Enhancing The Vehicular Public Key Infrastructure to Develop Privacy-Preserving Authentication Scheme for VANET By Using PCM And MSS Scheme

[1]Jyothi N and [2]Sujatha Terdal
[1,2] Department of Computer Science and Engineering, P.D.A College of Engineering, Gulbarga, Karnataka, India.
[1]jyothi.patil6@gmail.com, [2]sujatha.terdal@gmail.com

Correspondence should be addressed to Jyothi N : jyothi.patil6@gmail.com

Article Info
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi : https://doi.org/10.53759/7669/jmc202404097
Received 31 March 2024; Revised from 12 July 2024; Accepted 31 July 2024.
Available online 05 October 2024

Abstract – This article proposes a security-based authentication as well as efficient certificate management approach for VANET to detect fraudulent nodes with better precision, less latency and overhead. The primary purpose of the developed system is to establish effectual and heftiness of VANET security that lead to the stability of overall network. VANETs are composed of vehicles and Road Side Units (RSUs) assisting with network management and the vehicles connect with one another and RSUs to furnish roadside information and safety solutions. Security is an essential factor in VANETs because the confidentiality of humans (passengers) is paramount; hence, Vehicular Public Key Infrastructure (VPKI) is utilised to offer authentication and safety services in VANETs. The developed structure provides an encrypted VANET transmission infrastructure by utilising the concepts of Merkle Signature Scheme (MSS) and Pseudo-code Certificate Management (PCM) to minimise overhead for communication and latency while ensuring entity authenticity. Messages are authenticated by sender, encoded with a vehicular public key distributed by a PCM-MSS and decrypted by the destination, resulting in every transmission including a certification from a reliable authority. During that verification, the transmitter and receiver of message's authentication and validation is accomplished. Simulation findings show that the proposed approach improves the reliability of identifying hostile nodes and PDR while reducing authentication delays and overhead.

Keywords – VANETs, RSUs, Pseudo-Code Certificate Management (PCM), Merkle Signature Scheme (MSS), Vehicular Public Key Infrastructure (VPKI).

I. INTRODUCTION

VANET has arisen in recent years as a result of advancements in wireless communications and networking technologies, thereby improving traffic security as well as effectiveness. Every vehicle in a VANET possesses a wireless communication equipment called an On-Board Unit (OBU) is employed for Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications [1, 2]. By exploiting the wireless communication technique, an attacker is able to obtain authority over the communication channels and customise, eliminate, or duplicate communications. As a result, attacks like as, alteration, impersonation, replay and person in the middle attacks constitute severe dangers to VANETs. These possibilities may result in congestion in traffic or accidents, hence communication authentication is an essential necessity in VANETs [3, 4]. Furthermore, security of the vehicle's information has to be attained, because leaking of their identities may resulting in major concerns for drivers, as malevolent entities are track their messages and travel routes for crimes. However, absolute privacy preservation isn't ideal for VANETs, because malicious vehicles ought to be tracked and penalised in the case of any inappropriate behaviour [5, 6].

Several Public Key Infrastructure (PKI)-based methods of authentication [7] and [8] have been developed to address concerns regarding privacy and security in VANETs. These methods are inefficient because vehicles have to maintain an extensive amount of private key pairs and certificates, which are subsequently transmitted with messages. To alleviate certificate management in PKI based authentication methods, numerous privacy preserving identity based method of authentication have been presented [9-11]. These authentication systems operate on bilinear combinations and in spite of their high computational expenses, two new efficient authentication schemes have been presented in [12, 13]. For enhancing the efficacy of these systems, they developed identity-based signatures instead of bilinear pairings. However, these techniques are insufficiently quick when there's a significant number of communications in the service zone of a RSU. The hub decodes the packets using the shared key and transfers the combined set towards the objective **Fig 1**.

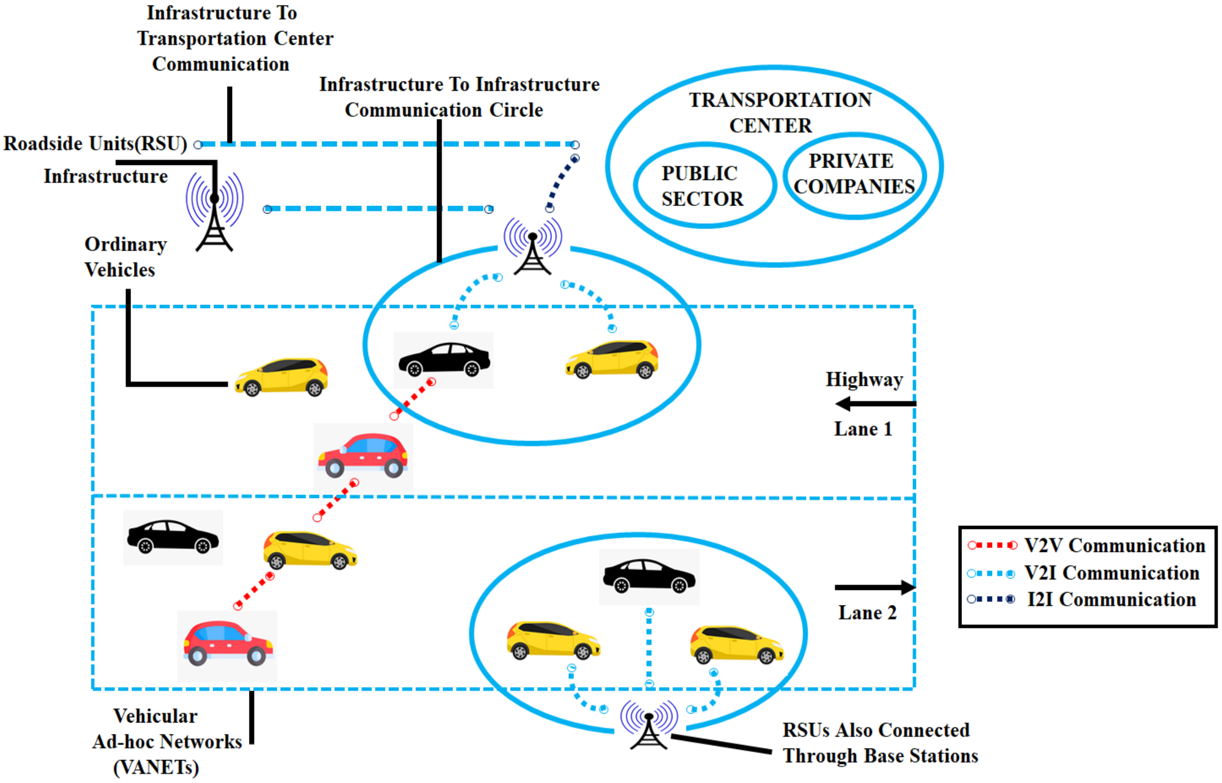

Infrastructure To Transportation Center Communication
Infrastructure To Infrastructure Communication Circle
TRANSPORTATION CENTER
PUBLIC SECTOR
PRIVATE COMPANIES
Roadside Units(RSU)
Infrastructure
Ordinary Vehicles
Highway
Lane 1
Lane 2
V2V Communication
V2I Communication
I2I Communication
Vehicular Ad-hoc Networks (VANETs)
RSUs Also Connected Through Base Stations

Fig 1. Architecture of VANET.

A VANET is susceptible to various security threats since informations are transmitted over a channel that is not encrypted, allowing attackers to observe, eliminate packets from network causing in interruption. A hacker is try to change the data sent via messages, counterfeit messages, or interrupt transmission [14]. Furthermore, an attacker is able to tune in on network communications and utilise the information gathered for malevolent factors. An attacker may intentionally manipulate traffic signals to cause road traffic jams and accidents [15]. If a hacker discovers the authentic identify of a vehicle, it could interfere with network by sending fraudulent messages. As a result, verifying the actual identity and authentication of the vehicle is a crucial safety desire for a VANET. It facilitates in determining if the received message originated from the network's authorised vehicle or not, and it safeguards the individual's privacy throughout the authentication process [16].

