I. J. Computer Network and Information Security, **2026, 2, 181-195**
Published Online on April 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2026.02.10

A Lightweight Framework Using Signcryption Based Key Agreement Scheme with Location Privacy for D2D Communications in 5G VANETs

Chinnam S. V. Maruthi Rao*
Department of Electronics and Communication Engineering of the Koneru Lakshmaiah Education Foundation, Aziznagar, Hyderabad, 500075, India
E-mail: maruthichinnam@gmail.com
ORCID iD: https://orcid.org/0000-0002-7510-2605
*Corresponding author

Rama Krishna Akella
Department of Electronics and Communication Engineering of the Koneru Lakshmaiah Education Foundation, Aziznagar, Hyderabad, 500075, India
E-mail: ramakrishna.a@kluniversity.in
ORCID iD: https://orcid.org/0009-0002-4730-3909

Received: 15 November 2025; Revised: 22 January 2026; Accepted: 25 February 2026; Published: 08 April 2026

Abstract: Device-to-Device (D2D) communications in 5G enabled vanet Networks offer significant advantages in terms of improved communication efficiency and reduced latency. However, ensuring secure and efficient key agreement among devices remains a critical challenge. In this study, we present a novel lightweight framework for D2D communications that addresses these concerns by employing a Signcryption-based key agreement scheme [1]. The proposed scheme is built on the foundation of Diffie-Hellman Hyper Elliptic Curve Cryptography and leverages two one-way cryptographic hash functions to enhance security. By integrating the signcryption technique, our framework achieves a seamless combination of encryption and signing [2], reducing computational overhead and conserving network resources in resource-constrained 5G-enabled devices. Furthermore, we prioritize user location privacy in our framework by employing advanced techniques, including the Chinese Remainder Theorem. This ensures that location information is protected and not exposed to unauthorized parties during D2D communication sessions. Through extensive simulations and performance evaluations using ns3, we demonstrate the effectiveness and efficiency of our proposed key agreement scheme for D2D communications in 5G enabled vanet Networks. The results show improved communication performance and reduced resource consumption, making our framework a promising solution for secure and efficient D2D interactions in the context of evolving 5G networks.

Index Terms: D2D, VANET, Signcryption, Key Agreement, 5G Networks, Security, Privacy.

1. Introduction

Vehicular Ad-Hoc Networks (VANETs) are a type of network that allows vehicles to communicate with each other and with roadside infrastructure. These networks are an essential part of the vision for future intelligent transportation systems (ITS). VANETs use wireless communication technologies such as Dedicated Short-Range Communication (DSRC) or Cellular-Vehicle-to-Everything (C-V2X) to enable vehicles to exchange information in real-time. Vehicles in a VANET communicate to share information about road conditions, traffic congestion, accidents, weather conditions, and other relevant data that helps drivers make informed decisions and improves overall road safety by enabling collision avoidance and warning systems. Vehicular Ad-Hoc Networks (VANETs) can be categorized into different types based on their applications, communication modes, and operational environments. Some most common types of VANETs are Vehicle-to-Vehicle (V2V), Vehicle-to-Network (V2N), Vehicle-to-Pedestrian (V2P), Vehicle-to-Infrastructure (V2I), Vehicle-to-Everything (V2X). The choice of VANET type depends on the application requirements, environmental conditions, and infrastructure availability in a particular deployment scenario. However, VANETs also face challenges such as ensuring robust security and privacy, managing network scalability, and addressing communication reliability in

diverse traffic conditions.

Security in Vehicular Ad-Hoc Networks (VANETs) is crucial due to the sensitive nature of the data exchanged and the potential impact of security breaches on road safety and operational efficiency. The key aspects and challenges of security in VANETs include Authentication and Access Control, Data Integrity, Privacy Preservation, Secure Communication, Trust Management, Resilience to Attacks, Secure Vehicle-to-Infrastructure (V2I) Communication, Update and Patch Management, Legal and Regulatory Frameworks. Overall, securing VANETs requires a comprehensive approach that integrates cryptographic techniques, secure protocols, trust management, privacy preservation, and resilience to attacks. Addressing these security challenges is crucial to realizing the full potential of VANETs in enhancing road safety and transportation efficiency.

Device to Device (D2D) Communication is a crucial technology in VANETs that allows the vehicles to communicate directly without any infrastructure like base station or access points in between and is used to enhance communication efficiency, connectivity and reliability. However, D2D can also be in connection with centralized network as is the case of V2X shown in Fig.1.

With the advent of technology and need for faster communication in high mobility networks, D2D in 5G VANETs leverages communication cost and computational cost bypassing the centralized network infrastructure by efficient spectrum utilization through Resource Reuse and localized data processing. D2D in 5G VANETs also support computation offloading and computational workload sharing for V2V interactions. However, the security concerns should be addressed to ensure confidentiality and integrity of data. Signcryption technique helps in ensuring the message authentication and prevents unauthorized modification by third party while maintaining the confidentiality. Secure Signcryption schemes like Ring, blockchain based, certificateless, conditional privacy preserving, multimode and quantum resistant signcryption are a work under research. Based on the existing studies and experimental works available it is suggested to secure the communication with a proper key agreement protocol that can mutually authenticate the vehicles and mitigate the possible attacks.

