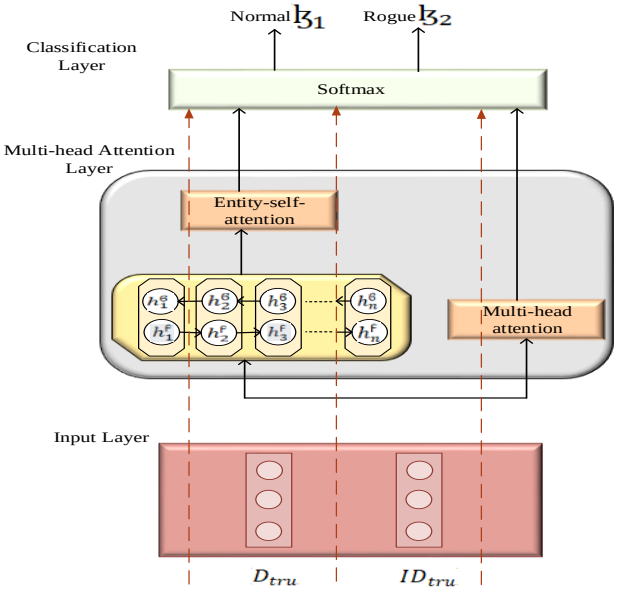

Fig.3 MHA-based Misbehavior detection

where i_t, f_t and O_t denotes the input gate, forget gate and output gate respectively, w_i, φ_i defines the weight matrix of i_t, the parameters w_f, φ_f are the weight matrix of f_t, the w_O, φ_O are the weight matrix of O_t. Furthermore, the parameters b_i, b_f and b_O denotes bias vectors of the input gate, forget gate and output gate. The w_c and φ_c refers to the weight matrix of recent memory content $\tilde{c}_t$. The h_t is the hidden state of LSTM, c_t is the state of current cell, $\odot$ defines the multiplication in element-wise and $\tan h$ is the function of hyperbolic tangent. At the time step t, the $i^t h$ trust is expressed as,

$$h_t = \left[\overrightarrow{h_t} \oplus \overleftarrow{h_t}\right] \quad (29)$$

where $\overrightarrow{h_t}, \overleftarrow{h_t} \in \mathbb{R}^{d^h}$ represents the hidden states of forward and backward LSTM in time step t. d^h denotes the hidden size of LSTM and $\oplus$ is the connection operator. Following that, we discrete vector of two entity h_t^{e1} and h_t^{e2} from LSTM output vector, which indicate he context information of tagged entity at time step t. Here, we incorporate attention layer after LSTM layer for solving dimension issues thereby capturing features effectively. In attention phase, we construct Q is the vector is the vector h_t^{e1} and h_t^{e2}, K, ύ is the LSTM output. To maintain the consistency of dimension, enlarge h_t^{e1} and h_t^{e2} to same dimension as LSTM. Then the attention of scaled dot-product is evaluated by the following equation,

$$Entity_c - Attention(Q, K, ύ) = softmax\left(\frac{QK^T}{\sqrt{(d_\ell)}}\right) ύ \quad (30)$$

$$Entity_c - head_i = Entity - Attention\left(w_i^Q Q, w_i^K K, w_i^{ύ} ύ\right) \quad (31)$$

$$ƀ_i = w^c\left[\left(Entity_c - head_1\right) \oplus \cdots \oplus \left(Entity_c - head_r\right)\right] \quad (32)$$

where $w^c \in \mathbb{R}^{d_\ell * r}$ refers to the mapping parameter from the space of input to representation, $d_\ell = 2 * d^h$ denotes the dimension of LSTM output, $ƀ_i$ is the entity i with the attention result of LSTM. BY utilizing attention mechanism, we obtain the output normal ($ƀ_1$) or rogue ($ƀ_2$).

