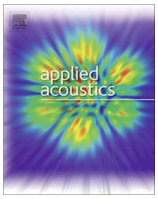
Applied Acoustics 165 (2020) 107331

Contents lists available at ScienceDirect

Applied Acoustics

journal homepage: www.elsevier.com/locate/apacoust



Fast-track message authentication protocol for DSRC using HMAC and group keys

Smith K. Khare

[a] *Electronics and Communication Engineering, PDPM Indian Institute of Information Technology, Design and Manufacturing Jabalpur, India - 482005*

ARTICLE INFO

Article history:
Received 18 February 2020
Received in revised form 11 March 2020
Accepted 12 March 2020
Available online 26 March 2020

Keywords:
VANET
Vehicle authentication
Hash message authentication code (HMAC)
Secret keys
Certificate revocation list (CRL)
Intelligent transportation system

ABSTRACT

The exchange of information between vehicle to vehicle and vehicle to infrastructure in vehicular ad hoc networks (VANET) should be secured to provide an intelligent transport system. VANET uses certificate revocation lists (CRL) and public key infrastructures (PKI) for its security. In any PKI algorithms validity of the messages received from the sender is executed by checking the senders certificate in current CRL and verify the authenticity of the signature and certificate of the sender. Checking the CRL and verifying the authenticity is time-consuming and affects system performance drastically. This paper offers an accelerated and secure authentication method that utilizes a hash message authentication code (HMAC) in combination with secret keys for the revocation checking process. By using HMAC and enhancing the CRL checking procedure, the algorithm provides improved performance of the system parameters like authentication delay, end-to-end delay, and packet delivery ratio. Also, this algorithm reduces the delay involved in vehicle authentication. This novel algorithm uses the random distribution of keys that enables the authenticated on-board unit to securely share and update a secret key. An authentication delay of 77.29 μs, end-to-end delay of 13.56 ms and packet delivery ratio of 81.2% is achieved.

© 2020 Elsevier Ltd. All rights reserved.

1. Introduction

Establishing communication between vehicles has been possible due to the recent advancements and the availability of cost-effective hardware. Vehicular ad hoc networks (VANET) is considered as the most trusted and intelligent transport system. The vehicles in VANET are capable of establishing the short-range as well as medium-range communication. These vehicles communicate via communication broadcast services and are also equipped with a global positioning system (GPS) modules. This facilitates the vehicles to track the position of other vehicles in the network. The VANET entities are comprised of three main components; a) Trusted authority (TA) being the fixed entity, b) Roadside unit (RSU) which are placed along the road separated from each other by 300 m to 1000 m and c) On-board unit (OBU) that are hardware equipments embedded in vehicles. Communication in VANET is possible between vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) through wireless channels. Hence, there is a need to secure this wireless channel since it is prone to outside attacks. IEEE wireless access vehicular environment (WAVE) [1] has integrated the elliptic curve digital signature algorithm (ECDSA) [2] protocol for authentication purposes. Dedicated short-range communication (DSRC) [3] is defined under WAVE standard states that every OBU in the network transmits the message every 300 ms [4]. This message contains the information of the vehicle regarding its position, direction, and speed. Each vehicle broadcasts this information to the neighboring vehicle using GPS. The integrity and authenticity of the message are verified by the receiver. One of the major challenges in this scenario is the speed of moving vehicles. The authentication process proposed must be very secure and fast enough to provide the opposite registration of vehicles into the system. The DSRC has standardized that to improve the system performance a minimum of 600 messages [4] should be verified per second. Generally, the number of messages verified (P) per second is given

$$P = \frac{1000}{9n+1} \tag{1}$$

where n is the number of revoked identity in CRL. To determine whether the vehicle is in CRL or not and to verify the identity of vehicle 9 msec is required. In the case of the group signature, the verification time is 11 msec. The current WAVE standard does not provide a comprehensively fast and secure authentication scheme simultaneously. The primary step of any authentication process is

E-mail address: smith7khare@gmail.com

https://doi.org/10.1016/j.apacoust.2020.107331
0003-682X/© 2020 Elsevier Ltd. All rights reserved.

to check the current revocation status of the sender in the CRL. This CRL checking procedure results in a long delay depending upon the number of entries in the CRL. It has been observed that more the size of the CRL more is the privacy of the user vehicle which maintains integrity. In addition to this, the signature verification also causes a certain amount of lag. Although this lag has negligible value and is of the order of few milliseconds, it may cause the system performance to degrade in case of heavy traffic. Hence there is a need for a faster and secure authentication technique in VANET for providing scalability and real-time coordination between vehicles. This paper proposes a unique technique for authenticating vehicles in a VANET. A group communication established and the faster process is achieved by sharing keys. The identity of a vehicle is determined by a combination of group public keys and group secret keys along with HMAC to authenticate the moving nodes. The performance of the proposed method is judged by evaluating authentication delay, packet delivery ratio, and end-to-end delay. The paper is arranged as; Section 2 briefly describes the techniques proposed in the past and the related work done by other researchers. Section 3 introduces the proposed authentication technique for VANET with a promising new approach. Section 4 proves its dominance over standard techniques generally used in vehicular ad hoc networks by plotting graphs. Finally, Section 5 gives the conclusion of the paper.

