International Journal of Mobile Computing and Multimedia Communications
Volume 13 • Issue 1

Multi-Level ECDH-Based Authentication Protocol for Secure Software-Defined VANET Interaction

Umesh K. Raut, Oriental University, India*
Vishwamitra L. K., Oriental University, India

ABSTRACT

The proposed multi-layer ECDH-based authentication model and the vehicles in the VANET are authenticated and authorized to protect the network from the attacks for which the vehicles undergo the registration process initially. After the successful registration, the messages generated from the vehicles are communicated through multi-step authentication, which assures the exactness of the received messages. Then, the authorization process is executed in the VANET so as to ensure the safe and secure interactions between the vehicles. The implemented authentication model is analyzed using the comparative methods based on the performance standards, such as detection accuracy, execution time, packet delivery ratio (PDR), and throughput. The detection accuracy, execution time, PDR, and the throughput of the network while executing the proposed multi-level ECDH-based authentication system are better than the prevailing security models as the security features of the existing models are enhanced better than the existing state-of-the-art methods.

KEYWORDS

Authentication, Elliptic Curve Cryptography (ECC), Road Side Unit (RSU), Software-Defined Vehicular Networks (SDVN), VANET

1. INTRODUCTION

The VANET attains a pre-eminent role in the initiative transport system (ITS) as it supports the transport system in various circumstances such as enabling mutual communication, minimizing accidents, enhancing the interaction efficiency, and reducing traffic congestion (Pournaghi, *et al.,* 2018; Zhou, *et al.,* 2020; Jiang, *et al.,* 2020). VANET (Mendiboure, *et al.,* 2020) is characterized as the network organization of the vehicles, which ensures seamless interactions between the RSU and the vehicles or any other well-developed frameworks within the network coverage area. Since the innovation is on the verge of assembling computerized managing automobiles, it is needed to normalize vehicle-to-vehicle (V2V) or vehicle-to-other specialist's correspondence (Mishra, *et al.,* 2020). Yet, the interaction in the vehicles is confronting some issues like the mobility of the vehicles, heterogeneity of correspondence channels, and rapid variation in network topologies (Mendiboure, *et al.,* 2020). The software-defined network (SDN) is one of the advanced technologies designed to restrain the interaction mentioned above issues experienced in the VANET. SDN in VANETs is a rapid-developing systems administration that permits adaptability and organization design by isolating information and control planes within the network organization (Baskett, 2013; Alouache, *et al.,* 2020). The SDN-based VANET design comprises RSU and automobile with the onboard unit

DOI: 10.4018/IJMCMC.297961 *Corresponding Author

(OBU). The RSUs are associated with the SDN regulator, which acts as a controller to get worldwide organization data (Raja, *et al.,* 2020).

In the real-world application, the SDVN is exposed to various attacks, such as jellyfish, man in the middle attack (MITM), sybil, and DOS, which acts as a great threat to the confidentiality privacy of the transferred data. Hence, SDVN has to satisfy security parameters such as availability, integrity, and authentication (Kim, *et al.,* 2017; Kumar, *et al.,* 2020) to ensure secure interaction between the vehicles. Hence, this research aims to develop a dynamic security scheme that enhances the privacy of the security of SDVN and makes the network resistant to numerous attacks including replay and sybil attacks. In SDVN Sybil attacks create the issues such as altering the voting base system and disturbance in routing. Recognizing the replay and Sybil attack is the significant process to be executed in the SDVN to manage the vehicles' privacy and intercept the genuine vehicle's connecting identity (Parham & Pouyan, 2020). Furthermore, a strong privacy potential that tracks the motorist's attitude is required in SDVN to prevent malicious vehicles from misusing the data and to avoid spreading fake information. An experience profile must be created to recognize and block the malicious vehicles from the genuine vehicles in the network organization.

The conventional methodologies employed for secure and safe interaction are dependent on key administration and data encryption. Hence, the conventional methodologies can just ensure secure message trade between known source and objective sets. These methodologies can't be straightforwardly applied regarding SDVNs because of the unique characteristics of VANETs (Manivannan, *et al.,* 2020). Whether there is an organization threat known as the distributed denial of service (DDoS) assault has been recognized, at that point, it very well may be presumed that there might be the possibility of an assault (Fung & Zhu, 2016; Kolandaisamy, *et al.,* 2019). The route tracking system is employed in the network to determine the assault (Kolandaisamy, *et al.,* 2019). In the RSU-dependent group authentication (RGA) strategy, the RSU gives a gathering ID and gathering key pair to every automobiles within reach to guarantee reliable interaction amidst the automobiles with minimized organization congestion. A private-collaborative ID (p-CIDS) detects the potential assaults with the collaborative learning (CL) strategy. The vehicles in the p-CIDS co-operate with other vehicles to learn collaborative ideas (Raja, *et al.,* 2020). The block chain (BC) innovation (Mendiboure, *et al.,* 2020) provides an appropriate solution for confirmation and access control issues (Xie, *et al.,* 2019; Mendiboure, *et al.,* 2018; Mendiboure, *et al.,* 2020). A packet checking dependent on adjusted stream areas (PMBASR) is possibly the most basic strategies to determine the security attacks. This component works out the most effective way for beating the disadvantages of traffic-based assault identification (Kolandaisamy, *et al.,* 2019). Considering the issues of the expenses brought about by the CRL through the invalidated authentication, many related researchers preferred a few effective validation plans by utilizing the hash message authentication code (HMAC), which maintain a strategic distance from aggressors varying the substance of messages conveyed by real automobiles or RSUs (Rajput, *et al.,* 2015; Jiang, *et al.,* 2020).

This research devises an authentication model based on the ECDH algorithm to empower the privacy and security of the transmitted message in the VANET through multi-level authentication. In the proposed multi-level ECDH authentication method, the vehicle within the network organization should register with the authorized trusted certified authority (TCA), before establishing the mutual interaction to protect the message from the vulnerable behavior of the malicious nodes. After the successful registration, the vehicles undergo multi-level authentication to empower the dispatched message's genuineness. Then, the authorization process is done to enable safer interaction between the vehicles. The major contribution of the research is enlisted below:

- Restraining the unauthenticated vehicles through the registration process, registering all the vehicles and the RSUs with the TCA.

- The multi-level ECDH based authentication model is proposed in the research to protect the vehicles from hazardous attacks and enable safer communication of the messages between the vehicles, thereby ensuring privacy for the transmitted vehicles in the network arrangements.
- The proposed multi-level ECDH based authentication model ensures security through the security parameters like session keys, encryption based on ECDH, and hashing function.

The structure of the research is cataloged as below: section 2 illustrates the motivation of the research, section 3 describes the issues prevailing in the VANET, section 4 demonstrates the proposed approach, section 5 depicts the results & discussion of the research, and section 6 concludes the research.

2. REVIEW OF THE EXISTING LITERATURE

In this section, the review of the existing literature is detailed. Mendiboure, *et al.,* (2020) suggested block-chain-based security approaches restrain the authentication and access control issues. Enhanced security, flexibility, and low cost are considered as the prime advantage of the blockchain-based security approach. Though the blockchain-based security approaches enhance the system's security, it suffers from drawbacks such as insufficient scalability for large SDVN. Furthermore, the system is not utilized for SDN as it lacks the validation and obtain authority for SDN controllers. Kumar, *et al.,* (2020) put forward the revised version of the AODV directing protocol to recognize and destroy the malignant nodes from the network organization. The revised AODV system fails to determine the attacks like end-and-end rounding overhead as it is revamped to determine the black hole attack. Kolandaisamy, *et al.,* (2019) utilized packet marking based on adapted stream region (PMBASR) so as to upgrade the safety levels of both the passenger and the vehicles. Even though the PMBASR system efficiently recognizes the DDOS attack, it fails to determine the other attacks such as the black hole, sybil, and malware attacks. Raja, *et al.,* 92020) suggested an efficient scheme for SDVN so called to enhance security and energy efficiency. The RGA technique utilized in this system restrains the overhead issues of the network. The main issue experienced in this system is that some devious vehicles will create inconvenience as they provide inaccurate information. Manivannan, *et al.,* (2020) suggest efficient techniques to restrain the issues in VANETs such as privacy, security, and authentication. The sophisticated sensors are utilized to track the lane automatically, avoid collisions and suggest the safest lane. However, the lack of standardized metrics is one of the main issues in the secured VANETS. Alouache, *et al.,* (2020) put forward an efficient routing protocol known as the HSDN-GR routing protocol to enhance the VANET system's reliability. The presence of introverted nodes, which acts as a stumbling block of the entire network, is the main drawback experienced in this system. Furthermore, the collaboration of entities remains a complex process in the HSDN-GR routing protocol. Parham & Pouyan, (2020) suggested a detection algorithm to recognize the Sybil attacks in-vehicle communication. The system also enhances the privacy of the transferred data. The high processing time for the validation of the accuracy is the main drawback of the system. Mishra, *et al.,* (2020) suggested the routing protocol, which provides better reliability to the network. The cryptographic mechanism adapted in the MHVB protocol enhances the security of the system. Yet, the system is susceptible to some the security attacks such as DoS and eavesdropping. Pal & Narwal (2021) suggested a validation scheme that includes a two-factor authentication process to obtain powerful non-repudiation and high reliability. The two-factor validation scheme effectively handles security threats such as identity theft, masquerading, and recreation of the original certificates. The responsibilities of trusted authority are decentralized, which is considered the greatest threat to the VANET. Jiang, *et al.,* (2020) put forward the high efficiency validating scheme based on a trusted authority. Privacy preservation and authentication are some of the advantages enlisted in the validation system. The delay is one of the main drawbacks experienced in this validation scheme, which degrades the performance of the function.

