

MAR SECURITY: IMPROVED SECURITY MECHANISM FOR EMERGENCY MESSAGES OF VANET USING GROUP KEY MANAGEMENT & CRYPTOGRAPHY SCHEMES (GKMC)

Mahabaleshwar Kabbur, Anand R and Arul Kumar V

School of Computer Science & Applications,
REVA University, Bengaluru-64, Karnataka, India

ABSTRACT

Vehicular Ad-hoc network (VANET) is one of the emerging technologies for research community to get various research challenges to construct secured framework for autonomous vehicular communication. The prime concern of this technology is to provide efficient data communication among registered vehicle nodes. The several research ideas are implemented practically to improve overall communication in VANETs by considering security and privacy as major aspects of VANETs. Several mechanisms have been implemented using cryptography algorithms and methodologies. However, these mechanisms provide a solution only for some restricted environments and to limited security threats. Hence, the proposed novel mechanism has been introduced, implemented and tested using key management technique. It provides secured network environment for VANET and its components. Later, this mechanism provides security for data packets of emergency messages using cryptography mechanism. Hence, the proposed novel mechanism is named Group Key Management & Cryptography Schemes (GKMC). The experimental analysis shows significant improvements in the network performance to provide security and privacy for emergency messages. This GKMC mechanism will help the VANET user's to perform secured emergency message communication in network environment.

KEYWORDS

Network Protocols, Wireless Network, Mobile Network, Virus, Worms & Trojan.

1. INTRODUCTION

The transportation system plays an important role in the development of any country's economic growth. Thus, the demand for vehicles increases. This increased utilization of vehicles has several advantages such as better and efficient transportation, and also it has several disadvantages related to road safety and other issues such as accidents. A recent study revealed that, a total of 232 billion accidents are reported in the United States and 100 thousand deaths are reported every year in China, and it is still increasing [1]. In these accidents, more than 57% of accidents are caused due to human error such as lack of attention, poor cooperation among vehicle drivers and poor decisions. The frequent exchange of accident alarm between vehicles can help to avoid these incidents. This communication between vehicles can be performed using wireless communication. Recently, increased growth of wireless communication has gained huge attraction in various real-time applications such as mobile communication, wireless sensor networks and satellite communications, etc.

The technological growth in networking, embedded technology has enabled various development opportunities for the automobile industry due to that vehicles are equipped with various types of smart devices such as Wi-Fi, GPS and other smart devices. Due to these smart devices, vehicles can communicate each other through wireless network and facilitates the formation of Vehicular Ad Hoc Network (VANET) where vehicles can communicate to avoid congestion and accidents.

Recently, numerous researches are conducted to the establishment of reliable Intelligent Transport System (ITS) which has several facilities such as traffic monitoring, collision control, traffic flow control, nearby location information services, and internet availability in vehicles. Generally, VANETs are characterized by the following factors such as dynamic network topology, on-board sensors, unlimited power, and storage, etc. Similarly, the VANET communication systems can be classified based on the communication types which are: Intra-Vehicular communication inside the vehicle, vehicle to vehicle communication (V2V), vehicle to infrastructure (V2I) and hybrid communication (V2X) where a vehicle can communicate to the vehicle and road-side units (RSU) [2].

During the last decade, the development of ITS and VANET have gained attention by research, industrial and academic field due to its promising nature of reliable transportation system. Several types of research have focused on this field and developed various approaches to improve the performance of VANETs. However, this communication is performed using wireless communication architecture where routing is considered a challenging task. VANETs have several applications which are mainly categorized into two categories like, safety and non-safety applications. The safety applications perform transmitting safety messages and warning messages for assisting the road to prevent accidents. These messages can include various types of information such as road accidents, traffic jams, emergency vehicles, and road construction, etc. Figure 1 shows actual research scenario of VANET and how emergency messages are unsafe in data transmission process.

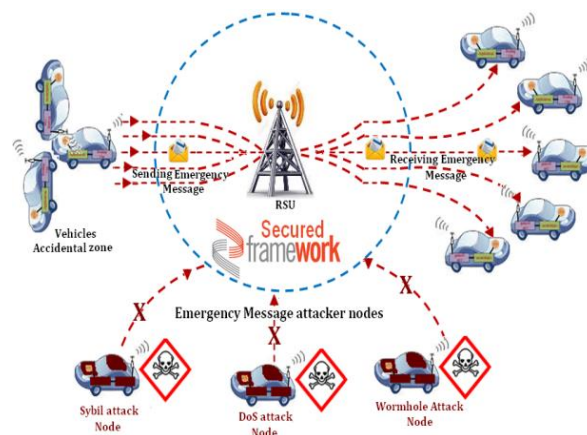


Fig. 1. Research scenario of VANET

These safety messages urges for high security and low latency. On the other hand, non-safety applications include traffic management tasks and infotainment. However, infotainment applications do not require higher security. The safety messages need to be transmitted quickly and reliably. The dynamic network topology becomes a tedious task in VANET to deliver the safety message.

Despite several advantages of VANET in safety and information application, these networks require high security which is considered a challenging task.

- Vehicles exchange secret information which can attract attackers to steal and misuse the information hence, a reliable security model is required.
- Due to high dynamic network topology, no authentication is performed due to this, the illegitimate nodes participate in the Security is a prime concern due to following reasons: communication to harm the VANET communication.
- The VANET architecture is infrastructure-less which is easy to attack by outsider attackers hence providing security is important to the users.
- Privacy preservation is an important factor of VANET.
- Transmitting and receiving accurate information without any tampering or spoofing for secure communication.
- Data reliability, confidentiality and user anonymity provides enhanced security to the network.

Due to the aforementioned reasons, VANET security is widely studied. These attacks include availability attacks such as denial of service (DoS) and black hole attack, authenticity attacks such as Sybil attack and GPS attack, data confidentiality such as eavesdropping and data trust, non-repudiation such as loss of event traceability. Figure 2 shows a classification of various attacks on VANET.

