Improving The Security Of Data Communication in Vanets Using ASCII-ECC Algorithm

Sajini S (sajinisham13@gmail.com)
SRMIST: SRM Institute of Science and Technology https://orcid.org/0000-0002-5914-6405
Mary Anita E.A
Christ University
J Janet
Sri Krishna College of Engineering and Technology

Research Article

Keywords: Vehicular Ad-hoc Network (VANET), Trusted Authority (TA), Authentication, Cluster Head (CH), On-Board Unit (OBU), Road Side Units (RSUs), Median based K-Means (MKM), Modified Cockroach Swarm Optimization (MCSO), and American Standard Code for Information Interchange based Elliptic Curve Cryptography (ASCII-ECC).

Posted Date: June 29th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-597331/v1

IMPROVING THE SECURITY OF DATA COMMUNICATION IN VANETS USING ASCII-ECC ALGORITHM

S. Sajini [1], E. A Mary Anita [2], J. Janet [3]

[1] Research Scholar, Anna University, Chennai & Assistant Professor, SRM Institute of Science and Technology, Ramapuram

[2] Professor, Department of Computer Science and Engineering, School of Engineering and Technology, Christ University, Bengaluru

[3] Professor, Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore

*Corresponding author E-mail: sajinisham13@gmail.com

Abstract: Now-a-days, with the augmenting accident statistics, Vehicular Ad-hoc Networks (VANET) are turning out to be more popular, which in-turn eradicates accidents in addition to damage to the vehicles together with populace. In a VANET, message can well be transmitted within a pre-stated region to attain safety of a system and also its efficacy. Next, it is challenge to ensure authenticity of messages in such a dynamic environment. Though some researchers have already worked on this, security has not been much focussed. Thus, secured data communication with enhanced security on the VANET environment utilizing the American Standard Code for Information Interchange centred Elliptic Curve Cryptography (ASCII-ECC) is proposed. The proposed scheme allows all vehicles to register with the Trusted Authority (TA) and uses Median-centred K-Means (MKM) to find out the cluster head among all cluster and at the last phase verification is done by TA. The

performance of the proposed algorithm ASCII-ECC is analysed and proved that the system renders better performance when it is weighed against the top-notch methods.

Key words: *Vehicular Ad-hoc Network (VANET), Trusted Authority (TA), Authentication, Cluster Head (CH), On-Board Unit (OBU), Road Side Units (RSUs), Median based K-Means (MKM), Modified Cockroach Swarm Optimization (MCSO), and American Standard Code for Information Interchange based Elliptic Curve Cryptography (ASCII-ECC).*

1. INTRODUCTION

The requirement for intelligent mobility augments with the instigation of the smart city. A smart city's major features are Traffic flow monitoring together with congestion management. An augmentation in the total incidents of traffic congestion along with incompetent wireless communication system aimed at traffic management brings about the Intelligent Transportation Systems (ITS) concept [1]. Lately, there are huge developments in the Information and Communication Technology (ICT), for instance mobile communications. Because of which, the modern lifestyle has significantly changed (i.e.) the people can exchange their data anytime as well as anywhere (even in moving vehicles). Cellular networks, say 3G and 4G, are also responsible for exchanging data in vehicles. VANET can implement the ITS's primary objective like road safety, traffic congestion control, together with effective infrastructure usage [2].

VANET generates an intelligent space aimed at vehicular communications. It is identified as a considerable constituent of the ITS. They can well be utilized for an extensive extent of secure and also non-secure applications, allowing esteem encompassing administrations, say programmed toll accumulation, vehicle well-being, enhanced route, traffic executives along with area-centred administrations, say finding the nearest restaurant, cornerstone, or traveling

spot together with entertainment applications [3]. It depends upon smart vehicles for network functionality since it doesn't encompass any fixed infrastructure. Each moving vehicle are deemed as the nodes. VANET utilizes every moving vehicle as the wireless router to establish a mobile network [4]. Infrastructure centered communication (Vehicle to Infrastructure (V2I)) and direct communication between vehicles (Vehicle to Vehicle (V2V)) are the prime communication types wherein the broad gamut of applications can well be enabled [5, 6].

Dynamic connectivity along with self-organizing is some features of VANET's nodes. Nevertheless, topology changes often regarding the vehicles' intense higher mobility [7], which in-turn lessens the network lifespan as well as augments the routing overhead. Clustering is basically the commonest solution adopted for this issue. In VANET, centered upon some rules or criterion or some common aspects, the vehicles are organized, this is called Clustering [8]. Data Transmission (DT) protocols were developed for rendering confidentiality together with integrity safety to the data transmitted for ensuring the communications' security betwixt the Road-Side Unit (RSU) and vehicle [9]. For the DT protocol, computational cost is another core issue. The vehicle together with the RSU is deeply troubled with the tremendously high computation cost as of running cryptographic algorithms owing to the traffic's higher speed together with short communication gamut [10].

Subsequent to Vehicle Safety Communication (VSC), huge prominence has been offered to the privacy together with security on VANET. For a safer and also comfortable driving experience, the pseudonym certificates' conception was rendered to the vehicles that effectively safeguard communication inside the network [11]. The safety together with non-safety services was included in these. In reality, there are numerous services, say the surveillance [12] together with route planning services [13]. Yet, several challenges still

present for the VANET's management and it's deployment in the instance of secured DC [14]. To secure communications between connected vehicles, Artificial Intelligence (AI) techniques, like [15], [16], [17], [18], are needed. The AI continuously utilizes the experience that it got in the augmentation of its cognitive capability concerning environment and also making the instant good decisions [19, 20]. Because of VANET's higher mobility along with vulnerability of attacks, it is tough to communicate securely. Sybil, Black hole, wormhole attack, etc., are a few attacks that affect the VANET. It also encompasses several flaws, which are exhibited below,

- The prevailing research methods couldn't detect some collection of malevolent activities or avert them as of such activities.
- The Key Management Centres (KMC) centred VANET communication was regarded in the prevailing research works. The complete scheme was no longer effectual if the KMC was compromised.
- Centred on location together with velocity, most clustering-centred system chooses the Cluster Head (CH). This is not an optimal choice, since, in accordance with the relative speed with the remaining vehicles prevalent on the network, the chosen vehicle's location might quickly change.
- One or two metrics centred cluster formation is managed in the top-notch works that was not an optimal choice.