A catastrophic scenario is possible when a vehicle sends fraudulent messages with the goal to maximise individual benefit. Message authenticity is essential in VANETs and every vehicle has to verify obtained messages [17, 18]. Vehicles with less computational capability, on the other hand, necessity to finish authentication in a particular duration as the no. of incoming messages rises over time [19]. Furthermore, a VANET has to satisfy authentication (e.g., non-repudiation, integrity, authentication) and privacy criteria (e.g. location privacy, identity privacy) to allow for the network to function efficiently.

Problem Statement

In general, VANET security is a predominant consideration owing to their open nature and dynamic, that exposes them to several security attacks. One of the primary challenges is ensuring the confidentiality, integrity, and availability of communication among vehicles and infrastructure components while maintaining user privacy. Existing methodologies often focus on addressing specific security issues such as message authentication, secure vehicle-to-vehicle communication, secure key management, and privacy preservation.

Contribution of the Work

The present research provides an effective Pseudo-code Certificate Management (PCM) approach that works in combination with the Merkle Signature approach (MSS) conditional privacy preserving authenticity strategy to enable authentication of vehicle and data authentication in VANETs. The primary contributions of the designed system are as follows:

- The PCM-MSS technique uses a pseudonym-based authentication method to authenticate a vehicle's actual identification. The authentication method aids in speedy vehicle authentication while a vehicle moves from one network to another.
- A Merkle Signature Scheme (MSS) is employed to offer secure message authentication without the need for a vehicle's actual identity.
- The PCM-MSS technique enables conditional privacy, indicating the actual identification of a threatening vehicle. As a result, a pseudonym is transmitted alongside a message signed using the Merkle signature, thereby helping to guarantee non repudiation.
- The safety proof demonstrates that the developed technique assures both secrecy and unforgeability.
- Finally, the proposed architecture outperforms existing VANET methods in terms of communication and computational overheads as demonstrated by simulations.

The structure of the paper is as follows: Related works are provided in Section 2. A thorough explanation of the Secure VANET environment with a PCM-MSS based authentication system is given in Section 3. Results and discussion are presented in Section 4. The research is concluded in Section 5.

II. RELATED WORKS

Several authentication approaches have been developed by researchers to accomplish scalability, security preservation and quick computation in V2I and V2G VANET configuration.

A robust hierarchical authenticating scheme for VANET has been presented in [20]. It considerably reduces calculation costs compared to other approaches, but, the security flaws make this system unsuitable for practical deployment. In addition, it face several significant drawbacks, particularly in the realms of security and privacy.

A VANET authentication mechanism that emphasises security, confidentiality and efficiency have proposed in [21]. This approach offers an excellent combination of security and efficiency. Nevertheless, it often fail to adequately protect identity and location privacy, exposing vehicles to tracking and surveillance.

A secure authentication system using group signatures for VANETs with the goal to deliver an enhanced anonymous authentication service for vehicles is presented in [22]. The proposed approach effectively balances efficiency and security as evidenced by both performance and security. However, it has high computational and communication overhead due to complex cryptographic operations.

An innovative authentication protocol based on temporary pseudonyms and bilinear pairings have proposed in [23]. Furthermore, a possible authentication system is able to prevent a third party from tracking the vehicle. However, the communication overhead is high, due to complex latency issues.

An effective and secure identity based authentication system utilized to improve the security of vehicle consumers is presented in [24]. This presented method helps to revoke the pseudonym and enable the users robust privacy protection efficiently. Nonetheless, pseudonyms cannot be distinguished from one another because they are all in aligned with the RSU clock.

A conditional privacy preserving authentication with signature technique for V2V communication is developed in [25]. This technique supports batch signature verification that enables numerous signatures to be validated efficiently and simultaneously. However, signature verification is delayed by a single bilinear pairing function.

A conditional privacy preserving authentication method with a double insurance that supports batch evaluation for VANETs which is developed in elliptic curves based cyclic groups is preseneted in [26]. The developed technique not only resists traditional attacks, but also have the ability to resolve the security issues produced by channel attack. However, the developed technique has a greater computational expenditures during the signature validation stage.

A privacy preserving communication scheme for VANET that fulfils the demands for contextual and content privacy have proposed in. This technique is also impermeable to several kinds of threats such as impersonation, replay, man-in-the-middle and modification threats. Nevertheless, the overhead has increased due to insufficient accumulated storage.

A privacy preserving and lightweight V2I authentication technique presented in. With the information of the subtracted RSUs, fast authentication is attained between the vehicle and each RSU on its route. However, overhead is continue to grow as the number of RSUs increases.

Thus, the PCM-MSS addresses these challenges by employing pseudonym-based authentication, which mitigates the risk of security attacks and enhances privacy through frequent pseudonym changes that protect both identity and location information. Additionally, the multi-signature scheme ensures that messages are authenticated by multiple entities, enhancing security, while cooperative management reduces overhead and improves efficiency, facilitating more scalable and timely communication in the network.

III. PROPOSED SYSTEM DESCRIPTION

The proposed framework provides an authenticated VANET communication infrastructure by utilising the concepts of PCM and MSS to minimize the communication overhead and latency while maintaining entity authentication. **Fig 2** depicts the proposed architecture; CA allocates the Certificate Revocation Lists (CRL) for RSUs, while the RSUs fail to deliver it to the vehicles.

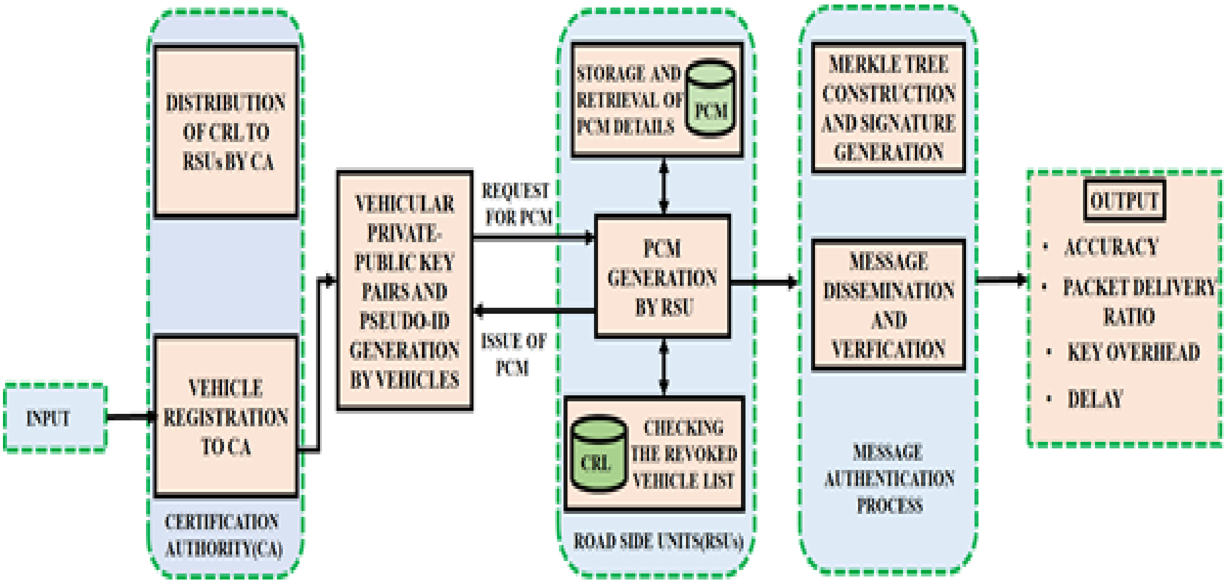

DISTRIBUTION OF CRL TO RSUs BY CA
VEHICLE REGISTRATION TO CA
INPUT
CERTIFICATION AUTHORITY(CA)
VEHICULAR PRIVATE-PUBLIC KEY PAIRS AND PSEUDO-ID GENERATION BY VEHICLES
REQUEST FOR PCM
ISSUE OF PCM
STORAGE AND RETRIEVAL OF PCM DETAILS
PCM
PCM GENERATION BY RSU
CHECKING THE REVOKED VEHICLE LIST
CRL
ROAD SIDE UNITS(RSUs)
MERKLE TREE CONSTRUCTION AND SIGNATURE GENERATION
MESSAGE DISSEMINATION AND VERFICATION
MESSAGE AUTHENTICATION PROCESS
OUTPUT
ACCURACY
PACKET DELIVERY RATIO
KEY OVERHEAD
DELAY

Fig 2. Secure VANET Environment Using PCM-MSS Based Authentication Scheme.