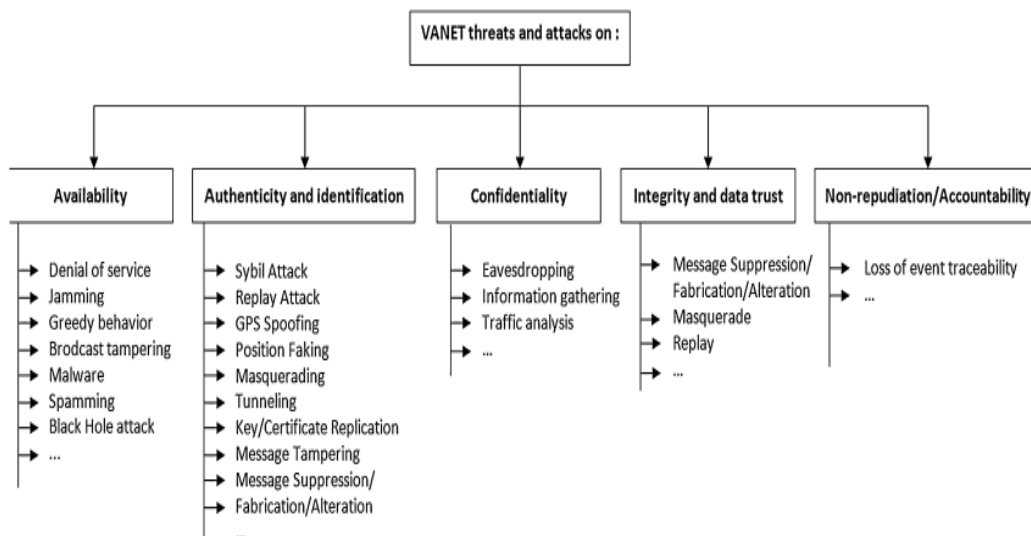


Fig 2. Examples of VANET threats and attacks

These attacks can lead the development of a poor ITS. Hence, security becomes the prime concern for these applications. Several routing approaches have been introduced which include AODV [3], DSDV [4], DSR [5] and OLSR [6] for efficient data delivery and communication. Moreover, heuristic optimization algorithms are also introduced such as Heuristic algorithm using Ant Colony Optimization [7], Meta-heuristic [8], CACONET [9], and improved hybrid ant particle optimization (IHAPO) [10], etc. Similarly, artificial intelligence schemes are also introduced such as Fuzzy Logic based routing [11], and neural networks [12]. Several techniques are introduced to overcome the security related issues in VANET. Recently, CARAVAN [13], AMOEBA [14], REP [15], VSPN [16] and many more approaches have been developed to facilitate location privacy. Similarly, cryptography based schemes are also introduced to secure the message. [17] Introduced cryptography approach to deal with the Sybil attacks. Some of the security schemes are introduced based on the key-management protocol such as [18] presented Diffie-Hellman key generation scheme. Key management and key generation are the crucial stages of authentication. [19] Presented ID-based authentication protocol. Furthermore, the

cryptographic schemes are expanded based on the symmetric and asymmetric cryptography schemes [7]. However, achieving security in these types of dynamic networks is always considered a challenging task and various researches are still in progress to provide more security in VANETs. This work focuses on security requirements of VANET and introduces a novel approach for secure communication in VANETs.

The main contributions of the work are as follows:

- Development of a novel approach for group key distribution which includes authentication process to improve the network security.
- Incorporating novel data encryption and decryption process based on the Elliptic Curve Cryptography (ECC) scheme.

The rest of the manuscript is organized as literature review study, which is presented in section 2. The proposed solution for the security and QoS enhancement in the VANET is presented in section 3 and section 4 presents the experimental study. The comparative analysis shows robust performance of the proposed model. Finally, section 5 presents concluding remarks.

2. LITERATURE SURVEY

✚ This section represents brief discussion about recent techniques of secure communication in VANETs. This section includes various schemes such as authentication, key generation, key exchange, hash function and cryptography schemes. Ref. by [20] presented a robust approach for secure and QoS aware routing approach for VANET. According to this approach, Ant colony optimization scheme is used to find the optimal route based on the data traffic type. The ACO scheme helps to achieve the best fit solution for the given problem. Later, VANET-oriented Evolving Graph (VoEG) model is developed to measure the likelihood among vehicles. Ref. by [21] introduced 2FLIP approach to maintain the location privacy. This process uses message authentication code (MAC) and hash operations to induce two factor authentications. This approach uses biometric system for each driver to collect the traces of each driver where this biometric is verified using the tamper-proof device (TPD) is embedded in onboard unit (OBU). The one-way hash function is generating to secure the V2V and V2R communication. This mechanism secures the message using MAC generation and a hash function is re-generated for verification. Ref. by [22] introduced an authentication model for anonymous users based on the signature and message recovery. This approach uses batch operations to authenticate the multiple signatures, which help to reduce the authentication time. The main contributions of this approach are as follows: The ID based anonymous signature scheme is developed for authentication where, length of the packet will be shorter, resulting in reduced communication overhead. In the next stage, the message is recovered using signature which reduces the computation overhead by neglecting invalid signature messages. Finally, batch authentication is used where all the messages can be authentication at the same time. Bad mouthing and providing false information are serious issues in VANETs. Generally, reputation management schemes are used for this purpose but, they cannot handle the self-promoting attack and it may violate location privacy. To deal with these issues, Ref. by [23] presented privacy preserving and reputation management model to mitigate bad mouthing attacks. This work presents a service reputation to compute QoS of the user, if any user provides low QoS then it is identified as malicious node. Furthermore, this work focuses on location privacy by presenting the hidden-zone and k-anonymity scheme. Ref. by [24] discussed that the current routing scheme will not ensure the on-time packet delivery due to, high dynamic nature of VANETs which affects the process of safety alert message. These safety messages require security to maintain the hassle free traffic

hence in this work a secure routing scheme VANSecis presented to avoid threats to the network. This approach is based on trust management which identifies the false and malicious nodes. Ref. by [25] presented Ad hoc On-demand Multipath Distance Vector (AOMDV) routing algorithm. This algorithm provides minimum of three paths to route the packets. However, AOMDV suffers from the lack of security schemes, cryptography and intrusion detection schemes because of these issues this protocol is vulnerable to various threats such as black holes and man-in-the-middle attack. Hence, this scheme introduces secure and efficient AOMDV protocol for VANETs. The security is enabled by detecting the malicious vehicles which are not authenticated and pose malicious behaviour. Furthermore, best path is obtained using Route Reply (RREP) packet. Ref. by [26] focused on the data security in VANETs and suggested that the secured data can be delivered using LEACH protocol. Hence, in this work, authors considered the combination of LEACH protocol and lightweight cryptographic model. For increasing security, the Random Firefly is used for identifying the trustworthy vehicles in the considered network topology. After identifying the reliable vehicles, the lightweight security and Hash function methods are used for securing the information for transmission. Ref. by [27] presented Security Aware Fuzzy Enhanced Reliable Ant Colony Optimization (SAFERACO) routing protocol to distinguish the malicious and trustworthy nodes during communication. The misbehaving nodes are discarded from the routing process. The user authentication plays an important role to improve the security of VANETs. Several approaches are developed based on authentication. Tan et al. [28] authentication based approach for increasing the security in VANETs. In this work, authors introduced elliptic curve cryptography which is further improved by using bilinear pairing. The vehicles which are in the defined range are selected and assigned a group key for authentication. Later, the encrypted message is delivered to the corresponding RSU which provides the vehicle priority and assessment information which helps to arrange the route for the vehicles to deliver the message in the optimal period of time. Lu et al. [30] introduced a trust and privacy model for improving the security in VANETs. This work presents block chain based anonymous reputation system (BARS) for trust management. In this work, certificate and revocation schemes are used based on the extended block chain technology. Furthermore, a reputation management scheme is presented which uses historical interaction of the vehicle and indirect opinions of other vehicles.

3. PROPOSED MODEL

This section presents the proposed model for secure and efficient communication in vehicular Ad-Hoc networks. The significant amounts of works have been carried out to improve communication performance but security remains a challenging task. Moreover, the dynamic network topology creates several challenging issues. Thus, user authentication and key management will be a tedious task to maintain the cure communication. This research work is focusing on key management and data security. The proposed model of GKMC organized as follows:

- A. First of all, we deploy a Vehicular Ad-Hoc network and define the preliminary and initial assumptions related to the network.
- B. In the next phase, V2V, V2 and V2X communication protocol is presented where key management, authentication, key exchange modules are presented.
- C. Finally, the cryptography scheme is presented to secure the data packets.