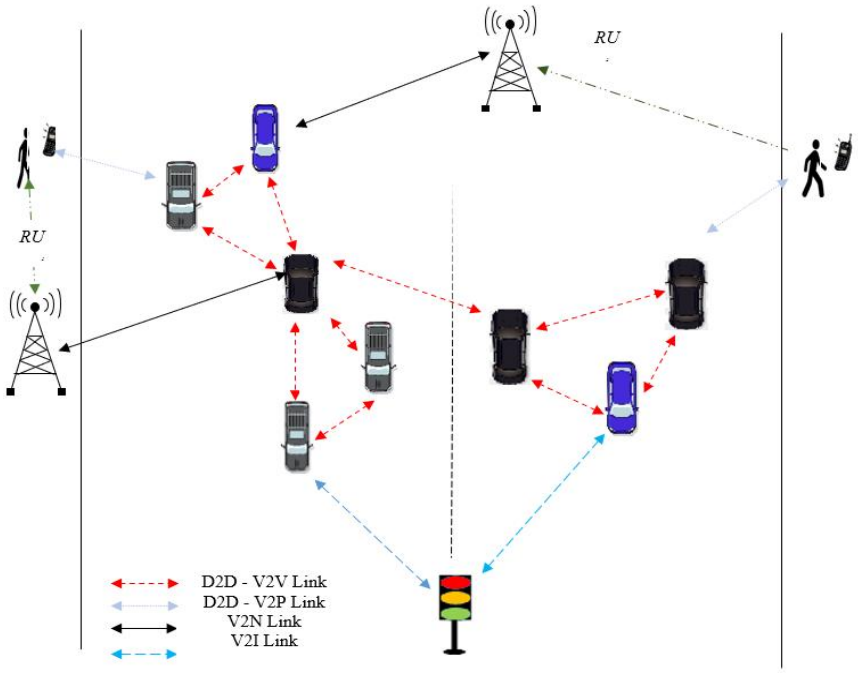

Fig.1. V2X Architecture

2. Research Motivation

The various types of VANETs and the security challenges for ensuring data integrity and confidentiality is discussed in the introduction. Existing works on addressing these challenges incur either high latency or lack forward secrecy or privacy location etc. Earlier works has also not addressed the trade-off between light weight crypto-algorithms and multi-attack resilience in a network. Also, it is observed that none of the research is based on D2D communication where information is shared quickly and securely. Signcryption technique addresses these challenges and is a best solution for securing the communication in VANETs. A comprehensive survey of the various existing key agreement schemes based on signcryption technique (mostly with elliptic curves [3]) for security implementation in VANETs is listed in Table 1. These techniques are mostly used with mutual authentication [4]. Majority of the work is done on certificateless Signcryption technique for different type of 5G VANETs. The simulation / Threat model, Random Oracle is proven to be good for evaluating signcryption schemes [5]. The main limitation of certificateless signcryption is when the key

generation center that holds the key to decrypt and sign is compromised. Also, this technique is based on ECC which is vulnerable as well as provides larger computational costs and delays due to its large key size. To avoid this, a certificate based signcryption is suggested that can use HECC. It is observed that there is no work currently available on certificate based Signcryption except for [6], where Gomathi et al., has implemented certificate based Signcryption on cluster based VANETs without D2D pairs and with a limited packet size of 512 bytes and limited to smaller network size.

Table 1. Comprehensive literature survey

Scheme	Year	Mechanism / Technology / Protocol	Simulation / Threat Model / Topology	Sim. Tool / Library	Network Support	D2D Support	Key Agreement Protocol	Advantage	Limitation
[5]	2013	Identity based Signcryption	Random Oracle Model	-	No	No	Authenticated Group Key	Optimal communication complexity, Authentication, Integrity & Confidentiality, Communication Efficiency and Computational Cost	Support for multiple recipients, Batch verification of signatures, Limited to small groups, Less secure to Collusion attacks
[6]	2024	Authentication & Trust based clustering	Guindy Kathipara Map OSM	Network Simulator with SUMO	5G enabled VANETs	Yes	Diffie Hellman Hyper Elliptic Curve Cryptography and Cryptographic Hash Functions	Increased Packet Delivery Ratio, Authentication & Integrity, Cluster based	System Complexity that increases latency, Scalability Issues, Security Trade-offs in dynamic environments, Less secure to Sybil and bad-mouthing attacks
[7]	2023	Unlinkable Signcryption	Multi-Receiver (USS - MR)	Network Simulator with SUMO	Multi-receiver VANETs	No	Elliptic Curve Cryptography and Chinese Reminder Theorem	Authentication, Integrity, Confidentiality, Conditional Privacy Preservation, Anonymity, Traceability, Revocability	Scale multiplication on ECC, Increased Computational & Communication Overhead, Reduced Reliability due to dynamic nature of VANETs, Less secure to Colluding & replay attacks
[8]	2023	Challenge Authentication Handshake	Random Oracle Model	MIRACL Library & PBC Library	VANETs	No	Key agreement based on Fuzzy Extractor and Schnorr Signature	Mutual Authentication, Forward Security, Dynamic Management	Vulnerability to insider attacks, Balance between Anonymity & Traceability, Less secure to Collusion and Sybil attacks
[9]	2020	Certificateless Key - Encapsulated Signcryption	Dolev-Yao	AVISPA	FANETs	Yes	Hyper Elliptic Curve Cryptography	Confidentiality, Unforgeability, Integrity, Computational Cost, Communication Efficiency	Resourced Constrained, Applicable only for FANETs, Less Secure to Forward Secrecy & Replay Attacks
[10]	2020	Group Signature	5G enabled VANET	MIRACL Library & PBC Library	5G enabled VANETs	Yes	Group Signature with a Pre Computed Lookup Table for modular exponentiation operation	Privacy Preservation, Reduced authentication overhead, Higher Service Capabilities, Anonymity, Robustness to network failures	Storage, Possible redundancy in local group signature, Increased dependency on infrastructure, Less secure to Man-In-The-Middle attacks
[11]	2021	Group Authentication	Chaotic Mapping in 5G	Scyther	5G VANETs	No	Chinese Reminder Theorem	Anonymity, Unlinkability, Reduced Computational & Communication overhead, Faster Authentication, Enhanced Privacy	Possible Single point of failure in group authentication, Vulnerable to Quantum Computing and Side-Channel Attacks, Privacy issues, Vulnerable to Insider attacks

[12]	2022	Provable security with single and batch signature verification	Random Oracle Model	Network Simulator with SUMO	5G VANETs	Yes	Elliptic Curve Cryptography and Chinese Reminder Theorem	No dependency on Infrastructure, Integrity, Confidentiality, Optimized bandwidth and faster Communication, Anonymity	Resource intensive mathematical operations, Decentralized communication, Key Revocation delays, Trust Issues between vehicles, Vulnerable to sybil attacks
[13]	2022	Certificateless Signcryption based on Elliptic Curve Digital Signature	Random Oracle Model	MIRACL Library	Internet of Vehicles in 5G	Yes	Elliptic Curve Digital Signature Cryptography	Confidentiality, Unforgeability, Forward Security, Anonymity	Pseudonym Management, Key Management overhead, Limited to single cipher text examination, Security assumptions
[14]	2021	Anonymous Certificateless Signcryption	Random Oracle Model	MIRACL Library	Internet of Vehicles in VANETs using 5G Cellular	No	Hyper Elliptic Curve Cryptography	Confidentiality, Unforgeability, Receiver Anonymity, Reduced Computational & Communication Costs	Need for Secure channel to share partial private keys, Need for Key Generation Centre, Vulnerable to MITM, DOS & Replay attacks
[15]	2023	Certificateless Authentication	Dolev-Yao	AVISPA	5G assisted vehicular N/W	Yes	Elliptic Curve Cryptography	Authenticity & Integrity, Confidentiality, Pseudonym Identity, Privacy	Computational Complexity, Key Revocation / update challenges, Trust issues, Latency in signcryption & key verification
[16]	2021	Light Weight D2D Authentication	3GPP 5G Network Scyther Tool with Burrows-Abadi-Needham Logic	Bouncy Castle v1.64 with Java SDK 13.0.1	5G Cellular	Yes	HMAC (Hash based Message Authentication Code) with Elliptic Curve Diffie-Hellman	Mutual Authentication, Traceability, Anonymity, Low Transmission Overhead & Computation Cost	Single Point of Failure of network, Trade-Off between Traceability & Privacy, Increased Computational overhead, Interoperability issues
[17]	2022	Trusted Blockchain based Signcryption	TB-SCDM using CRUD interface supplied by FISCO BCOS 2.0	FISCO BCOS 2.0	VANETs	No	Block Hash & Signcryption based on Schnorr (Provable Security)	Identity Authentication, Confidentiality, Unforgeability	High Computational & Storage requirements, Scalability issues, Latency, Blockchain forking and Consensus issues, Increased communication overhead
[18]	2016	ID-based Signcryption using bilinear pairing	Standard Model without Random Oracle Model		No	No	Computational Diffie-Hellman	Reduced Computational Cost, Confidentiality & Integrity, Unforgeability	Not effective when Confidentiality and authenticity are required together, Lack of forward secrecy, Over-Reliability on Trusted Authority
[19]	2022	HECC based IIOT Certificateless Signcryption	Real or Random Model with Dolev-Yao	AVISPA	IIOT (Low Speed VANET)	No	Hyper Elliptic Curve Cryptography	Mutual Authentication, Confidentiality, Integrity & Non-Repudiation, Reduced Communication Overhead	Key distribution and initial setup, Vulnerability to DOS attacks, Key Revocation and Management, Complex key management

