

Enhancing safety communication in autonomous vehicles with hybrid elliptic curve digital signatures

Ravi Kalkundri¹, Rajashri Khanai², Praveen Kalkundri³

¹Department of Computer Science and Engineering, Karnataka Law Society's Gogte Institute of Technology, Affiliated to Visvesvaraya Technological University, Belagavi, India

²Department of Computer Science and Engineering, KLE Dr. MS Sheshgiri College of Engineering and Technology, Affiliated to Visvesvaraya Technological University, Belagavi, India

³Department of Electronics and Communication, Karnataka Law Society's Gogte Institute of Technology, Affiliated to Visvesvaraya Technological University, Belagavi, India

Article Info

Article history:

Received Jul 4, 2023

Revised Jul 20, 2023

Accepted Aug 16, 2023

Keywords:

Ate pairing

Autonomous vehicles

ECDSA

Safety messages

VANET

ABSTRACT

The autonomous vehicles (AVs) are a part of vehicular ad hoc network (VANET) technology which is gaining a lot of researchers' attention for making the vehicle smarter and safer. In VANETs, the vehicles transmit various types of messages, some are important in terms of human lives while others are for infotainment. These messages give various information to the driver so that the driver can take appropriate precautions on the roads. In this work, the main aim was to concentrate on the safety messages that are very important in VANET infrastructure. In VANET the information transmitted are open, hence it is very easy for any attacker to manipulate or change the critical messages. Hence, in this paper, we intend to implement security to these safety messages by encrypting the elliptic curve digital signature algorithm (ECDSA) algorithm which is further optimized by ate pairing. The results have been compared with the traditional ECDSA in terms of throughput. By using the hybrid ECDSA, we increase the strength of ECDSA and still maintain the integrity of ECDSA, making sure that the authenticity of the vehicles and privacy of the messages is maintained within the VANET infrastructure.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ravi Kalkundari

Department of Computer Science and Engineering

Karnataka Law Society's Gogte Institute of Technology

Affiliated to Visvesvaraya Technological University

Belagavi, Karnataka, India

Email: ravi.kalkundri05@gmail.com

1. INTRODUCTION

The automobile industry has been improving and growing significantly in recent years. Improvements like computer systems and automation of mechanical and manual functions have been incorporated into modern vehicles. Modern vehicles are incorporated with multiple features that help and assist the driver like lane change warning, self-parking, adaptive cruise control, and identifying obstacles/barriers in the middle of the roads during fog or night, which assist the driver that helps to reduce human efforts. These improvements in vehicles impose the development of autonomous vehicles (AVs). The vehicle has improved and grown tremendously in terms of technology throughout the years. Further vehicle's computational power and computerization of mechanical and manual tasks have been developed in autonomous vehicles, enriching the vehicle performance and information to the drivers [1]. The AV assists drivers in reducing the occurrence of

accidents and reducing traffic congestion by taking alternative routes. These features also contribute to the reduction of carbon emissions, less travel time, and less traffic [2].

AVs are equipped with various electronic components like sensors, cameras, global positioning system (GPS), radars or antennas, and complex processing elements used to process the information that is gathered from other components. The vehicles are also integrated with software that makes the components work together and process the information [2]. Further, in the AV scenario, the vehicles also communicate with other vehicles and share various information, some of the information is very critical, forming a vehicular ad hoc network (VANET) scenario. The communication in the VANET infrastructure is between vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), but most of the communication takes place between V2V [3]. Typical AV vehicle components are shown in Figure 1 [4]. In Figure 1, it can be seen that the vehicles rely on various sensors and other devices that communicate wirelessly with other vehicles. Because the nature of communication is open, AVs are more prone to various security attacks. In most cases, the attacker has the advantage that he doesn't require physical contact with the vehicle, he just needs to get access to the communication [5]. In some cases, the attacker can gain control of the various parts of the vehicle, like applying sudden brakes, or sudden accelerating, steering, and other parts causing a major catastrophe. So not only it is required to secure the vehicle, but also the information that is being communicated between the vehicle and the infrastructure [5], [6]. The major issue in VANETs is the security of the nodes and the information.

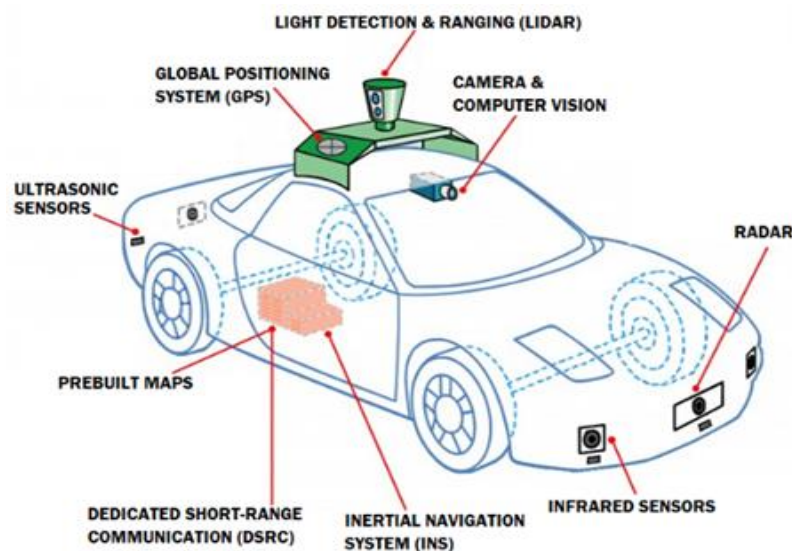


Figure 1. Inside the AV [4]