A. Preliminaries and Network Modelling

The VANET architecture contains several components such as trusted authority (TA), road side units (RSUs), service provider (SP), and onboard unit (OBU) mounted vehicles as shown in figure 2. Each entity of network has assigned specific tasks. Generally, TA is considered as car manufacturer or transport management department. Trust authority is responsible for registering the RSUs and to generate public and private keys to authenticate each user. TA performs several computations hence we assume that enough storage is provided to TA along with adequate computation capability. Road Side Units (RSUs) are the infrastructures, which are deployed at the road intersection and road side which act as relays for V2I communication. Figure 3 shows required architecture of VANET for proposed system.

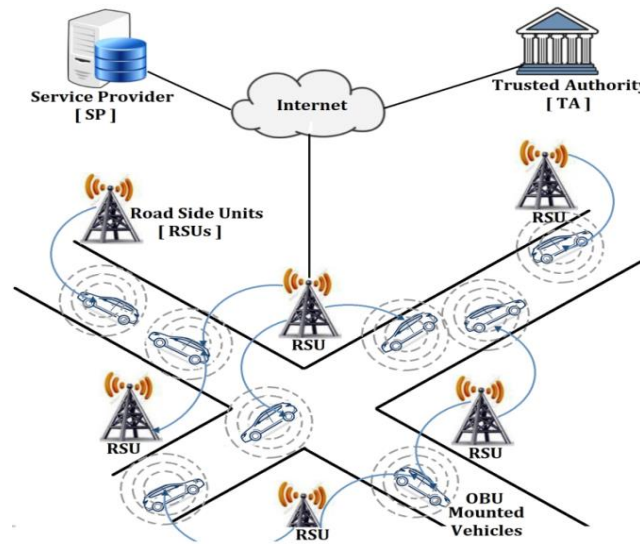


Fig 3: VANET Model

The communication between RSU and vehicle is performed using dedicated short-range communications (DSRC) protocol. The main task of RSU is to verify the legitimacy of the received message from vehicles [8]. The service provider provides different types of application to all vehicles. To provide an application services, the RSU receives the message from vehicles, verifies its legitimacy and if the message is valid then forwarded to the application server for providing the required service. The SA, TA and RSU can communicate through a safety cable channel. Similarly, OBU is a wireless unit, which is installed on the vehicle with GPS and a small device for short range communications.

B. Security Requirements

In VAETs, data security and privacy are considered as an important factor to develop the secure VANET model. This work focuses on the following security requirements [28][29][30]:

- **User authentication and message integrity:** in this architecture, once the message is transmitted to the receiver, then the receiver must ensure the message integrity and validity by verifying the signatures.
- **Vehicle identity protection:** the actual vehicle identity is only known by the trusted authority and the vehicles. This helps to maintain anonymity from other vehicles in the network.

- **Message traceability:** during communication, if any bogus message is received by the receiver, then TA should be able to track the original identity of the vehicle.
- **Message stealing:** during data communication of message transmission phase, the protocol should be able to secure the high confidentiality message by avoiding message stealing by attackers.
- **Fake Message attack:** the fake messages are disseminated to harm the network entities hence the protocol should restrict the fake message circulation in the network.
- **Fake identity:** according to this attack the real identity of vehicle is forged and used for concealing the information. Hence, the identity of vehicles should be anonymized to prevent this attack.

Similarly, here it focus on achieving the solution for non-repudiation attack, replay attack and DOS attack to develop a more robust and secure network architecture.

Hence, this work introduced a combined novel key management and data security approach for VANETs. The proposed model is implemented in two fold manner where first of all key management is performed and later, data encryption is applied. The proposed approach is denoted as GKMC (Group Key Management & Cryptography Schemes).

Table 1. Mathematical Properties

$\mathcal{G}_o, \mathcal{G}_N$	Additive cyclic group
p	Large prime order for additive cyclic group
F	Bilinear map function
\mathcal{R}_{RSU}	Random key for RSU
K_{RSU}	Public key of RSU
H	Hash function

C. GKMC(Group Key Management & Cryptography Schemes)

(I) Group Key Management

This work first describes the bilinear map generation to incorporate the security functionality in the network. Let us consider that \mathcal{G}_o and \mathcal{G}_N are the additive cyclic group with the large prime order p . A map function F is computed as in equation 1.

$$\hat{F}: \mathcal{G}_o \times \mathcal{G}_N \rightarrow \mathcal{G}_N \quad (1)$$

In which it should satisfy the following conditions to generate the bilinear pairing.

- **Bilinear:** for all $M, N \in \mathcal{G}_o$ and for all $a, b \in \mathbb{Z}_p^*$, the function is $\hat{F}(aM, bN) = \hat{F}(M, N)^{ab}$. Similarly, for all $M, N, Y \in \mathcal{G}_o$ the bilinear map as in equation 2 and 3.

$$\hat{F}(M + N, Y) = \hat{F}(M, Y) \hat{F}(N, Y) \quad (2)$$

$$\hat{F}(M, N + Y) = \hat{F}(M, N) \hat{F}(M, Y) \quad (3)$$

- **Non-degenerate:** there exists that the $M, N \in \mathcal{G}_o$, there is $\widehat{F}(M + N, Y) \neq 1$
- **Computability:** for all $M, N \in \mathcal{G}_o$ efficient approach is present to compute the $\widehat{F}(M, N)$
- **Symmetric:** As per equation C4 for all $M, N \in \mathcal{G}_o$

$$\widehat{F}(M, N) = \widehat{F}(N, M) \quad (4)$$

According to the proposed approach first, it represents the authentication process between RSU and vehicle. The complete authentication process is divided into three phases as initialization, authentication and distribution of group keys. The working process of these stages is described in the following subsections.

I.a. Initialization

In the first step of proposed GKMC approach, we perform user registration and key allocation for each vehicle in the network. In VANET architecture, a vehicle must be registered with the TA then TA assigns secret information to the corresponding vehicle. During this process, the TA stores driver information such as contact information, address and license plate number. Let us consider that the $G_{\mathcal{H}}$ as cyclic additive group, $Q_{\mathcal{H}}$ is the generator and unique vehicle id is denoted as id . Here, we adopt the Hash function as $\mathcal{H}: \{0,1\}^* \times G_{\mathcal{H}} \rightarrow \mathbb{Z}_p^*$ where \mathbb{Z}_p^* denotes the nonnegative integer set which is less than the prime number p . Based on these assumptions, the TA generates a secret key S_{id} for each vehicle in the network. The key is given as in equation 5.

$$S_{id} = \mathcal{H}(id, Q_{\mathcal{H}}) \quad (5)$$

The generated key is assigned to the appropriate vehicle after registration. The secret key for each user/vehicle is stored in the TA's key storage dataset. Simultaneously, the TA selects a random integer to assign the private key for RSU. This random number is selected as $\mathcal{R}_{RSU} \in \mathbb{Z}_p^*$. Let G_1 be an additive cyclic group of order q generated by P . Thus, the RSU public key can be computed as in equation 6.

$$K_{RSU} = \mathcal{R}_{RSU}P \quad (6)$$

Here, RSU public key, generator P , hash function \mathcal{H} and G_1 will be published to all devices whereas the RSU private secret key \mathcal{R}_{RSU} is kept secret during this process. This process is used for registering the vehicle. Let us assume that the registered vehicle is entering the range of RSU. If that vehicle demands for any service from the VANET, then key assignment is the necessary task. This vehicle v selects a partial private key as $R_v \in \mathbb{Z}_p^*$, and the corresponding partial public key is given as in equation 7.