2.1. Challenges

Some of the issues that are experienced in the VANET interaction are enlisted below

- The administration of reliable correspondences among those gadgets is experienced as a hectic challenge to deal with in an enormous spread organization. Therefore, the vehicle should validate all senders regarding renouncement status, i.e., they are not repudiated before responding to the occasion.
- Most of the conventional methods depend on key administration and data encryption. Hence, the conventional methodologies can just ensure secure message trade between known source and objective sets.
- The existing strategy only concentrates on RSU and vehicles; they fail to concentrate on the secure transmission between the vehicles in the network area.
- The authentication process's complexity enhance with the extension in the nodes of vehicles in the network area, as the large number of vehicles generates huge validation requests.
- The existing methods fail to recognize the security attacks including server spoofing attacks, replay attacks and Sybil attacks.

3. PROPOSED MULTI-LAYER ECDH BASED AUTHENTICATION MODEL FOR SECURE INTERACTION IN VANET

The authentication or validation is the significant process to be established in the well-organized VANET to enable the secure interaction between the vehicles in the organization. The authentication enhances the privacy and the security of the interaction by enabling access to the authenticated users. Furthermore, the authentication process aids the TCA in recognizing and restrict the malicious attackers from gathering confidential information from genuine vehicles and spreading false information. Hence, this research contributes to safe and secure interaction between the vehicles in the organization through the enhanced security model.

A well-structured security model named multi-level ECDH depended authentication scheme accompanied by conditional privacy preservation for VANET is proposed to enhance the security and provide smooth interaction within the vehicles. The proposed multi-level ECDH based authentication ensures the safest interaction between the vehicles and the RSUs restrain the assaults, known as replay and Sybil attacks. Furthermore, the proposed multi-level ECDH based authentication enhances the life expectancy of the network as it is reliable to those security attacks. It is developed with the aid of different security modalities, like hashing function, Chebyshev-defined polynomial, session password, and cryptography strategies for secure authentication of vehicles through the private, public keys, and other associated secrecy-assuring keys. Moreover, forward secrecy is assured by the proposed multi-level ECDH authentication model by ensuring the vehicles' authentication in the network for secure communication. In the SDVN, various vehicles communicate and interact in the network, which leads to a chance for the outflow of confidential data through the malicious vehicles during the mutual interaction. Furthermore, the malicious vehicles transmit hypocritical information, which leads to accidents or traffic infringements. Hence, a highly secured authentication model is requisite to block these malicious vehicles or attackers from communicating in the network. In this research, the multi-level ECDH based authentication is developed to ensure the safest interaction among the vehicles without the interference of the malicious attacker.

3.1 System Model

The geographic location of the vehicle is maintained using the GPS device. Here, the vehicle sends the messages to the neighbor vehicle for choosing the optimal path. The SDVN is comprised of On Board Units (OBUs), RSUs, and trusted certified authority (TCA). The process is executed based

on the multi-level authentication protocol. TCA's authentication process helps recognize and restrict the malicious attackers from gathering confidential information from genuine vehicles and spreading false information. In addition, the newly devised multi-level authentication protocol provides secure communication between the vehicles against the Sybil and replay attack. In the registration phase, vehicles and the RSU register with the network and obtain the unique ID for the interaction, which is depicted in Figure 1. After the registration, the validation of the vehicles is employed utilizing the proposed multi-level ECDH authentication process, in which 6 levels of validation are used for providing the authentication, shown in figure 2. Then, the key is updated, followed by the key authorization to provide secure communication, which is shown in figure 3.

Entities In The Authentication Model: The proposed authentication approach comprises TCA, RSU, and the vehicles. While registering the vehicles and RSUs with the TCA, TCA furnishes the private accreditation and stores the identities, which are the significant tasks assigned to the TCA. RSU is the predetermined framework in the SDVN, which is attached to the SDN controller that accomplishes the regiment layer instruction and enables the interaction between the RSUs. Thus, secure communication in VANET is enabled with the strengthened five security demands, such as source integrity, authentication, non-repudiation, confidentiality, and conditional anonymity. Hence, in this research, a vehicle attempting to communicate in the network undergoes an effective authentication, discussed below.

3.2 Registration Phase

The authentication model ensures safer and smoother communication in the network. The vehicles commuting in the network undergo the registration phase before the authentication, which restricts the users from malicious attacks. Every vehicle registers with the nearby registered RSU with their unique ID to enable the ceaseless interaction between the vehicles in the network. The registration process of the vehicle and the RSU are elaborated below.

Encryption Preliminaries: Let us consider J_a as the finite field over the prime order a and Y is considered as the additive group initiated through the point X in the multiple elliptical curve $E\left(J_a\right)$ of the order m. The TCA selects the secure hashing function H(), and the symmetric encryption standard is E(). Thus, the public key of TCA is given by,

$$Pub_{TCA} = S_{TCA} * a \tag{1}$$

where, S_{TCA} refers to the secret key and it is given by, $S_{TCA} \in J_a$. The elliptic curve equation is mathematically represented as,

$$E\left(J_a\right): z^2 = y^3 + py + q\left(\bmod a\right) \tag{2}$$

where $p, a \in J_a$, and $a > 3$, which is the finite field. The security of ECC depends on the modified ECDH algorithm and the TCA constructs the function, which is represented as,

$$f\left(y, z\right) = q_0 y + q_1 y + r \tag{3}$$

where, q_0, q_1 are constants that belong to the finite field J_a.

3.2.1. Vehicle Registration Phase

The registration phase ensures the registration of the incoming vehicles with the nearby registered RSUs. Consider the vehicle V_i requesting for communication in the network, then the vehicle provides the identity I_i to the TCA to enroll in the data communication process. The process involved in the registration phase of the vehicle is elucidated in the following stages.

Stage 1: The vehicle V_i selects the random number $R_i \in J_a$ and it estimates the public key in the initial stage, which is formulated as,

$$F_i = R_i \bmod a \tag{4}$$

Then, the vehicle V_i transmits the public key with the identity I_i to the TCA for registration. The identity of the vehicle V_i carries the credentials, such as the username and the password of the vehicle, which is given as, $I_i = \left\{ I_i^{\rho}, I_i^{u} \right\}$. At the TCA, the vehicle V_i is verified, and upon the absence of the vehicles' identity at the TCA, the registration begins; else, the authentication process is provoked.

Stage 2: In the second stage, the invocation from the vehicles is accumulated in the TCA, and the random number is chosen within $R \in J_a$. Then, the TCA computes the reconstruction data as given by,

$$C_i = F_i + R\,a \tag{5}$$

The TCA derives the equation mentioned above from computing the public key of the registering vehicle, which is followed by the generation of the private security factor.

Stage 3: In this step, the privacy of the received credentials is ensured using the ECDH algorithm so as to enhance the security to the credentials of the vehicles for which the TCA chooses the random numbers $\gamma, \lambda \in J_a$ and the identity of the vehicles I_i is encrypted to secure the credentials. The encrypted identity is expressed in the following equations as,

$$UI_i = E\left[I_i\right] = \left[U_1, U_2\right] \tag{6}$$

where, $U_1 = X\gamma * I_i$ and $U_2 = X\lambda * I_i$ are the secured credentials, using which the TCA enables the generation of the security factor.

Stage 4: Then, the TCA generates an experience profile W_i by concealing the public key C_i and UI_i, and generates the encoded message,

$$s = H_a\left(W_i\right) \tag{7}$$

where, s is the encoded message, and $H_a\left(W_i\right)$ is the hash function of the experience profile in order to generate the private security factor. The mathematical representation of the private security factor is expressed as,

$b = sR + K_{TCA}$ (8),

where, K_{TCA} is the public key, R is the Random number and s is the encoded message. The private security factor is broadcasted to the vehicle, which extracts the experience profile and decodes to generate the reconstruction data.

Step 5: The vehicle utilizes the hash function to compute the message $s = H_a\left(W_i\right)$ and it decodes the experience profile in order to extract the reconstruction data C_i.

Step 6: Using the decoded messages, the vehicles generate the private key, expressed in the following mathematical representation.

$$K_i^c = \left[R_i * H\left(S_i \| F_i \| t_i\right) W_i \left(\mathrm{mod}\, n\right)\right] \tag{9}$$

where, R_i is the random number, S_i is a pseudonym-based chebyshev polynomial, t_i refers to the time-stamp, and W_i be the experience profile generated by the TCA. The pseudonym S_i is computed by the following mathematical expression

$$S_i = \left[I_i \oplus H\left(W_i * F_i \| t_i\right)\right] \tag{10}$$

Step 7: The estimated public key of the vehicles is calculated in the following mathematical representation.

$$K_i^o = sF_i + H\left(K_i^c\right) * a \tag{11}$$

The public key ensures the secure transmission of the data and furthermore, the authenticity of the received information from the TCA is verified through checking the partial security factor.

Step 8: The vehicle V_i verifies the acquired message and the validation is carried out through computing the following equation

$$K_i^{o'} = K_i^c * P^{TCA} \tag{12}$$

The criterion, $K_i^{o'} = K_i^o$ validates the received information from the TCA. At the same time, P^{TCA} TCA's public key is saved in the vehicle and the RSUs. Finally, the vehicle broadcasts the information, such as S_i, t_i, K^c, K^o, F_i, ϕ_i to the TCA, which is stored for the further authentication of the vehicles for communication.

3.2.2. RSU Registration Phase

The registration of the RSU is a significant task related to the security process, where the RSUs must ensure the registration with the TCA such that the vehicles communicate with the nearby authenticated RSU. Following are the registration phases of RSU.

