HOMOMORPHIC AGGREGATE SIGNATURE SCHEME WITH OUTSOURCING ALGORITHM BASED PRIVACY PRESERVING IN VANETS

C.M.T.Karthigeyan[1], C.Satheeshpandian[2]

[1]Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering , Bargur (An Autonoumus Institution Affiliated to Anna University, Chennai) Krishnagiri, Tamilnadu, India.

[2]Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering , Bodinayakanur,Theni District, Tamilnadu, India.

Abstract:
One of the important paradigms of recent technological development has known to be Vehicular Ad-hoc Networks (VANETs) due to its current intelligent transportation network. Moreover, leakage of communication information or sensitive data in VANETs can leads to vulnerable attacks that may affect many properties and lives. For this reason, VANET systems need to have high-level security aspects. In addition, devices with less computing resources expected for fast computation power. Several researchers have analysed various privacy preserving models for VANETs to protect from different attacks, which is not enough to prevent from new attackers. In this research, a Homomorphic Aggregate Signature (HAS) scheme proposed for achieving unforgeable message attacks without having random oracle and new outsourcing algorithm is designed efficiently for exponential operations to reduce the computational cost in which matrices conjugate operation based on homomorphic mapping is used for achieving the security of both base and exponent numbers. In addition, a protocol based on privacy preserving is constructed for VANETs by using the proposed HAS scheme and outsourcing computing, in which the authentication is processed by presenting a proxy re-signature scheme. In this proposed protocol, RSU will act as an agent when TA authorizes it and OBU’s signatures are converted to TA’s signature by using RSU. Real-identity of OBU is traced by TA using its secret key when an unknown/malicious message is detected then the proposed protocol will provide traceability, privacy, and anonymity. Furthermore, pairing and exponential operations are not needed by the proposed scheme as ` complexity of calculations is reduced significantly for VANET system.

Keywords: Homomorphic Aggregate Signature, Outsourcing Computing, Privacy Preserving Protocol, Vehicular Ad-hoc Networks, Computational Cost, Security

1 INTRODUCTION

In recent technological advancement, Internet of Things (IoT) have emerged way beyond the imagination and become popular all over the world. IoT is a form of network that utilizes the full interconnection between the objects and people, vice-versa, and people-to-people itself [1] [2]. The sensors and radio frequency identification devices used to obtain the physical world information and make transmission by mobile and internet communication networks, which is one of the main features of IoT characteristics [3] [4]. Theintelligent controlling and decision-making achieved by enhancing the ability of technology world to process and analyse the information by adopting intelligence-computing technologies. Several sectors applied with IoT technology such as transportation,water network, energy saving, medical and health, power grid, smart home, military, logistics, industrial, environmental protection, and other fields [5] [6].

Obtaining data privacy for open environment when facing various kinds of attacks arethe most challenging aspects of different IoT applications and example overview of traffic on VANET is shown in figure 1 [7]. The user’s safety upon their properties and lives are related to the personal privacy information that is generally based on shopping habits, personal hobbies, and tourist routes

[8]. Therefore, the popularization and development of IoT is affected directly when concerning the identity privacy, location privacy, and data security [9]. Privacy is a major concern for each platform like social networks that vulnerable to spam, IoT devices to hack their data, Cloud service, and many more [10] [11]. The efficiency and comfort increased due to the advancement in Vehicular Ad-hoc Networks (VANETs) system that known nowadays as intelligent vehicular transportation networks [12].

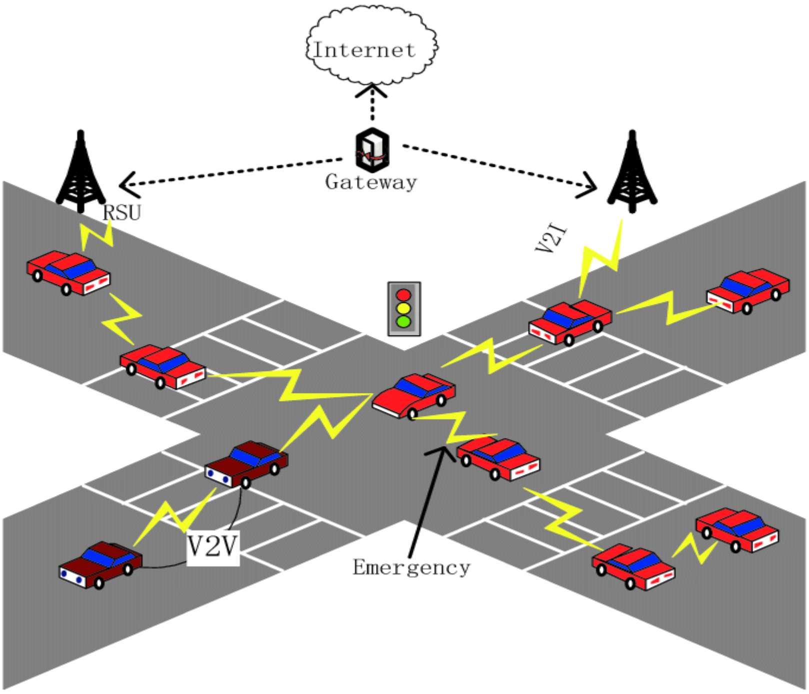


Fig. 1 Traffic on VANET

The technology of VANET system holds traffic information due to its self-organizing ability and support towards a fast mobile communication. The traffic congestion or accidents reported immediately to the roadside drivers for adjusting the route due to current developments and constant communication among Roadside Units (RU) and vehicles [13].There three main parties present in the VANET system and these are Road Side Unit (RSU), Trusted Authorities (TA), and On Board Unit (OBU). The information storage, revocation management, identity authentication, and certificate distribution for each node are processed by using TA, and can be mentioned as authority centre. The OBU is represented as vehicle node and it is capable to act as mobile terminal when used in the communication system. The roadside infrastructure node is denoted as RSU and it is similar to the communication base-station [14] [15].

