Journal of Ambient Intelligence and Humanized Computing (2023) 14:3567–3581
https://doi.org/10.1007/s12652-021-03486-1

ORIGINAL RESEARCH

SARP: secure routing protocol using anonymous authentication in vehicular Ad-hoc networks

Bhushan Yelure[1,2] · **Shefali Sonavane**[3]

Received: 13 February 2021 / Accepted: 31 August 2021 / Published online: 22 September 2021

Abstract
Vehicular Ad-hoc Network (VANET) is a collection of interconnected smart vehicles. Underlying wireless technology enables communication within vehicles as well as between road infrastructure and vehicles. Security plays a vital role during transmission of safety and important messages due to the open-access environment of VANET. Several security challenges need to be addressed in order to enable a real-time use of VANET. The significant goal of the paper is to propose a Secure Anonymous Routing Protocol (SARP) that is the extension of ACO-IBR. The SARP uses anonymous authentication methodology alongwith bilinear paring technique. The protocol verifies authenticity of the vehicles and integrity of the messages that participate in the communication process at the route discovery phase and it is resistant to various attacks. The simulation based QoS performance of the SARP routing protocol is evaluated using collision rate, packet delivery ratio, delay & throughput. SARP observed 0.023, 0.048, 0.028s less delay and 8.63, 11.52, 10.49 less overhead as compared to the ACO-IBR, GPSR and IBR. The performance is evaluated in terms of communication overhead and computational time that enhance security efficiently. It is observed that SARP requires 224.4ms computational time and 568-byte communication overhead for 100 vehicles.

Keywords VANET · Security · Anonymous authentication · Computational time · Communication Overhead

1 Introduction

Smart cities help to create an urban environment for adapting the community needs in a convenient, economical and social environment. These cities use data from people, vehicles, buildings and things. The collected data enhance the citizen's life and reduce the environmental impacts of the cities. Intelligent transportation is a building block of smart cities. Intelligent transportation system (ITS) is a domain that deals with smart transportation. VANET is an eminent technology that helps to build ITS. It is useful to attain real-time information on the road and make the decisions benefitting the transportation stakeholders. It is a network of roadside units (RSUs) and vehicles. An on-board unit (OBU) is inside the vehicle and RSUs are installed nearby roads that are helpful in the deployment of the VANET. There are various sensors associated with each vehicle that is useful for collecting observations inside a vehicle. OBU has the ability to process the information and transmits it to the vehicles or RSUs that are in the transmission range. The vehicle also attains the information for the internet with the help of RSUs (Lu et al. 2019; Manvi and Tangade 2017).

VANET consists of various types of communications such as vehicular communication (V_2V) (Azees et al. 2016), communication between RSUs and vehicles (V_2R) (Wei et al. 2019). The IEEE 802.11 task force and transportation department in the U.S. are making real effort to develop communication standards that meet the requirements of the ITS applications. V_2V and V_2R communication use wireless communication system and is achieved using the standard known as Dedicated Short Range Communication (DSRC) (Kenney 2011). Improvements in DSRC standards are currently known as IEEE 802.11p. It is widely useful

✉ Bhushan Yelure
bhushan.yelure@walchandsangli.ac.in

Shefali Sonavane
shefali.sonavane@walchandsangli.ac.in

[1] Depatment of Computer Science and Engineering, Walchand College of Engineering, Sangli, India

[2] Department of IT, Government College of Engineering, Karad, India

[3] Department of Information Technology, Walchand College of Engineering, Sangli, India

communication standard due to various characteristics such as secure communication, less transmission latency, robustness in any weather, rapid acquisition of the network and ability to deal with the frequent handover. Most of the applications in the VANET are message-oriented. Some of these are the status of the road, weather conditions, advertisements, traffic situation and video streaming. A driver can use these messages to get the real-time road situation, traffic and accordingly drive the vehicle to make comfortable and safe journey. Various communications in the VANET are shown in Fig. 1.

A hybrid approach is adopted by ACO-IBR that uses two protocols namely ACO and IBR (Yelure and Sonavane 2021). It is an intersection-oriented routing protocol and useful in the urban environment. The intersection rating with greedy is convenient for packet transmission. This improves the successful reception of the messages by minimizing overhead and delay. An inherent hybrid behavior of ACO-IBR is applicable in the urban environment that consists of intersections, traffic lights and determines the shortest route. The protocol adopts both proactive and reactive approach. Reactive approach uses route information at the setup stage to decide the route and proactive phase initiates the route maintenance. It uses latest and adaptive route information. It enables communication pairs and ants to work collectively and quickly update the latest pheromone. The protocol has efficient in overhead and required delay while transmission of packet.

ACO-IBR is designed for VANET environment and the work related to it was previously published (Yelure and Sonavane 2020). Security is of prime importance in the VANET, as there are multiple applications available related to the safety of the driver. The VANET has various features such as dynamic variation in mobility due to the speed variation, open and vulnerable wireless communication. It is mandatory to offer basic security requirements. If these

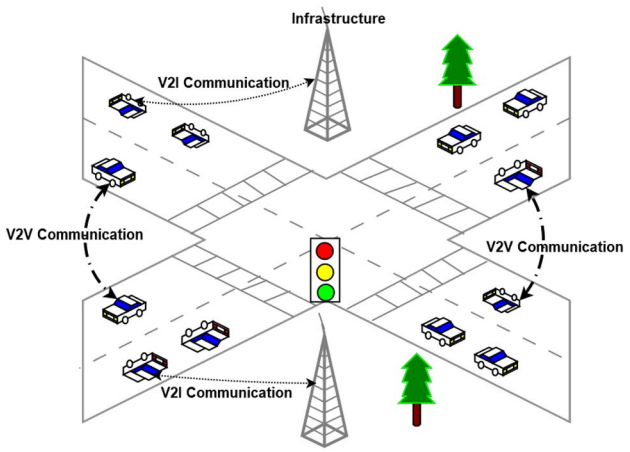


Fig. 1 Communications in VANET

security constraints are not incorporated, malicious users have a scope to attack the VANET environment and leak the information. In order to strenthen protocol and to keep malicious users away, secure communication is required between vehicles.

Authentication (Azees et al. 2017; Han et al. 2020) safeguards the message with its contents from unauthorized users. It has two stages. The user of the source vehicle (S_v) signs the message in the initial stage. Signature authentication of an expected message is done at the receiving vehicle (D_v) in the second stage. VANET supports node and message authentication where the vehicle acts as a node. Symmetric key authentication uses a single key to launch communication. An asymmetric key authentication scheme is another approach that uses a digital signature. Public and private keys that are used in asymmetric cryptography are related and unique. The public key is useful for message encryption and digital signature verification. The private key is useful for the generation of digital signature and helps to decrypt the message. The most conventional authentication technique is based on public key infrastructure (PKI) (Bhoi and Khilar 2014) and digital signature using elliptic curve cryptography (ECDSA) (Huang et al. 2020). Anonymous authentication provide users access to the VANET environment without prompting them for user credentials. As the user attempts to connect the VANET environment, the TA assigns the credentials. There are some constraints satisfied by each authentication technique and those are as follows:

1. Minimal overhead on communication and computation of the digital signature.
2. Strong and scalable authentication.
3. Provision for revocation and re-authentication.

