I. J. Computer Network and Information Security, **2024, 1, 113-122**
Published Online on February 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.01.09

An Enhancement of Identity Based Conditional Privacy-preserving Authentication Process in Vehicular Ad Hoc Networks

K. Lakshmi Narayanan
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Chennai, Tamilnadu, India
E-mail: lk6685@srmist.edu.in
ORCID iD: https://orcid.org/0000-0002-8416-340X

R. Naresh*
Department of Networking and Communications, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Chennai, Tamilnadu, India
E-mail: nareshr@srmist.edu.in
ORCID iD: https://orcid.org/0000-0001-6970-5322
*Corresponding author

Received: 17 August 2022; Revised: 19 September 2022; Accepted: 21 October 2022; Published: 08 February 2024

Abstract: In general, Vehicular Ad hoc Networks (VANETs) are permitting the communication between one vehicle with neighboring vehicles, infrastructure, and Road-Side Unit (RSU). In this, vehicle platoon is commonly known as the vehicle driving pattern it categorizes the batching of the vehicle in the on the trot fashion. It has been reviewed as an effective resolution to mitigate the reduction in traffic blockage and to widen the opulence of the travel. However, the malicious activities of any unauthorized person in VANET are increased the damage to authorized vehicles. In this manuscript, the Identity based Conditional Privacy-Preserving Authentication (ID-CPPA) signature scheme is proposed to detect the malignant command vehicle very efficiently by the consumer vehicle. In this, the proposed ID-CPPA method uses one-way hash functions for improving the efficiency of Road-Side Unit (RSU) signing and verification of a messages. In order to provide better concealment to the vehicle, Phase Truncated Fourier Transform based asymmetric encryption algorithm (PTFT-AE) is proposed. Thus, the proposed ID-CPPA-PTFT-AE approach has achieved 28.96%, 37.58%, 31.36% higher security rate and 25.8%, 37.9%, 42.6% lower delay than the existing MPDC-LPNS, PPSR-GS, and WCAA-TST methods respectively.

Index Terms: Vehicular Ad Hoc Networks, Vehicle Platoon, Privacy-preserving Authentication, Asymmetric Encryption Algorithm.

1. Introduction

The drastic increase in vehicle possession led to many evaluative communal difficulties namely traffic jam, accident and air pollution. To accord with this methodology a platoon-based driving fashion also known as vehicle platoon has gained significant outcome in past years. Basically, vehicle platoon comprises of the command vehicle and the consumer vehicle. The command vehicle performs the driving classically the rest of the consumer vehicle follow the same fashion [1,2]. Rather than traditional driving method the vehicle platoon technique provides comfort to the people. Later on, with the reduction in air forces it is capable of reducing the consumption of the fuel in the vehicle and the air pollution [3].

Though vehicle platoon has played a significant role there are also some disadvantages [4]. Henceforth the consumer vehicle gives entire driving control to the command vehicle, the driving pattern and the route are decided by the command vehicle. Very few commands vehicle may consciously or unconsciously lower the quality of the drivers or during dangerous situation they are misled. Due to this all-command vehicle are examined before joining the vehicle platoon [5].

To resolve this issue all the consumer vehicles should follow the trust value and the accumulation of the reputed value near to that of the feedback given by the consumer vehicle. Another criticizing issue is of maintaining the privacy

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

of the consumer vehicle. Although through epithets and undesignated conferment are used to obscure the identity of the driver the location of the vehicle may still be revealed by the trust value [6]. The purpose of VANET is to improve the privacy and urban and road traffic management that provide facilities to the passenger [7]. The messages are transmitted through the network that should be highly secure and confidential. However, security risks in the VANET network are the most important limitations. Because, the unauthorized or unwanted person interruption is leading the authorized vehicle damages. Thus, to overcome these issues, Identity based Conditional Privacy-Preserving Authentication (ID-CPPA) signature with Phase Truncated Fourier Transform based asymmetric encryption algorithm (PTFT-AE) method is proposed. The main objective of the proposed approach is to enhance the security of the VANET system using ID-CPPA-PTFT-AE approach.

Beneath comes the encapsulation of the entire work to be carried out,

- In this manuscript, Identity based Conditional Privacy-Preserving Authentication (ID-CPPA) signature with Phase Truncated Fourier Transform based asymmetric encryption algorithm (PTFT-AE) method is proposed for enhancing the security of VANET network.
- Initially, the Identity based Conditional Privacy-Preserving Authentication (ID-CPPA) signature model [8] is developed to detect the malicious activities in the network.
- Additionally, Phase Truncated Fourier Transform based asymmetric encryption algorithm (PTFT-AE) [9] is proposed for improving the maintenance of the consumer vehicles privacy.
- The vehicle verification protocol PTFT-AE is designed in such a fashion that only authorized vehicle can pass through the entry provided.
- The simulation of the model is done in network simulator and the performance metrics are calculated.
- Finally, the proposed ID-CPPA-PTFT-AE approach is compared with existing methods like multiparty delegated computation (MPDC) with lightweight privacy-preserving based real-time intelligent traffic navigation scheme (LPNS) (MPDC-LPNS), privacy-preserving signRecryption protocol (PPSR) with Group Signature (GS) (PPSR-GS), and Weight-based Conditional Anonymous Authentication (WCAA) with Two-Step Tracing (TST)(WCAA-TST) methods respectively.

