designs

MDPI

Article

Privacy-Aware Secure Routing through Elliptical Curve Cryptography with Optimal RSU Distribution in VANETs

Ghadeer Ghazi Shayea, Dheyaa Abdulameer Mohammed, Ali Hashim Abbas * and Nejood Faisal Abdulsattar

Department of Computer Technology Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad 10001, Iraq
* Correspondence: alsalamy1987@gmail.com

Abstract: Vehicular Ad-Hoc Networks (VANETs) are the backbone of the intelligent transportation system, which consists of high-speed vehicles with huge dynamic mobility. The communication takes place with a vehicle-to-vehicle, vehicle to infrastructure, with traffic signals. The major flaw of this kind of network is that due to high mobility in VANETs, the communication overhead is so high that it directly affects the efficiency of the network. Security is also holding a vital role in VANETs. The attackers can easily capture vehicle details of this type. To overcome this drawback, security should also need to get improved. This paper introduces Elliptical Curve Cryptography with Generic Algorithm based Privacy-Aware Secure Routing (ECC-GA-PASR), which is the combination of two methods such as optimal RSU distribution and elliptical curve cryptography (ECC) based authentication. RSU distribution is optimized by using the generic algorithm (GA) as well as to improve the authentication in trusted authority (TA) ECC algorithm is used. By using these two concepts, the proposed method reduced the communication overhead and increased the security of the network. The simulation is conducted throughput NS2 and SUMO. The performance analysis is performed concerning vehicle count, varying speed, and malicious activities. The parameters that are concentrated for this performance analysis are energy efficiency, packet delivery ratio, overhead, and packet loss. The performance of the proposed method is calculated and compared with earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV. Compared with the earlier works, the proposed ECC-GA-PASR produced 15% better efficiency, 12% better packet delivery ratio, 50% lower overhead, and 30% lower packet loss.

Keywords: VANETs; security; ECC; genetic algorithm; RSU distribution; trusted authority

Citation: Shayea, G.G.; Mohammed, D.A.; Abbas, A.H.; Abdulsattar, N.F. Privacy-Aware Secure Routing through Elliptical Curve Cryptography with Optimal RSU Distribution in VANETs. *Designs* **2022**, *6*, 121. https://doi.org/10.3390/designs6060121

Academic Editor: Bhanu Shrestha

Received: 6 October 2022
Accepted: 1 November 2022
Published: 1 December 2022

1. Introduction

The vehicular Ad-Hoc Network (VANETs) is the future generation technique for intelligent transportation system (ITS). In general, VANETs is the subdivision of the mobile Ad-Hoc Networks (MANETs) that gain more attention from the government, academic and industrial sector [1]. The main types of VANETs communicate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Commonly, the VANET network is equipped with a trusted authority (TA) and Road-Side Units (RSUs) to control the vehicles in the network. Each vehicle consists of a tamper-proof device called the On-Board Unit (OBU), which is mainly used to accumulate significant secret vehicle information and vehicle identity. Earlier, in a maximum of cases, vehicle-to-vehicle communication took place, but in recent days, information has been transmitted from vehicles to the nearby RSUs [2]. The significant challenges in VANETs are it needs low latency, high safety, speed, and stability [3]. Additionally, through an improper mobility model the energy consumption, latency and overhead are increased in the real traffic scenario [4].

VANETs are highly susceptible to malicious behaviors such as eavesdropping, impersonation, etc. To protect the network from such malfunctions, several authentications as well as cryptography techniques are developed, but it has certain drawbacks when applied

to huge dynamic mobility-based VANETs. In classic authorization and revocation schemes, digital signature and cryptography technologies overhead occur when it is applied to high-speed VANETs. The trustworthiness and messages are moderate. In a dynamic vehicular network, the road environment is complex, so achieving high stability is an essential task. Figure 1 shows the communication types in VANETs.

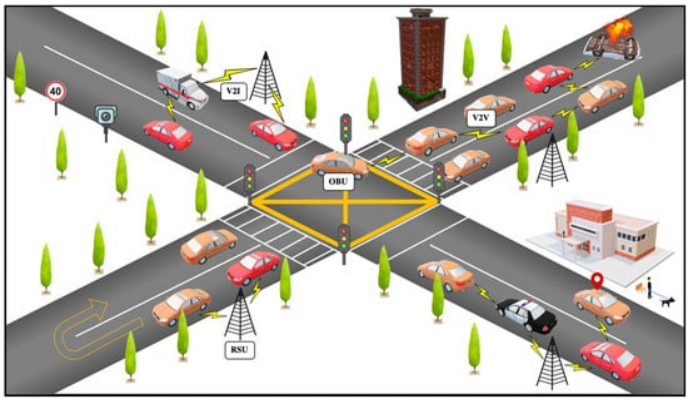

Figure 1. VANETs Communication.

Many concepts are introduced by the researchers to solve the privacy issues in VANETs in order to fulfill the indispensable prerequisite such as reliability, traceability, and link stability, etc., but those methods produce high communicational overhead during the process of communication in the network, and it requires substantial memory space [5–7]. In recent studies, pseudonym-based message authentication, as well as group-based message authentication, are initiated, which helps to improve the privacy of the trusted authority (TA) in VANETs [8,9]. Meticulously, privacy-preserving features must be guaranteed in VANETs. The process of authentication during communication secures the real identities of vehicles from attackers. Racing those vehicles, the TA needs an efficient method to find the real identities of vehicles, due to this criteria's creating high-speed VANETs with efficient real-time authentication, which is still an open research area [10]. In VANETs, communication takes place in open wireless communication. Vehicle-to-vehicle and vehicle-to-infrastructure communications are conducted through open wireless channels so that the attacker vehicle can, without difficulty, alter the process by interrupting and deleting the information. The attacker vehicle can easily arrest the real identities and other traffic-oriented details of the vehicles, which are very dangerous for the drivers. In some cases, the attacker vehicle broadcasts a false message that leads to traffic problems such as congestion and road accidents. For this reason, researchers provide more attention to VANETs security [11,12]. It is essential to design VANETs with well-organized security solutions. The efficiency of the VANETs is not only dependent on security; it is also related to the computational cost and communication overhead. The VANETs with high security and less computational overhead lead to efficient vehicular communication, so this research improves the security and reduces the computational cost of the VANETs. The contribution of the research study is given below. The contribution of this research is as follows:

- Enhancing the performance of high-speed VANETs in terms of security and computational overhead is concentrated.
- Proposed a privacy-aware secure routing using elliptical curve cryptography with optimal RSU distribution to improve the performance of VANETs
- Through the elliptical curve cryptography, the trusted authority becomes highly secured, which leads to improving the authentication and confidentiality of VANETs.
- To control the computational overhead of VANETs optimal RSU distribution is performed using a Genetic Algorithm.
- Thread models such as Sybil attacks and black hole attacks are introduced to analyze the performance of the network.

This paper is organized as follows. In Section 2, the related works are discussed in terms of optimization and security-based approaches. In Section 3, the network model, the thread model, the background of ECC, and the genetic algorithm are discussed. In Section 4, privacy-aware secure routing using elliptical curve cryptography with optimal RSU distribution is elaborated. In Section 5, results are analyzed in terms of the number of vehicles and speed. Section 6 concludes the research with future directions.

2. Related Works

2.1. Optimization-Based Approaches

Ref. [13] created a new routing protocol with the combination of an Ad-Hoc On-Demand Vector (AODV) and Ant Colony Optimization (ACO) technique to improve the concept of path selection. Hence, VANETs are highly dynamic in nature; it is essential to optimize the network, which helps to reduce the congestion in the network and also to reduce the consumption of energy. This method generates a path with the shortest distance that results in high throughput, low packet loss, and delay. However, it fails to reduce the routing overhead, and it is not suitable for a network with huge mobility.

Ref. [14] introduced Vehicular Ad Hoc Networks (VANETs) with Reliability Aware Multi-Objective Optimization Based VANETs Routing (RAMO), which is combined with Enhanced Gaussian Mutation Harmony Searching (EGMHS). The process behind this search is Gaussian mutation, objective decomposition, and a harmony memory extraction algorithm. This method helps to increase the parameters such as delay and packet delivery ratio. The drawback is that the throughput of the network is not concentrated.

Ref. [15] presented a model to address the One-Dimensional Roadside unit Deployment (D1RD) problem with the help of a greedy approach called Greedy2P3E. This method helps to achieve better performance in real vehicle trajectories. The achieved result is moderate. Ref. [16] created a Deep Independent Q-Learning model to reduce the delay in Unmanned Aerial Vehicles (UAVs). The concept behind this model is multi-agent reinforcement learning (MARL). This method helps to reduce the complexity of the highway models. The overall performance is moderate. The communication type of UAV shows in Figure 2.

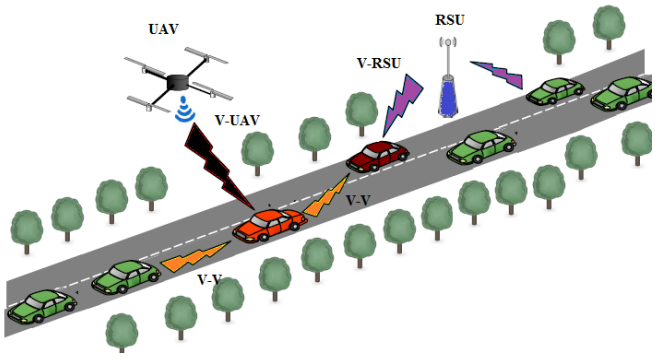

Figure 2. UAV Communication.

Ref. [17] proposed two discretized variants of cuckoo search optimization (CSO) to improve the routing performance in VANETs. The two variants are the Lévy flight-based discrete variant and the random walk-based discrete variant. High route reliability is achieved using this method. This method is suitable for networks with low vehicle density scenarios.

Ref. [18] presented a new approach to improve the optimization of routing. The drawbacks in traditional protocols such as AODV, OLSR, and DSDV are analyzed. To overcome that, the Hybrid Genetic Firefly Algorithm-based Routing Protocol (HGFA) is introduced. This method achieves better performance when compared with traditional optimization techniques such as PSO and ACO.

Ref. [19] proposed a model to secure the network from traffic congestion, and roadside accidents called the Multi-Objective Harris Hawks Optimization (2HMO-HHO) algorithm. It is based on a 2-Hop routing algorithm. The parameters that are improved by using this method are delay, packet delivery ratio, throughput, and overhead. This method is suitable for the network with low vehicle density scenarios, not for densely populated areas.

Ref. [20] introduced a method to reduce the end-to-end delay of the network called a hybrid-fuzzy logic-guided genetic algorithm (H-FLGA) approach. By the use of this method, the network flexibility and scalability are increased, which leads to minimizing the value of end-to-end delay. However, this method fails to concentrate on packet delivery ratio and throughput.

2.2. Security-Based Approaches

Ref. [21] presented a new mutual authentication and key agreement protocol to improve the security, anonymity, and intractability of the VANETs with an Intelligent Transportation System (ITS). The proposed method achieves low communication and computational overheads and better security. The method can be applied to the network with low-populated areas; hence, the throughput is low.

Ref. [22] proposed a Physical Unclonable Function to reduce overhead and network traffic and protect the network from cloning attacks. To minimize the overhead of authentication and to increase the network throughput, the network is constructed with three layers, namely roadside units, roadside unit gateways, and trusted authority. From the simulated results, it shows that this reduced greatly reduces the MAC/PHY overhead and improves security against various types of attacks. Hence, the throughput and bandwidth are low; this model becomes not suitable for densely populated areas.