2. Literature survey

The literature survey discusses the different authentication schemes and CRL checking models proposed by the researchers. The method proposed in (EMAP) [5] used the HMAC that replaces the slow CRL checking schemes. But the approach used in [5] considers the pseudonyms that may not support the group signature authentication. Another solution proposed in [6] depends on the anonymous certificate-based authentication where every OBU in the network has been preloaded with a large number of certificates. Each time OBU signs the message, a certificate is used from the pool. The major issue with this method is that a large number of certificates create the identity dispute that affects the system performance. The method in [7] combines the public key infrastructure and time-efficient stream loss tolerant authentication [8] protocol for VANETs. In this approach, if the first message has been verified by the receiver then the remaining messages are verified by examining the message authentication code (MAC) using a time-efficient stream loss tolerant authentication procedure. In [9] revocation using a compressed certification revocation list (RC2RL) has been proposed in which CRL size has been reduced using the bloom filters before broadcasting it. In this method, the CRL is issued by a trusted third party. Another technique proposed in [10] divides the CRL parts and distributes parts of it independently. The probabilistic approach has been used to consider the mobility of an entity which has been discussed in [11]. In the work proposed in [12] gives a detailed discussion of the identity-based cryptographic scheme (IBCS) and its application in mobile ad hoc networks. In IBCS, TA holds all the control to distribute the master secret necessary for the extraction of a private key. The scheme used in [13,14] depicted anonymous identity-based pseudonym schemes by use bilinear property. A method based on bloom filters and binary search has been used for vehicle security using group communication [15]. The group signature-based approach validates the entire group by verifying the signature of group manager [16]. In PACP [17] pseudonymous authentication-based conditional privacy protocol has been used tickets and tokens as secret keys and pseudonyms. Vehicle security has been enhanced by providing multiple tokens for the same ticket. Ring signature method described in [18] which uses node to obtain its vehicle's unique identity from TA to sign a message. Pseudonymous authentication scheme with strong privacy preservation [19] used the non-repeating identity-based scheme to sign the message by using vehicle unique identity for V2V and V2I communication in the network. GSIS proposed in [20] offers a new feature to the group based cryptography by adding an identity-based cryptographic scheme. Revocation strategies used in [21] give control to a central authority to access the database of hardware security module (HSM) in OBU and destroy the group key, hence this scheme overcomes the disadvantage to update the key sets by every group manager in the group. The method proposed in [22] uses TA to distribute and manage the key sets of the nodes in the network. Group public key, private secret key, CRL are all managed by TA in the network. Ring revocation signature protocol used in [23] achieves unlinkability and conditional privacy. The problem of region restriction and time duration has been overcome in the work proposed in [24] by efficient key distribution using distribution key management process. A blockchain-based traceable framework has been used for securing the identity of vehicles and RSU [25]. A semi-trusted authentication scheme based on self-healing key distribution has been proposed in [26]. Vehicular authentication has been achieved with proxy ring signature [27]. The authentication scheme used in [28] combines filtering and multi-key outsource computation for VANET. The method proposed in the literature used anonymous certificate distribution, large CRL size, longer delay and lack of group communication. This motivates us to develop compact CRL, expedite and group-based message authentication models for VANET.

3. HMAC and group key combination authentication technique in VANET

VANET is a combination of three entities that are interconnected by using some wired and wireless topologies which are described as follows.

- Trusted Authority (TA): It is the most crucial entity which is considered to be the central controller. A trusted authority is responsible for managing, issuing and updating all the required certificates. Every moving node (vehicles) in the scenario has to be registered with the TA. It is also responsible for broadcasting all the secret keys among the vehicles. TAs resolve the dispute between the vehicles or vehicles and RSU.
- Road Side Unit (RSU): These are stationary nodes and are placed along the roadside. RSU is the intermediating communication link between TA and OBU. Communication between OBU and TA is always setup via RSU. The RSU and TA communicate via a secured wired channel so there is a minimum threat of attackers in this scenario. The distance between two RSUs has not been fixed by 1609.2 IEEE WAVE standards. However, they are usually placed at a distance of 300 m to 1000 m [1].
- On Board Unit (OBU): They are fixed in the vehicles themselves and communicate with other OBUs via V2V communication through a wireless channel. They also communicate with RSU using V2I communication by wireless communication channels. The security standards 1609.2 IEEE WAVE has standardized each OBU to be equipped with the HSM that has all security components like public keys, secret keys and all the certificates issued by the TA. HSM can carry out many operations like signing and verification of the message, along with revocation and perform keys update.

A typical VANET scenario is illustrated in Fig.1.

