Hardware Assisted Protocol for Attacks Prevention in Ad Hoc Networks

Vincent Omollo Nyangaresi(✉)

Tom Mboya University College, Homabay, Kenya
vnyangaresi@tmuc.ac.ke

Abstract. The packet exchanges over open communication channels expose ad hoc networks data to numerous security and privacy attacks. To address this issue, many schemes have been developed based on public key infrastructure, tamper proof devices, bilinear pairings or trusted authorities. However, these techniques still have a number of security and privacy challenges or are inefficient in terms of communication, computation or storage overheads. In this paper, an attack prevention protocol is proposed based on elliptic curve cryptography and a combination of private keys and signatures. The results of simulations that were executed showed that the proposed protocol had the lowest computation costs, communication overheads, energy consumption and latencies in terms of signature signing and verification. In addition, this protocol offered non-repudiation, communication session unlinkability, mutual authentication, integrity, location privacy and anonymity. Moreover, it was resilient against message replays and impersonation attacks.

Keywords: Ad hoc networks · Authentication · Efficiency · Privacy · Security · TPD

1 Introduction

One of the most promising components of intelligent transportation system is the vehicular ad-hoc network (VANET) that can improve transport conditions through collaborative driving. However, message exchanges in VANETs is through dedicated short range communication (DSRC) over open wireless channels [1]. This exposes the transmitted packets to both security and privacy attacks such as eavesdropping, impersonation and modifications [2]. The leakage of vehicle's real identity can potentially expose driver's trajectory and locations. As such, it is critical for the messages to be authenticated by all the communicating entities in order to uphold integrity and confidentiality. In addition, authors in [3] explain that communication challenges such as efficiency, privacy and security need to be addressed in these ad hoc networks. Authors in [4] identify security and privacy as crucial issues in VANETs while message interception, tampering and tracking have been noted in [5] as some of the most dangerous attacks in this environment. Since these attacks compromise vehicle safety and privacy of its occupants, it is

M. H. Miraz et al. (Eds.): iCETiC 2021, LNICST 395, pp. 3–20, 2021.
https://doi.org/10.1007/978-3-030-90016-8_1

important that they are addressed. As explained in [6], private and secure communication in VANETs enhance safety and comfort of the drivers. Authors in [7] stress on the significance of message authentication between roadside units (RSUs) and vehicles, while in [8] authors explain that challenges such as privacy and reliability necessitate the enhancement of confidentiality and security of the exchanged data. Owing to the requirements for secure communication in VANETs, authors in [9] identify implementation of integrity, non-repudiation, confidentiality and authentication as being key in these networks. On the other hand, the importance of message authentication, integrity and reliability among vehicles has been highlighted in [10].

During deployments, privacy, security and efficiency have been discussed in [11] as being important for secure data exchanges. This requires that RSUs and vehicles verify the authenticity of all received messages before processing. In addition, captured messages over open channels may facilitate identification of real indentify of vehicles and their subsequent route tracking. To address this, enhanced unlinkability, privacy and anonymous communication need to be implemented in VANETs. On the other hand, the reliance on tamper proof devices (TPDs) and space complexity of authenticating techniques has been presented in [12] as significant challenges. One approach towards privacy protection in VANETs is anonymous authentication [4]. For attacks prevention, symmetric cryptography based approaches are more efficient compared to their asymmetric cryptography based techniques. However, as explained in [12], issues such as key management and non-repudiation still remain unresolved in symmetric cryptography.

1.1 Problem Statement

Security, privacy and efficiency during ad hoc communication are key issues and numerous schemes have been developed to address these issues. The conventional techniques either utilize bilinear pairing (BP), public key infrastructure (PKI), ideal tamper proof devices (TPD), trusted authority (TA), certificates or group signatures. However, BP operations and group signatures require high communication and computation overheads while TA may be a single point of failure during massive authentication process. On the other hand, the conventional authentication techniques based on TPD assume that this hardware device is highly resilient against security and privacy attacks. In addition, PKI based techniques result in problems regarding certificate storage and management. Consequently, conventional ad hoc authentication protocols either do not offer resilience against most of the ad hoc attacks or are inefficient in terms of communication, computation and energy overheads.

1.2 Our Contributions

The main contributions of this paper include the following:

I. Anonymous authentication protocol employing pseudonyms is developed to offer communication entity location and identity privacy in VANETs.
II. Realistic TPD devoid of system key pre-installation is deployed to address side-channel attacks in conventional hardware-based authentication schemes.

III. Intermediary ECC-based ephemerals are utilized to prevent key escrow problems in PKI based schemes.
IV. Individual vehicle signature and group signatures are implemented to provide non-repudiation and confidentiality.
V. We show that techniques in I–IV above rendered the proposed protocol resilient against conventional ad hoc attacks such as impersonation and message replays.

1.3 Organization of the Paper

The rest of this paper is organized as follows: Sect. 2 discusses related work while Sect. 3 details the system model. On the other hand, Sect. 4 presents the simulation and evaluation results while Sect. 5 concludes the paper and gives future directions.

2 Related Work

Over the recent past, numerous schemes have been developed to facilitate secure communication in vehicular networks. For instance, authors in [13] have presented a bilinear based anonymous authentication technique. However, this scheme has high computational costs and never incorporates session unlinkability in its design. Similarly, authors in [14–19] have developed bilinear based authentication schemes, but which have high computational costs. The elliptic curve (EC) pseudonym based technique in [20] has good computational efficiency but requires incorporation of trusted authority (TA) during authentication process. This effectively increases both communication latencies and costs, in addition to TA presenting a single point of failure [21]. Similarly, a hash function based scheme for privacy protection has been presented in [22], but which requires involvement of TA during the verification procedures. In addition, authors in [23] and [24] have deployed TA for the generation of authentication keys between vehicles and RSUs, and hence have similar challenges as schemes in [20] and [22]. Authors in [25] introduce certificate based authentication, but which requires high computation and space complexity. On the other hand, the schemes presented in [26–30] are prone to attacks and are also inefficient. In addition, the scheme in [26] results in high communication overheads. An identity based authentication approach is presented in [2] based on elliptic curve cryptography (ECC). However, this technique requires an ideal TPD for the storage of master keys of each vehicle.