Stage 1: In the first stage of the RSU registration, the RSU selects the security factor $R_j \in J_a$ with identity RSU_j and expiry time t_e. The RSU identity with the password and username are given below.

$$RSU_j = \left\{RSU_j^u, RSU_j^\rho\right\} \tag{13}$$

where, RSU_j^u represents the username of the RSU and the RSU_j^ρ represents the password of RSU.

Stage 2: In the second stage of the RSU registration, the invocation from the RSU is gathered such that the random number between $R_j \in J_a$ and with expiry time t_e is chosen to estimate the reconstruction data of the RSU. The estimated reconstruction data is mathematically represented as,

$$C_j = F_j + RG \tag{14}$$

The reconstruction data of the RSU is utilized to derive the public key of the RSU.

Stage 3: The privacy of the RSU credentials is protected using the encryption algorithm named ECDH algorithm. The TCA selects the random number of ω and υ within J_a to encrypt the privacy identity, which is mathematically represented as,

$$U\left[RSU_j\right] = E\left[RSU_j\right] = \left[RS_1, RS_2\right] \tag{15}$$

The RS_1 and RS_2 is mathematically expressed as,

$$RS_1 = X.\omega * RSU_j \tag{16}$$

$$RS_2 = X.\upsilon * RSU_j \tag{17}$$

Stage 4: In this stage, the TCA generates the experience profile of the RSU indicated as, W_i^{RSU} through encoding the public key C_j and the identity RS_j. The TCA forwards the experience profile with the RSU for the estimation of the public and the private credentials.

Stage 5: The experience profile of RSU W_i^{RSU} is utilized to evaluate the private key and the public key. Mathematical representation of private key generated by the experience profile is demonstrated as,

$$K_j^c = \left[R_j * H\left(RSU_j \| F_j \| t_e\right) + W_i^{RSU} \left(\mathrm{mod}\, n\right)\right] \tag{18}$$

where, R_j is the random number, RSU_j is the identity, F_j is the public key, t_e is the expiry time W_i^{RSU} is the experience profile and H() defines the hash functions. The public key generated is mathematically expressed as,

$$K_j^o = H\left(K_j^c\right) * a \tag{19}$$

Stage 6: Finally, the validation process is carried out through computing the message given by,

$$\theta_j^{'} = k_j^c * P^{TCA} \tag{20}$$

If the estimated $\theta_j^{'}$ is equal to the public key k_j^o then, the validation becomes successful and the RSU communicates the information, like RSU_j, t_e, K_j^c, K_j^o, R_j, θ_J with the TCA, which is stored for the effective RSU identity. After the successful registration of the vehicle and RSU, the TCA creates the private accreditation in addition with the experience profile, which is furnished to each vehicle commuting in the network.

3.2.3. Group RSU Initialization

The RSUs in the SDVN acquire unique private and public accreditations to initiate the group authentication. The group authentication model is given as,

$$GI_i = H\left[RSU_j \| I_r \| O_g\right] \tag{21}$$

where, O_g is the order of group $\in J_a$, RSU_j is the unique ID of the RSU, I_r is the ID of the RSU, and O_g is the group's order. RSU generates the hash chain of length l_c and perform the reverse hash function, which is represented as $T_{l-1} = H\left(T_1\right)$, $T_l = H\left(T_{l-1}\right)$, $b_{l-1} = H\left(b_1\right)$ And $b_l = H\left(b_{l-1}\right)$.

A unique group key is generated through the RSU so as to establish a secure interaction between the vehicles and the RSU. The mathematical model of each group key is mathematically represented as,

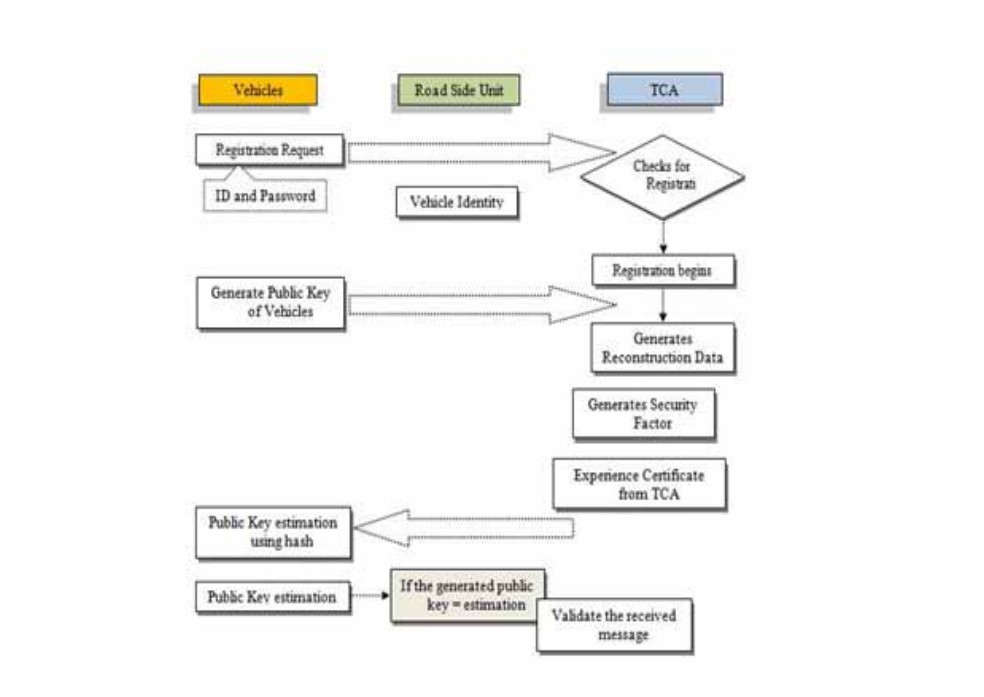
$$Gk_i = H\left(b_1, T_l\right) \tag{22}$$

The group key enables the communication between the vehicles with the group ID, pseudo ID, and the message, where the group ID is checked to accept or reject the message regarding the validation. The TCA then creates the retract polynomial ID $Ip_i^{'}$ with the aid of identities and the confidential key of the SDVN. The retracted polynomial is utilized to minimize the storage space and to reduce the searching space. The generated retracted polynomial ID is mathematically expressed as,

$$Ip_i^{'}\left(X\right) = \left(X - I_1\right)\left(X - I_2\right).....\left(X - I_k\right) \tag{23}$$

where, I_1 , I_2 ……. I_k represents the identification of the revoked vehicles and the retracted polynomial is distributed with all the RSUs to block the malicious automobiles commuting in the specific network organization. Figure 1 illustrtes the registration phases of the authentication process.

Figure 1. Block representation of Registration module



3.3. Authentication Process

After the registration process, the authentication of the vehicles is initiated, where the vehicle V_i obtains the generated group key and group ID from the accessible RSU. The trustworthiness of the acquired message is validated with the aid of group ID and the group key, which is obtained from the registration phase. This article proposes a multi-level ECDH authentication model to ensure secure authentication and authorization to initiate mutual interaction. The multi-level authentication process is elaborated in the following sub-sections.

3.3.1 Level-1 Validation

The level-1 validation is initiated in the SDVN with the aid of initial message M_1, which comprised of the password and user name stored in registration phase. The initial message is mathematically represented as,

$$M_1 = H\left(I_i^u \left\| I_i^p\right.\right) \oplus E\left(k_i^c\right) \tag{24}$$

The identity of the vehicle including the username and the password of the vehicle V_i are exposed to the hashing function, which is Ex-OR-ed with the encrypted privacy identity of the vehicle to generate the initial message. The generated initial message in the vehicles is communicated with the j^{th} RSU, which saves the initial message, where the estimation of x_1 and y_1 are done. The generated x_1 and y_1 is mathematically modeled as,

$$x_1 = H\left(I_i^{u,sav} \left\| I_i^{\rho,sav}\right.\right) \tag{25}$$

$$y_1 = M_1^{sav} \oplus x_1 \tag{26}$$

$$y_1^1 = E\left(k_i^c\right) \tag{27}$$

where, $I_i^{u,sav}$ and $I_i^{\rho,sav}$ are the saved username and password of the vehicle in the RSU, k_i^c is the private key of the i^{th} vehicle, and M_1^{sav} is the saved initial message in the RSU. Finally, the validation process is revoked such that if the generated y_1 is same as the encrypted privacy identity y_1^1 then, the level-1 verification is verified. Hence, the condition required for the level-1 verification is represented in the following equation.

$$y_1 = y_1^1 \tag{28}$$

3.3.2 Level-2 Validation

The level-2 validation process is established with the generation of the intermediate message M_2 and the generated M_2 message is formulated as,

$$M_2 = H\left(RSU_j^u \left\| RSU_j^\rho \right.\right) \oplus E\left(k_j^c\right) \tag{29}$$

The identities, such as the username and the password of the RSU are concatenated and hashed and the hashed function is Ex-ORed with the encrypted private key of the RSU, which is represented in the above equation. The message M_2 is then transmitted to the TCA and the intermediate message is saved as, M_2^{sav} using which the generation of x_2 and y_2 is done. The mathematical representation of x_2 and y_2 are given below.

$$x_2 = H\left(RSU_j^u \left\| RSU_j^\rho \right.\right) \tag{30}$$

$$y_2 = M_2^{sav} \oplus x_2 \tag{31}$$

$$y_2 = E\left(K_j^c\right) \tag{32}$$

At this point, the level-2 validation is initiated by comparing the messages y_2 and the encrypted private key of RSU. If the y_2 is found equal to the encrypted value of the private key of the RSU then, the second level verification is confirmed. The condition for the second level validation is expressed in the above mathematical representation.