The proposed framework provides an authenticated VANET communication infrastructure by utilising the concepts of PCM and MSS to minimize the communication overhead and latency while maintaining entity authentication. **Fig 2** depicts the proposed architecture; CA allocates the CRL for RSUs, while the RSUs fail to deliver it to the vehicles. The vehicles seek a pseudo code certificate from the RSU via a beacon signal and this query comprises of some vehicular public and private pairs of keys produced by vehicle for certification from RSU that is required for subsequent message. Employing these secret keys, the sender vehicle constructs a Merkle Tree to produce a root node public token. After obtaining request from vehicles, RSU is going to produce a pseudo code certificate to enable communication among the verified vehicles.

Certification Authority (CA)
The use of a certification authority in VANET security helps prevent various attacks, such as impersonation, data tampering, and unauthorized access. It ensures that vehicles can trust the identities and public key information of other network entities, enhancing the overall security and reliability of the VANET.

Distribution CRL to RLU
In VANETs, the CA needs to distribute CRLs to Roadside Units (RSUs) to ensure that revoked certificates are properly recognized and trusted by the vehicles and other entities in the network.

Vehicle Registration to CA
Registering vehicles with the CA allows for the verification of their identities. The CA can authenticate the identity of each vehicle and ensure that it is a legitimate participant in the VANET. This helps prevent unauthorized or malicious entities from accessing the network.

Vehicular Private-Public Key Pairs and Vehicle Pseudo-Id Generation
The vehicles utilize private-public key pairs and generate pseudo-IDs to enhance security and privacy.

Vehicular Private-Public Key Pairs
The private key is kept confidential and is used for signing digital messages and decrypting encrypted information. It should be securely managed to prevent unauthorized access. The public key is used by other vehicles or infrastructure components to verify digital signatures generated by the private key. The public key can be freely shared and is not kept secret.

Pseudo-Id Generation by Vehicles
To protect privacy in VANETs, vehicles generate pseudo-IDs. A pseudo-ID is a temporary identifier that conceals the vehicle's real identity and provides anonymity. It is used for communications within the network to prevent the tracking or identification of specific vehicles.

Involved Processes of Road Side Unit (RSUs)
RSUs act as infrastructure components that provide connectivity, services and security mechanisms to vehicles within the network.

Storage and Retrieval of Pseudo-code Certificate Management (PCM) Details

The RSU maintains a secure database for storing PCM details. Each entry in the database contains information such as pseudonym, certificate, vehicle ID and timestamps.

PCM Generation by RSU

PCM generation facilitates the authentication of vehicles within the VANET. By issuing certificates, the RSU or trusted authorities can verify the authenticity and identity of vehicles contributing in the system.

Checking the Revoked Vehicle List

Checking the revoked vehicle list is a crucial component of VANET security, helping to maintain the trustworthiness and integrity of network communications by identifying and mitigating potential security threats posed by compromised vehicles.

Message Authentication Process

Signature Generation and Merkle Tree Construction

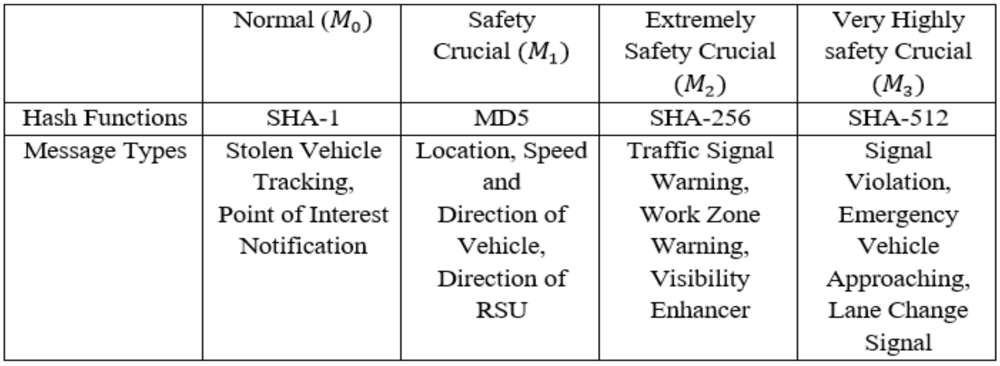
- A merkle tree is a hierarchical data structure that effectively verifies the integrity of enormous databases by hashing each of the data blocks and forming a tree structure of hash values. Merkle trees are frequently used in VANET security for expressing the integrity of message sets or data blocks that are transmitted across the network.
- Message signature generation is the process of generating digital signatures with cryptographic methods to verify the authenticity and origin of messages transmitted through the VANET.

Message Dissemination and Verification

Message dissemination and verification are crucial processes in VANET security to ensure the timely and secure exchange of information among vehicles and infrastructure components. After that the process of message dissemination and verification, the vehicle information efficiently authenticated with improved results regarding accuracy, PDR, key overhead and delay.

Messages have been prioritised as Normal ($M0$), Safety crucial ($M1$), extremely safety crucial ($M2$), or very highly safety crucial ($M3$), as per **Table 1**. The transmitter sends the message combined with an authenticated pathway established by Merkle tree and attached with certification. The vehicle in receiver side is capable of reassembling the MSS utilising an authentication pathway to assure non repudiation.

Table 1. Categorization Of Message Type



	Normal (M_0)	Safety Crucial (M_1)	Extremely Safety Crucial (M_2)	Very Highly safety Crucial (M_3)
Hash Functions	SHA-1	MD5	SHA-256	SHA-512
Message Types	Stolen Vehicle Tracking, Point of Interest Notification	Location, Speed and Direction of Vehicle, Direction of RSU	Traffic Signal Warning, Work Zone Warning, Visibility Enhancer	Signal Violation, Emergency Vehicle Approaching, Lane Change Signal

IV. SECURITY MECHANISMS FOR VANETs

Step 1: *CA Registration*

Each vehicle that require to get involved in VANET has to register with CA, which provides a vehicular public and private key pair ($Kr_u - Ku_v$) to each proper vehicle with a valid vehicle ID (V_{ID}). Vehicle is going to produce 4 vehicular private-public key pairs ($P_{u0}P_{r0}, P_{u1}P_{r1}, P_{u2}P_{r2}$ *and* $P_{u3}P_{r3}$) using the proposed method. The corresponding keys are used for subsequent interaction by vehicle following endorsement from RSU. **Table 1** shows VANET messages (M_0, M_1, M_2 *and* M_3) with varying priorities, necessitating the application of four keys.

