Traffic & Transportation

Chinese Remainder Cryptosystem-Based Multilayer Perceptron Signcryption for Secure Vehicular Communication

Jini KIZHAKKAYIL MEETHAL[1], Senthilkumar JAYAPRAKASAM[2], Suresh YUVARAJ[3], Mohanraj VIJAYAKUMAR[4]

Original Scientific Paper
Submitted: 13 Dec 2024
Accepted: 4 Apr 2025

[1] jini.km@gmail.com, Department of Information and Communication Engineering, Anna University, Chennai, India
[2] jsenthil10@gmail.com, Department of Information Technology, Sona College of Technology, Salem, India
[3] ysuresh33@gmail.com, Department of Information Technology, Sona College of Technology, Salem, India
[4] vmohanraj06@gmail.com, Department of Information Technology, Sona College of Technology, Salem, India

Publisher:
Faculty of Transport and Traffic Sciences, University of Zagreb

ABSTRACT

Vehicular ad-hoc networks (VANETs) are significant network environments for communication between vehicles to efficiently address the issues concerning traffic safety, traffic management and circumventing congestion. Signcryption has been employed in VANET owing to the reason that both signing and encryption are done simultaneously, therefore minimising computational cost. However, communication costs and verification processing time were increased. To address this issue, a Chinese remainder cryptosystem-based multilayer perceptron certificateless signcryption (CRC-MPCS) for secure data communication in VANET is proposed. The deep learning framework employing a multilayer perceptron possesses three layers. VANET vector parameters are provided as input to the input layer. The first hidden layer performs the sender vehicle node key generation, and the second hidden layer performs the receiver vehicle node credential generation. Finally, the output layer, along with the weight updates for each epoch and rectified linear unit (ReLU) activation, certificateless cryptosystem (CLC), performs secure vehicular communication. The proposed CRC-MPCS method reduces signcryption verification processing time and improves data confidentiality, data integrity, authentication accuracy and communication cost compared to conventional methods.

KEYWORDS

certificateless signcryption; Chinese remainder; cryptosystem; rectified linear unit; vehicular ad-hoc network.

1. INTRODUCTION

Owing to the increase in the frequency of vehicles over the past few years, urban traffic management has experienced a substantial traffic overhead with the accelerated growth in the number of vehicles. The developments in VANETs also ensure significant intelligent transportation. Therefore, distribution and execution are entirely converging protection necessities of data, verification, non-repudiation, as well as user security to a greater extent. With the objective of attaining protection, numerous verification mechanisms appropriate for VANETs were developed.

CP-CPPHSC was proposed in [1] employing bilinear pairings and ensuring security. By employing the designed method, the message was transferred with the vehicle utilising CLC with the aid of PKI. Moreover, the CP-CPPHSC method proposed batch unsigncryption that assists the vehicle to unsigncrypt synchronously. As a result, the method was proven to be imperceptible in opposition to ciphertext attacks and also reduces the computational cost.

Despite minimisation of the computational cost, the signcryption verification processing time was not focused on. To address this aspect, a Chinese remainder cryptosystem is first designed, which, with the aid of

Hermite interpolation, speeds up the computations, therefore reducing the signcryption verification processing time involved in data communication.

An effective IBS-CPPA method on ECC to communicate between vehicles was proposed in [2]. This IBS-CPPA method reinforces batch signature verification that, in turn, enables each vehicle to authenticate a large number of messages simultaneously. Also, a security proof was ensured for the IBS-CPPA method, therefore satisfying security requirements and minimising computational cost to a greater extent.

Though computational cost was reduced, the data confidentiality factor was not considered. To address this aspect, a deep learning-based signcryption mechanism called a multilayer perceptron-based signcryption mechanism is proposed in our work for communication between vehicles in VANET. The multilayer perceptron-based signcryption mechanism with Chinese remainder function, due to its adaptive learning potential, ensures security by improving data confidentiality.

One of the exemplary mechanisms to transfer messages in a secure and authenticated mode remains in following signcryption. A certificateless sign cryptography (CLSC) method was proposed in [3] for ensuring a safe and secure means of transmitting information between vehicles. Moreover, confidentiality, authentication and user privacy were also provided based on the pairing mechanism.

Conventional methods using RSUs have been utilised by vehicles to exploit cross-domain services, therefore causing a small amount of delay and large loads on the RSUs. To address these issues, a scheme was introduced in [4] to share data between distinct domains. Initially, edge computing vehicles (ECVs) were selected, and next, the data packets to be shared were forwarded, therefore reducing latency and load on the RSUs. Several certificateless signature works [4] concentrating on ensuring anonymous confirmation by protection have been discussed in recent years.

In [5], a novel certificateless aggregate signature-based authentication method, avoiding the complexity of managing public key issues over identity-based construction, was proposed. With this, the computation overhead was significantly minimised. However, privacy, authentication and secure message transmission are certain specific issues that need to be handled for the extensive deployment of VANETs.

An overview of the security and privacy issues in VANETs for message transmission was investigated in [6]. A holistic review of security vulnerabilities of the existing methods was conducted, and also improvements to identity-based conditional privacy-preserving authentication methods were presented in [7] to ensure security and enhance the effectiveness of VANET communications.

An extensive range of materials and methods was designed to ensure secure wrapping of data from malicious users. Such algorithms have their advantages and disadvantages. Therefore, effectiveness and privacy form the pivotal elements as far as content extraction signatures are concerned.

In the procedure of acquiring information pertaining to traffic, there exists certain private and sensitive information that can be easily tampered with by malicious users. Hence, it becomes vital to propose a method to safeguard vehicle data during the information reading phase. In [8], a novel and secure authentication mechanism that, in turn, negotiated a session key prior to traffic information transmission was proposed. Only after mutual authentication, a session key was said to be generated. Due to this, security was said to be improved.

A novel mechanism for generating a transmission key was proposed in [9]. Also, inverse operations are performed for deciphering data in a safe and secure manner. Finally, floating frequency with an encrypted bit stream resulted in better security. In [10], a secured and significant certificateless content extraction signature with privacy protection (SECCESPP) was designed where scalar elliptic curve multiplication was utilised to swap insignificant bilinear certificateless public key pairing, therefore ensuring privacy and security of data being transmitted.

1.1 Our contributions

The main contributions of this paper are summarised as follows.

1) To introduce the Chinese remainder cryptosystem-based multilayer perceptron certificateless signcryption (CRC-MPCS) to protect data communication.
2) The CRC-MPCS method does not employ costly pairing and instead employs the Chinese remainder theorem, enhancing the computational effectiveness of the system.
3) RSU aggregates every data packet received over vehicles within a single signature via the first hidden layer of a multilayer perceptron of RSU, and verifies data packets for communication. Hence, the signcryption verification processing time is reduced.

4) The proposed CRC-MPCS method with Hermite interpolation function is proven secure, as only the vehicles positioned within transmission range of the corresponding vehicles are used, and no vehicles outside the transmission range are used.
5) Compared with other certificateless signcryption methods, the CRC-MPCS method is efficient in communication cost, signcryption verification processing time and data confidentiality point of view.

1.2 Organisation of the paper

Section 2 presents the related work. Section 3 provides certain preliminaries, including the network model followed in the proposed method and the design of the proposed method, Chinese remainder cryptosystem-based multilayer perceptron certificateless signcryption (CRC-MPCS) with the aid of figurative representation and its security analysis. Section 4 presents the experimental setup and simulation parameters for the working of the proposed CRC-MPCS method, followed by a discussion in Section 5 with the aid of a table and graphical representation. Section 6 describes the conclusions of the article.

2. RELATED WORKS

Vehicular sensing was recommended for performing the collection of data by employing an abundance of vehicular on-board sensors collected by an on-board unit (OBU). Moreover, integration of vehicular sensing positioned RSUs measures fog nodes for obtaining the vehicular sensory data. But it persists in certain issues as far as security and reliable sensory data sharing are concerned. To address these aspects, in [11], an effective and verifiable sensory data collection method employing a permissioned blockchain was designed. This integrated mechanism resulted in secured access.

A lightweight and privacy-preserving certificateless authentication method was presented in [12]. Despite improvements in the security aspect, the signcryption verification process was not considered. Moreover, a novel authentication mechanism was presented employing a certificateless signature on the basis of elliptic curve cryptography (ECC) and a hash function. This integrated mechanism not only resulted in improving security but also reduced communication costs along with the overhead incurred. Secure anonymous data aggregation based on blockchain (BDB-SADA) was introduced in [13] to minimise communication costs. The security issue was addressed. However, the memory consumption was not considered.

Constrained computing potentialities, in addition to communication over an open wireless channel, aggravate security-related issues, making the vehicles unattainable for secure operations. In [14], an identity-based proxy signcryption method to address this issue, employing outsourcing decryption and member revocation, was designed. It was designed on the basis of hyper-elliptic curve cryptography (HECC), which in turn also enhanced the effectiveness of the network computation. Also, security aspects were concentrated on the random oracle model (ROM).