Key management is weak in the VANET and it causes more overhead in storage and communication. It cannot provide authentication for each vehicle due to lack of nonrepudiation (Azees et al. 2017; Han et al. 2020). In recent years, researchers have suggested various authentication techniques that address the security issue in the VANET. Many of these systems use anonymous authentication. In the meantime, to evade tracking attacks, vehicles are required to modify their pseudonyms periodically. The present techniques can validate the identity of vehicles that may avoid unauthorized vehicles from interacting with other genuine vehicles as well as RSUs and thereby safeguard the privacy of vehicles. It is challenging to achieve effective authentication as the innumerable authentication requests and certificate revocation list (CRL) (Huang et al. 2020) is immense in a short duration. Afterward, there is an increase in the transmission delay as there is a growth in the size of the CRL. In this phase, unauthorized vehicles can frequently compromise the VANET. In addition to that, broadcasting the CRL to

remaining vehicles is going to reveal revocation vehicles privacy, as the legitimate vehicles have pseudonyms of revoked vehicles. Problems such as inadequate authentication and overhead of the CRL cost brings into picture effective authentication methods that use hash message authentication code (HMAC) (Jiang et al. 2016). This method avoids assailants from modifying the message and content of the message that are transmitted by the authentic vehicles and RSUs. If any anonymous vehicle acts maliciously, then TA revokes its privacy and informs it to other vehicle users in the environment. Thus, revoked user no longer be an anonymous user. The revocation technique is helpful to validate the honesty of the vehicle users. Multicast communication (Zhang et al. 2014) plays a vital role in VANET routing. There is a necessity of source authentication in multicast communication. The symmetric authentication based on point to point (P_2P) is an inefficient way and unsuitable for the source authentication. The main limitation is that it is prone to impersonation attacks. Thus, there is need to incorporate anonymous authentication in a routing protocol to achieve secure communication in the VANET. To ease this, SARP protocol is proposed that adopts anonymous authentication. SARP protocol uses a bilinear pairing. RSUs and vehicles protect privacy by self-generating their anonymous certificates. There is no anonymous certificates repository on the TA site. TA revokes the anonymity of the misbehaving vehicle to reveal its identity. TA maintain vehicle revocation list. Based on the above-discussion, contributions are illustrated as follows:

1. SARP protocol is proposed that uses an anonymous authentication technique and it is an extension of ACO-IBR. The SARP is an integrity preservation and secure communication routing protocol. Here, TA plays a vital role to achieve anonymous authentication and communication services to the vehicles. The purpose behind using TA is to relieve burden on RSU and to minimize communication and computational cost of the certificate generation. The SARP has various stages such as initialization of the vehicles and users, registration of the users, key generation, certificate generation, signature generation and certificate verification.
2. The research work analysed security of SARP routing protocol against impersonation, modification and bogus message attacks.
3. The performance of the proposed protocol is evaluated using constraints such as QoS analysis and security evaluation. The QoS analysis is evaluated using packet delivery, collision rate, delay as well as overhead and compared with existing protocols. The protocols used for the comparison are GPSR, ACO-IBR and IBR. The security evaluation uses parameters such as the computational cost of the certificate and communication overhead. The various security protocols such as BLS, ECPP, CPAS and CPAV are used for the comparative analysis of computational cost. The CPPA, CPAS and PACP protocols are used for the communication cost comparison. Observation of performance and security evaluation shows that SARP preserves stability within security and lightweight in terms of computational cost of the certificate and communication overhead.

The outline of the paper is as follows. The related work is surveyed in Section II. The Section III consists of the security environment and the system model. The proposed SARP and its methodology is discussed in Section IV, followed by the security analysis in Section V. Section VI is dedicated to performance analysis and discussion. Conclusion and further scope are discussed in final section.

2 Related work

Many researchers have contributed towards the security in the VANET by improving authentication techniques. The major emphasis is on the techniques that use pseudonyms that effectively preserve the privacy of the vehicles. TA is required to change the pseudonyms frequently. Most of the techniques that use ECC are based on a bilinear map. This technique aims at avoiding privacy-related attacks. CPPA (Raya and Hubaux 2007) uses anonymous certificates. This uses improved PKI to guarantee authentication and integrity. The set of public and private keys and resultant certificates are preloaded into vehicles OBU that hide the real identity of the vehicle. The OBU makes random selection of public and private key to ensure security. Huge storage is required to preserve keys and the resultant certificates in the vehicle and TA site. When a user submits an erroneous message, it is challenging to establish the true identity of an attacker, so that the authority must perform an exhaustive search of all stored certificates. ECPP (Lu et al. 2008) protocol is proposed that uses bilinear map to attain the conditional privacy of the vehicles and overcomes weaknesses in the CPPA technique. RSU is useful to issue various anonymous keys for vehicles that avoid tracing the communication, but it incurs more delay as it uses the pseudonym. The vehicles completely rely on RSU to obtain pseudonyms with their keys for communication. RSU informs generated pseudonyms and keys to TA before it issues to the vehicle. Therefore, there is a scope for the RSU to be compromised and the environment is open to the attacks. The PACP (Huang et al. 2011) uses TA to generate pseudonyms with a longer time duration. These pseudonyms are considered as a ticket and used to attain tokens from the RSU. Vehicles use these tokens to get the pseudonyms and vehicular communication is achieved. RSU assigns a token to the vehicle depending

on the ticket allocated by TA without knowing some information about the vehicle. RSU does the mapping of tickets with the token. The anonymity of the vehicles is increased as a result of mapping same token to the multiple tickets. TA is dependent on RSU to obtain token for its ticket to identify vehicles from its aliases in the revocation. Short signature (Boneh et al. 2004) is used in vehicular communications. Group signature (Chaum and van Heyst 1991) methodology is suggested in which one of the members from the group signs the message. In case of any dispute, the user identity is revealed about the originator of the signature. In group signature technique (Lin et al. 2007), authentication is provided to the group of vehicles. Anonymous keys related to the respective vehicles are not required to persist in the OBU. If any of vehicles are behaving maliciously, then TA can track that malicious behavior of a vehicle. The revocation list is available at the vehicle site to prevent communication with the vehicle being revoked. Thus, the scheme is suitable for the small network because verification process is time-consuming for the large network. ECPB (Wang et al. 2016) uses batch authentication and group signature techniques. This scheme verifies the validity of the group membership when a vehicle is applied for group membership. It also ensures active participation of a vehicle in the group. There is a slight improvement observed in the verification time and average latency. HMAC (Hash Message Authentication Code) (Liu et al. 2015) is used in the CPPA technique. It is a key agreement protocol executed between the RSU and vehicle. The vehicle uses separate private, public keys and the certificates to communicate with the vehicle or RSU. It requires a huge information storage. DDSARP (Imran et al. 2015) a geographical location based protocol is a combination of ALERT (Shen and Zhao 2011) and GPSR (Karp and Kung 2000; Silva et al. 2019). It has emphasis on bursty traffic along with node-to-node encryption. The protocol uses a greedy method and uses position of the router and destination of packet. ALERT protocol is used to achieve anonymity and GPSR is used for routing process. SHARP (S and S 2015) is a cluster based routing protocol. The nodes are clustered based on their position and range. Anonymous routing is implemented using RSA-based cryptography in cluster based routing. SHARP offers route, source and destination anonymity. Encryption based inter group routing is established in SHARP. Anonymity can be enhanced by encrypting the intra-group communication. Therefore, the proposed SARP routing protocol based on an anonymous authentication. This protocol fulfils the security requirement by preserving real identification of the user from other users in the VANET. The protocol also verifies message integrity by confirming the anonymous signature of each message. Related to QoS parameters, it minimizes overhead, collision rate and delay required for the transmission of the messages and improves the PDR. Table 1 shows various notations.

3 Security environment for VANET

This section introduces various security attributes used in the VANET along with system model and concept of the bilinear mapping.

3.1 Security attributes

When the environment has authentication, only genuine users can make use of the environment. It is also possible to prevent several harmful attacks similar to impersonation and Sybil. Authentication is the prime defense methodology against fake vehicular messages. As per DSRC standard, every vehicle in the VANET regularly broadcasts safety messages that comprise speed, location and traffic status. In dense scenarios, there is a possibility that vehicles receive multiple safety messages at the same instant of time. The communication time between vehicles is less due to speed and dynamic topology. An authentication (Arif et al. 2019; Azees et al. 2017) scheme possesses the ability to verify multiple messages in a limited time to satisfy the computational efficiency criterion. Any illicit action of illegal users can equally harm people's life. So, it is probable that such user avoids receiving the ownership of sent packets and its contents. Non-repudiation is useful to identify such negotiated nodes. In case of any dispute, non-repudiation guarantees that the sending and the receiving side of the data cannot reject its transmission and reception. When integrity is provided, then it is ensured that the legitimacy of the message and its contents are preserved. This process verifies the content of the message at the sender and receiver side. Integrity ensures that the attacker does not manipulate the sent message. Availability (Arif et al. 2019; Han et al. 2020) ensures that the network is continuously running and information is accessible to the users at any time. In VANET, the wireless channel is always ready to accept the safety messages. Confidentiality (Arif et al. 2019; Bhoi and Khilar 2014) is the ability to avoid illegal and unauthorized vehicles from retrieving message content. Only designated vehicles have permission to access the data. Fig. 2. exemplifies the security attributes such as availability, confidentiality, data integrity, privacy, authentication and non-repudiation (Tyagi and Dembla 2017).