$$Q_v = \mathcal{R}_v P \quad (7)$$

Where P is the generator, using these parameters service request, public key and vehicle id are delivered to the corresponding RSU which are arranged as $\langle ServiceRequest, Q_v, id \rangle$. Once the partial public key Q_v is generated, the RSU request to TA for providing the secret key S for vehicle id i.e. RSU request to TA for S_{id} . At this stage, we generate a secure hash function as $\mathcal{H}: \{0,1\}^* \times G_1 \rightarrow G_1$. With the help of this, the partial keys can be generated as in equation 8.

$$Q_{id} = \mathcal{H}(id, Q_{RSU}) \quad (8)$$

Based on the secret key, partial public key and secret key of RSU, a certificate is delivered to the vehicle as in equation 9.

$$C = Q_{id} S_{id} \mathcal{R}_{RSU} \quad (9)$$

Thus, the partial private key can be derived as in equation 10.

$$R_u = R_{RSU} Q_{id} \quad (10)$$

Now, the public key can be presented as $\langle Q_v, id \rangle$ and the private key set is given as $\langle \mathcal{R}_v, \mathcal{R}_u \rangle$

I.b. Authentication

In this process, we present authentication process for the vehicle. We assume that at a time t , the vehicle starts using the road message service. The partial public key and time combine as in equation 11.

$$Q_1 = Q_v t = \mathcal{R}_v P t \quad (11)$$

Moreover, a cyclic group G_2 is generated with the prime order s and the bilinear operator is given as $\hat{F}: G_1 \times G_1 \rightarrow G_2$. Here, the intermediate value of partial public key can be obtained as in equation 12.

$$Q_{id} = H(id, Q_{RSU}) \quad (12)$$

Where id is the vehicle id, and Q_{RSU} is the public key of RSU which are already known to the vehicle. Along with this, we generate two important parameters α and β for authentication as in equation 13.

$$\begin{aligned} \alpha &= \hat{F}(Q_{RSU}, Q_{id}) \\ \beta &= h(t \parallel \alpha, \mathcal{R}_{id}) \end{aligned} \quad (13)$$

Where \mathcal{R}_{id} is the secret key of vehicle which is allocated during initialization phase. Based on these parameters, we generate the final signature as in equation 14.

$$U = \mathcal{R}_u + Q_{id} \mathcal{R}_v t v \quad (14)$$

From here, the vehicle sends the authentication request as $\langle U, id, t, v \rangle$ and RSU performs the verification process whether $\alpha = \frac{\hat{F}(P, U)}{\hat{F}(Q_1, Q_{id})^v}$. In order to deliver the message, the following verification condition must be satisfied as in equation 15.

$$\frac{\hat{F}(P, U)}{\hat{F}(Q_1, Q_{id})^v} = \hat{F}(P, Q_{id}, \mathcal{R}_{RSU}) = \hat{F}(\mathcal{R}_{RSU}, P, Q_{id}) = \hat{F}(\mathcal{R}_{RSU}, Q_{id}) \quad (15)$$

After satisfying this condition, the authentication phase is completed.

I.c. Key Distribution

In this phase, the generated group keys are distributed to each legitimate vehicle. This key assignment is done by TA. Let us assume that the secret $\mathcal{E} \in \mathbb{Z}_p^*$ is randomly selected by TA, and then RSU computes as in equation 16.

$$\mathbb{W} = \mathcal{E} Q_v T \quad (16)$$

$$\mathbb{F} = h(\mathbb{W} \parallel v, \mathcal{R}_u)$$

Here RSU is capable to generate the partial public \mathcal{R}_u as described before. Now, the $\langle \mathbb{W}, \mathbb{F}, T \rangle$ is computed by RSU and transmitted to vehicle. Here our aim is to combine the secret key with the current time stamp T . In this process, the vehicle compares the value of F with stored values and if it is found valid then secret is derived as in equation 17.

$$\begin{aligned} N &= \mathbb{W}T^{-1}\mathcal{R}_v^{-1} = Q_vT\mathcal{E}T^{-1}\mathcal{R}_v^{-1} \\ &= \mathcal{E}P \end{aligned} \quad (17)$$

Hence, the final group can be achieved as in equation 18.

$$G_k = h(N) = h(\mathcal{E}p) \quad (18)$$

(II) Data encryption and decryption

This phase presents the data encryption and decryption approach to provide secure data exchange. According to this process, the first task is to secure the data using encryption key which is used by receiver to encrypt and decrypt the data by sender and receiver. This phase uses the state value (*state*) of receiver vehicle as an encryption key. To maintain the location privacy, this methodology uses hash state value before transmitting to the corresponding vehicle.

II.a. Key Generation

This complete process of data encryption and process of key generation is shown in figure 4.

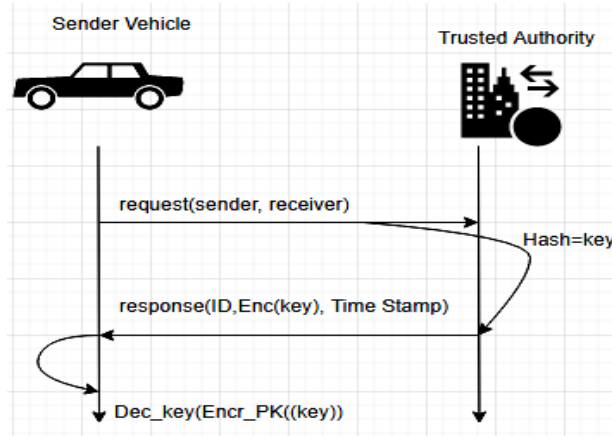


Fig 4: Data encryption process and key generation

As shown in Figure 4, complete process of key generation is completed by using following steps:

- (a) The sending vehicle v_s sends the message request ($Message_{req}$) of receiver vehicle v_r request to the trusted authority where public key is used for encrypting the message request. This is expressed as in equation 19.

$$Cipher_{V_{sTA}} = Encr_{TA_{pk}}(S_{Id} + R_{ID}) \quad (19)$$

As given in eq. 15, the public key of TA is used for encrypting the sender vehicle id S_{Id} and receiver vehicle R_{ID}

- (b) The trusted authority decrypts the cipher text of eq. (15) using its own secret key as in equation 20.

$$Dec_{Message} = Decr_{TA_{sk}}(Cipher_{V_sTA}) \quad (20)$$

- (c) This decryption process provides the state values of receiver vehicle and hashes these values. Hash values are considered as the key for sender vehicle to encrypt the data. This is denoted as in equation 21.

$$key = Hash(state_{r1}, state_{r2}, \dots, state_{rN}) \quad (21)$$

- (d) TA uses sender public key to encrypt the key, the encrypted data and time stamps are send to the sender vehicles from TA. The final received message from TA is denoted as in equation 22.

$$Cipher_{TAV_s} = Encr_{V_{spk}}(ID + key + Timestamp) \quad (22)$$

- (e) After receiving the data from (18) sender vehicle uses own private key to decrypt this data and gets the real key for further encryption along with the time stamps. This is computed as in equation 23.

$$Timestamp + key = Decr_{V_{spk}}(Cipher_{TAV_s}) \quad (23)$$

II.b. Data encryption

Before transmitting the data from sender vehicle to receiver vehicle we encrypt the data using time stamp and secret key to provide the data security during transmission. This encryption format is given as in equation 24.

$$Message = Timestamp + R_{ID} + Encr_{key}(ID + data) \quad (24)$$

This encrypted data is transmitted to the receiver vehicle where data decryption is performed through repeal mechanism.