Pseudocode : MHA-LSTM

Input: Tru_E
Output Normal or Rogue
Begin
Estimate Tru_E using D_{tru}, ID_{tru}
For
// MHA-LSTM
Initialize Tru_E
Estimate Attention Scaled dot-product (20)-(22)
Estimate i_t (23)
Estimate f_t (24)
Estimate O_t (25)
Determine h_t (28)
Determine $i^t h$ (29)
//Entity Attention
Evaluate Attention Scaled dot-product (30)-(32)
Classify $ƀ_1$ or $ƀ_2$
End

(b) Data Centric misbehavior detection

Data centric misbehavior is also one of the important processes in misbehavior detection, because the attackers act like a normal node and sends a false message to the environment. Hence, we need to verify the integrity and freshness of the message to avoid data centric misbehavior. Here, we calculate the similarity between the sender message (Sen_Ψ) and receiver message (Rec_Ψ)using fuzzy similarity which is a mismatch then the message is considered an illegitimate message. The steps are elaborated below for identifying similarity,

Step 1: To permit intra-user variability, for individual user, we generate: $m_{\Delta k} = mean\left(\mathcal{F}_{\Delta k}^{all}\right)$, $s_{\Delta k} = std_{dev}\left(\mathcal{F}_{\Delta k}^{all}\right)$,

Where $m_{\Delta k}$ and $s_{\Delta k}$ denotes the mean and standard deviation of feature vector k of user and receiver Δ, furthermore the values are determined by considering all the trained characteristics cha_Γ and features designed to Sen_Ψ and Rec_Ψ generated in training phase FS_j.

Step 2: Generate $\mathcal{F}_{\Delta k}^- = m_{\Delta k} - (Sen_\Psi) \times s_{\Delta k}$, $\mathcal{F}_{\Delta k}^+ = m_{\Delta k} + (Sen_\Psi) \times s_{\Delta k}$ denotes the valid limits of upper and lower. Likewise, entire feature vectors are demonstrated in interval-valued form. At last, $IVF_j = \left\{\left([\mathcal{F}_{\Delta k}^-, \mathcal{F}_{\Delta k}^+], m_{\Delta k}, s_{\Delta k}\right), FS_j\right\}$, where k alters from 1 to length (FS_j) are determined.

Step 3: To set the user particular receiving parameter, we formulate the following equation and the parameter (Sen_Ψ) is essential to fine-tuned.

$$\emptyset_j = mean\left(Fuzzy_{sim}\left(Rec_\Psi, IVF_j\right)\right) - Sen_\Psi \times std_{dev}\left(Fuzzy_{sim}\left(Rec_\Psi, IVF_j\right)\right) \quad (33)$$

where $Fuzzy_{sim}(cha_{\Gamma}, IVF_j)$ denotes the similarity among the vector of crisp values cha_{Γ} and interval valued vector IVF_j represented as,

$$Fuzzy_{sim}(cha_{\Gamma}, IVF_j) =$$
$$if\ T_{\Delta k} < \mathcal{F}^{-}_{\Delta k}\ or\ T_{\Delta k} < \mathcal{F}^{+}_{\Delta k} = \quad 0$$
$$if\ (m_{\Delta k} - \mathcal{T}_{\Delta k}) \le T_{\Delta k} \le (m_{\Delta k} + \mathcal{T}_{\Delta k}) = \quad 1 \quad (34)$$
$$if \mathcal{F}^{-}_{\Delta k} \le T_{\Delta k} < (m_{\Delta k} - \mathcal{T}_{\Delta k}) = (T_{\Delta k} - \mathcal{F}^{+}_{\Delta k}) \,/\, \left((m_{\Delta k} - \mathcal{T}_{\Delta k}) - \mathcal{F}^{-}_{\Delta k}\right) \quad (35)$$
$$if\ (m_{\Delta k} + \mathcal{T}_{\Delta k}) < T_{\Delta k} < \mathcal{F}^{+}_{\Delta k} = (\mathcal{F}^{+}_{\Delta k} - T_k\ ) \,/\, \left(\mathcal{F}^{+}_{\Delta k} - (m_{\Delta k} - \mathcal{T}_{\Delta k})\right) \quad (36)$$

where $1 <= t_r <= 10$. In each signature, k alters from $1 <= k <= len(FS_j)$, tr denotes the number of training samples. If the resultant value is higher than or equal to $\emptyset_j$then the message is categorized as normal. In this research, all the information's stored in the blockchain to increase security by performing both node centric and data centric misbehavior detection, this research achieved high security and QoS.