The actual identity of every vehicle is kept private from the other users in the environment that ensures vehicle's privacy against attacks. TA has potential to track the real identification of the vehicle to interrupt the traffic.

If any anonymous vehicle acts maliciously then trusted authority in the VANET revokes its privacy and informs it to other vehicle users in the environment. As a result,

Table 1 Notation table

Notation	Significance
G_1, G_2, G_T	Cyclic groups
q	Prime number
e	Bilinear map
g_1, g_2	Generator of G_1, G_2 respectively
X_1, X_2	Master keys
x, y	Random numbers used in the initialization
n_i	Random number used in the key generation
$P_b(k)$	Short time public key used in the certificate generation
H	Hash function
UID_{vi}	Unique user identity
BID_{vi}	Bogus user identity
UID_{rsui}	Unique identity of RSU
BID_{rsui}	Bogus identity of RSU
Z_q^*	Finite field
TA	Trusted authority
A_i	Random number used in the registration
E_i	Offline registration key
$m_1, m_2, ..., m_k$	Temporary short time private key used in the certificate generation
A_k	Authorization key
μ, k_1, k_2	Random numbers used in the certificate generation
T_i	Activation key
S	Sender vehicle certificate
$\gamma_u, \gamma_v, \lambda, \lambda_1, \lambda_2$	Random number selected while certificate generation
$Sign$	Short time anonymous signature
S_{cert}	Anonymous short time certificate at the sender
Msg	Anonymous message
$H(m)$	Message digest
R_{cert}	Anonymous short time certificate at the receiver
S_v	Source vehicle
D_v	Destination vehicle
$CPPA$	Conditional Privacy-Preserving Authentication
BLS	Boneh Lynn Scheme
$ECPP$	Efficient Conditional Privacy Preservation
$PACP$	Pseudonymous Authentication-Based Conditional Privacy
$CPAS$	Conditional Privacy-Preserving Authentication Scheme
$CPAV$	Computationally Efficient Privacy Preserving Anonymous Authentication
$DDSARP$	Dynamic Data Secure Anonymous Routing Protocol
$SHARP$	Secured Hierarchical Anonymous Routing Protocol

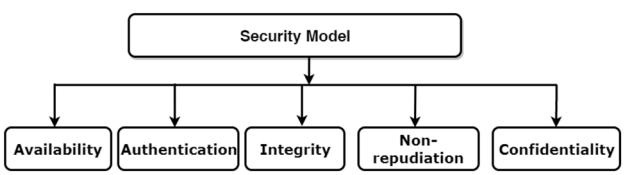


Fig. 2 Security attributes useful in VANET

revoked user no longer be an anonymous user. The revocation technique is helpful to validate honesty of the vehicle users.

3.2 System model

The framework of the proposed security system is represented in Fig. 3. There are three significant components specifically the TA, static RSU and OBU fitted inside mobile vehicles. A backbone network is useful for association of RSU and TA through the internet.

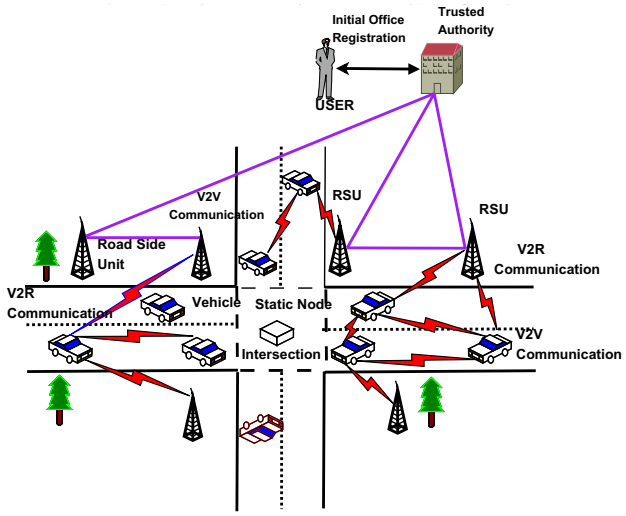


Fig. 3 System Model for the secure VANET environment

cles are roaming from one zone to another due to mobility support. During roaming, the legitimacy of the vehicle is validated using the respective TA's public key. After the successful registration, TA also issues basic security parameters to the vehicles and RSUs.

RSU is a static infrastructure that is deployed nearby road, and it works as a bridge between the RSU and TA. Wired connection is established between RSU and TA. RSU use a wireless channel to interact with vehicles within the transmission range. DSRC standard is applied in vehicles and RSUs to accomplish communications. RSU is trusted, but in partial manner, i.e. negotiation is possible with RSU to reveal private data to adversaries. If RSU is negotiated, then the negotiated RSU is detected in significantly less time.

Each vehicle has OBU that are fitted inside the vehicle to achieve communication with vehicles and RSUs. OBU periodically transmit direction, position and speed to other vehicles that alert drivers regarding present traffic situations as well as it evade road accidents.

3.3 Bilinear pairing

Bilinear pairing uses three multiplicative (cyclic) groups specified by G_1, G_2 and G_T. They have the same order with large prime number q. The g_1 is the generator of G_1, g_2 is the generator of G_2 and $\psi\ (g_2) = g_1$ that indicates an isomorphism from G_2 to G_1. The bilinear map is represented by $e: G_1 \times G_2 \rightarrow G_T$ and it has to satisfy bilinearity, computability and non-degeneracy.

1. Bilinearity-

   If $e\ (g_1^x, g_2^y) = e\ (g_1, g_2)^{xy}$ where $g_1 \in G_1$, $g_2 \in G_2$ and $a, b \in Z_q^*$, where $(Z_q^* = [1, .., q-1])$ then $e: G_1 \times G_2 \rightarrow G_T$ is said to be bilinear.
2. Computability-

   The bilinear map $e: G_1 \times G_2 \rightarrow G_T$ is computed in an easy way using an algorithm efficiently.
3. Non-degeneracy-

   $e\ (g_1, g_2) \neq 1 G_T$.

4 Design of SARP

The SARP uses ACO-IBR routing protocol as a basis. In addition to that, SARP incorporates an anonymous authentication technique to make it secure and accomplish secure communication in vehicles. SARP consists of various stages such as initialization of the vehicles and users, registration of the users, key generation, certificate generation, signature generation and certificate verification.

4.1 Initialization

TA initializes system parameters. To initialize the system, the applicable bilinear parameters are G_1, G_2, G_T, e and q. TA elects two random numbers x and y that belong to Z_q^* and act as the master private key. They are useful for the computation of two numbers such as

$$X_1 = g_1^x \quad X_2 = g_2^y \tag{1}$$

TA represents secure cryptographic hash function as shown in equation 2.

$$H: (0,1)^* \rightarrow Z_q^* \tag{2}$$

System parameters published by the TA are as follows.

$$param = (q, e, g_1, g_2, G_1, G_2, G_T, X_1, X_2, H) \tag{3}$$

4.2 Registration and key generation

In registration, vehicle users communicate with the TA. Personal data of the vehicle users are submitted to the TA. Registered vehicle users are then considered as a VANET user. After the user registration, TA initiates the process of key generation and generates the required keys for every participating vehicle. For this, TA generates unique user identity (UID_{vi}) and bogus identity (BID_{vi}) for the vehicle user in the VANET. To get the bogus identity, TA selects a random number n_i that belongs to Z_q^* and evaluates $BID_{v_i} = g_1^{n_i+x} \mod q$. RSU generates bogus identity (BID_{rsui}) by using the same process. TA is responsible for the mapping of exclusive user identity and bogus identity. The purpose of generating bogus identity is to validate the origin of a

message source. When these identities are withdrawn, they do not provide any information about the VANET users and do not reveal privacy of the vehicles and RSU users. Lastly, TA uses a random number $A_i \epsilon Z_q^*$ and evaluate $T_i = g_1^{A_i+x+y}.(UID_{vi}, BID_{v_i}, T_i^y)$. T_i^y is stored in the tracking list repository by TA. Authorization key A_k=(BID_{vi}, T_i, E_i) is returned to the user in an offline way with the help of smart card to prevent various online attacks. Here, $E_i = g_1^{-n_i} \mod q$. Then the user stores A_k in the tamper proof device (TPD). When the registration is completed successfully, then vehicle user does not interact further with TA. RSU is an interface between vehicle users and TA for future interactions that require registered user credentials from TA.