II.c. Data Decryption

The receiver vehicle receives the encrypted data packet as cipher text along with the time stamp. At the receiver end, we perform the data decryption to achieve the original data. The actual process of data decryption is shown in figure 5.

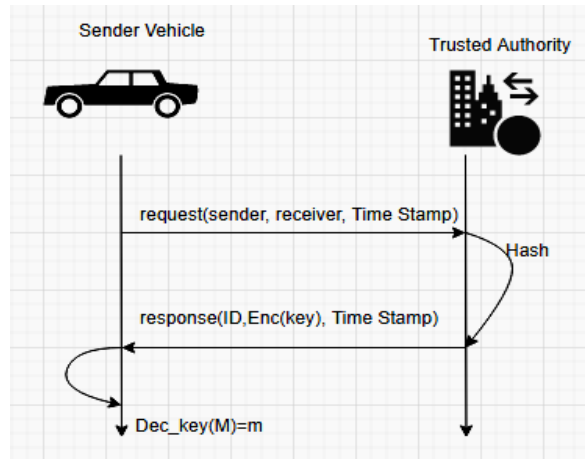


Fig 5. Data decryption process

The current time stamp is greater than the previous time stamp hence we use decryption key as its previous time stamp history. Figure 4 shows the decryption process with required parameters. This decryption is performed using following steps:

- (a) Receiver vehicle (v_r) sends the received cipher text to TA about status value from where it receives the cipher text as in equation 25.

$$Cipher_{VrTA} = Encr_{TA_{pk}}(R_{ID} + Timestamp) \quad (25)$$

- (b) After receiving the cipher text, the TA decrypts the data using its own secret key and the decrypted message is achieved as in equation 26.

$$Dec_{Message} = Decr_{TA_{sk}}(Cipher_{VsTA}) \quad (26)$$

- (c) In the next step, historical state values are achieved and hashed to generate the key for further encryption as

$$key = Hash(state_{r1}, state_{r2}, \dots, state_{rN}) . \quad (27)$$

- (d) Now the public key of receiver vehicle is used to encrypt the receiver ID, key and its time stamps as in equation 28.

$$Cipher_{TAV_r} = Encr_{Vr_{pk}}(R_{ID} + key + Timestamp) \quad (28)$$

- (e) In next step, the v_r uses private key to decrypt the cipher text and achieves the real key for decryption as in equation 29.

$$Timestamp + key = Decr_{Vr_{pk}}(Cipher_{TAV_r}) \quad (29)$$

- (f) Finally, this key is used for decrypting the cipher text and original message is received as in equation 30.

$$Dec_{Data} = Dec_{key}(Message) \quad (30)$$

4. RESULTS AND DISCUSSION

This section shows the experimental analysis using proposed approach. The obtained performance is compared with the existing techniques. This research work is mainly focused to ensure the security of VANET.

4.1. Achieved Security Issues

These proposed works achieve the following security issues such as:

- **Authentication:** in this work, authentication is an important task to avoid the attacker nodes to join the network. Later, Hash values are obtained from the key and an authentication process is performed after achieving the RREP message from the communicating node.
- **Message confidentiality:** this work applies symmetric cryptography where public and private secret keys are generated from the RSA key generation method.
- **Location privacy and anonymity:** this security aspect is obtained by generating the Hash of the location of the vehicle and vehicle ID.

4.2. Performance Measurement Parameters

This section presents the experimental analysis using proposed approach. The performance of proposed approach is measured in terms of packet loss, throughput, packet delivery, end-to-end delay, average message delay and message loss ratio. The simulation parameters are given in table 2.

Table 2. Simulation Parameters

Simulation Parameter	Used Value
Simulation Area	1500m x1500m
Simulation Time	100s
Data Traffic	CBR
Route protocol	AODV
Mobility	Random Waypoint
Channel bandwidth	6 Mbps

According to table 2, proposed approach is considered total of 100 nodes which are deployed in the 1500m x1500m area. The vehicles follow the Random Waypoint model with the constant bit rate data traffic. Total 10 nodes are considered as faulty node which is responsible for various attacks such as Denial-of-service, black hole and badmouthing etc. In this work, we measure the performance of proposed approach under various attacks to show the robust performance. The obtained performance is measured using following performance metrics:

- (a) **Packet Loss Ratio:** is measured by taking the ratio of the dropped packets which are generated from the source but not delivered to the destination as in equation 31.

$$PLR = \frac{P_{Sent} - P_{received}}{P_{Sent}} \times 100 \quad (31)$$

Where P_{Sent} denotes the number of sent data packets, $P_{received}$ denotes the received number of data packets.

- (b) **Throughput:** is measured by computing the total of bytes received successfully in one communication session. This is computed as in equation 32.

$$Throughput = \frac{P_{Sent} - P_{received}}{P_{Sent}} \times 100 \quad (32)$$

- (c) **Packet delivery ratio:** this is measured by taking the ratio of delivered packet to the destination which are generated from source nodes. It can be calculated as in equation 33.

$$PDR = \frac{P_{received}}{P_{Sent}} \times 100 \quad (33)$$

- (d) **Average end-to-end delay:** this is the time take by the data packet to reach to the destination. During this phase, the route discovery, data retransmission and propagation time etc. are considered. This is computed as in equation 34.

$$Delay = \frac{\sum_{i=1}^{P_{succes}} (D_i - s_i)}{P_{succes}} \times 100 \quad (34)$$

Where D_i denotes the i^{th} packet receiving time, s_i denotes the sending time for i^{th} packet and P_{succes} denotes the number of successfully transmitted packets.

- (e) **Average message delay:** this is the measurement of total delay occurred to deliver the message from one source to destination. This can be computed as in equation 35.

$$AverageDelay = \frac{\sum_i^{N_v} \sum_{m=1}^{M_{sent}} (T_{sign}^{i,m} + T_{trans}^{i,m,RSU} + T_{verify}^{i,m,RSU})}{\sum_{i=1}^{N_v} M_{sent}^i} \quad (35)$$

Where N_v is the total number of vehicles, M_{sent}^i is the total number of packet sent by vehicle i , $T_{sign}^{i,m}$ is the time required to sign a message by vehicle, $T_{trans}^{i,m,RSU}$ is the time require to transmit the message m to RSU and $T_{verify}^{i,m,RSU}$ is the time required for authentication. Similarly, we measure the message loss ratio as in equation 36.

$$Messagelossratio = \frac{\sum_{i=1}^{N_v} M_{sent}^i - \sum_{r=1}^{RSU^n} M_{rec}^r}{RSU^n * \sum_{i=1}^{N_v} M_{sent}^i} \quad (36)$$

4.3. Comparative Performance Analysis

This section shows the comparative experimental analysis where, performance of the proposed approach is compared with the existing techniques by varying the number of vehicles, speed and malicious nodes in the network.

4.3.1 Varying vehicles with fixed Speed

In this phase, performance is evaluated by varying the number of vehicles ranging from 20 to 100 with 10 numbers of malicious nodes present in the network and the speed of vehicles is fixed in the range of 70-72kmph. First, it computes the packet loss ratio for this experimental setup and compared the performance with AOMDV [25] and SE-AOMDV [25] protocols.

- a. **Packet loss ratio:** the comparative performance in terms of packet loss ratio is shown in figure6. According to this experiment, the existing protocols AOMDV [25] and SE-AOMDV [25] drop the packet due to malicious nodes in the network. However, the existing protocols suffer from the malicious nodes and drop the packets, whereas, proposed approach shows robust performance.