5. Experimental Results

This division deals with the experimentation of the proposed MHA-LSTM model to prove its efficacy in executing secure and reliable communication. This division is further sub-segment into three sub-sections which are illustrated as follows,

5.1 Simulation Setup

The simulation of the proposed MHA-LSTM model is illustrated in this sub-section. The Objective Modular Network tested in C++ (OMNeT++) for network simulation and Simulation of Urban Mobility (SUMO) for traffic simulation. The simulation tool can easily provide the specifications which are correlated to the proposed MHA-LSTM model. The simulation of the proposed MHA-LSTM model is implemented $2000 \times 2000m$ with an experimental area of about. Furthermore, the simulation is conducted using Intel Core i7-11370H processor with 8GB of RAM and Windows 10 pro 64 bits operating system is utilized. Table II describes the simulation parameters used for simulation of the proposed MHA-LSTM model.

Table II Network Parameters

Parameters	Value
Network Parameters	
No. of RSUs	6
No. of Local SDN Controller	3
No. of Global SDN Controller (cloud server)	1
No. of Vehicles	100
No. of Pedestrians	10
No. of 5G Base Station	1
Blockchain	1
Simulation Area	2000m×2000m
Simulation Time	100s
No. of Simulation Rounds	500
Mobility Model	TraCI model
Transmission Range	220-280m
Vehicle Speed	0-100 `km/hr
Packet Parameters	
Total Packets	7000 (approx..)
Type of Traffic	Traffic Control Interface
Packet Size	512 KB
Packet Interval	1s
Communication Parameters	
Model of Communication Model	Ray tracing attained model
Transmission Rate	240 Mbps
Communication Technology	5G
Channel Model	Path loss along with channel fading
MAC Protocol	CSMA/CA
Transport Protocol	TCP
Channel Bitrate	2Mbps
Channel Bandwidth	10MHz

5.2 Comparative analysis

The performance evaluation of the proposed MHA-LSTM model is accomplished in this sub-section by comparing the proposed MHA-LSTM model with various existing approaches which are HMM [29] and FUZZY [31] approaches respectively. Several parameters are contemplated for enumerating the proposed MHA-LSTM model ‘s performance include as average end to end delay, average packet loss ratio, packet delivery ratio, transmission overhead, throughput and accuracy respectively.

5.2.1 Analysis of Average End-to-End Delay

End-to-end delay (ETE_D) is the vital metric which is defined as average time held for the data to arrival the destination that can be expressed as,

$$ETE_D = \sum D_T^A - D_T^S \quad (37)$$

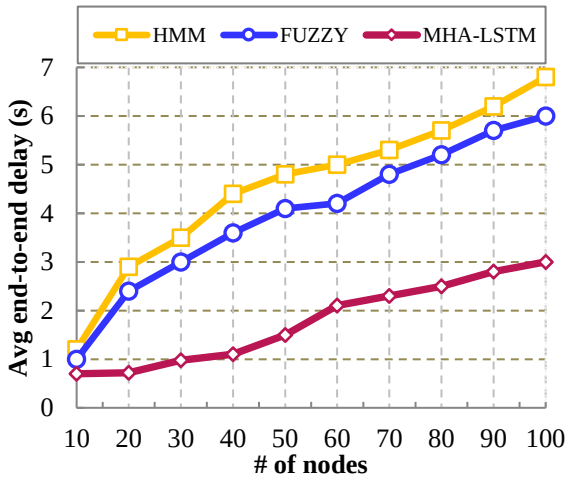

Fig.4 # of nodes vs End-to-End Delay

Where D_T^A represents the average time taken for data arrival, D_T^S represents the average time of data sent. Fig 4 shows that ETE_D comparison of existing works and proposed work in which, when the vehicles density is increases, the ETE_D also increases. Among that our proposed work attains low ETE_D where the main reason for low ETE_D in proposed work is due to performing dynamic clustering. Here, the LKCM algorithm is utilized for clustering and centroids are selected optimal using LBO algorithm. Furthermore, the significant parameters are considered for CH selection where the data of cluster member are collected and transmitted through CH thus reduces the end-to-end delay. Meanwhile, in existing works the delay is increased due to lack of clustering where the entire vehicle in the network communicates separately thus increases end-to-end delay. The numerical result shows that the proposed MHA-LSTM model achieves low end-to-end delay of 3s whereas the existing works faces high delay of 6ms-6.8s respectively.