Various RSUs can be made for traffic signs, roadside gas stations, street lamps, and other existing infrastructures of roadside. VANETs use Dedicated Short Range Communication (DSRC) to allow communication between the RSU and OBU or two OBUs. The broadcasting is done periodically for each vehicle that present in VANET about its traffic accidents and information in real-time [16] [17]. Therefore, other vehicles can make proper decisions and measures with effectively timely manner for improving the traffic conditions. Furthermore, the RSU has more capability not only just broadcasting information related to hotels, gas stations, and restaurants but also it broadcasts the parking warnings, traffic information, and road conditions [18].

Moreover, wireless channel is used for communications in VANETs within instability, which will cause different malicious attacks and ribs like replaying or modifying previous information, injecting false information, etc. [19].Some of the main attacks attempted in VANET system are as follows: (i) Illegal controlling, (ii) Forgery information, (iii) witch attacks, (iv) Replay attacks, (v) Tampering information, (vi) Privacy disclosure, and (vii) Message delaying. Therefore, security is more important when comes to VANET system as it closely related to property and lives of vehicle drivers [20] [21]. Reliability is reduced when network operations are affected by the malicious attacks. As population of the world is increasing, so as the vehicles increase, this will be a major impact on computational cost. Therefore, new privacy and secure system is necessary for VANET system. Furthermore, the computation cost is reduced by using the source of cloud servers [22].

In summary, this paper contributes a Homomorphic Aggregate Signature Scheme to achieve unforgeability against some threats or attacks without a random oracle. Furthermore, an efficient outsourcing algorithm is proposed for exponentiation computation. At last, privacy-preserving protocol is constructed for VANETs to efficiently secure the malicious attacks based on the proposed HAS scheme and outsourcing algorithms. This paper is organized as following segments: In Segment 2, the literature review of existing works is discussed. In Segment 3, the system model and basic security of VANETs reviewed. In Segment 4, presents the proposed HAS scheme with outsourcing algorithms for constructing privacy preserving protocol. In Segment 5, the performance analysis and security are shown. In Segment 6, conclusion of the work is given with some future enhancements.

2 RELATED WORKS

Different privacy-preserving protocols are proposed by various researchers to achieve reliable security for VANETs that are based on some Public-Key Cryptography schemes: Raya and Hubaux [23] used traditional PKI technology for preserving privacy in VANETs that help in protecting the OBUs real identity by occasionally replacing certificates. TA associates anonymous certificates for traceability by finding maintained table with real-OBU. Zhang et al. [24] used Hash Message Authentication Code (HMAC) symmetry key by presenting RSU-aided Messages Authentication Scheme (RAISE), without using message signature based Public Key Infrastructure (PKI) for reducing the signature cost. Moreover, high computational cost is obtained when using authentication scheme of RAISE that has capable to use asymmetric cryptography.

Jiang et al. [25] used binary authentication tree for V2I communication by presenting ID-authentication algorithm. Filtering bogus messages and many signatures are verified using this proposed algorithm and obtained a high efficiency. Marmol et al. [26] distinguished the selfish or malicious nodes accurately and quickly with the help of RSUs in VANET by proposing reputation and trust infrastructure based proposal (TRIP). Haddadou et al. [27] managed and allocated the credits securely by proposing Distributed Trusted Model (DTM2). Enough information is not possible to collect and evaluate in real-time due to its large mobility of vehicles.

Li and Song [28] analysed the VANETs malicious vehicles, and using the obtained multiple vehicles data the trustworthiness is evaluated. Based on recommendation-trust and functional-trust, the nodes trustworthiness is determined and indicates its functionality and recommendations trust level. The data sparsity is not considered by this proposed approach that pervasive to VANETs. Lin et al. [29] proposed secure protocol for privacy preserving named GSIS for categorizing the major requirements of VANETs privacy, which is based on identity-based signature techniques and group signature for reducing signature-overhead in roadside-to-vehicle communications. All the vehicles present in the model is considered one universal group.Yuan et al. [30] supported flexible operations on Cipher text by adopting BGN encryption having ‘doubly homomorphic’ and back propagation algorithm for privacy preserving is realized. Unlimited addition operations and only one multiplication are supported by the BGN cryptosystem.

Zhang et al. [31] performed outsourcing computation by utilizing fully homomorphic property. The authors used same public key for encryption of input data for outsourcing computation for privacy preserving. Barni et al. [32] secured ECG signal classifier by implementing two methods one with linear branching programs and other based on neural network. The garbled circuits and homomorphic encryption are two major key technical innovation used by the authors. Liu et al. [33] used Naïve Bayesian classification decision support system for securing patient centric clinic.

Furthermore, authors used homomorphic-proxy aggregation scheme for converting the encryption under various public keys with proxy public-key.