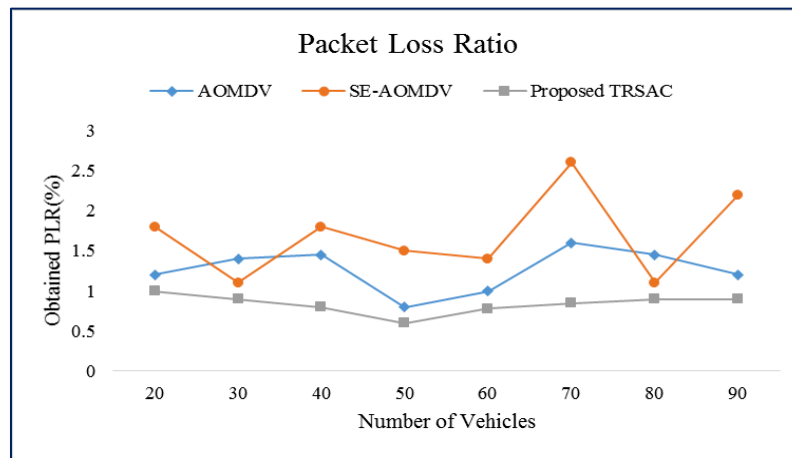


Fig 6. Packet Loss ratio performance

The average packet loss rate is obtained as 1.26%, 1.68% and 0.84% using AOMDV [25], SE-AOMDV [25], and Proposed approach. This experiment shows that the proposed approach achieves 0.66% and 0.49% improvement when compared with the AOMDV [25] and SE-AOMDV [25] methods.

- b. **Throughput performance:** in the next phase of the proposed approach, it measures the throughput performance for same experiment setup. The obtained performance is depicted in figure 7. The more number of vehicles creates issues in link stability and frequent selection of relay nodes creates a complex environment for communication leading towards the decreased throughput, whereas, proposed approach helps to main the network reliability and reduces packet drops.

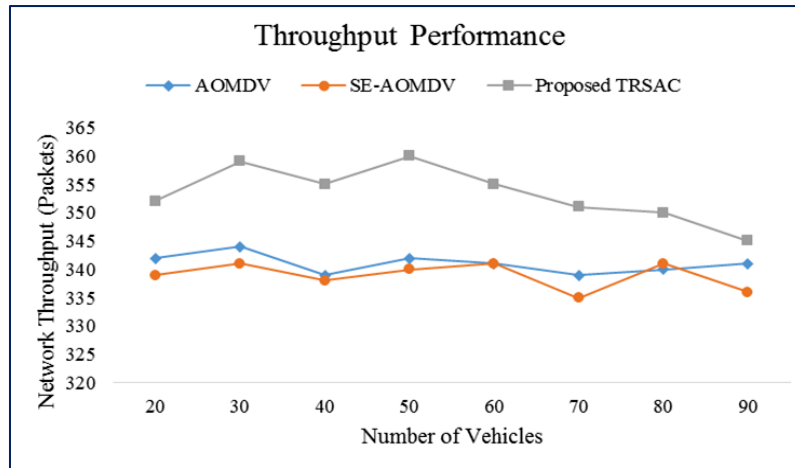


Fig 7. Throughput performance

The average network throughput performance is reported as 341, 338.875 and 353.375 using AOMDV [25], SE-AOMDV [25] and proposed approach.

- c. **End-to-End Delay:** the comparative performance in terms of end-to-end ratio is shown in figure8. Similarly, we compute the end-to-end delay performance for varied number of vehicles for the considered experimental scenario.

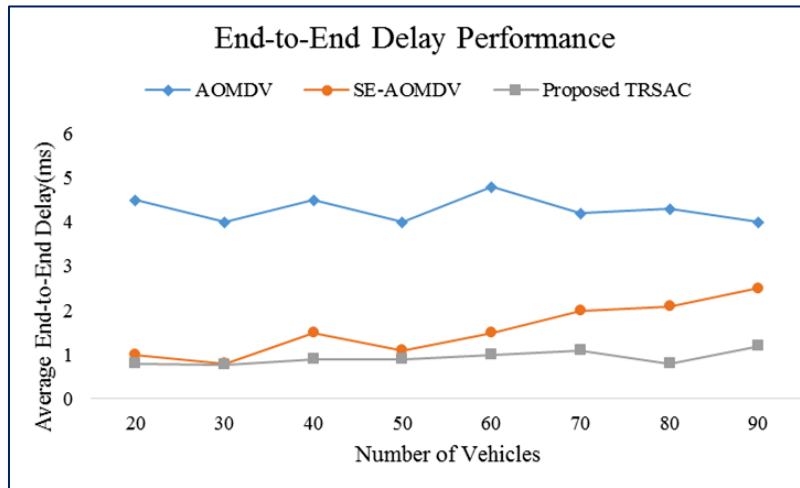


Fig 8. End-to-End delay performance

This experiment shows that the average end-to-end delay is obtained as 4.28ms, 1.56ms, and 1.1ms using AOMDV [25], SE-AOMDV [25] and proposed approach.

4.3.2 Varying speed with fixed vehicles

In this sub-section, experimental analysis considers 40 vehicles with a varied speed ranging from 5-30ms. The experimental study presented in AOMDV [25], SE-AOMDV [25]. This experiment shows that the increased vehicle speed causes packet loss.

- a. **Packet loss ratio:** first, it computes the packet loss ratio and compares the achieved performance with existing techniques. The obtained packet loss performance is depicted in figure 9.

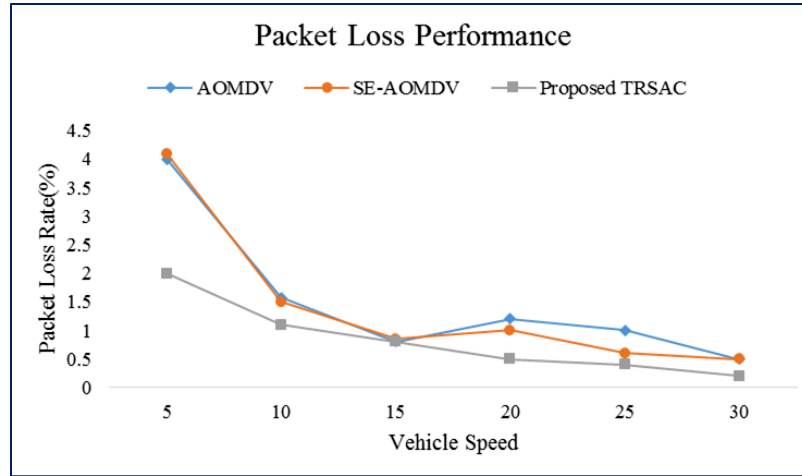


Fig 9. Packet Loss Performance

The proposed approach takes advantage of link connectivity and efficient relay node selection to reduce the packet loss. According to this experiment the average packet loss is obtained as 1.51%, 1.42% and 0.83% using AOMDV, SE-AOMDV and proposed approach,

- b. **Throughput performance:** similarly, it measures the system throughput for varied speed of vehicle and compared the obtained performance with existing technique. The achieved performance is depicted in figure 10.