The method used in previous papers does not employ group-based communication and Hash message authentication code

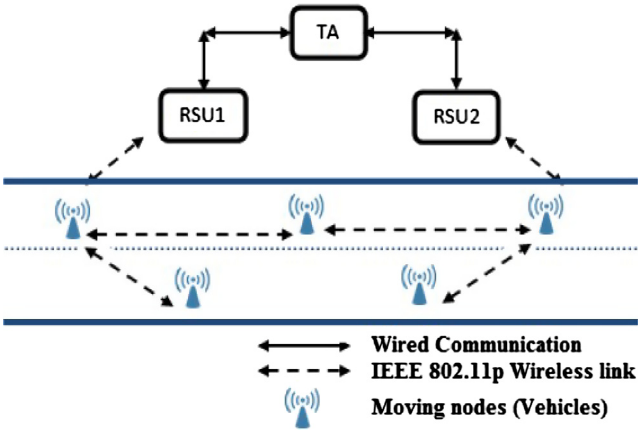


Fig. 1. VANET System Model.

(HMAC) together. HMAC proves very efficient and secure in terms of authentication and providing integrity to the vehicles. HMAC implemented in the previous papers has considered individual vehicles. The proposed method in this paper uses HMAC which performs hash implementation in combination with the secret keys making in very efficient and secure. The vehicles are grouped based on public and private vehicles. The purpose of the HMAC used in this algorithm is listed below:

- To verify senders identity in order to allow the users to generate correct HMAC.
- To maintain the integrity of the message before the verification or authentication.

The authentication technique proposed in this paper is carried out in four steps viz. system initialization, signing and verification of message, and revocation. The details of each step are explained below:

3.1. System initialization

The system undergoes an initialization process in this step that is delineated by the following steps.

```
1. Select two generators $A; B \epsilon \breve{G}_1 \breve{G}_2$ of order $z$.
2. **for** $\leftarrow$ **1 : J; do**
3. Select a random number $k_i \epsilon C_b^*$
4. Select a secret key $K_i = k_i B \epsilon \breve{G}$
5. Set the group public key $GPK_i^* = \frac{1}{k_i} A \epsilon \breve{G}$
6. **end for**
7. Select as initial secret key $K_a \epsilon \breve{G}_2$ distributed among the non revoked OBUs.
8. Select a master secret key $m \epsilon C_b^*$
9. Set the group key values $GPK = mX$
10. Select the hash functions $H : \{0,1\}^* \rightarrow \breve{G}_1 and h : \{0,1\}^* \rightarrow C_b^*$
11. Select a secret values $r \epsilon C_b^*$ and set $r_a = r$
12. **for i** $\leftarrow$ **1:l** obtain a hash chain values set $V$
13. Set $r_i = h(r_{i-1})$
14. **end for**
15. **TA** performs the following $\forall OBU_u$ in the network
16. **for i**$\leftarrow$ **1:n**;
17. A random number is selected $a \epsilon [1, N]$
18. Upload $K_i = k_i B$ and $GPK_i^* = \frac{1}{k_i} A$ in$HSM_u$ embedded in $OBU_u$
19. **end for**
20. **for i** $\leftarrow$ **1:k**;
21. Use step 22 to generate pseudonyms certificates
22. $CERT_u = \{cert_u(UID_u, GPK_u^i; UID_u||GPK_u^i))|1 \leqslant i \leqslant C\}, UID$ is the pseudo unique identity.
23. Upload the certificates in the HSM of OBU.
24. **end for**
25. Declare $H, h, A, B \forall OBU$
```

After initialization, TA and OBU determines the following sets of parameters.

- A pool of secret keys U_s
- A set of public keys U_p
- A master secret key m and set of group public keys GPK_u
- The secret key K_a
- Values of hash chain V.
- A set of anonymous certificates ($CERT_u$) for privacy-preserving and authentication.
- A secret keys
- Public keys
- A secret key K_a to be shared between all the legitimate OBUs.

3.2. Message signing

In this step, initialized parameters are distributed among the OBUs and RSUs. Before broadcasting the message by any OBU, it performs the revocation check. It is symbolized as REV_{check} and it is the function of HMAC, K_a, UID_u, and $Time_{stamp}$. TheRevocation check is calculated as follows:

$$REV_{check} = HMAC(K_a||UID_u||TIme_{stamp}) \tag{2}$$

where UID_u is pseudo unique identity of the vehicle, $Time_{stamp}$ is the current timestamp, —— denotes the concatenation. As the OBU calculates the revocations check it broadcast the message Z containing this REV_{check} which is given by:

$$\begin{aligned} &Z = (Msg||Time_{stamp}||Certificate(UID_u||privatekey) \\ &Signature_{TA}(UID_u||privatekey))||(UID_u||GPK) \\ &Signature_{TA}((Msg||Time_{stamp})||REV_{check}) \end{aligned} \tag{3}$$

3.3. Message verification

On receiving the message Z by any of the OBU, it performs verification of the message. To perform the verification, an OBU must have Z and the initial secret key (K_a). The following steps are carried out to ensure a valid message by a trusted entity in the network.

- Check the validity of timestamp if valid go to next step, **else** drop the message.
- Check if $REV_{check} = HMAC(K_a, (UID_u||Time_{stamp}))$ if invalid drop message, **else**.
- Check the validity of signature of TA, if invalid drop message, **else**.
- Verify signature of group using secret keys of the group, if valid **accept the message**, else drop the message.

