Mutual Authentication Protocol for Secure VANET Data Exchanges

Vincent Omollo Nyangaresi[1(✉)], Anthony J. Rodrigues[2], and Nidhal Kamel Taha[3]

[1] Tom Mboya University College, Homabay, Kenya
vnyangaresi@tmuc.ac.ke
[2] Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya
tonyr@jooust.ac.ke
[3] The World Islamic Science and Education University, Amman, Jordan
nidhal.omari@wise.edu.jo

Abstract. The initial signaling and data exchanges over open wireless transmission channels in vehicular ad hoc networks (VANETs) renders these networks susceptible to security and privacy violation attacks such as impersonation and packet replays. To curb this, a number of protocols have been proposed such as Public Key Infrastructure (PKI) based schemes, identity (ID) based schemes, anonymity based approaches and password or biometric based schemes. However, PKI based schemes have high computational overheads while ID based schemes are vulnerable to denial of service attacks (DoS). On the other hand, password and biometric based schemes employ the long term shared secrets stored in tamper proof devices (TPD) as the sole authentication factor, rendering them vulnerable to side-channel attacks. On their part, anonymity based approaches employ either digital certificates, pseudonyms or group signatures. However, these schemes do not offer trajectory privacy, conventional signature signing and verification is inefficient, and certificate storage or revocation leads to high storage and computation costs. In this paper, a multi-factor mutual authentication protocol that addressed some of these attacks is proposed. This scheme eliminates the requirement for long term storage of secret keys on TPD and remained secure even in the face of on-broad unit (OBU) active physical attack. Simulation results showed that the proposed protocol is robust against attacks such as privileged insider, masquerade and packet replay. It also preserved backward key secrecy, forward key secrecy, password secrecy and anonymity. Its performance evaluation revealed that it exhibited average computation and communication overheads, in addition to average beacon generation and verification latencies.

Keywords: Key management · Mutual authentication · Nonce · Time stamp · Privacy · Security · Session · VANETs

1 Introduction

A typical Vehicular ad-hoc network (VANET) consists of roadside units (RSUs), a trusted thirty part (Trust Authority-TA), vehicle on-broad units (OBUs), wheel rotation sensors and radars which employ IEEE 802.11p as the wireless access standard.

D. Perakovic and L. Knapcikova (Eds.): FABULOUS 2021, LNICST 382, pp. 58–76, 2021.
https://doi.org/10.1007/978-3-030-78459-1_5

Whereas sensors continually monitor driving data such as position, direction and speed, OBUs facilitate communication among vehicles as well as with RSUs through Dedicated Short Range Communications (DSRC). On the other hand, TA has to register RSUs and vehicles in addition to establishing the real identity of malicious vehicles. On its part, the RSU bridges both TA and OBU. VANETs proliferation can be attributed to emergence of smart cities and a surge in the number of vehicles, which necessitate communication among vehicles to obtain information such as traffic congestions and road conditions. Although this intelligent transportation system (ITS) offers road safety, their safety-critical communication is via open unsecured access wireless channels and hence the security of the transmitted data is a major concern [1]. In addition, authors in [2–4] and [5] explain that VANETs have numerous security and privacy (location and identity) issues owing to their open access. Further, security and privacy of communication over open wireless channels has been cited as a big challenge in VANETs [6]. As explained in [7], these open channels are susceptible to both active and passive attacks such as message interception or modification. Although numerous privacy preservation and secure authentication schemes have been developed to address these issues, majority of them have massive communication or computation overheads and have other privacy and security issues [8–10].

Researchers in [2] explain that security issues in these networks revolve around information confidentiality and integrity and hence the need for secure and user friendly authentication schemes. Moreover, authors in [11] concur that VANETs present novel security challenges that need to be addressed. Authors in [5] explain that efficient authentication among communicating entities, message integrity and preservation of privacy are key issues in VANETs, but which conventional security solutions do not fully satisfy. Further, although the fifth-generation (5G) cellular communication technology promotes the development of VANETs due to its higher capacity and data rates, and ultra-low latency, challenges such as security, privacy and efficiency remain unresolved [12]. Since 5G-VANET interfaces cyberspace and real space, attacks such as traffic analysis and privacy violation can lead to traffic accidents [13].

Although authentication can be deployed to address security issues in these networks [14], owing to the relatively high speed of vehicles and their resource-constrained OBUs, only lightweight authentication algorithms are ideal [5]. As explained in [9], conditional privacy preserving authentication (CPPA) schemes have been employed to solve privacy and security of VANETs. However, these schemes require highly tamper-proof devices (TPDs) to be installed in vehicles, which may be infeasible [9]. These authors explain that all VANET entities and transmitted messages should be authenticated to prevent attacks such as replay and masquerade that may endanger pedestrians or drivers' lives. Most TPD-based approaches require the storage of long-term secret sensitive data in TPDs. These secret key, password or biometric-based authentication techniques either employ the shared secret or stored sensitive data as the sole authentication factor, which is not adequate in VANET environment. The authentication secret information stored in TPDs is assumed to be robust against any attack since it is the axiom of these schemes that TPDs are robust against side-channel or cloning attacks and can never be compromised [15], which is unrealistic. For instance, TPDs might erase all secrets due to uneven road surfaces that may be mistakenly interpreted as malicious tampering [16]. In addition,

side-channel attacks exampled by electromagnetic radiation and power consumption analysis may be employed to learn secret information stored in TPDs.

To protect privacy in VANETs, anonymous communication is key, in which pseudonyms are deployed instead of real identities. Authors in [17] explain that the provision of efficient anonymous authentication in VANETs is very challenging. High communication and computational costs of the conventional pseudonymous authentication techniques has been cited by [18] as being detrimental to this process. Researchers in [19] point out that key management is another major issue in VANETs. Although Public Key Infrastructure (PKI) based schemes have been deployed for key management [20, 21], these schemes rely on a centralized TA which is susceptible to single point of failure [22], and require Certificate Revocation List (CRL) that generates immense communication overheads. Owing to the distributed nature and dynamic topology of VANETs, PKI based schemes are inefficient.

Identity-based signature schemes have been deployed in these networks to uphold privacy via mutual authentication. However, these approaches fall short of user privacy protection, are susceptible to attacks or have high computational complexity [23]. As pointed out in [24] and [25], the open nature of VANET environment calls for the development of robust authentication and privacy preserving techniques. Authors in [26] explain that majority of ID-based schemes are inefficient and have both high communication and computational overheads. As such, these schemes require some improvements. The contributions of this paper include the following:

I. A protocol that leverages pseudo-identities and dynamic intermediary security parameters is developed to offer both identity and location privacy.
II. Nonce and timestamps are deployed to protect the communication network against replay attacks.
III. We stochastically update pseudo-identities, intermediary security parameters and session keys to resist side-channel attacks.
IV. We utilize lightweight elliptic curve cryptography, hash functions and XOR operations in our protocol to lessen both computation and communication overheads.
V. We show that I-III above eliminate the need for TPD and by extension the single point of failure.

The rest of this paper is organized as follows: Sect. 2 discusses related work while Sect. 3 expounds on the system model employed to achieve the paper objectives. On the other hand, Sect. 4 presents results, discusses them and evaluates the developed protocol. Lastly, Sect. 5 concludes this paper and gives future direction in this research area.