The remaining segments of this manuscript are organized as: segment 2 portrays the related works, segment 3 describes the proposed framework, and segment 4 demonstrates the obtained outcomes. Finally, segment 5 concludes this manuscript.

2. Related Works

In general, the execution of the command vehicle is analyzed by the assessment given by the consumer vehicle. Basically, the consumer vehicle command may get varied due to several reasons such as various driving nature, false prediction and lack of observing capability. The traditional method such as voting or calculating the average may resolve these issues. Numerous works were presented previously in the literature related to privacy in VANET; a few works are reviewed here,

Mirsadeghi et al., [10] have presented the Trust based Authentication Approach (TBA) for the clustered VANET. In this, the developed approach was effectively identifying the malicious nodes in VANET and diminished the overhead as well as delay. Additionally, it develops the stable and trustworthy clusters for enhancing the stability of the whole network. For that, the trust degree was calculated for every vehicle by conjoining the value of trust among the vehicles and RSU. Finally, it enhanced the accuracy and packet delivery ratio for detecting malicious nodes but the processing time of the model was high.

Zhou et al., [11] have presented multiparty delegated computation (MPDC) with lightweight privacy-preserving based real-time intelligent traffic navigation scheme (LPNS). In this, the developed model was forecasted the optimal driving route with in a shortest time period. Thus, it provides high efficiency as well as accuracy but the model was high delay.

Kanchan et al., [12] have presented privacy-preserving signRecryption protocol (PPSR) with Group Signature (GS) for detecting intrusion of unauthorized and unwanted person in VANET. In this, the signcryption process improves the effectiveness of the model, re-encryption process enhanced the robustness, and privacy was attained by group signature model. However, the accuracy of the model was low.

Zhong et al., [13] have presented Weight-based Conditional Anonymous Authentication (WCAA) with Two-Step Tracing (TST) for solving inherent issues in VANET. In this, the vehicles are prioritized based on weighted values. Also, TST process punishes the vehicles in the network whose weight was reduced below the particular threshold. It was achieved better outcomes in computation cost but the privacy of the model was low.

Gyawali et al., [14] have presented Privacy-preserving based Misbehavior Detection system (PPMD) for securing vehicular communication. This model was detecting the misbehavior for improving the vehicle privacy. Additionally, additive homomorphic properties are used for transmitting the feedbacks from encrypted weights to vehicles. Thus, the model was attained better performance in computation cost but the accuracy of the model was low.

Nandy et al., [15] have presented enhanced lightweight and secure authentication protocol (ELSAP) for V2V

Communication in VANETs. Furthermore, two or more vehicles can securely perform mutual authentication, proven by Burrow–Abadi–Needham (BAN) logic. The result of this model shows that better communication cost and computational cost but it has attained lower security efficiency.

Eftekhari [16] have presented security-enhanced three-party pairwise shared key agreement protocol for fog-based vehicular communications. In addition to informal justifications, this protocol also verified formally by utilization of reputable "ProVerif" tool. In particular, comparative evaluations are presented in terms of security metrics. Thus, it provides 23.65% improvement in computational cost but the delay of the model was high.

Yang et al., [17] have presented an efficient blockchain-based batch verification scheme for VANETs using the Elliptic Curve Cryptography (ECC). It also provides security analysis to show its ability to resist current known attacks. Besides, it implemented corresponding blockchain system and the performance analysis shows that it is suitable for VANETs. However, the computational cost of this model was high.

Coruh and Bayat, [18] have presented fast and secure mechanism for revocation checking, processing and PKI key pair updating called the Enhanced Secure Authentication and Revocation (ESAR) scheme for VANETs. The ESAR V2V authentication method applies Keyed-Hash-based Message Authentication Code (H-MAC) cryptogram validation for On-Board-Unit (OBU) revocation checks instead of the CRL search. It improved the system performance, durability and also attack resistance but the packet delivery was low.

Abassi et al., [19] have presented trust-based security scheme for message exchange (TSME) in a VANET. VANET Grouping Algorithm (VGA) has the suitable clustering algorithm organizing the network into groups with elected Group-Heads and trust management scheme dealing with vehicles' reputations. Also, a formal specification of the scheme using an inference system, and conducted a formal validation to assess its completeness and soundness. The results obtained showed that the veracity of exchanged messages are formally sound and complete but the security enhancement was low.