Registration lists and hash functions have been incorporated in [31] during authentication while hash functions and XOR based authentication algorithm has been developed in [32]. Although the techniques in [31] and [32] enhance computational efficiency, their reliance on TA may potentially lead to some bottlenecks within the network. The batch authentication approach developed in [33] achieves some anonymity, but fails to offer resilience against collusion attacks. Authors in [34] have presented an aggregate signature based scheme for privacy preservation, but requires a trusted third for message verification. A PKI-based authentication protocol is developed in [35] but has high storage requirements for the generated vehicle certificates. Authors in [36] have presented an anonymous privacy preserving technique for vehicular networks, but has high communication costs. On the other hand, the anonymous authentication scheme in [37] requires

maintenance of certificate revocation list (CRL) which increases its storage costs. Group key based schemes have been presented in [10] and [38–40]. However, in most of these group key signature based schemes, group leaders have high communication energy and computational resources consumption. In addition, group signature verification is computationally intensive, and the group leader can potentially become a network bottleneck. Specifically, the protocol in [40] offers only one-way authentication between TA and participating vehicles.

A conditional privacy preservation technique has been developed in [41], but has high storage requirements. On the other hand, the batch authentication scheme in [42] is susceptible to replay attacks and cannot withstand non-repudiation of the generated signature. An anonymous authentication algorithm developed in [43] achieves low computation overheads but fails to consider communication session unlinkability. On the other hand, the scheme in [44] cannot withstand modification and impersonation attacks. Authors in [45] have combined pseudonyms with group signature for authentication. However, this technique has high space complexity for CRL and high computation costs for CRL verification. On the other hand, the symmetric cryptograph hash function and XOR based scheme in [46] achieves high communication and computation overheads, but fails to consider internal attacks. Identity based VANET authentication scheme has been presented in [47] for privacy preservation. However, these protocols are inefficient and do not offer effective certificate revocation techniques. Similarly, identity based techniques in [48, 49] utilize group signatures for authentication and anonymity enhancement. However, the approach in [48] has high space and computation overheads, while the algorithm in [49] is vulnerable to replay and tracing attacks and cannot offer both backward and forward key secrecy. In addition, they inherit high communication and computation overheads of group signatures. Moreover, the techniques in [49] and [47] have ineffective certificate revocation mechanisms and do not offer mutual authentication.

3 System Model

In this section, the design goals, mathematical preliminaries, system architecture and the procedures of the proposed protocol are discussed.

3.1 Design Goals

In light of the security, privacy and efficiency challenges of the current ad hoc authentication and key management protocols, this paper proposes a hardware assisted protocol for attacks prevention in ad hoc networks. The proposed protocol employs both secret keys and group signatures for mutual authentication, while pseudonyms are deployed to uphold anonymity of the communicating entities. The authentication process is devoid of TA so as to alleviate single point of failure problem. In addition, the deployed TPD is based on realistic security assumptions of it being susceptible to physical and side-channel attacks. As such, no system keys are pre-installed in TPD and hence its failure or capture of secrets stored in it cannot compromise the entire network. Some of the goals pursued include unlinkability, authentication, integrity, non-repudiation, location privacy, anonymity, and resilience against message replays and impersonation attacks.

3.2 Mathematical Preliminaries

The proposed protocol deployed elliptic curve cryptography (ECC) which is a widely implemented cryptographic algorithm due to its high efficiency and superb security. It utilizes less bits than Rivest–Shamir–Adleman (RSA) algorithm for encrypting same length message and hence has less communication, computation and storage complexity. In addition, it requires fewer computation parameters and shorter key lengths, rendering it ideal for resource constrained vehicle TPDs. The following definitions hold for ECC systems:

Denoting a set of all EC points over a restricted field F_θ as $\varepsilon(F_\theta)$ where $\theta > 3$, then $\varepsilon : y^2 = (x^3 + \alpha x + \psi) mod\ \theta$. Here, α, $\psi \epsilon F_\theta$ and $4\alpha^3 + 27\psi^2 \neq 0$.

Let ϕ and ω be two points of group $\bar{g}$. Then if ϕ is not equal to ω, for an additive EC group $\bar{g} = \{(x, y)\epsilon\varepsilon(F_\theta) : x, y\epsilon F_\theta\} \cup \{i\}$ where i is a point at infinity, $\bar{g}$ forms a cyclic group under addition operation $\beta = \phi + \omega$ for ϕ, $\psi\epsilon\bar{g}$. Here, β is the intersection of ε and the straight line connecting θ and ϑ. If $\phi = \omega$, then $\beta = \phi + \omega$, but if $\phi = -\omega$, then $\phi + \omega = 0$.

Let $\phi\epsilon\bar{g}_\theta$ and $\mu\epsilon Z^*_\vartheta$ for μ, in this case, scalar multiplication of ε is given by $\phi = \phi + \phi + \phi + \cdots\phi$.

Suppose that ϕ and ω are two randomly generated points on ε where $\phi\epsilon\bar{g}$ generates group $\bar{g}$ with large prime order ϑ. Then in EC discrete logarithm (ECDL), given ϕ,$\omega\epsilon\bar{g}$, then the problem is to find $x\epsilon Z^*_\vartheta$ such that $\omega = x\phi\epsilon\bar{g}$.

Let ϕ be a generator of $\bar{g}$, $\alpha\phi$,$\psi\phi\epsilon\bar{g}$ where α, $\psi\epsilon Z^*_\vartheta$ are unknown. Then the EC computational Diffie-Hellman (ECCDH) problem is to calculate $\alpha\psi\phi\epsilon\bar{g}$.

Given ϕ, $\alpha\phi$, $\psi\phi$, $\gamma\phi\epsilon\bar{g}_1$ where ϕ is the generator of $\bar{g}_1$ with large prime order ϑ. Then for α, ψ, $\gamma\epsilon Z^*_\vartheta$, it is computationally cumbersome to decide whether or not $\gamma \equiv \alpha\psi \bmod \vartheta$.

Suppose that algorithm $\mathfrak{B}$ solves ECDL problem in $\bar{g}$ within some polynomial time with success probability $\mathfrak{H}$, then:

$$\mathfrak{H} = \Pr\left[\mathfrak{B}(\phi, x\phi) = x : x\epsilon Z^*_\vartheta\right] \geq \xi$$

ECDL hypothesis is defined as $\mathfrak{B}$ in any polynomial time and $\mathfrak{H}$ is negligible.

If ECDL or ECCDH on a group $\bar{g}$ cannot be solved with non-negligible probability ξ in time t, then ECDL or ECCDH is said to be a complex problem on EC.

3.3 System Architecture

In the proposed protocol, the system architecture consists of vehicles Vi fully equipped with online board units (OBUs), roadside unit (RSU), the public internet and the cloud server (CS) as shown in Fig. 1. Each OBU device incorporates a tamper proof device (TPD) to buffer the security secrets. The CS and RSU are trusted network entities but the Vi and internet connections are un-trusted. Whenever Vi wants some services from the cloud server, full authentication must be executed among the CS, Vi and RSU so as to prevent security and privacy attacks that may emanate from the internet.