2 Related Work

Security and privacy issues in VANETs have attracted a lot of attention both in the industry and academia and hence numerous schemes have been developed or proposed. Authors in [5] proposed a lightweight multi-factor authentication technique for VANETs using pseudo-identities and physically unclonable functions. However, this scheme employs certificate authority which can be a single point of failure. In addition,

the assumption that RSUs are structured into domains with each of these domains enjoying autonomous regional private materials may not always hold. Techniques based on PKI and TPD are some of the conventional security and privacy preserving approaches for VANET security but as pointed out in [27], PKI based schemes exhibit high computational and communication costs. On the other hand, TPD based schemes employ static information stored in them for authentication, but this information can be captured by adversaries through side channel attacks. For instance, PKI –based schemes developed in [16] and [28] have not only high communication overheads but also complex certificate management. Authors in [28] developed a scheme that achieved anonymous authentication and privacy tracking but which had reduced efficiency due to frequent applications for anonymous certificates from RSUs. In [29], an identity-based authentication protocol is developed for VANETs which still lacks non-repudiation and is also susceptible to replay attacks.

Authors in [30] developed an authentication technique which researchers in [31] demonstrated to offer very weak security levels. The batch verification technique developed in [32] is susceptible to both tracking and forgery attacks while the group key agreement approaches in [33] and [34] are vulnerable to tracking attacks. To reduce computation overheads, researchers in [35] proposed batch verification technique, but which is susceptible to bogus message injection attacks. Although the cryptographic puzzle based technique in [17] can prevent Denial of Service (DoS) attacks, the initial certificate verification is computationally intensive. Authors in [36] develop a lightweight privacy-preserving authentication technique that upheld both privacy and security but is still vulnerable to insider attacks, privacy breaches and masquerade attacks. To curb these issues, researchers in [37] developed an Elliptic Curve Cryptographic (ECC) based mutual authentication for VANETs, but this technique cannot assure user anonymity and is susceptible to both identity guessing and impersonation attacks.

Symmetric cryptosystem based techniques developed in [38–40] achieved fast message authentication and verification but vehicles are unable to authenticate messages independently, requiring the incorporation of RSUs. Researchers in [41] proposed group signature based schemes for privacy protection but signature verification require high computation costs. Identity based cryptography has been employed in [18] and [42] to achieve conditional privacy while alleviating certificate management issues but have high time complexities due to bilinear pairing operations. Authors in [43] developed a lightweight mutual authentication, which is susceptible to location tracking attacks. Researchers in [15] developed a lightweight message authentication scheme to thwart DoS but it exhibits long message verification delays and fails to implement mutual authentication between vehicles. Blockchain based key management techniques have been proposed for VANETs in [44–46]. However, these approaches lack automatic key update in fast and highly dynamic applications. As pointed out in [11], although blockchain boosts trust through its tamper proof nature, it renders key update and revocation cumbersome. Authors in [47] propose an RSU based authentication scheme for regular updating of the master key. However, the scheme in [47] is susceptible to both privacy attacks and impersonation attacks and is computationally intensive due to bilinear pairings. To reduce complexity in bilinear pairing, ECC based scheme has been

developed in [48], which is however vulnerable to impersonation attacks and cannot offer privacy protection [49].

A privacy-preserving authentication method has been proposed in [50], which is inefficient due to bilinear pairings. Similarly, researchers in [51] proposed a bilinear based anonymous authentication method which is still vulnerable to replay and tracking attacks and cannot ensure both forward and backward security. To boost anonymity and integrity, authors in [49] proposed an authentication scheme which is still susceptible to tracking attacks. A two-factor authentication scheme has been proposed in [52] to improve authentication efficiency. However, the scheme in [52] is still vulnerable to DoS, masquerading attack and privacy leaks. The security technique in [53] is not robust against side channel attacks and as such, authors in [42] developed a scheme to address these attacks through periodic update of data stored in TPDs. However, as pointed out by [50], signature verification in [42] generates high communication overheads.

3 System Model

Provisions for malicious vehicle certificate revocation, packet source authentication, data integrity, conditional privacy in which vehicle private information is only known by authorized entities, and non-repudiation are characteristics of robust VANET authentication protocol [54]. It has been pointed out that most of the conventional VANET authentication schemes depend on system key and long-term secret keys stored in highly secured TPD. These approaches are therefore not ideal for resource-constrained OBUs. Consequently, a robust authentication protocol should take into consideration the resource constrained nature of OBUs [5]. In addition, user's private data such as real identity and trajectory have to be protected from eavesdropping. This calls for a robust vehicle authentication protocol that is also lightweight to satisfy efficiency requirements. To attain, these goals, lightweight pseudonyms-based protocol based on ECC is developed. Elliptic Curve Cryptographic (ECC) provides robust level of security with shorter keys and hence ECC based mathematical problems have been deployed in VANET authentication schemes. As such, this paper deployed ECC discrete logarithm for security enhancement. In particular, the Elliptic Curve Discrete Logarithm (ECDL) problem and Elliptic Curve Computational Diffe-Hellman (ECCDH) problem are complex problems for any Probabilistic Polynomial Time (PPT) algorithm to solve with non-negligible probability. For both EDL and ECCDH problems, the following hold:

Definition-1: Taking $\mathfrak{f}$ as an elliptic curve group defined by prime numbers ζ and generator ϱ, E as an elliptic curve $y^2 = x^3 + ax + b \bmod \zeta$, and $a, b \in_R Z_\zeta^*$, then given two random points ϱ and $\varkappa$ of group $\mathfrak{f}$ on E, the objective of the ECDL is to find an integer $a \in_R Z_\zeta^*$ that satisfies $\varkappa = a\varrho$, where the unknown number a is difficult to calculate. Consequently, the problem of ECDL is assumed to be computationally infeasible for any PPT algorithms to solve.

Definition-2: Given two random points R and $\varkappa$ of group $\mathfrak{f}$ on E, where R = $a\varrho$ and $\varkappa = b\varrho$, the goal of ECCDHP is to compute point $ab\varrho \in \mathfrak{f}$, where $a, b \in_R Z_\zeta^*$ are two unknown integers. Since point $ab\varrho \in \mathfrak{f}$ is difficult to compute, it is assumed that the problem of ECCDH is computationally infeasible for any PPT algorithms to solve.

Definition 3: Taking point ϱ on E, scalar point multiplication of E is computed by repeated addition of this point. Let ϻ $\in_R Z_\zeta^*$, then ϻϱ = ϱ + ϱ + ⋯ + ϱ(ϻ times), where ϻ > 0.

Definition 4: The discriminant of the elliptic curve is $4a^3 + 27b^2 \neq 0$, and E forms a cyclic additive group ʧ under point addition operation ϱ + ϰ = R.

Definition 5: Hash algorithms *h(.)* encode data into fixed digits digital signatures in such a way that it is infeasible to compute original data from the enciphered digits. Any *h(.)*: (a)generates fixed-length enciphered digits for any length of input data. (b) it is straightforward to generate ₭ = *h(ɣ)* from ɣ but infeasible to generate $ɣ = h^{-1}(₭)$ from ₭. (c) Given ɣ and ₭, finding *h(ɣ)* = *h(₭)* can be computationally infeasible.

As shown in Fig. 1, the simulated VANET consisted of one AS which acted as TA, two OBUs, two RSUs, and two vehicles (V_S and V_T) all communicating through the IEEE 802.11p protocol. The OBUs recorded vehicle data such as velocity and location while RSUs connected vehicles to the internet, in addition to information exchange with passing vehicles to establish road conditions.

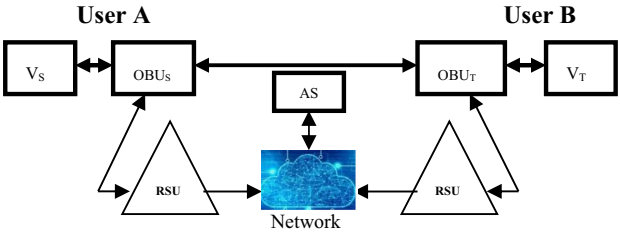

Fig. 1. VANET structure

In conventional authentication schemes, authentication of vehicles is through private keys stored in TPD which are used to generate digital signatures for each vehicle. In these schemes, TA provides RSUs and vehicles with public and private key pairs. However, the proposed protocol eliminated the requirement for the storage of private keys stored in TPD and instead, these keys were dynamically generated and refreshed using lightweight hashing functions and XOR operations. Table 1 gives the notations used in this paper and their brief descriptions.