3. Proposed ID-CPPA-PTFT-AE Methodologies

In this manuscript, the Identity based Conditional Privacy-Preserving Authentication (ID-CPPA) signature scheme with effective encryption method is proposed to detect the malignant command vehicle very efficiently by the consumer vehicle. In order to provide better concealment to the vehicle, Phase Truncated Fourier Transform based asymmetric encryption algorithm (PTFT-AE) is proposed. Thus, the security analysis of the proposed ID-CPPA-PTFT-AE approach shows high performance for enhancing the privacy of vehicles in the network. The block diagram representation of the proposed methodology is given in fig. 1.

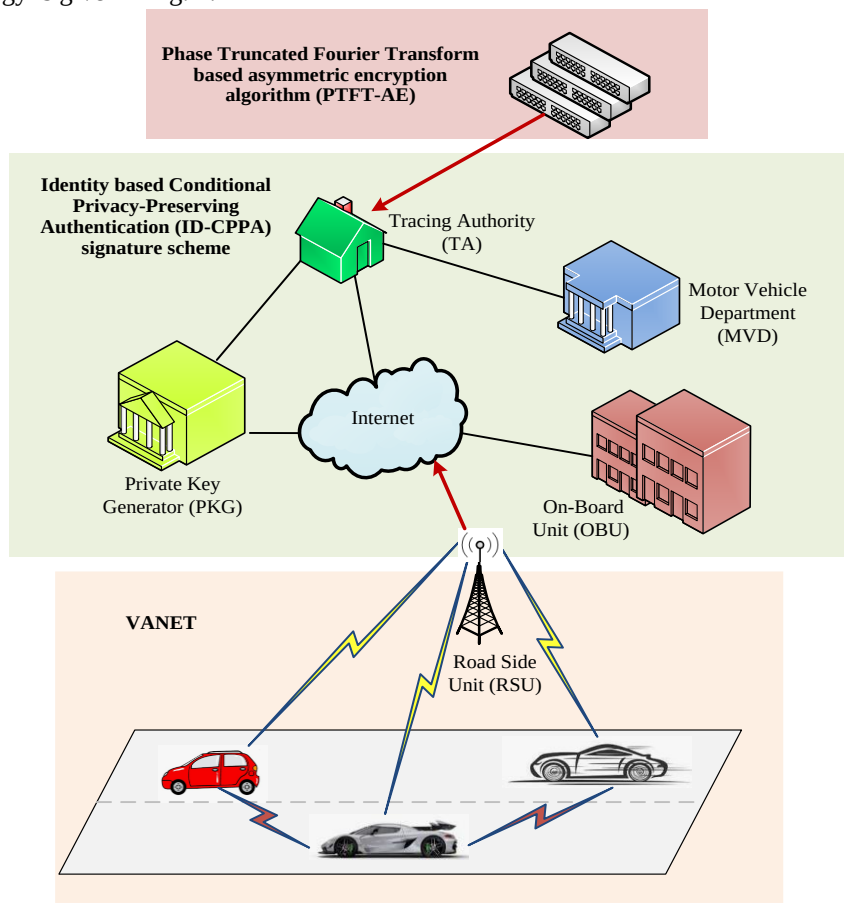

Fig.1. Block diagram representation of the proposed ID-CPPA-PTFT-AE approach

3.1. ID-CPPA Signature Model

In this work, Identity based Conditional Privacy-Preserving Authentication (ID-CPPA) signature scheme is proposed for enhancing the vehicle communication by detecting the malignant command vehicle. The proposed ID-CPPA approach is very effective model, easy to use and less complexity, which is processed based on several processes that are, setup, pseudo-identity Generation (*PIdGen*), Key generation (*KeyGen*), MsgSign, SignVerify and BigSign Verify.

A. Setup Initialization

The setup of the proposed ID-CPPA approach is calculated by tracing authority (TA) and Private Key generator (PKg) that is used the input as security parameter. It generates the additive cyclic group g_1, multiplicative cyclic group g_2 and bilinear map $b: g_1 \times g_1 \to g_2$ of prime order p. Subsequently, TA and PKg is initially selects the generator K of g_1 in a random manner and compute $e(K,k) = g$. After that, TA and PKg can selects the random integers θ, φ belongs to Z_p^* that is calculated as $TR_{pub} = \theta K, PKg_{pub} = \varphi K$, which is considered as master public key. Moreover, the general hash functions h_1, h_2, h_3 based on uniform cryptography is selected by TA and PKg that is denoted as $h_1, h_2, h_3 : \{0,1\}^* \to Z_p^*$. The hash functions are used for generating the pseudo-identity (PId_t) for a vehicle V_t. Finally, the initialized setup parameters are published across the VANET.