3.4. Revocation

After the message verification process is performed, the TA in the network looks after the legitimate vehicles and performs the revocation. In the revocation process, all the certificates and keys of the legitimate vehicle in the network are revoked. The steps carried out for revocation are:

- TA prepares the key updation message to carry out the process of revocation. The key update message is given by

$$K_{msg} = (Msg||ID_{revkey}||K_m) \tag{4}$$

where; ID_{revkey} is the list of identities of revoked key.
- With the help of this key update message, the TA broadcasts the revocation message which is calculated as

$$REV_{msg} = (CRL||K_{msg}||(Signature_{TA}(CRL||K_{msg}))) \tag{5}$$

- After receiving the Rev_{msg}, the signature of TA is verified by calculating $HMAC(CRL||K_{msg})$. If this condition is invalid then the algorithm exits, else the keys are updated.

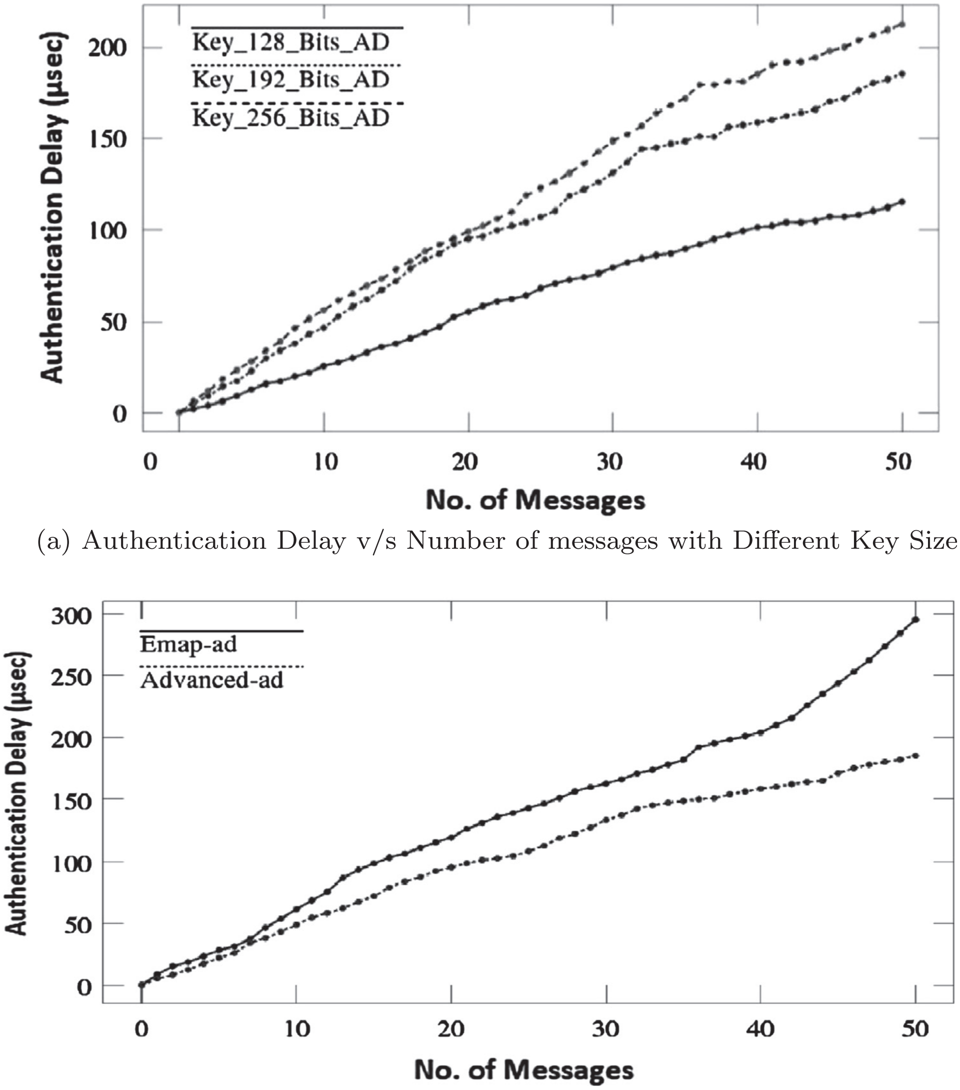
The updated keys are distributed among the valid OBUs shown below in Fig.2.

4. Performance analysis

To evaluate the proposed algorithm, a vehicle system is implemented in the NS-2 simulator [29,30]. The evaluation is carried on a 1000 m * 1000 m city street scenario. The location of one RSU server i.e. node number 50 is at the center of an area. A maximum of 40 private vehicles and 10 public vehicles are considered. In this model, the results are calculated by taking a combination of 5 vehicles in each group. While calculating system parameters the size of CRL is kept at 100000. The system performance is evaluated by

GROUP ID	MESSAGE-ID	TIME-STAMP	SIGNATURE OF TA	HMAC

Fig. 2. Updated Key if REV_{msg} verification is Valid.