4.3 Certificate generation

VANET users make use of A_k for generation of an anonymous certificate that is required for further communication in the VANET. Every VANET user is going to select random numbers $m_1, m_2, \ldots, m_l \epsilon Z_n^*$ where $l \leq n$. These random numbers act as a temporary private key for short time and useful for the computation of respective public key $P_b(k) = g_2^{m_k}$ for k =1, 2, .., l. For every $P_b(k)$, VANET users compute an anonymous certificate that is a short time in nature. Initially, $\mu, k_1, k_2 \epsilon Z_q^*$ are selected randomly by the user and γ_u, γ_v, λ, λ_1, λ_2 are evaluated and is shown by the following formulations:

$$\gamma_u = X_2^{\mu} \tag{4}$$

$$\gamma_v = T_i.X_1^{\mu} \tag{5}$$

$$\lambda = (\mu + r_k) \mod q \tag{6}$$

$$\lambda_1 = \gamma_u^{\mu+k_1} \tag{7}$$

$$\lambda_2 = \frac{\gamma_u^{\mu+k_1}}{\gamma_v^{\mu+k_2}} \tag{8}$$

After evaluation of γ_u, γ_v, λ, λ_1, λ_2 VANET user calculates the certificate S as given below.

$$S = H(BID_{vi} \| X_1 \| X_2 \| E_i \| \gamma_u \| \gamma_v \| P_b(k) \| \lambda \| \lambda_1 \| \lambda_2) \& \delta_1, \delta_2 \tag{9}$$

$$\delta_1 = (m_k - k_1) \mod q \tag{10}$$

$$\delta_2 = (m_k - k_2) \mod q \tag{11}$$

Lastly, the VANET user-produced certificate S_{cert} and it is known as an anonymous certificate.

$$S_{cert} = (P_b(k) \| E_i \| BID_{vi} \| \gamma_u \| \gamma_v \| S \| \lambda \| \delta_1 \| \delta_2) \tag{12}$$

When the vehicle moves into the new geographical area, TA of the new geographical area is used to authenticate vehicle with the help of the TA's public key of the registered area. In other words, when a vehicle moves into the new TA area, it sends an anonymous message (Msg) to the new TA. Here, S_{cert} is an anonymous certificate.

$$Msg = (M \| Sign \| P_b(k) \| S_{cert}) \tag{13}$$

By using the anonymous certificate, N_i is evaluated with the help of two parameters such as E_i, BID_{vi} and it is represented as follow:

$$N_i = E_i \times BID_{vi} = X_1 \tag{14}$$

4.4 Signature generation

By using anonymous key, the VANET user generates a short signature ($sign$) that is anonymous. It is useful for preserving authenticity and the integrity of the message M. Then, M is broadcasted. The $sign$ and M are represented as follow:

$$Sign = g_1^{\frac{1}{m_k + H(M)}} \tag{15}$$

$$Msg = (M \| Sign \| P_b(k) \| S_{cert}) \tag{16}$$

4.5 Certificate verification

The S_v sends the Msg to the D_v. At the receiver end, it cannot directly verify the Msg. The receiver validates the legitimacy of source of the Msg, and receiver evaluates N_i, λ_1', λ_2'.

$$N_i = E_i \times BID_{vi} \tag{17}$$

$$\lambda_1' = \frac{\gamma_u^{\lambda}}{\gamma_u^{\delta_1}} \tag{18}$$

$$\lambda_2' = \frac{\gamma_u^{\lambda} \gamma_v^{\delta_2}}{\gamma_u^{\delta_1} \gamma_v^{\lambda}} \tag{19}$$

Then the receiver computes R_{cert} and it is compared with S_{cert}. If it matches ($S_{cert} = R_{cert}$), the authentication of the source is validated by the receiver and it receives a public key and the anonymous certificate. As the condition does not hold, then the message is rejected by the receiver. The recipient validates the duplicate identity of S_v and it ensures

that only genuine vehicles participate in the communication. The R_{cert} is represented as follows:

$$R_{cert} = H(BID_{vi} \| N_i \| X_2 \| E_i \| \gamma_u \| \gamma_v \| P_b(k) \| \lambda_1' \| \lambda_2') \quad (20)$$

The Fig. 4. and algorithm 1 illustrates stepwise flow of the SARP.