B. Pseudo-identity Generation (*PIdGen*)

In this step, the vehicle V_t is tried to join the VANET that transmit the information of its real identity $RId_t \in Z_p^*$ to TA. Thus, TA can register the vehicle V_t through pseudo-identity (PId_t), which have following process,

- Initially, random integer $\alpha_t \in Z_p^*$ is generated by the vehicle V_t with real identity RId_t. Also, the vehicle V_t calculates $PId_{t,V} = \alpha_t K$ and transmits $(RId_t, PId_{t,V})$ to TR in a secure way.
- Subsequently, the TR verifies the real identity of vehicle and calculate the value is given in eqn. (1). If the verification of vehicle fails then TR reject the request.

$$PId_{t,TR} = RId_t \oplus h\left(\theta PId_{t,V}, TR_{pub}\right) \tag{1}$$

where, θ denotes the master private key of TR.

C. Key Generation (*KeyGen*)

The time stamp is analyzed when the private key generator receives the PId_t from TR that is given as eqn. (2)

$$PId_t = \left(PId_{t,V}, PId_{t,T}, T_t\right) \tag{2}$$

where T_t denotes the PId valid time period. In this, if $\Delta T \geq T_r - T_t$ (ΔT -difference among the clock period of vehicle and local clock, T_r -arrival time period and T_t departure time) then private key generator have performing by following functions. 1) Random integer $\gamma_t \in Z_p^*$ is selected by PKG. 2) PKG sets the private key as $S_t = \left(A_t, B_t\right)$ that is transmitted to the vehicle V_t through highly secured channel. Where, $A_t = \left(\gamma_t + d_t s\right) \bmod P$ and $B_t = \left(\frac{\gamma_t}{s} + d_t\right) PId_{pub}$, $d_t = h_1\left(PId_t, \gamma_t, PId_{pub}\right)$

D. MsgSign

Here, every traffic based messages are signed by vehicle V_t and that are send to RSU. Initially, an integer is $\delta_t \in Z_p^*$ randomly selected by vehicle V_t. Thus, the vehicles with its pseudo-identity used its private key S_t for signing process when receiving the message $msg_t \in \{0,1\}^*$. Also, the V_t sets the signature $Sign_t$ of msg_t with PId_t for a particular time period T_t.

E. Sign Verify

An RSU must ensure that no malicious vehicle tries to impersonate itself as a legitimate vehicle in order to trick the RSU when receiving traffic-related messages and their associated signatures. It is the responsibility of the RSU for verifying the integrity as well as the authenticity of messages that is developed using vehicles within its communication range. The RSU transmits the Msg Sign tuple $(msg_t, PId_t, sign_t, T_t)$ to vehicle V_t after receiving the message. Thus, the message is verified by RSU that is accepted or rejected by its pseudo-identity PId_t.

F. Big Sign Verify

At this stage, the RSU accepts multiple traffic-related messages sent from multiple vehicles and verifies their signatures simultaneously. Consequently, the number of linking operations is needed for reducing complete signature verification, which improves communication in VANETs. Also, RSU obtains the message signature tuple sequence as $(msg_1, PId_1, sign_1, T_1), (msg_2, PId_2, sign_2, T_2).....(msg_n, PId_n, sign_n, T_n)$ from $V_1, V_2, V_3.....V_n$ vehicles for $k = 1,2,3,.....n$. After the completion of verification, PTFT-AE process is initiated to secure the messages in the network.

3.2. PTFT-AE for Improving Security

In this work, Phase Truncated Fourier Transform based asymmetric encryption algorithm (PTFT-AE) is developed for enhancing the security of VANET communication. In this, the input data is ciphered by security keys, which are attained from random independent phase functions that are denoted as public keys. These are totally dissimilar from the deciphering keys of other random independent phase functions that are denoted as private keys. Additionally, the phase truncation procedure in the Fourier transform is demoralized by the PTFT model for developing templates for cancelling malicious activities through public keys. In this, the input plaintext $f(k)$ is denoted in eqn.(3),

$$f(j) = ft[b(i)] \tag{3}$$

where ft represent the Fourier transform operator, and $b(i)$ denoted the encrypted text. Here, the phase truncation (pt) is calculated using eqn.(4),

$$pt[f(j)] = |f(j)| \tag{4}$$

Additionally, the unwanted or unauthorized user or malicious attacks neglecting factor is mentioned in eqn. (5-6),

$$m_1(j) = pt[\, ft(b(i).R_1(i)] \tag{5}$$

$$m(i) = pt[Ift(m_1(j).R_2(j)] \tag{6}$$

where, Ift denotes the inverse Fourier transform, and $R_1(i), R_2(j)$ are represents the ciphering public keys, which are different from deciphering public keys $p_1(i), p_2(j)$ that is computed using eqn.(7,8),

$$p_2(j) = pr[\, ft(b(i).R_1(i))] \tag{7}$$

$$p_1(i) = pr[Ift(m_1(j).R_2(j))] \tag{8}$$

where pr denotes the phase retention and finally the secured outcome using deciphering public keys is obtained using eqn.(9-10),

$$m_1(j)p_2(j) = ft[b(i).R_1(i)] \tag{9}$$

$$m(i)p_1(i) = ft[m_1(j).R_2(j)] \tag{10}$$

When the authentication procedure of ID-CPPA is presented in the PTFT-AE ciphering, the malicious activities are neglected. The output of PTFT-AE is given to the tracing authority (TA) of ID-CPPA that is used for improving the privacy. The process of the proposed methodology is explained in flowchart in fig.2.

