Neural Parallel and Scientific Computations 29 (2021), No. 3, 130-145

AN EFFICIENT SECURE VANET COMMUNICATION USING MULTI AUTHENTICATE HOMOMORPHIC SIGNATURE ALGORITHM

G. KAVITHA[1] AND R. VARATHARAJAN[2]

[1]Department of Electronics and Communication Engineering Government College of Technology, Salem, India. Email : kavitha@gcesalem.edu.in

[2]Bharath University, Chennai, India. Email : varathu21@gmail.com

ABSTRACT

Vehicular Ad-hoc Networks (VANETs) is a wireless network that provides communication between vehicles and roadside infrastructure. It has been gaining high attention in the field mainly by researchers recently. It can provide various services, ranging from security-related early warning systems, enhanced navigation mechanisms, and information and entertainment applications. In VANET systems, some confidential data and contact information leakage can cause a severe loss of property. After that, it is a need for a higher level of security VANET system. Therefore, in VANET is the urgent priority need for security of privacy protection protocol. The proposed method Elliptic Homomorphic signature (EHS) the critical requirement is to allow VANETs privacy protection protocol to ensure its authenticity for the use of trademarks. When the user signs data, the signature is generated using the secret key, which is kept secure by the signer, and it encrypts the data. No one can create any signature items other than legitimate users. Destination to receive data using the public key confirms has not been modified in transit. The attacker can neither find the correct signature nor steal the data. The simulation results, when used in VANET, confirmed the level of effectiveness and security.

Keywords: EHS, Attacker, Vanet, Security, Protection, Authenticate

1. INTRODUCTION

A Vehicular Ad-hoc Network (VANET) usually consists of a fixed infrastructure component of the fast-moving vehicle, called the roadside unit (RSU). The car can be brought into contact with the help of an onboard group (OBU). The vehicle allows them to update the environment around them; it has been tested and expected to send every millisecond for each

Received July 13, 2021
www.dynamicpublishers.org;
https://doi.org/10.46719/npsc20212931

safety message in the stock around the car and yourself. These messages contain information about the use of digital signature programs to sign these messages for virtual maps, such as speed, level, acceleration level, the ability to send some other vehicle, cheat, or misuse any other malicious erroneous message or resource, and maintain virtual maps. A valid signature on a piece of information enables it to retain its original authenticity, protect its sovereignty, and provide the source irrefutability.

VANET supports a self-organized traffic information system called high-speed mobile communications. In a smart traffic environment, VANET enables the connection between any two vehicles. Drivers will be able to use emergency alarms with time risk and avoidance traffic changes and congestion traffic information, traffic sharing, information sharing basis, and contract communications do not adjust the routes of these vehicles. The system consists of three components: a Trusted Party (TA) onboard unit (OBU) and a roadside unit (RSU). The TA is responsible for the identification, certification, cancellation management, and storage of information at each node of the VANETs. The TA may be considered an authorized center; OBU is a terminal connected to a mobile terminal depending on the vehicle conversion communication system. RSUs have roadside infrastructure nodes as well as communication systems, communication base stations.

However, VANETs rely on unstable wireless channels for communication; they will undoubtedly change the transmission of false information such as or re-enacting previous information, altering the vulnerabilities in the VANET world by hiding the personal data of users who are vulnerable to various malicious attacks and attacks, these attacks and threats.