The proposed mutual authentication protocol comprised of five major phases: *AS* parameter setting, V_i registration, login phase, session authentication, and data exchange phases. Each of these major phases had sub-steps that realized the objectives of the major phases.

AS Parameter Setting, V_i Registration & Login Phase: The first step in the proposed protocol is for the authentication server (*AS*) to register V_i (step -1) after which the *AS* selects ʂ $\in_R Z_\zeta^*$ stochastically as its secret key. It then employs one way hash chain technique to compute secure key-sets as shown in step-2, which are sent to UBU_i together

Table 1. Notations

Notation	Description	Notation	Description
AS	Authentication server	P_T	Target *OBU* public key
Ş	*AS* secret key	χ_i	Protects security of $\hbar_i$
SKS	Secure key-sets	d_j	Validation parameter
V_i	i^{th} vehicle	q_j	Parameter for computation of d_j
V_S	Source vehicle	έ	Session key
V_T	Target vehicle	tmp_c	Current time stamp of OBU_i
ƥ	$i^{th} V_i$ password	OBU_S, OBU_T	Source *OBU*, target *OBU*
$\mathfrak{l}_i$	$i^{th} V_i$ pseudo-identity	tmp_S	Current time stamp of OBU_S
$\mathfrak{l}_j$	$j^{th} V_i$ pseudo-identity	tmp_T	Current time stamp of OBU_T
η_{AI}	*AS* nonce	tmp_v	Current time of V_i
h	Hash function	‖	Concatenation operator
$\hbar_i$	User of V_i private key	⊕	Exclusive OR (XOR) operator
$\hbar_S$	Source *OBU* private key	P_i	Public key of V_i
$\hbar_T$	Target *OBU* private key	P_S	Source *OBU* public key

with public parameters $\{tf, \varrho, \zeta\}$ (phase-3) for storage (step-4). Afterwards, the V_i registration begins with the selection of its password β and computation of its pseudo-identity $\mathfrak{l}_i$ (step-5) which are utilized to compute $G\mathcal{D}$ (phase -6). In step 7, $G\mathcal{D}$ is sent to *AS* which then selects nonce η_{AI} that is used to compute parameters q_j, ξ_i, δ_i, ϵ_i (step 8), where parameter ξ_i is only known to the *AS*. In phase 9, these security parameters $\{\delta_i, \epsilon_i, \eta_{AI}, h(), tf, \varrho, \zeta\}$ are sent to $OBU_i$for buffering. In step 10, the user in V_i supplies $\mathfrak{l}_i$ and β to OBU_i after which nonce $\hbar_i$ is selected as user of V_i's private key. This is followed by the computation of V_i's public key $\mathcal{P}_i$ as well as security parameter χ_i at UBU_i (phase-11) as shown in Fig. 2. In step 12, OBU_iemploys β and δ_i to retrieve q_j that is used to derive the validation parameter d_j (phase-13), before buffering $\{\mathcal{P}_i, \chi_i, \mathfrak{l}_i, \beta\}$. Here, χ_i protects $\hbar_i$ from side channel attacks.

In phase 14, the user commences the VANET login process by inputting $\{\mathfrak{l}_i, \beta\}$ into the OBU_i which, together with the re-computed q_j using δ_i (step 15) are used to derive $\mathfrak{y}$for authenticating user of V_i (phase -16). On condition that $\mathfrak{y}$and d_j are equivalent, the user in V_i is successfully authenticated, otherwise the login request is rejected (step-17).

Session Authentication: The next procedure is session authentication between OBU_S and OBU_T which starts by having OBU_S generate nonce R_i, re-compute security key sets, *SKS* (step 18), compute beacon $\bar{Q}$, followed by security parameters $Ł_1$ and $Ł_2$ (phase 19). In step 20, the authentication message $\{\bar{Q}, \epsilon_i, \eta_{AI}, Ł_1, Ł_2, tmp_c\}$ is sent to OBU_T which then checks its freshness. If timestamp tmp_c is beyond the set range, the message is flagged as replay attack (phase-22). If this is not the case, OBU_T re-computes security parameter ξ_i and retrieves R_i (step-23). This is followed checking of the validity

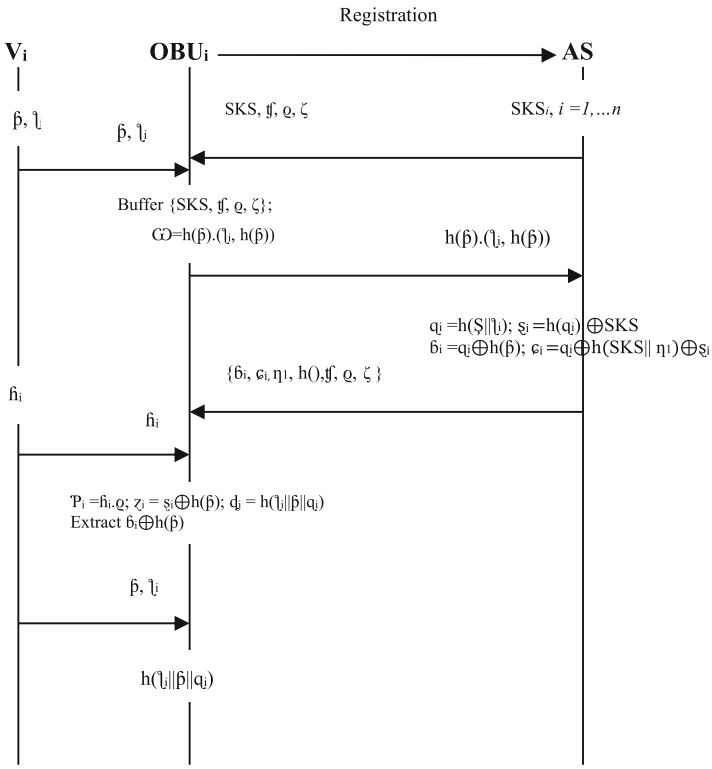

Fig. 2. Parameter setting, V_i registration and login phases

of security parameter $Ł_2$ such that if it is not valid, session authentication is rejected (phase -24). However, if it is valid, OBU_T generates nonce $Ŗ_j$ used to derive security parameter $ʒ$ and session key $ɛ$ (step-25). This is followed by the computation of security parameters $Ł_3$, $Ł_4$, and verification message $Ł_5$ (phase-26) after which message $\{ʒ, Ł_3, Ł_4, Ł_5, tmp_v\}$ is sent to the OBU_S (step-27). In phase 28, the validity of timestamp $tmp_v$is checked such that if it is invalid, the request is flagged as replay attack (step-29). However if tmp_v is within the set range, OBU_S re-computes security parameters $Ŗ_j$, $ş_i$ and session key $ɛ$ (phase-30). To fully trust OBU_T, verification message $Ł_5$ is re-computed and employed (step-31) such that if it is not valid, session authentication is terminated (phase-32). However, if it is valid, security parameter $Ł_6$ and $ϛ_i^*$are computed (step-33) before replacing security parameters $ϛ_i$ and $ηı$ with $ϛ_i^*$and $Ŗ_i$ respectively (phase-34). In step 35, OBU_S extracts *SKS* and computes security parameter $ϑ$ before buffering them as shown in Fig. 3. This ensures that an adversary cannot obtain data that can facilitate side channel attacks.