Step 2: *Generation of Beacon Frame and Pseudo ID*

Pseudo ID (P_{ID}) protects user confidentiality while preventing hackers from following vehicles. To generate a Vehicle ID (V_{ID}), fraudulent ID, with the hashing of V_{ID} as shown in Equation 1. The vehicle signs employing its vehicular private key (Kr_u) issued by CA and transmitted into RSU via beacon signal. While RSU becomes a beacon framing signal request from vehicle, it validates the signature with the vehicle's key (public (Ku_v)) supplied through the CA.

$$P_{ID} = Sigkr_u \oplus h(V_{ID}) \tag{1}$$

PCM is requested by the vehicle through a beacon signal sent to the RSU. A signal that includes the vehicle's V_{ID} and P_{ID}, four vehicular public-private key pairs $(P_{u0}P_{r0}, P_{u1}P_{r1}, P_{u2}P_{r2}\ and\ P_{u3}P_{r3})$ for message categories $(M_0, M_1, M_2\ and\ M_3)$, the root node key (PR_u) produced according to the Merkle Tree notion (step 4) and the hashing consider of the components.

$$\boldsymbol{pack} = [V_{ID}, P_{ID}, P_{u0}P_{r0}, P_{u1}P_{r1}, P_{u2}P_{r2}, P_{u3}P_{r3}, PR_u]$$

$$\boldsymbol{beaconframe} = [pack||h(pack)] \tag{2}$$

After obtaining the beacon frame, the RSU confirms with CRL to determine if vehicle has been forfeited or not. If V_{ID} is not terminated, RSU tracks vehicle's information and the PID given by it. When the P_{ID} has been utilised by another vehicle, the RSU fails to notify PCM. RSU is going to deliver a beacon notification to the vehicle requesting a new P_{ID} and other parameters.

Step 3: *RSU based Certificate issue*

The modified CRL is accessible by an enormous amount of vehicles, however there are also many with revoked certificates. Excessive CRL exchange could contribute to network congestion. To reduce distribution costs, CRL listings are restricted to RSUs instead of vehicles. After obtaining the beacon from the vehicle, the RSU sends PCM to vehicle, as demonstrated in **Fig 3**.

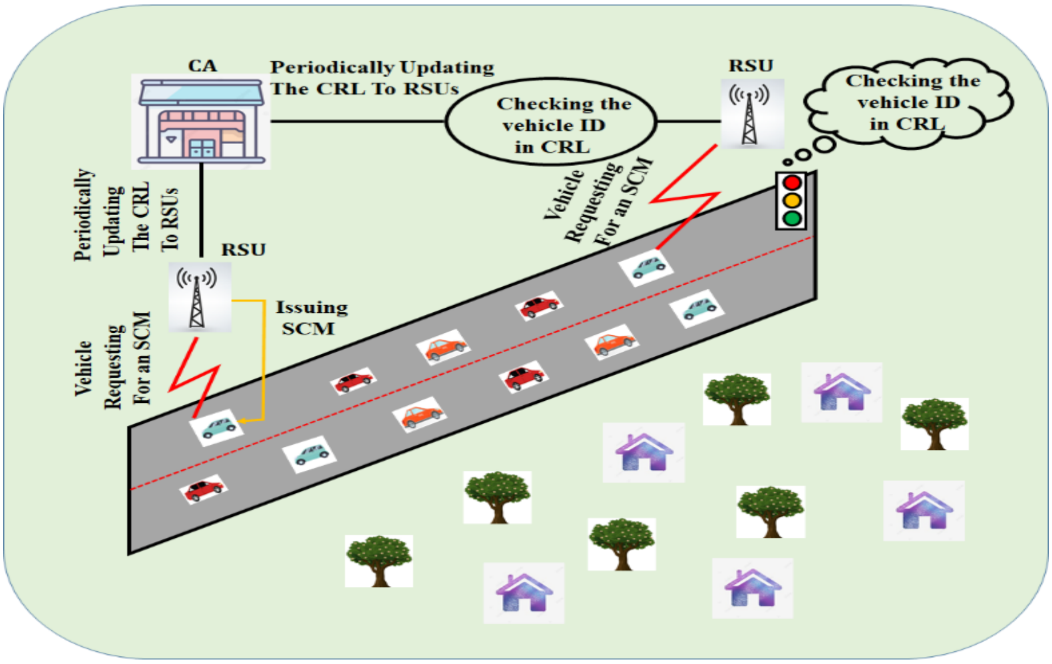

CA
Periodically Updating The CRL To RSUs
Checking the vehicle ID in CRL
RSU
Checking the vehicle ID in CRL
Periodically Updating The CRL To RSUs
Vehicle Requesting For an SCM
RSU
Issuing SCM
Vehicle Requesting For an SCM

Fig 3. Issue and Request of a PCM.

Each vehicle that desires to be involved in communication requires have a PCM, which is being obtained by the relevant RSUs for vehicles within their range. Equations 3 and 4 illustrate the structure of the PCM packets as well as the certificate format and **Table 2** lists multiple key PCM fields.

Table 2. Categorization of Message Type

Fields
Certificate Number (CN)
Time of PCM (T_{IS})
ID of the issuing RSU ((RSU_{ID})
Algorithm Identifier (A_{ID})
Vehicular Public Keys issued by RSU ($P_{u0}, P_{u1}, P_{u2}, P_{u3}$)
Signed contents using vehicular private key of RSU (Pr_{RSU})

$$PCM_{pack} = [CN||RSU_{ID}||T_{IS}||A_{ID}||P_{u0}, P_{u1}, P_{u2}, P_{u3}] \tag{3}$$

$$PCM_{cert} = [PCM_{pack}||Sig_{Pr_{RSU}}(PCM_{pack})] \tag{4}$$

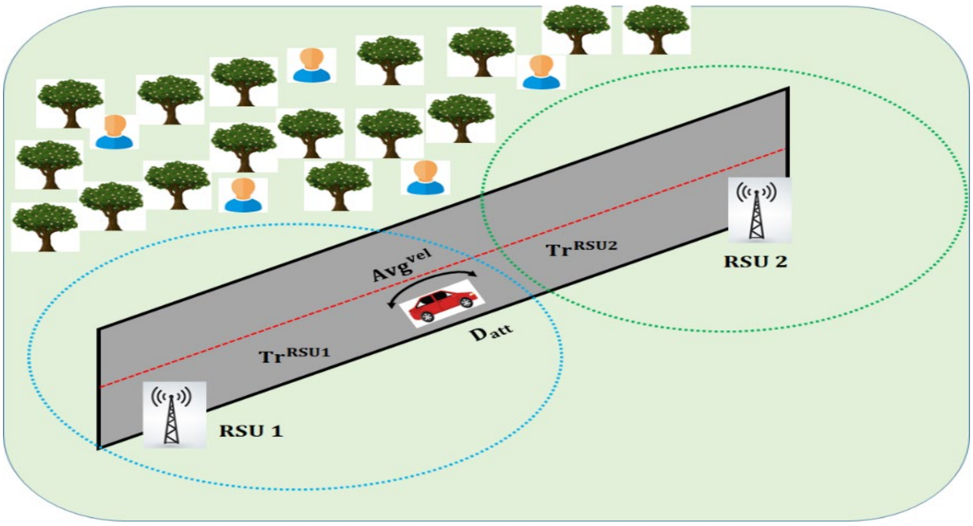


Fig 4. Calculating The Validity of a PCM.

The PCM is reactivated when two communications with identical priority are scheduled to be broadcast or when the PCM's validity ends. For instance, following broadcasting an M1 message, assuming the vehicle desires to broadcast another M1 message, it ought to apply for an additional PCM. When the vehicle fails to transmit any messages, the PCM expires following a specified time, which is established in equation 5. The reliability of PCM (VPCM), as indicated in **Fig 4**, is to be determined by the following features:

- Distance among two RSUs (D_{datt}).
- Average speed of a vehicle (Avg_{speed}).
- Transmission range of an RSU (Tr_{RSU}).
- This factor guarantees the certificate isn't revoked when the vehicle reaches the following RSU with a substantial likelihood (Δt).

$$V_{PCM} = \frac{D_{datt}+Tr_{RSU}}{Avg_{speed}} + \Delta_t \tag{5}$$

Step 4: *MSS Development*

MSS construction generates a Root Node Public Key (PR_u) for secure identity authentication. Assume a tree with nodes in factors of two, with every branch representing a distinct importance for categorised broadcast messages. The messages are processed employing multiple hash algorithms based on their criticality to create a Merkle tree. To transmit a message, the sender calculates the Merkle tree and obtains a PR_u. Merkle tree construction generates a Root Node Public Key (PR_u) for secure identity verification. Assume a tree with nodes in factors of two, with every branch representing a distinct importance for categorised broadcast messages. The messages are processed employing multiple hash algorithms based on their severity to create a merkle tree. To transmit a message, the sender calculates the Merkle tree and obtains a PR_u. The RSU requires vehicular public and private key pairs and a beacon frame to send all kinds of communications. Vehicular private public key pairs are refreshed following signing a specific type of message. The following phase is to determine the MSS that differs from the signature of message for entity verification.