Ref. [23] constructed a multi-tiered hybrid IDS to investigate the vulnerabilities of intra-vehicle and external networks. This method incorporates signature-based IDS and an anomaly-based IDS to detect active (known) and passive (unknown) attacks. The detection accuracy achieved for active attacks is 99%, and the detection accuracy achieved for passive attacks is 98%. However, this method fails to achieve high throughput and bandwidth; hence, this model is not appropriate for highly populated areas.

Ref. [24] presented a multi-level privacy preservation for the vehicles by introducing blockchain technology with homomorphic encryption and circle-based location verification. It is one of the decentralized location privacy-preserving models. This method achieves high security, and the system becomes efficient and feasible in practice.

Ref. [25] designed a novel blockchain-enabled certificate-based authentication scheme to achieve low communication and computational overheads. Through this authentication process, a secure transaction is conducted, Cluster Head (CH) and the RSU as show in Figure 3. The result, this system achieves low communication and computational overheads.

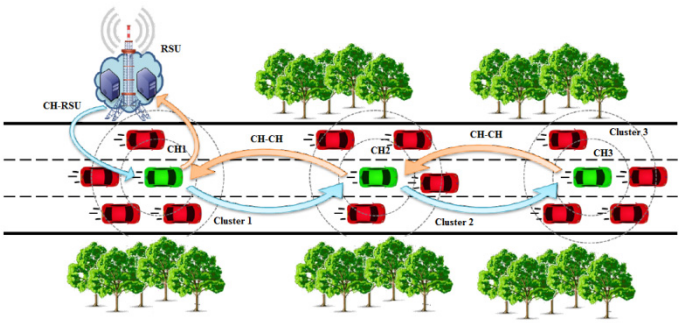

Figure 3. Cluster-based VANETs.

Ref. [26] presented an approach to provide security to VANETs during data transmission on both vehicles-to-vehicle as well as a vehicle to infrastructure communication. In general, a malfunction occurs in the network, so a secured AODV protocol is introduced

to protect the network from the black hole attack. Additionally, a cryptography function-based encryption and decryption is conducted to obtain better performance. This method achieves better performance in terms of packet delivery ratio as well as the drop, delay, and overhead are reduced. However, it fails to achieve high throughput.

Ref. [27] proposed a two-level detection system to protect the VANETs from Blackhole attacks. The first level is trusting value calculation of the neighboring vehicles, and the second level is authorized Road Side Units (RSUs) creations with the help of a blockchain system. The trust score of the vehicles is improved using these levels. The network efficiency and scalability are increased, which leads to achieving overall better performance. Table 1 describes the summary of the existing methods.

Table 1. Summary of related works.

Ref.	Objectives	Algorithms Used	Limitations
[13]	To provide the best path selection in AODV	Improved Ant Colony Optimization in AODV	High overhead and low vehicle density
[14]	To provide optimization in VANETs	Reliability Aware Multi-Objective Optimization Based VANETs Routing (RAMO) and Enhanced Gaussian Mutation Harmony Searching (EGMHS)	Low throughput
[17]	To provide optimization and routing performance in VANETs	Two discretized variants of the Cuckoo search optimization (CSO)	Low vehicle density scenario
[18]	To improve the optimization of VANETs routing	Hybrid Genetic Firefly Algorithm-based Routing Protocol (HGFA)	High overhead
[19]	To provide traffic congestion control in VANETs	Multi-Objective Harris Hawks Optimization (2HMO-HHO) algorithm	Low vehicle density scenario
[20]	To create delay aware VANETs network	hybrid-fuzzy logic guided genetic algorithm (H-FLGA) approach	Packet delivery ratio and throughput are moderate
[21]	To improve the security, anonymity, and untraceability of the VANETs	A new mutual authentication and key agreement protocol	Throughput is moderate
[22]	To provide security against attacks	Physical Unclonable Functions	Low vehicle density scenario
[23]	To improve detection accuracy of VANETs	A multi-tiered hybrid IDS	Throughput and bandwidth are low
[24]	To provide security against attacks	A multi-level privacy preservation	Low vehicle density scenario
[25]	To improve security in VANETs	Novel blockchain-enabled certificate-based authentication scheme	Packet delivery ratio and throughput are moderate
[26]	To provide security to VANETs	A cryptography function-based encryption and decryption	Throughput is moderate
[27]	To provide security of VANETs	A two-level detection system	Low vehicle density scenario

3. Basic Assumptions

3.1. Network Model

The network model of the proposed research includes N number of devices such as smart vehicles (SVs), roadside units (RSUs), static/mobile devices, and trusted authority (TA) [28] which are concerned through DSRC, wireless communication or 3G/4G/5G. Finally, the trusted authority is connected to the remote cloud (RC). The architecture of the proposed method is given in Figure 4.

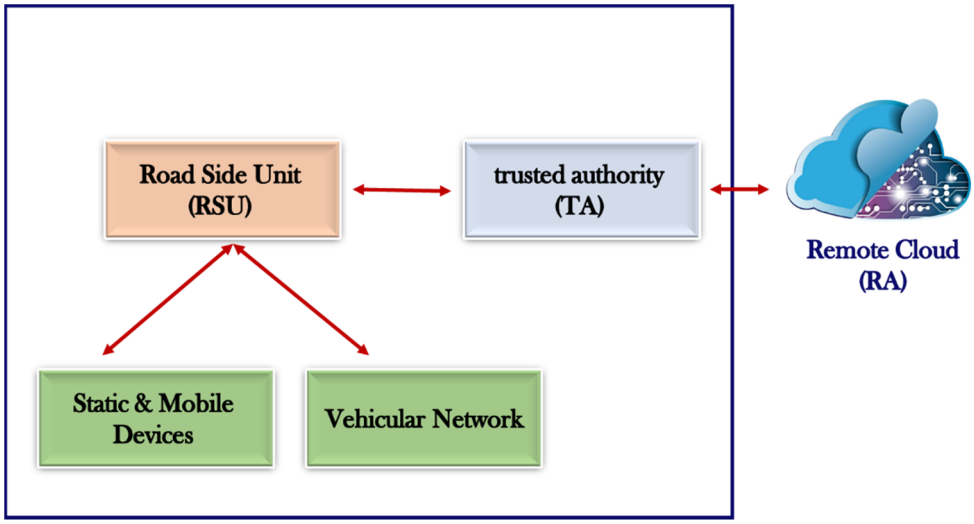

Figure 4. Proposed Network Architecture.

Smart Vehicles (SVs): Each individual SV in the network consists of certain devices for wireless communication. They are the On-Board Unit (OBU), IBC mechanism, and PKI mechanism for data transmission, a tamper-proof device (TPD), a global positioning system (GPS), and a graphical user interface (GUI). Additionally, it requires a routing protocol for wireless data transfer, energy, and storage capacity. Apart from this, the SVs will act smart through their new capabilities, as it consists of computing resource states with roles such as computing resource seller, computing resource buyer, or idle node. Any SVs, at any time instance, are able to share its computing resources for paid service to the buyer. The offloading tasks of the buyers using the currently received computing resources have to be handled by the seller vehicle [29].

Road Side Units (RSUs): In the network, the RSUs are present on the roadsides, and it is static in nature. It is mainly used to give service to the TA and the SVs. To perform the operation of communication with SVs, RSU uses routing protocols. RSUs will authenticate the SVs' communication from various environments. They should contain all the capabilities to manage the computing resource state of SVs which are present in its coverage area. The computing resource-sharing details of all the SVs are managed by the RSUs. Hence the storage and efficiency of the RSUs are very much closer to the TA. Additionally, the RSUs contain tamper resistance hardware (TRH), which acts as a memory device to store private information in a secure manner, and it also evaluates the quality of the messages during the process of communication between the SVs to RSUs.

Static/Mobile Devices: The portable computing device are able to communicate with the vehicles, such as wireless sensors, mobile phones, wearables, tablets, etc., using 3G/4G/5G or Wi-Fi [30]. Each device consists of a smart card (smart chip) to perform certain operations such as computation management and storage. That smart chip controls all the operations during the process of communication between the SVs/mobile devices to RSUs.

Trusted Authority (TA): The major functionalities of TA are to generate and transmit the public system parameters and additionally monitor the SVs and the RSUs. TA helps to protect the data transmission by assigning pseudo-identities to SVs, which leads to generating the private keys in the SVs. It maintains the database and stores the information on the SVs' pseudo-identities. TA is assigned with high energy and high storage when compared with the other sections.

Remote Cloud (RC): RC acts as the central registration center for the TAs of several regions. Through TAs, the RC will control all the devices, such as SVs, RSUs, and static/mobile devices. The localization process of RSUs is controlled directly by the RC according to the registration of the end users, such as SVs and static/mobile devices. It

maintains a private, secure database that consists of all the information of the system. The symbols and descriptions used in the research are given in Table 2.

Table 2. Symbols and Descriptions.

Symbols	Descriptions
SV	Smart Vehicle
RSU	Road Side Unit
TA	Trusted Authority
RC	Remote Cloud
DDoS	Denial of Services
RoS	Rank of Service
SV_1	Source Smart Vehicle
SV_2	Destination Smart Vehicle

3.2. Thread Model

In VANETs, huge devices are interconnected, and that leads to several security threads such as Denial of service (DoS), Bogus data, Information suspension, and Eavesdropping. Therefore, it is essential to ensure the safety perspective as well as improve the privacy of data. Consequently, the network has to be created in a form that, even under attack, the efficiency is not compromised. Among the predefined thread model, DDoS is the major attack that takes over VANETs. The DDoS attacks that are launched here are the Sybil attack and the Black hole attack.

3.2.1. Sybil Attack

Sybil attack is one among the distributed peer-to-peer networks; when it is applied to VANETs, any vehicle gets in/out with no limitations. The only requirement for the vehicles is that it has to maintain their real identities. Hence, there are no limitations; it becomes easy for the attacker to capture anyone's vehicle and gets multiplied and then broadcast false information to a neighbor vehicle. Commonly, it is difficult to identify the Sybil attack, and it will get launched in a fraction of seconds. When it occurs, the vulnerable vehicle produces numerous fake identities as Sybil vehicles which mimic the original vehicle [31]. The Sybil attack model is described in Figure 5.

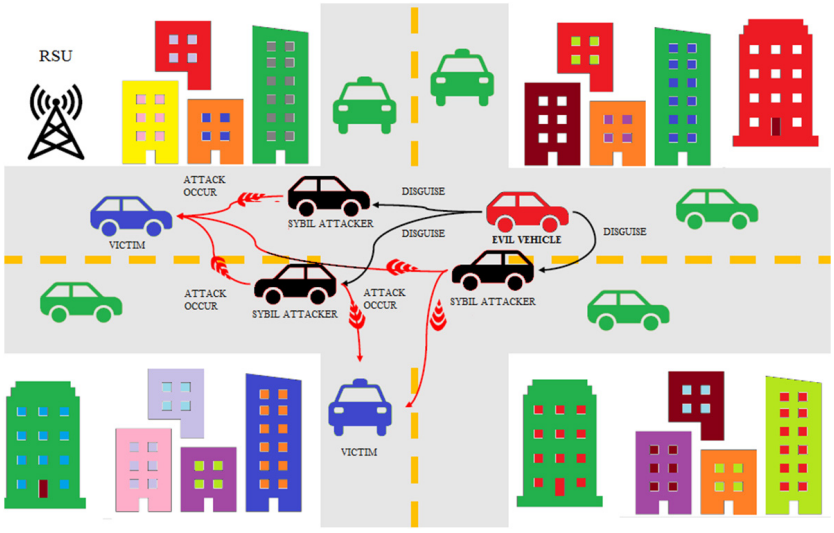

Figure 5. Sybil Attack Model [31].