Once mutual authentication is complete, the V_i need to sign each message transmitted to uphold both security and privacy.

Fig. 1. System architecture

3.4 Proposed Protocol

The proposed protocol consisted of five major phases including initialization, pseudo-identities generation, secret key generation, signature generation and verification. Table 1 presents the notations used in this paper and their brief description.

Table 1. Notations and their descriptions

Notation	Description
CS	Cloud server
V_i	i^{th} vehicle
RSU	Roadside unit
GS	Group signature
θ, ϑ	Large prime numbers
ε	Elliptic curve
$\mathcal{Z}$	CS master key
$\mathcal{B}$	CS public key
ψ	RSU master key
$\mathcal{Z}$	RSU public key
$\breve{y}$	Message signature
η_i	RSU nonce
$\mathcal{W}_i$	V_i pseudo-identity
X_1, X_2, X_3	Hash functions
η_i, R_i,$\hat{W}_i$	Nonces
τ_i	Timestamp
$\Delta\tau_i$	Legitimate duration of pseudo identity
β_i	Partial private key of V_i
RegReq	V_i registration request
β_iReq	β_i request
$\mathcal{H}_i$	V_i real identity
ζ_i	V_i secret parameter
ς_i	V_i public key
ϕ_i	V_i private key
$\oplus$	XOR operation

As shown in Algorithm 1, during the initialization phase, the RSU and CS agree on θ, ϑ after which they generate ε as in step 1 where α, $\psi \in Z_\theta^*$ and $(4\alpha^3 + \psi^2) \bmod \theta \neq 0$. In step 2, the CS chooses $\mathcal{Z} \in Z_\theta^*$as its private master key and utilizes it to derive its

public master key E. Next, the RSU stochastically chooses $\psi \in Z_\theta^*$ as its private master key and uses it to compute security parameter $\ddot{g}$. For improved security and privacy, $\mathcal{Z}$and ψ are only known to CS and RSU respectively and are never shared over the communication channels. In step 4, both CS and V i choose hash functions for subsequent authentication before publishing $\{\phi, \theta, \vartheta, \varepsilon, \chi_1, \chi_2\ \chi_3, \bar{g}_i, \ddot{g}, \mathcal{B}\}$(step 5). During V_i registration, the registration request RegReq , together with V_i's true identity $\mathcal{H}_i$ are sent to the corresponding RSU (step 6). At the same time, the V_i obtains the published security tokens which are then buffered in its TPD (step 7). To uphold anonymity, each V_i randomly chooses nonce η_i and employs it to derive its pseudo-identity $\mathcal{U}_i$ and other additional security token $\mho$ i for later authentication, before sending $\{\mathcal{U}_i,1, \mho_i\}$ to its RSU (step 9). To prevent impersonation and forgery attacks, the RSU re-computes V_i's $\mathcal{H}_i$ as shown in step 10. This identity is then validated in step 11 such that if it is invalid, RegReq is immediately discarded.

Algorithm 1: Authentication and Key Management

Input: θ, ϑ, $\mathcal{Z}$, ψ, χ_1, χ_2, χ_3, ϕ, η_i, τ_i, $\mathcal{R}_i$,$\hat{W}_i$, $\mathcal{L}_{2,i}$, ω_i, $\Delta\tau_i$

Output: ε, $\mathcal{B}$, $\ddot{g}$, $\mathcal{U}_{i,1}$, $\mho_i$, $\mathcal{H}_i$, $\mathcal{U}_{i,2}$, β_i, $\mathcal{L}_{1,i}$, β_i, ζ_i, ς_i, φ, $\mathcal{L}_{2,l}$, $\mathcal{L}_{3,l}$, sign_i, $\ddot{\mathcal{Y}}_i$, GS, $\ddot{\mathcal{Y}}_G$, λ

Begin:

1) Agree on θ and ϑ generate $\varepsilon: y^2 = (x^3 + \alpha x + \psi)\ mod\ \theta$
2) Choose $\mathcal{Z} \epsilon\ Z_\theta^*$ & compute $\mathcal{B}$=$\mathcal{Z}\phi$
3) Select $\psi\epsilon\ Z_\theta^*$ & compute $\ddot{g}$=$\psi\phi$
4) Choose χ_1, χ_2, χ_3:$\{0,1\}^* \rightarrow Z_\theta^*$
5) Publish $\{\phi, \theta, \vartheta, \varepsilon, \chi_1, \chi_2\ \chi_3, \bar{g}_i, \ddot{g}, \mathcal{B}\}$
6) $V_i \rightarrow$RSU: {RegReq, $\mathcal{H}_i$}
7) Buffer $\{\phi, \theta, \vartheta, \varepsilon, \chi_1, \chi_2\ \chi_3, \bar{g}_i, \ddot{g}, \mathcal{B}\}$in TPD
8) Choose $\eta_i\ \epsilon\ Z_\theta^*$ & compute $\mathcal{U}_{i,1}$= $\eta_i\phi$, $\mho_i$=$\eta_i\ddot{g}\oplus\mathcal{H}_i$
9) $V_i \rightarrow$ RSU: {$\mathcal{U}_{i,1}$, $\mho_i$}
10) Re-compute $\mathcal{H}_i$=$\mho_i \oplus \psi\mathcal{U}_{i,1}$
11) **IF** $\mathcal{H}_i$ is invalid **THEN**: Discard RegReq
12) **ELSE**:
13) Calculate $\mathcal{U}_{i,2}$=$\mathcal{H}_i\oplus\chi_1(\psi\mathcal{U}_{i,1}, \tau_i)$
14) RSU$\rightarrow$CS: {$\mathcal{U}_{i,1}$, $\mathcal{U}_{i,2}$,τ_i}
15) $V_i \rightarrow$CS: {β_iReq}
16) Select $\mathcal{R}_i\ \epsilon\ Z_\theta^*$ & compute β_i= $\mathcal{R}_i\phi$, $\mathcal{L}_{1,i} = \chi_1(\mathcal{U}_i, \beta_i, \mathcal{B})$, β_i=($\mathcal{R}_i$+ $\mathcal{Z}\mathcal{L}_{1,i}$) mod θ
17) CS $\rightarrow$ V_i:{β_i, β_i, $\mathcal{U}_i$}
18) **IF** $\beta_i\phi$!= β_i+$\mathcal{L}_{1,i}$ $\mathcal{B}$ **THEN**: Discard β_iReq
19) **ELSE:** Choose $\hat{W}_i\ \epsilon\ Z_\theta^*$ & compute ζ_i=$\hat{W}_i\phi$
20) Generate $\mathcal{L}_{2,i}$=$\chi_2(\mathcal{U}_i, \zeta_i)$, ω_i=β_i+$\mathcal{L}_{2,i}\zeta_i$
21) Set ς_i=(ω_i, β_i) as public key & φ=(β_i, $\hat{W}_i$) as private key
22) Choose $\bar{g}_i\ \epsilon\ Z_\theta^*$ & compute $\bar{G}_i$=$\bar{g}\phi$, $\mathcal{L}_{2,i}$=$\chi_2(\mathcal{U}_i, \zeta_i)$, $\mathcal{L}_{3,i}$=$\chi_3(\mathcal{U}_i, \rho_i, \zeta_i, \bar{G}_i, \tau_i)$, sign_i=[$\bar{g}_i$ + $\mathcal{L}_{3,i}(\beta_i + \mathcal{L}_{2,i}\hat{W}_i)$] mod θ, $\ddot{\mathcal{Y}}_i$=($\bar{G}_i$, sign_i)
23) $V_i \rightarrow$ RSU: {$\mathcal{U}_i$, ζ_i, ρ_i, τ_i, $\ddot{\mathcal{Y}}_i$}
24) **IF** $\Delta\tau_i$ and τ_i are invalid **THEN**: Discard sign_i
25) **ELSE:** Re-compute $\mathcal{L}_{1,i}$, $\mathcal{L}_{3,i}$
26) **IF** $\text{sign}_i\phi$!= $\bar{G}_i$+ $\mathcal{L}_{3,i}(\omega_i+\mathcal{L}_{1,i}\mathcal{B})$ **THEN:** Discard sign_i
27) **ELSE**: Trust sign_i
28) Generate $GS = \sum_{i=1}^{n} \text{sign}_i$ & compute $\ddot{\mathcal{Y}}_G$=($\bar{G}_1$, $\bar{G}_2$, $\bar{G}_3$,…, $\bar{G}_n$, GS)
29) WSNS$\rightarrow$CS: {$\ddot{\mathcal{Y}}_G$}
30) **IF** $\Delta\tau_i$ and τ_i are invalid **THEN**: Discard $\ddot{\mathcal{Y}}_G$
31) **ELSE:** Compute $\lambda = \sum \bar{G}_i + \sum \mathcal{L}_{3,i}(\omega_i + \mathcal{L}_{1,i}\mathcal{B})$
32) **IF** λ is invalid **THEN:** Deny resource access
33) **ELSE:** Grant resource access
34) **ENDIF;ENDIF;ENDIF;ENDIF;ENDIF**