The work proposed a secured Data Communication(DC) in VANET utilizing ASCII-ECC to trounce the prevailing challenges.

This paper's organizational structure is: Section 2 renders the associated works of DC via VANET. Section 3 renders with the work proposed, and section 4 exhibits the results and discussion for performance analysis. Finally, section 4 concludes the paper.

2. RELATED WORKS

Canhuang Dai et.al [21] recommended an indirect reciprocity security method with a scalar reputation allocated to every OBU. This methodology was employed to examine their hazardous level towards the VANET. Consensus techniques and encryption procedures that had been employed to prevent information from being damaged were utilized for the sender to record other OBU's activities by a block chain technique. Additionally, to select OBU with a reliable relay or decide whether to follow the source OBU's request or not, a reinforcement learning (RL) technique centred on action selection for an OBU was created by them. The learning speed was increased by employing a hot boot mechanism that was deployed aimed at the OBU with prior knowledge. The packet delivery ratio (PDR), the reputation, and every OBU's usage were augmented effectively using action selection methodology only via the in-built prior knowledge which was displayed in the results.

SowmyaKudva et.al [22] formulated the Proof of Driving (PoD) method to randomize honest miners' selection for producing the blocks effectively for blockchain-centred VANET applications. Also, grounded on the vehicular nodes' Service Standard Score, a filtering method was deployed to discover and remove the malicious nodes. This technique has formed consensus adaptability in a vast public vehicular network and honest miners' selection in a blockchain-centred VANET application. Additionally, the fairness and efficacy problems created via PoW and PoS were described by this technique. To remove the malicious vehicle nodes as of partaking in consensus, this method attained lesser consensus sets with higher quality and as well, it was effective and scalable, which was revealed as of

the outcomes. Participation of numerous nodes on the communication wasn't pondered by this method.

Ayan Roy and Sanjay Madria [23] offered distributed incentive-centred trust management system comprising a secured event detection design. This design utilized the Byzantine fault-tolerant Paxos technique and game theory. Unlike the top-notch methods, the broadcast information's accuracy can be verified via this model when the malicious vehicles from the majority than the non-malicious vehicles within the ROI. By completely addressing all possible use-case scenes and under the minimum non-malicious vehicle's impact at each RSU, the system's feasibility and also its efficacy were verified utilizing the VENTOS, SUMO, and Omnet++ simulators. In this instance, a problem was created by the DC betwixt the multiple nodes management.

Jitendra Bhatia et.al [24] recommended a design that applied the SDN technology by combining Network Coding with Multi-Generation-Mixing (MGM) functionalities. It augmented the reliability as well as security of DT in vehicular networks. Aimed at data encoding and decoding, a network coding protocol centred on MGM was formulated. Also, the vehicles' authentication was offered by a centralized SDN controller. At last, depending upon realistic traffic along with communication characteristics, they constructed a simulation model. Concerning the security and also reliability, the simulation outcomes exhibited that the SDN technique- supported protocol performed efficiently whilst analogized with the traditional network coding-centred protocol. It doesn't withstand any attack type as of the malevolent nodes.

ParulTyagi, and Deepak Dembla [25] presented a protocol to discover malicious nodes, obstruct black hole attacks, and yielded secure DT in VANET, called secured AODV routing technique. The algorithm was centred on the asymmetric public key infrastructure utilizing

the Elliptic Curve Cryptographic (ECC). Key generation was performed by ECC. The vehicle was validated by the Certification authority (CA). Aimed at storing routing information, a specific data structure (heap) was utilized by every vehicle. However, road safety was enhanced by offering secured and also timely information regarding road traffic circumstances; those traffic-related messages were authenticated. Attack resistance and malevolent node removal methods weren't rendered by this technique.

J.Jenefa and E.A Mary Anita presented[26] a proxy vehicle based message authentication scheme (ID-MAP) to decrease the overheads of the Road Side Unit by validating more than one messages at the same time. Even though it deals with the efficiency issues of RSU, the computational cost of signature generation is high. Since the ability of a vehicle to act as a proxy vehicle is based on the number of signed messages, it has a major impact. It also cannot guarantee privacy preservation and hence it is insecure against attacks based on privacy preservation.

3. PROPOSED METHODOLOGY

In the ITS, vehicular networks are evolving as a noticeable research field owing to the nature and characteristics of offering high-level road safety and also enhanced traffic management. Vehicles are furnished with heavy communication tools that require a high power supply, on-board computing device, and also data storage devices. It makes privacy and security as the serious challenging problems in VANET. This information's misuse can cause traffic accidents and human lives loss at worse scenarios; hence, vehicle authentication is the essential necessity. This work proposed boosts the DC's security within the VANET environment utilizing the ASCII-ECC technique. The methodology comprises network design, registration stage, cluster formation and CHS, verification, SP selection, and then secured DC phases. The system proposed utilized the MKM clustering technique aimed at

constructing the cluster and choose the CH effectively. The system utilizes the MCSO technique aimed at optimally choosing the SP, and it utilizes the ASCII-ECC technique aimed at securing DT. In the subsections below, these are detailed briefly. Figure 1 exhibits the DC's enhanced security in the VANET environment.