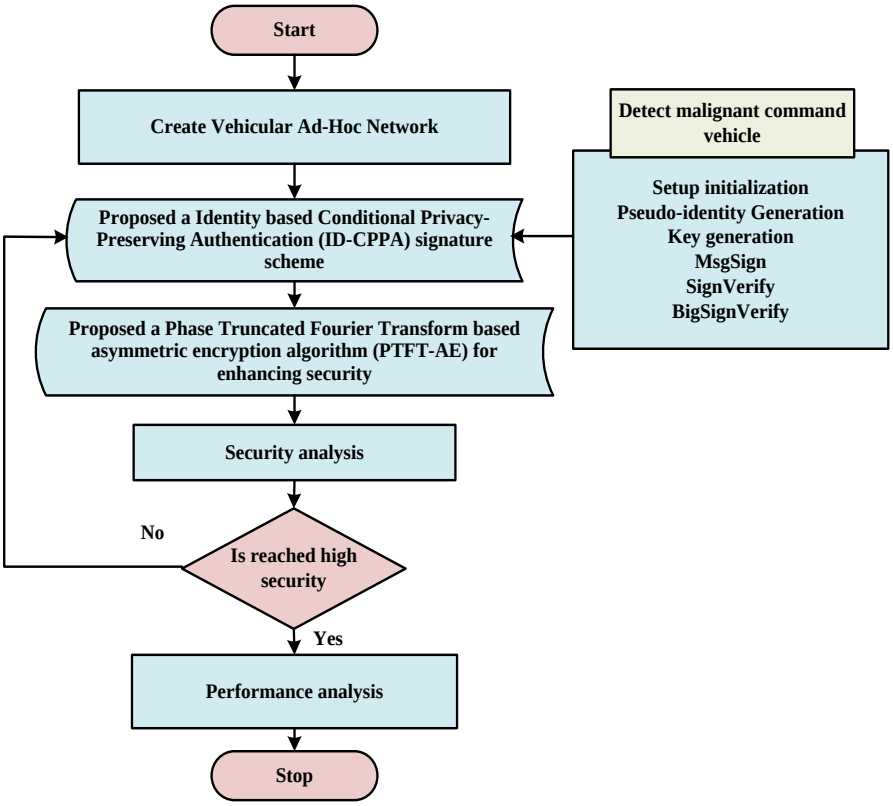

Fig.2. Flowchart representation of the proposed framework

3.3. Security Analysis

The proposed ID-CPPA-PTFT-AE method is very effective process to resist the malicious activities in the network. In this section, the security of the proposed model is analyzed by verifying some malicious activities. The proposed model consists of two trusted authorities, namely TRA and PKG. While the TRA generates fake identities for vehicles and detects their true identities, the PKG is responsible for generating unique keys for vehicles associated with their fake identities. It does not have access to the vehicles' true identities because it does not know the secret random integer selected by each vehicle and the TRA's primary private key.

- *Collision Resistance*

Based on the proposed ID-CPPA-PTFT-AE method, it is not possible for two or more vehicles to combine to generate a valid signature of another vehicle. Because, these vehicles are don't know the unique key calculated by the PKG for the vehicle and the random integer chosen by the vehicle V_t. Therefore, the proposed approach ensures collision resistance in vehicular communication.

- *Modification Attacks*

In this, the adversary is not able to develop the valid MsgSign tuple $(msg_t, PId_t, sign_t, T_t)$ and position as the vehicles. Because, the MsgSign tuple is verified by RSU that is accept the message or reject it. Thus, the proposed D-CPPA-PTFT-AE model can resist the modification attacks.

- *Reply attacks*

The proposed ID-CPPA-PTFT-AE methodology also resists the reply attacks in vehicular communication. In this, the time stamps are utilized in the MsgSign tuple $(msg_t, PId_t, sign_t, T_t)$ and pseudo-identity of vehicles. The freshness of the particular time stamps are enables a RSU for detecting reply attacks.

4. Results and Discussion

In this section, the efficiency of the proposed ID-CPPA-PTFT-AE methodology is analyzed based on the performance metrics. The simulation of this work is done by NS-2 simulator for predicting the network performance. It is implemented on a PC along Windows 10 operating system, 2GB random access memory, Intel i3 core processor. Finally, the performance metrics like throughput, delay, privacy rate, and packet loss are analyzed.