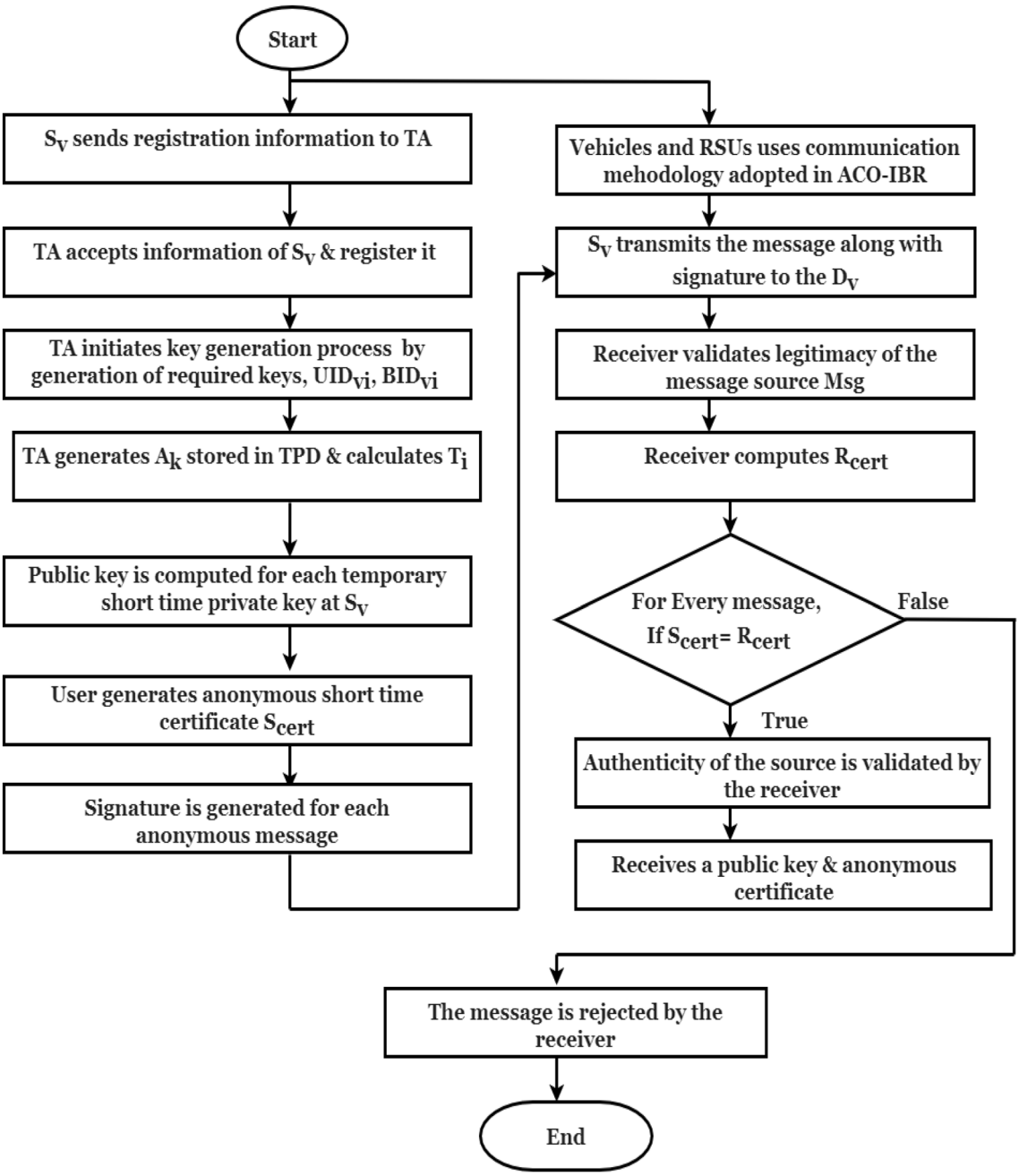


Fig. 4 Stepwise procedure for the SARP protocol

Algorithm 1: SARP algorithm pseudo-code

Data: TA initializes system parameters. TA selects random numbers x, y as master private key and H as a hash function.
Result: Secure communication between S_v and D_v.
Registration
S_v submits the personal data to the TA.
TA accepts information of S_v and register S_v.
Registered vehicle users are valid VANET user.
Key Generation
TA initiates the key generation process.
TA generates the required keys for vehicle.
TA generates UID_{vi} & BID_{vi} for the vehicle user in the VANET.
TA generates A_k= (BID_{vi}, T_i^y, E_i) and stored in TPD.
Vehicles compute distance between vehicles and RSUs using mehodology adopted in ACO-IBR.
TA computes $T_i = g_1^{\frac{1}{A_i+x+y}}.(UID_{vi}, BID_{v_i}, T_i^y)$.
Source vehicle
for *temporary short time private key* $m_1, m_2, ..., m_l$ **do**
  Public key $P_b(k) = g_2^{m_k}$ is computed.
end
for *every* $P_b(k)$ **do**
  User generates anonymous short time certificate S_{cert}.
  Signature is generated for each anonymous message.
  S_v transmits the message along with signature to the D_v.
end
Destination vehicle
The receiver validates legitimacy of the message source Msg.
Receiver computes R_{cert}.
for *Every message that is transmitted* **do**
  if S_{cert}= R_{cert} **then**
    Authenticity of the source is validated by the receiver.
    Receives a public key & anonymous certificate.
  else
    The message is rejected by the receiver.
  end
end

5 Security analysis

This section describes various attacks and their resistance on the proposed SARP protocol.

5.1 Impersonation attack

It is a kind of attack in which an attacker may claim to be a legitimate vehicle or RSU to cheat vehicular nodes by disguising identity of the vehicles. To carry out an impersonation attack, malicious user determines temporary short-term keys owned by a valid vehicle and private key of the respective vehicle supplied by TA. For this purpose initially, an adversary uses $\gamma_v = T_i.X_1^{\mu}$ the value that is derived from S_{cert}. The value of μ is a randomly selected number thereby value of γ_v is random. It is impossible to get a short time private key and μ to break the generated anonymous certificate. In addition, an attacker cannot compromise the registration process as it happened offline and the TA is involved in it. Thus, the SARP has resistance to the impersonation attack.

5.2 Message modification attack

Each vehicle user participates in vehicular communication by broadcasting an anonymous message. In the message, an attacker is having scope for the content modification while doing transmission through a wireless medium. Thus, there is a challenge to preserve the message integrity and source authentication. At the time of message generation, signature is attached with the message to guarantee integrity of the message. In addition to that, an anonymous certificate is also attached along with the message generated to achieve the source authentication. Signature attached with the message is $Sign = g_1^{\frac{1}{m_k+H(M)}}$. Here, m_k is a short time private key and it is temporary. Since this is a private key, only the corresponding vehicle knows it, and no other users can create the same signature. To reveal the signature, it is mandatory to know m_k, but it is changing periodically so it is a difficult task to achieve further communication. In addition to that, the authorization key (A_k) is useful in the process of certificate generation. A_k is securely issued to the vehicle by TA during the registration process. Therefore, no other users can forge the data and certificates without knowing the A_k and m_k.

5.3 Bogus message attack

Malicious users require BID_{vi} and E_i to calculate the value of N_i that is $N_i = E_i \times BID_{vi}$. Moreover, these values are calculated offline in the registration phase. Furthermore, correctness of the received message is validated by the signature attached to it. If the bogus message enters in the VANET, verification process fails and the bogus message gets discarded. Therefore, proposed protocol withstand against the bogus message attack.

5.4 Nonrepudiation

If the packet is delivered from S_v to the D_v, it does not repudiate. As D_v receives message, R_{cert} validates the message received by D_v and message integrity is achieved with a signature attached to the message. When there is a dispute, D_v takes the help of TA by sharing the message. By observing the message, it becomes easy for TA to recognize actual

identity of the S_v by the information available with TA. Afterward, TA can reveal the S_v's privacy and it is revoked.

6 Performance analysis and discussion

Simulation-based performance of the SARP is evaluated. Performance analysis is evaluated in terms of two aspects such as QoS evaluation of the routing protocol and security evaluation.

6.1 QoS evaluation

QoS evaluation of the SARP is evaluated in terms of PDR, Overhead, Delay, Collision Rate and Throughput. The trace files are created for various vehicle density ranging from 50-100 and used as an input to the simulation. VANETMobiSim (Ben Mussa et al. 2015; Harri et al. 2009) is the mobility generation tool used for the generation of traces. The simulation is executed for 300 s using NS 2.35 (Ben Mussa et al. 2015; Samatha et al. 2017). The performance of the SARP is compared with the ACO-IBR, GPSR and IBR protocols. ACO-IBR is a hybrid routing protocol that adopts the behavior of ACO and IBR. GPSR is a prime protocol in the position based category and IBR is intersection oriented routing that is the extension of position based routing. The simulation settings are listed in Table 2.

PDR indicates the successful data transmission of the sent packets. Higher PDR is an indication of the effectiveness of routing protocol. SARP attains 2.26%, 0.69% and 0.34% better PDR for 50, 60 and 70 vehicles. ACO-IBR attains 2.01%, 3.41% and 3.28% better PDR for 80, 90 and 100 vehicles. SARP attains 5.21%, 4.91%, 4.92%, 3.84%, 2.96% and 4.31% higher PDR as compared to GPSR for various vehicle densities ranging from 50 to 100. SARP attains 2.72%, 2.56%, 2.96%, 2.26%, 1.23% and 2.51% higher PDR as compared to IBR for various vehicle densities ranging from 50 to 100. The results for the PDR are as shown in the Fig. 5.

Table 2 Simulation settings

Parameter	Simulation value
Simulation time	300s
MAC protocol	IEEE 802.11p
Radio-propagation model	TwoRayGround
CBR connections	15
Communication range	250m
Mobility traces	IDM-IM using VANETMobiSim
Number of vehicles (nodes)	50–100
Vehicle speed	5–24 m/s
Packet size	512-byte
Evaluated routing protocols	ACO-IBR, GPSR, IBR and SARP

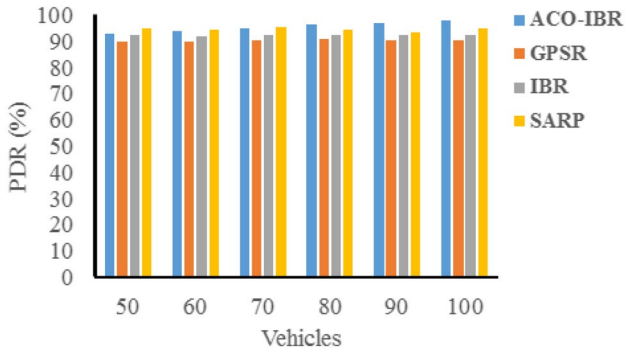


Fig. 5 PDR performance of SARP

Delay is the transmission time taken by the message from the S_v and D_v. SARP requires 0.020 s, 0.024 s, 0.029 s, 0.027 s, 0.024 s and 0.017 s less delay for transmission of messages as compared to ACO-IBR for 50, 60, 70, 80, 90 and 100 vehicles respectively. As compared to GPSR and IBR, SARP requires 0.049 s, 0.059 s, 0.039 s, 0.049 s, 0.050 s, 0.047 s and 0.029 s, 0.029 s, 0.028 s, 0.029 s, 0.030 s, 0.027 s less delay while transmitting messages. The performance of delay is depicted in Fig. 6.

Overhead is the ratio of generated control packets and total data packets that have been successfully delivered. The large number of control packets are generated in ACO-IBR specifically in case of 90 and 100 vehicles, so ACO-IBR produces high overhead as compared to SARP. SARP generates 0.72, 0.29, 1.15, 22.36 and 27.65 less overhead for 50, 60, 80, 90 and 100 vehicles. In case of scenario having 70 vehicles, ACO-IBR generates 0.39 less overhead and is shown in Fig. 7. As compared to GPSR and IBR, SARP generates 1.57, 1.91, 1.62, 3.78, 26.90, 33.35 and 0.80, 0.97, 0.69, 3.03, 25.59, 31.90 less overhead for various vehicular densities.