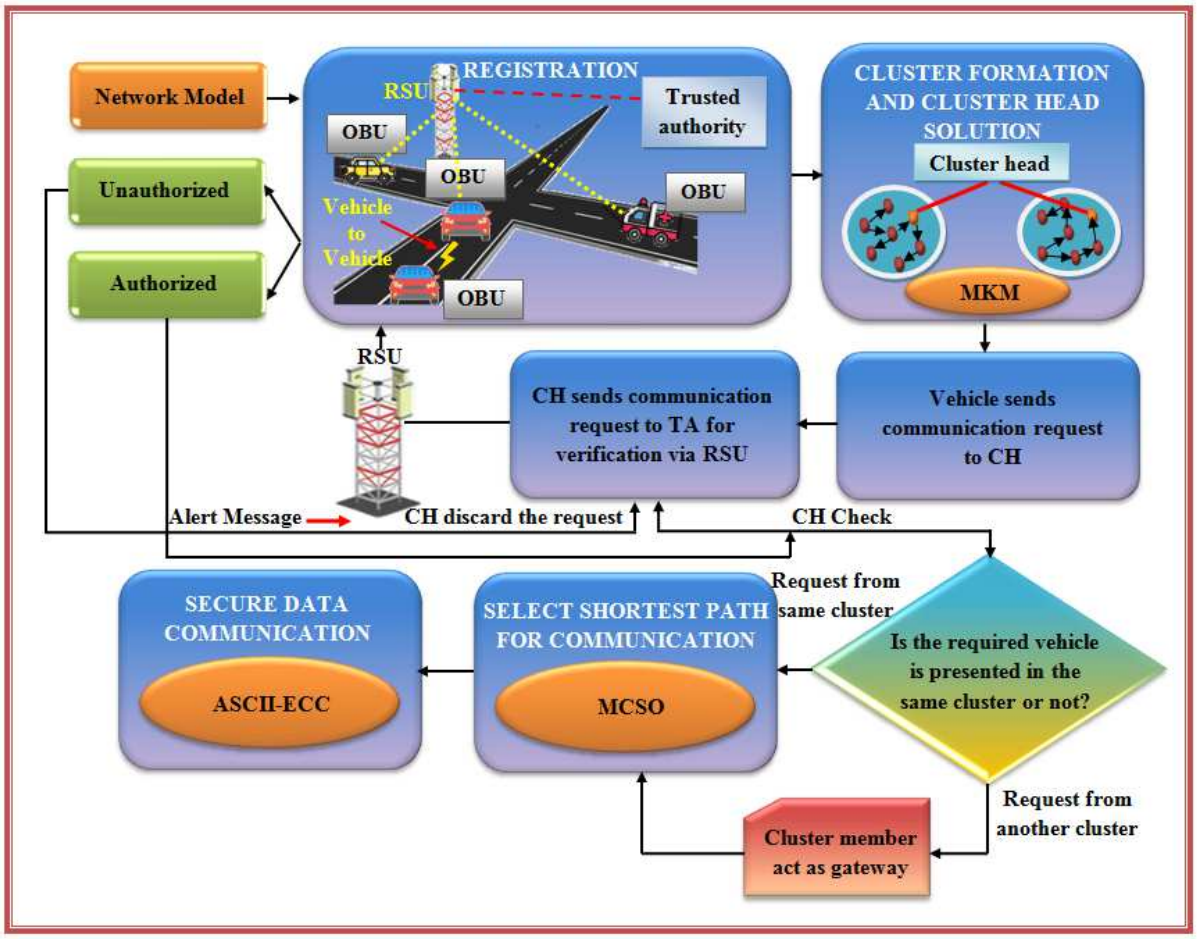

Figure 1: Architecture diagram of the system model

3.1 Network Model

Here, a VANET network possessing a huge number of vehicles or else nodes is employed in a random and uniform manner. A VANET is pondered by a set of 'a' Sensor Nodes (SN) that are arithmetically equated as:

$$(AV)_n = \{av_1, av_2, av_3, \ldots\ldots\ldots\ldots\ldots av_n\} \quad (1)$$

Herein, $(AV)_n$ implies the VANET; av_n signifies the n-number of nodes.

3.2 Registration Phase

Here, all vehicles are registered into the TA utilizing a unique vehicle ID. The TA is a trusted central data centre, which saves vehicles' real identities and information. TA produces a private key aimed at every vehicle utilizing the subsequent eqn. (2),

$$BP_{key}^{"} = \mathrm{H}\left(ID_{EV} \parallel RN_{EV}\right) \quad (2)$$

Herein, $BP_{key}^{"}$ signifies the private key aimed at the registered vehicle; $H(.)$ implies the secured hash function; ID_{EV} implies the ID aimed at the registered vehicle; RN_{EV} symbolizes the random number created by the TA. Simultaneously, all the vehicle users are registered in their OBU. The OBU is fitted in every vehicle, and it collects the data sensed as of the vehicles. Hence, it is accountable aimed at the data's acquisition and collection as of the diverse sensors furnished inside the vehicle.

3.3 Cluster Formation and Cluster Head Selection

After the network design's defining, the cluster's formation and CHS procedure is executed. Initially, the cluster formation is executed by the MKM clustering technique. Herein, the 1st SNs are grouped, and then, CH is elected as of the cluster group. The CH is elected centred on the vehicle's location, speed, velocity, and equipment. The normal K-Means technique is amidst the techniques, which resolve the eminent clustering issue. The technique categorizes the objects as a pre-defined number of clusters that is offered by the user (ponder k clusters).

This methodology targets to decrement an objective function that is in this circumstance a squared error function. Nevertheless, it yet comprises a few issues (i.e.) it is responsive to the primarily chosen points, and hence it doesn't constantly generate the identical output. Moreover, this process doesn't promise to discover the global optimum, even though it always terminates. The system proposed employs the median value aimed at decrementing the randomness effect. Hence, the term is named the MKM technique.

Initialize the clusters initially, and then centred on the cluster count, the cluster centroid is chosen. Select the 1st centre randomly aimed at the cluster centroid selection. The 2nd centre is chosen greedily as the point farthest as of the 1st. Every remaining centre is defined by employing the median value. All chosen centroid points are signified as,

$$\left(\left(CP\right)_i = \left(cp_1, cp_2, cp_3, \ldots\ldots\ldots cp_n\right)\right) \in \left(AV\right)_n \tag{3}$$

Herein, $\left(CP\right)_i$ signifies the centroids set; cp_n implies the n-number of chosen centroids; $i = 1,2,\ldots..,n$. After the cluster centroid's selection, the distance is computed betwixt the cluster centroids and nodes (vehicles) utilizing the Euclidean distance that is equated as,

$$Dist_i = \sqrt{\sum_{i=1}^{n} \left(\left(CP\right)_i - \left(AV\right)_n\right)^2} \tag{4}$$

Centred on the eqn. above, the similarity is enumerated betwixt all nodes prevalent within the network design and the centroids values selected. If it is chosen, then leave it; or else, continue the distance calculation (i.e.), Scan the listing of not-yet-chosen points aimed at locating the not grouped node, which comprises the maximal distance as of the points selected. Next, eliminate a point as of the not-yet-chosen points and add it to the end of the selected points' sequence. After clusters' creation, the CH is elected centred on a few factors,

namely the vehicles' location, speed, velocity, and also equipment, that is enumerated utilizing the subsequent eqn. (5),

$$Fact_{veh} = \sum \left(L_{veh}, S_{veh}, V_{veh}, E_{veh} \right) \tag{5}$$

Herein, L_{veh} implies the vehicle's location; S_{veh} symbolizes the vehicle's speed; V_{veh} implies the vehicle's velocity; E_{veh} signifies the vehicle's equipment. The system sets a threshold value. In the cluster node, the node that attains the threshold value centred on the eqn. (5) is elected as the CH.