5.2.2 Analysis of Average Packet Delivery Ratio

The amount of packet successfully transmitted to the receiver divides to the total number of packets transmitted without packet loss is known as packet delivery ratio (PDR^A) that can be expressed as,

$$PDR^A = \frac{Total_{ts}^p}{T_p} \times 100\% \quad (38)$$

Where $Total_{ts}^p$ denotes the average packet transmitted successfully from the total amount of packets, and T_p denotes the packet transmitted. Fig 5 portrays that PDR^A comparison of existing works and proposed work in which while the number of vehicles increases, PDR^A get decrease. Among that our proposed work attains high PDR^A due to the execution of misbehavior detection through trust estimation. In our work, the direct trust and indirect trust of the vehicles are calculated and classifies the vehicles entrenched on estimated trust values using MHA-LSTM clustering algorithm. However, in existing works the misbehavior detection was performed by secure agent which deployed local SDN controller that increases the robustness and more vulnerable to attacks. The numerical result illustrates that the proposed MHA-LSTM model achieves high PDR^A of 90% whereas the existing works reaches low PDR^A of 84%-75% respectively.

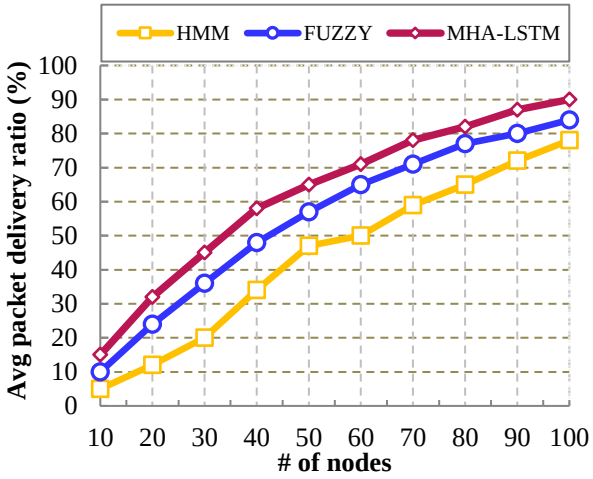

Fig.5 # of nodes vs PDR

5.2.3 Analysis of Average Packet Loss Rate

The amount of packets loss against the total number of packets while transmission is average packet loss ratio (PLR^A) that can be formulated as,

$$PLR^A = \frac{Total_{lost}^p}{T_p} \times 100\% \quad (39)$$

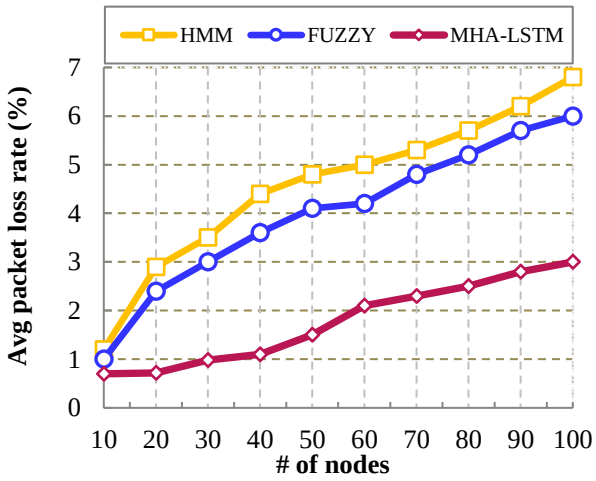

Fig.6 # of nodes vs packet loss ratio

Where $Total_{lost}^{p}$ defines the average packet get loss from total packets. Fig 6 illustrates that PDR^{A} comparison of existing works and proposed work in which while the number of vehicles increases, PLR^{A} also increased. Among that our proposed work reaches low PLR^{A} due to the utilization of imperative methods as data centric misbehavior detection. In data centric misbehavior detection the similarity based message verification is performed using fuzzy similarity where the sender and receiver message are verified to reduce false information distribution this result in low packet loss. Whereas in existing works faces high packet loss during message transmission that increases PLR^{A}. The numerical result demonstrates that the proposed MHA-LSTM model achieves low PLR^{A} of 3% whereas the existing works reaches high PLR^{A} of 6%-7% respectively.