Throughput is presented as maximum data transmitted in time unit and measured in kbps. SARP generates higher throughput as compared to ACO-IBR except scenario of 80 vehicles. 1.74 kbps, 0.48 kbps, 4.13 kbps, 42.67 kbps and

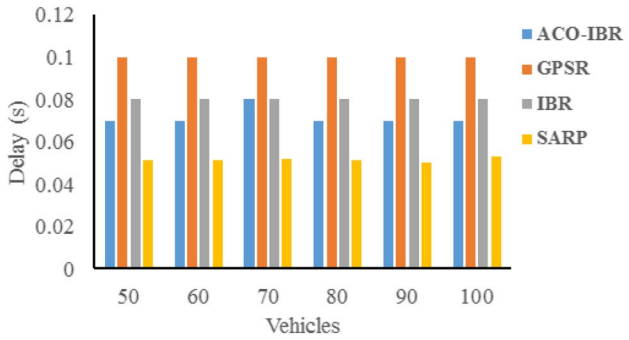
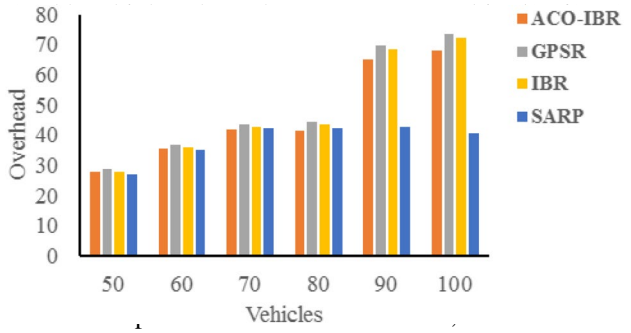


Fig. 6 Delay performance of SARP



cles. When there is an increase in the vehicles beyond 70, ACO-IBR records less collision. In case of GPSR and IBR protocols, SARP observes less collision. The collision rate

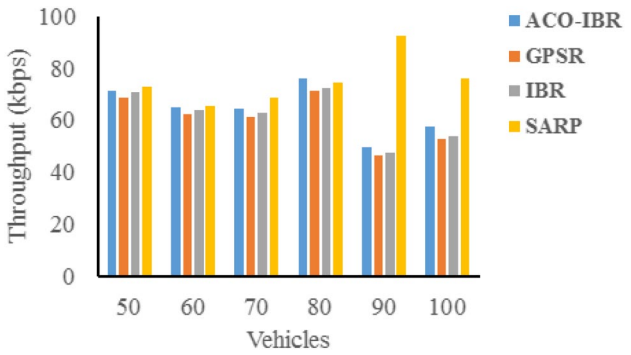


Fig. 8 Throughput performance of SARP

results are depicted in Fig. 9 and the simulation results are shown in Table 3.

6.2 Justification

Vehicular density has an influence on the QoS performance of the routing protocol. In SARP, for vehicles in between 50 and 70, enhancement in the PDR and less collision rate is observed. In the range of 80–100 vehicles, as vehicles participating in the communication are increasing, ACO-IBR has better PDR and less collision rate as compared to SARP. SARP has 4.35%, 2.37% better successful average

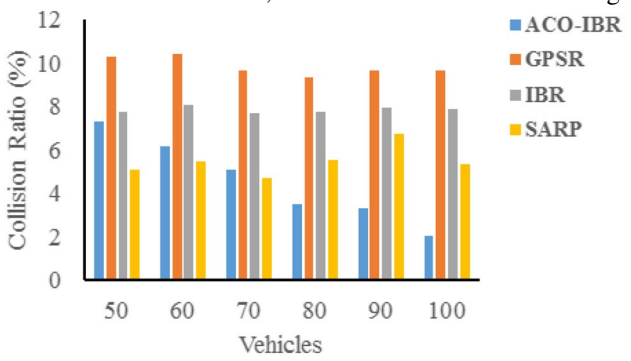


Fig. 9 Collision rate of SARP

Table 3 Simulation results

Vehicles	PDR (%)				Collision rate (%)				Delay (s)				Overhead				Throughput (kbps)			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
50	92.68	89.73	92.22	**94.94**	7.32	10.27	7.78	**5.06**	0.07	0.1	0.08	**0.051**	27.61	28.46	27.69	**26.89**	70.94	68.68	70.59	**72.68**
60	93.83	89.61	91.96	**94.52**	6.17	10.39	8.04	**5.48**	0.075	0.11	0.08	**0.051**	35.17	36.79	35.85	**34.88**	64.91	62	63.62	**65.39**
70	94.94	90.36	92.32	**95.28**	5.06	9.64	7.68	**4.72**	0.08	0.09	0.08	**0.052**	**41.54**	43.55	42.62	41.93	64.26	61.16	62.49	**68.39**
80	**96.51**	90.66	92.24	94.50	**3.49**	9.34	7.76	5.5	0.078	0.1	0.08	**0.051**	41.42	44.05	43.3	**40.27**	**75.75**	71.15	72.4	74.17
90	**96.7**	90.33	92.06	93.29	**3.3**	9.67	7.94	6.71	0.074	0.1	0.08	**0.050**	65	69.54	68.23	**42.64**	49.76	46.49	47.38	**92.43**
100	**97.94**	90.35	92.15	94.66	**2.06**	9.65	7.85	5.33	0.07	0.1	0.08	**0.053**	67.93	73.63	72.18	**40.28**	57.2	52.76	53.82	**76.1**

Bold values represent better results of each parameter with respect to other protocols used in the simulation
1- ACO-IBR, 2- GPSR, 3- IBR, 4- SARP

PDR as compared to GPSR and IBR. But, SARP has 0.90% less average PDR as compared to ACO-IBR. On an average, 4.56%, 9.82%, 7.84% and 5.46% collision rate are observed in ACO-IBR, GPSR, IBR and SARP respectively. The reason behind is the higher message exchange takes place as there is an increase in the vehicles. Less cooperation between vehicles causes a high collision rate in SARP as compared with ACO-IBR. In a dense environment, message authentication is not achieved in stipulated time as the transmitted message is high. The required message transmission time to arrive at the D_v from the S_v is 0.023 s, 0.048 s and 0.028 s less as compared to ACO-IBR, GPSR and IBR. In SARP, with the increase in the received messages, the application layer requires less processing time. The transmission delay of the SARP is less as compared to the protocols used in the simulation as there is less congestion between vehicles. Overhead generated is high with increasing participating vehicles. Overall SARP observes 8.63, 11.52 and 10.49 less overhead concerning the protocols as mentioned above. 11.05, 14.84 and 13.14 kbps higher throughput is observed in SARP. There is more significant interaction between vehicles with more successful message transmission. In SARP, enhancement in the throughput is observed according to increase in the vehicles. In case of 90 and 100 vehicles scenario, reduction in the throughput is observed for ACO-IBR, GPSR and IBR and shows unexpected behavior. Reduced throughput of GPSR and IBR is observed because communication links are broken easily and the load capacity of the network is deteriorated. Overall, throughput for the SARP routing protocol is higher as compared to ACO-IBR, GPSR and IBR with the reason that SARP has a lower routing overhead than ACO-IBR, GPSR and IBR. As the overhead observed is less that allows more bandwidth to be used for the data packets. SARP has robust link that enhances communication performance and it helps in throughput improvement. On the whole, the throughput of SARP is larger than that of ACO-IBR, GPSR and IBR as SARP selects the next hop node with more stable neighbor relationship and can build the more robust path than ACO-IBR, GPSR and IBR.

6.3 Security evaluation

Security is evaluated using authentication and data integrity. Security evaluation is assessed in terms of various parameters that are computational cost, communication cost of the certificate and time required for signature generation. There are many software environments and libraries available that are applicable for computation of cryptographic bilinear pairing and related mathematical operations in the groups. The most widely adopted libraries are PBC (Boneh 2012; PBC 2020), MIRACL (Miracl 2020) and RELIC (Kanenari et al. 2019). The pairing-based cryptography library is an open-source library. It uses 'C' programming environment that is built on GMP library. The PBC library is applied for the computation of various operations in the proposed methodology. It is used to evaluate mathematical operations underlying PBC cryptosystems. It comprises various procedures related to mathematical, pairing, key generation and generation of elliptic curve. The functions used are abstract. The user requires basic understanding of pairings so, PBC is easy to use and it produces a reasonable pairing time.