3.2.2. Black Hole Attack

Black hole is one among the DDoS attacks which try to destroy the communication link between smart vehicles (SVs). The idea behind the black hole attack is that the sender initiates path searching by transferring the route request (RREQ) packets. The malicious vehicle promotes the malicious path as the best path to the sender by transferring the false Route reply (RREP) packets. When the sender starts transmitting the data through the malicious path, at that time, the malicious vehicle in the path drops all the packets [32,33]. The working of the black hole attack is described in Figure 6.

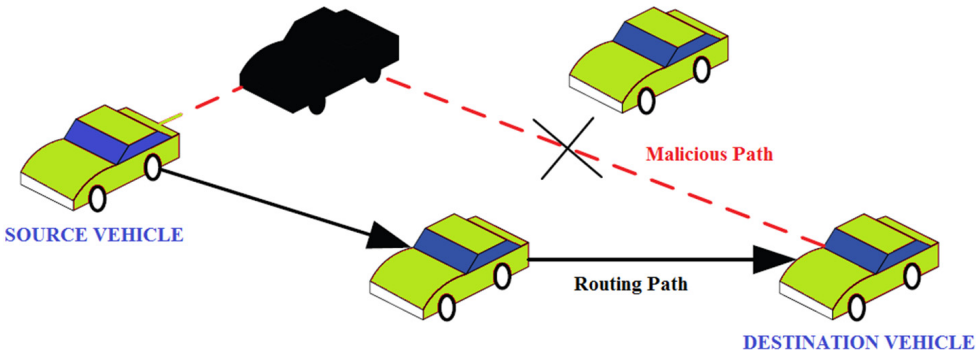

Figure 6. Working of Black hole attack [32].

The above Figure 6 shows that there are five vehicles in the network. To transfer the data from the source to the receiver, two paths are available, which consist of a smaller number of hops. If the sender selects the malicious path rather than selecting the original path, then automatically, the packets which are transmitted through the malicious path will be dropped. This attack type is classified into two they are Single and Collaborative attacks. A single attack is a normal attack, but a collaborative attack is more difficult to identify; hence, it deals with multiple vehicles, where a greater number of vehicles will conceal the routing information.

If the network is being attacked with the Sybil attack and the black hole attack, it degrades the network performance, which would lead to the reduction of efficiency and increase the overhead in the network. To overcome this problem, the attacks need to be detected, and the network has to get more secure.

3.3. Background of Elliptic Curve Cryptography (ECC) Algorithm

The idea of the Elliptic Curve Cryptography (ECC) algorithm is used in our proposed research. As so here, the basic features and characteristics of ECC are described. An asymmetric based elliptic curve is used in the key cryptosystems of ECC. The mathematical expression for the elliptic key of the generic ECC algorithm is given below [34].

$$y^2 = x^3 + ax + b \ (mod\ p) \ (\text{With } a \text{ and } b \text{ constants}) \quad (1)$$

Those integers have to satisfy the ECC properties $4a^3 + 27b^2 \neq 0$ as so to steer clear of singular points. A trapdoor function is used here; it is a one-way function it has a simple computation process in one direction. Hence, it is a one-directional process, and it becomes hard to compute in the opposite direction. In terms of key size, ECC is the most significant. Table 3 shows the key size comparison of DSA/RSA and ECC with equal security. Compared to other cryptographic key methods, it is very faster, effective as well as lightweight. It is able to provide short and fast keys during the communication process.

Table 3. Key size comparison of DSA/RSA and ECC.

Public Keys (Bits)			In Ratio	
Security (Bits)	**DSA/RSA**	**ECC**	**ECC to DSA/RSA**	**Validity**
80	1024	160–223	1:6	Up to 2010
112	2048	224–255	1:9	Up to 2030
128	3037	256–383	1:12	Beyond 2031
192	7680	384–511	1:20	Beyond 2031
256	15,360	512+	1:30	Beyond 2031

4. Proposed ECC-GA-PASR Approach

4.1. Genetic Algorithm (GA)-Based Optimized RSU Distribution

To address the multi-factor problem, the distribution of RSUs on road segments is concentrated. The parameters that are considered for this process are the distribution of SVs, mobility patterns, speed of SVs, frequency of accidents, and average distance. RSU deployment is not only based on the parameters; the selection of road segments is also an important factor. For this process, a genetic algorithm is used to find the best road segments than the insignificant or remote road segments.

4.1.1. Best Road Segment Selection

In our research, as mentioned before, the distribution of RSUs is controlled by the remote cloud (RC), where this process includes chromosome encoding and estimation, phenotype and genotype, and fundamental operations. The major criteria that are considered for the RSU placements are centralized; the majority of the area needs to get covered as well as it should not occurs any kind of RSU situation issues.

- Chromosome Encoding and Estimation: To achieve a viable stream of GA [35], a string of paired unravel chromosomes is used. During the evaluation, the fitness function is calculated then Basic Safety Message (BSM) is transmitted from SVs to RSU. The process of best road segment selection is described in Figure 7.

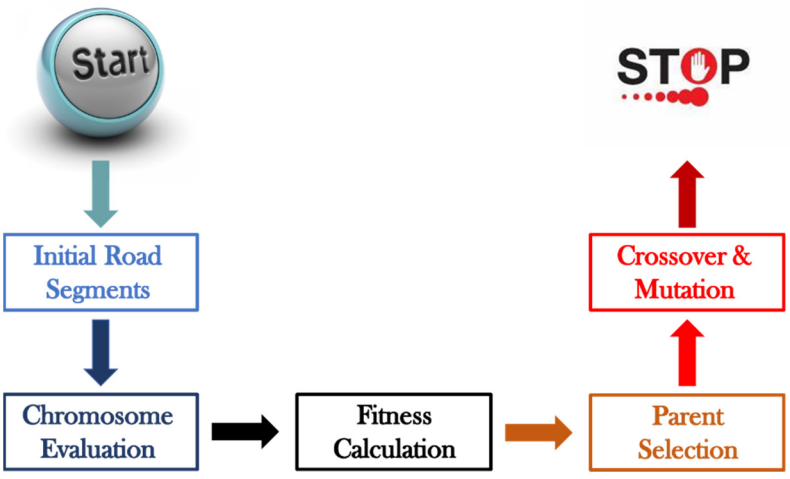

Figure 7. Best Road Segment selection.

- Phenotype and Genotype: In general, the genotype is defined as the digital data of the genetic code, and phenotype is represented as the genuine protest that acts as a visualization of the genotype.
- Fundamental Operations: After finding the initial population, the fundamental operations are taken care of, such as Selection, Crossover, and Mutation. The initial process is parent selection; here, the finest individuals from the initial population are chosen to transfer the genetic data to the subsequent generation, and then one finest

individual with the highest fitness value will turn into a talented parent. Secondly, crossover operation, in this process, any two talented parents are chosen to generate a new individual. For this process, the default recombination operator is used. Finally, Mutation operation, here probabilistic mutation is conducted, and it provides diversity to the population to avoid local minimal clarification with a constant probability. The procedure in the mutation process follows genotype so as to make one alteration in each individual on average.

4.1.2. Optimal RSU Distribution

In an emergency situation, parameter-based RSU distribution helps to distribute the information to other SVs in a safe and secure manner. The best road segments are chosen using GA, and in those individual road segment, the requirements of the number of RSUs needed to ensure the multiple requirement criteria have to be concentrated. The parameters such as Rank of Service (RoS), end-to-end distance of the road segment as well as the recorded number of accidents are considered [36]. The optimal number of RSU distribution (RSUOD) based on RoS is calculated below.

$$P_1 = RSU_{OD} = \sum_{r=1}^{n} RoS_r * \mu_r * B_r \quad (2)$$

In Equation (2), n represents the road segments, r represents the current road segment, μ_r represents the distance and accidents count in the road segment, B_r represents the binary value (0, 1) of rth road segment. Hence, there is a possibility to select or reject the road segment if $B_r = 1$, the corresponding rth road segment is taken, and if $B_r = 0$, the corresponding rth road segment is not taken.

The Rank of Service (*RoS*) is defined as the circumstance of the road segments, which includes momentum, density, traffic load, convenience, and security. According to these parameters, the *RoS* is identified. We consider four rank stages with labels A–D; here, A refers to the top-ranking operation form; likewise, D is the worst. *RoS* calculation for all the ranks is tabulated in Table 4, which is explained in terms of network traffic and momentum.

Table 4. Rank of Service calculation based on Labels.

Type	A	B	C	D
Momentum	0.0 to 0.3	0.3 to 0.6	0.06 to 0.09	0.09 to <1.0
Traffic	900	1350	2000	2300

RoS is the core parameter that is used to understand the overall circumstance of the road segment. It is primarily considered for the decision making in the process of *RSU* distribution. Based on the labels, the necessity of *RSU* is decided. Only a minimum number of *RSU* is required in free-flow traffic and momentum where the traffic increases; then, automatically, the momentum is reduced in that circumstance maximum number of *RSU* is required. The mathematical expression for the calculation of *ROS* is given below.

$$RoS = \frac{M}{1 + x(\frac{c}{p})^y} \quad (3)$$

In Equation (3), M, c, and p indicate free flow momentum, capacity, and power of the road segment, and x and y are the values of the constants here x = 0.25 and y = 5. The second parameter which is considered for RSU distribution is optimal path election, which is conducted using GA. According to the calculation of the fitness function, the optimal path is found. The mathematical expression for the calculation fitness function is given below.

$$P_2 = Fit_{Function} = XC_p + \frac{Y}{L_n} \quad (4)$$

In Equation (4), C_p indicates the present connect probability, L_n indicates the latency of the present individual, and the terms X and Y are the weighted parameters with 0 and 1 correspondingly.

The third parameter that is considered for RSU distribution is the cost of the installation, which is mainly based on the road segments. This is calculated according to the length, position, and other road activities of the road segment. According to the need, the RSU count in that particular location is decided. The mathematical expression for the calculation cost of installation is given below.

$$P_3 = I_{cost} = \sum_{r=1}^{n} N_r * I_r \tag{5}$$

In Equation (5), n represents the road segments, r represents the current road segment, N_r represents the number of RSU in the current road segment r, I_r and represents the installation cost of the current road segment r. By considering all these parameters, the final RSU distribution is conducted by calculating the minimizing function.

$$M_f = \alpha P_1 + \beta P_2 + \gamma P_3 \tag{6}$$

$$\alpha + \beta + \gamma = 1 \tag{7}$$

In Equation (6), M_f indicated the minimizing function for RSUs distribution. α, β, and γ are the weight factors used for the deployment process. P_1, P_2, and P_3 are decision-making parameters for RSU distribution. In GA, Phenotype and Genotype are used, which helps to represent the genetic code (binary in nature) congruent to the number of RSUs. This code represents the localization of RSUs in the given coverage area. The calculation of those parameters helps in finding the finest road segments and the required number of RSUs to cover the entire network. In Table 5, the genetic code illustration is shown. In the table, road division 2 and 4 need two RSUs those decisions are made by the reflection of the considered parameters according to the need of the road division.