The objective of this work is to achieve efficient and secure nodes and V2V and V2I communication. Various information is transmitted into the VANET infrastructure; among all the information, hence, our main aim is to work on the safety messages [7]. There are various methods of securing a network, but the simplest method for the VANET type of network is by applying cryptographic algorithms. There are various types of cryptographic algorithms, but one of the most popular is elliptic curve digital signature algorithm (ECDSA). Though the algorithm is a little mathematical complex, it is very suitable for the VANET network [8]. Hence, in this paper, we intend to implement security to these safety messages by encrypting the ECDSA algorithm which is further optimized by Ate pairing. The results have been compared with the traditional ECDSA in terms of throughput. By using the hybrid ECDSA, we increase the strength of ECDSA and still maintain the integrity of ECDSA, making sure that the authenticity of the vehicles and privacy of the messages is maintained within the VANET infrastructure.

The rest of the paper is organized as follows, section II provides the Security Requirements in VANET, where it discusses the security concern, the attacks, and security concerns. Section III discusses the ECDSA and the working of ECDSA and compared it with other algorithms. In section IV the Implementation Scheme has been discussed, and in section V, the results have been obtained. Finally, the conclusion and the future scope of the proposed work have been given.

2. LITERATURE SURVEY

Alazzawi *et al.* [9], they have proposed a security model called as lightweight-security and key-agreement-based identity (LSKA-ID) for the communications between the vehicles. In this work, they have utilized the ID-based-cryptosystem, elliptic-curve cryptography (ECC) and chinese-remainder theorem (CRT) to provide security. To prevent the trusted-authority from becoming a source of congestion, the LSKA-ID model attempts to lessen the reliance upon the TA while performing high-frequency handovers among the different groups. The results show that the LSKA-ID model provides better security as the model utilizes random-oracle method. Wuttidittachotti and Natho [10], they presented new technique for the reducing access-time for Ciphertext-Policy by utilizing the elliptic-curve (EC). For the decryption and encryption, this work utilized the Diffie-Hellman technique. The results show that the proposed work reduce the access-time in comparison with the existing works. Nandalal and Bhakthavatchalu [11], this work main focus was to provide a security hardware model for the integrated circuits in real-time by utilizing a cryptographic blockchain. In this work they have utilized the secure-hash-algorithm (SHA-256) as well as the EC digital-signature method to provide better security framework. Furthermore, the physical-unclonable-functions (PUFs) were utilized for performing the authentication process for the transactions that would be happening inside the blockchain. The results show that the proposed work provides better security in comparison to the existing work.

Trung *et al.* [12], they have used the ECC and vigenère-symmetry-key (VSK) for building key exchanges, decryption, coding methods, digital signature and encryption. The ECC and VSK were compared against the rivest-shamir-adleman (RSA) algorithm in terms of processing cost and key size. By utilizing the ECC and VSK, this work finally presented a novel cryptosystem for the encryption of the messages. The proposed work provided an effective, secure and safe cryptosystem in comparison to the existing models. Wuttidittachotti and Preelakha [13], they presented an asymmetric encryption model using ECC and Fischer-Yates Shuffling method for the 3D mesh models. The proposed work was evaluated in terms of peak-signal noise-ratio, entropy and mean-squared-error. The results of this work present that their model provides zero mean-squared-error and infinite-value peak-signal noise-ratio. Ayoub *et al.* [14], they presented a model called as lightweight-mutual authentication (LMA) which was built on the basic of the constrained application protocol (CoAP) for the internet of things (IoT) environment and cloud environment. They have utilized the CoAP as this protocol is the best protocol when compared with the hyper-text transfer-protocol. Further, in this work they have utilized the ECC for providing security during the transmission of the data among the Internet of Things devices and the cloud environment. For evaluating their model, they utilized the AVISPA toolkit and the results show better effectiveness for providing security. Obaid and Saffar [15], they solve the issue of image encryption done using the ECC. Hence, to solve this issue they have utilized the Hilbert matrix for generating a matrix which will be a key for the encryption. This will provide better encryption and will not compress the image providing high quality images. During the decryption, this work utilized the process of inverse matrix to decrypt the image which was encrypted. The results were evaluated in terms of unified-average changing-intensity (UACI) and peak-signal to noise-ratio (PSNR). The results show that the proposed model provided better quality of images for the grayscale images.