END

However, if it is valid, RSU computes pseudo-identity $\mathbb{M}_{i,2}$ (step 13) before forwarding $\{\mathbb{M}_{i,1}, \mathbb{M}_{i,2}, \tau_i\}$ to CS (step 14). Here, current timestamp τ_i served to thwart any packet replays. In step 15, the V_i makes a request $\beta_i Req$ for assignment of its partial secret key β_i from the CS. This secret key is deployed in subsequent signing of its messages to protect integrity of transmitted messages. Upon the receipt of $\beta_i Req$, the CS chooses ephemeral R_i which then it utilizes to derive security tokens β_i, $L_{\cdot 1,i}$ and β_i for later message signing and authentication (step 16). In step 17, the CS sends beacon $\{\beta_i, \beta_i, \mathbb{M}_i\}$ to V_i, which then validates it in step 18 such that if it is invalid, the $\beta_i Req$ is discarded. However, if it is valid, the V_i proceeds to randomly select private nonce $\hat{W}_i$ that it then utilizes to derive security token ζ_i (step 19). In step 20, the V_i derives security parameters $L_{\cdot 2,I}$ and ω_i employed for computation of its public key ς_i. Next, the V_i sets ς_i and φ as its public key and private keys respectively for payload protection (step 21). In step 22, signature $sign_i$ for authentication and integrity protection of message $\ell_i \in \{0, 1\}^*$ is derived. The process begins by having the V_i randomly choose security token $\bar{g}_i$before computing $\bar{G}_i$, $L_{\cdot 2,i}$, and $L_{\cdot 3,i}$. Thereafter, the V_i generates $sign_i$ and $\check{Y}_i$ before sending beacon $\{\mathbb{M}_i, \zeta_i, \rho_i, \tau_i, \check{Y}_i\}$ to its RSU (step 23) as shown in Fig. 2.

Upon receiving this beacon, the RSU validates the timestamp τ_i as well as the permissible duration of pseudo identity $\Delta\tau_i$ to prevent message replay attacks (step 24). If these two values are invalid, the received signature is discarded, otherwise the RSU proceeds to re-compute security tokens $L_{\cdot 1,i}$ and $L_{\cdot 3,I}$ (step 25) that are used to validate the received signature $sign_i$ in step 26. Here, if these security tokens are invalid, the received signature is discarded, otherwise the RSU trusts the V_i (step 27). The proposed protocol also supported group signature GS for authenticating a number of V_i's simultaneously. As evidenced in step 28, upon receiving multiple authentication tokens $\{\mathbb{M}_i, \varsigma_i, \rho_i, \tau_i \check{Y}_i\}$, $i \in \{1, 2, \ldots n\}$ from V_i group with signature pairs $\{\rho_i, \check{Y}_i\}$, it amalgamates these signatures through GS and $\check{Y}_G$. Thereafter, the RSU sends $\check{Y}_G$ to the CS (step 29) where $\Delta\tau_i$ and τ_i are verified such that if they are invalid, $\check{Y}_G$ is discarded (step 30). However, if it is valid, the CS proceeds to compute security token χ(step 31) which is then verified in step 32 such that if it is invalid, resource access is denied. However, if it is valid, the V_i group is granted access to the requested resources.

4 Results and Discussion

The proposed protocol was simulated in Network Simulator 2 (*NS2.35*) owing to its flexible environment that facilitated evaluation of this protocol with other related conventional protocols. For vehicle mobility modeling, VanetMobiSim was deployed.

As shown in Table 2, Ad-hoc On-demand Distance Vector (AODV) was utilized for routing due to its ability of operating in an environment characterized by network challenges such as packet losses, frequent node mobility and link failures. The simulations were executed on 1000 by 20 m^2 coverage area with maximum vehicle and RSU density of 50 and 6 respectively. A channel bandwidth of 5 Mpbs and slot time of 13 ms was adopted with 1 km maximum RSU transmission range. On the other hand, the least inter-vehicle distance was set to 30 m with 300 m maximum transmission range for each vehicle. The Media Access Control (MAC) layer protocol was IEEE 802.11p which is applicable in DSRC, and the maximum traffic lanes were 4. Thereafter, the simulations were run for 150 s as the required data items were collected.