It is observed that in certificateless Signcryption key computation time and authentication delay is high for most times with limited privacy. Also, existing protocols address only a subset of these problems but fails to have a comprehensive solution tailored for real-time 5G D2D VANET scenarios. This work SPARK, is a light weight framework based on certificate based signcryption with an enhanced key agreement that addresses the above problem and ensures mutual authentication, multi-attack resilience and location privacy and is optimized for real-time D2D communication in 5G D2D VANETs.

3. Proposed Work

Major efforts were put by the researchers to tackle the security and data processing issues in the 5G enabled D2D VANETs for secure communications. It was observed that majority of the flaws are because of the methodology adopted which resulted in high communication and processing costs due to modular exponentiation. As a result, these designs were not able to resist privileged insider attacks, impersonation and TA spoofing attacks thereby compromising privacy and anonymity. This in turn has resulted in security and performance imbalance. The main objective of this work is to create an efficient key agreement scheme based on signcryption and employs HECC and two one way cryptographic hash functions. HECC uses shorter key size compared to ECC (Elliptic Curve Cryptography) and results in lower computational head in a highly mobile and bandwidth constrained VANET environment (Eg. 160 bit ECC Key ≈ 80 bit HECC Key). Chinese Reminder Theorem is used to optimize the modular arithmetic operations involved in signature verification (reduced by ~40%) and hence reduces the computational cost and complexity. In this process, Chinese reminder theorem is used to secure the location privacy of the vehicle. The main contributions of this paper are as follows.

- We bring optimal scheme which is certificate based signcryption scheme for authentication and key agreement between and vehicle and RSU / TA. Here each vehicle is equipped with the signcryption module. The process includes

  (a) Certificate Issuance – by the TA
  (b) Signcryption Process – with message sent over the 5G network
  (c) Decryption and Verification - by the recipient

- We implement our proposed system using ns3 simulation tool and provide the performance analysis of our system with existing systems to show that the communication and computational costs are reduced.

The use of Certificate based Signcryption scheme guarantees data confidentiality, integrity and authenticity and the certificates generated are useful in preventing Man-in-the-Middle (MITM) and Replay attacks.

The work is compared with [11] and [16,17] that provide state of the art light weight and privacy aware key agreement mechanisms for VANET with 5G support and mostly addresses the critical security dimensions like mutual authentication, Forward Secrecy, resistance to DOS attacks etc. Other schemes fall outside the scope of this work and do not address location privacy, signcryption, light weight structure simultaneously which are core of this work and lack direct applicability to D2D based 5G VANETs. The basic notation and terminology used is given in Table 2.

Table 2. Notations/Terminology

Notation	Meaning
TA	Trusted Authority
RU	Road Side Unit
D	Vehicle
HEC	Hyper Elliptic Curve
D_{pk} & D_{psk}	Private and Public Keys of Vehicle
H_a& H_b	Hash Functions
Y_{pk}	Public Key of the TA
RU_i	Road Side Unit Identification
$Cert_{RU_i}$	Certificate for RU_i
D_n	Vehicle ID
Ω	Key received from RU_i
J	Divisor in HEC
φ & σ_i	Random number chosen from a set
SG_i	Signature generated
N_{once}	Time Stamp generated as Random or Pseudo Random number and used once
ϑ_{ds}	Session Key
ω_u	Registration Phase Secret Key

4. Implementation Methodology

The proposed architecture is comprised of three components: *TA*, *D* and *RU*. Each participant must first register with *TA* before being assigned to a practical activity. We assume that the *TA* is a fully trusted participant which may be a potential vulnerability as it introduces single point failure caused by DOS attacks and other potential risks of

impersonation, internal threats and location privacy. To address these, we used forward security where we refresh the session keys periodically and zero knowledge proof where the *TA* can issue the keys without the knowledge of its actual content enhancing privacy. Also, it was assured that *TA* doesn't generate all the keys but allows *D/RU* to generate their own private keys. *D* and *RU* are considered partially trusted. *D* is the most important component of the entire structure. When necessary, *RU* can access a specified *D* from anywhere, for example, to check on a large city's infrastructure, such as traffic surveillance and sidewalk monitoring, etc. *TA* has complete control over the transmission zone, vehicle validity, and external user data access. Similarly, the *TA* can be in charge of "Who has access to whom," and the entry of an unauthorized vehicle or user at any moment, as well as trajectory, waypoint, and data communication, is the exclusive responsibility of the *TA* related occurrence. Our proposed work consists of five steps

- Setup phase
- Registration Phase – *RU* & *D*
- Key Agreement Phase - Between *RU*, *D* & *TA*
- Update Phase – New Joining and Cancellation of Failed vehicles
- Location Privacy

- **Setup phase:** This Phase is initialized by the *TA* that creates Public and Private Keys. The Private Key, D_{pk} is selected by using HEC that considers a finite field F_g with $g > 1$ (we considered a genus 2) [20]. The divisor J of hyper elliptic curve (also called Jacobian of HEC) is the finite points sum that is given as $\Sigma_{pi \in HEC} m_i p_i$, here $m_i \in F_g$ and$\varphi, \sigma i \in [1,2,3,..(c-1)]$ [10]. The Public Key of TA (Y_{pk}) given as $\varphi.J$ is generated. Two hash functions H_a and H_b are chosen for signature generation and encryption key derivation respectively. To complete signcryption process using HEC, the public parameters are published for use by all the parties involved and is given as

$$K = [F_g, HEC, J, Y_{pk}, H_a, H_b] \tag{1}$$

- **Registration Phase –*RU* and *D*:** The registration of *RU* and *D* are handled by *TA* themselves. In the process of registering the *RSU*, the *TA* first allocates an ID for the *RU*, RU_i and computes its Private Key and Public Key as shown in equations (2) and (3) respectively.