Merkle Signatures include the authenticated message and validation pathway, they are needs to be delivered through a vehicle. Vehicular private key for authenticating this message is [Pr3], with the path to [PR_u] being [h_3, h_{23}]. The MS has been created as indicated in **Fig 5**. It is made up of a message signature (Sig_M) utilising the private key and an authorization *path (Auth_Path),* as seen in equation 7.

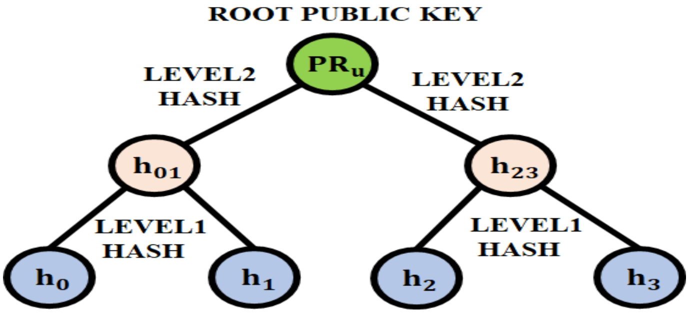


Fig 5. Construction of Merkle Tree.

Where,

$$h_0 = h(P_{u0}), h_1 = h(P_{u1})$$

$$h_2 = h(P_{u2}), h_3 = h(P_{u3})$$

then,

$$h_{01} = h(h_0||h_1)$$

$$h_{23} = h(h_2||h_3)$$

$$PR_u = h(h_{01}||h_{23})$$

$$Auth\_Path = [h_{01}||h_2] \tag{6}$$

$$MS = [Sig_M||\,Auth\_Path] \tag{7}$$

Step 5: *Verification by the Sender and Message Dissemination*

The developed solution does not require encryption for messages classified as highly or very extremely safety crucial. To broadcast y safety crucial messages, use a string (str) with Day, Date, Time and RSU_{ID} (as stated in equation 8). This is able to identify false information. The receiver is able to confirm the authenticity of the message by sending it to the specified RSU. When the communication is false, the RSU is able to report it to a CA and maintain the vehicle. A packet message ($MsgPack$) is made up of a message and MS (equation 9), whereas a message frame ($MsgFrame$) is made up of a string, its hash the information inside of the message packet, the authorization path, and the PCM certificate (equation 10).

$$str = [Day||Date||Time||RSU_{ID}] \tag{8}$$

$$Msg_{Pack} = [Msg||MS] \tag{9}$$

$$Msg_{Frame} = [str||h(str)||Msg_{Pack}||h\ (\mathrm{Auth_{Path}})||] \tag{10}$$

Thus, the proposed technology enables secure communication while reducing communication overhead. Because the CRL is moved to RSUs, time spent by the vehicle checking for revoked users is no longer required. The use of a one-time signature mechanism increases security when issuing a pseudo code certificate.

V. RESULTS AND DISCUSSION

To emulate the proposed strategy, analyse and compare it to different approaches, NS-2 software application is implemented. The NS-2 simulator is suitable software with outstanding performance for computational calculations that has been introduced as a network modelling solution. **Table 3** shows the modelling parameters and proposed configurations.

Table 3. Simulations Variables

Parameters	Values
$Number\ of\ vehicles$	72
$Simulation\ time$	$50\ s$
$Simulation\ area\ size$	$2500\ in\ 750\ m^2$
$Transmission\ range$	$250, 300, 350, 400\ m$
$Speed\ of\ vehicles$	$0\ to\ 20\ km/h$
α	0.6
β	0.4
τ	$Greater\ than\ or\ equal\ to$ 0.6
$Initial\ value\ of\ the\ direct\ trust\ degr$	0.2
$Number\ of\ malicious$	6,8,12,18,24,30

Performance Matrices

Accuracy of Detection

The amount of harmful nodes recognised properly while routing compared to the entire amount of malevolent nodes in VANET.

Packet Delivery Ratio (PDR)

The packets rates is obtained effectively by the destination via an encrypted path to total messages transmitted.

Delay

The period of time between a packets being transmitted by the source and receiving it at the destination.

Key Overhead

The number of activities required to produce a key and carry out encryption-related tasks in order to deliver and receive a data packet.

Accuracy Detection Calculation

The formula for calculating the accuracy detection in VANETs is given below:

$$Accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)} \tag{11}$$

Where, True Positives (TP) = Number of vehicles correctly detected as present, True Negatives (TN) = Number of vehicles correctly detected as not present, Total Number of Observations = TP + TN + False Negatives (FN) + False Positives (FP).

Changing Numbers of Malicious Vehicle

The simulation results are compared with the proposed scheme based on various benchmarks, including the Security Mechanism Clustering and Key Distribution (SCKD) scheme, Secure and Privacy-Preserving Navigation (VSPN) and Trust-Based Authentication Technique (TBAT) scheme are shown in **Figs 6, 7**, **8** and **9**. In addition, which is illustrates amount of malevolent nodes varies with packet delivery rate, detection accuracy, delay and key overhead. The detection accuracy as the number of hostile vehicles rises is depicted in **Fig 6**. All approaches' detection accuracy decreases as the amount of malevolent nodes rises. However, the PCM-MSS's prediction accuracy is higher than other approaches due to its more successful trust estimate mechanism In addition to trust between vehicles, which encompasses direct and indirect trust, trust between vehicles and RSUs, which encompasses both historical and segment trust, the impact is significant because there are two levels of trust.

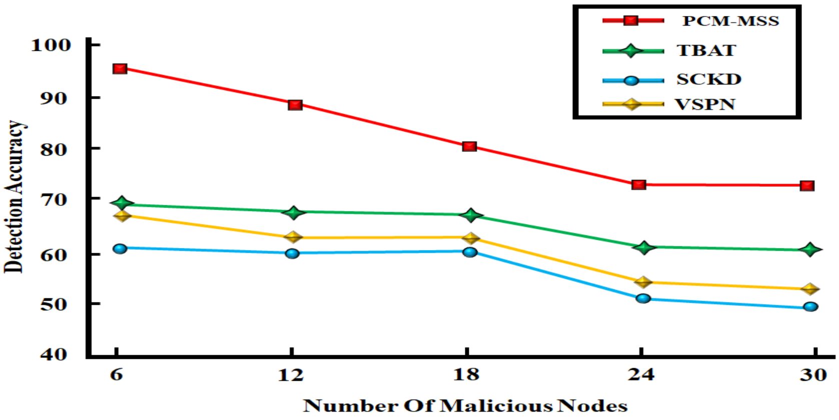


Fig 6. Accuracy Detection Vs No. Of Malicious Nodes.

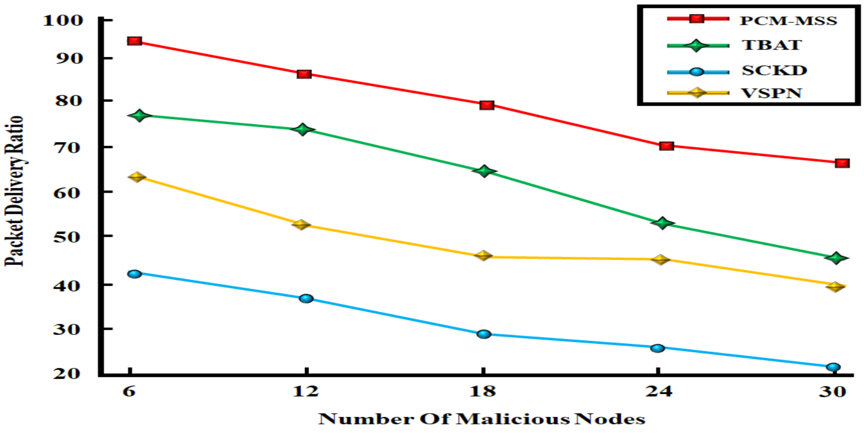


Fig 7. PDR vs No.Of Malicious Nodes.