In phase 36 through 40, OBU_S sends security parameters $\{h^*(Ŗ_j||ʒ)\}$ and $\{ɛ \oplus Ł_6\}$ to OBU_T which is used to verify that OBU_S is not malicious. This marks the end of the session authentication phase and the onset of data exchange.

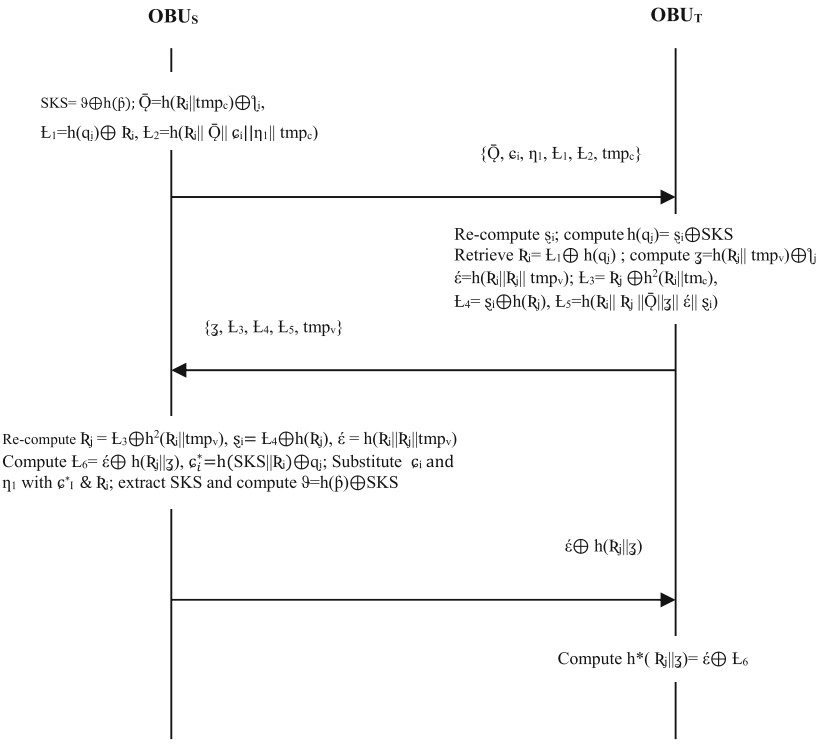

Fig .3. Session authentication

Data Exchanges: In step 41, OBU_S generate nonce R_S and beacon $\bar{Q}_S$ before computing security parameters r, $Ł_S$ and verification message $Ł_V$. Thereafter, message $\{Ł_S, Ł_V, \bar{Q}_S, tmp_S\}$ is sent to OBU_T (phase 42) where time stamp is validated (step 43 and 44) as before. If this time stamp is within the set range, OBU_T re-computes security parameter r using its own private key $ñ_T$ and OBU_S' public key P_S (phase- 45) as shown in Fig. 4. In step 46, the connection request is authenticated using $Ł_V$ such that it is rejected if $Ł_V$ is invalid (phase-47). However, provided it is valid, OBU_T chooses nonce R_T and calculates security parameters $ʒ_T$, $Ł_3$, $Ł_4$ and session key $\acute{e}$ (phase 49) before sending response message $\{Ł_3, Ł_4, ʒ_T, tmp_T\}$ to OBU_S (step-50). In phase 51, time stamp tmp_T is validated by OBU_S as before while security parameters R_T, $ℓ_T$ and session key $\acute{e}$ are re-calculated in step 53 at the OBU_S, provided tmp_T is within set range. In phase 54, the equivalence of message $\{h(ℓ_T||\acute{e})\}$ to verification message $Ł_4$ is checked as before and if it is valid, response message $Ł_5$ is generated (step-56) and sent to OBU_T (phase -57).

Upon receipt of $Ł_5$, OBU_T confirms its validity by re-calculating message $\{h(R_T||\acute{e})\}$ (step-58). If it is valid, V_S and V_T can start data exchanges (phase-61). To ensure robust security, upon completion of data exchanges, *SKS* is re-generated as shown in Fig. 5.

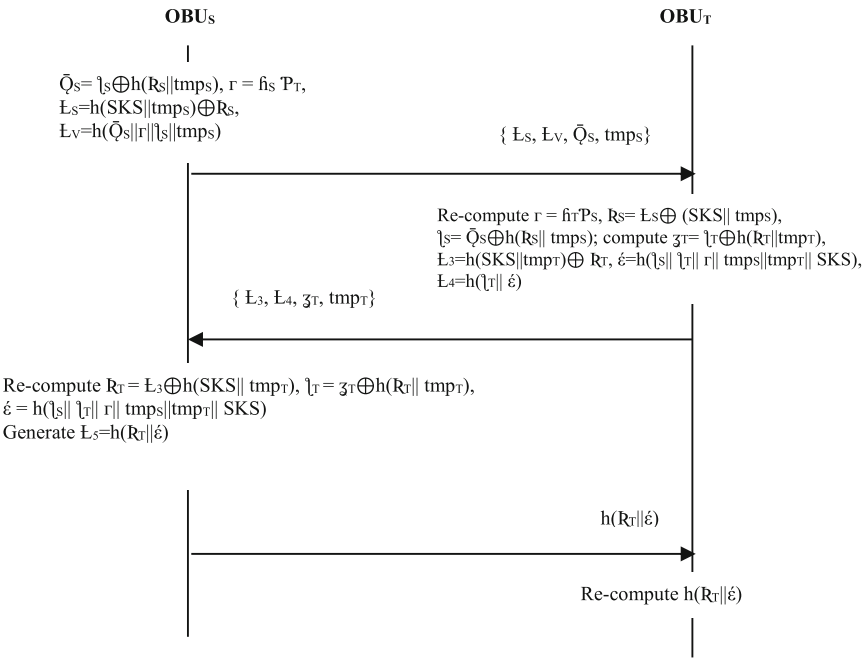

Fig. 4. Secure data exchanges

4 Results and Discussion

To simulate the proposed protocol, the parameters in Table 2 were employed. The vehicle speed was varied from 10 m/s to 50 m/s over the 4 km^2 by 4 km^2 simulation area. The number of vehicles lay between 50 and 250 while the communication range was between 200 m to 350 m. On the other hand, the simulation duration of 5 min was established to be optimum for the measurement of the required data.

Regarding the wireless communication protocol, IEEE 802.11p was deployed. The performance of the proposed protocol was then analyzed in terms of key performance indicators in VANETs. This included end-to-end (E2E) packet latency and packet delivery ratio (PDR), beacon signing and verification latencies. Afterwards, its performance was further compared with that of other mutual authentication schemes in [5, 15] and [52].

E2E Packet Latency: we sought to investigate how the number of vehicles and their speeds in the VANET environment affected network delays. To accomplish this, the generated beacon transmission under three vehicle speed scenarios were considered which included slow speed (20 m/s), average speed (30 m/s) and high speed (40 m/s) as shown in Fig. 6. It can be observed that under a particular vehicle speed scenario, as the number of vehicles increases, so does E2E latencies.