Over the recent years, several certificateless signature mechanisms have been designed with the objective of not only enhancing the communication speed but also safeguarding communication contents from malicious nodes. In [15], a significant privacy-preserving certificateless public key signature method employing blockchain was proposed. With this blockchain mechanism, not only was the identity privacy of the vehicle safeguarded, but also by means of signature aggregation, computation cost was minimised to a greater extent. However, the overhead incurred was not focused on. Yet another message authentication method employing the Diffie-Hellman protocol and an effective version of the RSA algorithm was used in [16] that minimised the computation overhead incurred during secured communication. However, with the reliance on the third party, security breaches were in the spotlight. To address this factor, an identity-based cryptography method was designed in [17], employing a novel mutual authentication scheme was proposed.

A novel model of certificateless crypto system (CLC) and identity-based cryptosystem (IBC) called heterogeneous generalised signcryption was presented in [18] to address the pivotal security requirements. Moreover, the proposed method addressed the security characteristics based on the situational requirements without affecting the structural policy.

Certain certificateless signcryption techniques are designed based on the standard model. However, most signcryption methods employed in traditional security approaches are unable to guarantee the security with minimum time. The certificateless signcryption method in [19] was designed to ensure security. Lattice-based conditional privacy-preserving certificateless aggregate signature scheme (LB-CLAS) was introduced in [20] to minimise the signcryption verification process time. The designed scheme was based on aggregate signatures and batch verification to improve security. However, the authentication accuracy was not improved.

In recent years, electronic recommendations have been acknowledged, as far as countries are concerned. However, with constrained legal requirements, rules and regulations with regards to privacy, two significant aspects to be clarified are authorization and data confidentiality. An improved certificateless proxy signcryption method was designed in [21] based on the basis of ECC. The proxy method was identified and provides computational efficiency. The advantage of CLSC remains in providing encryption and a certificateless signature simultaneously. However, several CLSC methods necessitate high computational overhead. Random oracle was presented in [22] for selecting the receiver improved the communication, hence minimising computational overhead during pairing operations.

Elliptic curve-based signcryption methods were presented in [23] to address the security-related issues and provided both integrity and authentication. Moreover, certificateless signcryption methods were better in computational cost. Certificateless generic signcryption was proposed by [24] with lesser overhead, but it failed to consider authentication accuracy. Novel CLS and certificateless aggregate signature (CL-AS) methods were designed in [25] based on ECC. The method was significant in computation cost as well as computation overhead.

2.1 Research gap

VANETs are crucial for communication between vehicles. Various certificateless aggregate signature schemes were developed in VANETs. However, these schemes of computation cost and communication overhead were not reduced. Signcryption is used to transmit messages in a secure and authenticated manner. Also, the signcryption verification processing time was higher and data confidentiality factor was not focused. In addition, security is the main issue in VANETs. To address the issue, a proposed new CRC-MPCS method is used to address security and performance issues in VANETs. Through the CRC-MPCS method, a message or data packet is transmitted by a vehicle using the Chinese remainder cryptosystem model in a deep learning framework employing a multilayer perceptron. In this way, the computation cost and communication overhead were minimised. The signcryption process is employed in CRC-MPCS to achieve higher security and signcryption verification processing time.

3. CHINESE REMAINDER CRYPTOSYSTEM-BASED MULTILAYER PERCEPTRON CERTIFICATELESS SIGNCRYPTION (CRC-MPCS)

In this section, first, a secure data communication model is introduced. Following it, a security policy based on the Chinese remainder cryptosystem is modelled. Then, we analyse the characteristics of the multilayer perceptron and each layer of the network to integrate it with the certificateless signcryption for secured vehicular communication. Finally, secure data communication is ensured between vehicles in VANET.

3.1 Secure data communication model

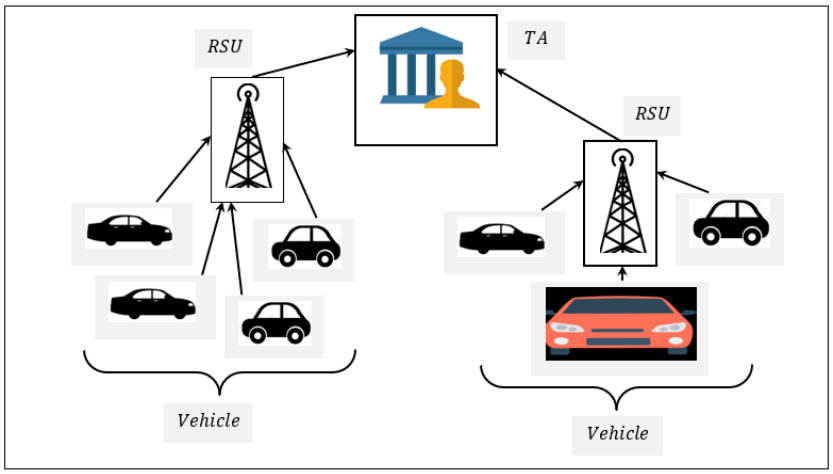

Figure 1 – Secure data communication model in VANET

In this section, a secure data communication model followed in the proposed deep learning and certificateless signcryption-based secured data communication in VANET is given. VANET consists of three

entities, the vehicle node '$V=V_1, V_2, \ldots, V_n$', road side unit 'RSU' (i.e. installed on road side to support infrastructure necessitate for VANET deployment) and the trusted authority 'TA'.

Trusted authority 'TA' is set to be trusted by both the '$OBUs$' and '$RSUs$' that in turn generates system parameters in addition to the secret key 'SK' for each vehicle 'V_i' and preloads them into the correlated vehicle. Also, the vehicle nodes in VANET utilises an on-board unit 'OBU' (i.e. installed to vehicles) to sense messages or data packets '$DP = DP_1, DP_2, \ldots, DP_n$' from its surrounding vehicles. The second entity is the road side unit '$RSUs$' that is associated with the 'TA'. Its main function is to store and forward the information between vehicles, the 'TA' and other '$RSUs$'. Along with it, the 'TA' formulates the Chinese remainder cryptosystem model for ensuring secure data communication between vehicles in VANET. Finally, each vehicle communicates with other vehicles, and every emerging data packet 'DP'originating from vehicles 'V_i' necessitates to be signed prior to being sent to adjacent vehicles 'V_j'. Finally, the job of a trusted authority remains in ensuring secure communication between vehicles in VANET. Every vehicle in VANET is loaded with an OBU to ensure communication between vehicles. With the above-mentioned structure and data communication model, a secured method is designed by employing a certificateless signcryption mechanism.

3.2 Chinese remainder cryptosystem model

The Chinese remainder theorem (CRT) represents a theorem of number theory, hypothesizes that upon knowing the Euclidean division of transmission range of vehicle 'V_i', then the subsequent vehicle 'V_j'can determine uniquely remainder of the transmission range and transmission rate by product of these integers, based on pair-wise co-prime factor. With this hypothesis, the secure version of this proposed CRC-MPCS method works with the Chinese remainder cryptosystem and takes advantage of the above 'TA' based system architecture so as to exploit the secure pair of congruences. The advantage of the CRC is used to enhance efficiency in key generation, and minimise computational cost and memory consumption compared to RSA or ECC. *Figure 2* below shows the structure of the Chinese remainder cryptosystem model.