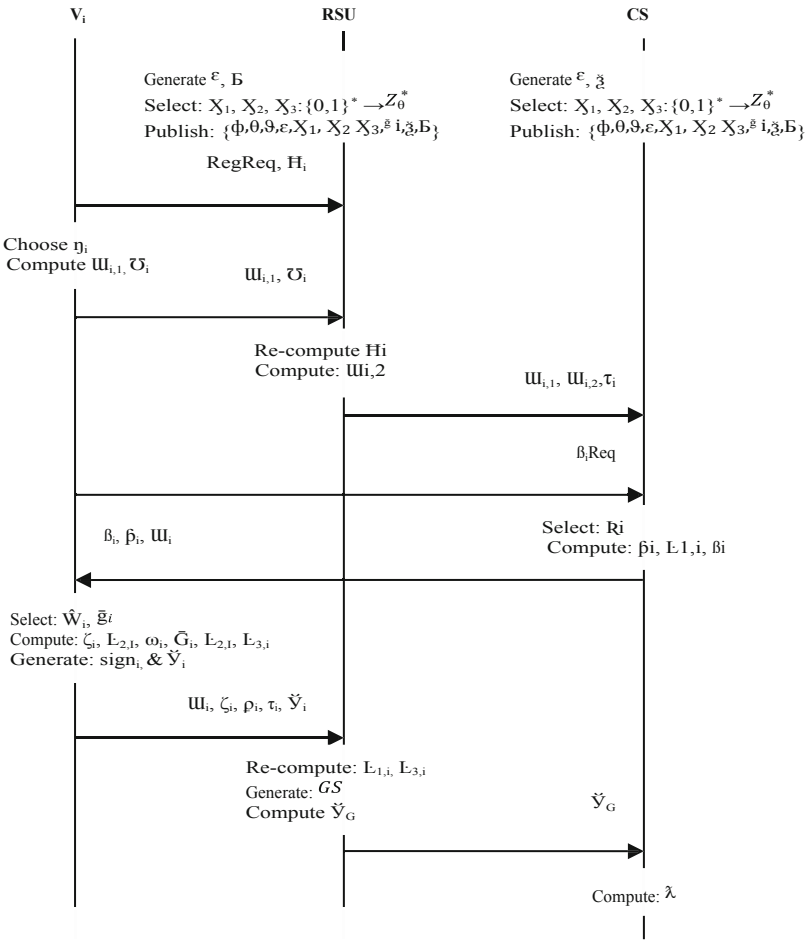

Fig. 2. Message exchanges in the proposed protocol

4.1 Security Evaluation

To assess the security posture of the proposed protocol, Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege (STRIDE) model was utilized. In this model, the desired security and privacy features include authenticity, integrity, non-repudiability, confidentiality, availability, and authorization for upholding spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege respectively.

Unlinkability: to prevent an adversary from associating any two messages of the same V_i, randomly generated security parameter $\bar{g}_i$was incorporated in signature $sign_i$. This offers strong anonymity to beacon $\{\mathit{Wi}_i, \zeta_i, \rho_i, \tau_i, \ddot{Y}_i\}$ exchanged between the V_i and RSU.

Table 2. Simulation parameters

Parameter	Value
Routing protocol	AODV
Network coverage area	1000×20 m^2
Channel bandwidth	5 Mpbs
Slot time	13×10^{-6}s
RSU density	6
RSU's maximum transmission range	1000 m
Maximum Vehicle density	50
Simulation time	150 s
Traffic lanes	4
MAC layer protocol	IEEE 802.11p
V_i maximum transmission range	300 m
Least inter - V_i distance	30 m

Authentication and Integrity: in the proposed protocol, the V_i and RSU authenticate each other using $\mathcal{H}_i$. On the other hand, the RSU and CS authenticate each other using security parameter β_i and $\{\rho_i + L_{1,i}\ E\}$. For message integrity, the V_i signs each message using $sign_i$, which is comprised of current timestamp τ_i, V_i's pseudo-identity $\mathcal{ID}$, secret parameter ζ and private key φ.

Non-repudiation: since the RSU can easily associate each V_i with its actual identity $\mathcal{H}_i$ and pseudo-identity $\mathcal{ID}_i$, it is not possible for a particular V_i to deny its message signature $sign_i$.

Location Privacy: during the communication process, pseudo-identities are utilized instead of the real identities of vehicles. As such, it is not possible for an attacker to track V_i*'s* trajectories within the network. It is only the RSU with its master secret key ψ that can validate $\mathcal{ID}_i$ by executing the following operation: $\mathcal{H}_i = \mathcal{O}_i \oplus \psi \mathcal{ID}_{i,1}$. Consequently, without ψ, an adversary is unable to establish $\mathcal{H}_i$ and hence the proposed protocol upholds authorization. Moreover, since ψ is never sent over the communication channel, it is infeasible for an attacker to eavesdrop it. Consequently, the proposed protocol upholds confidentiality.

Anonymity and Privacy: To uphold anonymity of the V_i, only the RSU has the master key ψ necessary for the derivation of real identity of the V_i, $\mathcal{H}_i$. As such, other vehicles have no knowledge of the real identities of their neighbours. The utilized pseudo-identities such as $\mathcal{ID}_{i,1}$ and $\mathcal{ID}_{i,2}$ coupled with signature $sign_i$ on every message ensures that the exchanged messages are kept secret from the spying eyes of adversaries.

Resilience Against Message Replays and Impersonation Attacks: in the proposed protocol, each message sent by any V_i is signed using $sign_i$ and hence it is infeasible for an

attacker to forge this signature for possible impersonation. The usage of timestamps τ_i during the communication process, coupled with the verification of the legitimate duration of pseudo identity $\Delta\tau_i$ thwarts any message replay attacks. As such, an adversary is unable to launch denial of service attacks against legitimate users through impersonating their network access credentials which might knock off these users from the network.

4.2 Performance Evaluation

The cryptographic operations in [50] executed on MIRACL software on a computer system running on Pentium 4 processor were utilized to evaluate the proposed protocol. Here, modular multiplication in Z_θ^*, T_M takes approximately 0.2325 ms, modular exponential operation T_{MX} takes 55.2 ms, modular point addition T_{MA} takes 0.12 ms, EC scalar point multiplication T_S takes 6.38 ms, bilinear paring T_{BP} takes 20.01 ms, while map to point hashing operation T_H takes 6.38 ms.