3.4 Verification Process

The communication request is sent by the vehicle to the CH in this verification phase. Next, through RSUs, the CH forwards the communication request to the TA for verification (i.e., simply named the intermediate authentication process which falls under the token centered authentication scheme herein, the token is provided for every SN, the token means ID number of SN centered upon the ID number, the verification process is performed in the TA). All the information is stored by the RSU stores. RSU is positioned on the road's sides or in particular places, like parking places, road curves, etc. It contains an antenna, processor, sensors, along with a transceiver. The services like road intersections are offered by these units on the road's sides to the vehicles. For controlling the traffic in that particular intersection and reducing accidents, road intersection is used.

The TA checks if the vehicle is an authorized (or) unauthorized vehicle after the request is sent by the CH to the TA. If the vehicle is an authorized one, then the CH checks whether the requested vehicle is existing in the same cluster group or not (i.e., the checking process is conducted by the threshold value, the threshold value is allotted centered upon the

SN's distance for each cluster that the distance threshold value is set). After that, the SP is selected and the information is securely transmitted. The alert message is sent by the TA to the CH via RSU if the vehicle is unauthorized, then the CH rejects the request. These are briefly explained in the subsequent section.

3.5 Select Shortest path

The SP is computed for DC if the requested vehicle is an authorized vehicle that is verified by the CH through RSU in this phase. Herein, utilizing the MCSO algorithm, the SP is calculated. The one constant parameter is employed by the common cockroach swarm in chase-swarming behavior. The traveling habit is possessed by the cockroach for searching their food. It chooses the top path, and also it is quick in looking for food. Therefore, the cockroach swarm optimization algorithm is employed for the SP selection for this traveling habit. However, it comprises a convergence premature problem. Another constant parameter is included for increasing the search space in this proposed MCSO. The convergence premature issue is also decreased by this modification. Besides, to enhance accuracy, the levy distribution function is employed for random number selection in chase-swarm behavior updation. The steps comprised in the MCSO algorithm are elucidated below:

Step 1: Initially, the algorithm's parameters ($\hat{s}_{sp}, visual-$ visual scope, $K-$ space dimension, stopping criteria) are initialized. Then, a populace of z-individuals is generated. Chase-swarming, dispersing, along with ruthless behavior are the '3' procedures included by the MCSO algorithm for resolving different optimization problems. If a cockroach p_i is local optimal, then it reaches the global best solution (q_i), or else, the cockroach p_i attains local best solution (r_i) in the chase-swarming procedure, which expressed as,

$$p_i = \begin{Bmatrix} i_{we}.p_i + \hat{s}_{sp}.\mathrm{L}(\mathrm{t}).(r_i - p_i), & p_i \neq r_i \\ i_{we}.p_i + \hat{s}_{sp}.\mathrm{L}(\mathrm{t}).(q_i - p_i), & p_i = r_i \end{Bmatrix} \tag{6}$$

$$\mathrm{L}(\mathrm{t}) \sim |R_s|^{1-\varpi} \tag{7}$$

Wherein, p_i signifies the cockroach position, $\hat{s}_{sp}$ indicates a fixed value, $\mathrm{L}(\mathrm{t})$ signifies a levy distribution function for arbitrary number selection, i_{we} signifies the inertial weight, which is a constant aimed at enhancing the convergence speed of p_i, which is also a constant, R_s symbolizes the random Levy step along with ϖ indicates the parameter, which is utilized ranging from (0,1].

Step 2: After that, the local best position along with global best position are calculated as,

$$r_i = Opt_j \left\{ p_j, \left| p_i - p_j \right| \leq visual \right\} \tag{8}$$

$$q_i = Opt_j \{ p_i \} \tag{9}$$

Wherein, perception distance $visual$ is a constant, $i = 1,2,.....z$, $j = 1,2,.....z$.

Step 3: Next, for preserving the cockroach's diversity, dispersion is performed from time to time. The procedure comprises every cockroach executing a random step in the search space, which is specified as,

$$p_i = p_i + Rand(1, K) \tag{10}$$

Where, $Rand(1, K)$ signifies a K-dimensional random vector that is fixed in a certain range.

Step 4: A random individual is changed by the present best individual in a ruthless behavior,

$$p_k = q_i \tag{11}$$

Wherein, p_k is a random integer within $[1, k]$. The above 3 steps are repeated until a stopping criterion is met and the SP is outputted to effective DC. The cluster member (i.e. individual node or vehicle) acts as the gateway for DT if the request comes from another cluster. Minimizing the flooding of broadcast messages within the network by decreasing duplicate retransmissions in the same region is the gateway nodes' function. When member nodes obtain messages from over one CH, they are transformed into gateways. Every member in the cluster read along with process the packet, but the broadcast message is not retransmitted. The number of retransmissions in a flooding or broadcast procedure in dense networks is considerably reduced by this technique. It transmits the route information towards the destination CH. The requested route information is returned by the destination CH to the source CH. Finally, the route information is forwarded by the source CH to its intended cluster member. Then, for determining the SP, the above same procedure is recurred. The pseudocode for the SP selection utilizing the MCSO algorithm is depicted in the below figure,

Input: Requests from the Cluster
Output: Shortest Path

Begin
Initialize algorithm's parameters and generate population of z - individuals

For ($t = 0$ to t_{max})
If (requests comes from same cluster) do
{
//Shortest path generation
Search local position using, $r_i = Opt_j \{p_j, |p_i - p_j| \leq visual\}$
Search global position using, $q_i = Opt_j \{p_i\}$
//Dispersing behaviour
Carry out dispersing behaviour, $p_i = p_i + Rand(1, K)$
//Ruthless behaviour
Carry out ruthless behaviour, $p_k = q_i$
Generate shortest path
}
Else
Cluster member act as the gateway for data transmission
End if
End for
End

Figure 2: Pseudocode for the MCSO algorithm

3.6 Secure Data Communication

The secure DC process is executed after finding the shortest path. Detailed information regarding installation in the user manual on beltoll is gathered by the QBU. Utilizing the ASCII-ECC algorithm, this information is safely transmitted to the requested vehicle. Centred upon elliptic curve theory, the normal ECC is a public key encryption method that could be utilized for creating quicker, smaller, along with more effective cryptographic keys. Indirectly, by merging the key agreement with the symmetric encryption scheme, they can be employed for encryption. It offers a superior security level. But, the private key is chosen

arbitrarily in a normal ECC algorithm, which doesn't offer higher security. Therefore, the private key is chosen by multiplication of the random number with the ASCII value of the OBU password in this proposed method. This sort of technique enhances security in DC. The procedures incorporated in the ASCII-ECC algorithm are described in the below steps.