4.1. Performance Metrics

Here, various performance metrics are utilized to calculate the results. Therefore, performance metrics are measured below,

A. Throughput

Throughput describes the rate of data transferred from source to different number of nodes that is given in eqn. (11),

$$Throughput = \frac{No.of\ \ packets\,sent * packet\,size}{Time} \tag{11}$$

B. End-to-end-delay

It is the time taken to deliver packet from sender to the receiver that is determined using eqn. (12),

$$delay = P_{ST} - P_{RT} \tag{12}$$

where P_{ST} represented as packet sending time and P_{RT} represented as packet receiving time.

C. Packet Loss Ratio

It is the total count of data packets lost divided by the total count of data packets transferred. Hence, it is calculated using eqn. (13),

$$PLR = \frac{Total\quad packets - Total\quad number\quad of\quad received\quad packets}{Total\quad Packets} \tag{13}$$

4.2. Comparative Analysis

In this section, the parameters like throughput, delay, packet loss, and security rate of the proposed ID-CPPA-PTFT-AE approach is compared with existing methods like multiparty delegated computation (MPDC) with lightweight privacy-preserving based real-time intelligent traffic navigation scheme (LPNS) (MPDC-LPNS), privacy-preserving sign Recryption protocol (PPSR) with Group Signature (GS) (PPSR-GS), and Weight-based Conditional Anonymous Authentication (WCAA) with Two-Step Tracing (TST) (WCAA-TST) methods respectively.

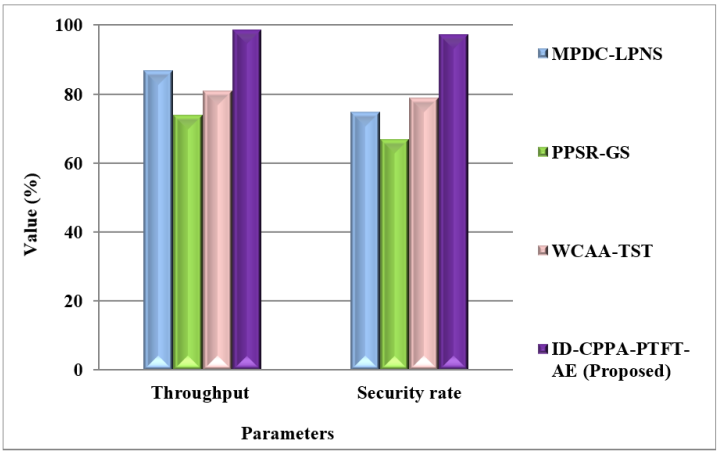

Fig.3. Comparison of throughput and security rate

Fig.3 shows that the comparison outcome of throughput rate and security rate. In this, the proposed ID-CPPA-PTFT-AE approach has achieved 26.7%, 35.7% and 29.8% higher throughput rate than the existing methods like MPDC-LPNS, PPSR-GS, and WCAA-TST methods respectively. Also, the proposed approach has achieved 28.96%, 37.58%, and 31.36% higher security rate than the existing MPDC-LPNS, PPSR-GS, and WCAA-TST methods respectively.

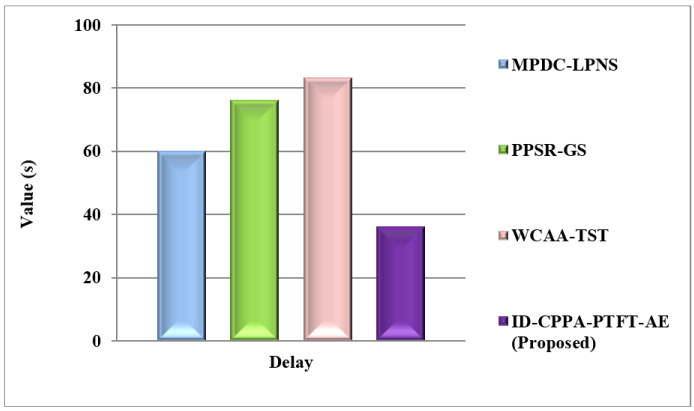

Fig.4. Comparison of delay

Fig. 4 shows that the comparison outcome of delay. In this, the proposed ID-CPPA-PTFT-AE approach has achieved 25.8%, 37.9% and 42.6% lower delay than the existing methods like MPDC-LPNS, PPSR-GS, and WCAA-TST methods respectively.

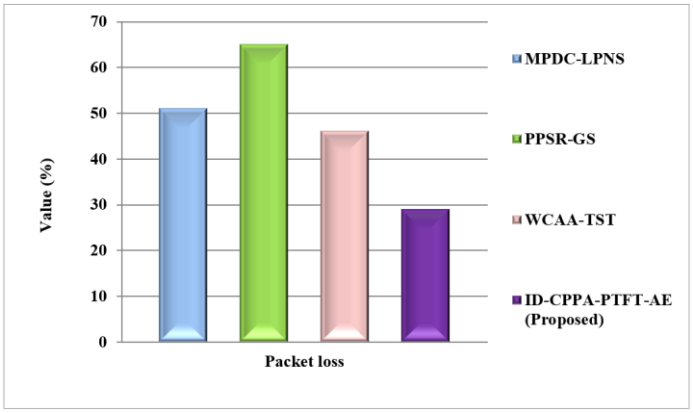

Fig.5. Comparison of packet loss

Fig. 5 shows that the comparison outcome of packet loss. Also, the proposed ID-CPPA-PTFT-AE approach has achieved 19.8%, 29.45%, and 15.75% lower packet loss than the existing MPDC-LPNS, PPSR-GS, and WCAA-TST methods respectively.