5.2.4 Analysis of Transmission Overhead

Transmission overhead (Tm_O) is referred as the ratio of overhead packets while transmission to the transmitted that can be mathematically formulated as,

$$Tm_O = \frac{P_{ot}}{T_p} \qquad (40)$$

Where P_{ot} illustrates the overhead packets while transmission. Fig 7 shows that Tm_O comparison of existing works and proposed work in which while the number of vehicles increases, Tm_O also increased.

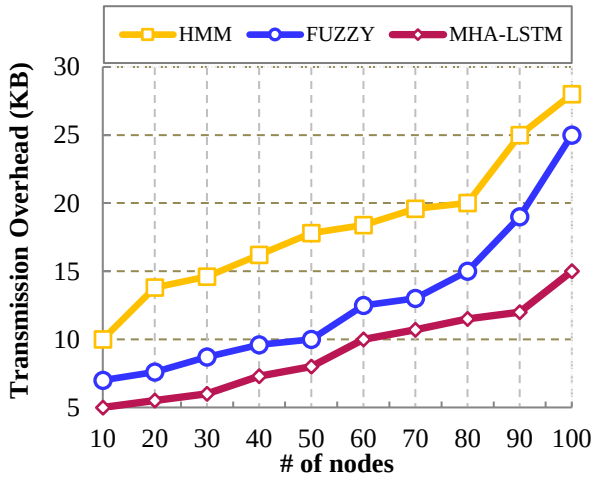

Fig.7 # of nodes vs transmission overhead

Among that our proposed work reaches low Tm_O due to the implementation of authentication. In our work, we have performed quantum cryptography based authentication to ensure the vehicle legitimacy and legitimate vehicles are only permitted into the VANET. Therefore, the malicious traffic in the network are reduced thus result in transmission overhead. Whereas, in existing works, due to lack of ensuring legitimacy the malicious traffic in the network is increased that result in high transmission overhead. The numerical result represents that the proposed MHA-LSTM model achieves low Tm_O of 15KB whereas the existing works reaches high Tm_O of 25KB-28KB respectively.

5.2.5 Analysis of Throughput

Throughput ($Tr_{\propto}$) is described as the amount of data packets are transmitted successfully across the afford period of time which can be expressed as,

$$Tr_{\propto} = \frac{\sum s_{p*} Avg_{ps}}{T} \times 100\% \qquad (41)$$

Where s_p denotes the successful packets, Avg_{ps} denotes the average size of the packet and T denotes the total time taken for packet transmission. Fig 8 shows that $Tr_{\propto}$ comparison of existing works and proposed work in which, when the simulation time is increases, the $Tr_{\propto}$ getting decreased. Among that our proposed work achieves high $Tr_{\propto}$ where the main reason for achieving high $Tr_{\propto}$ in proposed work is due to execution of dynamic clustering. In our work, the LKCM algorithm is used for clustering where the centroids are selected optimal using LBO algorithm to enhance the throughput and data transmission reliability. Moreover, the important parameters are contemplated for CH selection where CH collect the data of cluster member and transmitted through CH thus enhance $Tr_{\propto}$. Meanwhile, in existing works the high $Tr_{\propto}$is decreased due to lack of clustering that minimizes high $Tr_{\propto}$. The numerical result shows that the proposed MHA-LSTM model achieves high $Tr_{\propto}$ of 95% whereas the existing works achieves low $Tr_{\propto}$of 75%-70% respectively.

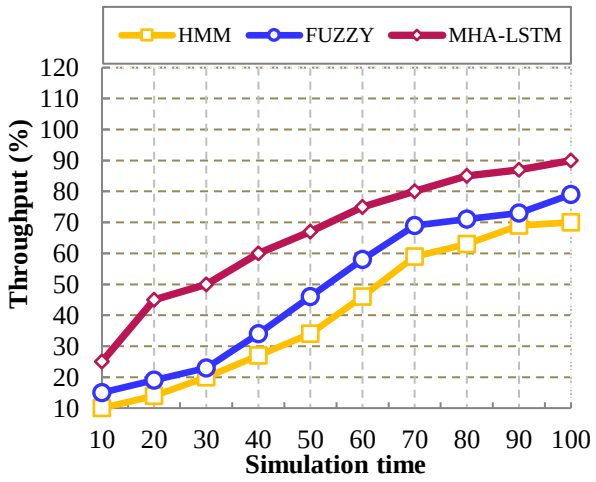

Fig.8 simulation time vs throughput

5.2.6 Analysis of Accuracy

Accuracy is one of vital metrics which is utilized for evaluate the accuracy of misbehavior detection. A VANET with high accuracy in misbehavior detection increases the security against the attacks. Accuracy $Acc_{\mathfrak{U}}$ is describes as the summation ration of true positive (T_p) and true negative (T_N) to the addition of true positive, true negative, false positive (F_p) and false negative (F_N) which can be mathematically formulated as,