Computation Costs: in this evaluation, the signing and verification overheads of individual as well as amalgamated signature are computed. Based on Algorithm 1, signature generation in the proposed protocol requires only one T_S of approximately 6.38 ms that is equivalent to $27.44T_M$ operations. On the other hand, signature verification requires three T_S and two point additions. As such, the total computation overheads for signature verification is ((3* 6.38) + (2*0.12)), yielding 19.38 ms(approximately $83.35T_M$) as shown in Table 3.

Table 3. Computation overheads comparisons

Scheme	Computation overheads			
	Signing		Verification	
	T_M	ms	T_M	ms
[15]	140	32.55	502	116.72
[17]	97	22.55	331	76.96
[19]	110	25.58	384	89.28
[18]	137	31.85	385	89.51
[16]	187	43.48	478	111.14
[14]	113	26.27	388	90.21
Proposed	27.44	6.38	83.35	19.38

The obtained computation overheads are then compared to schemes in [14, 15, 16, 17, 18, 19] as shown in Fig. 3. As shown in Fig. 3, the scheme in [15] had the highest signature verification overheads of 116.72 ms while the proposed protocol had the least signature verification overheads of 19.38 ms.

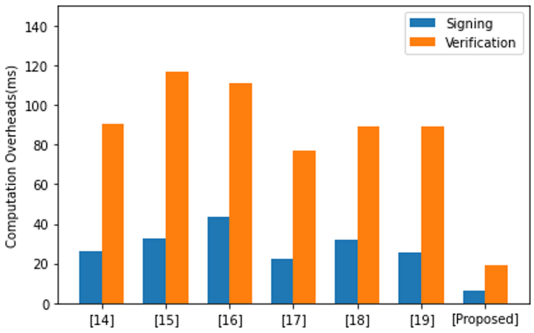

Fig. 3. Computation costs comparisons

On the other hand, the scheme in [16] had the highest signature signing costs of 43.48 ms while the proposed protocol had the least signing costs of 6.38 ms. As such, the proposed protocol was lightweight and hence applicable in resource constrained vehicular OBUs compared with its peers.

Signing and Verification Latencies: to evaluate the proposed protocol against the signature generation and verification latencies, the number of vehicles was varied between 10 and 50 as the values of these latencies were observed. Table 4 presents the results that were obtained.

Table 4. Signature signing and verification latencies

Scheme	Latencies (T_M)									
	Signing					Verification				
	10	20	30	40	50	10	20	30	40	50
[15]	1482	2921	4267	6115	7229	19935	44937	74592	91289	110937
[17]	983	1989	2376	3852	4198	21093	57026	78317	99727	120273
[19]	1128	2392	3949	4372	6061	16038	28723	41218	59022	81291
[18]	1388	2827	4164	6011	7127	18034	30781	43297	61037	82093
[16]	1923	3965	5782	7026	8893	2374	20156	23076	39092	42047
[14]	1022	2298	3845	4278	5967	2103	4315	10097	18092	20136
Proposed	756	984	1023	1793	1931	421	478	512	558	687

As shown in Table 4, there was a general increase in signature signing and verification latencies as the number of vehicles were increased from 10 to 50. This is attributed to the increasing processing at the OBU, RSU and CS as the increment of vehicles implies a surge in the number of transmitted messages. The scheme in [16] had longest signing latencies while the proposed protocol had the shortest signing latencies for all vehicle

densities. On the other hand, the scheme in [17] had the longest signature verification latencies while the proposed protocol had the shortest latencies for all vehicle densities.

Transmission Costs: in the proposed protocol, the transmission costs consisted of timestamp τ_i, pseudo-identities $\mathbb{ID}_i$, $sign_i$ length, β_i, and $\hat{W}_i$. During the authentication process, the V_i sent $\mathbb{ID}_i$, ζ_i, $\breve{Y}_i = (\bar{G}_i, sign_i)$, τ_i, in which $\mathbb{ID}_i$, $\zeta_i \in \bar{g}_i$ and $sign_i \in Z_\vartheta^*$. As such, the total transmission cost is 184 bytes as shown in Fig. 4, which is the aggregation of the total length of $4(\bar{g}_i)$, Z_ϑ^* and τ_i.

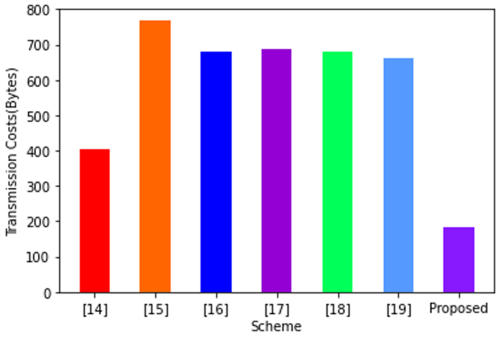

Fig. 4. Transmission costs comparisons

As shown in Fig. 4, the scheme in [15] had the highest transmission costs of 768 bytes followed by the schemes in [14, 16–19] and the proposed protocol with values of 689 bytes, 680 bytes, 680 bytes, 660 bytes, 404 bytes and 184 bytes respectively. Consequently, the proposed protocol had the least bandwidth requirements among its peers. This is due to its bilinear pairing free computations based on lightweight ECC, compared to its peers all of which are based on pairing operations. To investigate how the communication costs were influenced by the increase in signatures, the number of transmitted signatures was increased from 10 to 50 as shown in Fig. 5, below.

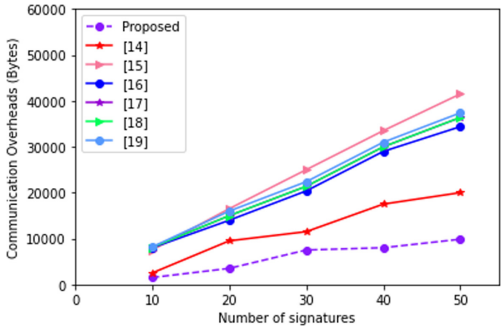

Fig. 5. Communication overheads variations

It is evident from Fig. 5 that as the number of signatures was increased, there was a corresponding increase in communication overheads among all the schemes. As such, the graphs of all schemes assumed nearly the same shape. While the scheme in [15] had the highest communication overheads for all signature densities, the proposed protocol had the least communication overheads for all signature densities. Basically, an increase in the number of signatures imply surging signaling among the network entities during signaling and verification processes, and hence the increase in bandwidth requirements.

Energy Consumption: for this evaluation, energy is obtained from the product of central processing unit maximum power (10.88 watts) and message generation or verification. As such, the energy consumption for the proposed protocol included message signing and verification as shown in Table 5.