Analysing the interaction between PDR and hostile nodes in VANETs offers important insights about the security and resilience of the network infrastructure. One important performance indicator that shows the dependability and effectiveness of data transmission inside the VANET is PDR, which is calculated as the ratio of successfully received data packets to the total number of transmitted packets. System managers can find out how resilient the network is to malicious assaults and how well it transports the data by measuring the PDR in relation to the number of malicious nodes in the network. The PDR increases as the number of malevolent vehicles increases as seen in **Fig 7**. The no. of packets that are eliminated in the path and erased generally increases with the no. of malevolent vehicles, which lowers the PDR. Furthermore, the certification-based authentication approach excludes the higher no. of fraudulent nodes, since the authentication of nodes has to be recognised. As a result, the PDR in PCM-MSS is greater than in other techniques.

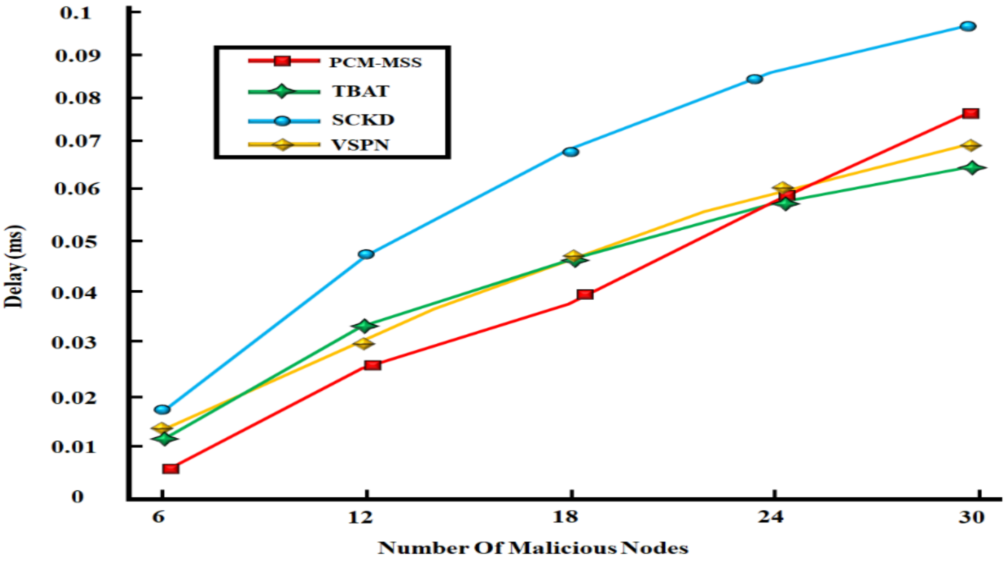


Fig 8. Delay (ms) vs No.Of Malicious Nodes.

In **Fig 8**, while the number of malicious nodes increases, the time taken to calculate authentication and trust rises, resulting in latency. In addition to reducing the number of computations required for trust estimate, the PCM-MSS's reduced detection latency for fraudulent nodes also results in a significantly shorter generation time and associated cryptographic operations. The PCM-MSS has a reduced latency as a result compared to other techniques.

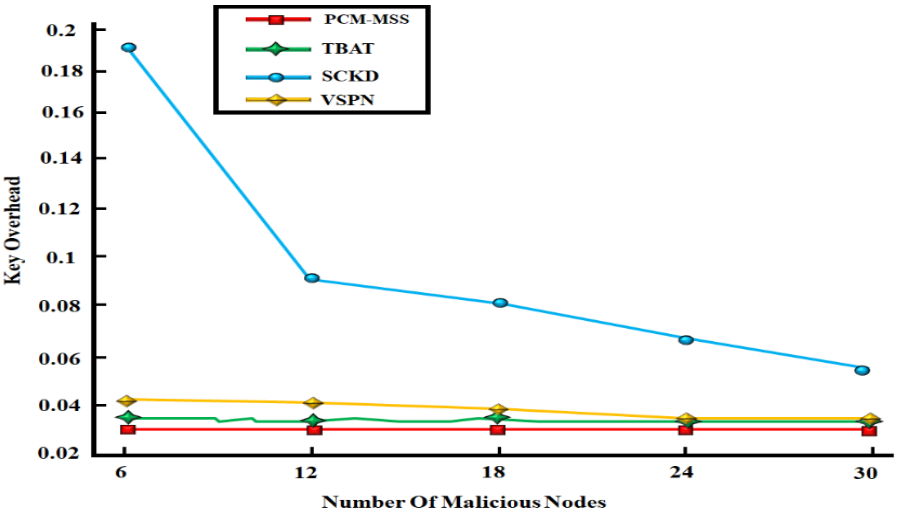


Fig 9. Key Overhead Vs No. of Malicious Nodes.

Analysing the key overhead as a function of the number of malicious nodes in a VANET offers a number of crucial technical benefits for comprehending the security and effectiveness of the network. As key management protects the confidentiality, integrity, and validity of data transferred between vehicles and infrastructure, it is a vital component of VANET communication security. The significant overhead increases as the number of malevolent vehicles increases, as seen in **Fig 9.** Considering the PCM-MSS and TBAT techniques lack a complex key generation procedure or associated cryptography activities, they have minimal overhead.

Variable Transmission Range

The simulation results are compared with the proposed scheme based on various benchmarks, including the TBAT scheme, SCKD scheme and VSPN and are shown in **Figs 10, 11, 12** and **13**. In addition, which is illustrates transmission range variable with detection accuracy, packet delivery rate, delay and key overhead.

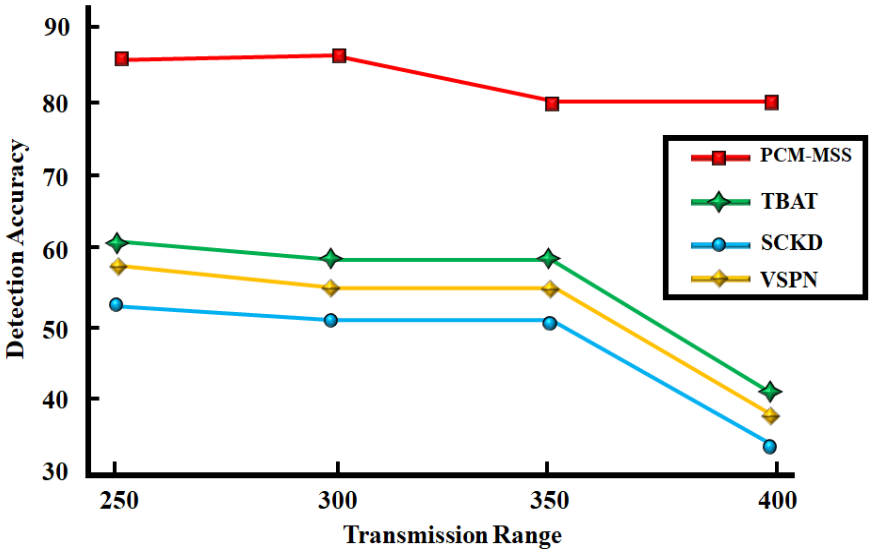


Fig 10. Accuracy Detection vs Transmission Range.

The accuracy of detection as the broadcast range improves is depicted in **Fig 10**. Considering its trust estimation technique is more precise than that of other approaches, the PCM-MSS has a better detection accuracy. Furthermore, the PCM-MSS mechanism is adaptable in that it constantly monitors network performance and modifies its parameters to preserve the appropriate ratio of transmission range to accuracy detection. By optimising trade-offs to ensure dependable and effective vehicle monitoring and communication, this adaptive optimisation guarantees that the mechanism can adjust to variations in the VANET environment, such as shifts in vehicle density or the entrance of new malicious nodes.