3.3.3 Level-3 Validation

The generation of the authentic message A_3 is responsible for the initiation of the level-3 validation and for the generation of the A_3 message, the partial security factor and the private key is required. The private key of the RSU is hashed and the concatenation of the hashing function and the encrypted function of the security factor of TCA, w_{TCA} is performed to generate M_3 as given by,

$$M_3 = H\left(k_j^{c,\ sav}\right) \left\| E\left(w_{TCA}\right)\right. \tag{33}$$

The message M_3 is forwarded to the RSU, where M_3 is saved message and a new authentic message M_3^* is calculated as follows:

$$M_3^* = H\left(k_j^c\right) \left\| E\left(w_{TCA}^{sav}\right)\right. \tag{34}$$

where, w_{TCA}^{sav} is the saved partial security factor of the TCA in the RSU. The third-level authenticates terminates when the generated message M_3^* and M_3^{sav} are equal.

3.3.4 Level-4 Validation

The fourth level of verification is initiated using the partial security factor of RSU and the TCA. If the generated message is equivalent with the saved message then, the fourth-level validation is terminated. The condition for the fourth level of validation is specified as,

$$w_{RSU}^{*} = w_{RSU}^{sav} \tag{35}$$

3.3.5 Level-5 Validation

The level-5 verification is based on the encrypted message M_4, which is initiated using the private key of RSU and the security factor of the TCA as,

$$M_4 = H\left(k_j^c\right) \| E\left(w_{TCA}\right) \tag{36}$$

The estimated encrypted message is forwarded to the vehicle and saved as M_4^{sav}. Now, the message, M_4^{*} is estimated using the saved partial security factor and the private key saved, which is mathematically represented as,

$$M_4^{*} = H\left(k_j^{c,sav}\right) \| E\left(w_{TCA}^{sav}\right) \tag{37}$$

The level-5 validation terminates upon verification of the below function.

$$M_4^{sav} = M_4^{*} \tag{38}$$

3.3.6 Level-6 Validation

The authenticated-partial security factor w_{TCA}^{*} is generated through estimating the modulo of the saved partial factor. The initial message is represented through the following mathematical expression as,

$$w_{TCA}^{*} = w_{TCA}^{sav} . \mathrm{mod} . k_i^o \tag{39}$$

where, k_i^o symbolizes the public key of the vehicle and w_{TCA}^{sav} is the saved security factor of TCA. The level-6 validation is terminated when the following equation is terminated.

$$w_{TCA}^{*} = w_{TCA}^{sav} \tag{40}$$

Thus, the multi-level authentication highlights the pair authentication process, which is facilitated using the security factors, session passwords, private keys, public keys, and intermediate messages.

3.4 Group Authentication Phase

The group authentication process is instigated through the vehicles V_i in the SDVN to obtain the group ID and group key from the adjacent vehicles to enable proper interaction between them. Furthermore, the trustworthiness of the acquired message is ensured with the group key and the group ID from respected vehicles. The stages involved in the group authentication process are elucidated below.

Stage 1: The vehicles initiate the validation process by transferring their identities and group keys to the adjacent RSU.

Stage 2: In the second stage, the RSU validates the retracted polynomial ID and if the ID is abrogated then, the retracted polynomial ID is $p_i^{'}\left(X\right)=0$, further it validates whether the orientation of the vehicles are within the range $Range^{i}=\left\{I_i,k_i\right\}$. If the condition satisfies, the connection is enabled and or else the random number R_2 is generated. The random number is the ECC multiplication of the random number R_i and the time stamp t_j, which is mathematically expressed as,

$$R_2=ECC\left[R_i*t_j\right] \tag{41}$$

3.5 Key Updating Phase

In the key updating phase, the retracted polynomial key is acquired by SDVN from the TCA and initiates the key updating process. The retracted key generated is mathematically represented as,

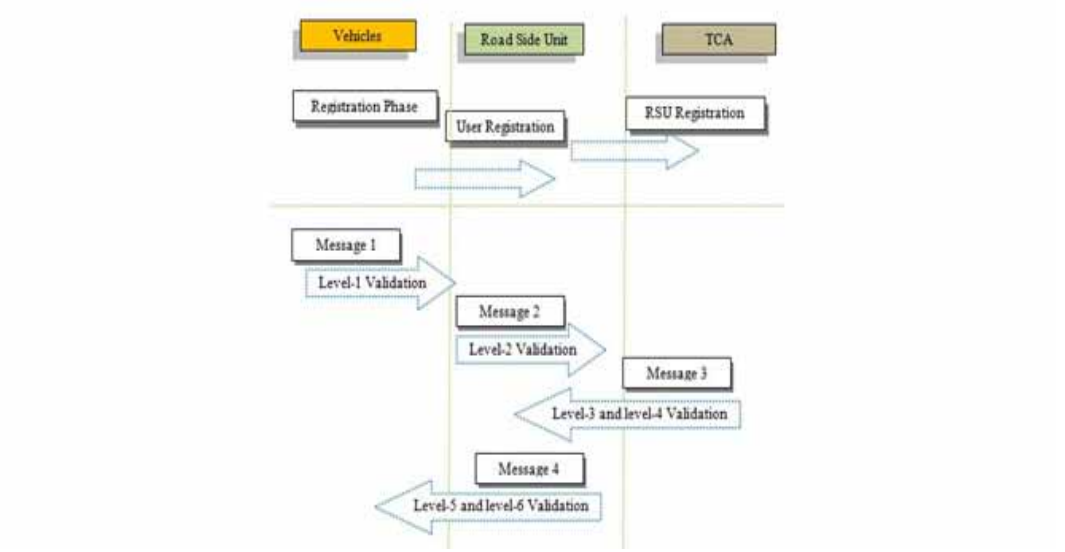
$$K_{\Re}^{i}\left(X\right)=\left(X-S_{TCA1}\right)\left(X-S_{TCA2}\right)\left(X-S_{TCAk}\right) \tag{42}$$

where, S_{TCA1}, S_{TCA2} and S_{TCA3} are mentioned in the above equation that represents the secret key of the retracted automobiles. The RSU_j gathers the retracted polynomial key and it transmits the message to the particular automobiles within the range. Authentication phase is demonstrated in the figure 2.

3.6 Authorization Phase

The authorization is the final phase in the proposed multi-level ECDH based authentication model, which assures the vehicles to transfer the data without any delay or attack. The authorization is carried out based on the log file, feedback, and private key verification. All the successive steps are validated appropriately to enable the ceaseless interaction between the vehicles in the network. The data size permitted for the ceaseless communication is mathematically represented as,

Figure 2. Authentication phase in proposed multi-level ECDH based authentication



$$D_z = f\left(D_y\right) \tag{43}$$

where,

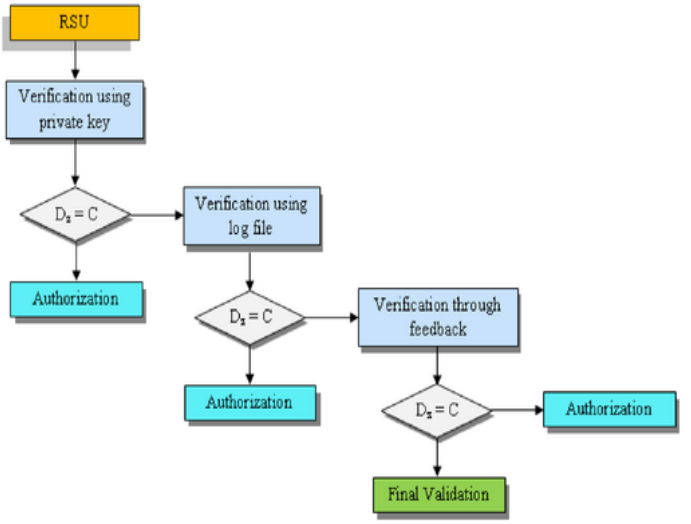
$$f\left(D_y\right) = \begin{cases} 1, if\ y < 0.25 \\ 2, if\ 0.25 \le y \le 0.5 \\ 3, if\ 0.5 \le y \le 0.75 \\ 4, if\ y > 0.75 \end{cases} \tag{44}$$

where, y is the factor which is mathematically represented as

$$y = D_{\min} + \left(D_{\max} - D_{\min}\right) * \left\lfloor \frac{D_y}{\tau} \right\rfloor \tag{45}$$

The minimum and the maximum values of the data is represented by $D_{\min}$ and $D_{\max}$ respectively, the threshold value is denoted by τ and it is varied from 0 to 1. The verification of the authentication is shown in the figure 3.

Figure 3. Authorization phase



3.6.1 Authorization by Private Key

In this step, the private key of the vehicle is hashed to verify the hashing function of the vehicles' private key, and hashing function of the vehicles' private key in the RSU are compared. It is noteworthy to note that the private keys of the vehicles are communicated with the RSUs and saved for future reference during the authentication and authorization. If the hashing functions are similar, the authorization counter is set '1', such that value evaluated using the data size must be equal to the authorization counter to ensure the communication of the vehicles in the network.

3.6.2 Authorization by Log File

Upon the failure in the authorization using the private key of the vehicles, the log file is verified for which the vehicle's experience profile is hashed compared with the generated experience profile w_{TCA} by the TCA. If the hashing function is similar, the authorization counter is set '2', and the value y evaluated using the data size should be equal to the authorization counter to ensure the vehicle for safer communication.