Graepel et al. [34] described the implementation of two binary classification algorithms namely Fisher's-Linear Discriminant and Linear Means over encrypted domain by using privacy preserving technique with homomorphic encryption. Some information is learned by the clients regarding classification model even when it is working with the private-classification. Bost et al. [35] used full homomorphic encryption-scheme and developed two-party computation framework as privacy preserving technique. In this paper, the authors proposed model that can realize hyperplane decision, Binary Decision tree, and Naïve Bayes from classifier model. However, large communication and computation cost is obtained by using this model. Shokri et al. [36] designed, implemented, and evaluated a privacy-preserving scheme by using parallel deep learning. In this work, the local dataset of his/her of every participant is trained with the same neural network model and selective parameter is used as a technique with sharing of model to the benefits of participants. However, some computations are needed to be used for training for every participant.

III **PROPOSED WORK**

1. Preliminaries

In this section, some basic concepts regarding security are discussed.

Standard RSA Assumption (SRSA):

Two large primes are defined as a and b and the set n=ab, randomly an element is chosen as $r \in \mathrm{Z}_n$ and the prime number p $<$ n. Computing q is difficult which defined to be $q^p = r(mod\ n)$. For any time$T_{RSA} - time$, the assumption of standard RSA is expressed as $(T_{RSA}, \varepsilon_{RSA})$-RSA, the advantage Adv_{At} of an attacker $\mathcal{A}t$ is to solve the problem of RSA that meets$Adv_{At} < \varepsilon_{RSA}$.

A natural approach is provided by the RSA problem for designing the digital signatures in which the public key is denoted as PK and the secret-key is defined as (a, b, q). Then, the signature will consists of(e, q), where q is signature and e is depends on given message [38].

Equivalent RSA problem (ERSA):

Given, $r \in \mathrm{Z}_n$,

Prime =e,

Output = β, x

Such that, $\beta^e = r^x$,

Where,

$$gcd(x, e) = 1$$

Therefore, $z = \beta \frac{\mathrm{gcd}(e,x)}{x} = \beta^{\frac{1}{x}}$ can be efficiently computed as,

$$z^e = (\beta^e)^{1/x} = (r^x)^{1/x} = r,$$

,

The SRSA problem has the solution defined as z. Moreover, (β, x) is one solution when an output z is obtained for $z^e = r$ as like equivalent RSA problem. Here, x is randomly chosen and derived the β from the oracle of SRSA problem as $\beta^e = r^x$.

2. Security Model of HAS Scheme

In this section, the description of security model for Homomorphic Aggregate Signature (HAS) Scheme is discussed. The major definition about the Homomorphic Aggregate Signature (HAS) schemes given by the Zhang Peng et al. [37].This security model is unforgeable in which for any probabilistic polynomial time-adversary TA for all k that is negligible for the following game with the advantage of TA in the security parameter n.

- **Setup:** The setup runs by the challenger as $Setup(1^n, 1^k)$ for obtaining public-key and security-key as (PK_i, SK_i) where (i=1.......k). The challenger sends the public-key $PK_i(i = 1, \dots \dots, k)$ to TA, and the security-key$SK_i(i = 1, \dots \dots, k)$ kept itself.
- **Queries:** The query stage is used with same tag $ID \in \{0,1\}^n$ and the message $(mg_1, \dots \dots, mg_q)$ is specified with A. The user's private key $PK_i(SK_1, \dots \dots, SK_{q_s}) \subset (SK_1, \dots \dots, SK_k)$is chosen randomly by the challenger and $\theta_i \leftarrow Sign(ID, SK_i, mg_i)(i = 1, \dots, q_s)$ is computed.Then, the tag ID is given to A, with signature $\theta_i(i = 1, \dots, q_s)$and corresponding public-key PK_i.For each stage, the most query times is denoted asq_s.
- **Output:** The tuple output of the public key is given by adversary A, signature and message PK^*, mg^*, θ^*.

If $Verify(ID, PK^*, mg^*, \theta^*) = 1$ then the adversary A wins and either,

(a) $PK^* \notin \{PK_1, \dots \dots \dots, PK_{q_s}\}, and\ mg^* \neq 0$

Or

(b) $PK^* \in \{PK_1, \dots \dots \dots, PK_{q_s}\}, for\ example\ PK^* = PK_j, and\ mg^* \neq mg_j$.

3. VANETs Security Requirements

The main objective for the security requirement of VANETs is to improve the traffic management efficiency, protect personal safety of passengers and drivers, and reduce congestion of road traffic. However, the VANET system is threatened seriously by common attacks. Following are the requirements that should be satisfied by the VANETs security protocol.

- Authentication: The source of the transmitting messages from VANETs is verified which is the basic requirement for secure communication. Messages cannot be sent by malicious user that having false named, which can be guaranteed by message authentication.
- Non-Repudiation: in this type, message sender cannot deny the transmitted messages. The vehicle users are misled in VANET, which has false message and that is why it is responsible of each user for their sent message. Forgery attacks can be effectively fought by non-repudiation that is the false information from malicious user are failed to invest into VANET.
- Integrity: When it comes for sending or broadcasting course, messages cannot be changed. The reliability and authenticity of messages is ensured by integrity and the system security is improved.
- Privacy: Some information sent through VANET system is related to user's privacy that cannot be exposed to any unknown/unauthorized party. The replay attacks and privacy leakage is blocked effectively when it comes for confidentiality of messages.
- Anonymity: Tracking of vehicle users or their personal information according to the transmitted messages cannot be obtained by anybody without having owner's permission.
- Traceability: TA can trace the real identity after the traffic accident for the vehicle and then legal responsibility is investigated. In VANET's, the identity and safety of vehicle monitoring is responsible by TA.
- Revocation: TA can revoke the malicious users present in the VANET system and illegal infringement is terminated effectively. Furthermore, the vehicle user's safety is ensured.
- Real-Time: The traffic roads effective order is destroyed and overload is caused in VANET system due to changeable network topology and huge network scale. Therefore, system security especially needs real-time in VANETs.