Table 5. Signature energy consumption

Scheme	Energy consumption (mJ)	
	Signing	Verification
[15]	367	1247
[17]	220	881
[19]	294	953
[18]	367	953
[16]	440	1173
[14]	293	953
Proposed	69	210

For message signing, the computation involved was: (27.44*0.2325*10.88) while message verification computation was: (83.35*0.2325*10.88). This yielded 69 mJ for signing and 210 mJ for verification. These results were then compared with the values of schemes in [14, 15, 16, 17, 18, 19] as shown in Fig. 6 below. It is clear from Fig. 6 that the protocols in [15] and [18] had the largest signature signing energy consumption of 367 mJ while the proposed protocol had the least energy consumption of 69 mJ. On the other hand, the scheme in [15] had the largest signature verification energy consumption of 1247 mJ followed by the protocol in [16]. The proposed protocol had the least signature verification energy consumption of 210 mJ.

The high energy consumptions for protocols in [14, 15, 16, 17, 18, 19] is due to the computationally intensive bilinear pairing operations that have to be executed during signature signing and verification. On the other hand, the proposed protocol requires lightweight ECC modular multiplications and scalar point multiplication operations, hence its lower energy consumptions. To investigate the effects of increase in number of vehicles on energy consumptions, the number of vehicles was varied between 10 and 50 as shown in Fig. 7.

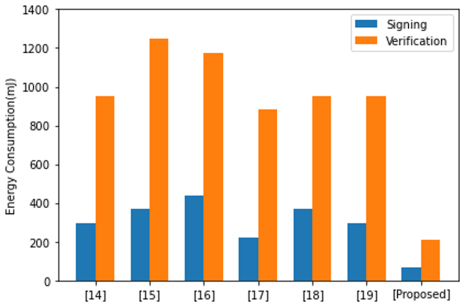

Fig. 6. Signature energy consumption

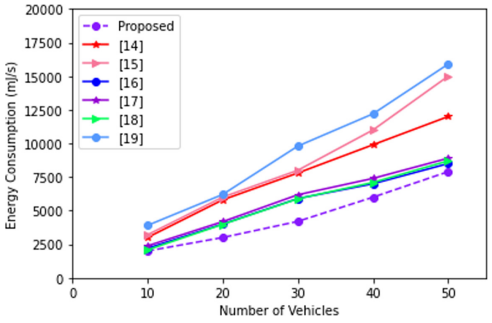

Fig. 7. Energy consumption variations

Based on the results in Fig. 7, there is a general increase in energy consumption as the number of vehicles is slowly incremented from 10 to 50. This is attributed to the surge in the number of transmitted messages when vehicle density is high. Among all these protocols, the one in [19] had the highest energy variations while the proposed protocol had the least energy variations.

5 Conclusion and Future Work

The goal of this paper was to develop an attack prevention protocol for ad hoc networks. To accomplish this, hardware based TPD was deployed, operating under realistic security assumptions. For cryptographic operations, modular multiplication and scalar point multiplication operations over ECC was deployed, coupled with simple XOR operations. The simulations results showed that this protocol had the least computation, communication, energy, and signature signing and verification costs compared with its peers. In addition, signature signing and verification analysis showed the proposed protocol had the lowest latencies. In terms of security, the proposed protocol offered unlinkability, authentication, integrity, non-repudiation, location privacy, anonymity, and was resilient against message replays and impersonation attacks. Future work lies in the formal verification of the security features provided by this protocol.

References

1. Rafsanjani, M.K., Fatemidokht, H.: FBeeAdHoc: a secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs. AEU-Int. J. Electron. Commun. **69**(11), 1613–1621 (2015)
2. He, D., Zeadally, S., Xu, B., Huang, X.: An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans. Inf. Forensics Secur. **10**(12), 2681–2691 (2015)
3. Muhammad, M., Safdar, G.A.: Survey on existing authentication issues for cellular-assisted V2X communication. Veh. Commun. **12**, 50–65 (2018)
4. Sun, M., Guo, Y., Zhang, D., Jiang, M.: Anonymous authentication and key agreement scheme combining the group key for vehicular ad hoc networks. Complexity **2021**, 1–13 (2021)
5. Bayat, M., Barmshoory, M., Rahimi, M., Aref, M.R.: A secure authentication scheme for VANETs with batch verification. Wireless Netw. **21**(5), 1733–1743 (2014). https://doi.org/10.1007/s11276-014-0881-0
6. Hamdi, M.M., Audah, L., Rashid, S.A., Mohammed, A.H., Alani, S., Mustafa, A.S.: A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs). In: 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), pp. 1–7. IEEE (2020)
7. Asaar, M.R., Salmasizadeh, M., Susilo, W., Majidi, A.: A secure and efficient authentication technique for vehicular ad-hoc networks. IEEE Trans. Veh. Technol. **67**(6), 5409–5423 (2018)
8. Mirsadeghi, F., Rafsanjani, M.K., Gupta, B.B.: A trust infrastructure based authentication method for clustered vehicular ad hoc networks. Peer-to-Peer Netw. Appl. **14**(4), 2537–2553 (2020). https://doi.org/10.1007/s12083-020-01010-4
9. Zhao, H., Sun, D., Yue, H., Zhao, M., Cheng, S.: Dynamic trust model for vehicular cyber-physical systems. IJ Netw. Secur. **20**(1), 157–167 (2018)
10. Cui, J., Tao, X., Zhang, J., Xu, Y., Zhong, H.: HCPA-GKA: a hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs. Veh. Commun. **14**, 15–25 (2018)
11. Nyangaresi, V.O., Rodrigues, A.J., Taha, N.K.: Mutual authentication protocol for secure VANET data exchanges. In: Perakovic, D., Knapcikova, L. (eds.) Future Access Enablers for Ubiquitous and Intelligent Infrastructures, vol. 382, pp. 58–76. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-78459-1_5
12. Liu, Z.C., Xiong, L., Peng, T., Peng, D.Y., Liang, H.B.: A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Access **6**, 26307–26317 (2018)
13. Azees, M., Vijayakumar, P., Deboarh, L.J.: EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **18**(9), 2467–2476 (2017)
14. Xu, Z., He, D., Kumar, N., Choo, K.K.R.: Efficient certificateless aggregate signature scheme for performing secure routing in VANETs. Secur. Commun. Netw. 2020 (2020)
15. Kumar, P., Kumari, S., Sharma, V., Li, X., Sangaiah, A.K., Islam, S.K.H.: Secure CLS and CL-AS schemes designed for VANETs. J. Supercomput. **75**(6), 3076–3098 (2018). https://doi.org/10.1007/s11227-018-2312-y
16. Mei, Q., Xiong, H., Chen, J., Yang, M., Kumari, S., Khan, M.K.: Efficient certificateless aggregate signature with conditional privacy preservation in IoV. IEEE Syst. J. **15**, 245–256 (2020)
17. Li, J., Yuan, H., Zhang, Y.: Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. Networks **317**, 48–66 (2015)