3.6.3 Authorization by Feedback

The final verification uses the vehicle's feedback from the other nodes. The vehicles' performance and the RSU are gathered as the feedback level to enable the authorization mechanism. The RSU determines the authorized vehicle with reputation level, and the threshold value is endorsed during the validation process to enhance the security level. The reputation factor is mathematically equated as

$$\nu\rho = \frac{1}{\tau n * \nu n} \sum_{i=1}^{\tau n} \sum_{j=1}^{\nu n} \left(\frac{D_y^{ij}}{\tau} \right) * fb_{ij} \tag{46}$$

where, $\nu\rho$ determines the reputation factor, τn determine the number of the transmitter, νn determines the number of receiver, fb represents the feedback level. If the reputation level meets the

threshold constraint then, the vehicle is authorized. Thus, the vehicle is authorized for data transfer in the network based on the private keys, log file, and feedback, which ensures that the malicious nodes never communicate or distort the communication of other vehicles.

3.7 Security Properties and Attack Analysis

The proposed multi-level ECDH authentication enhances security prospects such as integrity, confidentiality, mutual and multi-level authentication with the aid of different security modalities, like hashing function, Chebyshev defined polynomial, session password, and cryptography. The attack analysis for a few dangerous attacks are deliberated below.

a. *Reply attack:* Almost in all security systems, the confidential message is hashed to ensure the system's privacy before the data transfer, yet the requester tracks the values with the aid of advanced equipment. Though the requesters track the message, they are protected from replying to the message; thus, this category of attacks is known as reply attacks. The experimental analysis shows that the proposed authentication method is resilient to the reply attack.
b. *Sybil attack:* In the proposed authentication method, the password and the user password are utilized to enhance the privacy of the transferred data. The introducer experiences difficulty in determining both the password and the username in the data. Therefore, the proposed multi-level ECDH authentication is secure against the most common Sybil attacks.
c. *Impersonation attack:* The proposed multi-level authentication comprised of the experience profile, which includes the feedback of registered vehicles. With the help of the experience profile, the multi-level authentication process blocks the requester, who involves in the malicious activities. Hence, the proposed multi-level authentication is resistant to the impersonation attack.
d) *Server spoofing attack:* The request message from the vehicles is obtained by the RSU, and with the help of the obtained message, it computes the hashed function. Then, the hashed function generated by the vehicle and the estimated hash function is validated by the RSU to make the system resilient to the server spoofing attack.
e) *Stolen verifier attack:* The validated data from the vehicles are sometimes pilfered by the stolen verifier attack. The proposed multi-level authentication system enhances the system's privacy by utilizing the hash function, which restricts the introducer from stealing confidential data.

4. RESULTS AND DISCUSSION

To prove the effectiveness of the proposed security model, comparative analysis is accomplished in this research, and the obtained results are briefly discussed in the following section.

4.1 Experimental Setup

The implementation of proposed security model is done in MATLAB, one of the leading programming platforms installed in the windows 10 operating system with 4GB network. The number of nodes used is 50 and 100 with the simulation area 100 x 100.

4.2 Performance Metrics

The key parameters, such as detection accuracy, execution time, PDR, and throughput, are analyzed in this research to evaluate the productiveness of the proposed authentication model.

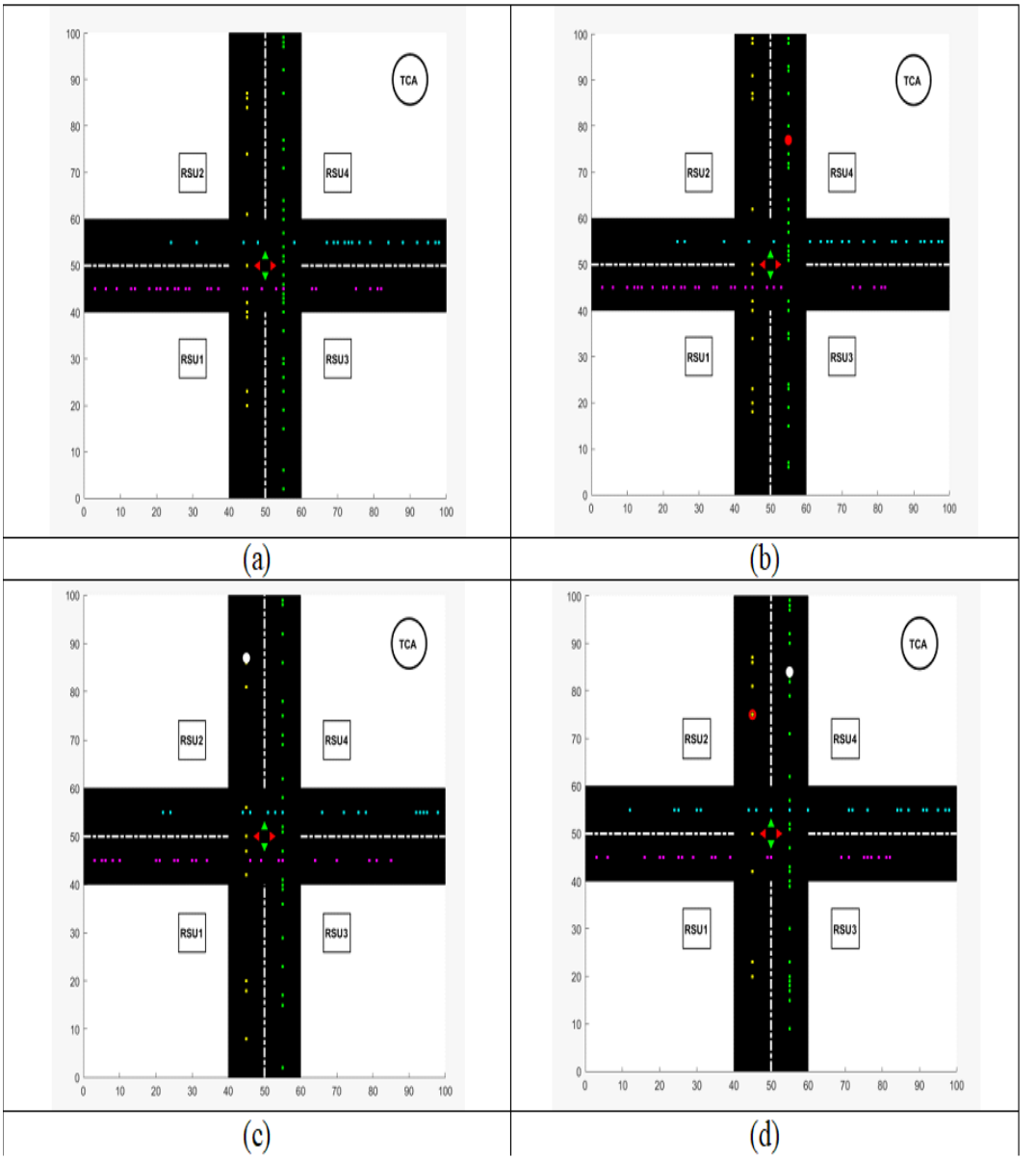
4.2.1 Detection Accuracy

Accuracy is characterized as the exactness or closeness of the observed value to the standard or the true values. The accuracy is mathematically represented as-

$$A_{cc} = \frac{Tp_v + TN_v}{Tp_v + TN_v + Fp_v + FN_v} \tag{46}$$

where Tp_v represents the true positive value, TN_v represents a true negative value, FP_v represents false positive value, and FN_v false negative value.

Figure 4. Simulation result of the proposed method



4.2.2 Execution Time

It is characterized as the time required for a system to execute the task assigned to it, and it is mathematically represented as-

$$t_{exe} = \frac{Task_{exec}}{t} \tag{47}$$

4.2.3 Packet Delivery Ratio (PDR)

PDR is characterized as the ratio of the total quantity of the packets delivered to the total quantity of the packets generated from the source node.

$$PDR = \frac{Pac_{delivered}}{Pac_{source}} \tag{48}$$

where, $Pac_{delivered}$ is the total quantity of the packets delivered and Pac_{source} is the packets generated from the source node.

4.2.4 Throughput: Term throughput is characterized as the total quantity of the packets delivered to the destination within the given amount of time.

$$Throughput = \frac{Pac_{delivered}}{t} \tag{49}$$

4.3 Simulation Output

The simulation result of the proposed method is depicted in figure 4 given below. The RSU is the road side unit, and TCA represents the Trusted Certification Authority. The red color circle indicates the Sybil attack and the white color circle indicates the reply attack.

4.4 Comparative Methods

The comparative methods utilized for the comparative analysis in this research is taken from the research article of Qin & Li, 2020; Cui, *et al.,* 2020; Zhong, *et al.,* 2020; Ouaissa, *et al.,* 2020; Geng, *et al.,* 2018).

4.5 Comparative Analysis

The comparative analyze is carried out in the research with the aid of aforementioned comparative techniques that are presented by Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* 2020), Ouaissa, *et al.,* 2020) and Geng, *et al.,* (2018) in order to manifest the supremacy of the proposed multi-level ECDH authentication. The comparative analysis is executed under two attacks, known as sybil and the replay attack.

4.5.1 Comparative Analysis Under Sybil Attack

The comparative evaluation of the framework is done in the network under the existence of the sybil attacks with 50 and 100 nodes, respectively. The deep insight over the comparative evaluation of the strategy is discussed below.

i) Comparative evaluation utilizing 50 nodes enclosed in simulation area under Sybil attack: The comparative evaluation in the presence of the sybil attack with respect to the execution time, detection accuracy, throughput and the PDR are elaborated in this section. In the figure 5, the comparative evaluation of the methods in the presence of the sybil attacks is enumerated. Figure 5 a) illustrates the comparative analysis in terms of the detection accuracy. At the fifth iteration, the detection accuracy observed in the proposed multi-level ECDH authentication is 96%. The comparative methods, which were presented by the authors, Qin & Li, (2020), Cui, *et al.,* (2020) , Zhong, *et al.,* (2020) , Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) highlighted the detection accuracy of about 82%, 85%, 64.5%, 64% and 72%, respectively. Thus, the performance improvement of about 17.0731%, 12.94%, 48.8372%, 50% and 33.33%, respectively are achieved through the proposed multi-level ECDH authentication.