(a) Authentication Delay v/s Number of messages with Different Key Size

(b) Authentication Delay of Proposed Model V/s EMAP

Fig. 3. Authentication delay of the proposed method.

using three different key sizes viz. 128, 192 and 256 bits, respectively. The system specifications taken here for calculating the system parameters are the same as that of EMAP and the comparisons are made considering the same city scenarios as that considered in [5]. There is a two way randomly generated traffic scenario by VanetMobiSim software [31]. To simulate vehicle traffic, 50 vehicles are deployed randomly. The performance parameters viz. authentication delay (AD), end-to-end delay (E2E delay) and packet delivery ratio (PDR) are evaluated.

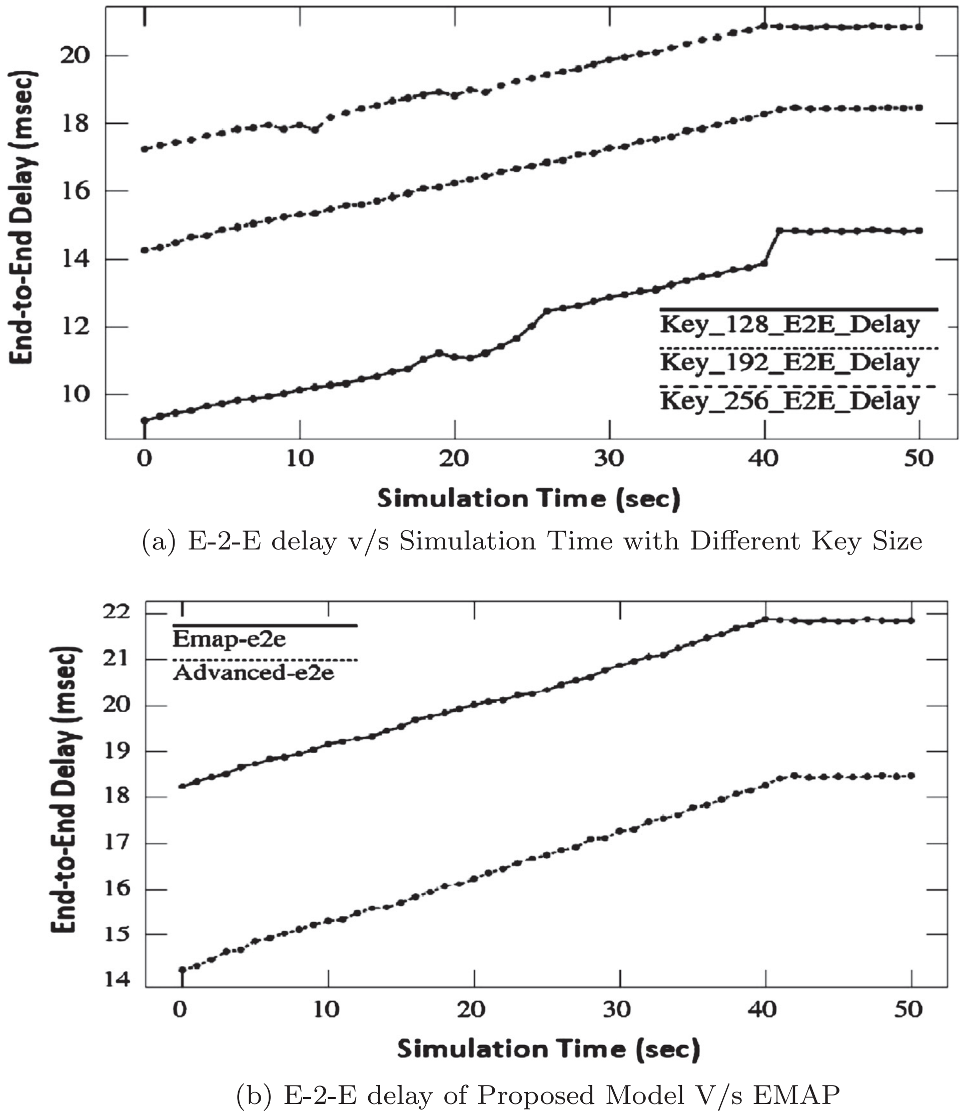
4.1. Authentication delay

Authentication is due to validating the revocation status of the sender, verification of certificate of the sender, and checking the status of the senders signature. A comparison of the authentication delay of the message employing the proposed model with EMAP to verify the revocation check of an OBU is performed. To check the status of evocation, the proposed method employs cipher block chaining advanced encryption standard (CBC–HMACAES) and secure hash algorithm 1 (SHA-1) as the HMAC [32]. For EMAP, the proposed method uses MD-5 as an HMAC function. Fig.3. (a) gives a comparison of authentication delay. As seen from the fig, an increase in the size of the key increases AD. The average delay obtained with a key size of 128, 192 and 256 bits is 77.29 µs, 132.45 µs and 169.78 µs, respectively. By considering UID of OBU and Timestamp both have a length of 10 bytes. Fig.3. (b) shows the overall authentication delay in microseconds versus total messages using the proposed method and EMAP. It is observed that for a constant authentication delay, the proposed scheme gives a better result than EMAP. The authentication delay obtained with the proposed method and EMAP is 132.67 µs and 187.59 µs, respectively. The proposed method verifies a maximum of 156 messages whereas in the case of EMAP it verifies only 124 messages. Hence the proposed method is proving to be efficient in terms of verifying the total number of messages by 25.80 when compared with existing EMAP scheme.