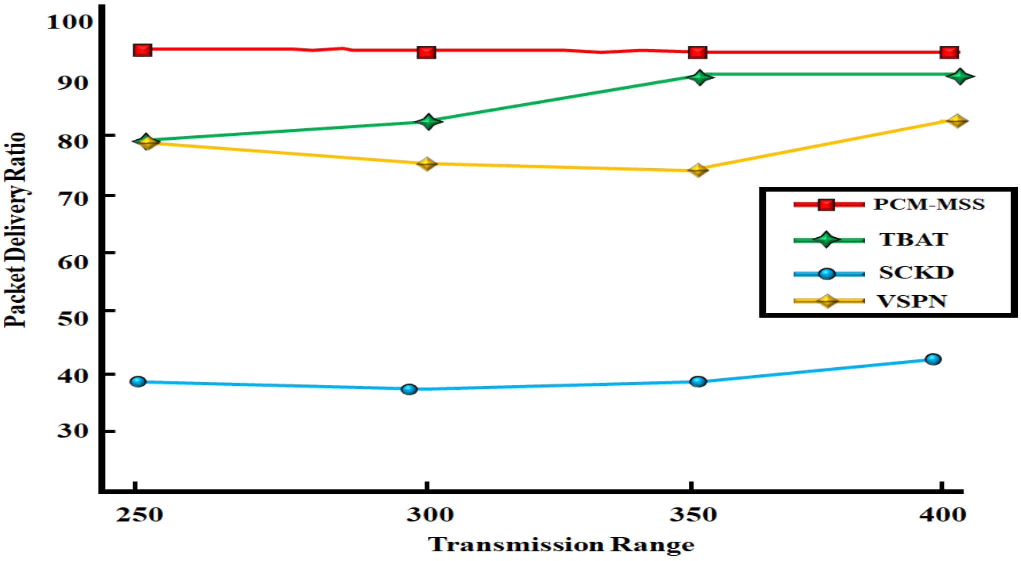


Fig 11. PDR vs Transmission Range.

The PDR as the transmission range expands is displayed in **Fig 11**. Less packets are discarded or deleted in the PCM-MSS which has greater effects on node selection and trust calculations during routing. As the transmission range increases, the coverage area of the network also expands, allowing vehicles to communicate over longer distances. This can be beneficial in terms of extending the reach of the network and enabling greater connectivity between vehicles. By adaptively managing the trade-off between PDR and transmission range, the PCM-MSS mechanism can maintain reliable and efficient communication within the VANET, ensuring that vehicles can effectively exchange critical information and data while optimizing the utilization of network resources.

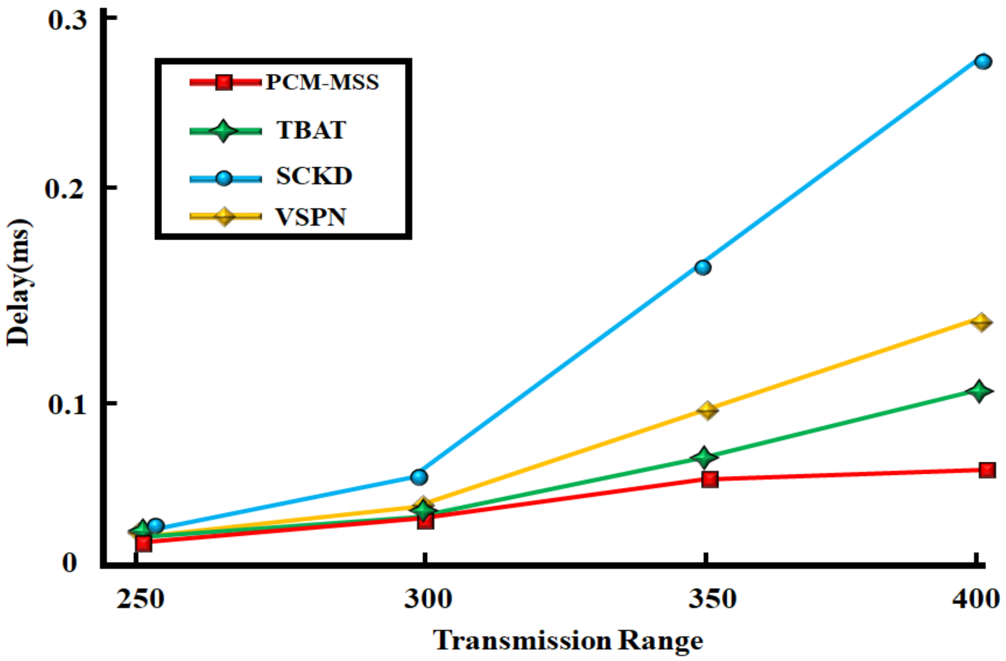


Fig 12. Delay (ms) vs Transmission Range.

The delay as the transmission range expands is depicted in **Fig 12**. Because there is a shorter detection delay, the PCM-MSS estimates trust faster, requires less complex creation of keys and cryptography processes and has a quicker authentication latency. Consequently, compared to other approaches, the proposed PCM-MSS strategy has a shorter delay. The PCM-MSS mechanism aims to manage the trade-off between delay and transmission range by dynamically adjusting the communication parameters based on the network conditions

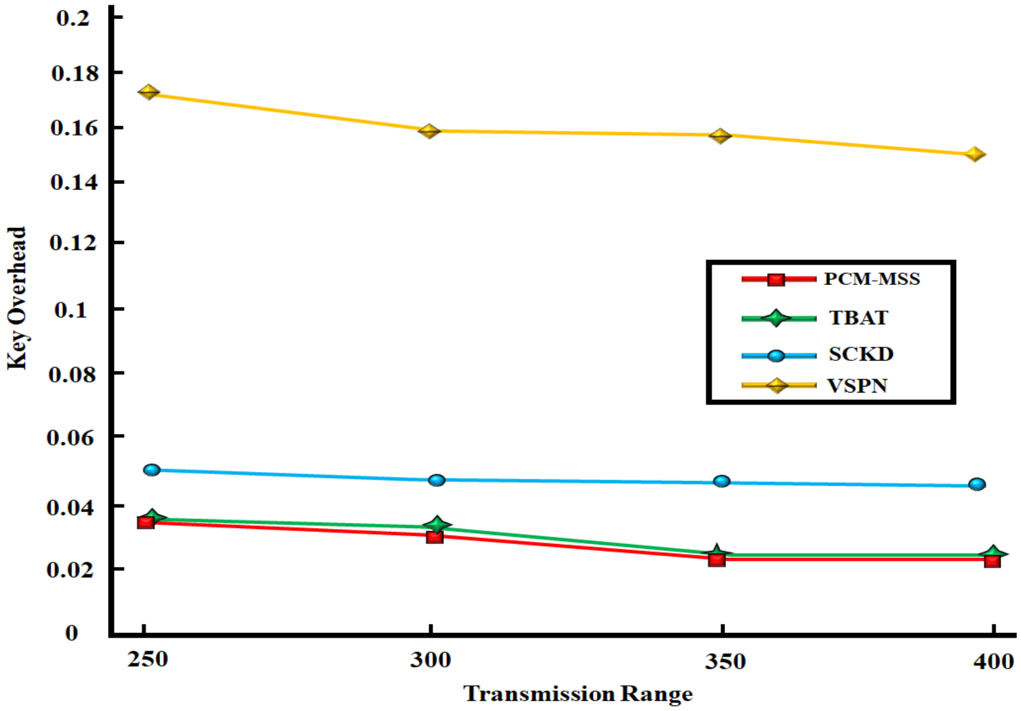


Fig 13. Key overhead vs Transmission Range.

It is evident from **Fig 13** that key overhead increases as the transmission's range increases. Because of the absence of complex key creation and cryptography procedures, the PCM-MSS and TBAT approaches have lower key overhead than the SCKD and VSPN approaches. Additionally, the PCM-MSS mechanism reduces the key overhead and maintain the desired level of security within the VANET.