$$Acc_{\mathfrak{U}} = \frac{T_p+T_N}{T_p+T_N+F_p+F_N}$$

(42)

Fig 9 illustrates that $Acc_{\mathfrak{U}}$ comparison of existing works and proposed work in which, when the number of malicious nodes is increases, the $Acc_{\mathfrak{U}}$ getting decreased. Among that our proposed work achieves high $Acc_{\mathfrak{U}}$ where the main reason for achieving high $Acc_{\mathfrak{U}}$in proposed work is due to proposing of hybrid misbehavior detection. In our proposed work, the node centric misbehavior detection is performed to detect the attacks in VANET through the estimation of nodes trust in direct and indirect manner. Based on the trust estimation score, the MHA-LSTM algorithm classifies the node as normal or rouge. Furthermore, the data centric misbehavior detection is implemented using fuzzy similarity where the attackers are identified through examining the message similarity among sender and receiver. As a consequence, usage of sufficient parameters and methods the misbehavior detection accuracy is improved. Meanwhile, in existing works either data centric or node centric misbehavior detection was accomplished with the consideration of inadequate parameters thus leads to low accuracy. The numerical result shows that the proposed MHA-LSTM model achieves high $Acc_{\mathfrak{U}}$ of 95% whereas the existing works faces low $Acc_{\mathfrak{U}}$ of 79%-70% respectively.

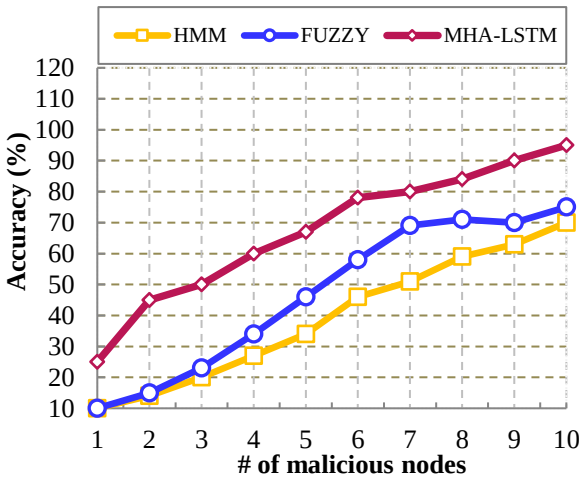

Fig.9 # of malicious nodes vs accuracy

Research Summary

This section illustrates the proposed MHA-LSTM model's overall performance. Table II denotes that our proposed work outperforms other existing works. These various performance metrics are attained efficiently in the proposed work by implementing multiple processes such as quantum authentication, dynamic clustering and hybrid misbehavior detection. The comparative analysis obtained from the aforementioned sub-phase proven that the proposed work outperforms other earlier works in terms of end-to-end delay, packet delivery ratio, packet loss ratio, transmission overhead, throughput and accuracy. The highlight of this research are illustrated below,

Table II Performs Analysis

Metrics	HMM	FUZZY	MHA-LSTM
End-to-end delay (ms)	4.58	4	1.77
Packet delivery ratio (%)	78	84	90
Packet loss rate (%)	6.8	6	3
Transmission Overhead (KB)	18.34	12.74	9.1
Throughput (%)	41.2	48.3	66.4
Accuracy (%)	39.4	48.7	67.4

- For providing security, we perform quantum authentication for vehicles, pedestrians, and RSUs using quantum key distribution methods which increase high security and perform against external and position falsification attacks.
- For reducing energy consumption and latency during messaging broadcasting, we perform dynamic clustering, in which the CH broadcast the information to the CMs that increase communication efficiency.
- For increasing the detection accuracy, we perform deep learning-based misbehavior detection which detects both node centric and data centric misbehaviors that leads to high throughput and attack detection rate.
- To increase scalability and management, we proposed a hierarchical SDN controller which leads to efficient network management, in addition, edge servers are deployed to reduce energy consumption and latency during communication.