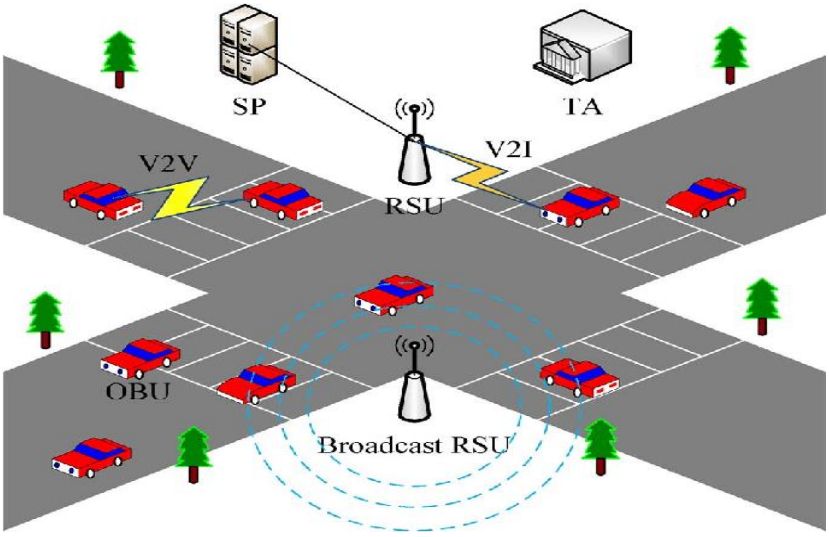

Figure 1: VANET Communication

[https://www.researchgate.net/figure/VANET-communication-system-is-supported-by-DSRC-which-offers-V2V-and-V2I-communications_fig1_280970636]

The VANET communication system supports v2v and V2I communication provided by the Dedicated Short-Range Communication (DSRC). All information is there to meet security requirements and can be exchanged by the system to verify the data and ensure that it is reliable. The temporary vehicle network allows communication between OBU and RSU via DSRC. At VANETs, each vehicle enables us to periodically broadcast its necessary vehicle information and traffic accidents in real-time. This fact allows other cars to improve traffic conditions to take relevant action promptly effectively. RSU broadcasts some details of restaurants, hotels, and gas stations within its jurisdiction, road conditions, parking alerts, and traffic information.

A pseudonym will be assigned for privacy protection purposes so that the vehicle's true identity is not disclosed to other vehicles and roadside units. The security requirement that signatures cannot be forged makes it computerized so that any information on the attack can produce the correct names. The proposed scheme includes essential security functions such as news authentication, non-refundable, and privacy protection. Our proposed signature scheme's effectiveness is based on verification time and RSU forecast, and the results confirm its high efficiency.

Route driver information is one of the main requirements of speed motorists regarding the protection of their travel identity. It is necessary to protect their data, a process that restricts unauthorized users based on the information obtained through access. Therefore, there is a great need for a security framework that provides VANET with the expected security level, so personal data and time can be exchanged over the most critical data wireless channel.

Thus, it is essential to ensure that the information is transmitted via VANET so that it is not accessible by malicious users or attackers. On the other hand, the VANET has become a challenge on an extensive network scale due to its current security issues, random speed of the vehicle, fixed node position, and wireless connection to the VANET vehicle's connecting errors. It can identify malicious users from the network's attackers and ensure that it provides the level of demand it needs.

A homomorphic signature allows you to create a direct synchronous name that represents the original signature. Since then, we have demonstrated that adaptive selection based on the CDH hypothesis random prediction model may be a news attack signature fraud. The length of our signature project is concise, our plan is suitable for a low bandwidth communication environment.

2. RELATED WORK

Infrastructure is a smart transportation system, and Vehicle ad-hoc networks (VANETs) have, therefore, become transportation capabilities. However, transparency, trust, and VANET privacy are still two challenges that must be handled in a highly secure network environment: Detected Guaranteed Vehicle Privacy when sending messages to the vehicle [1]. VANETs are presented based on the Blockchain Trust Management Model and the notice of the conditional privacy protection program.

Combined with cloud computing technology, Auto Temporary Network (VANET) allows companies to enjoy better security and computing services provided by some cloud service providers. However, the advantages of hybrid VANET applications do not come free, as there are many new security and privacy requirements. It has the status of immediate, uninterrupted monitoring, cloud-based road conditions [2] power needs supply, monitoring real-time road conditions with the help of cloud servers.

5G technology should promote the creation of VANET. However, almost all existing authorization protocols rely on a fully Trusted Authority (TA). On the other hand, the following protocols can rarely resist some specialized attacks, such as registration officers and brief leak attacks information disclosure attacks [3]. The existing system, a random prediction model, has been demonstrated under the Diffie-Hellman assumption.