Step 1: An elliptic curve's equation is presented as,

$$U^2 = v^3 + \gamma v + \eta \tag{12}$$

Wherein, γ and η denotes the elements of a finite field with w^s elements. Here, w signifies a prime number.

Step 2: Key generation

A vital part is key generation, wherein the user has to create a public key together with a private key. If a sender needs to transmit a message, initially, the message will be encrypted with the receiver's public key, along with that ciphertext will be decrypted with its private key. Herein, a number X_{rn} is chosen by the system within the range of 's'. The public key ($UP_{key}^{"}$) is produced by utilizing the following equation,

$$UP_{key}^{"} = X_{rn} * BP_{key}^{"} \tag{13}$$

Wherein, X_{rn} signifies the arbitrary number i.e. chosen from 1 to $s-1$, $BP_{key}^{"}$ indicates the private key.

Step 3: Encryption

Let the original message (i.e.) transmitted to the requested vehicle be '$\overleftarrow{O}_{msg}$'. Two ciphertexts will be created let it be CT_1 and CT_2.

$$CT_1 = RN * PC \tag{14}$$

$$CT_2 = \overleftarrow{O}_{msg} + RN * UP''_{key} \tag{15}$$

Where, RN signifies the random number along with PC indicates the curve's point. These ciphertexts will be transmitted to the requested user.

Step 4: Decryption

Hither, the ciphertext message with its private key will be decrypted by the receiver for obtaining the message (original) in this decryption process. It is mathematically denoted as:

$$\overleftarrow{O}_{msg} = CT_2 - X_{rn} * CT_1 \tag{16}$$

In this way, for preventing numerous attacks and also preserving the driver's privacy, the requested user obtains the information securely.

4. RESULT AND DISCUSSION

The proposed ASCII- ECC centered secured DC on VANET is applied in MATLAB with the system configuration of Intel Core i7 processor, 3.20 GHz CPU speed, along with 4GB RAM. The outcomes attained for the ASCII- ECC is detailed in this section and analogized to the existent ECC, Rivest-Shamir-Adleman (RSA), together with Data Encryption Standard (DES). PDR, End to End Delay (EED), Collision Ratio (CR), Network Life-Time (NLT) together with Through-Put (TP) are the statistical measures utilized in the estimation. The nodes' sizes are differed as 10, 20, 30, 40, along with 50 correspondingly for every

comparison. The evaluated outcomes attained for the prevailing with proposed techniques are tabularized below.

.

Table 1: Results of the proposed ASCII- ECC with the existing algorithms

Metrics	No. of sensor nodes	Proposed ASCII-ECC	ECC	RSA	DES
PDR	10	87	80	72	60
	20	90	84	88	64
	30	94	82	84	67
	40	94	91	88	73
	50	96	93	91	76
Collision Ratio	10	30	42	65	82
	20	35	46	69	85
	30	38	50	73	88
	40	42	55	78	90
	50	46	61	80	95
End-to-End Delay	10	32	40	63	70
	20	38	52	69	75
	30	42	58	74	78
	40	54	60	79	80
	50	60	68	80	84
	10	85	80	73	64

Network Lifetime	20	88	83	76	68
	30	90	86	78	73
	40	93	88	82	76
	50	95	90	86	79
Throughput	10	90	80	77	64
	20	91	81	79	70
	30	93	84	82	75
	40	93	86	86	79
	50	95	89	84	80

Table 1 exhibits the obtained outcomes of the ASCII- ECC with the ECC, RSA, along with DES concerning PDR, EED, CR, TP and also NLT. The SN deemed for the comparative analysis is 10, 20, 30, 40, and also 50. For every SN, the proposed work acquires the maximum values aimed at PDR, NLT, TP, together with reduced rates for CR and the EED as displayed by the attained outcomes. When analogized to the existent ones, the proposed one works well for the secured DC in VANET, which is obviously clear. A detailed explanation of results for every measure is presented below,

(i) Packet Delivery Ratio (PDR)

The PDR is acquired by the sum of Data Packets (DP) attained by the receivers divided by the sum of DPs sent via the transmitter.

$$PDR = \frac{\sum \left(R_{pkt}^{r}\right)_{N}}{\sum \left(T_{pkt}^{t}\right)_{N}}, \quad N = 1....S \tag{17}$$

Wherein, PDR signifies the PDR, $\left(R_{pkt}^{r}\right)_{rc}$ implies the packet received by the receiver, besides, $\left(T_{pkt}^{t}\right)_{rc}$ implies the packets transmitted by the transmitter and S implies the total SN on the network. Figure 3 exhibits the performance comparison graph aimed at proposed ASCII- ECC with existent methods concerning PDR.