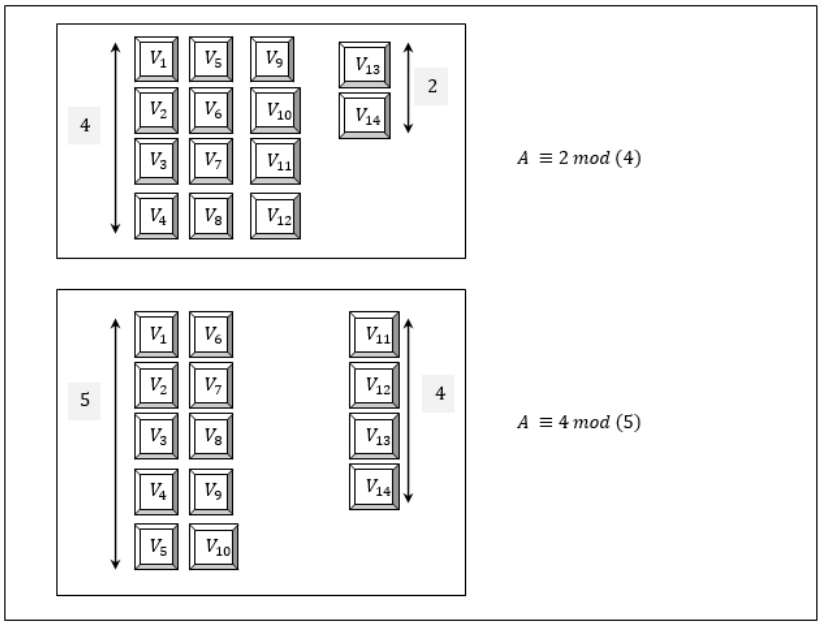

Figure 2 – Structure of the Chinese remainder cryptosystem model

As shown in the above *Figure 2*, let '$p_1, p_2, \ldots, p_n$' be pair-wise relative prime numbers and let 'P_i^{-1}' represent the modular multiplicative inverse of transmission range of a vehicle '$P_i\ mod\ p_i$' and modelled in such a manner to satisfy the given equation below.

$$P_i P_i^{-1} \equiv 1\ (mod\ p_i), i = 1,2, \ldots, n \tag{1}$$

Let '$q_1, q_2, \ldots, q_n$' represent the 'n' positive numbers, then CRT for the corresponding pair of congruences between sender vehicles 'V_i' and receiver 'V_j' is stated as given below.

$$A\ (V_1) \equiv\ q_1\ mod\ p_1; A\ (V_2) \equiv\ q_2\ mod\ p_2; A\ (V_3) \equiv\ q_n\ mod\ p_n \tag{2}$$

From the above *Equation 2*, the congruences between vehicles possess a unique solution '$mod\ \partial g = p_1, p_2, \ldots, p_i = \pi_{i=1}^{n}(p_i)$'. With the congruences between vehicles, the trusted authority 'TA' can acquire the solution to ensure secured access with the function as given below.

$$A\ (V) = q_1 + q_2 + \ldots + q_n(mod\ \partial g) \tag{3}$$

$$= \sum_{i=1}^{n} q_i \alpha_i \beta_i, where\ \alpha_i = \frac{\partial g}{p_i}; \alpha_i \beta_i = 1\ mod\ p_i \tag{4}$$

In addition, to minimise the signcryption verification processing time involved in data communication, the Hermite interpolation function is employed that involves moduli of arbitrary degree (i.e. arbitrary transmission range of vehicle) and is mathematically formulated as given below.

$$A\ (V) = A_i(V) + (V - v_i)^n \tag{5}$$

From the above *Equation 5*, '$A_i(V)$' denotes the Taylor polynomial of order 'n' at 'v_i' that is '$A\ (V)$' which addresses the Hermite interpolation. With this, both security and message (i.e. data packets) distribution rate are said to be improved while performing vehicular communication in VANET. The security proof of adversarial attacks in machine learning illustrates an attacker. The proof aims to measure the success rate of an adversarial attack. It shows that a high percentage of generated adversarial examples is needed to validate the robustness.

3.3 **Multilayer perceptron-based certificateless signcryption**

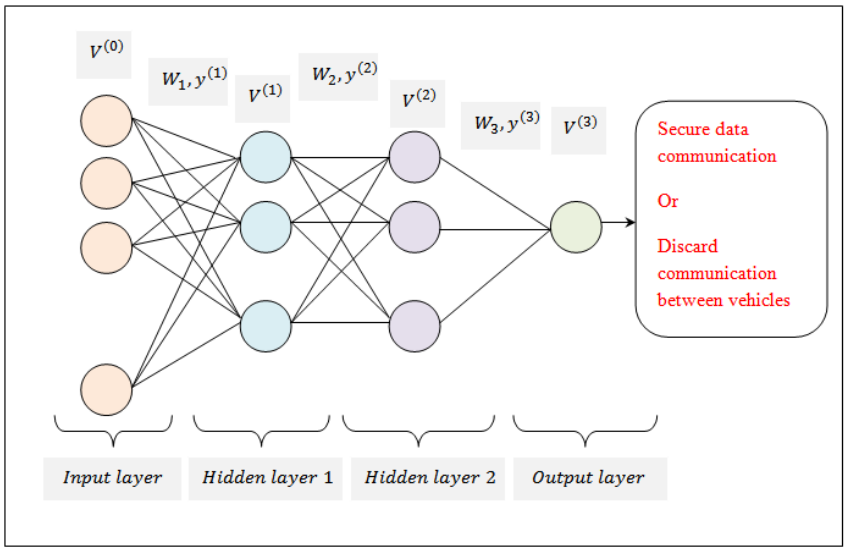

Figure 3 – Structure F

With the above design of the Chinese remainder cryptosystem model, the proposed method, multilayer perceptron-based certificateless signcryption method, CRC-MPCS, is designed. The proposed CRC-MPCS method consists of perceptrons arranged in distinct layers and described in *Figure 3*.

As shown in the above figure, the first layer obtains as input the vehicle node data in the form of a vector '$V = \{V_i\}_{i=1,2,3,\ldots,n}$' as '$n$' denotes number of perceptron input. Multilayer perceptron includes one input layer, two hidden layers and one output layer. Input layer size is nine (i.e. area, transmission range, transmission rate, SNR, vehicles mobility, number of vehicles, data packets, simulation time and message life time, respectively). Hence, the number of neurons was 9. Next, two hidden layers are employed for secure communication between vehicles. The specific reason to choose two hidden layers in MLP is to offer superior complexity and learning capability. It is used to learn complex patterns and extract meaningful features from input data. The sender vehicle node processing is performed in the first hidden layer and the receiver vehicle node processing is done within the second hidden layer. In this way, the computation cost and memory are minimised. At last, rectified linear unit (ReLU) activation is employed at the output layer to offer secure vehicular communication or reject communication among vehicles. Then, neurons are mathematically formulated in the input layer as given below.

$$No\ of\ neurons\ (HL) = \frac{2}{3}(Size_{IL}) + Size_{OL} \quad (6)$$

From *Equation 6*, neurons are determined by size of input layer '$Size_{IL}$' and the size of output layer '$Size_{OL}$', respectively (7 neurons). Also, the perceptron here refers to the classifier that maps the input (i.e. an integer value vector 'V') to an output 'y' value as given below.

$$y = f\left(U =< W : V \geq f\left(\sum_i W_i V_i\right)\right) \quad (7)$$

From *Equation 7* above, 'W' denotes the perceptron weight (i.e. '0.2') of size 'n' and '$f(.)$' denotes the activation function. To make the proposed CRC-MPCS method function properly, it should be trained so as to identify the perceptron values of weights. MLP is used to adjust the perceptron weights to provide minimal error in the training data.

The proposed CRC-MPCS method applies supervised training where the classes of data or data packets to be communicated between the vehicles are known in prior. Hence, the vehicle issues labelled data '$TainData\ (TrD) = \{TrD_i\}_{i=1,2,..n}$' where '$n$' remains the size of training data packets and 'TrD_i' refers to the class label of the '$i-th$' training input data, respectively. Initially, with the above formulated integer value vector mapping, the system parameter is generated by means of the security parameter 'l' and is mathematically stated as given below.

$$Setup(1^l) \rightarrow param \quad (8)$$

From *Equation 8*, using the security parameter 'l' as input, the multilayer perceptron with the input neurons in the input layer (i.e. nine factors) generates the system parameter (i.e. $param = 9$) for further processing. Next, with the parameters '$param$'as input trusted authority key generator '$TAKGen$' generates the private key and public key as given below.

$$TAKGen(param) \rightarrow (PR_{TA}, PB_{TA}) \quad (9)$$

Followed by which, with the parameter '$param$' and private key of trusted authorityas given in above *Equation 9*, 'PR_{TA}' as input, generates private key 'PR_{SV}' and public key 'PB_{SV}' of sender vehicle node, forming the sender vehicle key generator '$SVKGen$' as given below.

$$SVKGen(param, PR_{TA}) \rightarrow (PR_{SV}, PB_{SV}) \quad (10)$$

Next, with the parameter '$param$', public key of trusted authority 'PB_{TA}' and security parameter 'l'as input denotes security of verifier, the receiver vehicle node credential '$RVCre$' is modelled as given below.

$$RVCre(param, PB_{TA}, L) \rightarrow RVKCre \quad (11)$$

With the parameter '$param$', private key of sender vehicle 'PR_{SV}', public key of sender vehicle 'PB_{SV}', 'PB_{TA}' and data packet 'DP' to be communicated is processed via Chinese congruences between vehicles as security factor 'A', sender's ciphertext '$\mathcal{C}$' by employing certificateless signcryption function 'SC' as given below.

$$SC(param, DP, PR_{SV}, PB_{SV}, PB_{TA}, A) \rightarrow \mathcal{C} \quad (12)$$

Finally, with the '$param$', 'DP', 'PB_{TA}', 'PB_{SV}', 'A' and '$RVKCre$' as input, the unsigncryption function 'USC'returns with the output 'y' and is stated as given below.