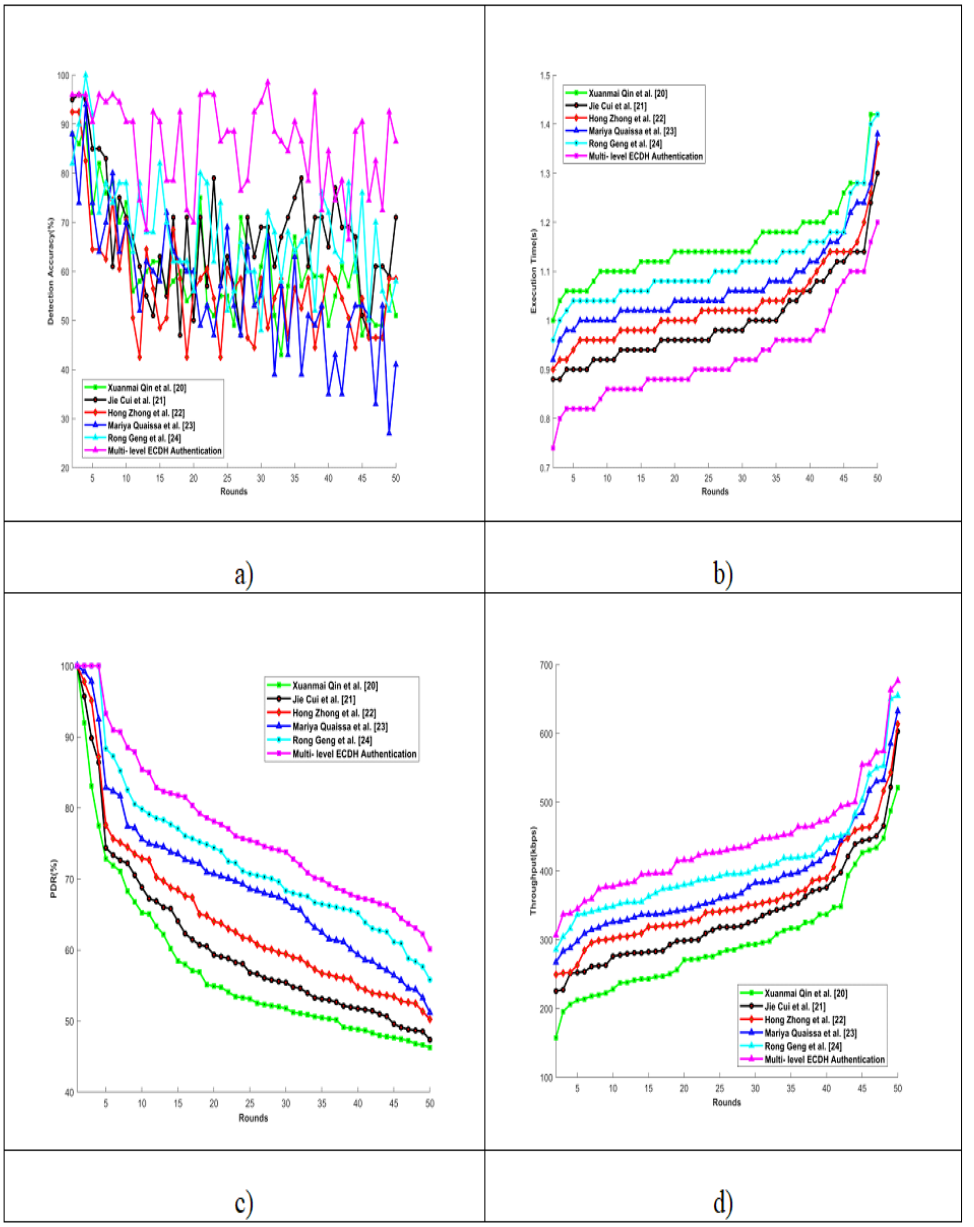
The comparative evaluation of the conventional strategies with respect to execution time is demonstrated in the figure 5 b). The execution time of 0.9 sec is achieved by the proposed multi-level ECDH authentication at the 25th iteration, which is low when compared to all the conventional methods utilized in the research articles of Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) . The values obtained by the above mentioned comparative methods for the 25th iteration are 1.14s, 0.98s, 1.02s, 1.04s and 1.1s respectively. Hence, it proves that the proposed multi-level ECDH authentication model holds the better execution time than the other conventional methods.

The comparative analysis in terms of PDR of the conventional methods is illustrated in the Figure 5 c). The packet delivery ratio of 93.2914% is achieved by the proposed multi-level ECDH authentication at 5th iteration, which outperforms all the existing methods. The PDR obtained by the comparative methods presented by Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) are 72.8460%, 74.3740%, 77.5963%, 82.8911% and 88.3617%, respectively.

Figure 5 d) demonstrates the comparative analysis of the competent and the proposed multi-level ECDH authentication in terms of throughput. The maximum throughput of 697.1957Kbps is observed in the proposed multi-level ECDH authentication at the 50th iteration. The throughput values obtained by the competent methods presented by Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) are 598.5894 Kbps, 612.1593 Kbps, 624.3755Kbps, 651.0979 Kbps and 673.9720 Kbps, respectively.

ii) Comparative evaluation utilizing 100 nodes enclosed in simulation area under Sybil attack: In this section, comparative evaluation of the methods under sybil attack using 100 nodes enclosed in simulation area is elaborated in this section. Detection accuracy of the comparative method is analyzed using the sybil attack and the result is demonstrated in the figure 6 a). The better detection accuracy is observed from the proposed multi-level ECDH authentication at the 10th iteration level and the obtained detection accuracy is 96%. The detection accuracy values of the competent methods presented by Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) are 72.35%, 80%, 56.35%, 88.1% and 63.6%, respectively. Thus, the performance improvement of the proposed multi-level ECDH authentication with respect to the comparative methods presented by Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,*

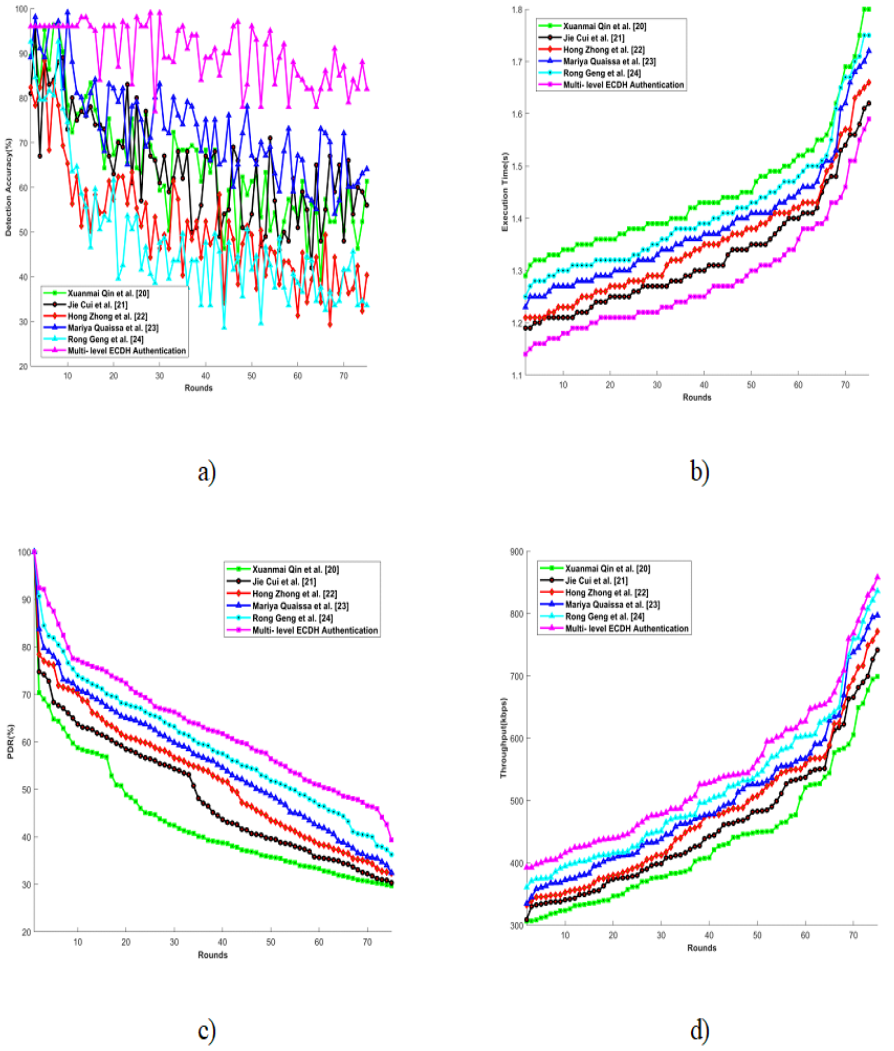
Figure 5. Comparative evaluation utilizing 50 nodes in the simulation area under Sybil attack, a) Detection Accuracy, b) Execution time, c) PDR, d) Throughput



(2020) , Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) are 32.689%, 20%, 70.3638%, 8.9670% and 50.9434%, respectively.