$$RU_{pk} = \varphi.H_a(RU_i) mod\ c \tag{2}$$

$$RU_{psk} = RU_{pk}.J \tag{3}$$

The certificate for RU_i is calculated as (4)

$$cert_{RUi} = Y_{pk} + (RU_{pk}) H_a(RU_i || RU_{psk}) \tag{4}$$

To track the exact location of the vehicles ID_n, *TA* provides a secret key $\omega_u \in [1,2,3,...(c-1)]$ to the RU_i. Finally, *TA* will update memory of RU_i as$(RU_i, cert_i, RU_{pk}, RU_{psk})$. Once the registration of *RU* is completed, the *TA* will initiate the registration of vehicle asD_n. The Public and Private keys are computed in the similar way as for *RU* and in shown in equations (5) and (6).

$$D_{pk} = \varphi.H_a(D_n) mod\ c \tag{5}$$

$$D_{psk} = D_{pk}.J \tag{6}$$

The certificate for D_n is calculated as (7)

$$cert_{Di} = D_{psk} + (D_{pk}) H_a(D_n || D_{psk}) \tag{7}$$

Finally, *TA* will update memory of D_n as$(D_n, cert_{Di}, D_{pk}, D_{psk})$.

- **Key Agreement Phase - Between *RU*, *D* & *TA*:** When two vehicles, say, D_{ns} and D_{nr} wants to communicate, a key agreement should be available. For this purpose, we used a key agreement phase among *RU, D* & *TA*. Initially we generated a certificate for signature and transmitted the key from RU_i to D_{ns}. First a Public Key $\varepsilon_i = \sigma_i.J$ is generated and the corresponding Private key (α_i) is generated as $\varepsilon_i.RU_i.D_{psk}$. Then we encrypted the message from RU_i with a timestamp produced as Nonce (Δ_i) as $RU_{\alpha_i}(RU_i || Nonce_i)$. The certificate and corresponding signature are then generated as

$$Cert_{RUi2D} = cert_{Di} + H_b(message||RU_i||Nonce_i) \tag{8}$$

$$SG_i = \left(\frac{\sigma_i}{Cert_{RUi2D}+RU_{pk}} RU_i\right) mod\ c \tag{9}$$

The Signcrypted key from RU_i is sent to D_{nr} as

$$\Omega_1 = (SG_i, Cert_{RUi2D}, \Delta_i, \varepsilon_i, \alpha_i) \tag{10}$$

Once D_{nr} receives Ω_1 from the RU_i, its validity is checked by verifying the Time Stamp $Nonce_i$ after decryption and $Cert_{RUi2D}$ and signature are verified using the following conditions

$$Y_{pk} + (RU_{psk})H_a(D_{ns}||D_{psk}) = cert_{Di}.J \tag{11}$$

$$SG_i\left(D_{psk} + Cert_{RUi2D}.\varphi_i.J\right) = D_{ns}.\varepsilon_i.D_{pk} \tag{12}$$

If signature is valid, ε_i and SG_i are recalculated using equation (9) with RU_i replaced by D_{ns} and the later part multiplied by σ_i. The session key (ϑ_i) will updated as $\sigma_i\varepsilon_i$ in D_{ns}. The relation of Nonce with session key is obtained from

$$\Delta_i = RU_{\alpha_{ds}}(Nonce_{ns}||Nonce_{ns}) \tag{13}$$

The session shared with D_{ns} is

$$\vartheta_{ns} = H_b(message||D_{ns}||Nonce_{ns}||\vartheta_i) \tag{14}$$

and can be verified as

$$H\vartheta_{ns} = H_b(Nonce_i||\vartheta_i) \tag{15}$$

This key is sent as

$$\Omega_2 = (H\vartheta_{ns}, Nonce_{ns}, \varepsilon_i, D_{ns}, RU_{pk}, Cert_{RUi2D}) \tag{16}$$

to the *TA* through RU_i through Unsigncryption. The *TA* decrypts the key and verifies freshness of the $Nonce_{ns}$. The certificate of D_{ns} is verified using equation (11) and signature validation is done using (12). The certificate is computed as

$$SG_{TA} = Cert_{TA} + H_b(message||D_{nr}||Nonce_{TA}||TA) \tag{17}$$

The session key for *TA* is updated in the similar way as for RU_i and sends the key as

$$\Omega_3 = (H\vartheta_{TA}, Nonce_{TA}, \varepsilon_i, D_{nr}, RU_{pk}, SG_{TA}) \tag{18}$$

to D_{nr}. The D_{nr} then decrypts the key and checks the freshness of $Nonce_{TA}$ to send the data to RU_i. It then verifies the D_{ns} (source vehicle) certificate and signature through

$$Y_{pk} + Y_{nrpk}.H_a(TA||Y_{nrpk}) = cert_{nr}.J \tag{19}$$

$$SG_{nr}(Y_{nr} + Cert_{D2RUi}.J) = D_{nr}.\varepsilon_{nr}.D_{nrpk} \tag{20}$$

Once verified, the session key needs to be updated in a similar process as for *TA* and RU_i. The relation used is

$$\vartheta^*_{drTA} = H_b(message||D_{nr}||TA||Nonce_{nrTA}||\vartheta^*_{drTA}) \tag{21}$$

and verified as

$$H\vartheta^{*}_{drTA} = H_b(Nonce_{nrTA}||\vartheta^{*}_{drTA}) \tag{22}$$

The session key is sent as

$$\Omega_4 = (\Delta_{drTA}, H\vartheta^{*}_{drTA}) \tag{23}$$

to RU_i. Finally, when the RU_i receives Ω_4 and decrypted for checking the freshness of the *Nonce* using

$$(message||D_{ns}||RU_i||Nonce_{RUi2D}) = D_{\alpha}(\Delta_{RUi2D}) \tag{24}$$

It is observed that the freshness *Nonce* is new and calculates

$$H\vartheta^{**}_{RUi2D} = H_b(Nonce_{RUi2D}||\vartheta_{RUi2D}) \tag{25}$$

Then it checks the relation ϑ^{**}_{RUi2D} is true or false ($H\vartheta^{**}_{RUi2D} = H\vartheta^{*}_{RUiD}$). The following equivalence can be verified as well ($H\vartheta^{*}_{RUi2D} \doteq H\vartheta_{RUi2D}$).