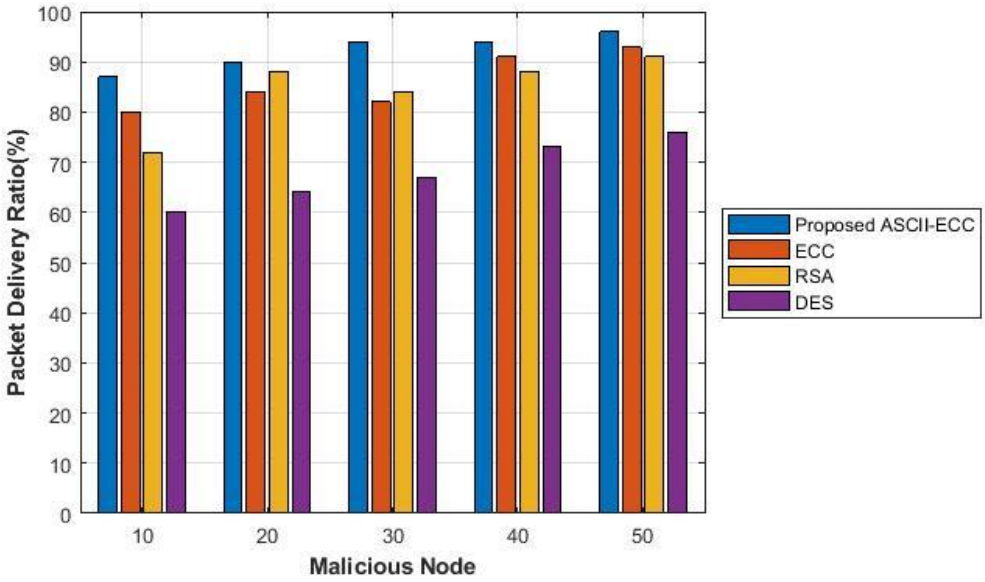

Figure 3: PDR of proposed and existing techniques

The proposed together with prevailing techniques' PDR graph is displayed in Figure 3. PDR exhibits efficiency in which the network sends its data amongst the nodes with respect it's routing. If the PDR is greater, then their performance would be higher while delivering the data betwixt every mobile node devoid of any loss. The ASCII- ECC got 87% while considering 10 SN. However, for the same SN, the ECC, RSA, and DES attain 80%, 72%, and 60%. If 50 nodes are considered, it exhibits 96%, 93%, 91%, along with 76% for the ASCII- ECC, ECC, RSA, along with DES, respectively. In contrast with the ECC, RSA, and DES, it can well be perceived that the ASCII- ECC delivers the packets more effectively as of source - destination.

(ii) Collision ratio

The packet's CR stands as the total DP collisions that occur on a network over a provided time period (i.e.) the rate in which data collides or get lost on collisions. It is assessed as a level of the DP conveyed effectively. Figure 4 exhibits the CR of every technique.

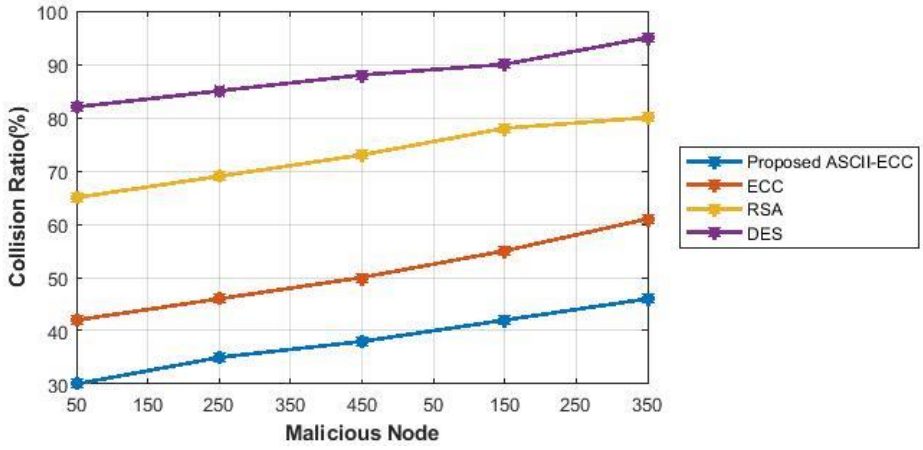

Figure 4: CR of the proposed and existing techniques

Figure 4 exhibits the comparative analysis of proposed and existing techniques' CR. While considering 10 SN, the ASCII- ECC is 35% and the existent methods got 42%, 65%, along with 82%. In addition, for 50 SN, which is the highest, proposed one exhibits 46% and DES got 95%. The proposed ASCII- ECC analogized to the existent ones achieves lesser nodes collision during DT.

(iii) End-to-End delay:

The average time taken while routing the data betwixt a source and the target node is called the delay. It is regarded in seconds. The time required aimed at the data to be transmitted as of the sender towards the recipient amongst the networks is called the average delay.

$$E^d = \frac{\sum_{t=1}^{N} D_t}{P_r} \tag{18}$$

Wherein, E^d implies the end-to-end delay output, D_t implies packet delivery time to the receiver, P_r exhibits the number of packets that the receiver obtained. Figure 5 exhibits the EED measure's visualization.

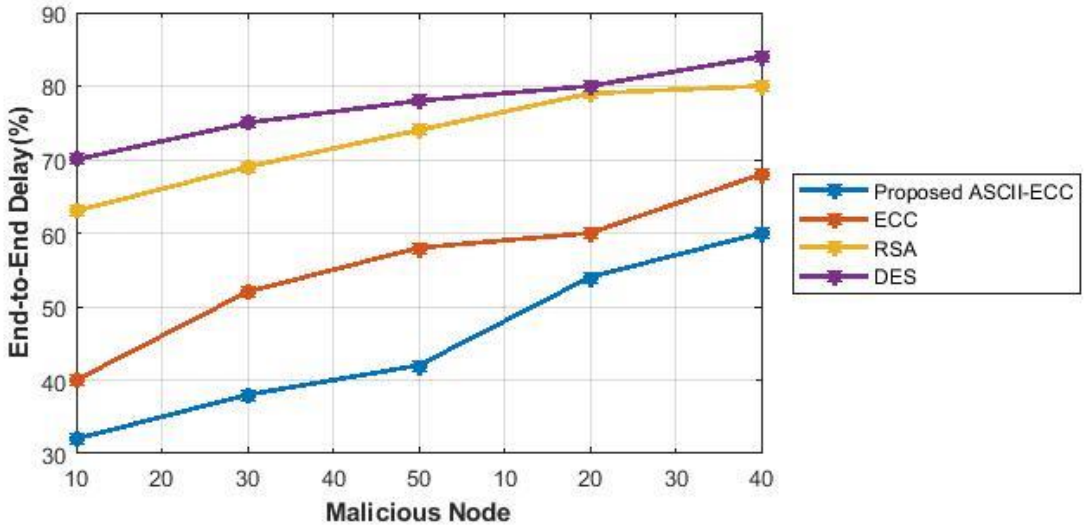

Figure 5: EED of the proposed and existing techniques

The proposed along with the prevailing method's EED comparison is conducted by considering SN from 10 to 50, which is depicted in figure 5. And the network's delay is gauged in seconds. If 10 SN is deemed, the proposed work had 32% delays whereas the existent one had 40%, 63%, and 70% correspondingly. Similarly, for the 50 SN, the ASCII-ECC attains a delay of 60%, which is lesser when weighted against the prevailing method. The delay attained by the ASCII- ECC is lower analogized to the prevailing methods for the remaining (20, 30, and 40) nodes. Hence, it is perceived that the proposed work attains superior performance concerning secure DC while deeming the delay.