Table 5. Genetic code illustration using GA.

Genetic Code	0	1	0	1	1	0	1	1	1
Road Division	1	2	2	3	4	4	5	. . . . .	n

This is the process behind the distribution of RSUs in the VANETs-based network. Hence in VANETs, providing security becomes essential due to the intervention of DDoS attacks. In the upcoming section, ECC-based authentication is used to protect the network from the Sybil and black hole attack.

4.2. ECC-Based Authentication for the Trusted Authority (TA)

In the research, the trusted authority (TA) is used as the main source for the authentication process, which secures the network using the public-private key pair using ECC. The work of TA is that it is accountable for SVs management through a pair of cryptographic keys as well as it controls the verification process that the SVs contain any kind of misbehavior reports that are not using the trust values of SVs. Subsequently, the TA creates a certificate that upholds key pairs for every SVs; it is called the initial registration within a network. The proper utilization of this process is verified by the RSU, which will check whether the SVs hold their valid certificates issued by the TA. RSU is highly secured to preserve the privacy of the network. In the part of ECC key generation, it is applied to the dynamic network with high speed and huge mobility because it reduces the complexity by using data with decreasing key size with high security. To provide secure vehicular communication, ECC is modified with a top-secret key which is shown in Figure 8. The generated public-private key pairs are used during the process of communication between the SVs. The messages maintain a speed of SV, location, direction, and authenticated and private key that gets broadcasted at each instance of time during transmission. The

transmitted message is encrypted with SV's private key, and then at the time of decryption, the SV's uses the public key for verification. The mathematical expression for the typical elective curve for ECC is expressed as

$$y^2 = x^3 + ax + b \ (mod \ p) \tag{8}$$

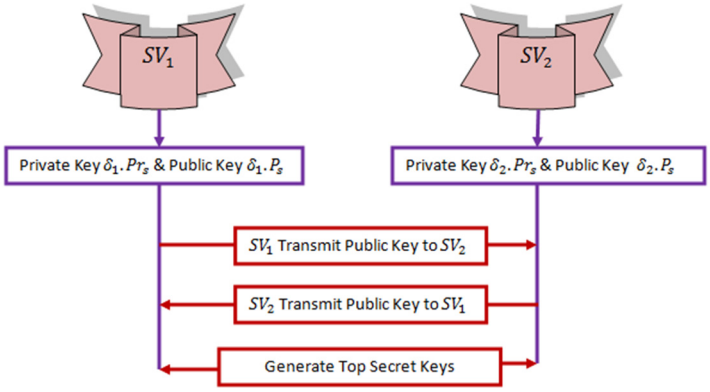

Figure 8. Vehicular Communication with ECC-based Top Secret Key.

In Equation (8), a and b represent the integer values that assure the properties of ECC $4a^3 + 27b^2 \neq 0$. The public-private key pairs for SVs and the secret shared key of any two SVs are generated using the following process. For example, if SV_1 wants to communicate with SV_2, at the initial condition, these SVs need to secure the legitimacy of the message. SV_1 choose the private key such as secret key δ_1 and private key (Pr_s). In the same way, SV_2 chooses the private key such as secret key δ_2 and private key (Pr_s). Then the private keys of the SV_1 and SV_2 are expressed below.

$$SV_1 = \delta_1.Pr_s \tag{9}$$

$$SV_2 = \delta_2.Pr_s \tag{10}$$

In Equations (9) and (10) δ_1 and δ_2 are the secret keys, and Pr_s is the private key. The vehicle which initiates malfunction that fails to identify the values of the secret keys δ_1 and δ_2. At this condition SV_1 maintain the secret key δ_1 and the top-secret key TS_1. Similarly, SV_2 maintain the secret key δ_2 and the top-secret key TS_2. The expression for the top-secret keys is given below.

$$TS_1 = t_1 \ * \ ts_1 \tag{11}$$

$$TS_2 = t_2 \ * \ ts_2 \tag{12}$$

In Equations (11) and (12) t_1 and t_2 are the random values and the ts_1 and ts_2 are top-secret keys. So, the public key of $SV_1 = \delta_1.P_s$. Similarly, for $SV_2 = \delta_2.P_s$. After that, the SV_2 transmits the public key SV_2 to SV_1. Then, SV_1 receives the message that $SV_2 = (X_{SV_2}, Y_{SV_2})$ as well as the SV_1 transmits the public key SV_1 to SV_2. Then, SV_2 receives the message that $SV_1 = (X_{SV_1}, Y_{SV_1})$. In this way, the create key is shared between two SVs. In the next stage, a two-way hash function and addition operation is performed.

$$M = P_s + HF(TS_1) + HF(TS_2) \tag{13}$$

At the final stage, the top-secret key of SV_1 and SV_2 are given below.

$$\text{Top sec ret key of } SV_1 = K_1 = \delta_1 \ * \ \delta_2 \ * \ HF(TS_1) \tag{14}$$

$$\text{Top sec ret key of } SV_2 = K_2 = \delta_2 \ * \ \delta_1 \ * \ HF(TS_2) \tag{15}$$

As a result, the intruder fails to identify the private and top-secret keys among the *SVs*.

This is the process of ECC-based Authentication that is given to the trusted authority (TA) in the network. Through this method, the vehicle identity is highly secured, and it gets free from all kinds of misbehavior activities.

Pseudo code of the proposed ECC-GA-PASR

START

Initiate Network Model Construction:

- Static and Mobile Devices
- Vehicular Network
- Roadside units
- Trusted Authority
- Remote Cloud

Initiate Thread Model Construction:

- Sybil Attack
- Blackhole Attack

Initiate Security Model:

- Elliptic Curve Cryptography (ECC)

Initiate Algorithm:

- Genetic Algorithm

Proposed ECC-GA-PASR Approach:
Genetic Algorithm (GA) based Optimized RSU Distribution:

- Best road segment selection
- Optimal RSU distribution
- $P_1 = RSU_{OD} = \sum_{r=1}^{n} RoS_r * \mu_r * B_r$
- $P_2 = Fit_{Function} = XC_p + \frac{Y}{L_n}$
- $P_3 = I_{cost} = \sum_{r=1}^{n} N_r * I_r$

$M_f = \alpha P_1 + \beta P_2 + \gamma P_3$ with $\alpha + \beta + \gamma = 1$
ECC-based Authentication for the Trusted Authority (TA):

- ECC Expression $y^2 = x^3 + ax + b\ (mod\ p)$
- Private Key Creation $SV_1 = \delta_1 . Pr_s$ and $SV_2 = \delta_2 . Pr_s$
- Secret Key Creation $TS_1 = t_1 * ts_1$ and $TS_2 = t_2 * ts_2$
- Hash Key Creation $M = P_s + HF(TS_1) + HF(TS_2)$
- Top secret key of SV_1= $K_1 = \delta_1 * \delta_2 * HF(TS_1)$
- Top secret key of SV_2= $K_2 = \delta_2 * \delta_1 * HF(TS_2)$

STOP

5. Simulation and Experimental Results

For implementing the idea of the research Ubuntu 16.04, NS-2.35 and SUMO-1.1.0 are used. To construct real-time traffic, mobility files are generated using open street mapping and SUMO. The coverage area taken for the simulation environment is 1500 × 1500 m with the varying speed from 15 to 35 (m/s). The other essential parameters that are involved in the process of simulation are given in Table 6. The analysis is conducted using three different scenarios, which are a varying number of vehicles, varying speeds, and the presence of malicious vehicles in the network. The parameters which are considered for this analysis are energy efficiency, packet delivery ratio, overhead, and packet loss. For comparison, the considered earlier research for the purpose of performance analysis is S-AODV [26], ES-AODV [32], and ECC-ACO-AODV [37]. S-AODV is a security-based routing protocol that is mainly used to detect the blackhole attack using enhanced route request and route reply transmission in the routing protocol. Additionally, security-based encryption and decryption are included with it. The major parameters which are concentrated are packet delivery ratio, delay, and throughput. The results are moderate, and it is given the analysis. ES-AODV provides enhanced security to overcome the blackhole attack, which uses a flag status-based technique that includes route discovery, route reply, detection, and prevention

process. The simulation results of this model mainly concentrate on packet delivery ratio, delay, routing overhead, and throughput. This kind of security is suitable for a network with a low density of vehicles which is less than 100, and it is not suitable for a network with huge density mobility and high density. In the ECC-ACO-AODV protocol, both the ECC algorithm and ACO algorithm are combined with the AODV protocol to achieve effective performance. The secured optimal path selection is performed using this method. The simulation results include packet delivery ratio, throughput, delay, and overhead. The results are moderate and need improvement.

Table 6. Simulation Parameters.

Parameters	Values
Simulator Version	NS-2.35
Simulation Time	200 ms
Simulation Coverage Area	1500 × 1500 m
MAC interface	MAC/802.11
No of Vehicles	500 vehicles [37]
Malicious Vehicles	50 Vehicles [37]
Network Speed	50 to 250 (KM/Hr) [37]
Channel	Channel/Wireless
Radio Propagation Model	Two-Ray Propagation Model
Connections	Multiple
Mobility Model	Random Mobility Model
Antenna Type	Omni-directional Antenna
Queue Type	DropTail
Data Packet Size	512 bytes
Traffic Agent Type	Transmission Control Protocol
Traffic Application Type	Constant Bit Rate

5.1. ECC-Based Authentication for the Trusted Authority (TA)

The parameters that are considered for this analysis concerning the number of vehicles are energy efficiency, packet delivery ratio, overhead, and packet loss. Figure 9 shows the graphical representation of the energy efficiency for the methods such as S-AODV, ES-AODV, ECC-ACO-AODV, and the proposed ECC-GA-PASR. The results stated that the proposed ECC-GA-PASR outperforms the earlier works in terms of energy efficiency, which is achieved with the concept of optimal RSU distribution. For the process of optimal RSU distribution genetic algorithm is used, which helps to reduce the energy utilization in the network, which reflects in the increase in energy efficiency.

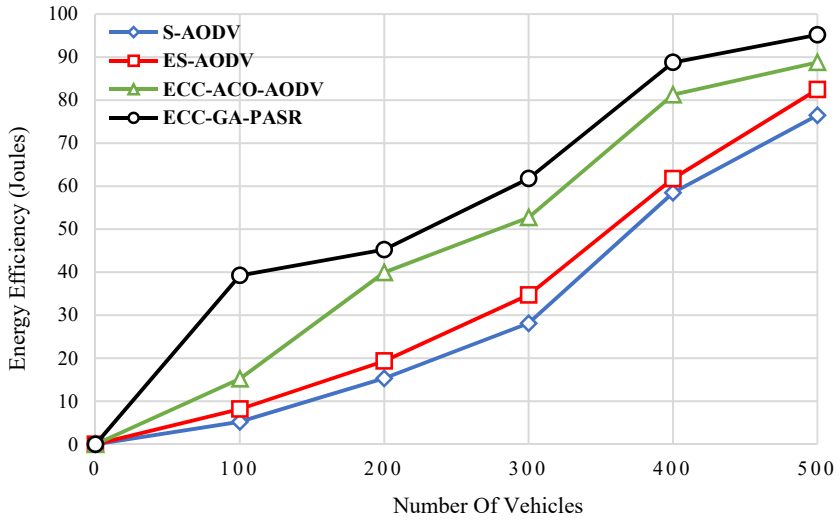

Figure 9. Efficiency Energy Calculation based on number of vehicles.