3. PROPOSED METHODOLOGY

3.1. Elliptical curve point representation

Many types of elliptical curves are available, but few elliptical curves have been proven as NIST standard curves like the P224, P256, and P521 [16]. Among all the ECC curves, P-256 is one of the most popular curves. The NIST P-256 curve is the most extensively used prime curve in critical infrastructure projects for the ECDSA algorithm. For the curve, NIST P-256, 'k' and 'd' are the domain parameter which is 32-byte length each, and the points on the curve G of x-value and Q (public key) of y-value, consists of 32 bytes each. Thus making the signature total length of 64 bytes, i.e. 'r' 32 bytes, and s 32 bytes. Now let E be an elliptic curve of a prime field F_p with the affine (1) [17]–[19].

$$y^2 = x^3 - 3x + b \quad (1)$$

Where 'a' and 'b' are elliptical curve parameters, $a=q-3$ for the P256 curve, and $G = (xG, yG)$, a point on the curve, known as the base point. The NIST P-256 curve uses prime field FP_{256} , defined by [19].

$$P_{256} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1 \quad (2)$$

In (2), the prime field is represented by either the addition of the numbers or either by a subtraction of numbers, where the numbers are of power 2 and the exponents are multiple of 8 [19]. Let P and Q be the two points on the curve, where (3) and (4):

$$P = x_p, y_p \quad \text{and} \quad Q = x_q, y_q \quad \text{with} \quad P \neq -Q, \text{ then} \quad (3)$$

$$R = P + Q = x_r, y_r \quad (4)$$

the group of the elliptical curve can be formed in two ways, point multiplication (PM) and point doubling (PD). Consider two points P and Q, then (5):

$$P(x_p, y_p), \text{ and } Q(x_q, y_q) \quad (5)$$

are two points, thus when $P \neq Q$, it is called point addition, shown in (6),

$$R(x_R, y_R) = P(x_p, y_p) + Q(x_q, y_q) \quad (6)$$

and when $P=Q$, it is called point multiplication [14] as shown in (7) and (8):

$$R(x_R, y_R) = 2P(x_p, y_p) \quad (7)$$

$$x_R = \left(\frac{3x_p^2}{2y_p} \right) \quad (8)$$

depending upon the formation of the points P and Q the method can be selected [19].

3.2. Ate pairing using the NIST P-256 curve

There are various techniques of using the pairing-based scheme, like Weil, Tate, Miller, Ate, and Eat that can be used [20]. The millers' algorithm is used as the base for the computation of the Tate pairing algorithm. Further, Ate is another pairing algorithm that is inherited from Tate pairing [21]–[23]. Once, the points P and Q from the elliptical curve have been achieved, the Ate pairing can proceed, which further can be used for ECDSA [24]. Let π_p be the Frobenius map on the elliptical curve, defined in (9),

$$\pi_p(x, y) = (x^p, y^p) \quad (9)$$

let 't' be the trace of the Frobenius on the $E(\mathbb{F}_p)$ and $T=t-1$. Further, let as shown in (10) and (11):

$$P \in G_1 = E(F'_p)[r] \cap \text{Ker}(\pi_p - [1]) \quad (10)$$

$$Q \in G_2 = E(F'_p)[r] \cap \text{Ker}(\pi_p - [p]) \quad (11)$$

that means that Q satisfies as shown in (12):

$$\pi_p(Q) = [p]Q, \quad (12)$$

further, let $G_3 = \mu_r$ be the subgroup of \mathbb{F}_p , consisting of r^{th} roots of unity, then Ate pairing is the map in (13):

$$e_{A,r}: G_2 \times G_1 \rightarrow G_3 \\ (Q, P) \mapsto \int T, Q(P) \frac{q^k - 1}{r} \quad (13)$$

where k is called the embedded degree concerning r.

3.3. Formulating throughput and latency

Generally, throughput or network throughput is one of the important metrics to measure the performance of the network which can be measured in VANET also. To measure the throughput, other parameters like bytes sent, simulated time, and bytes per node are required.

$$simulated_{time} = simulation_{time} slot \times time_{per\ slot} \quad (14)$$

The total simulation time in (14), is calculated by the product of the simulation time slot and time per slot. For our work, a total of 65-time slots for every run for the simITS simulator has been considered, for example, if

30 nodes are considered for one simulation, then, a 65-time slot for every simulation run or simulation slot has to be considered [25]. The safety message size varies with the type of messages being sent in the network. Generally, the Safety message size ranges from 100 bytes to 200 bytes, out of which half are data and half of the message are extra bits added by the layers of the protocol. The formula below defines the bytes sent successfully concerning message size as shown in (15) [26].

$$byte_{sent} = message_{transmitte_{successful}} \times message_{size} \quad (15)$$

Further, most of the communication in the network takes between the nodes, hence node-to-node communication is excessive. Hence, in this work, define the bytes sent per user in the network have been defined as shown in (16) [25],

$$byte_{sent\ per\ user} = \frac{byte_{sent}}{number\ of\ users} \quad (16)$$

throughput refers to the amount of data being sent by a sender to the intended destination. Thus, throughput is measured by how many data or packets have been received by the receiver successfully. The total throughput can be calculated as in (17) [25].