IVEXPERIMENTAL SETUP

In this section, the security analysis of proposed HAS method is discussed with two outsourcing algorithms and then the construction of privacy preserving protocol is processed.

1. Security Analysis of HAS

HAS scheme is broken over $\mathbb{Z}_q$ by given an adversary; the $ISIS_{q,mg,\theta}$ problem is solved by constructing an adversary over $\mathbb{Z}_q$. Therefore, based on the assumption of $ISIS_{q,mg,\theta}$ the proposed model is secure.

Proof: The signature queries q_{sg} are made by an adversary, which denoted as A. The vector $v^* \in \mathbb{Z}_q^n$ and random matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n\times 2mg}$ are taken as input which constructed by this algorithm.

- **Setup:** The $Setup(1^n, 1^k)$ is passed for getting $\boldsymbol{M}$ and $\boldsymbol{X_1}, \dots \dots, \boldsymbol{X_k}$, and public key is sent from $\boldsymbol{M}$ to A.
- **Queries:** Randomly the messages $v_1, \dots \dots \dots, v_q$ are chosen by A, and the following challenges occurred.

(a)The private keys $\boldsymbol{X_1}, \dots \dots, \boldsymbol{X_{q_s}}$with signers are chosen randomly.

(b)Process the algorithm $Sign(ID, X_i, v_i)$.

(c)The messages ($\boldsymbol{X_1}, \dots \dots, \boldsymbol{X_{q_s}}$) signatures $\left(s_1, \dots \dots, s_{q_s}\right)$ are returned.

- **Output:** The tuple for the public key is the output by A, signature and message (PK^*, v^*, s^*).

The first forgery $PK^* \notin \left(PK_1, \dots \dots, PK_{q_s}\right)$ is impossible due to the usage of similar public key and the second successful forgery when A wins is (PK^*, v^*, e^*) $\left(v^* \notin \left\{v_1, \dots \dots, v_{q_s}\right\}\right)$.

2. Outsourcing Algorithms

Here, two outsourcing algorithms are proposed for cloud server using the the exponential operation $v^a (mod\, n)$. The outsourced algorithms are categorized into two situations based on the privacy of v and a. (1) a is secret, v is public and (2) Both a and v are secret. The algorithms for the corresponding category are given as below. i.e., $A1(v, a_i) = v^{a_i}$ for the secret a_i.

Algorithm 1 (A1):

Here, the secret is given as a_i for $i = 1, \dots \dots, n_0$ and v be the public. The target of using untrusted third party (cloud server) is to compute v^{a_i},

- **Setup:** The v and $a_i - a_0$ are sent to the cloud server by the user, after user computing and keeping $v_0 = v^{a_0}$.
- **Outsourcing Computation:** The $v^{a_i - a_0}$ is returned by cloud server to the user.
- **Output:** The output produced by the user is $v^{a_i} = v^{a_0}.v^{a_i - a_0}$.

Algorithm 2 (A2): For $(i = 1, \dots \dots, n_0)$, the secret for algorithm 2 assigned as a_i and v. The target of this algorithm is to outsource v^{a_i}without revealing a_i and v. That is, for the secret v, a_i the algorithm is A2(v, a_i) = v^{a_i}.

Setup: The $v_0 = v^{a_0}$ is computed and kept first by the user and randomly choosing the invertible matrix M of 2 X 2, and $a_i - a_0$ is sent, and for cloud server is

$$\boldsymbol{A_i} = \boldsymbol{M}.\begin{pmatrix} v & p_i \\ 0 & v^l \end{pmatrix}.\boldsymbol{M}^{-1}$$

Where,

p_i is randomly selected for l=2.

- **Outsourcing Computation:** The user is returned with $O_i = A_i^{a_i - a_0}$ from the cloud server.

- **Output and Verification:** The output from the user is determined as $v^{a_i} = v^{a_0}.v^{a_i - a_0}$, when calculating $V_i = M^{-1}B_iM$ and gets $(M_i)_{11}(M_i)_{22}$. It checks firstly whether $(V_i)_{11}^2 = (V_i)_{22}$ or not. Then, $(V_i)_{11} = v^{a_i - a_0}$ if it holds.

Correctness: Immediately the correctness is obtained.

Since $MAM^{-1}.MBM^{-1} = MABM^{-1}$, then

$$B_i = A_i^{a_i - a_0} = M.\begin{pmatrix} v & p_i \\ 0 & v^l \end{pmatrix}^{a_i - a_0}.M^{-1}$$
$$= M.\begin{pmatrix} v^{a_i - a_0} & p_i' \\ 0 & (v^l)^{a_i - a_0} \end{pmatrix}.M^{-1}$$

If valid B_i is returned by the cloud server, then $(V_i)_{11} = v^{a_i - a_0}$ and $(V_i)_{22} = v^{2(a_i - a_0)}$.

3. VANETs Privacy-Preserving Protocol using Proposed Method

The basic concept of privacy-preserving protocol for VANETs is that RSU is authorized by TA to act as an agent and proxy re-signature algorithm is processed. The proposed OBU's scheme is converted into TA's signature by RSU for protecting the OBU identity. At the same time, TA traces the OBU's real identity quickly and accurately and OBU is revoked when malicious messages found by any party. The protocol of the proposed privacy preserving is given as below.

- **Setup:** Two large primes a and b are selected by TA. Then, n=ab. A random element $r \in Z_n^*$ is chosen and the hash function resistant collision $M: Z_n^2 \to Z_n, M_0: U \times Z_n \to Z_n,$ where the identity set is defined as U.
- **Key Generation:** In this stage, it is divided into three sub-categories.