(iv) Network lifetime:

The system's lifetime for a specific period is gauged by the NLT. This is inversely proportional to the packet loss.

$$T_l^n = 1 - \frac{t}{\mu_t} \tag{19}$$

Where, T_l^n signifies the network's lifetime and μ_t denotes the mean time betwixt failure nodes. Its graphical depiction is exhibited below.

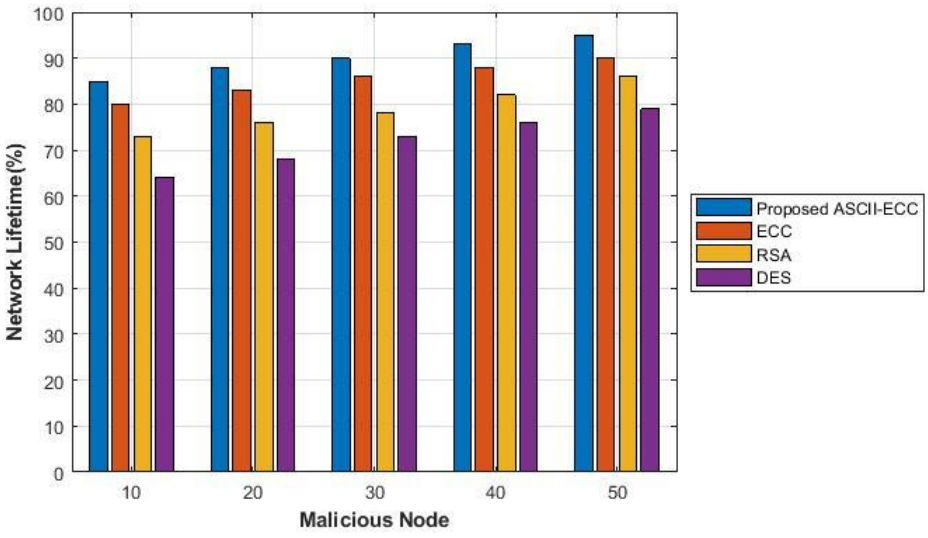

Figure 6: NLT of the proposed and existing techniques

Figure 6 exhibits the proposed together with existing techniques' NLT performance. If the NLT is higher, then there would be no loss in the packet delivery to the destination. The NLT is gauged by varying the SN from 10 to 50. The proposed one attains a better NLT of 85% for 10 SN and 95% for 50 SN. In considering these rates, the existent technique generates much lower outcomes for the NLT detection.

(v) Throughput:

The total packets achieved at the receiver by the packet transmission delayed during the procedure is called the TP, which is mathematically specified below,

$$N_i^e = \frac{P_r^t}{D_l} \tag{20}$$

Wherein, N_i^e signifies the throughput, P_r^t indicates the number of received packets and D_l signifies the delay. Figure 7 illustrates the graphical depiction of the TP.

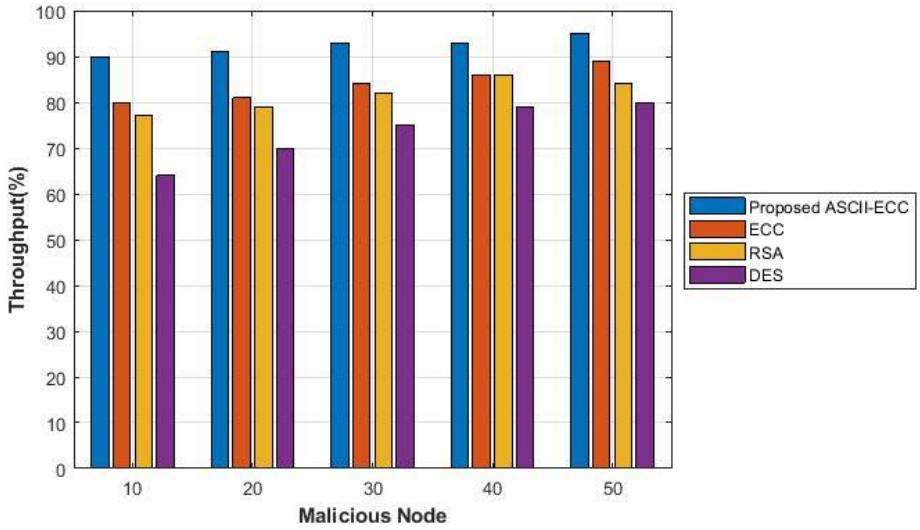

Figure 7: TP of the proposed and existing techniques

The proposed with existing methods' TP graph is depicted in figure 7. 95% TP is attained by the ASCII- ECC and also the prevailing ones attain 89%, 84%, along with 80% aimed at the initial 50 nodes. Similarly, the ASCII- ECC attains the highest TP values of 90%, 91%, 93%, together with 93% in contrast to ECC, RSA, along with DES for the remaining (10, 20, 30, along with 40) nodes. During DC, the TP must be higher for a mobile node that can well be made possible in the proposed work. The proposed one is much effectual for secured DC with less collision and also much more TP ratio on the higher NLT.