Figure 10 shows the graphical representation of the packet delivery ratio calculation. The performance achieved by the proposed ECC-GA-PASR is high when compared with the earlier works. It is attained by using private and public-based authentication processes through ECC-based authentication. It greatly prevents the network from malfunctions and improves the packet delivery ratio of the network.

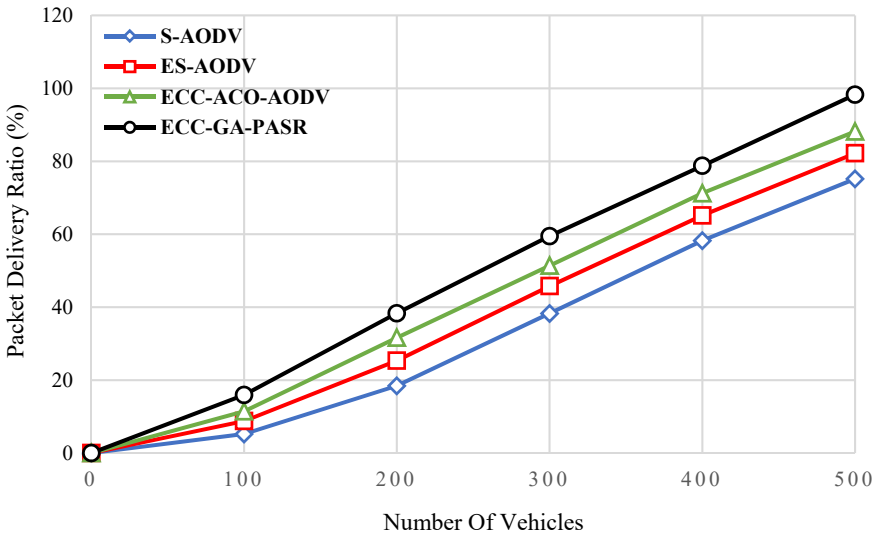

Figure 10. PDR Calculation based on number of vehicles.

Figure 11 shows the graphical representation of the overhead calculation. The results confirmed that the proposed ECC-GA-PASR produces lower overhead when compared with the earlier research. Hence, in the proposed ECC-GA-PASR, GA-based RSU distribution is conducted, and ECC-based security is provided. Through the optimal RSU distribution process, all the vehicles are able to get access to the RSU without any time delay and routing overhead, and through the ECC-based security, the packet loss in the network is greatly reduced. Both ideas are combined here; as a result, the overhead of the network is reduced.

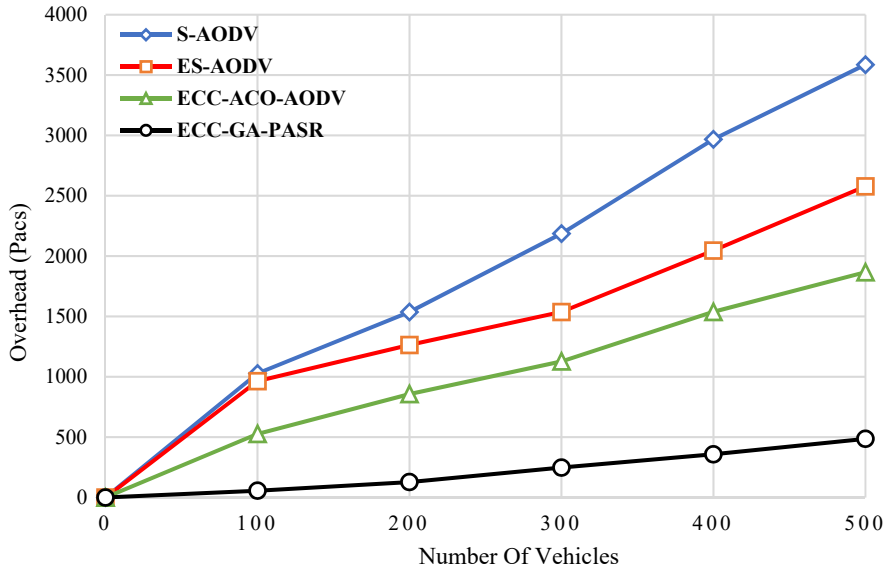

Figure 11. Overhead Calculation based on number of vehicles.

Figure 12 shows the graphical representation of the packet loss calculation. The output proves that the packet loss of the proposed ECC-GA-PASR is lower than that of the earlier works, and it is reached by the process of ECC-based key generation during the process of

data transmission between the vehicles. To a great extent, this method protects the network from malicious activities, and that reflects in the reduction of packet loss in the network.

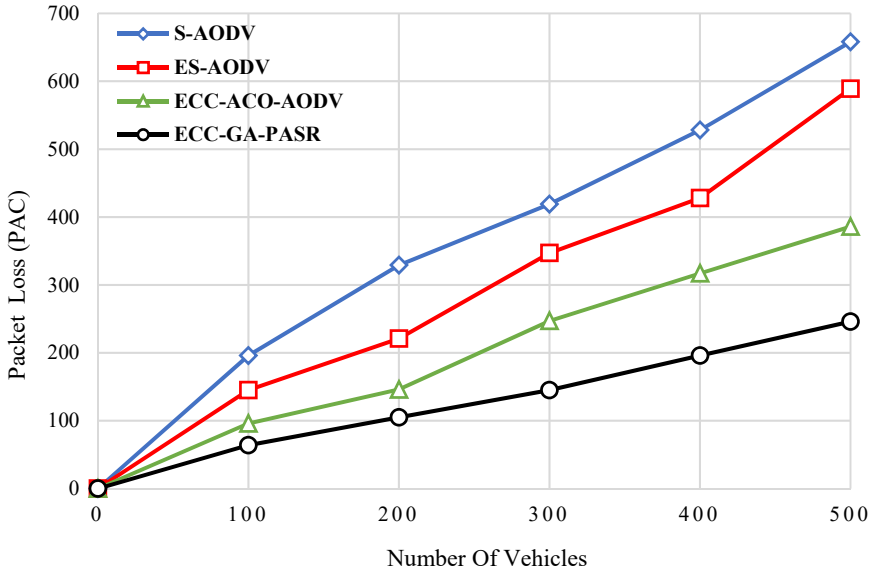

Figure 12. Packet Loss Calculation based on number of vehicles.

Result Discussion Concerning Vehicles

In this section, the results are discussed, and the performance analysis values of the calculated parameters are shown in Table 7.

Table 7. Performance Analysis of Energy Efficiency, Packet Delivery Ratio, overhead, and Packet Loss concerning number of vehicles.

Parameters	No. Vehicles	S-AODV	ES-AODV	ECC-ACO-AODV	ECC-GA-PASR	S-AODV
Energy Efficiency (%)	100	5.22	8.17	15.21	39.24	5.22
	200	15.34	19.34	39.93	45.24	15.34
	300	28.13	34.71	52.71	61.76	28.13
	400	58.47	61.74	81.25	88.76	58.47
	500	76.46	82.46	88.78	95.17	76.46
Packet Delivery Ratio (%)	100	5.24	8.76	11.44	15.93	5.24
	200	18.44	25.33	31.64	38.33	18.44
	300	38.28	45.76	51.38	59.48	38.28
	400	58.24	65.13	71.25	78.76	58.24
	500	75.18	82.19	88.17	98.28	75.18
Overhead (packets)	100	1028	964	527	56	1028
	200	1537	1264	857	128	1537
	300	2186	1537	1128	248	2186
	400	2968	2046	1538	358	2968
	500	3586	2578	1867	486	3586
Packet Loss (packets)	100	196	145	96	64	196
	200	329	221	146	105	329
	300	419	347	247	145	419
	400	528	428	317	196	528
	500	658	589	386	246	658

According to the number of vehicles, the efficiency achieved by the proposed ECC-GA-PASR is 95.17%, whereas the earlier works, such as S-AODV, ES-AODV, and ECC-ACO-AODV achieved the efficiency of 76%, 82%, and 89%, respectively. Therefore, the proposed ECC-GA-PASR achieves 10–20% better efficiency when compared with the earlier

works. The packet delivery ratio achieved by the proposed ECC-GA-PASR is 98.28%, whereas the earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV achieved the packet delivery ratio is 75%, 83%, and 89%, respectively. Therefore, the proposed ECC-GA-PASR achieves a 9–18% better packet delivery ratio when compared with the earlier works. The proposed ECC-GA-PASR achieved high efficiency and packet delivery ratio when compared with the earlier, which is attained by incorporating the network with both highly effective security and optimization methods.

The overhead produced by the proposed ECC-GA-PASR is 486 packets, whereas the earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV is 3586 packets, 2578 packets, and 1867 packets, respectively. The performance of the proposed ECC-GA-PASR achieves 3000–1500 packets lower overhead when compared with the earlier works. The packet loss proposed by the proposed ECC-GA-PASR is 246 packets, whereas the earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV are 658 packets, 589 packets, and 386 packets, respectively. The proposed ECC-GA-PASR produced around 150 packets to 400 packets, lower packet loss when compared with the earlier works. Both the overhead and packet loss produced by the proposed ECC-GA-PASR is lower than that of the earlier works, which is mainly due to the presence of the ECC security and optimization method; this combination process better result that leads to the improved overall performance of the network.

5.2. Performance Analysis Concerning Varying Speed

The parameters which are considered for this analysis concerning varying speeds are energy efficiency, packet delivery ratio, overhead, and packet loss. In Figure 13, the performance of energy efficiency is shown for the methods. From the figure, it is understood that the performance of efficiency decreases due to an increase in speed for all the methods. Compared to the other methods, the proposed ECC-GA-PASR produced better efficiency that is reached by the concept of optimal RSU distribution. RSU distribution helps to reduce and properly monitor the road segments so that network delay and congestion are reduced; likewise, energy consumption is also reduced, which reflects in the increase in energy efficiency.

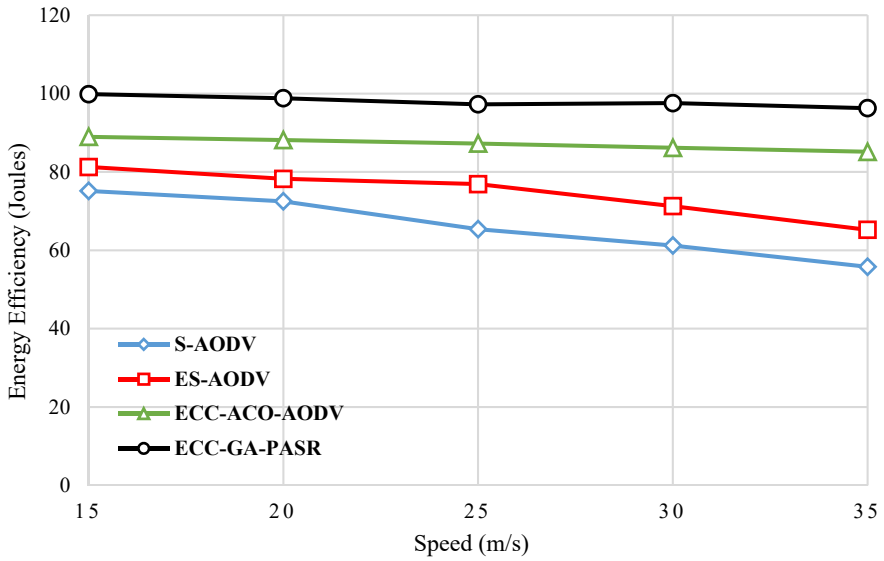

Figure 13. Efficiency Calculation based on vary speed of vehicle.