- g, e is picked by TA such that $g.e \equiv 1(mod\theta(n))$ and publishes g. Then, TA has the secret key as e.

- $w_{OBU} = M_0(ID, u_{OBU})$ is computed by TA and private key is sent as $d_{OBU} = d^{w^{-1}OBU}$

- The ENC_{RSU} with (PK_{RSU}, SK_{RSU}) is established by RSU of its own.

- **Re-Signature Key Generation:** The S_{OBU} is chosen randomly by TA for computing $A1(d, S_{OBU}) = d^{S_{OBU}}$. Then, the re-signature key $(ID, d^{S_{OBU}}, z_{OBU})$ for OBU is given for RUS.

Where, $z_{OBU} = e.w_{OBU}.S_{OBU}$

- **Signature for OBU:** The vehicle OBU includes four domains when sending the message and these are: Type of message (ID_{type}), PL-message payload obtained from vehicle direction, traffic incident, speed, location, and other basic information, Time-Stamp (Time) for identifying the correct time for generating the messages, and finally first three information's signature. Following algorithm is processed by OBU.

- Randomly p is selected by OBU for message $M = ID_{type} \parallel PL \parallel Time$ and Outsourcing Algorithm 2 is processed for obtaining

$\theta = d_{OBU}^{M(M,p)} = A2(d_{OBU}, M(M,p))$

- The RSU public key is used by OBU for encrypting $X = (ID, u_{OBU}, M, p, \theta)$, and then $ENC_{RSU}(X)$ is sent to RSU from OBU.

- **RSU Re-Signature:** The $ENC_{RSU}(X)$ is decrypted RSU to get $X = (ID, u_{OBU}, M, p, \theta)$, and checking whether $(\theta)^{M_0(ID, u_{OBU})} = d^{M(M,p)}$ or not.
- **Signature Verification:** The validity of $(M, p, \theta', (d^{S_{OBU}})^p)$ can be verified by any party. The verifier gives 1 as output if the verification holds as $(\theta')^e = (d^{pS_{OBU}})^{M(M,p)}$, otherwise zero.

- **Revocation and Tracing:** TA runs the tracing process and executes the revocation-process with RSU.

- **Tracing:** The corresponding OBU's real identity is traced by TA, which has access if $(\theta')^{e} \neq (d^{p.S_{OBU}})^{M(M,p)}$. The corresponding $\{ID, d^{S_{OBU}}\}$ is found by TA in the local list T when uses its secret key for computing $A1(d^{p.S_{OBU}}, p^{-1}) = (d^{p.S_{OBU}})^{p^{-1}} = d^{s_{OBU}}$ and $p^{-1}(mod\theta(n))$.

- **Revocation:** The $d^{s_{OBU}}$ is sent to RSU by TA once it finds OBU malicious vehicle, and revoke this OBU. The ID and $d^{s_{OBU}}$ are deleted from the list T by TA and RSU.

The correctness of proposed scheme is as follows:

- **OBU's Signature Correctness:**

Since, $M_0(ID, u_{OBU}) = w_{OBU}$ and $\theta = d_{OBU}^{H(M,p)} = \left(d^{w_{OBU}^{-1}}\right)^{M(M,p)}$, then

$\theta^{M_0(ID,u_{OBU})} = \theta^{w_{OBU}} = d^{M(M,p)}$

- **RSU's Re-Signature Correctness:**

Since, $g.e \equiv 1mod(\theta(n))$ and $\theta' = \theta^{(z_{OBU})p}$

$$= d^{eM(M,p)p.S_{OBU}}$$

Then, $(\theta')^{e} = (d^{p.S_{OBU}})^{M(M,p)}$

V Results and Discussions

In this section, the proposed privacy-preserving protocol based on HAS for VANETs efficiency and security aspects are presented.

1. Analysis of Security Aspects

The VANET protocol has some security aspects that include, Verifiability of Message, Privacy of Message, Key-Security, Non-Forgery, Traceability, and Anti-Replay Attack.

- **Verifiability of Message:** The validity of message M is checked by RSU after obtaining OBU's public key. Other users use the public key of TA to verify the new signature after doing re-signature. The authenticities of messages are ensured by the verifier, because two signatures from the non-forgery.
- **Privacy of Messages:** The security of communication and OBU's identity anonymity is included in privacy between OBU and RSU.
- **Key-Security:** The OBU's secret key according to key-generation is $d_{OBU} = d^{w_{OBU}^{-1}}$. Because of intractability for factorizing n into a and b, the w_{OBU}^{-1} is failed to compute by RSU.
- **Non-Forgery:** The new privacy protocol provides non-forgery due to the proposed HAS non-forgery scheme.
- **Traceability:** TA uses its secret key when the malicious code is found to be as message for computing $d^{S_{OBU}}$. The OBU's real-identity ID is found by TA and it remove from the list T. Therefore, the vehicles which affected by malicious code will not allowed to participate in the authorized communications through RSU and breaking of system could not possible.
- **Anti-Replay Attack:** Attack existing can be tested by RSU when the time-stamp (Time) is modified by adversary. The message freshness is guaranteed by the time-stamp and effectively can avoid/resist the replay-messages attack.

2. Performance Analysis

In this section, the performance analysis of the proposed privacy-preserving protocol for VANET using HAS scheme is obtained in terms of Storage-Cost, Computation-Cost, and Computation-Cost.