$$total_throughput = \frac{byte_{sent} \times 8}{simulated_{time}} \quad (17)$$

Throughput can be optimized by minimizing the latency in data delivery during data transmission. Latency is inversely proportional to throughput. More the latency, the poor the throughput, and the less the latency, the better the throughput. To calculate latency, the propagation delay is also required as calculated in (18), and the sterilization delay as calculated in (19):

$$propodation_{delay} = \frac{distance}{speed} \quad (18)$$

$$serilization_{delay} = \frac{packet_{size\ bits}}{transmission_{rate\ pps}} \quad (19)$$

the latency can be calculated and reduced using (20). For calculating, other parameters i.e., distance, speed, packet size, and transmission rate are required.

$$latency = propogation_{delay} \times serilization_{delay} \quad (20)$$

To obtain better throughput, latency has to be avoided in the network. Common reasons for latency in the network are unnecessary data luring or transmitted in the network, noise, lost packets, and node failure. Also, in VANET there are more chances for the data to be in the network for any of the reasons [25], [26].

3.4. Integrating pairing based ECDSA on point-to-point topology for VANET application

The encryption algorithm, ECDSA is used to digitally sign the message to authenticate that the data is from an intended sender and not from any malicious node. By integrating ECDSA with Ate pairing, the key size can be decreased and the complexity of the algorithm can be increased. Ate not only inherits the features of Tate but it is also proven to be fast as twice. The aim of using the pairing technique is to reduce the key size without compromising the security level of the ECDSA algorithm. Hence, in this work, it is intended to integrate ECDSA and Ate pairing algorithm and create a hybrid algorithm [16], [20]. In the VANET scenario, most communication takes place between V2V, the communication is in point-to-point (P2P) protocol. The main aim is to collect information regarding any obstacles or hindrances in the communication of the vehicles in the VANET infrastructure. Further, the use of P2P in VANET speeds up the communication between V2V [27].

As shown in Figure 2, both the sender vehicle and the receiver vehicle must use the integration of the ECDSA and the Ate pairing based scheme. The only issue is that both the sender and receiver must use the same pairing technique. Further, there are two methods like point doubling (PD) or point multiplication (PM) in an ECDSA. But there is more delay in key generation rather than key verification. Thus, there is possibly a delay in encrypting and less delay during decryption. But as per our results, the delay is in the initial nodes, as the communication is within a large number of nodes, and the delay has reduced in the later stages [20], [28].

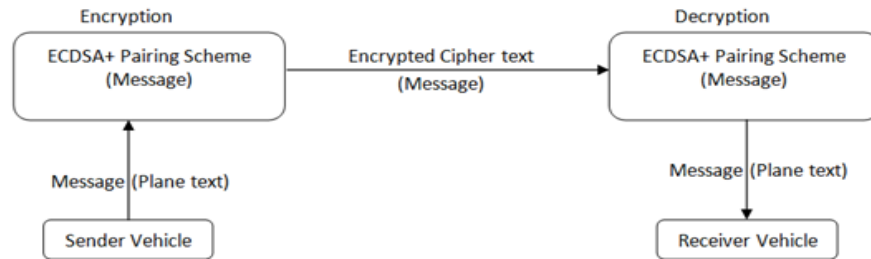


Figure 2. Integration of pairing based scheme with ECDSA

4. RESULTS AND DISCUSSIONS

In this section, ECDSA with Ate pairing has been integrated into the simITS simulator. As the Ate algorithm inherits the properties of TATA, it also adds more features. The Pairing algorithm is used to add more security without adding more complexity to the key generation and the key generation time. The results obtained are startling. In this work, the US-based dedicated short range communications (DSRC) standards have been used. Further, the US-based DSRC standards, hence the data transfer ranges from 3 Mbps, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, and 27 Mbps have been followed. For our work, the least 3 Mbps and the maximum of 27 Mbps, are considered for our results. Further for the safety message, the specified delay or latency ranges from 100 ms, 150 ms, 200 ms, 250 ms, and 300 ms. The throughput vs delay parameter for a better analysis of our results has been compared. Hence first select the data transfer rate as 3 Mbps and the message size as 50 bytes. In this work, the ECDSA and the hybrid ECDSA which is integrated with Ate pairing have been compared. Further, the Curve fitting for the values obtained from our results has been plotted. In curve fitting, the trendline can be used as a fitting function, that is of the highest-order polynomial, and the R² is a calculation for the goodness of fit for the model values obtained. In this work, by selecting the data rate as 3 Mbps and the message size as 50 bytes the experimentation is started.

From Table 1, it can be observed that the hybrid ECDSA takes slightly more time than the simple ECDSA, but on the other hand, the strength of ECDSA and the security of the message is increased. By taking the values from Table 1, the curve fitting graph has been plotted, and it can be observed that both the curves almost meet at 250ms delay. Thus, for the simple ECDSA, the polynomial (21) can be obtained,

$$y = 1E - 09x^4 - 1E - 06x^3 + 0.0003x^2 - 0.0264x + 2.3419 \quad (21)$$

and the R² = 1, indicating the values are ideal. Similarly, for the hybrid ECDSA, the following polynomial (22) is obtained,

$$y = 2E - 09x^4 - 1E - 06x^3 + 0.0005x^2 - 0.061x + 4.05 \quad (22)$$

and the obtained R² = 1, indicates that the values are ideal. For the second comparison, the data rate of 3 Mbps and the message size is 100 bytes are chosen. The comparison of the results can be seen in Table 2.