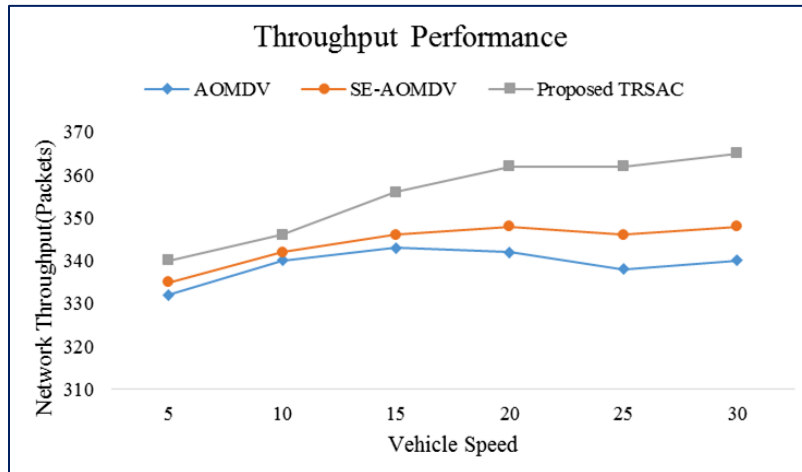


Fig 10. Network Throughput Performance

According to this experiment the average Network Throughput Performance is obtained as 1.27%, 1.38% and 1.62% using AOMDV, SE-AOMDV and proposed approach,

- c. **End-to-End delay:** later, experimental analysis has been done for end-to-end delay computation. The proposed approach uses light weight computations and less

computational cost helps to achieve the less delay. The obtained performance is compared as depicted in figure 11.

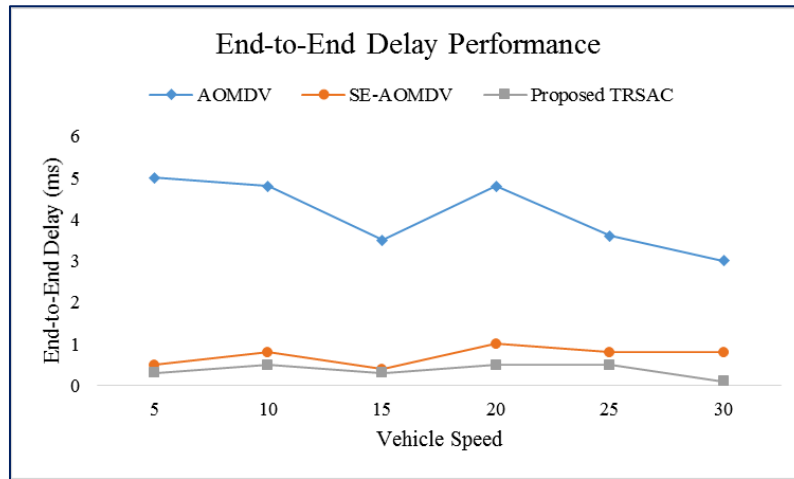


Fig 11. End-to-End delay performance

According to this experiment, the average end-to-end delay performance is obtained as 4.11ms, 0.71ms, and 0.36ms using AOMDV, SE-AOMDV, and proposed approach.

- d. Packet delivery rate:** in order to show the robust performance of proposed approach we extend the experimental study with SUMO mobility model where 100-900 vehicles are considered. The performance is measured in terms of average packet delivery and average delay for varied number of vehicles. Figure 12 shows a comparative performance in terms of packet delivery. As discussed before, the proposed approach archives better throughput due to link connectivity and optimal relay selection.

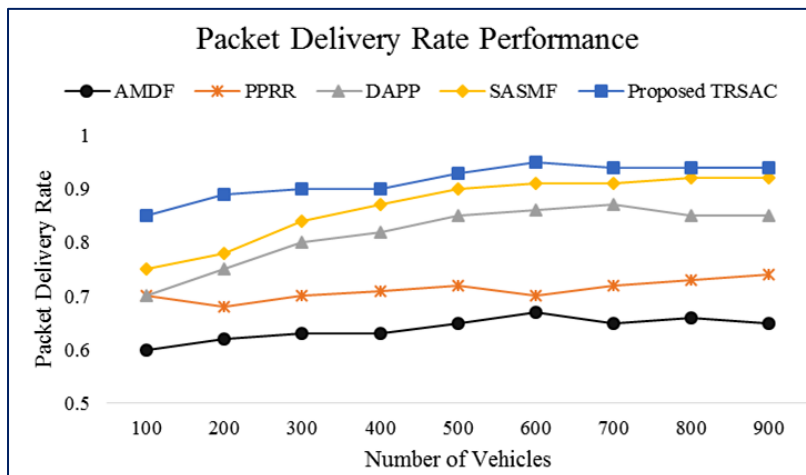


Fig 12. Packet delivery performance

Figure 11 shows a comparative performance where the packet delivery performance is obtained as 0.64, 0.71, 0.81, 0.86, and 0.91 using AMDF [32], PPRR [33], DAPP [31], SASMF [34] and Proposed approaches.

5. CONCLUSION

This proposed approach focused on improving the VANET by incorporating key management and data cryptography process. According to the proposed approach first, it introduces a novel key management scheme where any new upcoming vehicle is registered with Trusted Authority (TA) and authenticated to perform the communication. This helps to maintain security and reduces outsider attacks. In the next phase, introduced Elliptic curve cryptography scheme to encrypt and decrypt the data during vehicle communication. Hence, the proposed approach provides better security. Moreover, the proposed approach uses lightweight computations which help to reduce the computational overhead of the network. The comparative study is carried out which shows the improved performance using proposed approach.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

- [01] Liu, J., Wan, J., Wang, Q., Deng, P., Zhou, K., & Qiao, Y. (2015). A survey on position-based routing for vehicular ad hoc networks. *Telecommunication Systems*, 62(1), 15–30. doi:10.1007/s11235-015-9979-7.
- [02] Tomar, R., Prateek, M., & Sastry, G. H. (2016). Vehicular adhoc network (VANET)-an introduction. *International Journal of Control Theory and Applications*, 9(18), 8883-8888.
- [03] Zhang, W., Xiao, X., Wang, J., & Lu, P. (2018, November). An improved AODV routing protocol based on social relationship mining for VANET. In *Proceedings of the 4th International Conference on Communication and Information Processing* (pp. 217-221). ACM.
- [04] Yang, X., Sun, Z., Miao, Y., Wang, N., Kang, S., Wang, Y., & Yang, Y. (2015, March). Performance Optimisation for DSDV in VANETs. In *2015 17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim)* (pp. 514-519). IEEE.
- [05] Abdelgadir, M., Saeed, R. A., & Babiker, A. (2017). Mobility routing model for vehicular Ad-Hoc networks (VANETS), smart city scenarios. *Vehicular Communications*, 9, 154-161.
- [06] Kadadha, M., Otrók, H., Barada, H., Al-Qutayri, M., & Al-Hammadi, Y. (2017, June). A street-centric QoS-OLSR protocol for urban vehicular ad hoc networks. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 1477-1482). IEEE.
- [07] Silva, R., Lopes, H. S., & Godoy, W. (2013, September). A heuristic algorithm based on ant colony optimization for multi-objective routing in vehicle ad hoc networks. In *2013 BRICS Congress on Computational Intelligence and 11th Brazilian Congress on Computational Intelligence* (pp. 435-440). IEEE.
- [08] Taherkhani, N., & Pierre, S. (2012, October). Congestion control in vehicular ad hoc networks using meta-heuristic techniques. In *Proceedings of the second ACM international symposium on Design and analysis of intelligent vehicular networks and applications* (pp. 47-54). ACM.
- [09] Aadil, F., Bajwa, K. B., Khan, S., Chaudary, N. M., & Akram, A. (2016). CACONET: ant colony optimization (ACO) based clustering algorithm for VANET. *PloS one*, 11(5), e0154080.
- [10] Jindal, V., & Bedi, P. (2018). An improved hybrid ant particle optimization (IHAPO) algorithm for reducing travel time in VANETs. *Applied Soft Computing*, 64, 526-535.
- [11] Li, G., Ma, M., Liu, C., & Shu, Y. (2017). Adaptive fuzzy multiple attribute decision routing in VANETs. *International Journal of Communication Systems*, 30(4), e3014.
- [12] Bagherlou, H., & Ghaffari, A. (2018). A routing protocol for vehicular ad hoc networks using simulated annealing algorithm and neural networks. *The Journal of Supercomputing*, 1-25.
- [13] Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., & Sezaki, K. (2005). CARAVAN: Providing location privacy for VANET. Washington Univ Seattle Dept of Electrical Engineering.
- [14] Sampigethaya, K., Li, M., Huang, L., & Poovendran, R. (2007). AMOEBA: Robust location privacy scheme for VANET. *IEEE Journal on Selected Areas in communications*, 25(8), 1569-1589.