(i) Storage-Cost

Here, the parameter setting is presented first in the proposed HAS scheme. The proposed HAS scheme's security is ensured by the underlying hard problem known to be the public key $n = a.b$ for IFP. Then, let $\rho = \log n \approx 1024$ be the secure parameter in which a, b is given as 512bits. Based on three various parties OBU, TA, and RSU, the storage cost is analysed.

- **Storage Cost of OBU:** The signature key d_{OBU} with size 1024 bits is only needed to carried by OBU.
- **Storage Cost of TA:** TA assigns the secret key as a, b, g. The revocation list $T = \{ID, d^{S_{OBU}}\}$ should be maintained by TA where $d^{S_{OBU}}$ is 1024-bit and ID is 32-bit.
- **Storage Cost of RSU:** The encryption secret-key SK_{RSU} is carried by RSU and each one acts as proxy to re-signature and $\{ID, d^{OBU}, z_{OBU}\}$ for n-OBUs'

(ii) Communication Cost

- **TA to RSU:** The communications from TA-to-RSU has two rounds. In Revocation-Phase: The ID of OBU is revoked by TA when it sending $d^{S_{OBU}}$ to RSU. In Key-Generation: The re-signature key $\{ID, d^{S_{OBU}}, z_{OBU}\}$ of TA is sent to RSU.
- **TA to OBU:** Corresponding secret key d_{OBU} of TA is sent to each OBU in the key-generation. Then, 1024N bits are needed to transmit data.
- **OBU to RSU:** The encrypted signature is sent by OBU-to-RSU. The first three elements ID_{type}, Pay-Load (PL), and Time-Stamp (Time) are set to be 32-bit, and 1024-bit is assigned to signature.

(iii) Computation Cost

Different stages are used for analysing the computation cost and these are: Key-Generation, Re-Signature, Signature, and Tracing, in which it ignores hash computing cost. The outsourced and non-outsourced protocol is discussed by using the advantage of outsourcing algorithms. The non-outsourced protocol for VANETs privacy preserving is first computed as,

- The secret key $d_{OBU} = d^{w_{OBU}^{-1}}$ of OBU is calculated by TA in the key-generation and w_{OBU}^{-1} is got by the multiplication of the TA's secret-key. In addition, the re-signature key is created for RSU by TA and computed $d^{S_{OBU}}, z_{OBU} = e.S_{OBU}.w_{OBU}$. Therefore, TA requires three multiplications (MUL) and two exponential operations in the key-generation stage.
- One exponential operation is required by OBU for calculating $\theta = d_{OBU}^{M(M,r)}$ in the signature phase.
- RSU is checking whether $(\theta)^{M_0(ID, u_{OBU})} = d^{M(M,p)}$ or not in the re-signature phase. Three exponential operations are needed by RSU.
- One exponential operation is executed by TA for computing $(d^{p \cdot S_{OBU}})^{p^{-1}}$ in the tracing phase.

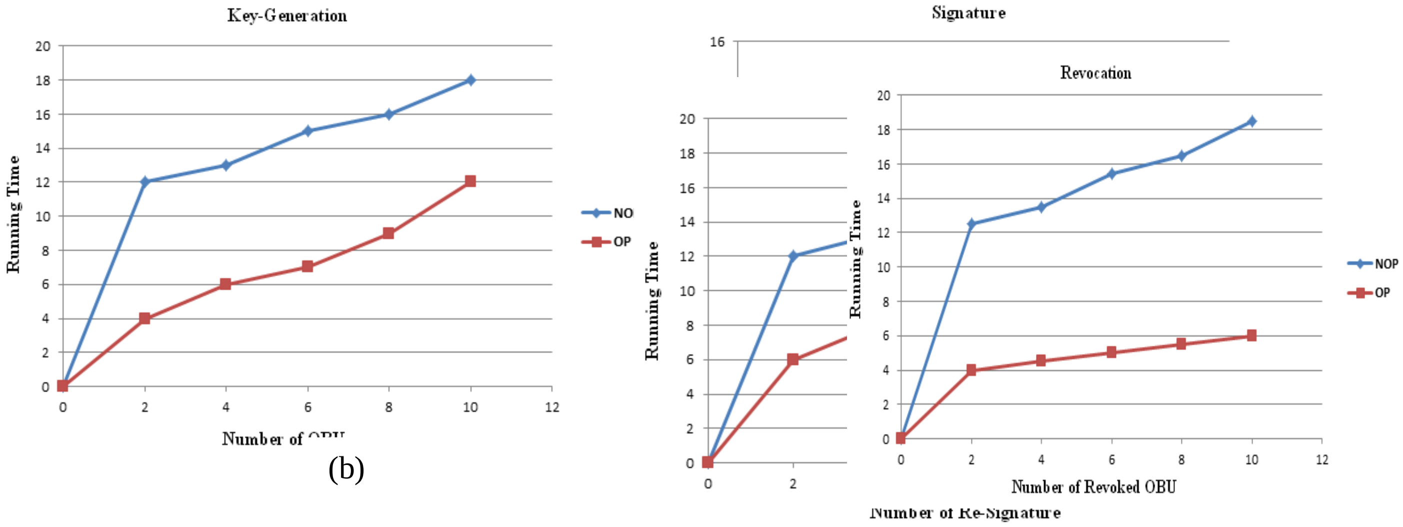
Therefore, the outsourced scheme is analysed based on the given algorithms. The user does pre-calculation for each exponential operation. However, one exponential operation is computed by only one multiplication that needed by the user in outsourced algorithm 1. Moreover, 20 multiplications are needed by the user to compute one exponential operation in the outsourced algorithm 2. Therefore, Table 1 shows the comparison of computation cost between outsourced (OP) and non-outsourced protocol (NOP).