5. CONCLUSIONS

Routing in VANET is a tough task to attain owing to its higher mobility. Secured routing is the prime challenge in VANET. This work proposed the DC's enhanced security within the VANET environment utilizing the ASCII-ECC technique. The system primarily comprises six phases, namely, network model, registration phase, cluster formation, CHS verification process, select SP, and secured DC. The proposed ASCII-ECC's performance is analogized with a few traditional techniques, like, ECC, RSA, and also DES techniques grounded on a number of SNs ranging as of 10 to 50 nodes. The performance analogy is executed utilizing a few performance metrics, like, PDR, CR, EED, NLT, and also TP. Aimed at 50 nodes, the technique proposed attains 96 % PDR, 46 % CRs, 60 % EEDs, 95 % NLTs, 95 % TP that is high-level performance analogized to the existent ECC, RSA, and also DES methodologies. In the forthcoming future, the protocol proposed is boosted by identifying the vehicles' misbehavior, and pondering the signature centered authentication technique in the TA phase aimed at the security level's incrementation.

Declarations

We declare that this manuscript is original has not been published before and is not currently being considered for publication elsewhere.

Funding: there has been no financial support for this work that could have influences its outcomes.

Conflicts of interest/Competing interests: no conflicts of interests associated with this publication

Availability of data and material (data transparency):NA

Code availability (software application or custom code):NA

Authors' contributions: ASCII-ECC algorithm

REFERENCES

1. Sahil Khatri et al(2020) “Machine learning models and techniques for VANET based traffic management: Implementation issues and challenges”, Peer-to-Peer Networking and Applications, pp. 1-28, 10.1007/s12083-020-00993-4.
2. Huan Zhou et al,(2018) “Data offloading techniques through vehicular ad hoc networks: A survey”, IEEE Access, vol. 6, pp. 65250-65259.
3. Sahil Garg et al(2019), “Edge computing-based security framework for big data analytics in VANETs”, IEEE Network, vol. 33, no. 2, pp. 72-81.
4. Muhammad Arif et.al(2019),“A survey on security attacks in VANETs: Communication, applications and challenges”, Vehicular Communications, vol. 19, pp. 100179.
5. Dakshnamoorthy Manivannan et al(2020),”Vehicular Communications”, vol. 25, pp.100247, 10.1016/j.vehcom.2020.100247.
6. Rasheed Hussain et al(2018),“Realization of VANET-based cloud services through named data networking”, IEEE Communications Magazine, vol. 56, no. 8, pp.168-175.
7. Rajendra S.Hande and Akkalakshmi Muddana(2016), “Comprehensive survey on clustering-based efficient data dissemination algorithms for VANET”, In IEEE International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), pp. 629-632, 10.1109/SCOPES.2016.7955516.
8. Lei Liu et al(2018),“A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs”, Vehicular Communications, vol. 13, pp. 78-88.

9. Hasan Ali Khattak et al(2019),"Integrating fog computing with VANETs: A consumer perspective", IEEE Communications Standards Magazine, vol. 3, no. 1, pp. 19-25.

10. Changsheng Wan and Juan Zhang(2018),"Efficient identity-based data transmission for VANET", Journal of Ambient Intelligence and Humanized Computing, vol. 9, no. 6, pp. 1861-1871.

11. Nisha Malik et al(2018),"Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks", In 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 674-679, 10.1109/TrustCom/BigDataSE.2018.00099.

12. Mevlut Turker Garip et al(2018),"Botveillance: A vehicular botnet surveillance attack against pseudonymous systems in vanets", In IEEE 11th IFIP Wireless and Mobile Networking Conference (WMNC), pp. 1-8, 10.23919/WMNC.2018.8480909.

13. Ibrahim Rashdan et al(2016),"Performance evaluation of traffic information dissemination protocols for dynamic route planning application in VANETs", In IEEE 84th Vehicular Technology Conference (VTC-Fall), pp. 1-5, 10.1109/VTCFall.2016.7881161.

14. Danda B.Rawat et al(2016),"Securing vehicular ad-hoc networks from data falsification attacks", In IEEE Region 10 Conference (TENCON), pp. 99-102, 10.1109/TENCON.2016.7847967.

15. Nikita Lyamin et al(2018),"AI-based malicious network traffic detection in VANETs", IEEE Network, vol. 32, no. 6, pp. 15-21.

16. Azzedine Boukerche et al(2020), “Artificial intelligence-based vehicular traffic flow prediction methods for supporting intelligent transportation systems”, Computer Networks, vol. 182, pp. 107484.

17. Aaqib Khalid et al(2018),“Autonomous data driven surveillance and rectification system using in-vehicle sensors for intelligent transportation systems (ITS) ”, Computer Networks, vol. 139, pp.109-118.

18. Manickam P et al(2019),“Secure data transmission through reliable vehicles in VANET using optimal lightweight cryptography”, In Cybersecurity and secure information systems, Springer Cham, pp. 193-204, 10.1007/978-3-030-16837-7_9.

19. Prinkle Sharma et al(2017), “Securing wireless communications of connected vehicles with artificial intelligence”, In IEEE international symposium on technologies for homeland security (HST), pp. 1-7, 10.1109/THS.2017.7943477.

20. Yujie Tang et al(2019), “Delay-minimization routing for heterogeneous VANETs with machine learning based mobility prediction”, IEEE Transactions on Vehicular Technology, vol. 68, no. 4, pp. 3967-3979.

21. Canhuang Dai, Xingyu Xiao, Yuzhen Ding, Liang Xiao, Yuliang Tang, and Sheng Zhou, “Learning based security for VANET with blockchain”, In IEEE International Conference on Communication Systems (ICCS), pp. 210-215, 2018, 10.1109/ICCS.2018.8689228.

22. Sowmya Kudva et al(2020), “Towards secure and practical consensus for blockchain based VANET”, Information Sciences, vol. 545, pp. 170-187.

23. Ayan Roy and Sanjay Madria(2020), “Distributed Incentive-Based Secured Traffic Monitoring in VANETs”, In 21st IEEE International Conference on Mobile Data Management (MDM), pp. 49-58, 10.1109/MDM48529.2020.00026.

24. Jitendra Bhatia et al(2019),"SDN-enabled Network Coding Based Secure Data Dissemination in VANET Environment", IEEE Internet of Things Journal, 10.1109/JIOT.2019.2956964.

25. Parul Tyagi, and Deepak Dembla(2018), "Advanced secured routing algorithm of vehicular ad-hoc network", Wireless Personal Communications, vol. 102, no. 1, pp. 41-60.

26. J.Jenefa and E.A Mary Anita(2021),"Identity-based message authentication scheme using proxy vehicles for vehicular ad hoc networks", Wireless Networks, https://doi.org/10.1007/s11276-021-02655-6.