4.2. Evaluation of end-to-end (E-2-E delay) delay

The time need to send packet from source to destination is given by

$$End - to - EndDelay = \frac{\sum(arivetime - sendtime)}{\sum Numberofconnections} \tag{6}$$



(a) E-2-E delay v/s Simulation Time with Different Key Size

(b) E-2-E delay of Proposed Model V/s EMAP

Fig. 4. End-to-End delay of the proposed method.

To evaluate the proposed method further, city street scenarios are examined by end-to-end delay. E-2-E delay is plotted versus simulation time and it is observed that E-2-E delay increases with time as the total number of packets received increases with simulation time. The application layer of each OBU introduces a longer waiting time to process each packet. As the simulation time increases E-2-E delay tends to remain constant because a number of packets received to reach the maximum number that OBU can verify. Fig.4. (a) gives the comparison of E-2-E delay with different key sizes, which shows the effect of a higher key size is not very significant. As the size of key increases, E-2-E delay increases. The average E-2-E delay is 13.56 ms, 15.29 ms, and 18.77 ms for a key size of 128, 192 and 256 bits, respectively. Also, from Fig.4. (b) it can be observed that employing the proposed scheme minimizes the E-2-E delay as compared to the EMAP CRL checking process. The E-2-E delay of the proposed and EMAP is 16.12 ms and 20.97 ms. The proposed method is about 4 ms faster as compared to its counterpart.

4.3. Packet delivery ratio (PDR)

It is the ratio of the total number of data packets delivered to the destination to the total number of packets sent.

$$Packet\,Delivery\,Ratio = \frac{\sum Number\ of\ packets\ received}{\sum Number\ of\ packets\ sent} \tag{7}$$

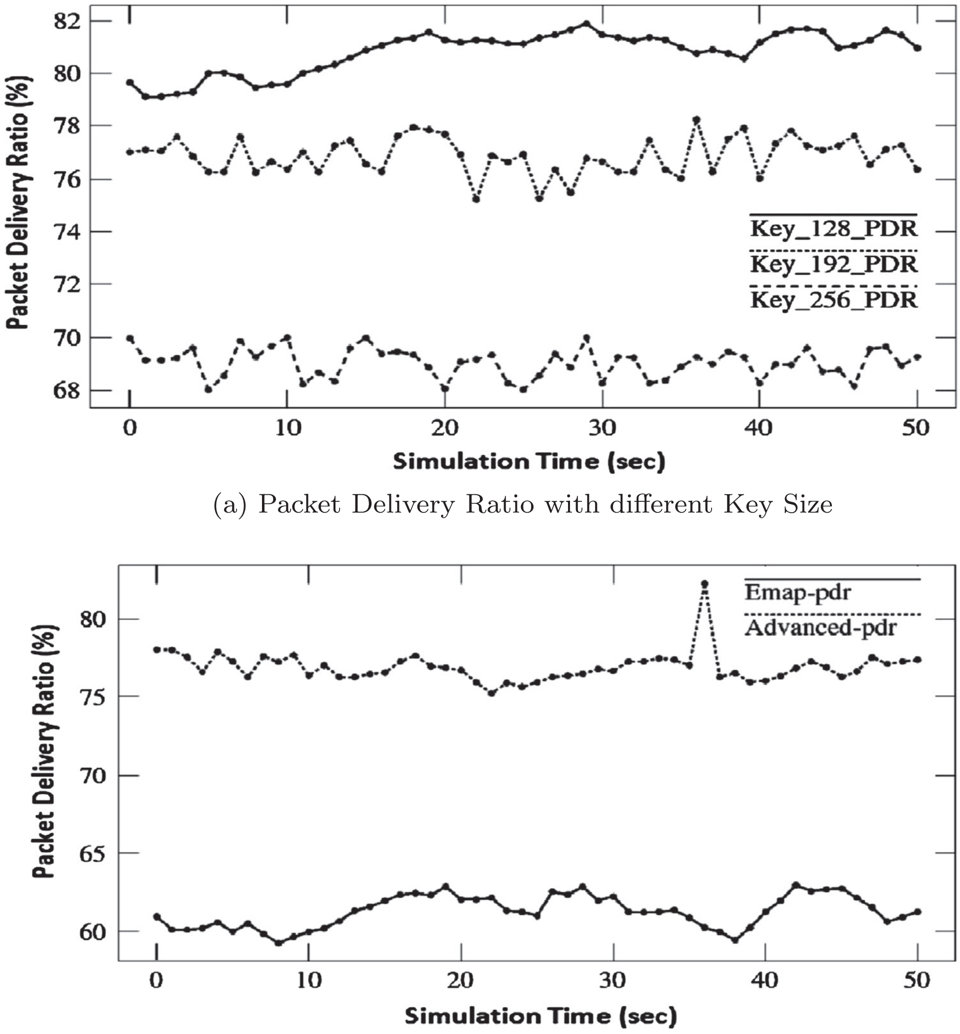
Due to the delay caused by message authentication, the overall packets sent by an OBU in every 300 msec. Hence, in the proposed method PDR is measured every 300 ms. Fig.5.a shows the effect of key size on the packet delivery ratio (PDR) that shows, as the key size increases the PDR reduces. The average PDR for a key size of 128 bits is 81.2%, for 192 bits it is 77.59% and for 256 bits PDR is 69.85%, respectively. Fig.5.b illustrates a calculation of average PDR of OBU within a range for proposed scheme and EMAP. The average PDR for the proposed method is 76.21%, while for EMAP it is 60.48%. The proposed scheme significantly decreases the message loss ratio as compared to EMAP.