- [15] Wasef, A., &Shen, X. S. (2010). REP: Location privacy for VANETs using random encryption periods. *Mobile Networks and Applications*, 15(1), 172-185.
- [16] Chim, T. W., Yiu, S. M., Hui, L. C., & Li, V. O. (2012). VSPN: VANET-based secure and privacy-preserving navigation. *IEEE transactions on computers*, 63(2), 510-524.
- [17] Rahbari, M., &Jamali, M. A. J. (2011). Efficient detection of Sybil attack based on cryptography in VANET. arXiv preprint arXiv:1112.2257.
- [18] Mejri, M. N., Achir, N., &Hamdi, M. (2016, January). A new group Diffie-Hellman key generation proposal for secure VANET communications. In *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 992-995). IEEE.
- [19] Lu, H., Li, J., &Guizani, M. (2012, January). A novel ID-based authentication framework with adaptive privacy preservation for VANETs. In *2012 Computing, Communications and Applications Conference* (pp. 345-350). IEEE.
- [20] Eiza, M. H., Owens, T., & Ni, Q. (2015). Secure and robust multi-constrained QoS aware routing algorithm for VANETs. *IEEE Transactions on Dependable and Secure Computing*, 13(1), 32-45.
- [21] Wang, F., Xu, Y., Zhang, H., Zhang, Y., & Zhu, L. (2015). 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. *IEEE Transactions on Vehicular Technology*, 65(2), 896-911.
- [22] Liu, Y., He, Z., Zhao, S., & Wang, L. (2016). An efficient anonymous authentication protocol using batch operations for VANETs. *Multimedia Tools and Applications*, 75(24), 17689-17709.
- [23] Wang, J., Zhang, Y., Wang, Y., &Gu, X. (2016). RPREP: A robust and privacy-preserving reputation management scheme for pseudonym-enabled VANETs. *International Journal of Distributed Sensor Networks*, 12(3), 6138251.
- [24] Ahmed, S., Rehman, M. U., Ishtiaq, A., Khan, S., Ali, A., & Begum, S. (2018). VANSec: Attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead. *Journal of Sensors*, 2018.
- [25] Makhoulouf, A. M., &Guizani, M. (2019). SE-AOMDV: secure and efficient AOMDV routing protocol for vehicular communications. *International Journal of Information Security*, 1-12.
- [26] Manickam, P., Shankar, K., Perumal, E., Ilayaraja, M., & Kumar, K. S. (2019). Secure Data Transmission Through Reliable Vehicles in VANET Using Optimal Lightweight Cryptography. In *Cybersecurity and Secure Information Systems* (pp. 193-204). Springer, Cham.
- [27] Zhang, H., Bochem, A., Sun, X., &Hogrefe, D. (2018, June). A security aware fuzzy enhanced reliable ant colony optimization routing in vehicular ad hoc networks. In *2018 IEEE Intelligent Vehicles Symposium (IV)* (pp. 1071-1078). IEEE.
- [28] Tan, H., Choi, D., Kim, P., Pan, S., & Chung, I. (2018). Secure certificateless authentication and road message dissemination protocol in VANETs. *Wireless Communications and Mobile Computing*, 2018.
- [29] Islam, S. H., Obaidat, M. S., Vijayakumar, P., Abdulhay, E., Li, F., & Reddy, M. K. C. (2018). A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. *Future Generation Computer Systems*, 84, 216-227.
- [30] Lu, Z., Liu, W., Wang, Q., Qu, G., & Liu, Z. (2018). A privacy-preserving trust model based on blockchain for vanets. *IEEE Access*, 6, 45655-45664.
- [31] Tang D, Ren J (2016) A novel delay-aware and privacy-preserving data-forwarding scheme for urban sensing network. *IEEE TransVehTechnol* 65(4):2578–2588
- [32] Xia Y, Chen W, Liu X, Zhang L, Li X, Xiang Y (2017) Adaptive multimedia data forwarding for privacy preservation in vehicular ad-hoc networks. *IEEE Trans IntellTranspSyst* 18(10):2629– 2641
- [33] Rabieh K, Mahmoud MMEA, Younis M (2017) Privacy preserving route reporting schemes for traffic management systems. In: *IEEE international conference on communications*, pp 7286–7291.
- [34] Yang, P., Deng, L., Yang, J., & Yan, J. (2019). SASMF: Socially Aware Security Message Forwarding Mechanism in VANETs. *Mobile Networks and Applications*.

AUTHORS

Mr. Mahabaleshwar Kabbur, research scholar of REVA University. He has obtained his Master's degree in Computer Applications (MCA) and research degree in Master of Philosophy in computer science (M.Phil). He has 14 years of experience in teaching and 03 years of experience in research. He is pursuing his doctoral research on "Security on Wireless networking for VANET". He is published 12 research articles in UGC approved international journals and presented 15 articles in various National and International conferences. His specializations and research interests include Network Security, Content-Based Image Retrieval Techniques & IoT.



Dr. Anand R, Assistant Professor in School of Computer Science & Applications REVA University holds doctoral degree in Computer Science from SCSVMV University, Tamil Nadu. He has completed B. Sc (Computer Science) from Madurai Kamaraj University, Tamil Nadu and M.Sc (Computer Science) from Manonmanium Sundarnar University, Tamil Nadu. He has 18 Years of experience in teaching and 10 years of experience in research. He has published 11 research articles in various International / National Journals and conferences and also his 02 Patents got published on topic "Anti-Intrusion Device for Computer Network" Application No: 201941013025 and "Vital Sign Monitoring System" Application Number Application No: 201941030703. His research areas include Data mining, Software engineering, Cloud security and Cryptography.



Dr. V. ARUL KUMAR, Assistant Professor in School of Computer Science & Applications REVA University holds doctoral degree in Computer Science from Bharathidasan University-Tamil Nadu. He has completed B. Sc (Applied Sciences – Computer Technology), M.Sc (Applied Sciences – Information Technology) from K.S.R College of Technology and M.Phil in Computer Science from Bharathidasan University, Tamil Nadu. He has 6 Years of experience in teaching and 8 years of experience in research. He has qualified in State Eligibility Test (SET) conducted by Mother Teresa Women's University. He has published 24 research articles in various International / National Journals and conferences. His research areas includes data Mining, cloud security and cryptography.