This can be attributed to the fact that an increase in the number of vehicles in VANETs lead to increased packet congestion which then increase the processing and delivery time

INPUT: $S, \beta, \mathfrak{g}, \varrho, \zeta, \eta_1, \mathfrak{f}_i, R_c, R_j, R_S, R_T$
OUTPUT: $\mathfrak{l}_j, G\mathfrak{O}, q_j, \mathfrak{s}_j, \mathfrak{b}_i, \mathfrak{c}_i, P_i, \mathfrak{z}_i, d_j, \gamma, SKS, \bar{Q}, \acute{\varepsilon}, \mathfrak{z}, Ł_1, Ł_2, Ł_3, Ł_4, Ł_5, Ł_6, \mathfrak{c}^*_i, \vartheta, \bar{Q}_S, r, Ł_S, Ł_V, \mathfrak{l}_S, \mathfrak{z}_T, \mathfrak{l}_T$

BEGIN:

1. AS registers V_i via a secure channel */* start of AS parameters setting*/*
2. Randomly select S and compute secure key sets $\{SKS_i, i = 1, \ldots n\}$
3. AS→ OBU_i: {SKS, $\mathfrak{g}$, ϱ, ζ }
4. Buffer {SKS, $\mathfrak{g}$, ϱ, ζ } in OBU_i */* End of AS parameters setting*/*
5. V_i selects its β and computes its pseudo-identity $\mathfrak{l}_j$ */* start of V_i registration*/*
6. Compute $G\mathfrak{O}=h(\beta).(\mathfrak{l}_j, h(\beta))$
7. OBU_i →AS: $\{h(\beta).(\mathfrak{l}_j, h(\beta))\}$
8. AS chooses nonce η_1 and computes $q_j = h(S||\mathfrak{l}_j)$, $\mathfrak{s}_j = h(q_j) \oplus SKS$, $\mathfrak{b}_i = q_j \oplus h(\beta)$, $\mathfrak{c}_i = q_j \oplus h(SKS||\ \eta_1) \oplus \mathfrak{s}_j$
9. AS→ OBU_i: {$\mathfrak{b}_i$, $\mathfrak{c}_i$, η_1, h(),$\mathfrak{g}$, ϱ, ζ }
10. V_i inputs $\mathfrak{l}_j$ and β to OBU_i and selects $\mathfrak{f}_i$
11. Calculate $P_i = \mathfrak{f}_i . \varrho$ and $\mathfrak{z}_i = \mathfrak{s}_j \oplus h(\beta)$
12. Using β and $\mathfrak{b}_i$, OBU_i extracts $q_j = \mathfrak{b}_i \oplus h(\beta)$
13. Compute the validation parameter $d_j = h(\mathfrak{l}_j||\beta||q_j)$ */* end of V_i registration*/*
14. V_i → OBU_i: {$\mathfrak{l}_j$,β} */* start of VANET login phase */*
15. Re-compute q_j using $\mathfrak{b}_i$ and calculate $\gamma = h(\mathfrak{l}_j||\beta||q_j)$
16. **IF** γ!= d_j **THEN:**
17. Reject login request */* End of VANET login phase */*
18. **ELSE:** OBU_S generates nonce $R_j \in Z^*_\zeta$ & compute $SKS = \vartheta \oplus h(\beta)$ */* Start of session authentication */*
19. Calculate $\bar{Q}=h(R_j||tmp_c)\oplus\mathfrak{l}_j$, $Ł_1=h(q_j)\oplus R_i$, $Ł_2=h(R_j||\ \bar{Q}||\ \mathfrak{c}_i||\eta_1||\ tmp_c)$
20. OBU_S→ OBU_T: {$\bar{Q}$, $\mathfrak{c}_i$, η_1, $Ł_1$, $Ł_2$, tmp_c}
21. **IF** tmp_c not within range **THEN:**
22. Flag as replay
23. **ELSE:** Re-calculate $\mathfrak{s}_j$ using $\mathfrak{c}_i \oplus h(SKS||\ \eta_1)$, $h(q_j) = \mathfrak{s}_j \oplus SKS$ & retrieve $R_i = Ł_1 \oplus h(q_j)$
24. **IF** $Ł_2$!=$h(R_i||\ \mathfrak{c}_i||\bar{Q}||\eta_1||\ tmp_c)$ **THEN:** Terminate session authentication request
25. **ELSE:** Generate nonce $R_j \in Z^*_\zeta$ and compute $\mathfrak{z} = h(R_j||\ tmp_v) \oplus \mathfrak{l}_j$ & $\acute{\varepsilon} = h(R_i||R_j||\ tmp_v)$
26. Compute $Ł_3 = R_j \oplus h^2(R_i||tm_c)$, $Ł_4 = s_j \oplus h(R_j)$, $Ł_5 = h(R_i||\ R_j\ ||\bar{Q}||\mathfrak{z}||\ \acute{\varepsilon}||\ s_j)$
27. OBU_T → OBU_S: {$\mathfrak{z}$, $Ł_3$, $Ł_4$, $Ł_5$, tmp_v}
28. **IF** tmp_v not within range **THEN**:
29. Flag as replay
30. **ELSE**: Re-compute $R_j = Ł_3 \oplus h^2(R_i||tmp_v)$, $s_j = Ł_4 \oplus h(R_j)$, $\acute{\varepsilon} = h(R_i||R_j||tmp_v)$
31. **IF** $Ł_5$!=$h(R_i||R_j||\bar{Q}||\mathfrak{z}||\ \acute{\varepsilon}||\ s_j)$**THEN:**
32. Terminate authentication process
33. **ELSE:** Trust OBU_T & compute $Ł_6 = \acute{\varepsilon} \oplus h(R_i||\mathfrak{z})$, $\mathfrak{c}^*_i = h(SKS||R_i) \oplus q_j$
34. Substitute $\mathfrak{c}_i$ and η_1 with $\mathfrak{c}^*_1$ & R_i
35. Using $\mathfrak{s}_j \oplus h(q_j)$, extract SKS and compute $\vartheta = h(\beta) \oplus SKS$
36. OBU_S → OBU_T: {$Ł_6$}
37. Calculate $h^*(\ R_j||\mathfrak{z}) = \acute{\varepsilon} \oplus Ł_6$
38. **IF** $h^*(\ R_j||\mathfrak{z})$!= $h(R_i||\mathfrak{z}||)$ **THEN**:
39. Flag as replay
40. **ELSE**: Trust OBU_S */* End of session authentication */*

/ Start of V_S & V_T Data Exchanges */*

41. OBU_S randomly chooses R_S and computes $\bar{Q}_S = \mathfrak{l}_S \oplus h(R_S||tmp_S)$, $r = \mathfrak{f}_S . P_T$, $Ł_S = h(SKS||tmp_S) \oplus R_S$, $Ł_V = h(\bar{Q}_S||r||\mathfrak{l}_S||tmp_S)$
42. OBU_S→ OBU_T: { $Ł_S$, $Ł_V$, $\bar{Q}_S$, tmp_S}
43. **IF** tmp_S not within range **THEN:**
44. Flag as replay
45. **ELSE**: Re-compute $r = \mathfrak{f}_T . P_S$, $R_S = Ł_S \oplus (SKS||\ tmp_S)$, $\mathfrak{l}_S = \bar{Q}_S \oplus h(R_S||\ tmp_S)$
46. **IF** $h(SKS||tmp_S) \oplus R_S$!= $Ł_V$ **THEN:**
47. Reject connection request
48. **ELSE**:
49. Randomly choose R_T and compute $\mathfrak{z}_T = \mathfrak{l}_T \oplus h(R_T||tmp_T)$, $Ł_3 = h(SKS||tmp_T) \oplus R_T$, $\acute{\varepsilon} = h(\mathfrak{l}_S||\ \mathfrak{l}_T||\ r||\ tmp_S||tmp_T||\ SKS)$, $Ł_4 = h(\mathfrak{l}_T||\ \acute{\varepsilon})$
50. OBU_T→ OBU_S: { $Ł_3$, $Ł_4$, $\mathfrak{z}_T$, tmp_T}
51. **IF** tmp_T not within range **THEN**:
52. Flag as replay
53. **ELSE:** Re-compute $R_T = Ł_3 \oplus h(SKS||\ tmp_T)$, $\mathfrak{l}_T = \mathfrak{z}_T \oplus h(R_T||\ tmp_T)$, $\acute{\varepsilon} = h(\mathfrak{l}_S||\ \mathfrak{l}_T||\ r||\ tmp_S||tmp_T||\ SKS)$
54. **IF** $h(\mathfrak{l}_T||\ \acute{\varepsilon})$!= $Ł_4$ **THEN**:
55. Reject connection request
56. **ELSE:** Generate response $Ł_5 = h(R_T||\acute{\varepsilon})$
57. OBU_S→ OBU_T: {$Ł_5$}
58. Re-compute $h(R_T||\acute{\varepsilon})$
59. **IF** $h(R_T||\acute{\varepsilon})$!= $Ł_5$ **THEN**:
60. Reject connection request
61. **ELSE:** Commence data exchange */* Secured by $\acute{\varepsilon}$ */*
62. **IF** sender window is empty **THEN**:
63. Re-compute SKS and close session