- **Update Phase – New Joining and Cancellation of Failed vehicles:** In Vanet scenario, vehicles have a high mobility and will be either entering or leaving the network area. The procedure for adding or removing a vehicle is handled by the *TA*. Once a new vehicle enters into the network the *TA* identifies it as D_{new} and computes its private and public keys in the same way as registration and generation of certificates of vehicles as shown in equations (5) to (7) and are shown as below

$$D_{newpk} = \varphi.H_a(D_n) mod\ c \tag{26}$$

$$D_{newpsk} = D_{newpk}.J \tag{27}$$

The certificate for D_{new} is calculated just as for equation (7) and given as

$$cert_{Dnewi} = Y_{pk} + (D_{newpk})H_a(D_{new}||D_{newpsk}) \tag{28}$$

Finally, *TA* will update memory of D_{new} as $(D_{new}, cert_{Dnewi}, D_{newpk}, D_{newpsk})$. Similarly, when some of the vehicles are leaving the network, their information has to be removed from the memory.

$$D_{delete} = H_a(D_{delete}||D_{pskdelete}||TA) \tag{29}$$

The same remedy will be consider when a vehicle is compromised due to the attack by hackers or when the data has to be safeguarded in the *RU*.

- **Location Privacy:** In case of failure of a vehicle, D_{ns} or D_{nr} due to loss of energy or external issues, it will be replaced by RU_i. Prior to that the real location GC_D of $D_{nsfail} or\ D_{nrfail}$ will be by RU_i. To provide privacy of the location, we need to know Latitude (μ), longitude (θ), and altitude (τ). For providing privacy to GC_{st} the following steps of Chinese Remainder Theorem [21] is used.

Calculate R_i for each ω_i using $\mathcal{R}_i = \omega_u/\omega_i$ (30)

Define Congruence with $\mathcal{R}_i\mathbb{N}_i \equiv 1\ mod\ \omega_i$ (31)

$$\mho_i = \mathcal{R}_i\mathbb{N}_i \tag{32}$$

$$h = \sum \mho_i \tag{33}$$

$$\mathrm{F} = h * \eta \tag{34}$$

Here η indicates $Enc(\mu||\theta||\tau)$ that suggests it is an encrypted value.

After the above process, final value of F will be shared to the RU_i. In the registration phase, secret key ω_u is given to RU_i, that will calculate η using equationF $mod\ \omega_i$. While decrypting η with the help of *TA* public key,RU_i can retrieve the coordinates of the vehicles.

5. Simulation Results

The Proposed design is implemented with NS 3.26. Here we have chosen 5G enabled LTE package in NS3 to create the 5G network and enabled D2D communication features over the LTE package. The simulation parameters and the various libraries used in the design are mentioned in Table 3. To bring security into NS3 we linked Open SSL and libHEC packages. For realistic vehicular mobility simulation with utmost accuracy SUMO is the best choice when integrated with network simulator to generate the required topology. SUMO allows for Online and Offline Communication for real-time road traffic scenarios [22]. The system is implemented on Intel ® Core ™ i7-7700 @ 3.6GHz with 32 GB RAM.

To validate SPARK's practical feasibility, key performance metrics of authentication delay, communication overhead and computational cost are benchmarked using NS3 simulation and observed that SPARK outperforms [11], [16,17] in terms of speed while maintaining robust security.

Table 3. Simulation parameters

Parameter	Value
Simulation Area (Sq.m)	5000 x 5000
Simulation Time (Sec)	600
Topology	Highway
Number of D2D Pairs	50, 100, 150, 200
Speed of vehicles (Km/h)	30
Packet Size	1024
Propagation Model	Long Distance Propagation loss
Routing Protocol	AODV
Frequency and Bandwidth	28GHz and 100 MHz
Traffic Type	CBR & UDP
Hash Algorithm	SHA-256
Modules used	Antenna, Config store, Mobility, Flow Monitor, LTE and Internet
External libraries used	NFL library, OpenSSL and Crypto++
SUMO version	1.19.0

The graphs Fig.2. to Fig.4. display the authentication delay, communication overhead and computational cost parameters that are evaluated using the proposed algorithm – SPARK and compared with results of HDMA [11], ECA-VFOG [16] and LT – AKA [17] that are certificate less based methods. The performance is analyzed over the number of D2D pairs used in the environment. Under practical conditions, those maximum numbers of D2D pairs that can be sustained while using each of these algorithms are 150, 120 and 180 for [11], [16] and [17] respectively. However, SPARK can sustain up to 200 pairs. The authentication delay refers to the total delay experienced when D_{nr} verifies the identity and authenticity of D_{ns} & RU_i. From Fig.2., it is observed that as the number of D2D pairs is 50, SPARK faster compared to ECA – VFOG by 2.01 times, 1.67 times compared to HDMA and 3.48 times compared to LT – AKA. The number of nodes are taken as multiples of 50 and up to a maximum of 200 pairs. It is observed that SPARK performs 3.47, 3.78 and 2.74 times faster compared with ECA – VFOG and 1.95, 2.12 and 1.96 times faster compared to HDMA and 4.53, 4.13 and 3.15 times faster compared to LT – AKA. The Communication overhead refers to the additional bits along with the original message communicated from D_{ns} *to* D_{nr} and includes certificates, keys and signcryption headers. A minimal communication overhead is very critical in ensuring effective bandwidth utilization and reduced latency for ensuring safety in high mobility environments. From Fig.3., it can be observed that the communication overhead is decreased for SPARK by 1.63, 1.42 and 2.08 times of ECA – VFOG, HDMA and LT – AKA for 50 D2D pairs. When the number of D2D pairs are increased to 100, the same is improved for SPARK by 1.83, 1.67 and 2.73 times, for 150 D2D Pairs it is improved by 1.58, 1.46 and 2.68 times and for 200 D2D pairs it is improved by 1.73, 1.28 and 2.66 times compared with ECA - VFOG, HDMA and LT – AKA. The computational cost is the total time taken for Key management, Certificate verification, Signcryption and Unsigncryption with cryptographic operations for encryption and decryption. From Fig.4., it is observed that the Computational cost of SPARK is only 13.25, 17.99, 10.51 % of the time taken in milli-seconds by ECA - VFOG, HDMA and LT – AKA respectively for 50 D2D pairs. Similarly, the computational cost of SPARK consumes 13.23, 20.64 and 10.59 % of the time for 100 D2D Pairs, 20.56, 27.22 and 17.87% of the time for 150 D2D Pairs and 25.86, 32.69 and 22.93% of the time for 200 D2D Pairs of ECA - VFOG, HDMA and LT – AKA. There is a huge improvement in the computational cost compared to other algorithms. The SPARK algorithm is compared with [11] and [16,17] in terms of authentication delay, communication overhead and computational cost and tabulated in Table 4., Table 5. and Table 6. respectively. It can be observed that SPARK has a clear edge over the other algorithms with respect to the above mentioned parameters.