6. Conclusion

In VANET environment, the security issues are the still remains the major concern. To encounter this issue, we have proposed deep learning based misbehaviour detection using blockchain. Initially, the vehicle legitimacy are ensured by quantum authentication using QKD, where the legitimate vehicles are authenticated by blockchain. After that, we have performed dynamic clustering using LCKM, to optimal centroid selection we have employed LBO thus enhance communication. Here, we have also integrated SDN network for enhancing VANET efficiency. Furthermore, the hybrid misbehaviour detection is executed to improve security. Data centric misbehaviour detection is implemented by trust estimation and behaviour classification utilizing MHA-LSTM At last, similarity base message verification for node centric misbehaviour detection is accomplished using fuzzy similarity. By this way the VANET security is enhanced in our work. The proposed work outperforms other existing works in terms of end-to-end delay, packet delivery ratio, packet loss ratio, transmission overhead, throughput and accuracy.

References

[1] Lee, M., & Atkison, T. (2020). VANET applications: Past, present, and future. *Veh. Commun., 28*, 100310.

[2] Jabbar, R., Fetais, N., Kharbeche, M., Krichen, M., Barkaoui, K., & Shinoy, M. (2021). Blockchain for the Internet of Vehicles: How to Use Blockchain to Secure Vehicle-to-Everything (V2X) Communication and Payment? *IEEE Sensors Journal, 21*, 15807-15823.

[3] Tagliaferri, D., Brambilla, M., Nicoli, M., & Spagnolini, U. (2021). Sensor-Aided Beamwidth and Power Control for Next Generation Vehicular Communications. *IEEE Access, 9*, 56301-56317.

[4] Junejo, M.H., Rahman, A., Shaikh, R.A., & Yusof, K.M. (2021). Location Closeness Model for VANETs with Integration of 5G. *Procedia Computer Science, 182*, 71-79.

[5] Weber, J.S., Neves, M.C., & Ferreto, T.C. (2021). VANET simulators: an updated review. *Journal of the Brazilian Computer Society, 27*, 1-31.

[6] Sharma, P.K., & Jain, S. (2020). Review of VANET Challenges and Protocol for Architecture Design and Intelligent Traffic System. *2nd International Conference on Data, Engineering and Applications (IDEA)*, 1-4.

[7] Liu, L., Chen, C., Pei, Q., Maharjan, S., & Zhang, Y. (2019). Vehicular Edge Computing and Networking: A Survey. *Mobile Networks and Applications, 26*, 1145 - 1168.

[8] Zhang, D., Yu, F.R., & Yang, R. (2022). Blockchain-Based Multi-Access Edge Computing for Future Vehicular Networks: A Deep Compressed Neural Network Approach. *IEEE Transactions on Intelligent Transportation Systems, 23*, 12161-12175.

[9] Islam, M.M., Khan, M.T., Saad, M.M., & Kim, D. (2020). Software-defined vehicular network (SDVN): A survey on architecture and routing. *J. Syst. Archit., 114*, 101961.

[10] Alaya, B., & Sellami, L. (2023). Toward the Design of an Efficient and Secure System Based on the Software-Defined Network Paradigm for Vehicular Networks. *IEEE Access, 11*, 43333-43348.

[11] Perera, M.N., Nakamura, T., Hashimoto, M., Yokoyama, H., Cheng, C., & Sakurai, K. (2022). Certificate Management Scheme for VANETs Using Blockchain Structure. *Cryptogr., 6*, 20.

[12] Nayak, R.P., Sethi, S., Bhoi, S.K., Sahoo, K.S., Jhanjhi, N.Z., Tabbakh, T., & Almusaylim, Z.A. (2021). TBDDoSA-MD: Trust-Based DDoS Misbehave Detection Approach in Software-defined Vehicular Network (SDVN). *Computers, Materials & Continua*.

[13] Sangwan, A., Sangwan, A., & Singh, R. (2022). A Classification of Misbehavior Detection Schemes for VANETs: A Survey. *Wireless Personal Communications, 129*, 285-322.