VANETs are called elementary beacon messages sent from vehicles and surrounding RSUs cars to help them create logical maps of their surroundings. The words should be Beacon, the source attack designed to ensure the correctness of this map is authorized to protect vehicles and fake news networks [4]. Computation is a beacon, an efficient linear synchronization program, with a code for messages delivered by a third party. VANET has recently received a great deal of attention in industry and education to improve traffic safety and performance. Foundation Modeling VANETs play an essential role. However, the already trusted model does not primarily match the characteristics of VANETs. The existing a novel

layer-based Trust Cascading-based Emergency Message Dissemination (TCEMD) [5] model that combines data-based trust value with a data-based trust rating in an effective way.

VANETs are one of the most promising applications for communication between smart cars and smart transport systems. However, two critical issues with user authentication and privacy licenses continue on VANET persist. Private vehicles must be prevented from transmitting fake news. The vehicle and roadside units (RSUs) [6], as a traceable and intelligent vehicle first-vehicle communication vehicle is proposed through the use of a secure access authentication scheme between the decentralized webs of the system structure.

Vehicle Temporary Network (VANET) is a collection of moving vehicles that implement roadside communication and vehicle first infrastructure operating modes by the first vehicle. Network independence requires comprehensive security measures to protect discussions from such attacks [7]. The existing system is a Trusted Distributed Authentication (TDA) system based on the global trust server and vehicle status to avoid conflict attacks.

With the rapid advancement of automotive telematics and communication technology, the proliferation of vehicular ad hoc networks (VANETs) and the intelligent transportation system (ITS) advantage is being seen. Due to the built-in wireless communication functionality in the open environment, secure transmission between many VANET companies is still an important issue. A safe stabilization and essential management plan can be an existing method [8]. In edge computing infrastructure has been adopted to provide adequate computing and storage capabilities than the new VANET models adopted by the traditional VANET system.

VANET is several modern transportation systems technologies that have been activated to deliver valuable information safely and securely from active congestion attacks. Detection systems are a useful tool that can further reduce the threat of malicious behavior Intrusion Detection Systems (IDs) [9]. The existing system is VANETs may is a joint as privacy-preserving machine-learning-based collaborative IDS (PML-CIDS).

Unfortunately, due to the excessive or ineffective Location-based service (LBS) messages transmitted on VANETs, the public critical Synchronous Encryption (SE), or not tolerated, can be tolerated in each period of re-authentication using existing work confirmation keys, message identifier filter or overhead public keys On-Board Units (OBUs) or VANETs are improperly controlled for real-time control requirements [10]. The VANETs lightweight privacy-preserving authentication protocol proposes to eliminate pseudo-ineffective encryption pound messages when LPPA authentication.

Also, all vehicles are created by malicious devices, or some of them malicious attacks, to enable the pre-authentication feature of the recovery messages needed. In this case, it can be used in a relatively short period to stabilize large amounts of erroneous messages, and even denial of service (DOS) attacks can be discarded. The vehicle has limited computing power and memory control [11]. The existing method can significantly reduce the unnecessary authorization load on the vehicle side.

Serves as a guide to the policy emphasis and practical policy analysis of VANET Highway Links to reduce traffic accidents and improve traffic efficiency. An existing method of cooperative communication is to describe the various vehicles that use the Cell Transmission Model (CTM) and the two-way high-speed repair of the two-way on-ramp / out-ramp and effectively damaged chain flow [12].

The multi-hop relay can effectively increase the VANET average Packet Loss Rate (PLR) over a specific area of interest. Depending on the vehicle, radio channel conditions, and medium access control (MAC), the choice of circuits does not present a moving average PLR challenge since a course is distributed. The existing average PLR is taken into account in the analysis sample by the above three factors [13]. However, the general PLR closed exposure stubbornness is one of the most important for integrating distance distributions along with channel conditions and vehicle movement.

A three-dimensional (3D) VANET, which significantly reduces the probability of packet reception in vehicle dynamics, complex node distribution, and severe path loss can dramatically increase connection interference. Once a reliable pathway (PPR) is in place, serial protocol connection reliability [14] should be improved based on packet reception probability. In particular, the packet reception probability model 3D networks and 3D VANETs connection reliability personal property classification has been combined with this model.