Table 1. Throughput vs delay for data rate 3 Mbps and message size 50 bytes

Delay in milliseconds	ECDSA (only)	ECDSA with Ate pairing
100	1.268987989	1.393603333
150	1.21665471	1.458089889
200	1.332145654	1.488730667
250	1.354135265	1.428363333
300	1.246897973	1.409855111

Table 2. Throughput vs delay for data rate 3 Mbps and message size 100 bytes

Delay in milliseconds	ECDSA (only)	ECDSA with Ate pairing
100	1.23654871	1.461747889
150	1.262134153	1.454369
200	1.23301231	1.456874333
250	1.234562142	1.43171178
300	1.243652146	1.327777333

The curve fitting can be observed in Figures 3 and 4. In Figure 3, the hybrid ECDSA has a stable throughput of around 1.45 ms till 250 ms delay, and after 250 ms the throughput is reduced. Though the ECDSA has a stable throughput, the overall throughput of simple ECDSA is less compared to hybrid ECDSA. Further, in Figure 4, the Hybrid ECDSA has a stable throughput of around 1.45 ms till a 250 ms delay, and after 250 ms the throughput is reduced. Though the ECDSA has a stable throughput, the overall throughput of simple ECDSA is less compared to Hybrid ECDSA. The polynomial equation for simple ECDSA can be obtained using the (23),

$$y = -9E - 11x^4 - 1E - 08x^3 + 8E - 0.6x^2 - 0.002x + 1.5886 \tag{23}$$

and the $R^2 = 1$, indicates that the values are ideal. Similarly, the Hybrid ECDSA can be obtained using the following polynomial (24),

$$y = -7E - 10x^4 + 6E - 07x^3 + 0.0002x^2 - 0.0246x + 0.137 \tag{24}$$

and the obtained $R^2 = 1$, indicates that the values are ideal. Further, in this work, the transfer rate has been increased to 27 Mbps which is the maximum transfer rate of DSRC, and set the message size to 50 bytes. The results of ECDSA and hybrid ECDSA are shown in Table 3.

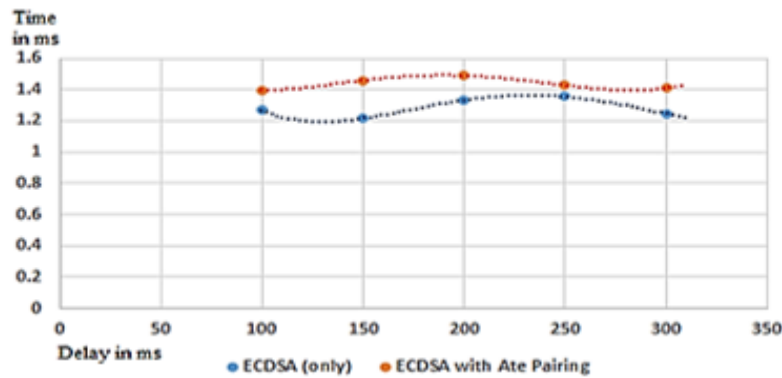


Figure 3. Throughput vs delay for data rate 3 Mbps and message size 50 bytes

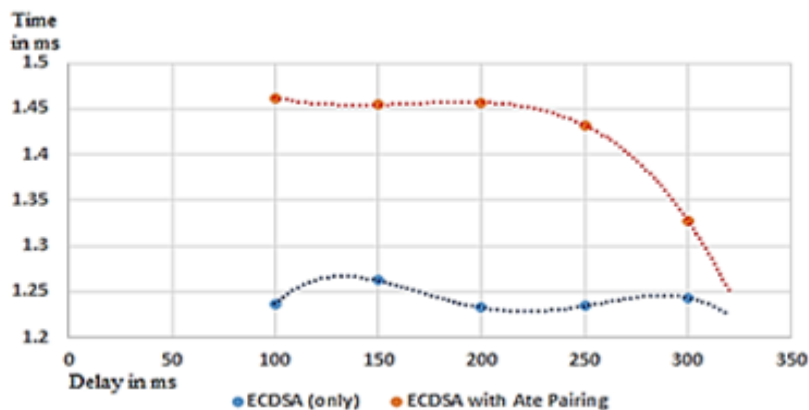


Figure 4. Throughput vs delay for data rate 3 Mbps message size 100 bytes

Table 3. Throughput vs delay for data rate 27 Mbps and message size 50 bytes

Delay in milliseconds	ECDSA (only)	ECDSA with Ate pairing
100	11.36547891	13.21534289
150	11.36541562	12.71053244
200	12.45698745	12.76881322
250	12.65474125	12.5797942
300	13.00120132	12.87629889

The comparison can be seen in Figure 5. The throughput of simple ECDSA is unstable, and further, the throughput increases gradually with the increase in the delay. On the other hand, in Hybrid ECDSA, the throughput is better and more stable compared to the simple ECDSA. The polynomial equation for simple ECDSA can be obtained using the (25),

$$y = 1E - 08x^4 - 8E - 06x^3 + 0.0024x^2 - 0.3065x + 26.872 \tag{25}$$

and the $R^2 = 1$, indicates that the values are ideal. Similarly, the Hybrid ECDSA can be obtained using the following polynomial (26),

$$y = 2E - 08x^4 - 2E - 05x^3 + 0.005x^2 - 0.6152x + 37.722 \tag{26}$$

and the obtained $R^2 = 1$, indicates that the values are ideal. In the last case, the Transfer rate of 27 Mbps has been selected but increased the message size to 100 bytes. The results are shown in Table 4.