Table 1 Computation Cost of NOP and OP

	Signature		**Key-Generation**		**Revocation**		**Re-Signature**	
	Exp	**Mul**	**Exp**	**Mul**	**Exp**	**Mul**	**Exp**	**Mul**

OP	0	17	0	5	0	1	0	57
NOP	1	0	2	3	1	0	3	0

Figure 2 shows the computation cost comparison between the outsourced and non-outsourced algorithms. In which the number of vehicles (OBU) is represented in ‘x-axis’ and corresponding running time is denoted in ‘y-axis’. The multiplication module n is used by the outsourced algorithm for explicitly identify the huge gap between the NOP and OP protocol.



(b)

Fig. 2 Comparison between NOP and OP Protocols

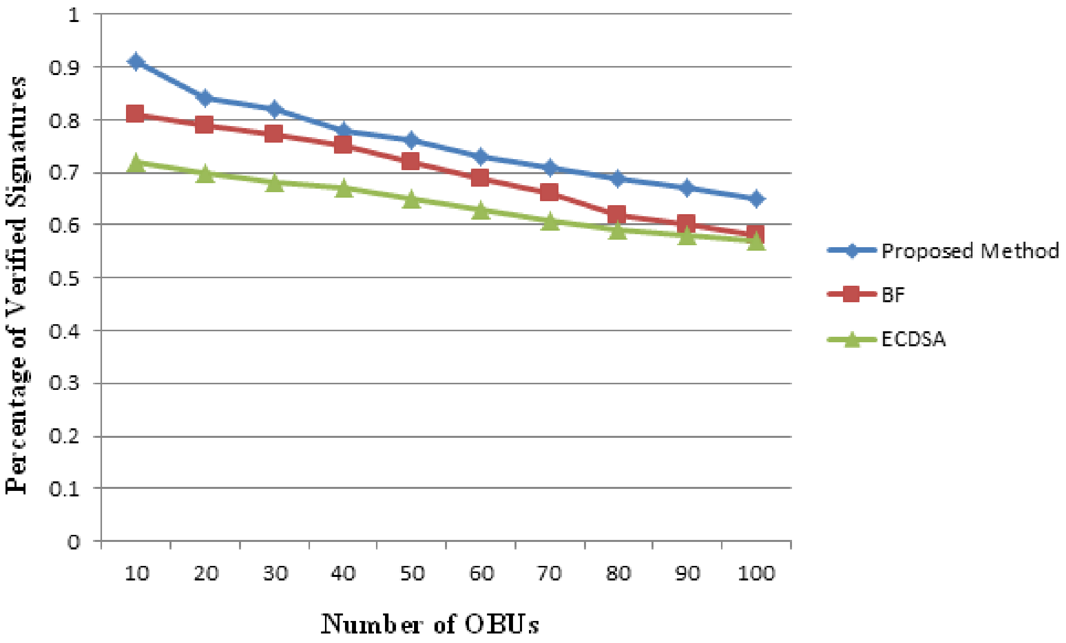


Fig. 3 Comparison of Verified Signatures

Figure 3 shows the percentage of verified signatures for the proposed HAS scheme and compared the results with Bloom Filter (BF) and Elliptic Curve Digital Signature Algorithm (ECDSA). Moreover, figure 3 shows the authenticate number of commitment keys using proposed scheme, BF, and ECDSA. The proposed method can authenticate all messages sent by vehicles in the VANET and has highest percentage of verifying signature as compared to BF and ECDSA.

VICONCLUSION

In this research, Homomorphic Aggregate Signature (HAS) scheme is proposed to protect against the message attack that chosen without random oracle. Two efficient and secure outsourcing algorithms are presented to reduce the computational cost for the exponential operations. The cryptosystems are generally applicable by the outsourcing algorithms within exponential operations. Furthermore, the proposed HAS scheme and outsourcing algorithms are used to construct the VANET's privacy-preserving protocol in which the authentications are analysed by the proxy re-signature. Therefore, traceability, privacy, and anonymity are provided by the proposed VANET protocol. Moreover, the pairing of exponential operations is not needed with respect to efficiency. Significantly, the calculation burden is reduced for the VANET systems. In addition, the proposed VANET protocol has higher percentage of verified signatures when compared with ECDSA and BF. The future work leads to improve the efficiency of the key signature by improving the outsourced algorithms.

REFERENCES

1. Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., & Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*, *92*, 265-275.

2. Aswale, P., Shukla, A., Bharati, P., Bharambe, S., &Palve, S. (2019). An Overview of Internet of Things: Architecture, Protocols and Challenges. In *Information and Communication Technology for Intelligent Systems* (pp. 299-308). Springer, Singapore.

3. Zhao, K., & Ge, L. (2013, December). A survey on the internet of things security. In *2013 Ninth international conference on computational intelligence and security* (pp. 663-667). IEEE.

4. Umer, T., Rehmani, M. H., Kamal, A. E., &Mihaylova, L. (2019). Information and resource management systems for Internet of Things: Energy management, communication protocols and future applications.

5. Atzori, L., Iera, A., &Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

6. Kopetz, H. (2011). Internet of things. In *Real-time systems* (pp. 307-323). Springer, Boston, MA.

7. Gan, G., Lu, Z., & Jiang, J. (2011, August). Internet of things security analysis. In *2011 international conference on internet technology and applications* (pp. 1-4). IEEE.

8. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266-2279.

9. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, *4*(5), 1125-1142.

10. Murugan, N. S., & Devi, G. U. (2018).Detecting streaming of Twitter spam using hybrid method. *Wireless Personal Communications*, *103*(2), 1353-1374.

11. Murugan, N. S., & Devi, G. U. (2019). Feature extraction using LR-PCA hybridization on twitter data and classification accuracy using machine learning algorithms. *Cluster Computing*, *22*(6), 13965-13974.

12. Qu, F., Wu, Z., Wang, F. Y., & Cho, W. (2015). A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems*, *16*(6), 2985-2996.

13. Jayapal, C., & Roy, S. S. (2016, March). Road traffic congestion management using VANET.In *2016 International Conference on Advances in Human Machine Interaction (HMI)* (pp. 1-7). IEEE.

14. Sharma, B., Sharma, M. S. P., &Tomar, R. S. (2019). A Survey: Issues and Challenges of Vehicular Ad Hoc Networks (VANETs). *Available at SSRN 3363555*.

15. Ali, I., Hassan, A., & Li, F. (2019).Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. *Vehicular Communications*.

16. Guo, J., &Balon, N. (2006). Vehicular ad hoc networks and dedicated short-range communication. *University of Michigan*.

17. Kumar, V. D., Kumar, V. V., &Kandar, D. (2018). Data Transmission Between Dedicated Short Range Communication and WiMAX for Efficient Vehicular Communication. *Journal of Computational and Theoretical Nanoscience*, *15*(8), 2649-2654.

18. Tonguz, O., Wisitpongphan, N., Bait, F., Mudaliget, P., &Sadekart, V. (2007, May). Broadcasting in VANET.In *2007 mobile networking for vehicular environments* (pp. 7-12). IEEE.

19. Yousefi, S., Mousavi, M. S., &Fathy, M. (2006, June). Vehicular ad hoc networks (VANETs): challenges and perspectives. In *2006 6th International Conference on ITS Telecommunications* (pp. 761-766). IEEE.

20. Sumra, I. A., Ahmad, I., &Hasbullah, H. (2011, April).Classes of attacks in VANET.In *2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)* (pp. 1-5).IEEE.

21. Rawat, A., Sharma, S., & Sushil, R. (2012). VANET: Security attacks and its possible solutions. *Journal of Information and Operations Management*, *3*(1), 301.

22. Ashritha, M., & Sridhar, C. S. (2015, January). RSU based efficient vehicle authentication mechanism for VANETs. In *2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)* (pp. 1-5). IEEE.

23. Raya, M., &Hubaux, J. P. (2005, November). The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks* (pp. 11-21). ACM.

24. Zhang, C., Lin, X., Lu, R., & Ho, P. H. (2008, May).RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks in *2008 IEEE international conference on communications* (pp. 1451-1457). IEEE.

25. Jiang, Y., Shi, M., Shen, X., & Lin, C. (2008).BAT: A robust signature scheme for vehicular networks using binary authentication tree. *IEEE Transactions on Wireless Communications*, *8*(4), 1974-1983.

26. Mármol, F. G., & Pérez, G. M. (2012). TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of network and computer applications*, *35*(3), 934-941.

27. Haddadou, N., Rachedi, A., &Ghamri-Doudane, Y. (2014). A job market signaling scheme for incentive and trust management in vehicular ad hoc networks. *IEEE transactions on vehicular technology*, *64*(8), 3657-3674.

28. Li, W., & Song, H. (2015). ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *17*(4), 960-969.

29. Lin, X., Sun, X., Ho, P. H., & Shen, X. (2007). GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on vehicular technology*, *56*(6), 3442-3456.

30. Yuan, J., & Yu, S. (2013). Privacy preserving back-propagation neural network learning made practical with cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, *25*(1), 212-221.

31. Zhang, Q., Yang, L. T., & Chen, Z. (2015). Privacy preserving deep computation model on cloud for big data feature learning. *IEEE Transactions on Computers*, *65*(5), 1351-1362.

32. Barni, M., Failla, P., Lazzeretti, R., Paus, A., Sadeghi, A. R., Schneider, T., &Kolesnikov, V. (2009, December). Efficient privacy-preserving classification of ECG signals. In *2009 First IEEE International Workshop on Information Forensics and Security (WIFS)* (pp. 91-95). IEEE.
33. Liu, X., Lu, R., Ma, J., Chen, L., & Qin, B. (2015).Privacy-preserving patient-centric clinical decision support system on naive Bayesian classification. *IEEE journal of biomedical and health informatics*, *20*(2), 655-668.
34. Graepel, T., Lauter, K., &Naehrig, M. (2012, November). ML confidential: Machine learning on encrypted data. In *International Conference on Information Security and Cryptology* (pp. 1-21). Springer, Berlin, Heidelberg.
35. Bost, R., Popa, R. A., Tu, S., &Goldwasser, S. (2015, February). Machine learning classification over encrypted data. In *NDSS* (Vol. 4324, p. 4325).
36. Shokri, R., &Shmatikov, V. (2015, October). Privacy-preserving deep learning. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security* (pp. 1310-1321).ACM.
37. Zhang, P., Yu, J., & Wang, T. (2012).A homomorphic aggregate signature scheme based on lattice. *Chinese Journal of Electronics*, *21*(4), 701-704.
38. Wei, Z., Li, J., Wang, X., & Gao, C. Z. (2019). A Lightweight Privacy-Preserving Protocol for VANETs Based on Secure Outsourcing Computing. IEEE Access, 7, 62785-62793.