Implement testing and new connection status and evaluate the performance of autonomous driving functions; it is essential to obtain bundle loss characteristics as the vehicle (V2X) communication channel is reduced. Pseudo-Markov Chains (PMC) is an algorithm for creating an additional dependent bandage loss model [15]. The PMC-based model requires only a short training sequence with less computational complexity but provides a more accurate approximation than known techniques.

The original identity-based (IB) homomorphic signature scheme proposes a unique tool using any IP-signature project as a framework. They are a new type of planned attack: the

associated Related-key attack (RKA) is widely considered encryption primitive [16]. In particular, for the first time, the security of an IP-compatible signature program is defined by RKA.

The linear homomorphic signature schemes allow the performance of approved data direct operations. They have smart phases, e-maps, proxy signatures can be registered on behalf of the original name, and proxy signing schemes such as signing the contractor to authenticate him/her. It is an essential resource for signature teams with many uses. This scheme demonstrates safety in a random prediction model. Also, the signature length is short and constant [17]. The linear symmetry can be used in e-commerce and cloud computing applications such as the homomorphic Signature Scheme.

Public keys are identification-based encryption means that phone numbers, email addresses, and social security numbers can be obtained directly from user identifiers. An existing scheme identity-based homomorphic signature scheme avoids errors using linear public vital certificates [18]. This program demonstrates the ID attack on the presence of pseudo-adaptive selection messages and random prediction models.

Accelerate your infrastructure and smart applications to generate electricity at the ever-increasing integration of Internet-driven networks due to advances (smart phases, smart traffic, smart cities, etc.), Things (demographics) technology to provide an unprecedented amount of volume and physical systems. Like our essential commodities in the current information technology era, big data is a significant competitive core in modern business. An existing system, Privacy-Preserving Auction Scheme (PPAS), includes two private companies, a trusted platform for bidding and intermediate platform [19].

Ensuring vehicles' safety and privacy is one of the critical requirements of vehicle safety and reliability at Hog Networks. Programs for various (conditional) anonymous identity verification, including group/ring signatures, pseudo-identity based, and Indonesian communist party-based methods, are existing to current privacy protection accreditation as a recent endeavor, i.e., random verification, the identity self-generated verification to achieve complete unknown uses the vehicle's symmetric encryption integer [20].

3. MATERIALS AND METHODS

VANETs are the most efficient technology for communicating between vehicle communication and framework units. Data transmission must be secure; delayed data transfer

causes various security issues. So rapid growth in automotive network development has increased security requirements. VANET networks demand protection based on the confidentiality and availability of users' data. The attacker finds the target path and receives data information and communication. To overcome the problem, the higher the distribution rate, the lower the contact overhead and energy consumption, to ensure the proposed work Elliptic Homomorphic signature (EHS) algorithm in the system includes the compilation process, the use of names, and the integrated encryption algorithm. The advanced scheme Elliptic Homomorphic signature (EHS) is being used to prevent attacks by malicious nodes or attackers. In this proposed algorithm, a unique security process when the source node signed a secret data key generating for encrypting data and destination using the public key for decrypt data to receive is more secure than other methods at the same time the invalid user is not accepted.

Figure 2: Block Diagram

Figure 2 describes source node send data with signature and trusted party to verify the sender's name. Then, it packets analysis of the path and avoids traffic to receive the destination.

3.1 Advanced Data Encryption Standard algorithm

Data encryption is used to provide secure, confidential data, which thereby denies unauthorized access quality. An incomprehensible form of encryption called cyber text is the function of converting data or text. A method of messaging is proposed securely with a secret key on the VANET using Advanced Data Encryption Standard (ADES) algorithm. The asymmetric system provides not only integrity, availability, and reliability but also reliable and

non-repudiation. The authenticity and asymmetric pattern accomplished by creating a digital signature, which can then be used to verify the sender and prevent the sender from rejecting the message.

Step 1-Initialize the data to encrypt.

Step 2-Delete all spaces in the text.