The execution time of the proposed multi-level ECDH authentication is analyzed with various comparative methods and the obtained results are demonstrated in the figure 6 b). Initially, the comparative methods utilized by Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020), Geng, *et al.,* (2018) and the proposed multi-level ECDH authentication attains the execution time of 1.29s, 1.19s, 1.21s, 1.23s, 1.25s and 1.14s, which is gradually increased with increase in the iteration levels. At the 10th iteration, the execution time obtained by the proposed multi-level ECDH authentication is 1.18s and the conventional methods utilized in the research article of Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) attains the execution time of 1.34s, 1.21s, 1.23s, 1.27s and 1.3s, respectively.

Figure 6. Comparative evaluation utilizing 100 nodes in simulation area under Sybil attack, a) Detection Accuracy, b) Execution time, c) PDR, d) Throughput



The evaluation of packet delivery ratio is also carried out under the sybil attack and the evaluation result is illustrated in the figure 6 c). The best PDR of 92.40% is achieved through proposed multi-level ECDH authentication at 1st iteration. The PDR achieved by the competent methods preferred by Qin & Li, (2020), Cui, *et al.,* (2020) , Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) are 70.333%, 74.7436%, 78.40%, 83.7846% and 90.6522%, respectively.

The throughput of the comparative methods is analyzed under sybil attack in figure 6 d). The throughput achieved by the comparative methods utilized in the research articles of Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020) , Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) at 75th iterations are 718.7905318Kbps, 761.9852941Kbps, 783.537079Kbps, 797.9455Kbps and 843.1769Kbps, respectively. At the 75th iteration, the throughput obtained by the proposed multi-level ECDH authentication is 867.8595Kbps.

4.5.2 Comparative Analysis Under Replay Attack:

The comparative evaluation of the proposed framework is done in network under the presence of the replay attacks with 50 and 100 nodes, respectively. The deep insight over the comparative evaluation of the framework is discussed below.

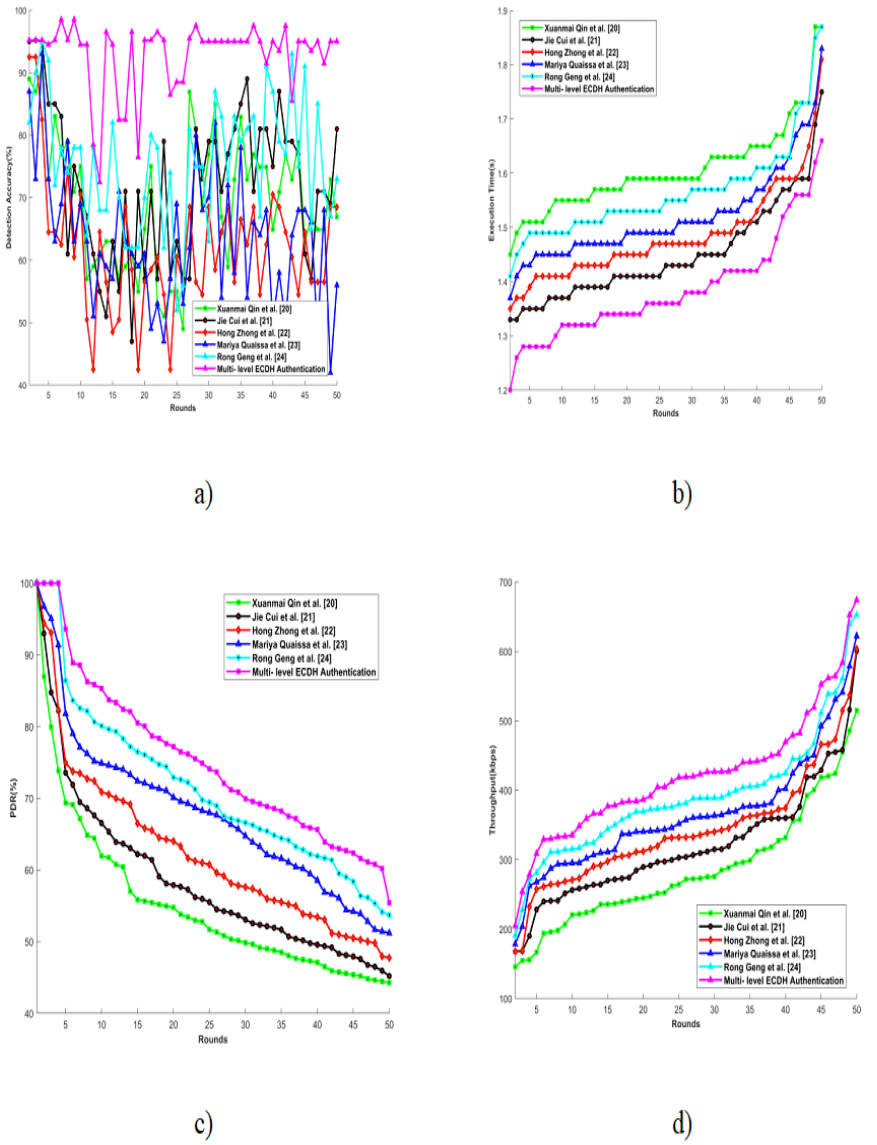
i) Comparative evaluation utilizing 50 nodes in the simulation area under replay attack: Figure 7 a) illustrates the comparative analysis in terms of the detection accuracy. At the 27rd iteration the detection accuracy observed in the proposed multi-level ECDH authentication model is 97.5%. The comparative methods utilized by Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) attain the detection accuracy of about 80.9%, 81%, 56.5%, 80% and 75%. It is clear that the proposed multi-level ECDH authentication attains high detection accuracy while comparing with the exiting techniques.

The comparative evaluation of the conventional methods with respect to the execution time is demonstrated in the figure 7 b). The execution time of 1.32s is achieved by the proposed multi-level ECDH authentication at the 10th iteration, which is lowest of all execution time when compared to the conventional methods used by Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) . The values obtained by the above mentioned comparative methods for the 10th iteration are 1.55s, 1.37s, 1.41s, 1.45s and 1.49s. Hence, it proves that the proposed multi-level ECDH authentication method demonstrate better performance in terms of execution time.

The comparative evaluation with respect to PDR of the conventional methods is illustrated in the figure 7 c). At the 5th iteration the PDR values obtained through proposed multi-level ECDH authentication method is 93.633%, which is greater than all the other comparative methods. The PDR values yield by the comparative methods presented by Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) are 69.3743%, 73.555%, 74.9484%, 81.8316% and 86.4204% respectively. The proposed multi-level ECDH authentication method exceeds all the other existing methods in terms of PDR.

Figure 7 d) illustrates the comparative evaluation of the competent methods with respect to the throughput. The maximum throughput of 689.1582Kbps is observed in the proposed multi-level ECDH authentication model at the 50th iteration. The throughput values obtained by the competent methods preferred by Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Rong geng (Geng, *et al.,* 2018) are 588.797Kbps 602.145Kbps, 621.9811Kbps, 648.6010Kbps and 666.2023Kbps respectively.

Figure 7. Comparative evaluation utilizing 50 nodes in the simulation area under replay attack, a) Detection Accuracy, b) Execution time, c) PDR, d) Throughput



ii) Comparative evaluation utilizing 100 nodes enclosed in simulation area under replay attack: In this section, comparative evaluation of the comparative methods under replay attack utilizing 100 nodes enclosed in simulation area is illustrated. Detection accuracy of comparative method is observed in the presence of replay attack and the result is demonstrated in the figure 8 a). The better detection accuracy is observed from the proposed security model at the 74th iteration level and the obtained detection accuracy is 98.35%. The detection accuracy values of the competent

methods presented by Qin & Li, (2020), Cui, *et al.,* (2020) , Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) are 75%, 68%, 76.2%, 81.5% and 77.85% respectively. Thus, the performance of the proposed multi-level ECDH authentication method is improved and the performance improvement is given as 31.133%, 44.632%, 29.0682%, 20.674% and 26.332% respectively with respect to the competent methods.

The execution time of the proposed model is analyzed with the comparative methods and the obtained results are demonstrated in the figure 8 b). At the 10^{th} level of iteration the comparative methods utilized by Qin & Li, (2020), Cui, *et al.,* (2020) , Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) and proposed multi-level ECDH authentication attains the execution time of 1.3956s, 1.2956s, 1.3156s, 1.3356s, 1.3556s and 1.2456s respectively. At the 10^{th} iteration the execution time obtained by the proposed multi-level ECDH authentication technique is 1.2856s and the competent methods preferred by Xuanmei Qin (Qin & Li, 2020), Jie Cui (Cui, *et al.,* 2020), Hong Zhong (Zhong, *et al.,* 2020), Mariya Ouaissa (Ouaissa, *et al.,* 2020) and Rong geng (Geng, *et al.,* 2018) methods attains the execution time of 1.4456s, 1.3156s, 1.3356s 1.3756s and 1.4056s respectively.

The evaluation of packet delivery ratio is also carried out under the replay attack and the evaluation result is illustrated in the Figure 8 c). The best PDR value of 89.55% is achieved by the proposed multi-level ECDH authentication technique at 2^{nd} iteration. The PDR achieved by the competent methods utilized by Qin & Li, (2020), Cui, *et al.,* (2020), Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) are 67.2421%, 72.7600%, 74.4178% 78.7184% and 87.3170% respectively.