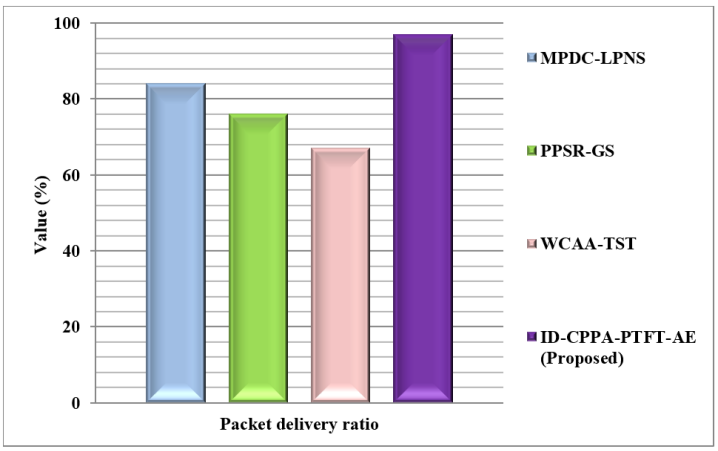

Fig.6. Comparison of packet delivery ratio

Fig. 6 shows that the comparison outcome of packet delivery ratio (PDR). The proposed ID-CPPA-PTFT-AE approach has achieved 21.3%, 25.5%, and 29.7% higher PDR than the existing MPDC-LPNS, PPSR-GS, and WCAA-TST methods respectively.

In this work, Identity based Conditional Privacy-Preserving Authentication (ID-CPPA) with Phase Truncated Fourier Transform based asymmetric encryption algorithm (PTFT-AE) is proposed for enhancing then security of the

vehicle platoon in VANET. The developed methods are robust, required less time, lower computational complexity and provide high efficiency that guarantees better routing in VANETs. Also, it improves the Quality of Service in VANET and the network traffic is reduced due to the relative position information of the neighbouring vehicles and location servers. Subsequently, it significantly enhanced the network stability and from the results, the proposed approach shows that the improved performance in terms of PDR, packet loss, throughput, delay and security rate than the existing works.

5. Conclusions

In this study the Identity based Conditional Privacy-Preserving Authentication (ID-CPPA) with Phase Truncated Fourier Transform based asymmetric encryption algorithm (PTFT-AE) for privacy safeguarding platoon are successfully implemented for consumer vehicle before joining the vehicle platoon. Security and the effectiveness of the proposed scheme are explained by the simulation results and by various security analyses. Thus, the proposed ID-CPPA-PTFT-AE approach has achieved 26.7%, 35.7%, 29.8% higher throughput rate and 19.8%, 29.45%, 15.75% lower packet loss than the existing MPDC-LPNS, PPSR-GS, and WCAA-TST methods respectively. The proposed methodology may applicable for real time application of VANET. Here, fog computing can be used in implementing real-time VANET applications. The secured details of vehicle platoons are processed in fog computing by Identity based Conditional Privacy-Preserving Authentication (ID-CPPA) with Phase Truncated Fourier Transform based asymmetric encryption algorithm (PTFT-AE) approach. Fog computing addresses the limitation of location awareness of cloud computing. For example, a person visiting a new city would like to seek information on the places of interest, news, and weather conditions of this city rather than interested in other city information. Fog computing can be used for distribution of any type of information (safety or non-safety). For example, if a particular section of a road is blocked due to some accident or natural hazard. This information can be conveyed by the fog servers to vehicles approaching towards this site. Future work includes designing of the vehicle platoon scheme without installation of the RSU unit.

References

[1] M. Mukhtaruzzaman, M. Atiquzzaman. “Clustering in vehicular ad hoc network: Algorithms and challenges”. *Computers & Electrical Engineering*, vol.88, pp.106851, 2020.

[2] S. Xiao, X. Ge, Q. L. Han, Y. Zhang. “Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks”. *IEEE Transactions on Cybernetics*. 2021.

[3] R. Sultana, J. Grover, M. Tripathi. “Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges”. *Vehicular Communications*, vol. 27, pp. 100284, 2021.

[4] M .Zhou, L. Han, H. Lu, C. Fu. “Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant”. *Computer Networks*, vol.172, pp.107174, 2020.

[5] N.A. Fida, N. Ahmad, Y. Cao, M.A. Jan, G. Ali. ‘An improved multiple manoeuver management protocol for platoon mobility in vehicular ad hoc networks’. *IET Intelligent Transport Systems*. vol.15, no. 7, pp.886-901, 2021.