$$USC(param, DP, PB_{TA}, PB_{SV}, A, RVCre) \rightarrow y \quad (13)$$

Finally, the output layer provides the class of input data, with one neuron that either proceeds with secure data communication or discards communication between vehicles. In our work, the rectified linear unit '$ReLU$' activation function is employed owing to its accuracy and ensuring security via homomorphic operators.

$$f(y) = \begin{cases} y, if\ y \geq 0 \\ 0, Otherwise \end{cases} \quad (14)$$

Upon completion of one epoch, the feed-forward phase in a multilayer perceptron consists of measuring the multilayer perceptron's output for a given input vehicle node. This is mathematically stated as given below.

$$SCWS = \prod_{i=1}^{n} A_i^{V_1 V_2}(SC\ [IL_i], SC[W_i]) \quad (15)$$

From the above *Equation 15*, the secured or the sigcrypted weighted sum '$SCWS$' is measured by employing the Chinese remainder function 'A' between vehicles 'V_1' and 'V_2', the signcrypted input vectors '$SC\ [IL_i]$' and the corresponding weight '$SC[W_i]$', respectively. Next, the weight updates are performed according to the mean square error (MSE) value. The updated value 'W_i'' of its weight 'W_i' is mathematically stated as given below.

$$W_i' = W_i + \frac{1}{\lambda}\left[\frac{\partial E}{\partial W_i}\right], where\ \partial E = \frac{1}{2}\sum_{i=1}^{n}(y_i - y_i')^2 \quad (16)$$

From *Equation 16*, the weight update 'W_i'' results are obtained based on the initialised weight 'W_i' and the error calculated using MSE '∂E', respectively. Hence, by employing the Chinese remainder theorem in multilayer perceptron-based certificateless signcryption, secured vehicular communication is established with minimum cost and time. The pseudo-code representation of deep learning and Chinese remainder-based certificateless signcryption is given below.

Algorithm 1 – Deep learning and Chinese remainder-based certificateless signcryption

Input: Nodes '$N = (N_1, N_2, \ldots N_n)$', sender vehicle node ID 'SID', receiver vehicle node ID 'RID', data packets 'DP', data packets size 'DP_{size}', on-board unit 'OBU', road side unit 'RSU', trusted authority 'TA'

Output: computationally efficient and secure vehicular communication

Initialise pair-wise relative prime numbers 'p_i', 'p_j'
Initialise input layer size '$Size_{IL}$', output layer size '$Size_{OL}$'
Initialise parameters '$param$', security parameter 'l', data packet 'DP', learning rate 'λ'
Begin
For each node 'N' with sender vehicle node ID 'SID' and receiver vehicle node ID 'RID'
//Chinese remainder cryptosystem
Model the modular multiplicative inverse of the transmission range of a vehicle as in *Equation (1)*
Evaluate a pair of congruences between sender vehicles 'V_i' and receiver 'V_j' as in *Equation (2)*
Estimate the Hermite interpolation function as in *Equations (3), (4) and (5)*
Formulate the number of neurons as in *Equation (6)*
Obtain input vector mapping as in *Equation (7)*
//System parameters
Formulate system parameter as in *Equation (8)*
//Key generator
Formulate a trusted authority key generator as in *Equation (9)*
Generate private key 'PR_{SV}' and public key 'PB_{SV}' of the sender vehicle as in *Equation (10)*
Obtain receiver vehicle node credential as in *Equation (11)*
//Signcryption
Formulate the signcryption function 'SC' as in *Equation (12)*
//Unsigncryption
Formulate the unsigncryption function 'USC' to return the output 'y' as in *Equation (13)*
If '$y \geq 0$'
Perform secure data communication between vehicles
Else
Discard data communication between vehicles
End if
Evaluate the sigcrypted weighted sum as in *Equation (15)*
Update weight as in *Equation (16)*
End for
End

4. EXPERIMENTAL SETUP

Simulations of Chinese remainder cryptosystem-based multilayer perceptron certificateless signcryption (CRC-MPCS) for secure data communication in VANET and existing CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3] are simulated in NS2.34 simulator. In our work, the network simulation 3 is a simulation tool. NS-3 simulation function is a discrete-event network simulator to simulate networks and traffic between vehicles. The software tool is TCL 830, utilised in the proposed CRC-MPCS method. The results of proposed methods are evaluated with different parameters such as security level (in terms of data confidentiality), communication cost and signcryption verification processing time, data integrity and authentication accuracy. The network area is 0.5 km^2. The proposed CRC-MPCS considers 1,000 vehicle nodes, and data packets are taken from 80 to 800. Random waypoint mobility is used as a mobility mode for performing the simulation process. The transmission range is 300 m and transmission rate is 3 $Mbps$. The SNR is set as 20 dB. The simulation parameters and hyperparameters employed are provided in *Tables 1* and *2*.

Table 1 – Simulation parameters

S. No	Parameters	Description
1	Area	0.5 km^2
2	Transmission range	300 m
3	Transmission rate	3 $Mbps$
4	SNR	20 dB
5	Vehicle mobility model	Random Waypoint mobility
6	Number of vehicles	100, 200, 300, 400, 500, 600, 700, 800, 900 and 1,000
7	Data packets	80, 160, 240, 320, 400, 480, 560, 640, 720, 800
7	Simulation time	15 min
8	Message lifetime	1 min
9	Iterated simulations	10 times/scenario

Table 2 – Hyperparameter description

S. No	Hyper parameters	Description
1	Number of layers	3
2	Input layer size	9
3	Hidden layer size	2
4	Output layer size	1
5	Number of neurons in the input layer	9
6	Number of neurons in the hidden layer	7
7	Perceptron weight	0.2
8	Learning rate	0.5

With the aid of the above simulation and hyperparameter values, the results and discussions are given below.

5. RESULTS AND DISCUSSION

Simulations of Chinese remainder cryptosystem-based multilayer perceptron certificateless signcryption (CRC-MPCS) for secure data communication in VANET and CP-CPPHSC [1], IBS-CPPA [2], as well as CLSC [3], were presented using various metrics, namely communication cost, signcryption verification processing time, data confidentiality, data integrity and authentication accuracy.

5.1 Comparison results of communication cost or run time

The first and foremost significant metric to be analysed for secured vehicular communications is the communication cost or run time. This is owing to the reason that while performing certificateless signcryption, a notable amount of cost or time is incurred for holding the intermediary values. The communication cost is measured as given below.

$$CC = \sum_{i=1}^{n} V_i * Time\ [SC + USC] \tag{17}$$

From *Equation 17*, the communication cost 'CC' is calculated on vehicles in the experimental process 'V_i' and time taken for measuring the signcryption 'SC' and unsigncryption 'USC' process, respectively. It is calculated in milliseconds (ms). Comparisons of the communication cost using the proposed CRC-MPCS method and existing methods, CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3] are listed below in *Table 3*.

Table 3 – Comparison of communication costs

Vehicles	Communication cost (ms)			
	CRC-MPCS	**CP-CPPHSC**	**IBS-CPPA**	**CLSC**
100	1.6	1.95	2.25	2.55
200	1.68	2.05	2.55	3.25
300	1.95	2.45	3.45	4.55
400	2.15	2.85	4.15	5.25
500	2.45	3.15	4.55	5.75
600	2.95	4.55	5.55	6.65
700	3.55	5.15	5.95	7.15
800	4.15	5.55	6.45	7.65
900	4.75	6.15	6.95	7.95
1,000	4.95	6.75	8.35	9.85