The throughput of the comparative methods and the proposed methods are analyzed under replay attack. The results observed from the throughput analysis are illustrated in the Figure 8 d). The throughputs achieved by the comparative methods used by Qin & Li, (2020), Cui, *et al.,* (2020) , Zhong, *et al.,* (2020), Ouaissa, *et al.,* (2020) and Geng, *et al.,* (2018) at 75th iterations are 668.1928Kbps, 721.3832Kbps, 728.0241Kbps, 768.7296Kbps and 776.7791Kbps respectively. At the 75^{th} iteration the throughput obtained by the proposed security model is 812.7976 Kbps.

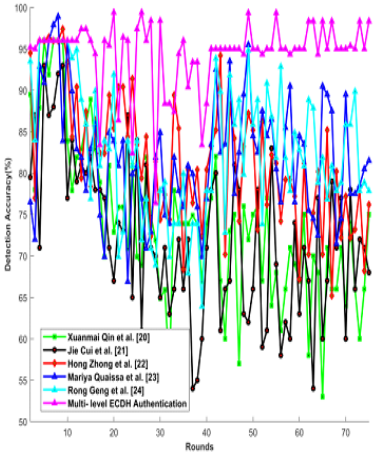
5. CONCLUSION

An advanced multi-layer ECDH authentication method is proposed in this research so as to empower privacy of the transmitted data in the VANET networks. In the proposed multi-layer ECDH based authentication model, the vehicles in the VANETs are exposed to the registration process. After the successful registration, the messages generated from the vehicles are subjected to multi-step ECDH-based authentication so as to ensure the exactness of the obtained message. Then, the authorization process is executed to confirm the safe and secure interactions between the vehicles in the SDVN. The detection accuracy, execution time, PDR and the throughput of the network while executing the proposed multi-level ECDH based authentication system under sybil attacks is 96%, 1.14s, 92.4086% and 867.8596Kbps, respectively, while for the metrics under the presence of the replay attacks is 98.35%, 1.2456s, 51.0951% and 812.7976Kbps, respectively. In future, AI-based security authentication protocol shall be designed, which would promote the attack resistance from various other dangerous vulnerabilities.

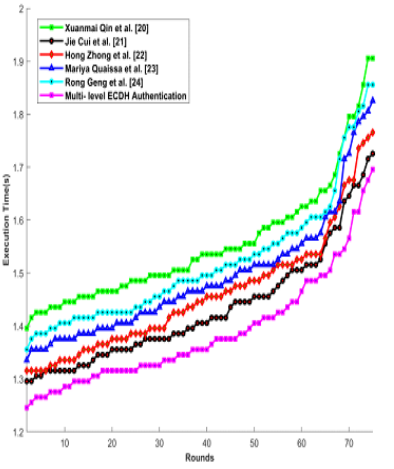
FUNDING AGENCY

Publisher has waived the Open Access publishing fee.

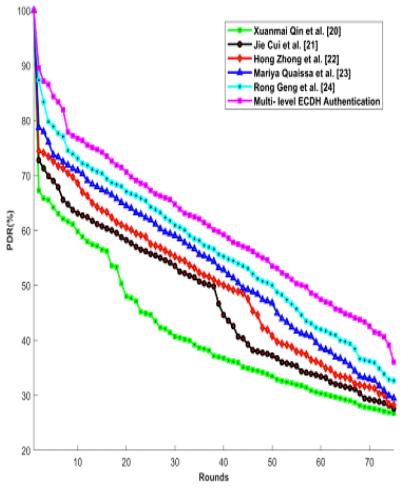
Figure 8. Comparative evaluation utilizing 100 nodes enclosed in the simulation area under replay attack, a) Detection Accuracy, b) Execution time, c) PDR, d) Throughput



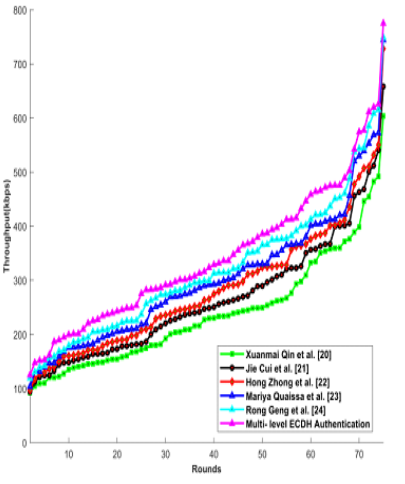
a)



b)



c)



d)

REFERENCES

Alouache, L., Maachaoui, M., & Chelouah, R. (2020). *Securing Hybrid SDN-based Geographic Routing Protocol using a Distributed Trust Model*. Academic Press.

Baskett, P. (2013). SDNAN: Software-Defined Networking in Ad-Hoc Networks of Smartphone's. *Proceedings of 10th IEEE Consumer Communications and Networking Conference (CCNC)*, 861–862.

Cui, J., Xu, W., Han, Y., Zhang, J., & Zhong, H. (2020). Secure mutual authentication with privacy preservation in vehicular ad hoc networks. *Vehicular Communications*, *21*, 100200.

Fung, C. J., & Zhu, Q. (2016). FACID: A trust-based collaborative decision framework for intrusion detection networks. *Ad Hoc Networks*, *53*, 17–31.

Geng, R., Wang, X., & Liu, J. (2018). A software defined networking-oriented security scheme for vehicle networks. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 58195–58203.

Jiang, H., Hua, L., & Wahab, L. (2020). SAES: A self-checking authentication scheme with higher efficiency and security for VANET. *Peer-to-Peer Networking and Applications*, 1–13.

Kim, D., Velasco, Y., Wang, W., Uma, R. N., Hussain, R., & Lee, S. (2017). A new comprehensive RSU installation strategy for cost-efficient VANET deployment. *IEEE Transactions on Vehicular Technology*, *66*, 4200–4211.

Kolandaisamy, R., Noor, R. M., Z'aba, M. R., Ahmedy, I., & Kolandaisamy, I. (2019). Adapted stream region for packet marking based on DDoS attack detection in vehicular ad hoc networks. *The Journal of Supercomputing*, *76*(8), 5948–5970.

Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. A., Panigrahi, B. K., & Veluvolu, K. C. (2020). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems*, 103352.

Manivannan, D., Moni, S. S., & Zeadally, S. (2020). Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc Networks (VANETs). *Vehicular Communications*, *1*(25), 100247.

Mendiboure, L., Chalouf, M. A., & Krief, F. (2018). Towards a block chain based SD-iov for applications authentication and trust management. *Proceedings of International Conference on Internet of Vehicles,* 265–277.

Mendiboure, L., Chalouf, M. A., & Krief, F. (2020). A scalable blockchain-based approach for authentication and access control in software defined vehicular networks. In *Proceedings of Computer Communications and Networks* (pp. 1–11). ICCCN.

Mendiboure, L., Chalouf, M. A., & Krief, F. (2020). Survey on block chain based applications in internet of vehicles. *Computers & Electrical Engineering*, *84*, 106646.

Mishra, A.K., Tripathy, A.K., Sinha, M. (2020). Customized Score-Based Security Threat Analysis in VANET. *Advances in Distributed Computing and Machine Learning,* 3-13.

Ouaissa, M., Houmer, M., & Ouaissa, M. (2020). An Enhanced Authentication Protocol based Group for Vehicular Communications over 5G Networks. *Proceedings of 3rd International Conference on Advanced Communication Technologies and Networking (CommNet),* 1-8.

Pal, H., & Narwal, B. (2021). A Novel Authentication Scheme for VANET with Anonymity. *Progress in Advanced Computing and Intelligent Engineering*, 267-276.

Parham, M., & Pouyan, A.A. (2020). An Effective Privacy-Aware Sybil Attack Detection Scheme for Secure Communication in Vehicular Ad Hoc Network. *Wireless Personal Communications*, *20*, 1-3.

Pournaghi, S. M., Zahednejad, B., Bayat, M., & Farjami, Y. (2018). NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET. *Computer Networks*, *134*, 78–92.

Qin, X., & Li, X. (2020). An ECC-based access control scheme with lightweight decryption and conditional authentication for data sharing in vehicular networks. *Soft Computing*, *24*(24), 18881–18891.

Raja, G., Anbalagan, S., Vijayaraghavan, G., Dhanasekaran, P., & Al-Otaibi, Y., & Bashir, A.K. (2020). Energy-Efficient End-to-End Security for Software Defined Vehicular Networks. *IEEE Transactions on Industrial Informatics*.

Rajput, U., Abbas, F., Eun, H., Hussain, R., & Oh, H. (2015). A two level privacy preserving pseudonymous authentication protocol for VANET. Proceedings of on Wireless and Mobile Computing, Networking and Communications, 643–650.

Xie, L., Ding, Y., Yang, H., & Wang, X. (2019). Block chain-based secure and trustworthy internet of things in SDN-enabled 5g-vanets. *IEEE Access, 7*, 656–666.

Zhong, H., Geng, Y., Cui, J., Xu, Y., & Liu, L. (2020). A weight-based conditional privacy-preserving authentication scheme in software-defined vehicular network. *Journal of Cloud Computing*, *9*(1), 1–13.

Zhou, H., Xu, W., Chen, J., & Wang, W. (2020). Evolutionary V2X technologies toward the internet of vehicles: Challenges and opportunities. *Proceedings of the IEEE*, *108*(2), 308–323.

Umesh K. Raut has received BE(CSE) degree from Govt. College of Engineering, Amravati and ME (Computer Engineering) degree form Govt. College of Engineering Pune (COEP). Currently, he is a Research Scholar in department of Computer Science Engineering at Oriental University, Indore (MP). His areas of interests are Computer Networks, Wireless sensor Network, Network Security.

L. K. Vishwamitra is working as a Professor in Computer Science Engineering at Oriental University, Indore (MP). His area of interests are Digital Image Processing, Artificial Intelligence and Soft Computing.