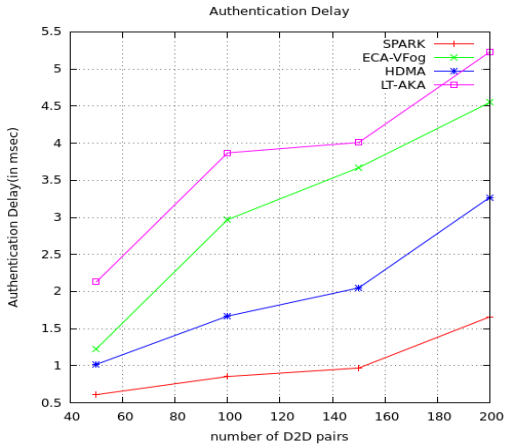

Fig.2. Authentication delay analysis

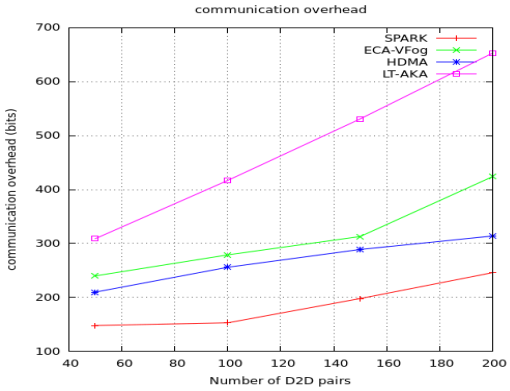

Fig.3. Performance analysis of communication overhead

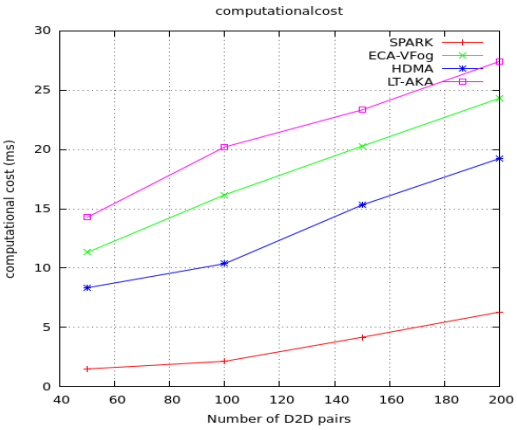

Fig.4. Computational cost analysis

Table 4. Comparison of authentication delay (in ms) for various D2D Pairs with specific quantitative benchmarks

No. of D2D Pairs	LT-AKA [11]	ECA-VFOG [16]	HDMA [17]	SPARK (Proposed)
50	2.13	1.23	1.02	**0.612**
100	3.87	2.97	4.29	**0.856**
150	4.01	3.67	5.81	**0.97**
200	5.23	4.55	6.14	**1.66**

Table 5. Comparison of communication overhead (in bits) for various D2D Pairs with specific quantitative benchmarks

No. of D2D Pairs	LT-AKA [11]	ECA-VFOG [16]	HDMA [17]	SPARK (Proposed)
50	309	240	210	**148**
100	417	279	256	**153**
150	531	313	289	**198**
200	653	424	314	**246**

Table 6. Comparison of computational cost (in ms) for various D2D Pairs with specific quantitative benchmarks

No. of D2D Pairs	LT-AKA [11]	ECA-VFOG [16]	HDMA [17]	SPARK (Proposed)
50	14.28	11.32	8.34	**1.5**
100	20.21	16.18	10.37	**2.14**
150	23.34	20.28	15.32	**4.17**
200	27.43	24.32	19.24	**6.29**

6. Security Analysis

Forward Secrecy: In SPARK, the session key is updated in the private keys of D_{ns}, RU_i and D_{ns} and is difficult for the malicious vehicles to find this value because of HECDH. As all the session keys are locally generated, unauthorized vehicles will not be able to read or use the messages and hence this scheme ensures forward secrecy.

Man-in-the-Middle Attack: SPARK strengthens MITM attacks by ensuring mutual authentication, encrypting communications, establishing secure session keys, and integrating with 5G's network slicing capabilities. HECDH assures mutual authentication using valid certificates issued by *TA*. Signcryption ensures that the data remains private while verifying the source. Also, since every message is to be signed and verified, any changes to this would invalidate the signature. Dynamic session key generation helps in the cause.

We considered 'I' that aims to modify message 'φ_1' that is forwarded between vehicles 'D_a' and 'D_b'. 'φ_1' includes several factors of

$$message_1 = (Nonce_a, \Omega_a, \Delta_a, \delta_a, \varepsilon_a, Cert_a) \tag{35}$$

To be effective in the malevolent effort, 'I' should determine 'Δ_a' and '$Nonce_a$':

$$\Delta_a = \left(Cert_a + h(D_a||Cert_a||\delta_a||RU_{pk})(\varepsilon_a + p_a)\right) \tag{36}$$

$$Nonce_a = E_{\delta_b}(N_a) \tag{37}$$

'I' must have the values of 'ε_a', 'p_a' and 'p_b' that can only be got from ensuing relations below

$$\Omega_a = \varepsilon_a.D, \delta_a = p_a.D \text{ and } \delta_b = p_b.D \tag{38}$$

Performing such calculation is unfeasible as it is comparable to solving HECDLP thrice. Hence, the scheme proves to be robust in resisting Man-In-The-Middle Attacks.

Impersonation Attack: When a malicious vehicle tries to forge a message as $\{message, mD_{ns}, Nonce_i, Y_{pk}, D_{psk}, SG_i\}$ such that it satisfies equation (9) then only the message might be compromised. However, it is almost impossible to implement. So, this technique is highly secure against such type of attacks.

Resistance to Denial of Service (DOS) and Replay Attacks: A malicious vehicle tries to reuse the previous message but fails due to continuous verification of freshness of Time Stamp using $Nonce_i$. Since the time stamp doesn't match SPARK is secure against these attacks. Based on $Nonce_i$ and when complemented with signature checks the incorrect messages can be identified and rejected. SPARK technique secures the messages from DOS attacks by terminating the session.

The proposed mechanism offers security against DoS attack. If 'D_b' sends

$$message_2 = (Nonce_b, \Omega_b, \Delta_b, \delta_b, \vartheta X_b, Cert_b, Cert_{RUi2D}, D_b) \tag{39}$$

to 'D_a', by calling $Nonce_{ab} = E_{\delta_a}(N_a, N_b)$. on receiving '$\varphi_2$', '$D_a$' computes the following. It decrypts,

$$(N_a, N_b) = D_{p_b}(Nonce_a) \tag{40}$$

and ensures newness of 'N_b' along with certificate of source correspondingly to ascertain

$$\left(\omega_{RU} + RU_{pkb}.h\left(D_b \| RU_{pkb}\right)\right) = Cert_b.D \tag{41}$$

It lastly confirms the signature by ensuring the application of ensuing condition:

$$\left(Cert_b.D + (\Omega_b + \delta_b).h\left(RU_{pkb} \| \Omega_b \| Cert_b \| \delta_b \| Nonce_{ab}\right)\right) = \Delta_b.D \tag{42}$$

Nevertheless, the aforesaid calculation is complex for 'I' to determine information which ensures that the system is secured to DOS attacks.