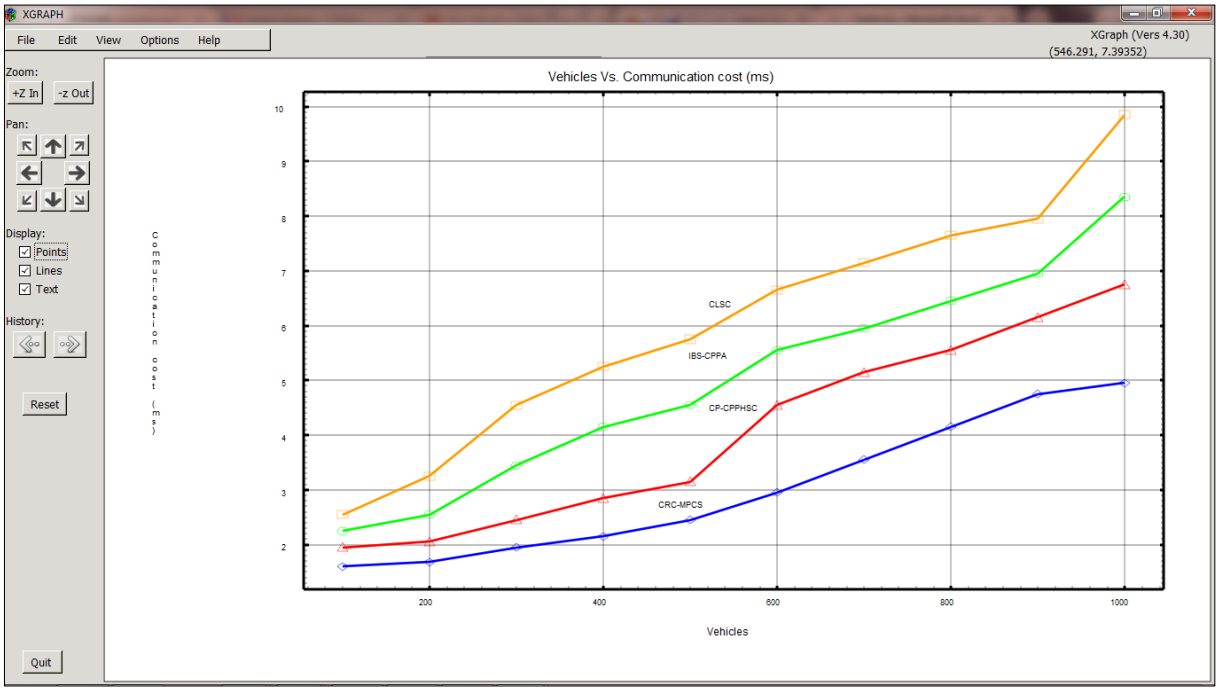

Figure 4 – Communication cost versus vehicles

Table 3 shows the performance analysis of communication costs for proposed and existing methods. To conduct experimental work, a different number of vehicles in the range of 100 to 1,000 is considered. The simulation is conducted by comparing the proposed CRC-MPCS method with existing methods such as CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3], respectively. From the table values, it is observed that the proposed CRC-MPCS method has a lower communication cost than the other existing methods.

Figure 4, given above, illustrates the graphical representation of communication cost for different numbers of vehicles ranging between 100 and 1,000. From the above figure, an increasing trend is said to be seen or to be more specific, increasing the vehicles enhances the number of data packets communicated among vehicles via a trusted authority. This, in turn, results in an increase in the corresponding communication cost. However, simulations performed with 100 vehicles saw communication cost of 1.6 ms using the proposed CRC-MPCS method and 1.95 ms, 2.25 ms and 2.55 ms employing the existing methods [1], [2] and [3], respectively. With this, the communication cost using the CRC-MPCS method was said to be reduced upon comparison with [1], [2] and [3]. This helps to show that the proposed CRC-MPCS method has a significantly shorter time. It is achieved using two aspects, signcrypt and verification, followed in the proposed CRC-MPCS method. The proposed CRC-MPCS method enhances network security via the Chinese remainder cryptosystem. Based on this, only authorised users or vehicle nodes can access the data packets, as well as unauthorised users or vehicle nodes. The CRC-MPCS method of computation cost is minimised as 24%, 40% and 50% compared with CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3], respectively.

5.2 Comparison results of signcryption verification processing time

The second factor of importance for secure vehicular communication is the signcryption verification process time. Signcryption verification processing time is measured because faster verification increases the speed of signcryption process. The signcryption verification process time is mathematically stated as given below.

$$SVPT = \sum_{i=1}^{n} V_i * Time[USC] \tag{18}$$

In (18), signcryption verification processing time '$SVPT$' is calculated on vehicles in the experimental process 'V_i' actual time consumed in performing unsigncryption '$Time[USC]$'. It is calculated in milliseconds (ms). Signcryption verification processing times using the proposed CRC-MPCS method and existing methods, CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3] are listed below in *Table 4*.

Table 4 – Comparison of signcryption verification processing time

Vehicles	Signcryption verification processing time (ms)			
	CRC-MPCS	**CP-CPPHSC**	**IBS-CPPA**	**CLSC**
100	0.85	0.95	1.15	1.35
200	0.92	1.05	1.25	1.45
300	1.15	1.35	1.55	1.75
400	1.25	1.55	1.85	2.05
500	1.35	1.7	2.15	2.35
600	1.45	1.9	2.45	2.65
700	1.55	2.15	2.7	2.95
800	1.65	2.35	2.95	3.25
900	1.85	2.45	3.15	3.75
1,000	2.2	2.7	3.35	3.95

The experimental performances of signcryption verification processing time for determining secure data communication in VANET using proposed and existing techniques are listed in *Table 4* above. For experimental purposes, different vehicles are considered in the range of 100 to 1,000 for efficient performance analysis.

Here, the proposed CRC-MPCS method is compared with the existing methods named CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3], respectively. From the table value, it is illustrative that the time taken for determining secure communication or discarding communication using the proposed CRC-MPCS method is lower when compared to other existing methods. Based on the table value, the graph is drawn below to analyse the performance of the proposed method.

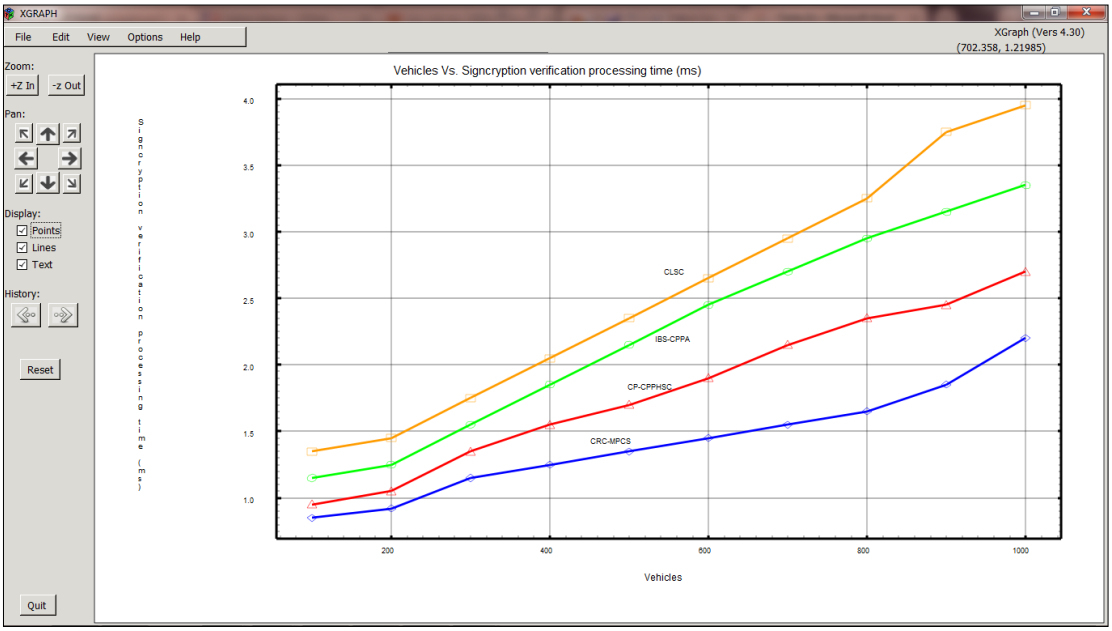

Figure 5 – Signcryption verification processing time versus vehicles

Figure 5, given above, shows the graphical representation of signcryption verification processing time using the four methods, CRC-MPCS, [1], [2] and [3]. The CRC-MPCS method employs less time for verifying the validity of the receiver vehicle node compared with [1], [2] and [3]. Owing to the fact that the network transmission is found to be large, numerous unauthorised users are said to be engaged in heterogeneous message communication between senders and receivers. The CRC-MPCS method is developed to secure data transmission using a shorter verification processing time. CRC-MPCS employs a signcryption process that applies private key, secret key and public key on deep learning. The Hermite interpolation function is employed for converting the original data packet. Also, these processes are performed separately in two different layers for the sender and receiver vehicle node. Therefore, the proposed CRC-MPCS method enhances secure vehicular communication among senders and receivers with lesser overhead. Besides, multiple messages were handled via the input layer of a multilayer perceptron that in turn reduces the signcryption verification processing time by 20%, 35% and 43% compared to existing CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3], respectively.

5.3 Comparison results of data confidentiality

Finally, the data confidentiality rate is measured. The data confidentiality rate refers to the percentage of data packets sent by the sender vehicle nodes that were received by the intended recipient without any compromise in confidentiality. To be more specific, data confidentiality refers to the ratio of the number of data packets of sender vehicle nodes being protected from unauthorised users with respect to the total number of data packets involved in the simulation process. It is computed as

$$DC = \frac{DP_{prot}}{DP} * 100 \tag{19}$$

From *Equation 19*, data confidentiality 'DC' is evaluated based on the data packet being protected from the unintended recipient 'DP_{prot}' to the overall data packets 'DP' involved in the simulation process. Data confidentiality is calculated by percentage (%). Finally, a comparative analysis of the data confidentiality rate using the proposed CRC-MPCS method and existing methods, CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3], is listed below in *Table 5*.