END

Fig. 5. Proposed VANET mutual authentication protocol

at the *OBUs* and *RSUs*. Considering all the three vehicle speed scenarios, it is evident that as the vehicle speed increases, E2E latencies also increase. This can be attributed to the intermittent connectivity among the vehicles and RSUs resulting from very fast motion of the vehicles.

Table 2. Simulation parameters

Parameter	Value
Vehicle speeds	10–50 m/s
Area	4 by 4 km^2
Number of vehicles	50–250
Communication range	200-350 m
Simulation duration	5 min
Wireless protocol	802.11p

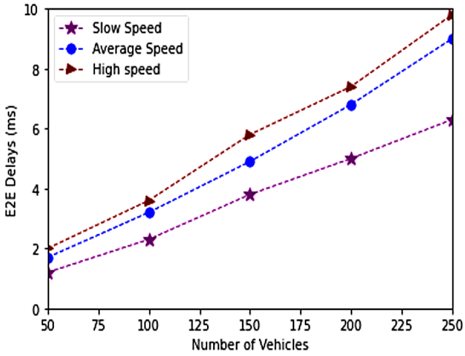

Fig. 6. E2E delays comparisons

PDR: To assess how PDR in the proposed protocol was affected by the increase in vehicle density, the same setting as that of E2E was employed. As shown in Fig. 7, the value of PDR is reduced when the number of vehicles in a VANET environment is increased.

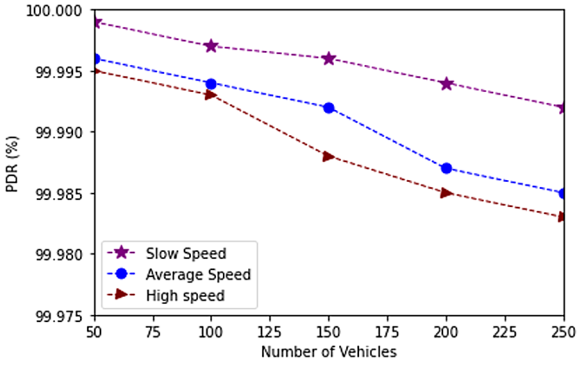

Fig. 7. PDR comparisons

The rationale for this observation is that congestion crops in with the high density of vehicles which overwhelms both *RSUs* and *OBUs*. Consequently, some of the packets may be dropped when the receiver window is full to its maximum capacity. It is clear from Fig. 7 that in all the three vehicle speed scenarios, the values of PDR remained well above 99%.

Stability: To analyze the stability of the proposed protocol, the number of vehicles in a VANET environment was increased from 50 to 250 as the value of PDR was measured. The obtained results are shown in Fig. 7, from which it is clear that PDR remained above 99.984% even in the presence of a very high vehicle density.

4.1 Security Analysis

To analyze the security features of the developed protocol, the Random Oracle model was employed. In this model, it is assumed that an adversary has access to all oracles and hence both authentication and data exchanges can be effectively controlled by an attacker. Insider attacks, attacks against anonymity, forward and backward key secrecy, password secrecy, and resilience against both masquerading and replay attacks were the specific attack models that were employed to assess the security of the proposed protocol.

Insider Attack: In this attack, it was assumed that *AS* stores β in plaintext. Although V_i sends $\{h(\beta).(\gamma_j, h(\beta))\}$ to *AS* over the communication channel, an attacker is unable to re-compute β owing to the one –way characteristic of the hash function *h()* and hence β cannot be misused.

Anonymity: In the proposed protocol, both location and identity privacy are safeguarded by the utilization of pseudo-identities γ_j, timestamps (tmp_c, tmp_S, tmp_T), random nonce (r_i, R_i, R_j, R_S, R_T), XOR operations $(\oplus)$ and hashing *h()*. As such, the interception of the transmitted parameters cannot yield location and real identity of the users.

Forward and Backward Key Secrecy: The session key $\acute{\epsilon}$ is generated from random parameters such as R_i and R_j, incorporates time stamps and is finally hashed. As such, its value is dynamically changed and consequently, an attacker with the present $\acute{\epsilon}$ is unable to discern the previous session key nor can the session key for the subsequent communication be computed.

Password Secrecy: The password β is encapsulated in other parameters such as pseudo-identity γ_j before being hashed and sent to the *AS*. Consequently, even if an attacker captures the hash value, its value cannot be determined from the one way hash.

Masquerading Attacks Resilience: During the computation of the session key $\acute{\epsilon}$, random parameters such as R_i, R_j, γ_j and time stamps are employed. Since R_i, R_j are enciphered using key q_j which is only known to *AS* and *OBU*, an adversary is unable to compromise the session key to access the communication entities' real identities.

Replay Attack Resilience: In the proposed protocol, all exchanged messages have current time stamps which are validated against the mutually agreed range. Due to these time stamp freshness checks, replayed messages are easily detected.

4.2 Performance Evaluation

To assess the performance of the developed protocol against other similar schemes, performance metrics such as computation costs, communication overheads, beacon generation and beacon verifications latencies were used.

Computation Costs: The execution times presented in [52] were adopted for this evaluation. Here, the SHA-256 hash function operation (T_{hash}) takes 0.006 ms, while the hash-based message authentication code, HMAC (T_{HMAC}) takes 0.0167 ms. Then, the goal here was to establish the duration that the proposed protocol took to login, sign and verify a single beacon. Let beacon generation be *BG* and a single beacon verification be *BV*. To login, the V_i computed the validation parameter q_j from γ_i, β, and q_j which were then hashed. Since q_j computation also involves hashing, q_j generation required two *h()* operations. Afterwards, for the login phase, OBU_i had to re-compute q_j which required one *h()* operation. For message $\bar{Q}$ signing, one *h()* operation was required. As such, login and message signing required 4 *h()*. To verify message $\bar{Q}$, Ł_2 was employed which required 3 *h()* operations. Therefore, *BG* and *BV* required a total of 7 *h()* operations. This value was then compared with those of schemes in [5, 15] and [52] as shown in Table 3.