Table 4. Throughput vs delay for data rate 27 Mbps and message size 50 bytes

Delay in milliseconds	ECDSA (only)	ECDSA with Ate pairing
100	10.36547891	12.27756033
150	10.36541562	12.05954444
200	11.45698745	12.83492578
250	11.65474125	12.493456
300	12.00120132	12.994127

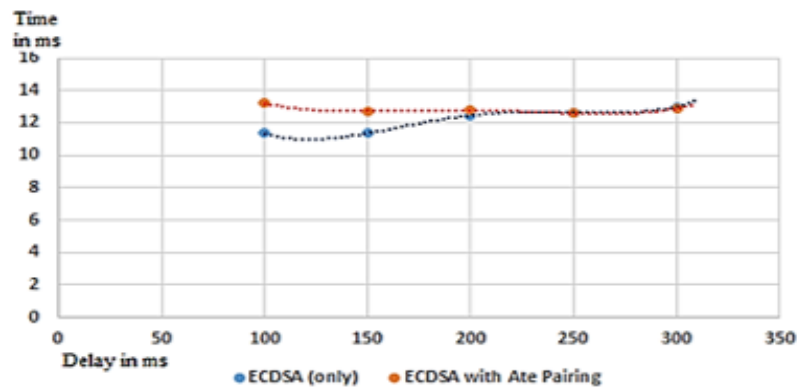


Figure 5. Throughput vs delay for data rate 27 Mbps and message size 50 bytes

In Figure 6, it can be seen that in both the simple ECDSA and hybrid ECDSA, the throughput is increasing gradually and both curves appear to be identical. The Hybrid ECDSA has a slightly more delay otherwise both the curves are identical.

The polynomial equation for simple ECDSA can be obtained using the (27),

$$y = 3E - 08x^4 - 2E - 05x^3 + 0.00063x^2 - 0.7591x + 44.481 \tag{27}$$

and the $R^2 = 1$, indicates that the values are ideal. Similarly, the Hybrid ECDSA can be obtained using the following polynomial (28),

$$y = 2E - 08x^4 - 2E - 05x^3 + 0.005x^2 - 0.6512x + 36.722 \tag{28}$$

and the obtained $R^2 = 1$, indicates that the values are ideal. Further, it can be observed that (26) and (28) are the same. The polynomial equations obtained for a data rate of 27 Mbps are the same for any message size. In all the cases, it can be observed that, by adding Ate pairing to ECDSA, the overall performance of ECDSA is improved in terms of key generation time and data communication time. By adding ECDSA, the authentication, and privacy of the vehicles are maintained. In this work, the NIST-specified standard curve has been used, and the strength of the ECDSA algorithm is maintained. The main goal is to see the performance of the hybrid ECDSA, as to reduce the complexity with maintaining the strength of ECDSA.