Table 5 – Comparison of data confidentiality

Vehicles	Data confidentiality (%)			
	CRC-MPCS	**CP-CPPHSC**	**IBS-CPPA**	**CLSC**
100	**94.35**	**90.25**	**89.15**	**86.55**
200	93.25	89.05	88.15	85.25
300	**93**	**88.25**	**85.35**	**82.35**
400	92.25	86.35	84.25	79.25
500	**91.55**	**85.25**	**82.35**	**76.25**
600	91	84.35	80	74.35
700	**89.55**	**82.15**	**79**	**73.15**
800	89	80.35	78.35	70
900	**88.55**	**79.35**	**76.55**	**68.35**
1,000	88	79	73.15	66.25

Table 5 shows the performance analysis of the data confidentiality rate for proposed and existing methods with respect to the different numbers of vehicles. Vehicles in the range of 100 to 1,000 are used to conduct experimental work. The simulation is conducted by comparing the CRC-MPCS method with existing methods such as CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3]. From the above result, it is observed that the proposed CRC-MPCS method improves the data confidentiality rate more than other existing methods.

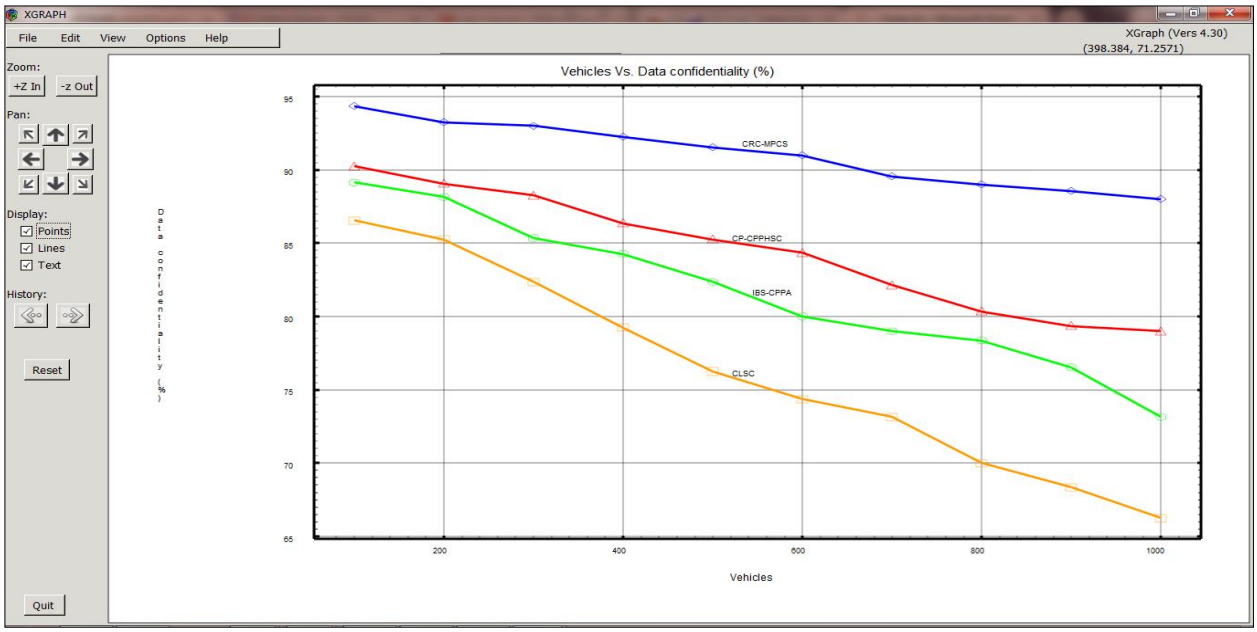

Figure 6 – Data confidentiality versus vehicles

Figure 6 explains the data confidentiality rate of 1,000 various vehicles for ensuring smooth and secure vehicular communication. From the figure, the data confidentiality rate decreases with the increase in the number of messages being sent. The CRC-MPCS method enhances the data confidentiality rate. The reason behind this is that a multilayer perceptron-based certificateless sign encryption process was utilised to allocate data packets between the sender vehicle node and receiver vehicle by employing secret key and public key generation by the trusted authority. In addition, the error rate is obtained and based on the estimated and actual error weight update is performed using an if-then condition. Upon satisfaction of the condition, validity credentials are ensured and vice versa. This helps to further enhance the data confidentiality rate using the proposed CRC-MPCS method and enhances VANET protection. As a result, the data confidentiality rate is improved by 8%,12% and 20% when compared to the CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3].

5.4 Comparison results of data integrity rate

The data integrity rate is an important parameter to secure data communication among vehicle nodes in VANET. The data integrity is defined as the number of data packets of sender vehicle nodes that are not altered by unauthorised users, to the total number of data packets. It is computed as given below.

$$DIR = \frac{DP_{NA}}{DP} * 100 \tag{20}$$

In *Equation 20*, the data integrity 'DIR' is estimated. 'DP_{NA}' denotes the data packets of sender vehicle nodes not altered, and 'DP' represents the total data packets. It is estimated in terms of percentage (%). *Table 6* demonstrates the comparison of data integrity rates with four dissimilar methods, such as the proposed CRC-MPCS method and existing methods, CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3], respectively.

Table 6 – Comparison of data integrity rate

Vehicles	Data integrity rate (%)			
	CRC-MPCS	**CP-CPPHSC**	**IBS-CPPA**	**CLSC**
100	95.15	91.25	87.45	83.65
200	**94.45**	**86.75**	**83.75**	**81.35**
300	92.75	84.65	81.55	78.55
400	**90.85**	**82.85**	**79.15**	**76**
500	90	81.45	76.35	73.55
600	**89.75**	**80.15**	**74.55**	**71.85**
700	88.45	78.55	73.75	70
800	**87.15**	**77.75**	**72**	**69.45**
900	86.65	77	70.85	67.55
1,000	**84.75**	**76.25**	**70**	**66.65**

Table 6 describes the comparative result analysis of data integrity rate with respect to different numbers of vehicles in the range of 100 to 1,000 using the proposed and existing methods. From the table, while increasing the input vehicles for secure communication, the data without any modification gets varied. The above table values provide the result analysis of the data integrity rate by comparing the CRC-MPCS method with existing CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3].

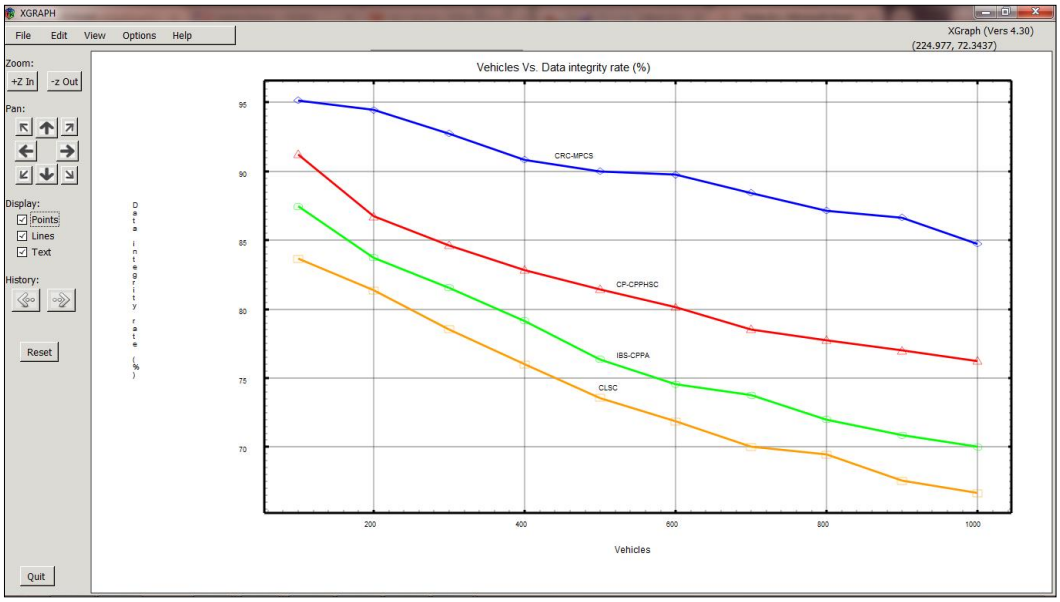

Figure 7 – Data integrity rate versus vehicles

Figure 7 portrays the data integrity rate based on the number of vehicles ranging from 100 to 1,000 nodes. The data integrity rate of the proposed CRC-MPCS method with respect to distinct data packets ranging between 100 and 1,000 sent by 1,000 dissimilar vehicle nodes in VANET is significantly improved. Then, the data integrity rate is 84.75%, 76.25%, 70% and 66.65% using the proposed CRC-MPCS method and existing [1], [2] and [3], respectively. All the results provided in *Figure 7* confirm that the proposed CRC-MPCS method significantly outperforms the other three methods. This is because the CRC-MPCS method uses deep learning-based certificateless signcryption to perform secure communication based on key generation, signcryption and unsigncryption. In the key generation, a session key pair is generated for each transaction. In signcryption, the encryption and signature generation are performed. Therefore, the data were not altered by any intruders. This, in turn, increases data integrity. As a result, data integrity rate is enhanced by 11%, 17% and 22% when considering the CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3].