[14] Peng, L., Feng, W., Yan, Z., Yan, Z., Li, Y., Zhou, X., & Shimizu, S. (2020). Privacy preservation in permissionless blockchain: A survey. *Digit. Commun. Networks, 7*, 295-307.

[15] Alharthi, A., Ni, Q., & Jiang, R.M. (2021). A Privacy-Preservation Framework Based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET. *IEEE Access, 9*, 87299-87309.

[16] Ercan, S., Ayaida, M., & Messai, N. (2022). Misbehavior Detection for Position Falsification Attacks in VANETs Using Machine Learning. *IEEE Access, 10*, 1893-1904.

[17] Alladi, T., Kohli, V., Chamola, V., & Yu, F. (2022). A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems. *Digital Communications and Networks*.

[18] Gyawali, S., Qian, Y., & Hu, R.Q. (2020). Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks. *IEEE Transactions on Vehicular Technology, 69*, 8871-8885.

[19] A. Ghaleb, F., Saeed, F., Al-Sarem, M., Ali Saleh Al-rimy, B., Boulila, W., Eljialy, A.E., Aloufi, K.S., &

Alazab, M. (2020). Misbehavior-Aware On-Demand Collaborative Intrusion Detection System Using Distributed Ensemble Learning for VANET. *Electronics*.

[20] Sharma, A., & Jaekel, A. (2022). Machine Learning Based Misbehaviour Detection in VANET Using Consecutive BSM Approach. *IEEE Open Journal of Vehicular Technology, 3*, 1-14.

[21] Sharma, P., & Liu, H. (2021). A Machine-Learning-Based Data-Centric Misbehavior Detection Model for Internet of Vehicles. *IEEE Internet of Things Journal, 8*, 4991-4999.

[22] Zhang, D., Yu, F.R., Yang, R., & Zhu, L. (2022). Software-Defined Vehicular Networks With Trust Management: A Deep Reinforcement Learning Approach. *IEEE Transactions on Intelligent Transportation Systems, 23*, 1400-1414.

[23] Li, F., Guo, Z., Zhang, C., Li, W., & Wang, Y. (2021). ATM: An Active-Detection Trust Mechanism for VANETs Based on Blockchain. *IEEE Transactions on Vehicular Technology, 70*, 4011-4021.

[24] Abdelmaguid, M.A., Hassanein, H.S., & Zulkernine, M. (2022). SAMM: Situation Awareness with Machine Learning for Misbehavior Detection in VANET. *Proceedings of the 17th International Conference on Availability, Reliability and Security*.

[25] Alzahrani, M., Idris, M.Y., Ghaleb, F.A., & Budiarto, R. (2022). An Improved Robust Misbehavior Detection Scheme for Vehicular Ad Hoc Network. *IEEE Access, 10*, 111241-111253.

[26] Anyanwu, G.O., Nwakanma, C.I., Lee, J.M., & Kim, D. (2022). Novel hyper-tuned ensemble Random Forest algorithm for the detection of false basic safety messages in Internet of Vehicles. *ICT Express, 9*, 122-129.

[27] Rashid, K., Saeed, Y., Ali, A., Jamil, F., Alkanhel, R., & Muthanna, A. (2023). An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs). *Sensors (Basel, Switzerland), 23*.

[28] Gyawali, S., Qian, Y., & Hu, R.Q. (2021). A Privacy-Preserving Misbehavior Detection System in Vehicular Communication Networks. *IEEE Transactions on Vehicular Technology, 70*, 6147-6158.

[29] Liu, H., Han, D., & Li, D. (2021). Behavior analysis and blockchain based trust management in VANETs. *J. Parallel Distributed Comput., 151*, 61-69.

[30] Mao, M., Yi, P., Hu, T., Zhang, Z., Lu, X., & Lei, J. (2021). Hierarchical Hybrid Trust Management Scheme in SDN-Enabled VANETs. *Mob. Inf. Syst., 2021*, 7611619:1-7611619:16.

[31] Ghaleb, F.A., Saeed, F., Alkhammash, E.H., Alghamdi, N.S., & Al-rimy, B.A. (2022). A Fuzzy-Based Context-Aware Misbehavior Detecting Scheme for Detecting Rogue Nodes in Vehicular Ad Hoc Network. *Sensors (Basel, Switzerland), 22*.