Step 3: Change the text to ASCII and then to binary code.

Step 4: Delete two digits with every six figures and save them to the file.

Step 5: Have two bits of data and separate them.

Step 6: Divide the data into three parts

Step 7: Generate a secret key for encrypting data.

Step 8: Exit

In this algorithm, delete unnecessary spaces in the message text, change the text into ASCII values, and then ASCII values to binary values, the user generates the secret key.

3.2 Elliptic Homomorphic signature

The VANETs make it ideal for a wide range of applications while causing many wireless secure data transfer problems. EHS algorithm only considers authenticating data and functional evaluation data signature. When the user signs data, the signature is generated using the secret key, which is kept secure by the signer, and it encrypts the data. No one can create any signature items other than legitimate users. Destination to receive data using the public key confirms has not been modified in transit. EHS is an ideologically simple and elegant authentication data signature scheme framework in which secure data information transfer privacy is ability. The attacker can neither find the correct signature nor steal the data the simplicity of the method allows for significant signatures and higher performance with greater efficiency. This algorithm ensures that the information sent by VANET is not accessible by malicious users or attackers.

Signature Algorithm Steps

The source code must be signed to use secret key and parameters using EHS algorithm and the critical utility process established during the setup process:

Input: Sign the process in which take the input Data (d) must be signed.

Output: Signature σ = (x, y)

Step 1: Generating a key pair (S, P)

Step 2: Signature compute σ = f$(d)^S$, data identifier τ ∈ $\{0,1\}^{SP}$ then

If (if σ ← Sig (S, τ, d), then

Vy (A, S, τ, r, σ) = 1

Step 3: Compute (A, S, τ, $\sum_{n=1}^{dl} f, r$)

Step 4: Combine (A, S, τ, {(f, σ)}) = 1

Step 5: Output Signature σ = (x, y)

Exit

Specification of EHS includes an x, y is an Integer, dl it denotes data length, f is a hash function, P is a Public key, S is a Secret key, n is a variable, r it means vector, A is an Original signer, SP security parameter, Vy is a Verify. In this algorithm steps creating a key pair, source node signed data using a secret key (S) for encrypting data. The output will be signed data with encrypting data for secure data sharing in VANET.

Verify Signature Algorithm Steps

The destination node should be used to verify signing using EHS algorithm parameters and keys during the installation process are the following:

Input: Signed data (σ)

Output: Signature Accept or Invalid

Start

Step 1: Calculate the hash function established f = f$(d)^P$

Step 2: if σ ← Sig (P, τ, r)

Check e (σ, j)=e(P, j). e ((||f$(\tau, j)^S, J$) = e(f(MW), P)

Step 3: If Vy = (A, P, mω, τ ∗, r∗, σ∗) = 1

Accept

Else

Invalid sign

Exit

Let σ∗ is an output signature, A is an original signer, mω data warrant, τ ∗ data identifier, r∗ is a vector, Vy is verification, and P is a public key. In this algorithm, verify the sender's signature if the condition is 1 (accept); otherwise, it will be an invalid signature.

3.3 Decryption Data

Data decryption is the reverse method of encrypting data. Decryption is a method of encrypting data in its original form. The critical value is provided by the message decrypt authorized person.

Algorithm Steps:

Step 1: Encryption Message

Step 2: Enter the public key.

Step 3: Change corresponding binary values to ASCII values

Step 4: Change ASCII values into character for decrypt message

Step 5: obtain original data.

In this algorithm, decrypt the message, convert binary values into ASCII values, and then change ASCII values into a character get the original news.

4. RESULT AND DISCUSSION

This section discussed the implementation of the proposed system Elliptic Homomorphic signature (EHS) algorithm with the existing methods Privacy-Preserving Auction Scheme (PPAS) and Trust-based Distributed Authentication (TDA) for simulation performance analysis. The execution simulation result tested on the developed NS2 tool with OTCl (Object Tool Command Language) developed by NS-2 of the device; it is similar to the object-oriented language.