5.5 Comparison results of authentication accuracy

The authentication accuracy is defined as the measure of the number of vehicles that are correctly authenticated as authorised or unauthorised, to the total number of vehicles. The authentication accuracy is evaluated in terms of percentage (%). It is calculated by

$$AA = \frac{Number\ of\ vehicles\ that\ are\ correctly\ authenticated\ as\ authorised\ or\ unauthorised}{Total\ number\ of\ vehicles} * 100 \quad (21)$$

In *Equation 21*, authentication accuracy 'AA' is computed. It is measured in terms of percentage (%). *Table 7* reveals the comparison of authentication accuracy with the proposed CRC-MPCS method and existing methods, CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3], respectively.

Table 7 – Comparison of authentication accuracy

Vehicles	Authentication accuracy (%)			
	CRC-MPCS	**CP-CPPHSC**	**IBS-CPPA**	**CLSC**
100	**93.45**	**86.25**	**82.35**	**79.55**
200	91.65	84.45	80.65	76.65
300	**93.45**	**86.25**	**81**	**77**
400	92	83.85	78.45	74.15
500	**91.55**	**81**	**76**	**72.05**
600	90	78.15	73.35	69
700	**92.25**	**80.55**	**76.15**	**71.55**
800	90.45	79.35	72.75	68.25
900	**89.65**	**78**	**71.85**	**67.45**
1,000	91	80.25	73	68

The experimental performances of authentication accuracy for detailed experiments using proposed and existing methods are listed in *Table 7* above. For experimental purposes, a different number of vehicles that range from 100 to 1,000 is considered from a dataset.

Figure 8 demonstrates the comparative analysis of authentication accuracy for a varied number of vehicles. As shown in the reported results, the authentication accuracy of the proposed CRC-MPCS method is higher than the other three existing methods, CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3], respectively. For example, 100 vehicles are considered for evaluating the authentication accuracy. By applying a CRC-MPCS method, 93 vehicles are correctly authenticated, and their authentication accuracy is 93.45%. Similarly, CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3] correctly identify 86, 82 and 79 vehicles, and their accuracy is

86.25%, 82.35% and 79.55%, respectively. The comparison results prove that the authentication accuracy is found to be increased by 12%, 19% and 28% as compared to existing methods [1] [2] [3], respectively. With the application of deep learning-based certificateless signcryption, authorised users are identified. Based on key generation, signcryption and unsigncryption, valid users are authorised. Thus, correctly authorised users are allowed to secure data communication. This helps to enhance the performance of authentication accuracy.

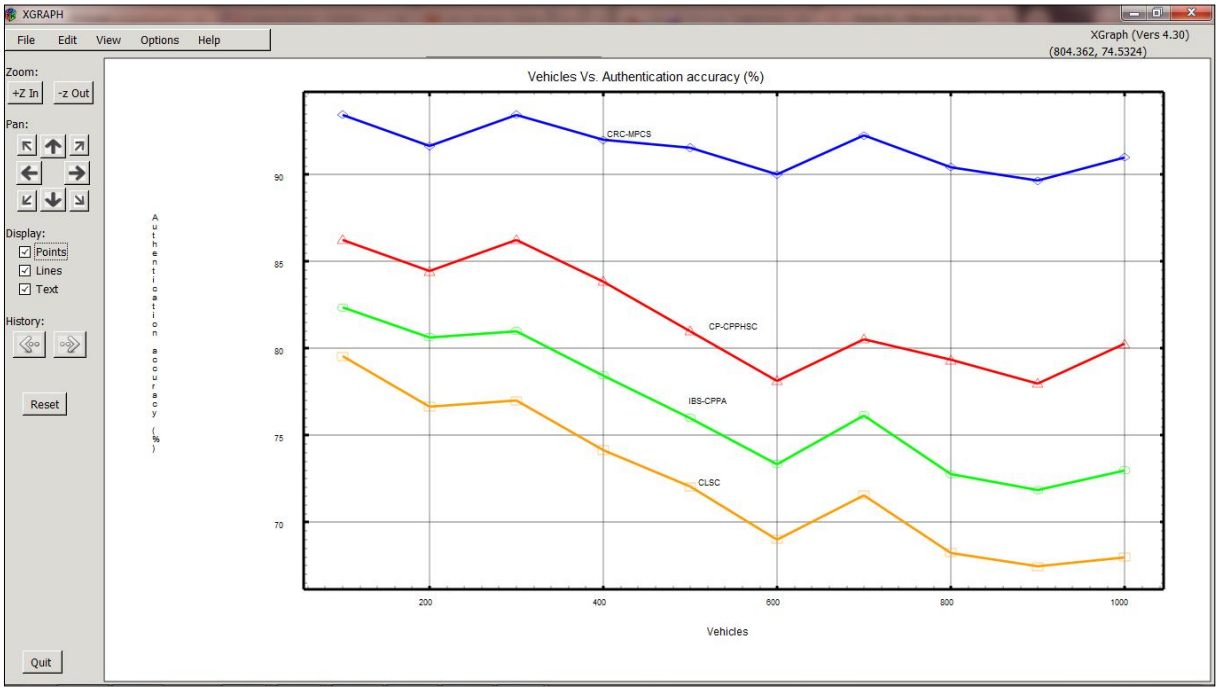

Figure 8 – Authentication accuracy versus vehicles

5.6 Comparison results of memory consumption

The memory consumption (MC) is defined as the amount of memory required for secure VANET communication while taking into account the number of vehicle nodes from the given dataset. The mathematical expression for determining the memory consumption is given by the following equation:

$$MC = V_i \times m\,[SC + USC] \tag{22}$$

where V_i denotes the vehicles, $m\,[SC + USC]$ indicates memory taken to estimate signcryption 'SC' and unsigncryption 'USC' process, respectively. The memory consumption is determined in terms of kilobytes (KB). The comparisons of the memory consumption using the proposed CRC-MPCS method and existing methods, CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3] are listed below in *Table 8*.

Table 8 – Comparison of memory consumption

Vehicles	Memory consumption (KB)			
	CRC-MPCS	CP-CPPHSC	IBS-CPPA	CLSC
100	22	26	30	32
200	**24**	**29**	**34**	**37**
300	27	32	37	40
400	**31**	**37**	**42**	**45**
500	34	41	50	53
600	**38**	**47**	**55**	**58**
700	42	52	61	64
800	**46**	**55**	**67**	**69**
900	48	59	69	73
1,000	**52**	**63**	**71**	**75**

Table 8 shows the performance analysis of memory consumption with respect to the different number of vehicles in the range from 100 to 1,000.