Table 3. Computation costs comparisons

Scheme	BG	BV	BG + BV(ms)
Scheme in [5]	0.018	0.006	0.024
Scheme in [15]	0.0587	0.0227	0.0814
Scheme in [52]	0.0287	0:0167	0.0454
Proposed protocol	0.024	0.018	0.042

In the proposed protocol, the computation cost for *BG* needs four hash function operations, so the overall cost of *BG* is $4T_{hash} = 0.024$ ms; On the other hand, *BV* needs three a hash function, so the *BV* overall cost is $T_{HMAC} = 0.018$ ms. On the other hand, the scheme in [15] requires 7 T_{hash} and one T_{HMAC} for *BG* computation and hence the overall cost of *BG* is $7T_{hash} + T_{HMAC} = 0.0587$ ms. On the other hand, the message verification *BV* requires one T_{hash} and one T_{HMAC} and hence total *BV* is 0.0227 ms. For the scheme in [52], *BG* needs two T_{hash} and one T_{HMAC} and hence total BG cost is $2T_{hash} + T_{HMAC} = 0.0287$ ms. The *BV* phase requires only one T_{HMAC} and hence its cost is 0.0167 ms. Regarding the scheme in [5], *BG* needs only three T_{hash}, and hence total cost of *BG* is $3T_{hash} = 0.018$ ms, while *BV* needs only one T_{hash}, implying that *BV* cost is $T_{HMAC} = 0.006$ ms.

Communication Overhead: In this evaluation, the developed protocol was analyzed in terms of the size of the beacons transmitted across the VANET. In our protocol, a single beacon $\bar{Q}$ consisted of pseudo-identity, hash signature, nonce, and time stamp of sizes 20,

20, 2, and 4 bytes respectively, leading to an overall size of 46 bytes. This communication cost was then compared with costs for schemes in [5, 15] and [52] as shown in Table 4.

Table 4. Communication overheads comparisons

Scheme	Beacon components	Beacon Size (Bytes)
Scheme in [5]	pseudo-identity, h(), time stamp	44
Scheme in [15]	pseudo-identity, MAC sig., time stamp	47
Scheme in [52]	pseudo-identity, a truncated MAC sig., index no., time stamp	60
Proposed protocol	h(), R_i, tmp_c, ϑ_i	46

The single beacon scheme in [5] has a total of 44 bytes, which consists of pseudo-identity, hash signature, and time stamp of sizes 20, 20, and 4 bytes respectively while a single beacon for the scheme in [15] has a total size of 47 bytes comprising of pseudo-identity, MAC signature and time stamp of sizes 23, 20, and 4 bytes respectively. On the other hand, a single beacon for the scheme in [52] has a total size of 60 bytes, consisting of pseudo-identity, a truncated MAC signature, index number, and time stamp of sizes 40, 12, 4 and 4 bytes respectively, leading to an overall size of 60 bytes.

Beacon Generation and Beacon Verifications Latencies: The schemes in [5, 15] and [52] have been evaluated in terms of beacon generation and verification latencies. As such, the beacon generation and verification of the proposed protocol was compared to these schemes as shown in Fig. 8(a) and Fig. 8(b). As shown in Fig. 8(a), the scheme in [5] had the least beacon generation latency while the scheme in [15] had the greatest beacon generation latency. On the other hand, the proposed protocol's beacon generation latency was slightly higher than that of the scheme in [5] but lower than the values for both [15] and [52].

Regarding beacon verification latencies, Fig. 8(b) shows that the scheme in [5] had the least latency while the scheme in [15] had the longest latency. This observation can be attributed to the increase in the computation costs as the number of T_{hash} and T_{HMAC} operations increases in all the four schemes. Although the scheme in [5] has better performance than the proposed protocol, this scheme employs certificate authority which can be a single point of failure. Moreover, its assumption that *RSUs* are structured into domains with each of these domains enjoying autonomous regional private materials may not always hold. In addition, the scheme in [5] employs time stamps as the only technique for replay attack prevention while our protocol further introduces nonce as another layer of pseudonomy during the session key generation. The security on the scheme in [15] is mainly dependent the system key, rendering it susceptible to attacks such as man-in-the-middle and common key compromising attacks. On the other hand, the scheme in [52] is vulnerable to attacks such as DoS, masquerade and privacy leaks.

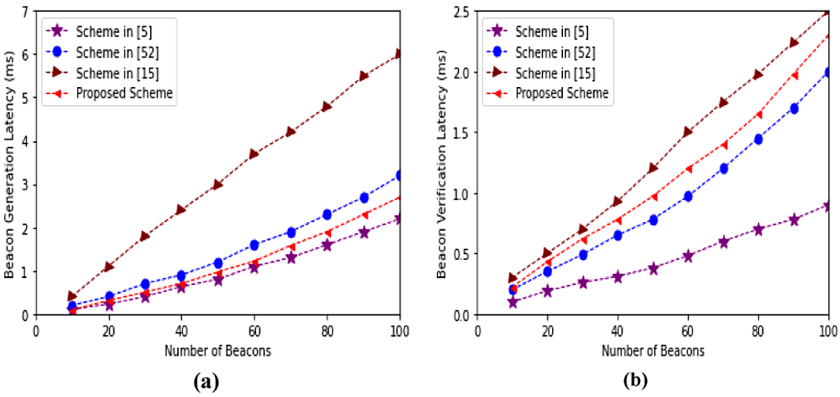

Fig. 8. (a) Beacon generation latency (b) Beacon verification latency

It further assumes a totally secure TPD that is immune against side channel attacks, an assumption that is too idealistic. Moreover, since schemes in [15] and [52] permanently store sensitive private information *TPD,* practically this information is vulnerable due to both cloning and side channel attacks against TPD.

5 Conclusion and Future Work

Many schemes have been proposed to offer security and privacy in VANET environment. However, it has been shown that these approaches either have high communication and computation overheads or are still vulnerable to other security or privacy violations. In this paper, a mutual authentication protocol for VANET entities has been developed and simulated. The results have indicated the robustness of the proposed protocol against privileged insider, masquerade and packet replay attacks. Moreover, the security analysis has shown that this protocol offers backward key secrecy, forward key secrecy, password secrecy and anonymity, which are key for the protection of sensitive data being transmitted over VANETs. Although the lightweight multi-factor authentication technique for VANETs using pseudo-identities and physically unclonable functions performed relatively better than our protocol, it is prone to single point of failure and does not assure robust pseudonomy. Future work in this area involves the deployment of the proposed protocol in a real VANET environment so that its security and performance can be evaluated in real-time.

References

1. 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)
2. Wu, L., et al.: An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular ad hoc network. IEEE Access **7**, 55050–55063 (2019)
3. Sari, A., Onursal, O., Akkaya, M.: Review of the security issues in vehicular ad hoc networks (VANET). Int. J. Commun. Netw. Syst. Sci. **8**(13), 552–566 (2015)