In Figure 14, the performance of the packet delivery ratio is shown for the considered methods. From the figure, it is stated that the performance of the packet delivery ratio decreases due to an increase in speed for all the methods. Compared to the other methods, the proposed ECC-GA-PASR produced a better packet delivery ratio it achieved using the concept of ECC-based authentication in the network.

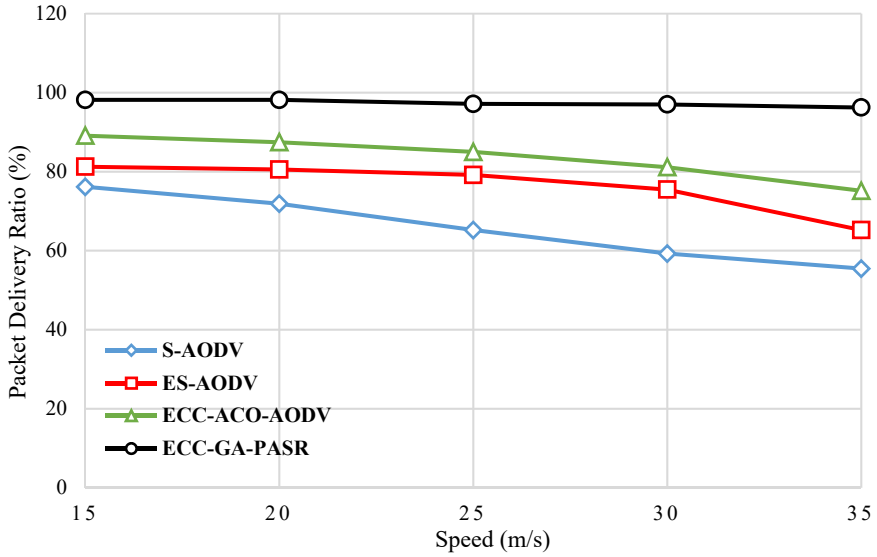

Figure 14. PDR Calculation based on vary speed of vehicle..

In Figure 15, the performance of overhead is shown for the considered methods. From the figure, it is proved that the performance of overhead increases when the speed of the network increases for all the methods compared to the other methods; the proposed ECC-GA-PASR produces low overhead. That is achieved by the process of GA-based RSU distribution process, where the reduced congestion and delay increase the rate of packets received by the destination.

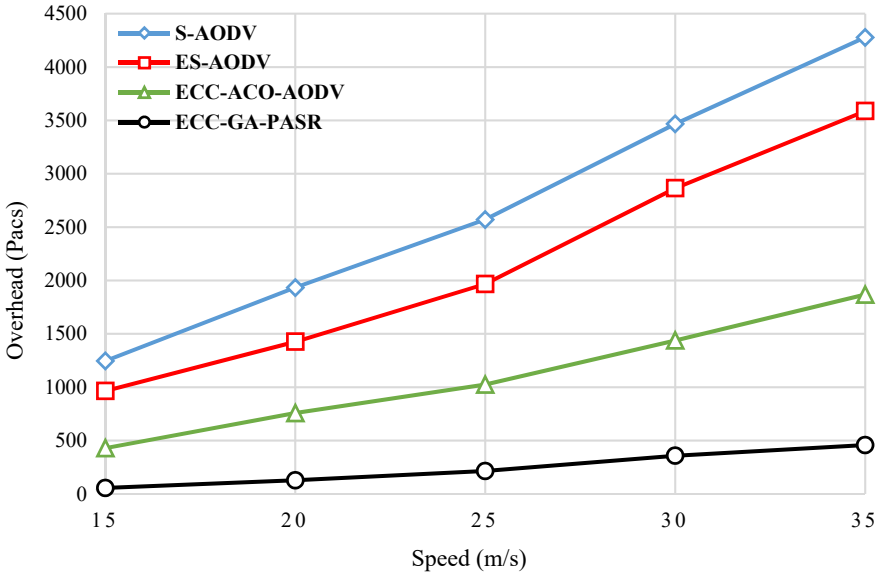

Figure 15. Overhead Calculation based on vary speed of vehicle..

In Figure 16, the performance of packet loss is shown for the considered methods. From the figure, it is shown that the performance of packet loss increases when speed increases for all the methods compared to the other methods; the proposed ECC-GA-PASR produces low packet loss. As a result of securing the network using the ECC method, the packet loss is low for the proposed ECC-GA-PASR.

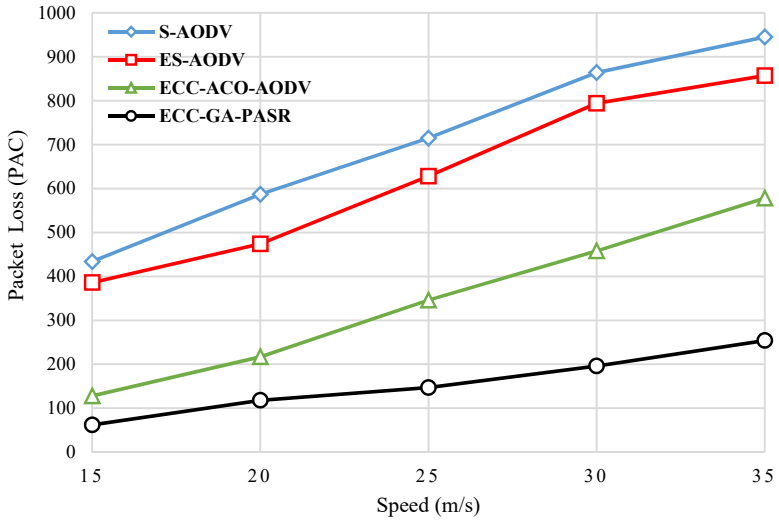

Figure 16. Packet Loss Calculation based on vary speed of vehicle.

Result Discussion Concerning Varying Speed

In this section, the results are discussed in terms of efficiency, packet delivery ratio, overhead, and packet loss for varying speeds from 15 to 35 m/s. The performance analysis values of those parameters are shown in Table 8.

Table 8. Performance Analysis of Energy Efficiency, Packet Delivery Ratio, overhead, and Packet Loss concerning varying speed.

Parameters	Speed	S-AODV	ES-AODV	ECC-ACO-AODV	ECC-GA-PASR	S-AODV
Energy Efficiency (%)	50	75.16	81.25	88.96	99.85	75.16
	100	72.49	78.23	88.15	98.81	72.49
	150	65.39	76.89	87.25	97.25	65.39
	200	61.23	71.28	6.17	97.56	61.23
	250	55.78	65.23	85.13	96.28	55.78
Packet Delivery Ratio (%)	50	76.18	81.26	89.13	98.17	76.18
	100	71.89	80.56	87.47	98.18	71.89
	150	65.24	79.17	85.01	97.16	65.24
	200	59.27	75.46	81.13	97.02	59.27
	250	55.47	65.23	75.16	96.25	55.47
Overhead (packets)	50	1246	964	429	56	1246
	100	1934	1426	758	128	1934
	150	2571	1967	1025	215	2571
	200	3467	2864	1438	358	3467
	250	4278	3587	1868	458	4278
Packet Loss (packets)	50	434	386	128	62	434
	100	587	474	217	118	587
	150	715	628	346	147	715
	200	864	794	458	196	864
	250	945	857	578	254	945

According to varying speed from 15 to 35 m/s, the energy efficiency of the proposed ECC-GA-PASR varies from 99% to 96%, whereas earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV vary from 75% to 55%, from 81% to 65%, and from 88% to 85%, respectively. As per the speed variation, the efficiency of the proposed ECC-GA-PASR lowered by around 3%, and the earlier such as S-AODV lowered by around 20%, ES-AODV lowered by around 16%, and ECC-ACO-AODV lowered by around 3%. The final results

indicate that the overall efficiency performance of the proposed ECC-ACO-AODV is higher than the others.

According to varying speed from 15 to 35 (m/s), the packet delivery ratio of the proposed ECC-GA-PASR varies from 98% to 96%, whereas earlier works such as S-AODV, ES-AODV and ECC-ACO-AODV vary from 76% to 55%, from 81% to 65%, and from 89% to 75%, respectively. As per the speed variation, the packet delivery ratio of the proposed ECC-GA-PASR lowered by around 2%, and the earlier such as S-AODV lowered by around 21%, ES-AODV lowered by around 16%, and ECC-ACO-AODV lowered around 14%. The results show that the overall packet delivery ratio performance of all the methods is reduced when increases speed, but the variation is very low in the proposed ECC-GA-PASR, which is reached by concentrating on both optimization and network security.

According to varying speed from 15 to 35 (m/s), the overhead of the proposed ECC-GA-PASR increase from 56 packets to 458 packets, whereas earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV vary from 1246 packets to 4278 packets, from 964 packets to 3587 packets, and from 429 packets to 1868 packets, respectively. As per the speed variation, the overhead of the proposed ECC-GA-PASR increased by around 400 packets, and the earlier such as S-AODV, increased by around 3000 packets, ES-AODV increased by around 2000 packets, and ECC-ACO-AODV increased by around 1500 packets. For all the methods, due to increasing the speed, the overhead is increased, but the variation which is generated by the proposed ECC-GA-PASR method is very low when compared with the others, which is achieved by focusing on data protection and optimization in the network.

According to varying speed from 15 to 35 (m/s), the packet loss of the proposed ECC-GA-PASR increased from 62 packets to 254 packets, whereas earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV varied from 434 packets to 945 packets, from 386 packets to 857 packets, and from 128 packets to 578 packets, respectively. As per the speed variation, the packet loss of the proposed ECC-GA-PASR increased by around 200 packets, and the earlier such as S-AODV, increased by around 500 packets, ES-AODV increased by around 450 packets, and ECC-ACO-AODV increased by around 400 packets. For all the methods, due to increasing the speed, the packet loss is increased, but the differences are very low for the proposed ECC-GA-PASR, which shows that the performance of the proposed method is better than the other.

5.3. Performance Analysis Concerning Malicious Activities

In Figure 17, the energy efficiency of the proposed ECC-GA-PASR is calculated, and it is compared with the earlier works. From the figure, it is understood that due to the increase in malicious activities in the network, the efficiency is reduced. Hence, the proposed work provides high security and optimal RSU distribution in the high-speed VANETs; the achieved efficiency is higher than the earlier works.