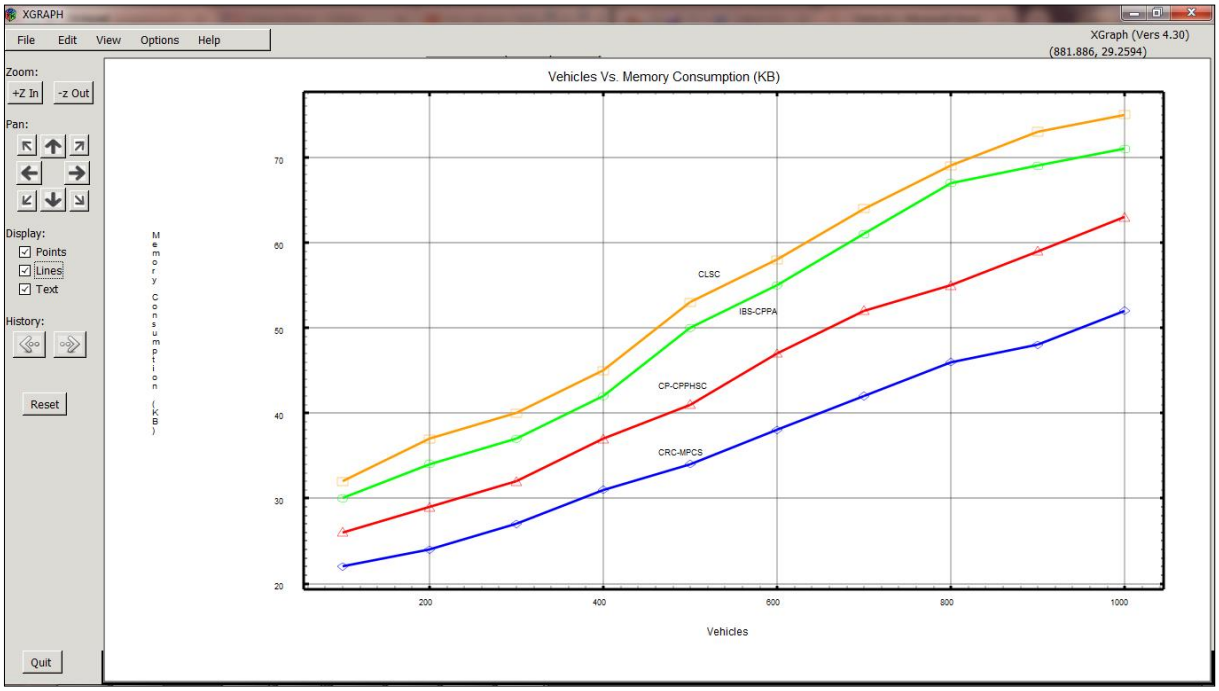

Figure 9 – Memory consumption versus vehicles

Figure 9 provides the measurement of the memory consumption based on the number of vehicles taken from the given dataset for four different methods. From *Figure 8*, the number of vehicles taken on the horizontal axis, and the memory consumption are shown on the vertical axis. The graphical plot indicates that the proposed CRC-MPCS method minimises memory consumption compared to the other four existing methods. This is due to the effective performance of two significant processes, such as signcryption and unsigncryption, using a multilayer perceptron. Thus, the proposed CRC-MPCS method efficiently minimises memory consumption by 17%, 29% and 33% when compared to CP-CPPHSC [1], IBS-CPPA [2] and CLSC [3], respectively.

6. CONCLUSION

Chinese remainder cryptosystem-based multilayer perceptron certificateless signcryption (CRC-MPCS) is developed for enhancing secure data in VANET. The CRC-MPCS method achieves multiple data packets distribution using a lower communication cost. The sender vehicle node in multilayer perceptron-based certificate less environment performs signcryption with private and public keys of the sender and receiver. In the CRC-MPCS method, the certificateless signcryption achieves encryption and digital signature, where encryption is an efficient method to encrypt a file as well as transform plain text into ciphertext. Next, a digital signature is confirmed in the CRC-MPCS method as well, and unsyncryption is achieved to produce the secret key. It aids in guaranteeing VANET privacy. Besides, the Chinese remainder cryptosystem is employed by the CRC-MPCS method for decreasing memory consumption, therefore contributing to better communication cost. A single syncrption operation with multiple bits via the Hermite interpolation function is utilised to highly secure the broadcasted data packet in the CRC-MPCS method. Experimental evaluation is performed with various metrics, namely communication cost, signcryption verification processing time, data confidentiality, data integrity and authentication accuracy. The CRC-MPCS method enhances data confidentiality, data integrity and authentication accuracy with minimal communication cost, lesser signcryption verification processing time and higher data confidentiality than the state-of-the-art methods. In future work, the research will be carried out using a security framework to consider data loss for secured data transmission in VANET. Thus, the future enhancement will focus on overcoming data security to perform authentication to avoid unauthorised nodes for data communication.

REFERENCES

[1] Ali I, et al. Bilinear Pairing-Based hybrid signcryption for secure heterogeneous vehicular communications. *IEEE Transactions on Vehicular Technology*. 2021;70(6):5974–89. DOI: 10.1109/tvt.2021.3078806.

[2] Ali I, Lawrence T, Li F. An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs. *Journal of Systems Architecture*. 2019;103:101692. DOI: 10.1016/j.sysarc.2019.101692.

[3] Hongzhen D, Qiaoyan W, Shanshan Z, Mingchu G. A Pairing-Free certificateless signcryption scheme for vehicular ad hoc networks. *Chinese Journal of Electronics*. 2021;30(5):947–55. DOI: 10.1049/cje.2021.07.006.

[4] Pan J, et al. Secure data sharing scheme for VANETs based on edge computing. *EURASIP Journal on Wireless Communications and Networking*. 2019;2019(1). DOI: 10.1186/s13638-019-1494-1.

[5] Thumbur G, et al. Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks. *IEEE Internet of Things Journal*. 2020;8(3):1908–20. DOI: 10.1109/jiot.2020.3019304.

[6] Manivannan D, Moni SS, Zeadally S. Secure authentication and privacy-preserving techniques in vehicular ad-hoc NETworks (VANETs). *Vehicular Communications*. 2020;25:100247. DOI: 10.1016/j.vehcom.2020.100247.

[7] Al-Shareeda MA, Anbar M, Manickam S, Hasbullah IH. Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Access*. 2021;9:113226–38. DOI: 10.1109/access.2021.3104148.

[8] Wu TY, Lee Z, Yang L, Chen CM. A provably secure authentication and key exchange protocol in vehicular ad hoc networks. *Security and Communication Networks*. 2021;2021:1–17. DOI: 10.1155/2021/9944460.

[9] Sarkar A, Dey J, Bhowmik A. Multilayer neural network synchronized secured session key based encryption in wireless communication. *Indonesian Journal of Electrical Engineering and Computer Science*. 2019;14(1):169. DOI: 10.11591/ijeecs.v14.i1.pp169-177.

[10] Zhao C, et al. A secure and efficient certificateless content extraction signature with privacy protection. *PLoS ONE*. 2021;16(11):e0258907. DOI: 10.1371/journal.pone.0258907.

[11] Kong Q, Su L, Ma M. Achieving Privacy-Preserving and verifiable data sharing in vehicular fog with blockchain. *IEEE Transactions on Intelligent Transportation Systems*. 2020;22(8):4889–98. DOI: 10.1109/tits.2020.2983466.

[12] Ali U, et al. Enhanced lightweight and secure certificateless authentication scheme (ELWSCAS) for Internet of Things environment. *Internet of Things*. 2023;24:100923. DOI: 10.1016/j.iot.2023.100923.

[13] Yang R, et al. A privacy-preserving data aggregation system based on blockchain in VANET. *Blockchain Research and Applications*. 2024;5(3):100210. DOI: 10.1016/j.bcra.2024.100210.

[14] Khan MA, et al. Securing internet of drones with identity-based proxy signcryption. *IEEE Access*. 2021;9:89133–42. DOI: 10.1109/access.2021.3089009.

[15] Ren Y, et al. Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks. *Journal of Information Security and Applications*. 2021;58:102698. DOI: 10.1016/j.jisa.2020.102698.

[16] Mohamed TM, Ahmed IZ, Sadek RA. Efficient VANET safety message delivery and authenticity with privacy preservation. *PeerJ Computer Science*. 2021;7:e519. DOI: 10.7717/peerj-cs.519.

[17] Di C, Wu W. A novel identity-based mutual authentication scheme for vehicle ad hoc networks. *Wireless Communications and Mobile Computing*. 2022;2022:1–13. DOI: 10.1155/2022/7881079.

[18] Rehman M, et al. A lightweight nature heterogeneous generalized signcryption (HGSC) scheme for named data networking-enabled internet of things. *Wireless Communications and Mobile Computing*. 2020;2020:1–20. DOI: 10.1155/2020/8857272.

[19] Zhou C, Gao G, Cui Z. Certificateless signcryption in the standard model. *Wireless Personal Communications*. 2016;92(2):495–513. DOI: 10.1007/s11277-016-3554-8.

[20] Xu SW,et al. LB-CLAS: Lattice-based conditional privacy-preserving certificateless aggregate signature scheme for VANET. *Vehicular Communications*. 2024;50:100843. DOI: 10.1016/j.vehcom.2024.100843.

[21] Li L, et al. An efficient and provably-secure certificateless proxy-signcryption scheme for electronic prescription system. *Security and Communication Networks*. 2018;2018:1–11. DOI: 10.1155/2018/7524102.

[22] Yu H, Yang B. Pairing-free and secure certificateless signcryption scheme. *The Computer Journal*. 2017;60(8):1187–96. DOI: 10.1093/comjnl/bxx005.

[23] Zia M, Ali R. Cryptanalysis and improvement of an elliptic curve based signcryption scheme for firewalls. *PLoS ONE*. 2018;13(12):e0208857. DOI: 10.1371/journal.pone.0208857.

[24] Zhang B, Jia Z, Zhao C. An efficient certificateless generalized signcryption scheme. *Security and Communication Networks*. 2018;2018:1–11. DOI: 10.1155/2018/3578942.

[25] Kamil IA, Ogundoyin SO. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks. *Journal of Information Security and Applications*. 2018;44:184–200. DOI: 10.1016/j.jisa.2018.12.004.