4. Zhang, Z., Han, B., Chao, H.C., Sun, F., Uden, L., Tang, D.: A new weight and sensitivity based variable maximum distance to average vector algorithm for wearable sensor data privacy protection. IEEE Access **7**, 104045–104056 (2019)
5. Alfadhli, S.A., Lu, S., Chen, K., Sebai, M.: Mfspv: a multi-factor secured and lightweight privacy-preserving authentication scheme for vanets. IEEE Access **8**, 142858–142874 (2020)
6. Cheng, H., Liu, Y.: An improved RSU-based authentication scheme for VANET. J. Internet Technol. **21**(4), 1137–1150 (2020)
7. Bagga, P., Das, A.K., Wazid, M., Rodrigues, J.J., Park, Y.: Authentication protocols in internet of vehicles: taxonomy, analysis, and challenges. IEEE Access **8**, 54314–54344 (2020)
8. Al-Shareeda, M.A., Anbar, M., Hasbullah, I.H., Manickam, S., Hanshi, S.M.: Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks. IEEE Access **8**, 144957–144968 (2020)
9. Wang, B., Wang, Y., Chen, R.: A practical authentication framework for VANETs. Secur. Commun. Netw. **2019**, 1–12 (2019)
10. Cui, J., Xu, W., Han, Y., Zhang, J., Zhong, H.: Secure mutual authentication with privacy preservation in vehicular ad hoc networks. Veh. Commun. **21**, 100200 (2020)
11. Ma, Z., Zhang, J., Guo, Y., Liu, Y., Liu, X., He, W.: An efficient decentralized key management mechanism for VANET with blockchain. IEEE Trans. Veh. Technol. **69**(6), 5836–5849 (2020)
12. Wang, P., Chen, CM., Kumari, S., Shojafar, M., Tafazolli, R., Liu, Y.N.: HDMA: hybrid D2D message authentication scheme for 5G-enabled vanets. IEEE Trans. Intell. Transp. Syst., 1–10 (2020)
13. Huang, Z., Liu, S., Mao, X., Chen, K., Li, J.: Insight of the protection for data security under selective opening attacks. Inf. Sci. **412–413**, 223–241 (2017)
14. Wang, D., Li, W., Wang, P.: Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans. Ind. Inf. **14**(9), 4081–4092 (2018)
15. Wang, F., Xu, Y., Zhang, H., Zhang, Y., Zhu, L.: 2FLIP: a two factor lightweight privacy-preserving authentication scheme for VANET. IEEE Trans. Veh. Technol. **65**(2), 896–911 (2016)
16. Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
17. Sun, C., Liu, J., Xu, X., Ma, J.: A privacy-preserving mutual authentication resisting DoS attacks in VANETs. IEEE Access **5**, 24012–24022 (2017)
18. Liu, J., Yong, Y., Zhao, Y., Jia, J., Wang, S.: An efficient privacy preserving batch authentication scheme with deterable function for VANETs. In: Man Ho, A., et al. (eds.) NSS 2018. LNCS, vol. 11058, pp. 288–303. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-02744-5_22
19. Qu, F., Wu, Z., Wang, F.-Y., Cho, W.: A security and privacy review of vanets. IEEE Trans. Intell. Transp. Syst. **16**(6), 2985–2996 (2015)
20. Kang, J., Elmehdwi, Y., Lin, D.: Slim: secure and lightweight identity management in vanets with minimum infrastructure reliance. In: Lin, X., Ghorbani, A., Ren, K., Zhu, S., Zhang, A. (eds.) SecureComm 2017. LNICSSITE, vol. 238, pp. 823–837. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78813-5_45
21. Xiong, W., Tang, B.: A cloud based three layer key management scheme for vanet. In: Yuan, H., Geng, J., Liu, C., Bian, F., Surapunt, T. (eds.) GSKI 2017. CCIS, vol. 849, pp. 574–587. Springer, Singapore (2018). https://doi.org/10.1007/978-981-13-0896-3_57
22. Albarqi, A., Alzaid, E., Al Ghamdi, F., Asiri, S., Kar, J.: Public key infrastructure: a survey. J. Inf. Secur. **6**(1), 31 (2015)
23. Wu, L., Wang, J., Choo, K.R., He, D.: Secure key agreement and key protection for mobile device user authentication. IEEE Trans. Inf. Forensics Secur. **14**(2), 319–330 (2019)

24. Kumar, S., Mann, K.S.: Prevention of dos attacks by detection of multiple malicious nodes in VANETs. In: International Conference on Automation, Computational and Technology Management (ICACTM), pp. 89–94. IEEE (2019)
25. Yao, Y., et al.: Multi-channel based Sybil attack detection in vehicular ad hoc networks using RSSI. IEEE Trans. Mobile Comput. **18**(2), 362–375 (2018)
26. 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)
27. Zhang, L., Men, X., Choo, K.R., Zhang, Y., Dai, F.: Privacy- preserving cloud establishment and data dissemination scheme for vehicular cloud. IEEE Trans. Depend. Secure Comput., 1–14 (2018)
28. Lu, R., Lin, X., Zhu, H., Ho, P.-H., Shen, X.: Ecpp: efficient conditional privacy preservation protocol for secure vehicular communications. In: Proceedings of IEEE 27th Conference Computing Communications, pp. 1229–1237 (2008)
29. Zhang, C., Lu, R., Lin, X., Ho, P.-H., Shen, X.: An efficient identity-based batch verification scheme for vehicular sensor networks. In: Proceedings of 27th Conference Computing Communiations (INFOCOM), pp. 246–250 (2008)
30. Shim, K.-A.: Cpas: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. IEEE Trans. Veh. Technol. **61**(4), 1874–1883 (2012)
31. 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)
32. Lee, C.-C., Lai, Y.-M.: Toward a secure batch verification with group testing for VANET. Wirel. Netw. **19**(6), 1441–1449 (2013)
33. 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)
34. 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)
35. Jiang, S., Zhu, X., Wang, L.: An efficient anonymous batch authentication scheme based on HMAC for VANETs. IEEE Trans. Intell. Transp. Syst. **17**(8), 2193–2204 (2016)
36. Chuang, M.C., Lee, J.F.: TEAM: trust-extended authentication mechanism for vehicular ad hoc networks. IEEE Syst. J. **8**(3), 749–758 (2014)
37. Zhou, Y., Zhao, X., Jiang, Y., Shang, F., Deng, S., Wang, X.: An enhanced privacy-preserving authentication scheme for vehicle sensor networks. Sensors **17**(12), 2854 (2017)
38. Zhang, C., Lin, X., Lu, R., Ho, P.-H.: RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks. In: Proceedings of IEEE International Conference on Communication, pp. 1451–1457 (2008)
39. Lyu, C., Gu, D., Zeng, Y., Mohapatra, P.: PBA: prediction based authentication for vehicle-to-vehicle communications. IEEE Trans. Depend. Secure Comput. **13**(1), 71–83 (2016)
40. Shen, J., Zhou, T., Wei, F., Sun, X., Xiang, Y.: Privacy preserving and lightweight key agreement protocol for v2g in the social internet of things. IEEE Internet Things J. **5**(4), 2526–2536 (2018)
41. Zhu, X., Jiang, S., Wang, L., Li, H.: Efficient privacy preserving authentication for vehicularAdHoc networks. IEEE Trans. Veh. Technol. **63**(2), 907–919 (2014)
42. 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)
43. Cespedes, S., Taha, S., Shen, X.: A multihop-authenticated proxy mobile IP scheme for asymmetric VANETs. IEEE Trans. Veh. Technol. **62**(7), 3271–3286 (2013)

44. Lu, Z., Liu, W., Wang, Q., Qu, G., Liu, Z.: A privacy-preserving trust model based on blockchain for vanets. IEEE Access **6**, 45 655-45 664 (2018)
45. Lasla, N., Younis, M., Znaidi, W., Arbia, D.B.: Efficient distributed admission and revocation using blockchain for cooperative ITS. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–5. IEEE (2018)
46. Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, Z., Sun, C.P.A.: Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet Things J. **4**(6), 1832–1843 (2017)
47. Bayat, M., Pournaghi, M., Rahimi, M., Barmshoory, M.: NERA: a new and efficient RSU based authentication scheme for VANETs. Wirel. Netw. **26**, 1–16 (2019)
48. 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 (2016)
49. 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)
50. Zhong, H., Han, S., Cui, J., Zhang, J., Xu, Y.: Privacy-preserving authentication scheme with full aggregation in VANET. Inf. Sci. **476**, 211–221 (2019)
51. Shao, J., Lin, X., Lu, R., Zuo, C.: A threshold anonymous authentication protocol for VANETs. IEEE Trans. Veh. Technol. **65**(3), 1711–1720 (2016)
52. Hakeem, S.A.A., El-Gawad, M.A.A., Kim, H.: A decentralized lightweight authentication and privacy protocol for vehicular networks. IEEE Access **7**, 119689–119705 (2019)
53. 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)
54. 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)