Table 4 Computational time and key generation delay of SARP

Vehicles	Key generation Delay (ms)	Computational Time (ms)
10	0.013	17
20	0.026	23
30	0.033	38
40	0.054	43
50	0.057	43
60	0.069	43
70	0.080	97
80	0.074	100
90	0.068	143
100	0.078	189

The simulation based experimentation is carried out on Intel core i-5 machine that has 2.60 GHz processor along with 8GB RAM. The simulations are executed randomly for 30 times and the average value is considered for the parameters. The computational time of the certificate is the entire time taken by the system to perform secure vehicular communication. It is the time taken to validate one signature along with certificate or n certificates along with n signatures that authenticate vehicles, ensures message integrity and secure message exchange between vehicles. Signature generation time is the time taken by the message to generate one signature or n signature. The key generation delay is the time taken by the system to generate the keys that are private and public. The computational time increases as the number of vehicles are higher. Similar behavior is observed for the key generation delay for various vehicles. The results are shown in Table 4.

6.4 Computational cost

P_T is the time taken by the authentication protocol to perform bilinear operations. H_T is the time required for the hash operation in the protocol. M_T is the time required to perform multiplication operation. T_{ep-1} and T_{ep-2} are the time taken by the protocol to initiate the exponentiation operation. Table 5 shows the computational cost of various authentication protocols with their formulations. Table 6 shows the

Table 5 Computational cost for various protocols

Protocol	Computational cost of one certificate	Computational cost of n certificate
BLS (Boneh et al. 2004)	$4P_T + 2H_T$	$(2_n + 2)P_T + 2_nH_T$
ECPP (Lu et al. 2008)	$3P_T + 11M_T$	$3_nP_T + (10 + n)M_T$
CPAS (Shim 2012)	$5M_T + 3P_T$	$(5_n + 1)M_T + 3_nP_T$
CPAV (Vijayakumar et al. 2015)	$2P_T + H_T + 2T_{ep-1}$	$(1 + n)P_T + nH_T + 2_nT_{ep-1}$
Proposed (SARP)	$2P_T + 4T_{ep-1} + T_{ep-2}$	$(1 + n)P_T + 4T_{ep-1} + nT_{ep-2}$

Table 6 Parameters and their values used in the simulation

Parameter	Required time (ms)
P_T	1.6
H_T	2.7
M_T	0.6
T_{ep-1}	0.7
T_{ep-2}	0.6

Table 7 Simulation results for computational cost (ms) of various authentication protocols

Vehicles	BLS	ECPP	CPAS	CPAV	SARP
10	89.2	60	78.6	58.6	26.4
20	175.2	114	156.6	115.6	48.4
30	261.2	168	234.6	172.6	70.4
40	347.2	222	312.6	229.6	92.4
50	433.2	276	390.6	286.6	114.4
60	519.2	330	468.6	343.6	136.4
70	605.2	384	546.6	400.6	158.4
80	691.2	438	624.6	457.6	180.4
90	777.2	492	702.6	514.6	202.4
100	863.2	546	780.6	571.6	224.4

various parameters and their obtained values in the simulation. Computational cost for various protocols are shown in Fig.10 and Table 7 respectively.

6.5 Discussion

The BLS takes four pairing operations and two hash operations to calculate the computational cost for one certificate. BLS requires 11.8 ms for the generation and verification of one signature and 863.2 ms for 100 signatures. The ECPP takes three pairing operations and eleven scalar multiplication operations for bilinear pairings. This is the computational cost of one certificate. ECPP requires 11.4 ms for the generation and verification of one signature and 546 ms for 100 signatures. The CPAS requires five scalar point multiplication operations over elliptic curve and three pairing operations for the computation of one certificate generation

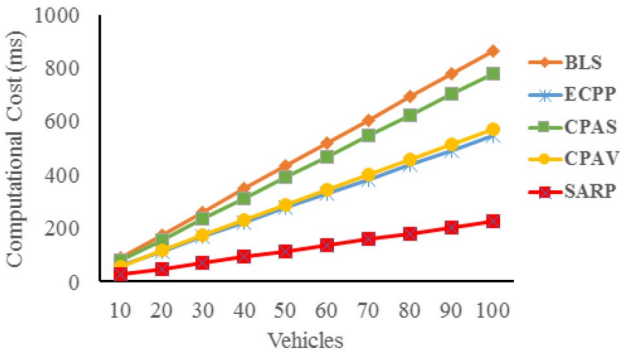


Fig. 10 Computational cost for various authentication protocols

and verification. CPAS requires 7.8ms for the generation and verification of one signature and 780.6 ms for 100 signatures. The CPAV takes two pairing operations, one hash operation and two exponentiation operations for generation and verification of one certificate. CPAV requires 7.3 ms for the generation and verification of one signature and 571.6ms for 100 signatures. The proposed protocol SARP requires two pairing operations and two separate exponentiation operations for generation and verification of one certificate. SARP requires 6.6 ms for generation and verification of one signature and 224.4 ms for 100 signatures. It also requires 5.2 ms, 4.8 ms, 1.2 ms and 0.7 ms less time for generation and verification of one certificate as compared to the BLS, ECPP, CPAS and CPAV. For generation and verification of 100 certificates, 638.8 ms, 321.6 ms, 556.2 ms and 347.2 ms less time taken by the SARP as compared to the protocols under study. It is observed that the SARP requires less computational cost for the certificate generation and verification. This is because it makes use of less number of hash, pairing, multiplication and exponentiation operations as compared to the standard protocols used for the comparative analysis.

6.6 Communication cost analysis

Communication cost (Bayat et al. 2020; Gao et al. 2018) is the overhead observed during communication that results while computing and exchanging parameters used in V_2V communication. It is expressed in byte. The type-A curve is used for secure communication. Bilinear pairings are built

upon the curve $y^2 = x^3 + x$ over the finite field. In the initial registration phase, the various vital parameters are published and stored in TPD. Various operations are used to evaluate communication cost and are shown in the Table 8. G_1, G_2 and G_T are the group of points over finite field. Since q is 64-byte, an element in the group G_1 is 2×64=128-byte. The type–A curve uses symmetric pairings and group G_2. G_T element has 128-byte each.

The CPPA (He et al. 2015) consists of the authentication message as $(M, AID_i, T_i, R_i, \sigma_i)$ where AID_i $=(AID_i, 1, AID_i, 2)$. T_i is the timetamp. So the size of authenticated message is $64 \times 5 + 4 = 324$-byte. In the CPAS (Shim 2012), the vehicle transmits an authentication message (PID_i, M_i, t_i, T_i) and receives $(PID'_i, M'_i, t'_i, T'_i)$ from other vehicles. Therefore, communication cost of the CPAS is $(128 \times 6) + (20 \times 4) + (4 \times 2) = 856$-byte. In PACP (Huang et al. 2011), vehicle transmits (PN^j, σ_j) and receives (PN^j, σ_j) where $PN^j = (T_{(a,i)}, t_{(a,i)}, SIG(T_{(a,i)}, t_{(a,i)}, certR_i)$. So, the communication cost for the PACP is $(128 \times 10) + 4 + (120 \times 2)$ $+ (40 \times 2) = 1604$-byte. The authentication message of the proposed protocol comprises $Msg = (M \| sign \| Pb_{(k)} \| S_{cert})$. The total size for the message is $(128 \times 3) + 64 + 120 =$ 568-byte. The Table 9 shows various security protocols with their communication cost.

7 Conclusion and further research direction

The proposed SARP protocol uses ACO-IBR and anonymous authentication. Anonymous authentication enables secure communication by incorporating message authenticity and integrity. The proposed protocol achieves an anonymous authentication that meets the requirements of VANET applications such as less verification time for the certificate and signature generation. The communication cost of an authenticated message produced is 1036-byte and 288-byte less as compared to the PACP and CPAS protocol adopted for the comparison. SARP requires 638.8 ms, 321.6 ms, 556.2 ms and 347.2 ms less computational cost for 100 vehicles as compared to BLS, ECPP, CPAS and CPAV. The SARP is resistant to various attacks such as bogus message, message modification and impersonation attack. Thus, SARP is integrity preservation protocol. The QoS performance is evaluated by making variations in the vehicles. By observation of simulation results, it is found that SARP has observed less delay and overhead compared to protocols studied and simulated. SARP observed 0.023, 0.048 and 0.028s less delay and 8.63, 11.52, 10.49 less overhead while packet transmission as compared to the ACO-IBR, GPSR and IBR. It is possible in future to extend the research work to reduce computational cost of the certificate. In this, batch authentication technique can be used that is suitable for the VANET environment.