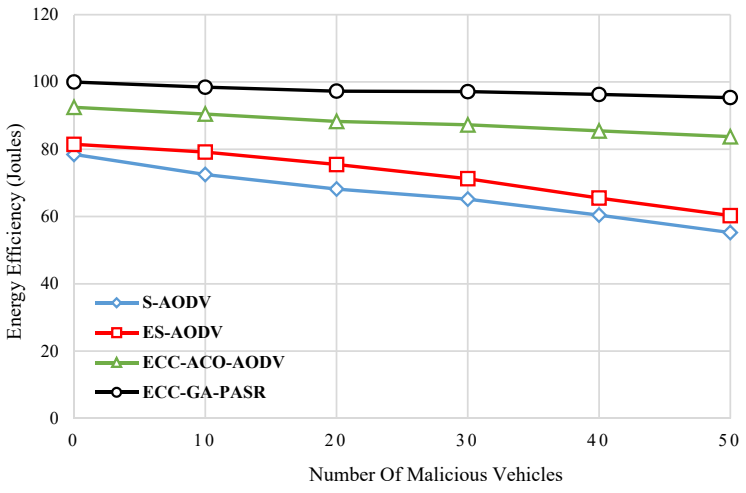

Figure 17. Energy Efficiency Calculation based on number of malicious vehicles.

In Figure 18, the packet delivery ratio of the proposed ECC-GA-PASR is calculated, and it is compared with the earlier works. An increase in malicious activities reduces the packet delivery ratio of the methods used in this research, but the proposed ECC-GA-PASR achieved a high packet delivery ratio even in this scenario when compared with the earlier works that are mainly attained using the ECC-based authentication in the network.

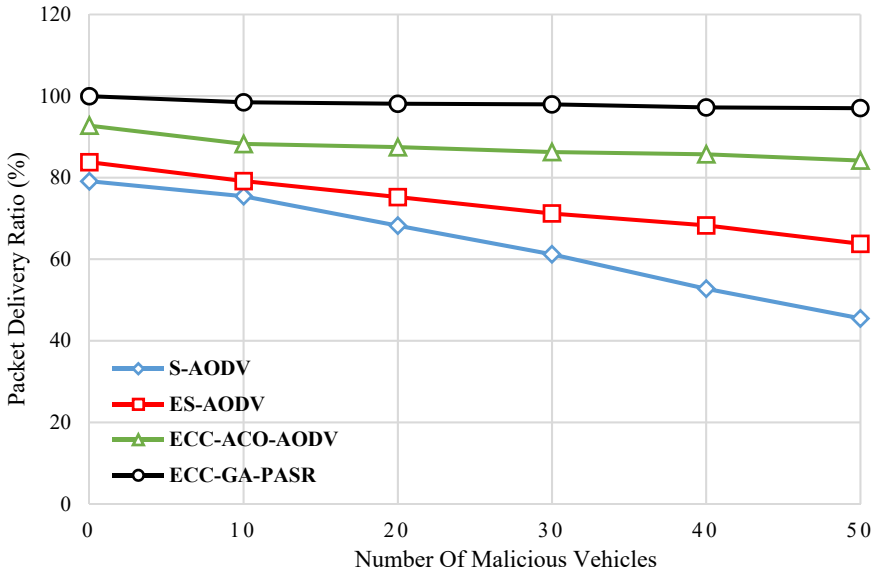

Figure 18. Packet Delivery Ratio Calculation based on number of malicious vehicles.

In Figure 19, the overhead of the proposed ECC-GA-PASR is calculated, and it is compared with the earlier works. From the figure, it is understood that due to the increase in malicious activities, the overhead of the network is increased. As a result of providing high security and optimization in the proposed ECC-GA-PASR, the production of overhead is comparatively low.

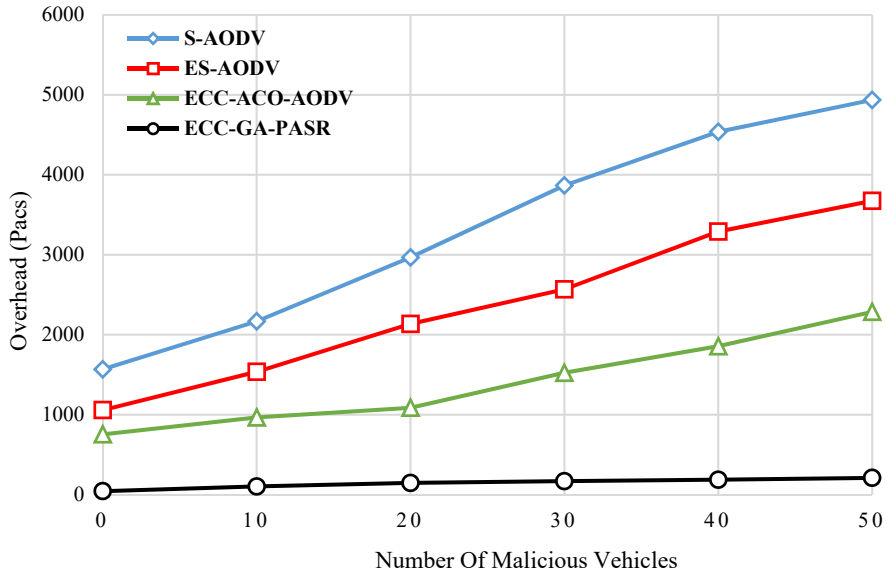

Figure 19. Overhead Calculation based on number of malicious vehicles.

In Figure 20, the packet loss of the proposed ECC-GA-PASR is calculated, and it is compared with the earlier works. The calculation of packet loss is increased due to the increase in the malicious activities in the network, but in the proposed ECC-GA-PASR, the

network is secured from the malicious activities through ECC-based authentication that greatly reduced the packet loss even with the increase in malicious activities in the network.

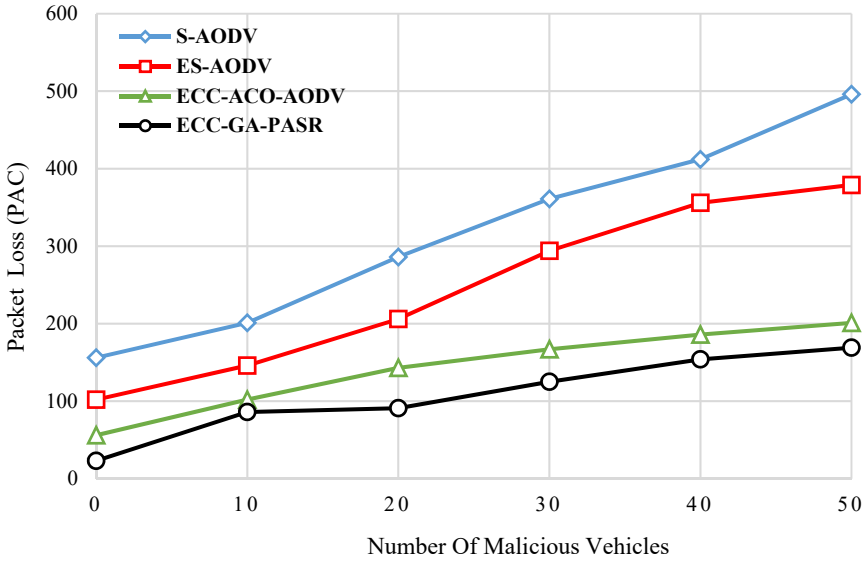

Figure 20. Packet Loss Calculation based on number of malicious vehicles.

Result Discussion Concerning Malicious Activities

In this section, the results are discussed in terms of efficiency, packet delivery ratio, overhead, and packet loss with the increase in malicious vehicles. The performance analysis values of those parameters are shown in Table 9.

Table 9. Performance Analysis of Energy Efficiency, Packet Delivery Ratio, overhead, and Packet Loss concerning increase in malicious vehicles.

Parameters	Malicious Vehicle	S-AODV	ES-AODV	ECC-ACO-AODV	ECC-GA-PASR	S-AODV
Energy Efficiency (%)	0	78.46	81.46	92.47	99.99	78.46
	10	72.48	79.17	90.47	98.45	72.48
	20	68.17	75.47	88.27	97.26	68.17
	30	65.17	71.25	87.26	97.13	65.17
	40	60.41	65.49	85.46	96.28	60.41
	50	55.23	60.28	83.74	95.34	55.23
Packet Delivery Ratio (%)	0	79.13	83.79	92.76	99.95	79.13
	10	75.46	79.17	88.26	98.46	75.46
	20	68.24	75.23	87.49	98.12	68.24
	30	61.21	71.22	86.28	97.96	61.21
	40	52.76	68.29	85.74	97.21	52.76
	50	45.49	63.77	84.21	97.03	45.49
Overhead(packets)	0	1567	1056	754	43	1567
	10	2167	1536	965	102	2167
	20	2967	2134	1086	146	2967
	30	3867	2567	1524	168	3867
	40	4538	3289	1856	186	4538
	50	4937	3674	2286	209	4937
Packet Loss(packets)	0	156	102	56	23	156
	10	201	146	102	86	201
	20	286	206	143	91	286
	30	361	294	167	125	361
	40	412	356	186	154	412
	50	496	379	201	169	496

According to the increase in malicious activities from 0 to 50 vehicles, the energy efficiency of the proposed ECC-GA-PASR varies from 99% to 95%, whereas earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV vary from 78% to 55%, from 81% to 60%, and from 92% to 83%, respectively. An increase in malicious vehicles affects the

performance so that the efficiency of the proposed ECC-GA-PASR is lowered by around 4%, and the earlier works such as S-AODV lowered by around 23%, ES-AODV lowered by around 21% and ECC-ACO-AODV lowered around 9%. In the earlier works, the performance is reduced from 9% to 23%, but in the proposed ECC-GA-PASR, it is only 3%. This proves that the efficiency of the proposed ECC-GA-PASR is higher than the earlier works.

According to the increase in malicious activities from 0 to 50 vehicles, the packet delivery ratio of the proposed ECC-GA-PASR varies from 99% to 97%, whereas earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV vary from 74% to 55%, from 83% to 63%, and from 92% to 84%, respectively. An increase in malicious vehicles affects the performance so that the packet delivery ratio of the proposed ECC-GA-PASR is lowered by around 3%, and the earlier works such as S-AODV lowered by around 19%, ES-AODV lowered by around 20%, and ECC-ACO-AODV lowered around 9%. The packet delivery ratios of the earlier works are affected by the malicious activities, and it gets lowered by around 9–20%, but for the proposed work, it is only 2%. This proves that the proposed work performed better when compared with the others.

According to the increase in malicious activities from 0 to 50 vehicles, the overhead of the proposed ECC-GA-PASR increased from 43 packets to 209 packets, whereas earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV varied from 1567 packets to 4937 packets, from 1056 packets to 3674 packets, and from 754 packets to 2286 packets), respectively. Due to the increase in malicious vehicles, the network overhead is increased from around 1500 packets to 2500 packets for the earlier works. In the case of the proposed ECC-GA-PASR, it is only 150 packets. This proves that the performance of the proposed ECC-GA-PASR is better than others.

According to the increase in the malicious activities from 0 to 50 vehicles, the packet loss of the proposed ECC-GA-PASR increased from 45 packets to 169 packets, whereas earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV varied from 156 packets to 496 packets, from 102 packets to 379 packets, and from 56 packets to 201 packets, respectively. Due to the increase in malicious vehicles, packet loss is increased. In the earlier works, the packet loss is increased from 150 packets to 300 packets, but for the proposed ECC-GA-PASR, 120 packets. Comparatively, it is better than the earlier methods.