Location Privacy: SPARK secures the privacy of the location by using Chinese remainder theorem. Only the RU_i can retrieve the location of the vehicle. It is not possible to impersonate the RU_i as it needs the Public Key from *TA*.
So, practically it is not possible to retrieve key from both.

Secure Data Transmission: In SPARK, actual session key is never transmitted individually. The session key is generated by the HECDH and even when a malicious vehicle tries to get information about all the keys, it cannot find the exact public and private keys used in the certificates during signcryption.

Table 7. Comparison of Resistance to security attacks against various Algorithms

	LT-AKA [11]	ECA-VFOG [16]	HDMA [17]	SPARK (Proposed)
Location Privacy	√	x	√	√
Forward Secrecy	√	√	x	√
Impersonation	√	√	√	√
Mutual Authentication	√	√	√	√
Replay Attack	√	x	√	√
DOS Attacks	√	x	x	√
Man-in-the-Middle	x	x	x	√
Sybil Attack	x	x	x	√

Along with resistance to above mentioned attacks, SPARK also offers resistance against Sybil attacks by linking a valid certificate issued by *TA* to each vehicle pseudonym thereby avoiding false identities. In the process, only one pseudonym is allowed in a session. Signcryption ensures the messages authenticated using valid keys only. This is possible because only valid nodes are allowed to participate as D2D pairs. *TA* can revoke cloned and unwanted nodes using certificate revocation list. [11] and [16,17] does not resist Sybil attacks.

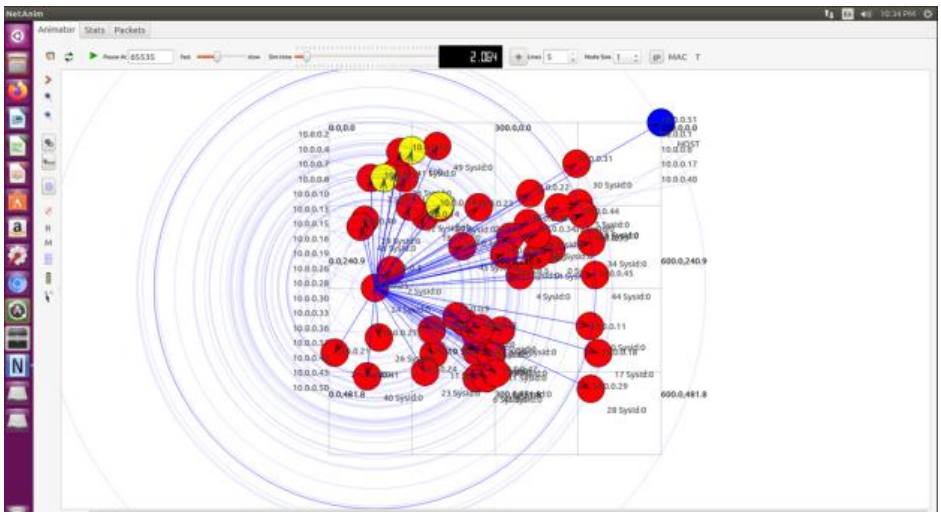

Fig.5. Simulation Scenario with malicious nodes using NS3.26

7. Conclusions

In this paper, a Certificate based Signcryption authentication and key management framework is presented for D2D communication in 5G enabled VANETs by using HECDH. From the results, it is observed that vehicles communicate securely among themselves and Road Side Units and Trusted Authorities as a D2D pair maintaining privacy with reduced latency, Communication overhead and Computational Cost. This scheme ensures confidentiality, authenticity, integrity and non-repudiation for large density of vehicles. The privacy of the location is increased with the use of Chinese reminder algorithm. To our knowledge, it is the second signcryption system in the certificate-based cryptographic scenario that achieves security and privacy in 5G enabled VANETs. Proper research on integrating AI with our technique can help to predict possible threats and integration of edge computing technology can and enhance real-time decision making.

Author Contributions Statement

Chinnam S. V. Maruthi Rao – Corresponding Author - Conceptualization, Methodology, Software Implementation, Formal Analysis, Visualization, and Statistical Analysis, Drafted the initial manuscript, contributed to the literature survey, and documented the technical background of the study.
Rama Krishna Akella – Supervised project execution, Review and edited the manuscript, ensured clarity and coherence, and helped coordinate project milestones and deadlines and validated results using standard metrics

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

This research has not received any grant from any Public / Private funding agency.

Data Availability Statement

Not Applicable as no public data set is used

Ethical Declarations

Not Applicable as the study does not involve human subjects and/or animals.

Acknowledgments

We sincerely thank the experts for their professional evaluation and valuable recommendations, which have contributed to improving the quality of the experiment and the reliability of its results.

Declaration of Generative AI in Scholarly Writing

Authors did not use AI and AI-assisted technologies during in the writing of manuscript.

Abbreviations

The following abbreviations are used in this manuscript:

D2D - Device to Device
VANET - Vehicular Ad-Hoc Networks
DSRC - Dedicated Short-Range Communication
C-V2X - Cellular-Vehicle-to-Everything
V2V - Vehicle-to-Vehicle
V2N - Vehicle-to-Network
V2P - Vehicle-to-Pedestrian
V2I - Vehicle-to-Infrastructure
V2X - Vehicle-to-Everything
ECC - Elliptical Curve Cryptography
HECC - Hyper Elliptical Curve Cryptography
OSM - Open Street Map
SUMO - Simulation of Urban Mobility
MIRACL - Multiprecision Integer and Rational Arithmetic Cryptographic
PBC - Pairing based Cryptography
FANET - Flying Ad-Hoc Network
AVISPA - Automated Validation of Internet Security Protocols and Application

3GPP - 3rd Generation Partnership Project
FISCO - Financial Blockchain Open Source
BCOS - Be Credible, Open & Secure
TB-SCDM - Table-based Study Data Tabulation Model or similar database-centric management
CRUD - Create, Read, Update, and Delete
IIOT - Industrial Internet of Things
TA - Trusted Authority
RSU - Road Side Unit
MITM - Man-in-the-Middle
DOS - Denial of Service
HEC - Hyper Elliptic Curves
Nonce - Number used Once
NS - Network Simulator
LTE - Long Term Evolution
HECDH - Hyper Elliptic Curve Diffie-Hellman

APPENDIX A\B\C…, with appendix tile

NIL

References

[1] Zheng, Y., 1997. Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption). In *Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17* (pp. 165-179). Springer Berlin Heidelberg.