4.4. Security analysis

The forward secrecy and resistance to replay attacks are being monitored with the proposed method. The method provides forward secrecy and resistance to replay attacks.

4.4.1. Forward secrecy

Hash chain values are given to only unrevoked OBU in revocation messages. The hash keys are irreversible and cannot be used



(a) Packet Delivery Ratio with different Key Size

(b) Packet Delivery Ratio of Proposed Model V/s EMAP

Fig. 5. Packet Delivery Ratio of the proposed method.

by revoked OBU. Also, the hash keys of the previous revocation cannot be used to generate the current hash values. This results in the non-updation of secret keys by revoked OBUs. Hence, a revoked OBU cannot get K_M to generate K_a from the other OBUs. The certificates of the canceled OBUs are in the updated CRL to prevent non-revoked OBU from passing K_a to the revoked OBUs. In this way, the presented scheme ensures forward secrecy.

4.4.2. Resistance to replay attacks

The current time stamp is included in each message in the revocation check: $REV_{check} = HMAC(K_a, UID_u, Time_{stamp})$, an intruder cannot record $REV_{c}heck$ at time T_n and using it to some other time T_{n+1} to pass the revocation checking process. Hence, proposed method has proved secured when undertaking the replay attacks.

5. Conclusion

Performance evaluation of the proposed algorithm is illustrated with numerical results that are obtained from NS-2 simulations for an intelligent vehicular system in random city scenarios with different vehicle density and for different keys size of 128, 192 and 256 bits. It has been observed that variation in key size does not significantly affect the performance of the system. Also, a lower authentication is achieved with lower delay when the proposed algorithm is compared with EMAP. Also, an improved packet delivery ratio is guaranteed when the default scheme is used. This paper focuses mainly on how grouping is done among the vehicles and an expedite authentication process is explained. The presented method uses a unique key distribution mechanism that permits an OBU to upgrade its jeopardize keys even though it has missed some previous revocations.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Supplementary data

Supplementary data associated with this article can be found, in the online version, athttps://doi.org/10.1016/j.apacoust.2020.107331.

References

[1] IEEE trial-use standard for wireless access in vehicular environments – security services for applications and management messages, IEEE Std 1609.2-2006 (2006) 01–105.https://doi.org/10.1109/IEEESTD.2006.243731..

[2] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). Int J Inf Secur 2001;1(1):36–63. https://doi.org/10.1007/s102070100002.

[3] Laurendeau C, Barbeau M. Threats to security in DSRC/WAVE. In: Proceedings of the 5th International Conference on Ad-Hoc, Mobile, and Wireless Networks. Berlin, Heidelberg: Springer-Verlag; 2006. p. 266–79. https://doi.org/10.1007/11814764_22.

[4] Raya M, Hubaux J-P. Securing vehicular ad hoc networks. J Comput Secur 2007;15(1):39–68.

[5] Wasef A, Shen X. EMAP: expedite message authentication protocol for vehicular ad hoc networks. IEEE Trans Mob Comput 2013;12(1):78–89. https://doi.org/10.1109/TMC.2011.246.

[6] Zhang C, Lin X, Lu R, Ho P, Shen X. An efficient message authentication scheme for vehicular communications. IEEE Trans Veh Technol 2008;57(6):3357–68. https://doi.org/10.1109/TVT.2008.928581.

[7] Jhang M, Liao W. On cooperative and opportunistic channel access for vehicle to roadside (V2R) communications. IEEE GLOBECOM 2008–2008 IEEE Global Telecommunications Conference 2008:1–5. https://doi.org/10.1109/GLOCOM.2008.ECP.966.

[8] Perrig A, Canetti R, Tygar J, Briscoe B. Timed efficient stream loss-tolerant authentication (TESLA): multicast source authentication transform introduction, 2005..

[9] Raya M, Jungels D, Papadimitratos P, Aad I, Hubaux J-P. Certificate revocation in vehicular networks..

[10] Papadimitratos PP, Mezzour G, Hubaux J-P. Certificate revocation list distribution in vehicular communication systems. In: Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking, VANET '08. New York, NY, USA: Association for Computing Machinery; 2008. p. 86–7. https://doi.org/10.1145/1410043.1410062.