18. Kamil, I.A., Ogundoyin, S.O.: On the security of privacy-preserving authentication scheme with full aggregation in vehicular ad hoc network. Secur. Privacy **3**(3), e104 (2020)
19. Daxing, W., Jikai, T.: Probably secure cetificateless aggregate signature algorithm for vehicular ad hoc Network. J. Electron. Inf. Technol. **40**(1), 11–17 (2018)
20. Alazzawi, M.A., Lu, H., Yassin, A.A., Chen, K.: Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network. IEEE Access **7**, 71424–71435 (2019)
21. Nyangaresi, V.O., Rodrigues, A.J., Abeka, S.O.: Neuro-fuzzy based handover authentication protocol for ultra dense 5G networks. In: 2020 2nd Global Power, Energy and Communication Conference (GPECOM), pp. 339–344. IEEE (2020)
22. Islam, S.H., Obaidat, M.S., Vijayakumar, P., Abdulhay, E., Li, F., Reddy, M.K.C.: A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. Future Gener. Comput. Syst. **84**, 216–227 (2018)
23. Wu, L., Fan, J., Xie, Y., Wang, J., Liu, Q.: Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks. Int. J. Distrib. Sensor Netw. 13(3), 1550147717700899 (2017)
24. Cui, J., Zhang, J., Zhong, H., Xu, Y.: SPACF: a secure privacy-preserving authentication scheme for VANET with cuckoo filter. IEEE Trans. Veh. Technol. **66**(11), 10283–10295 (2017)
25. Raya, M., Hubaux, J.P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
26. Lu, R., Lin, X., Zhu, H., Ho, P.H., Shen, X.: ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In: IEEE INFOCOM 2008-The 27th Conference on Computer Communications, pp. 1229–1237. IEEE (2008)
27. Chim, T.W., Yiu, S.M., Hui, L.C., Li, V.O.: SPECS: Secure and privacy enhancing communications schemes for VANETs. Ad Hoc Netw. **9**(2), 189–203 (2011)
28. Shim, K.A.: CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. IEEE Trans. Veh. Technol. **61**(4), 1874–1883 (2012)
29. Liu, J.K., Yuen, T.H., Au, M.H., Susilo, W.: Improvements on an authentication scheme for vehicular sensor networks. Expert Syst. Appl. **41**(5), 2559–2564 (2014)
30. Lim, K., Manivannan, D.: An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. Veh. Commun. **4**, 30–37 (2016)
31. Zhong, H., Huang, B., Cui, J., Xu, Y., Liu, L.: Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks. IEEE Access **6**, 2241–2250 (2017)
32. Li, X., Liu, T., Obaidat, M.S., Wu, F., Vijayakumar, P., Kumar, N.: A lightweight privacy-preserving authentication protocol for VANETs. IEEE Syst. J. **14**(3), 3547–3557 (2020)
33. Huang, J.L., Yeh, L.Y., Chien, H.Y.: ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. IEEE Trans. Veh. Technol. **60**(1), 248–262 (2010)
34. Zhang, L., Wu, Q., Domingo-Ferrer, J., Qin, B., Hu, C.: Distributed aggregate privacy-preserving authentication in VANETs. IEEE Trans. Intell. Transp. Syst. **18**(3), 516–526 (2016)
35. Ying, B., Makrakis, D., Mouftah, H.T.: Dynamic mix-zone for location privacy in vehicular networks. IEEE Commun. Lett. **17**(8), 1524–1527 (2013)
36. Rajput, U., Abbas, F., Oh, H.: A hierarchical privacy preserving pseudonymous authentication protocol for VANET. IEEE Access **4**, 7770–7784 (2016)
37. Wang, S., Yao, N.: LIAP: a local identity-based anonymous message authentication protocol in VANETs. Comput. Commun. **112**, 154–164 (2017)
38. Nyangaresi, V.O., Rodrigues, A.J., Abeka, S.O.: Efficient group authentication protocol for secure 5G enabled vehicular communications. In: 2020 16th International Computer Engineering Conference (ICENCO), pp. 25–30. IEEE, Cairo (2020)

39. Zhang, J., Cui, J., Zhong, H., Chen, Z., Liu, L.: PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. IEEE Trans. Dependable Secure Comput. **18**(2), 722–735 (2019)
40. Azees, M., Vijayakumar, P.: CEKD: computationally efficient key distribution scheme for vehicular ad-hoc networks. Aust. J. Basic Appl. Sci. **10**(2), 171–175 (2016)
41. Lo, N.W., Tsai, J.L.: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Trans. Intell. Transp. Syst. **17**(5), 1319–1328 (2015)
42. Zhang, C., Lu, R., Lin, X., Ho, P. H., Shen, X.: An efficient identity-based batch verification scheme for vehicular sensor networks. In: IEEE INFOCOM 2008-The 27th Conference on Computer Communications, pp. 246–250. IEEE (2008)
43. Wei, F., Zeadally, S., Vijayakumar, P., Kumar, N., He, D.: An intelligent terminal based privacy-preserving multi-modal implicit authentication protocol for internet of connected vehicles. IEEE Trans. Intell. Transp. Syst. 1–13 (2020)
44. Li, J., Lu, H., Guizani, M.: ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Trans. Parallel Distrib. Syst. **26**(4), 938–948 (2014)
45. Calandriello, G., Papadimitratos, P., Hubaux, J.P., Lioy, A.: Efficient and robust pseudonymous authentication in VANET. In: Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks, pp. 19–28 (2007)
46. Vinoth, R., Deborah, L.J., Vijayakumar, P., Kumar, N.: Secure multi-factor authenticated key agreement scheme for industrial IoT. IEEE Internet Things J. **8**(5), 3801–3811 (2021)
47. Tzeng, S.F., Horng, S.J., Li, T., Wang, X., Huang, P.H., Khan, M.K.: Enhancing security and privacy for identity-based batch verification scheme in VANETs. IEEE Trans. Veh. Technol. **66**(4), 3235–3248 (2017)
48. Lin, X., Sun, X., Ho, P.H., Shen, X.: GSIS: A secure and privacy-preserving protocol for vehicular communications. IEEE Trans. Veh. Technol. **56**(6), 3442–3456 (2007)
49. Shao, J., Lin, X., Lu, R., Zuo, C.: A threshold anonymous authentication protocol for VANETs. IEEE Trans. Veh. Technol. **65**(3), 1711–1720 (2015)
50. Cao, X., Kou, W., Du, X.: A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. Inf. Sci. **180**(15), 2895–2903 (2010)