[2] Zheng, Y. and Imai, H., 1998. How to construct efficient signcryption schemes on elliptic curves. *Information processing letters*, *68*(5), pp.227-233.

[3] Kim, R.H. and Youm, H.Y., 2006, November. Secure authenticated key exchange protocol based on EC using signcryption scheme. In *2006 International Conference on Hybrid Information Technology* (Vol. 2, pp. 74-79). IEEE.

[4] Singh, A.K., Solanki, A., Nayyar, A. and Qureshi, B., 2020. Elliptic curve signcryption-based mutual authentication protocol for smart cards. *Applied Sciences*, *10*(22), p.8291.

[5] Mailloux, N., Miri, A. and Nevins, M., 2013. COMPASS: Authenticated group key agreement from signcryption. In *Foundations and Practice of Security: 5th International Symposium, FPS 2012, Montreal, QC, Canada, October 25-26, 2012, Revised Selected Papers 5* (pp. 95-114). Springer Berlin Heidelberg.

[6] Gayathri, M. and Gomathy, C., 2024. Design of CSKAS-VANET model for stable clustering and authentication scheme using RBMA and signcryption. *Frontiers in Computer Science*, *6*, p.1384515.

[7] Liang, Y., Yan, H. and Liu, Y., 2023. Unlinkable Signcryption Scheme for Multi-Receiver in VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *24*(9), pp.10138-10154.

[8] Zhou, Y., Tan, H. and Iroshan, K.C.A.A., 2023. A secure authentication and key agreement scheme with dynamic management for vehicular networks. *Connection Science*, *35*(1), p.2176825.

[9] Khan, M.A., Ullah, I., Nisar, S., Noor, F., Qureshi, I.M., Khanzada, F.U. and Amin, N.U., 2020. An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network. *IEEE Access*, *8*, pp.36807-36828.

[10] Wang, P., Chen, C.M., Kumari, S., Shojafar, M., Tafazolli, R. and Liu, Y.N., 2020. HDMA: Hybrid D2D message authentication scheme for 5G-enabled VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *22*(8), pp.5071-5080.

[11] Miao, J., Wang, Z., Miao, X. and Xing, L., 2021. A secure and efficient lightweight vehicle group authentication protocol in 5G networks. *Wireless Communications and Mobile Computing*, *2021*(1), p.4079092.

[12] Al-Shareeda, M.A., Manickam, S., Mohammed, B.A., Al-Mekhlafi, Z.G., Qtaish, A., Alzahrani, A.J., Alshammari, G., Sallam, A.A. and Almekhlafi, K., 2022. Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU). *Sustainability*, *14*(16), p.9961.

[13] Cui, B., Wei, L. and He, W., 2022. A new certificateless signcryption scheme for securing internet of vehicles in the 5G era. *Security and Communication Networks*, *2022*(1), p.3214913.

[14] Ullah, I., Khan, M.A., Alsharif, M.H. and Nordin, R., 2021. An anonymous certificateless signcryption scheme for secure and efficient deployment of Internet of vehicles. *Sustainability*, *13*(19), p.10891.

[15] Almazroi, A.A., Aldhahri, E.A., Al-Shareeda, M.A. and Manickam, S., 2023. ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing. *Plos one*, *18*(6), p.e0287291.

[16] Chow, M.C. and Ma, M., 2021. A lightweight traceable D2D authentication and key agreement scheme in 5G cellular networks. *Computers and Electrical Engineering*, *95*, p.107375.

[17] Su, J., Ren, R., Li, Y., Lau, R.Y. and Shi, Y., 2022. Trusted Blockchain-Based Signcryption Protocol and Data Management for Authentication and Authorization in VANETs. *Wireless Communications and Mobile Computing*, *2022*(1), p.9572992.

[18] Karati, A. and Biswas, G.P., 2016, September. A practical identity based signcryption scheme from bilinear pairing. In *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 832-836). IEEE.

[19] Ali, U., Idris, M.Y.I., Frnda, J., Ayub, M.N.B., Alroobaea, R., Almansour, F., Shagari, N.M., Ullah, I. and Ali, I., 2022. Hyper elliptic curve based certificateless signcryption scheme for secure IIoT communications. *CMC-Comput. Mater. Contin*, *71*, pp.2515-2532.

[20] Devarajan, M. and Sasikaladevi, N., 2020. An hyper elliptic curve based efficient signcryption scheme for user authentication. *Journal of Intelligent & Fuzzy Systems*, *39*(6), pp.8487-8498.

[21] Zhang, J., Cui, J., Zhong, H., Chen, Z. and Liu, L., 2019. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Transactions on Dependable and Secure Computing*, *18*(2), pp.722-735.

[22] Mallissery, S., Pai, M.M., Mehbadi, M., Pai, R.M. and Wu, Y.S., 2019. Online and offline communication architecture for vehicular ad-hoc networks using NS3 and SUMO simulators. *Journal of High Speed Networks*, *25*(3), pp.253-271.

Authors' Profiles

Chinnam S. V. Maruthi Rao completed his B.Tech in Electronics and Communication Engineering from Nimra College of Engineering and Technology, Jawaharlal Nehru Technological University, Hyderabad in 2001 and done M. S in Embedded Systems & Robotics from University of Essex, U.K in the year 2004. He also holds a M.E degree in Digital Systems from University College of Engineering, Osmania University, Hyderabad from 2022. He is currently pursuing part-time PhD in Koneru Lakshmaiah Education Foundation, Hyderabad in the area of Physical Layer security in D2D Communications. He has teaching experience of more than 16 years and currently working as an Associate Professor in the Department of E.C.E at Sreyas Institute of Engineering and Technology. He published around 10 research papers in international / national conferences and journals. His areas of interest include Digital Systems, Embedded Systems, Cloud Computing, Network Security and Communication Systems. He is a Senior Member of IEEE and also had worked as Student branch counselor for 3+ Years.

RamaKrishna Akella completed his B.Tech in Electronics and Communication Engineering from Jawaharlal Nehru Technological University, Hyderabad and done M. S in Telecommunication and Electronic Engineering from Sheffield Hallam University, U.K with merit grade. He completed his PhD in wireless communications from KL University, Vaddeswaram, AP in the year 2018. He is currently working as Associate Professor in the Department of Electronics and Communication Engineering as well as Principal and Director Campus Placements in Koneru Lakshmaiah Education Foundation, Hyderabad. He has 11+ years of teaching & 2+ years of industry experience. He has good number of publications in reputed international / national journals.

How to cite this paper: Chinnam S. V. Maruthi Rao, Rama Krishna Akella, "A Lightweight Framework Using Signcryption Based Key Agreement Scheme with Location Privacy for D2D Communications in 5G VANETs", International Journal of Computer Network and Information Security(IJCNIS), Vol.18, No.2, pp.181-195, 2026. DOI:10.5815/ijcnis.2026.02.10