Table 1: Simulation parameters

Parameters	Value

Tool	NS2
Transfer Pattern	UDP
Data Size	60 bytes
Type of node	Mobile Node
Number of nodes	70
Network Area	400 * 400

The Elliptic Homomorphic signature (EHS) method used by VANET is highlighted in Table 1 simulation parameters.

4.1 Analysis of Failure performance

The packet loss rate is the leakage of some critical data or contact information that causes a significant loss.

$$\textbf{Failure Performance} = \frac{\textbf{Total number of dropped packet data}}{total\ number\ of\ sent\ packet\ data}\ X\ 100 \text{ ------ (1)}$$

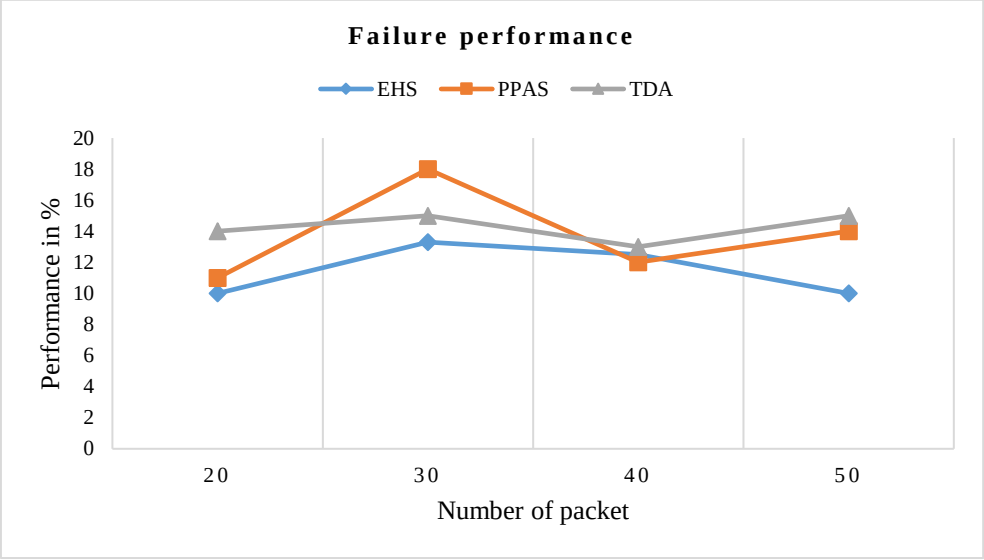

Figure 3: Analysis of failure performance

Figure 3 shows the analysis of data failure performance in %. The proposed method result in Elliptic Homomorphic signature (EHS), is 10% compared to the existing system are Privacy-preserving Auction Scheme (PPAS) is 14%, and Trust-based distributed

Authentication (TPA) is 15%. In this proposed is failure performance low compared to methods.

4.2 Analysis of Security performance

The security performance is always measured as the number of packets of data transmitted from the target node and source node that is total no data transferred to the network. What is expected is that the data packets should reach the maximum number of data to the target. Due to the security performance value, network performance will increase accordingly.

$$\textbf{Security Performance} = \frac{\text{Number of Delivered packet data}}{Total\ Number\ of\ sent\ packet\ data}\ X\ 100 \text{ ------ (2)}$$

Table 2: Evolution of security performance

Number of Vehicles	EHS in %	PPAS in %	TDA in %
100	90	65	70
200	93.3	75	68
300	95	79	76
400	96	85	88

Table 2 describes the packet delivery performance. It is a calculated packet delivery ratio.