[11] Studer A, Shi E, Bai F, Perrig A. TACKing together efficient authentication, revocation, and privacy in VANETs. In: 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. p. 1–9. https://doi.org/10.1109/SAHCN.2009.5168976.

[12] Zhao S, Aggarwal A, Frost R, Bai X. A survey of applications of identity-based cryptography in mobile ad-hoc networks. IEEE Commun Surv Tutorials 2012;14(2):380–400. https://doi.org/10.1109/SURV.2011.020211.00045.

[13] Kim BH, Choi KY, Lee JH, Lee DH. Anonymous and traceable communication using tamper-proof device for vehicular ad hoc networks. In: 2007 International Conference on Convergence Information Technology (ICCIT 2007). p. 681–6. https://doi.org/10.1109/ICCIT.2007.298.

[14] Sun X, Lin X, Ho P. Secure vehicular communications based on group signature and id-based signature scheme. IEEE Int Conf Commun 2007;2007:1539–45. https://doi.org/10.1109/ICC.2007.258.

[15] Chim T, Yiu S, Hui LC, Li VO. SPECS: secure and privacy enhancing communications schemes for VANETs. Ad Hoc Netw 2011;9(2):189–203. https://doi.org/10.1016/j.adhoc.2010.05.005.

[16] Chaum D, van Heyst E. Group signatures. In: Davies DW, editor. Advances in Cryptology — EUROCRYPT '91. Berlin Heidelberg, Berlin, Heidelberg: Springer; 1991. p. 257–65.

[17] Huang D, Misra S, Verma M, Xue G. PACP: an efficient pseudonymous authentication-based conditional privacy protocol for VANETs. IEEE Trans Intell Transp Syst 2011;12(3):736–46. https://doi.org/10.1109/TITS.2011.2156790.

[18] Gamage C, Gras B, Crispo B, Tanenbaum AS. An identity-based ring signature scheme with enhanced privacy. Securecomm and Workshops 2006;2006:1–5. https://doi.org/10.1109/SECCOMW.2006.359554.

[19] Sun Y, Lu R, Lin X, Shen X, Su J. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. IEEE Trans Veh Technol 2010;59(7):3589–603. https://doi.org/10.1109/TVT.2010.2051468.

[20] Lin X, Sun X, Ho P, Shen X. GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans Veh Technol 2007;56(6):3442–56. https://doi.org/10.1109/TVT.2007.906878.

[21] Rabadi NM, Mahmud SM. Privacy protection among drivers in vehicle-to-vehicle communication networks. 2007 4th IEEE Consumer Communications and Networking Conference 2007:281–6. https://doi.org/10.1109/CCNC.2007.62.

[22] Zhang J, Ma L, Su W, Wang Y. Privacy-preserving authentication based on short group signature in vehicular networks. In: The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007). p. 138–42. https://doi.org/10.1109/ISDPE.2007.53.

[23] Liu D, Liu J, Mu Y, Susilo W, Wong D. Revocable ring signature. J Comput Sci Technol 2007;22:785–94. https://doi.org/10.1007/s11390-007-9096-5.

[24] Sun Y, Feng Z, Hu Q, Su J. An efficient distributed key management scheme for group-signature based anonymous authentication in VANET. Secur Commun Networks 2012;5:79–86. https://doi.org/10.1002/Section 302.

[25] Zheng D, Jing C, Guo R, Gao S, Wang L. A traceable blockchain-based access authentication system with privacy preservation in VANETs. IEEE Access 2019;7:117716–26. https://doi.org/10.1109/ACCESS.2019.2936575.

[26] Cui J, Wu D, Zhang J, Xu Y, Zhong H. An efficient authentication scheme based on semi-trusted authority in VANETs. IEEE Trans Veh Technol 2019;68(3):2972–86. https://doi.org/10.1109/TVT.2019.2896018.

[27] Liu L, Wang Y, Zhang J, Yang Q. Efficient proxy ring signature for VANET. J Eng 2019;2019(9):5449–54. https://doi.org/10.1049/joe.2018.5311.

[28] Zhou J, Cao Z, Qin Z, Dong X, Ren K. LPPA: lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in vanets. IEEE Trans Inf Forensics Secur 2020;15:420–34. https://doi.org/10.1109/TIFS.2019.2923156.

[29] Li X, Ye X, An L. Research on optimizing strategy for self-adaptively adjusting the contention windows of broadcasting in vanet based on the model of vehicle fleet. 2012 Fifth International Symposium on Computational Intelligence and Design, vol. 1. p. 468–71. https://doi.org/10.1109/ISCID.2012.123.

[30] Issariyakul T, Hossain E. Introduction to Network Simulator NS2. 1st Edition. Incorporated: Springer Publishing Company; 2010.

[31] Härri J, Filali F, Bonnet C, Fiore M. Vanetmobisim: generating realistic mobility patterns for VANETs. In: Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks, VANET '06. New York, NY, USA: Association for Computing Machinery; 2006. p. 96–7. https://doi.org/10.1145/1161064.1161084.

[32] Frankel S, Glenn R, Kelly S. RFC3602: the AES-CBC cipher algorithm and its use with IPSection; 2003..