6. Conclusions

The major drawbacks of high-speed VANETs such as security and communication overhead are taken into consideration. To overcome these drawbacks, privacy-aware secure routing is introduced with the combination of Genetic algorithm (GA)-based optimal RSU distribution and ECC-based Authentication. Optimal RSU distribution is mainly employed to control the communication overhead, and ECC is used to improve the security of the VANETs. The simulation is performed using NS2, and three types of analysis are conducted for performance evaluation that are in terms of number of vehicles, varying speed, and increase in malicious vehicles. The performance of the proposed ECC-GA-PASR is calculated and then compared with the earlier works, such as S-AODV, ES-AODV, and ECC-ACO-AODV. According to number of vehicles, the efficiency of the proposed method reaches up to 95%, which is around 15% higher than the earlier works. The Overhead of the proposed ECC-GA-PASR is very low in terms of vehicles. According to varying speeds, the efficiency is reduced for all the methods but is only 3% for ECC-GA-PASR, which is 10% better than others. The Overhead of the proposed ECC-GA-PASR is very low in terms of increase in speed. According to the increase in the malicious vehicles, the efficiency of the proposed ECC-GA-PASR is reduced by around 3%, which is significant when compared with the earlier works such as S-AODV, ES-AODV, and ECC-ACO-AODV. In the future, the research will be continued by providing hybrid security so that an increase in speed should not affect the performance of the network.

Author Contributions: Conceptualization, Funding acquisition, Resources, Investigation, Writing—original draft, G.G.S.; Data curation, Funding acquisition, D.A.M.; Investigation, Funding acquisition, Funding acquisition, Methodology, Validation, Writing—review and editing, Visualization, Supervision, A.H.A.; Investigation, Funding acquisition, N.F.A.; All authors have read and agreed to the published version of the manuscript.

Funding: Partial support by Imam Ja'afar Al-Sadiq University.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alshudukhi, J.S.; Mohammed, B.A.; Al-Mekhlafi, Z.G. Conditional Privacy-Preserving Authentication Scheme without Using Point Multiplication Operations Based on Elliptic Curve Cryptography (ECC). *IEEE Access* **2020**, *8*, 222032–222040. [CrossRef]
2. Li, X.; Liu, T.; Obaidat, M.S.; Wu, F.; Vijayakumar, P.; Kumar, N. A Lightweight Privacy-Preserving Authentication Protocol for VANETs. *IEEE Syst. J.* **2020**, *14*, 3547–3557. [CrossRef]
3. Al-Heety, O.S.; Zakaria, Z.; Ismail, M.; Shakir, M.M.; Alani, S.; Alsariera, H. A comprehensive survey: Benefits, Services, Recent works, Challenges, Security and Use cases for SDN-VANET. *IEEE Access* **2020**, *8*, 91028–91047. [CrossRef]
4. Waqas, M.; Niu, Y.; Li, Y.; Ahmed, M.; Jin, D.; Chen, S.; Han, Z. Mobility-Aware Device-to-Device Communication: Principles, Practice and Challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1863–1886. [CrossRef]
5. Habelalmateen, M.I.; Ahmed, A.J.; Abbas, A.H.; Rashid, S.A. TACRP: Traffic-Aware Clustering-Based Routing Protocol for Vehicular Ad-Hoc Networks. *Designs* **2022**, *6*, 89. [CrossRef]
6. Abbas, A.H.; Mansour, H.S.; Al-Fatlawi, A.H. Self-Adaptive Efficient Dynamic Multi-Hop Clustering (SA-EDMC) Approach for Improving VANET's Performance. *Int. J. Interact. Mob. Technol.* **2022**, *17*, 136–151. [CrossRef]
7. Abbas, A.H.; Ahmed, A.J.; Rashid, S.A. A Cross-Layer Approach MAC/NET with Updated-GA (MNUG-CLA)-Based Routing Protocol for VANET Network. *World Electr. Veh. J.* **2022**, *13*, 87. [CrossRef]
8. Wang, P.; Liu, Y. SEMA: Secure and Efficient Message Authentication Protocol for VANETs. *IEEE Syst. J.* **2021**, *15*, 846–855. [CrossRef]
9. Li, B.; Liang, R.; Zhu, D.; Chen, W.; Lin, Q. Blockchain-Based Trust Management Model for Location Privacy Preserving in VANET. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3765–3775. [CrossRef]
10. Lo, N.W.; Tsai, J.L. CPPA-D: Efficient Conditional Privacy-Preserving Authentication Scheme with Double-Insurance in VANETs. *IEEE Trans. Veh. Technol.* **2021**, *70*, 3456–3468.
11. Jan, S.A.; Amin, N.U.; Othman, M.; Ali, M.; Umar, A.I.; Basir, A. A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues. *IEEE Access* **2021**, *9*, 153701–153726. [CrossRef]
12. Nazib, R.A.; Moh, S. Reinforcement Learning-Based Routing Protocols for Vehicular Ad Hoc Networks: A Comparative Survey. *IEEE Access* **2021**, *9*, 27552–27587. [CrossRef]
13. Sindhwani, M.; Singh, R.; Sachdeva, A.; Singh, C. Imprvisation of optimization technique and AODV routing protocol in VANET. *Mater. Today Proc.* **2022**, *49*, 3457–3461. [CrossRef]
14. Rashid, S.A.; Alhartomi, M.; Audah, L.; Hamdi, M.M. Reliability-Aware Multi-Objective Optimization-Based Routing Protocol for VANETs Using Enhanced Gaussian Mutation Harmony Searching. *IEEE Access* **2022**, *10*, 26613–26627. [CrossRef]
15. Gao, Z.; Wu, H.-C.; Cai, S.; Tan, G. Tight Approximation Ratios of Two Greedy Algorithms for Optimal RSU Deployment in One-Dimensional VANETs. *IEEE Trans. Veh. Technol.* **2021**, *70*, 3–17. [CrossRef]
16. Jiang, B.; Givigi, S.N.; Delamer, J.-A. A MARL Approach for Optimizing Positions of VANET Aerial Base-Stations on a Sparse Highway. *IEEE Access* **2021**, *9*, 133989–134004. [CrossRef]
17. Bello-Salau, H.; Onumanyi, A.J.; Abu-Mahfouz, A.M.; Adejo, A.O.; Mu'Azu, M.B. New Discrete Cuckoo Search Optimization Algorithms for Effective Route Discovery in IoT-Based Vehicular Ad-Hoc Networks. *IEEE Access* **2020**, *8*, 145469–145488. [CrossRef]
18. Singh, G.D.; Prateek, M.; Kumar, S.; Verma, M.; Singh, D.; Lee, H.N. Hybrid Genetic Firefly Algorithm-Based Routing Protocol for VANETs. *IEEE Access* **2022**, *10*, 9142–9151. [CrossRef]
19. Hossain, M.A.; Noor, R.M.; Yau, K.-L.A.; Azzuhri, S.R.; Z'Abar, M.R.; Ahmedy, I.; Jabbarpour, M.R. Multi-Objective Harris Hawks Optimization Algorithm Based 2-Hop Routing Algorithm for CR-VANET. *IEEE Access* **2021**, *9*, 58230–58242. [CrossRef]
20. Khan, A.A.; Abolhasan, M.; Ni, W.; Lipman, J.; Jamalipour, A. A Hybrid-Fuzzy Logic Guided Genetic Algorithm (H-FLGA) Approach for Resource Optimization in 5G VANETs. *IEEE Trans. Veh. Technol.* **2019**, *68*, 6964–6974. [CrossRef]
21. Bagga, P.; Das, A.K.; Wazid, M.; Rodrigues, J.J.; Choo KK, R.; Park, Y. On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1736–1751. [CrossRef]
22. Aman, M.N.; Javaid, U.; Sikdar, B. A Privacy-Preserving and Scalable Authentication Protocol for the Internet of Vehicles. *IEEE Internet Things J.* **2020**, *8*, 1123–1139. [CrossRef]

23. Yang, L.; Moubayed, A.; Shami, A. MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles. *IEEE Internet Things J.* **2021**, *9*, 616–632. [CrossRef]
24. Zhang, J.; Yang, F.; Ma, Z.; Wang, Z.; Liu, X.; Ma, J. A Decentralized Location Privacy-Preserving Spatial Crowdsourcing for Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 2299–2313. [CrossRef]
25. Vangala, A.; Bera, B.; Saha, S.; Das, A.K.; Kumar, N.; Park, Y.H. Blockchain-Enabled Certificate-Based Authentication for Vehicle Accident Detection and Notification in Intelligent Transportation Systems. *IEEE Sens. J.* **2020**, *21*, 15824–15838. [CrossRef]
26. Kumar, A.; Varadarajan, V.; Kumar, A.; Dadheech, P.; Choudhary, S.S.; Kumar, V.A.; Panigrahi, B.; Veluvolu, K.C. Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocess. Microsyst.* **2021**, *80*, 103352. [CrossRef]
27. Kudva, S.; Badsha, S.; Sengupta, S.; La, H.; Khalil, I.; Atiquzzaman, M. A scalable blockchain based trust management in VANET routing protocol. *J. Parallel. Distrib. Comput.* **2021**, *152*, 144–156. [CrossRef]
28. Vasudev, H.; Deshpande, V.; Das, D.; Das, S.K. A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6709–6717. [CrossRef]
29. Lin, X.; Wu, J.; Mumtaz, S.; Garg, S.; Li, J.; Guizani, M. Blockchain-Based On-Demand Computing Resource Trading in IoV Assisted Smart City. *IEEE Trans. Emerg. Top. Comput.* **2020**, *9*, 1373–1385. [CrossRef]
30. Limbasiya, T.; Das, D.; Das, S.K. MComIoV: Secure and Energy-Efficient Message Communication Protocols for Internet of Vehicles. *IEEE/ACM Trans. Netw.* **2021**, *29*, 1349–1361. [CrossRef]
31. Li, J.; Xue, Z.; Li, C.; Liu, M. RTED-SD: A Real-Time Edge Detection Scheme for Sybil DDoS in the Internet of Vehicles. *IEEE Access* **2021**, *9*, 11296–11305. [CrossRef]
32. Oberoi, V. Enhancement of QoS in Security Algorithm for Blackhole Attack in VANET. In Proceedings of the 2020 IEEE Pune Section International Conference (PuneCon), Pune, India, 16–18 December 2020; pp. 33–37.
33. Lyu, J.; Chen, C.; Tian, H. Secure Routing Based on Geographic Location for Resisting Blackhole Attack in Three-dimensional VANETs. In Proceedings of the 2020 IEEE/CIC International Conference on Communications in China (ICCC), Chongqing, China, 9–11 August 2020; pp. 1168–1173.
34. Sharma, S.; Kaushik, B.; Rahmani, M.K.I.; Ahmed, E. Cryptographic Solution-Based Secure Elliptic Curve Cryptography Enabled Radio Frequency Identification Mutual Authentication Protocol for Internet of Vehicles. *IEEE Access* **2021**, *9*, 147114–147128. [CrossRef]
35. Zhang, G.; Wu, M.; Duan, W.; Huang, X. Genetic Algorithm Based QoS Perception Routing Protocol for VANETs. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 3897857. [CrossRef]
36. Sankaranarayanan, M.; Mala, C.; Mathew, S. Genetic Algorithm Based Efficient RSU Distribution to Estimate Travel Time for Vehicular Users. In Proceedings of the Second International Conference on Soft Computing and Machine Intelligence, Hong Kong, 23–24 November 2015.
37. Safavat, S.; Rawat, D.B. On the Elliptic Curve Cryptography for Privacy-Aware Secure ACO-AODV Routing in Intent-Based Internet of Vehicles for Smart Cities. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 5050–5059. [CrossRef]