Table 8 Operations used to determine communication cost

Operations	Size (byte)
The size of the hash digest	20
Timestamp	4
Z_q	20
Random prime number	64
Asymmetric encryption/decryption	64
Signature operation	128
G_1, G_2 and G_T in group	128
OBU certificate	120

Table 9 Communication cost analysis of various protocols in VANET

Protocol	Communication cost (byte)
CPPA	324
CPAS	856
PACP	1604
Proposed (SARP)	568

Data availability statement The data used to support the findings of this study are available from the corresponding author upon request.

References

(2020) Pbc library - pairing-based cryptography - about. https://crypto.stanford.edu/pbc/, Accessed 03/10/2020

Arif M, Wang G, Bhuiyan MZA, Wang T, Chen J (2019) A survey on security attacks in vanets: Communication, applications and challenges. Veh Commun 19:1–36

Azees M, Vijayakumar P, Deborah L (2016) Comprehensive survey on security services in vehicular ad-hoc networks. IET Intell Transp Syst 10:379–388

Azees M, Vijayakumar P, Deboarh LJ (2017) Eaap: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Trans Intell Transp Syst 18(9):2467–2476. https://doi.org/10.1109/TITS.2016.2634623

Bayat M, Barmshory M, Pournaghi SM, Rahimi M, Farjami Y, Aref M (2020) A new and efficient authentication scheme for vehicular ad hoc networks. J Intell Transp Syst 24:171–183

Ben Mussa SA, Manaf M, Ghafoor KZ, Doukha Z (2015) Simulation tools for vehicular ad hoc networks: A comparison study and future perspectives. In: 2015 International Conference on Wireless Networks and Mobile Communications (WINCOM), pp 1–8, https://doi.org/10.1109/WINCOM.2015.7381319

Bhoi SK, Khilar PM (2014) Vehicular communication: a survey. IET Netw 3(3):204–217

Boneh D (2012) Pairing-based cryptography: Past, present, and future. In: Wang X, Sako K (eds) Advances in Cryptology – ASIACRYPT

2012. Lecture notes in computer science, vol 7658. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-34961-4_1
Boneh D, Lynn B, Shacham H (2004) Short signatures from the weil pairing. J Cryptol 17:297–319
Chaum D, van Heyst E (1991) Group signatures. In: Davies DW (ed) Advances in Cryptology – EUROCRYPT '91. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 257–265
Gao T, Li Y, Guo N, You I (2018) An anonymous access authentication scheme for vehicular ad hoc networks under edge computing. Int J Distrib Sens Netw 14(2):1–16. https://doi.org/10.1177/1550147718756581
Han M, Liu S, Shidian M, Wan A (2020) Anonymous-authentication scheme based on fog computing for vanet. PLoS One 15:1–19. https://doi.org/10.1371/journal.pone.0228319
Harri J, Filali F, Bonnet C (2009) Mobility models for vehicular ad hoc networks: a survey and taxonomy. IEEE Commun Surv Tutor 11(4):19–41. https://doi.org/10.1109/SURV.2009.090403
He D, Zeadally S, Xu B, Huang X (2015) An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans Inf Forensics Secur 10(12):2681–2691. https://doi.org/10.1109/TIFS.2015.2473820
Huang D, Misra S, Verma M, Xue G (2011) Pacp: an efficient pseudonymous authentication-based conditional privacy protocol for vanets. IEEE Trans Intell Transp Syst 12(3):736–746. https://doi.org/10.1109/TITS.2011.2156790
Huang J, Fang D, Qian Y, Hu RQ (2020) Recent advances and challenges in security and privacy for v2x communications. IEEE Open J Veh Technol 1:244–266. https://doi.org/10.1109/OJVT.2020.2999885
Imran S, Karthick RV, Visu P (2015) Dd-sarp: Dynamic data secure anonymous routing protocol for manets in attacking environments. In: 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 39–46. https://doi.org/10.1109/ICSTM.2015.7225388
Jiang S, Zhu X, Wang L (2016) An efficient anonymous batch authentication scheme based on hmac for vanets. IEEE Trans Intell Transp Syst 17(8):2193–2204. https://doi.org/10.1109/TITS.2016.2517603
Kanenari T, Takahashi Y, Hashimoto Y, Kodera Y, Kusaka T, Nogami Y, Nakanishi T (2019) A comparison of relic-toolkit and elips libraries for a pairing-based homomorphic encryption. In: 2019 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), 1–4. https://doi.org/10.1109/ITC-CSCC.2019.8793446
Karp B, Kung HT (2000) GPSR: greedy perimeter stateless routing for wireless networks. In: Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom'00), Association for Computing Machinery, New York, NY, USA, pp 243–254
Kenney JB (2011) Dedicated short-range communications (dsrc) standards in the united states. Proceedings of the IEEE 99(7):1162–1182. https://doi.org/10.1109/JPROC.2011.2132790
Lin X, Sun X, Ho P, Shen X (2007) Gsis: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans Veh Technol 56:3442–3456
Liu Y, Wang L, Chen HH (2015) Message authentication using proxy vehicles in vehicular ad hoc networks. IEEE Trans Veh Technol 64(8):3697–3710. https://doi.org/10.1109/TVT.2014.2358633
Lu R, Lin X, Zhu H, Ho PH, Shen X (2008) Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications. In: IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, 1229–1237. https://doi.org/10.1109/INFOCOM.2008.179
Lu Z, Qu G, Liu Z (2019) A survey on recent advances in vehicular network security, trust, and privacy. IEEE Transactions on Intelligent Transportation Systems 20(2):760–776. https://doi.org/10.1109/TITS.2018.2818888
Manvi SS, Tangade S (2017) A survey on authentication schemes in vanets for secured communication. Veh Commun 9:19–30. https://doi.org/10.1016/j.vehcom.2017.02.001
Miracl (2020) https://miracl.com/about-miracl/, Accessed 04/30/2020
Raya M, Hubaux J-P (2007) Securing vehicular ad hoc networks. J Comput Secur 15(1):39–68
S R, S LK (2015) Sharp: Secured hierarchical anonymous routing protocol for manets. In: 2015 International Conference on Computer Communication and Informatics (ICCCI), 1–6. https://doi.org/10.1109/ICCCI.2015.7218121
Samatha B, Kumar DR, Karyemsetty N (2017) Design and simulation of vehicular adhoc network using sumo and ns 2. Adv Wirel Mobile Commun 10(5):1207–1219
Shen H, Zhao L (2011) Alert: an anonymous location-based efficient routing protocol in manets. IEEE Trans Mobile Comput 12:1079–1093
Shim KA (2012) Cpas: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. IEEE Transactions on Vehicular Technology 61(4):1874–1883. https://doi.org/10.1109/TVT.2012.2186992
Silva A, Reza N, Oliveira AM (2019) Improvement and performance evaluation of gpsr-based routing techniques for vehicular ad hoc networks. IEEE Access 7:21722–21733
Tyagi P, Dembla D (2017) Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (vanet). Egypt Inf J 18(2):133–139. https://doi.org/10.1016/j.eij.2016.11.003
Vijayakumar P, Azees M, Deborah LJ (2015) Cpav: Computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks. In: 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, pp 62–67. https://doi.org/10.1109/CSCloud.2015.32
Wang Y, Zhong H, Xu Y, Cui J (2016) Ecpb: efficient conditional privacy-preserving authentication scheme supporting batch verification for vanets. Int J Netw Secur 18:374–382
Wei Z, Li J, Wang X, Gao CZ (2019) A lightweight privacy-preserving protocol for vanets based on secure outsourcing computing. IEEE Access 7:62785–62793. https://doi.org/10.1109/ACCESS.2019.2915794
Yelure B, Sonavane S (2020) Aco-ibr: a modified intersection-based routing approach for the vanet. IET Netw 9:348–359
Yelure B, Sonavane S (2021) Performance of routing protocols using mobility models in VANET. In: Deshpande P, Abraham A, Iyer B, Ma K (eds) Next generation information processing system, advances in intelligent systems and computing, vol 1162. Springer, Singapore, pp 272–280. https://doi.org/10.1007/978-981-15-4851-2_29
Zhang J, Xu M, Liu L (2014) On the security of a secure batch verification with group testing for vanet. Int J Netw Secur 16:355–362