[6] R.N. Kamoi, L.A. Júnior, F.A. Verri, C.A. Marcondes, C.H. Ferreira, R.I. Meneguette, A.M. Da Cunha. “Platoon Grouping Network Offloading Mechanism for VANETs”. *IEEE Access*, vol. 9, pp.53936-51, 2021.

[7] R. Hussain, F. Hussain, S. Zeadally, J. Lee. “On the adequacy of 5G security for vehicular ad hoc networks”. *IEEE Communications Standards Magazine*, vol.5, no. 1: pp.32-9, 2021.

[8] M.A. Al-Shareeda, M. Anbar, S. Manickam, I.H. Hasbullah. “Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks”. *IEEE Access*. 2021.

[9] A. Alarifi, M. Amoon, M.H. Aly, W. El-Shafai. “Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system”. *IEEE Access*, vol.8, pp.221246-68, 2020.

[10] F .Mirsadeghi, M.K. Rafsanjani, B.B. Gupta. “A trust infrastructure based authentication method for clustered vehicular ad hoc networks”. *Peer-to-Peer Networking and Applications*, vol.14, no. 4, pp.2537-53, 2021.

[11] J. Zhou, S. Chen, K.K. Choo, Z. Cao, X. Dong. “EPNS: Efficient Privacy Preserving Intelligent Traffic Navigation from Multiparty Delegated Computation in Cloud-Assisted VANETs”. *IEEE Transactions on Mobile Computing.* 2021.

[12] S. Kanchan, G. Singh, N.S. Chaudhari. “SPSR-VCP: secure and privacy preserving Sign Recryption in vehicular cyber physical systems.” *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 1, pp.1-20, 2022.

[13] H. Zhong, Y. Geng, J. Cui, Y. Xu, L. Liu. “A weight-based conditional privacy-preserving authentication scheme in software-defined vehicular network”. *Journal of Cloud Computing*, vol. 9, no. 1, pp.1-3, 2020.

[14] S. Gyawali, Y. Qian, R.Q. Hu. “A privacy-preserving misbehavior detection system in vehicular communication networks”. *IEEE Transactions on Vehicular Technology*, vol. 70, no.6: pp.6147-58, 2021.

[15] T. Nandy, M.Y.I. Idris, R.M. Noor, A.K. Das, X. Li, N.A. Ghani and S. Bhattacharyya, “An enhanced lightweight and secured authentication protocol for vehicular ad-hoc network.” *Computer Communications*, vol. 177, pp.57-76, 2021.

[16] S.A. Eftekhari, M. Nikooghadam and M. Rafighi, Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications. *Vehicular Communications*, vol. 28, pp.100306, 2021.

[17] Y. Yang, D. He, H. Wang, L. Zhou. “An efficient blockchain-based batch verification scheme for vehicular ad hoc networks”. *Transactions on Emerging Telecommunications Technologies*, vol.33, no. 5, pp.e3857, 2022

[18] U. Coruh and O. Bayat, “ESAR: Enhanced Secure Authentication and Revocation Scheme for Vehicular Ad Hoc Networks.” *Journal of Information Security and Applications*, vol. 64, pp. 103081, 2022.

[19] R. Abassi, A. Ben Chehida Douss, and D. Sauveron, “TSME: a trust-based security scheme for message exchange in vehicular Ad hoc networks.” *Human-centric Computing and Information Sciences*, vol. 10, no. 1, pp.1-19, 2020.

Authors' Profiles

K. Lakshmi Narayanan Completed his Master of Engineering in the field of Computer Science and Engineering in Annamalai University Chidambaram in the year 2012. He completed his Bachelor of Engineering under Annamalai University Chidambaram in the year 2009. He Worked as a Assistant Professor at Mailam Engineering College, Mailam, India from 2012 to 2018. He also worked as a Senior Customer support Executive at HCL Technologies, Chennai from 2018 to 2020. He is presently a Research Scholar in the Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, India. His main thrust research areas are Network Security and Cloud Security.

R. Naresh completed his Ph.D in Computer Science and Engineering in Anna University Chennai in the year 2017.He Completed Master of Engineering in the field of Computer Science and Engineering in Anna University Chennai in the year 2011. He completed his Bachelor of Engineering under Anna University Chennai in the year 2007. He was working as a Assistant Professor at Anna University Chennai (University College of Engineering, Tindivanam), Chennai, India from 2011 to 2018. He is presently working as an Associate Professor at Department of Networking and Communications, SRM Institute of Science and Technology, Chennai, India. His main thrust research areas are Group Key management in Network Security and Cloud Security.

How to cite this paper: K. Lakshmi Narayanan, R. Naresh, "An Enhancement of Identity Based Conditional Privacy-preserving Authentication Process in Vehicular Ad Hoc Networks", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.1, pp.113-122, 2024. DOI:10.5815/ijcnis.2024.01.09