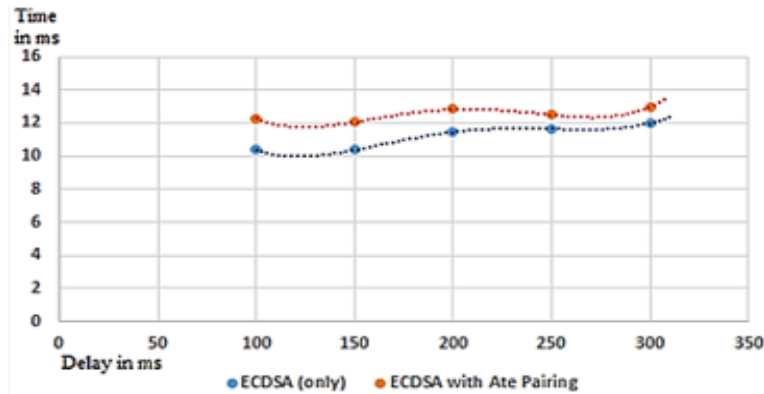


Figure 6. Throughput vs delay for data rate 27 Mbps and message size 100 bytes

5. CONCLUSION

VANET is the most upcoming and growing rapidly network. The communication in VANET is between the vehicles and between the vehicle and the road side unite, but mostly the communication is between the vehicles themselves. There are various types of data being exchanged between the vehicles, like infotainment data or Safety information. In this work, the main aim has been to target the Safety Messages that are very critical in the VANET network. The purpose of these messages is that they give critical information to the driver and the vehicle, resulting in saving the lives of the driver and the passengers in the vehicle. The delay for the safety messages is in the range of 100 milliseconds to a maximum of 300 milliseconds. The major concern in VANET is that the communication is open, making the network vulnerable to any attack. In this work, ECDSA for the VANET network onto a simITS simulator has been implemented. For implementation, this work has chosen the standard 256 elliptical curves for ECDSA. For communication, the US-based DSRC standards for selecting the data transfer rate have been used. The least 3 Mbps and the maximum 27 Mbps data transfer rate has been selected. Further, the ECDSA has been optimized by integrating Ate pairing algorithm into it. The advantage of including the Ate pairing algorithm is that it increased the ECDSA strength, but it also helps to reduce the complexity of ECDSA to generate the public and private keys. It can be seen in the obtained results, that hybrid ECDSA has better throughput than the simple ECDSA-based throughput. In the future, other pairing based algorithms can be implemented to see if the ECDSA can further be optimized to get better throughput. Implementing PBC can also be extended on any elliptical curve rather than implemented on standard curves.




REFERENCES

- [1] F. Khan, R. L. Kumar, S. Kadry, Y. Nam, and M. N. Meqdad, "Autonomous vehicles: A study of implementation and security," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 4, pp. 3013–3021, Aug. 2021, doi: 10.11591/ijece.v11i4.pp3013-3021.
- [2] R. Mariani, "An overview of autonomous vehicles safety," in *IEEE International Reliability Physics Symposium Proceedings*, Mar. 2018, vol. 2018-March, pp. 6A.11-6A.16, doi: 10.1109/IRPS.2018.8353618.
- [3] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Networks*, vol. 90, p. 101823, Jul. 2019, doi: 10.1016/j.adhoc.2018.12.006.
- [4] "Autonomous vehicles factsheet," *Center for Sustainable Systems*. <https://css.umich.edu/publications/factsheets/mobility/autonomous-vehicles-factsheet>.
- [5] A. O. A. Zaabi, C. Y. Yeun, and E. Damiani, "Autonomous vehicle security: Conceptual model," May 2019, doi: 10.1109/ITEC-AP.2019.8903691.
- [6] T. Shon, "In-vehicle networking/autonomous vehicle security for internet of things/vehicles," *Electronics*, vol. 10, no. 6, p. 637, Mar. 2021, doi: 10.3390/electronics10060637.
- [7] R. Passerone *et al.*, "A methodology for the design of safety-compliant and secure communication of autonomous vehicles," *IEEE Access*, vol. 7, pp. 125022–125037, 2019, doi: 10.1109/ACCESS.2019.2937453.
- [8] S. Long, "A comparative analysis of the application of hashing encryption algorithms for MD5, SHA-1, and SHA-512," *Journal of Physics: Conference Series*, vol. 1314, no. 1, p. 12210, Oct. 2019, doi: 10.1088/1742-6596/1314/1/012210.
- [9] M. A. Alazzawi, M. T. Almalchy, A. Al-Shammari, A. S. Al-Khaleefa, and H. M. Albehadili, "LSKA-ID: A lightweight security and key agreement protocol based on an identity for vehicular communication," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 21, no. 4, pp. 784–796, Aug. 2023, doi: 10.12928/TELKOMNIKA.v21i4.24388.
- [10] P. Wuttidittachotti and P. Natho, "Improved ciphertext-policy time using short elliptic curve Diffie-Hellman," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 4, pp. 4547–4556, Aug. 2023, doi: 10.11591/ijece.v13i4.pp4547-4556.
- [11] D. K. Nandalal and R. Bhakthavathalu, "Design of programmable hardware security modules for enhancing blockchain based security framework," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 3, pp. 3178–3191, Jun. 2023, doi: 10.11591/ijece.v13i3.pp3178-3191.
- [12] M. M. Trung, L. P. Do, D. T. Tuan, N. Van Tanh, and N. Q. Tri, "Design a cryptosystem using elliptic curves cryptography and Vigenère symmetry key," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 2, pp. 1734–1743, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1734-1743.