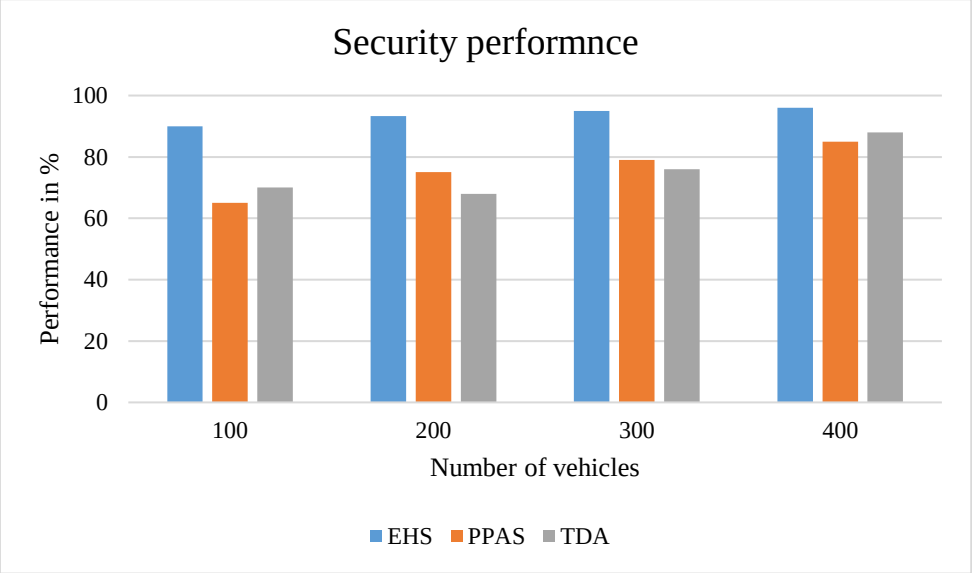

Figure 4: Analysis of Security performance

Figure 5 shows that the analysis of the security performance scheme Elliptic Homomorphic signature (EHS) is 96% similarly existing methods are Privacy-preserving Auction Scheme (PPAS) and Trust-based distributed Authentication (TPA) respectively 85%, 88%.

4.3 Analysis of Time Complexity

Upcoming vehicles have relatively high-speed and secure data communications due to the time, and Packet delivery time is a complicated task. Big O is used to describe the required execution time complexity.

$$\text{Time complexity } T(x) = x - 1 \leq 1, \; x \text{ when } x \geq 1. \text{ ---- (3)}$$

Where T is time and x is the variable execution time of the input.

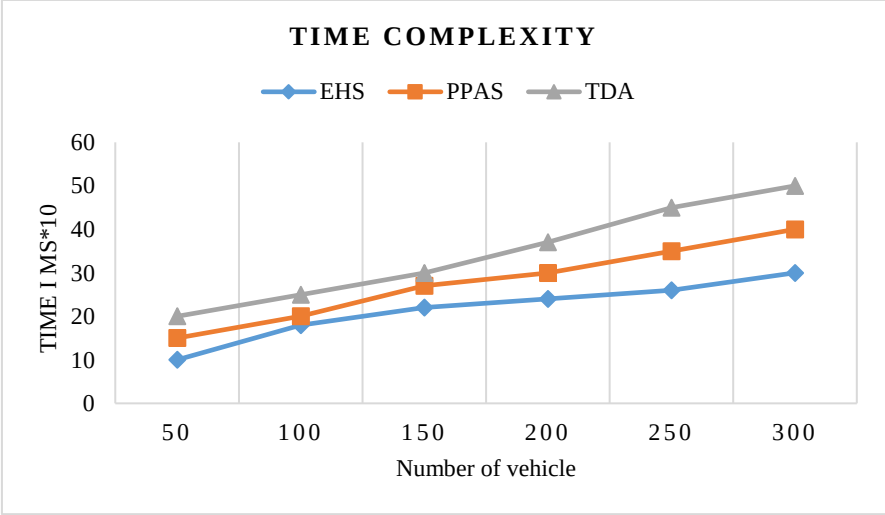

Figure 5: Analysis of Time Complexity

Figure 5 shows the time complexity is based on the number of vehicle data communication in the time complexity calculate Msec proposed method gives 300 Msec; the existing techniques are PPAS and TDA, respectively 400Msec, 500Msec. The proposed method decreases the time compared to other existing systems.

5. CONCLUSION

The proposed Elliptic Homomorphic signature (EHS) algorithm is intended for unforgeable data attacks and VANET security. Then, to reduce the cost of forecasting, the proposed trusted party verify the sender signature and attacker not be allowed. These outsourced algorithms are universally available in faster performance. EHS algorithm is a

performance very efficient and more secure for data transfer in VANET. This proposed algorithm provides a packet failure performance of 10%, security performance is 96%, and Time complexity is 300Msec. It gives an efficient performance compared to the existing system.