VI. CONCLUSION

This paper proposes an effective certification management strategy and security-based authentication for VANET to identify fraudulent nodes more accurately with less overhead and delay. The VPKI is implemented in VANETs for providing authentication and safety features while privacy is crucial since human confidentiality is of utmost importance. The proposed topology uses the principles of PCM and MSS to decrease communication overhead and delay while maintaining entity authenticity, hence offering an encrypted VANET transmission infrastructure. Every transmission includes a certificate from a reputable organisation since messages are verified by the transmitter, encoded employing a vehicular public key that is disseminated by a PCM-MSS, and decoded by the recipient. Authentication is completed and the sender and recipient of the message are verified during that process. The results of the simulation demonstrate that the proposed approach reduces overhead and authentication latency while increasing the accuracy of identifying hostile nodes and PDR.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests.

References

[1]. T. Nandy et al., "A Secure, Privacy-Preserving, and Lightweight Authentication Scheme for VANETs," IEEE Sensors Journal, vol. 21, no. 18, pp. 20998–21011, Sep. 2021, doi: 10.1109/jsen.2021.3097172.

[2]. M. Umar, S. H. Islam, K. Mahmood, S. Ahmed, Z. Ghaffar, and M. A. Saleem, "Provable Secure Identity-Based Anonymous and Privacy-Preserving Inter-Vehicular Authentication Protocol for VANETS Using PUF," IEEE Transactions on Vehicular Technology, vol. 70, no. 11, pp. 12158–12167, Nov. 2021, doi: 10.1109/tvt.2021.3118892.

[3]. C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar, "A Novel Lightweight Authentication Protocol for Emergency Vehicle Avoidance in VANETs," IEEE Internet of Things Journal, vol. 8, no. 18, pp. 14248–14257, Sep. 2021, doi: 10.1109/jiot.2021.3068268.

[4]. Y. Wang, H. Zhong, Y. Xu, J. Cui, and G. Wu, "Enhanced Security Identity-Based Privacy-Preserving Authentication Scheme Supporting Revocation for VANETs," IEEE Systems Journal, vol. 14, no. 4, pp. 5373–5383, Dec. 2020, doi: 10.1109/jsyst.2020.2977670.

[5]. R. I. Abdelfatah, N. M. Abdal-Ghafour, and M. E. Nasr, "Secure VANET Authentication Protocol (SVAP) Using Chebyshev Chaotic Maps for Emergency Conditions," IEEE Access, vol. 10, pp. 1096–1115, 2022, doi: 10.1109/access.2021.3137877.

[6]. S. A. Soleymani, S. Goudarzi, M. H. Anisi, M. Zareei, A. H. Abdullah, and N. Kama, "A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET," Vehicular Communications, vol. 29, p. 100335, Jun. 2021, doi: 10.1016/j.vehcom.2021.100335.

[7]. L. Wei, J. Cui, H. Zhong, Y. Xu, and L. Liu, "Proven Secure Tree-Based Authenticated Key Agreement for Securing V2V and V2I Communications in VANETs," IEEE Transactions on Mobile Computing, vol. 21, no. 9, pp. 3280–3297, Sep. 2022, doi: 10.1109/tmc.2021.3056712.

[8]. H. Liu, H. Wang, and H. Gu, "HPBS: A Hybrid Proxy Based Authentication Scheme in VANETs," IEEE Access, vol. 8, pp. 161655–161667, 2020, doi: 10.1109/access.2020.3021408.

[9]. J. S. Alshudukhi, Z. G. Al-Mekhlafi, and B. A. Mohammed, "A Lightweight Authentication With Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography," IEEE Access, vol. 9, pp. 15633–15642, 2021, doi: 10.1109/access.2021.3053043.

[10]. S. Khan, A. Raza, and S. Oun Hwang, "An Enhanced Privacy Preserving, Secure and Efficient Authentication Protocol for VANET," Computers, Materials &amp; Continua, vol. 71, no. 2, pp. 3703–3719, 2022, doi: 10.32604/cmc.2022.023476.

[11]. Z. Qiao et al., "An Anonymous and Efficient Certificate-Based Identity Authentication Protocol for VANET," IEEE Internet of Things Journal, vol. 11, no. 7, pp. 11232–11245, Apr. 2024, doi: 10.1109/jiot.2023.3330580.

[12]. I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs," Vehicular Communications, vol. 22, p. 100228, Apr. 2020, doi: 10.1016/j.vehcom.2019.100228.

[13]. P. Wang and Y. Liu, "SEMA: Secure and Efficient Message Authentication Protocol for VANETs," IEEE Systems Journal, vol. 15, no. 1, pp. 846–855, Mar. 2021, doi: 10.1109/jsyst.2021.3051435.

[14]. A. Aghabagherloo, M. Delavar, J. Mohajeri, M. Salmasizadeh, and B. Preneel, "An Efficient and Physically Secure Privacy-Preserving Authentication Scheme for Vehicular Ad-hoc NETworks (VANETs)," IEEE Access, vol. 10, pp. 93831–93844, 2022, doi: 10.1109/access.2022.3203580.

[15]. M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Secure Communication in a Vehicular Ad Hoc Network," Symmetry, vol. 12, no. 10, p. 1687, Oct. 2020, doi: 10.3390/sym12101687.

[16]. S. A. Alfadhli, S. Lu, A. Fatani, H. Al-Fedhly, and M. Ince, "SD2PA: a fully safe driving and privacy-preserving authentication scheme for VANETs," Human-centric Computing and Information Sciences, vol. 10, no. 1, Sep. 2020, doi: 10.1186/s13673-020-00241-x.

[17]. B. Samra and S. Fouzi, "New efficient certificateless scheme-based conditional privacy preservation authentication for applications in VANET," Vehicular Communications, vol. 34, p. 100414, Apr. 2022, doi: 10.1016/j.vehcom.2021.100414.

[18]. D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)," Vehicular Communications, vol. 25, p. 100247, Oct. 2020, doi: 10.1016/j.vehcom.2020.100247.

[19]. X. Li, Y. Han, J. Gao, and J. Niu, "Secure hierarchical authentication protocol in VANET," IET Information Security, vol. 14, no. 1, pp. 99–110, Jan. 2020, doi: 10.1049/iet-ifs.2019.0249.

[20]. Y. Jiang, S. Ge, and X. Shen, “AAAS: An Anonymous Authentication Scheme Based on Group Signature in VANETs,” IEEE Access, vol. 8, pp. 98986–98998, 2020, doi: 10.1109/access.2020.2997840.

[21]. J. Zhang, Q. Zhang, X. Lu, and Y. Gan, “A Novel Privacy-Preserving Authentication Protocol Using Bilinear Pairings for the VANET Environment,” Wireless Communications and Mobile Computing, vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/6692568.

[22]. J. Qi and T. Gao, “A Privacy-Preserving Authentication and Pseudonym Revocation Scheme for VANETs,” IEEE Access, vol. 8, pp. 177693–177707, 2020, doi: 10.1109/access.2020.3027718.

[23]. I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, “An Efficient and Provably Secure ECC-Based Conditional Privacy-Preserving Authentication for Vehicle-to-Vehicle Communication in VANETs,” IEEE Transactions on Vehicular Technology, vol. 70, no. 2, pp. 1278–1291, Feb. 2021, doi: 10.1109/tvt.2021.3050399.

[24]. Xiong, W., Wang, R., Wang, Y., Zhou, F. and Luo, X., 2021. CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs. IEEE Transactions on Vehicular Technology, 70(4), pp.3456-3468.

[25]. M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, “VPPCS: VANET-Based Privacy-Preserving Communication Scheme,” IEEE Access, vol. 8, pp. 150914–150928, 2020, doi: 10.1109/access.2020.3017018.

[26]. S. Lv and Y. Liu, “PLVA: Privacy-Preserving and Lightweight V2I Authentication Protocol,” IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 6633–6639, Jul. 2022, doi: 10.1109/tits.2021.3059638.