- [13] P. Wuttidittachotti and P. Praelakha, "An asymmetric encryption method for 3D mesh model using elgamal with elliptic curve cryptography," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 27, no. 2, pp. 959–969, Aug. 2022, doi: 10.11591/ijeecs.v27.i2.pp959-969.
- [14] A. Ayoub, R. Najat, and A. Jaafar, "A lightweight secure CoAP for IoT-cloud paradigm using elliptic-curve cryptography," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 3, pp. 1460–1470, 2020, doi: 10.11591/ijeecs.v20.i3.pp1460-1470.
- [15] Z. K. Obaid and N. F. H. Al Saffar, "Image encryption based on elliptic curve cryptosystem," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 2, pp. 1293–1302, Apr. 2021, doi: 10.11591/ijece.v11i2.pp1293-1302.
- [16] J. Petit, "Analysis of ECDSA authentication processing in VANETs," *2009 3rd International Conference on New Technologies, Mobility and Security, Cairo, Egypt*, Dec. 2009, doi: 10.1109/NTMS.2009.5384696.
- [17] K. Ravi, R. Khanai, and K. Praveen, "Survey on pairing based cryptography for wireless sensor networks," in *Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016*, 2016, vol. 2, doi: 10.1109/INVENTIVE.2016.7824802.
- [18] M. Adalier and A. Teknik, "Efficient and secure elliptic curve cryptography implementation of curve p-256," *In Workshop on elliptic curve cryptography standards*, vol. 66, no. 446, pp. 2014–2017, 2015.
- [19] D. W. Park, N. S. Chang, S. Lee, and S. Hong, "Fast implementation of NIST p-256 elliptic curve cryptography on 8-bit AVR processor," *Applied Sciences (Switzerland)*, vol. 10, no. 24, pp. 1–16, Dec. 2020, doi: 10.3390/app10248816.
- [20] J. M. Miret, D. Sadornil, and J. G. Tena, "Pairing-based cryptography on elliptic curves," *Mathematics in Computer Science*, vol. 12, no. 3, pp. 309–318, Jun. 2018, doi: 10.1007/s11786-018-0347-3.
- [21] N. B. Mbiang, D. D. F. Aranha, and E. Fouotsa, "Computing the optimal ate pairing over elliptic curves with embedding degrees 54 and 48 at the 256-bit security level," *International Journal of Applied Cryptography*, vol. 4, no. 1, pp. 45–59, 2020, doi: 10.1504/IJACT.2020.107167.
- [22] L. Ghammam and E. Fouotsa, "Improving the computation of the optimal ate pairing for a high security level," *Journal of Applied Mathematics and Computing*, vol. 59, no. 1–2, pp. 21–36, Feb. 2019, doi: 10.1007/s12190-018-1167-y.
- [23] A. Guillevic, S. Masson, and E. Thomé, "Cocks–Pinch curves of embedding degrees five to eight and optimal ate pairing computation," *Designs, Codes, and Cryptography*, vol. 88, no. 6, pp. 1047–1081, Mar. 2020, doi: 10.1007/s10623-020-00727-w.
- [24] E. Khamseh, "The review on elliptic curves as cryptographic pairing groups," *Mathematics and Computational Sciences*, vol. 2, no. 2, pp. 50–59, 2021.
- [25] M. Manzano, F. Espinosa, Á. M. Bravo-Santos, and A. Gardel-Vicente, "Cognitive self-scheduled mechanism for access control in noisy vehicular ad hoc networks," *Mathematical Problems in Engineering*, vol. 2015, pp. 1–12, 2015, doi: 10.1155/2015/354292.
- [26] S. Yousefi, M. Fathy, and A. Benslimane, "Performance of beacon safety message dissemination in vehicular ad hoc networks (VANETs)," *Journal of Zhejiang University: Science A*, vol. 8, no. 12, pp. 1990–2004, Nov. 2007, doi: 10.1631/jzus.2007.A1990.
- [27] D. Kosmanos, A. Argyriou, and L. Maglaras, "Estimating the relative speed of RF jammers in VANETs," *Security and Communication Networks*, vol. 2019, pp. 1–18, Nov. 2019, doi: 10.1155/2019/2064348.
- [28] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs," *Journal of Systems Architecture*, vol. 103, p. 101692, Feb. 2020, doi: 10.1016/j.sysarc.2019.101692.

BIOGRAPHIES OF AUTHORS






Ravi Kalkundri    completed his Bachelor of Engineering in Computer Science and Engineering and completed in 2009 from Gogte Institute of Technology, Belgaum. He worked in industries at different positions like Software Engineer and Senior Software Engineer. In 2011, he went on to peruse Masters in Technology in Computer Science and Engineering, from Gogte Institute of Technology, Belgaum. Currently he is working as Assistant Professor at Gogte Institute of Technology in the Department of Computer Science and Engineering, and currently perusing his Ph.D. in the field of network security. His research interests are in the area of ad hoc networks specializing in the area of VANETS and security. Assistant Professor Ravi is a Life Member of Indian Society for Technical Education. He can be contacted at email: ravi.kalkundri05@gmail.com.



Rajashri Khanai    received her Ph.D. in "error correction coding and cryptography for wireless networks" from the Visvesvaraya Technological University, Belagavi, India. Her research interests include error control codes, cryptography, machine learning applications to signal analysis. She is currently Head and Professor in Department of Computer Science and Engineering, at KLE's Dr. M. S. Sheshgiri College of Engineering and Technology, Belagavi, Karnataka, India. She has published over 20 academic papers. Dr. Rajashri is a member of IEEE. She can be contacted at email: rajashrikhanai@klescet.ac.in.



Praveen Kalkundri    completed his Bachelor of Engineering in Electronics and Communication Engineering and completed in 2009 from Gogte Institute of Technology, Belgaum. He worked in industries at different positions like Software Engineer and Senior Software Engineer. In 2011, he went on to peruse Masters in Technology in VLSI design in Embedded Systems, from KLE Dr. M.S. Sheshgiri College of Engineering and Technology, Belgaum. Currently he is working as Assistant Professor at Gogte Institute of Technology in the Department of Electronics and Communication Engineering, and currently perusing his Ph.D. in the field of VLSI design. Assistant Professor Praveen is a Life Member of Indian Society for Technical Education. He can be contacted at email: pukalkundri@git.edu.