REFERENCES

[1]. Xingchen Liu; Haiping Huang, "A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs," IEEE Internet of Things Journal (Volume: 7, Issue: 5, May 2020).

[2]. Yuja Wang, Yong Ding, "Privacy-Preserving Cloud-Based Road Condition Monitoring with Source Authentication in VANETs," IEEE Transactions on Information Forensics and Security (Volume: 14, Issue: 7, July 2019).

[3]. Xuelian Li; Yue Han. "Secure hierarchical authentication protocol in VANET," IET Information Security (Volume: 14, Issue: 1, 1 2020).

[4]. Vasudha, Fahiem Altaf. "Linearly Homomorphic Signature Based Secure Computation Outsourcing in Vehicular Adhoc Networks," Innovations in Power and Advanced Computing Technology (i-PACT), 2019.

[5]. Zhiquan Liu; Jian Weng "TCEMD: A Trust Cascading-Based Emergency Message Dissemination Model in VANETs," IEEE Internet of Things Journal (Volume: 7, Issue: 5, May 2020).

[6]. Dong Zheng; Chunming Jing, "A Traceable Blockchain-Based Access Authentication System with Privacy Preservation in VANETs," IEEE Access (Volume: 7)2019.

[7]. A.M.R. Tolba, "Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs," IEEE Access (Volume: 6)2018.

[8]. Haowen Tan; Ilyong Chung "Secure Authentication and Key Management with Blockchain in VANETs," IEEE Access (Volume: 8), 2019.

[9]. Tao Zhang, Quanyan Zhu" Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs," IEEE Transactions on Signal and Information Processing over Networks (Volume: 4, Issue: 1, March 2018).

[10]. Jun Zhou; Zhenfu Cao, "LPPA: Lightweight Privacy-Preserving Authentication from Efficient Multi-Key Secure Outsourced Computation for Location-Based Services in VANETs," IEEE Transactions on Information Forensics and Security (Volume: 15), 2019.

[11]. Haowen Tan; Ziyuan Gui, "A Secure and Efficient Certificateless Authentication Scheme With Unsupervised Anomaly Detection in VANETs," IEEE Access (Volume: 6), 2018.

[12]. Hailin Xiao; Qiuyu Zhang, "Connectivity Probability Analysis for VANET Freeway Traffic Using a Cell Transmission Model," IEEE Systems Journal (Early Access), 2020.

[13]. When Lai; Wei Ni, "Analysis of Average Packet Loss Rate in Multi-Hop Broadcast for VANETs," IEEE Communications Letters (Volume: 22, Issue: 1, Jan. 2018).

[14]. Chuan Xu; Zhengying Xiong "A Packet Reception Probability-Based Reliable Routing Protocol for 3D VANET", IEEE Wireless Communications Letters (Volume: 9, Issue: 4, April 2019).

[15]. Irina Bocharova; Boris Kudryashov, "Characterizing Packet Losses in Vehicular Networks," IEEE Transactions on Vehicular Technology (Volume: 68, Issue: 9, Sept. 2019).

[16]. Jinyong Chang; Hui Ma, "RKA Security of Identity-Based Homomorphic Signature Scheme," IEEE Access (Volume: 7),2019.

[17]. Qun Lin; Jin Li, "A Short Linearly Homomorphic Proxy Signature Scheme," IEEE Access (Volume: 6), 2018.

[18]. Hongyang Yan; Zheng Huang, "An ID-Based Linearly Homomorphic Signature Scheme and Its Application in Blockchain", IEEE Access (Volume: 6), 2018.

[19]. Weichao Gao; Wei Yu, "Privacy-Preserving Auction for Big Data Trading Using Homomorphic Encryption," IEEE Transactions on Network Science and Engineering (Volume: 7, Issue: 2, April-June 1 2020).

[20]. Cong Sun; Jiao Liu, "Ridra: A Rigorous Decentralized Randomized Authentication in VANETs," IEEE Access (Volume: 6), 2018.