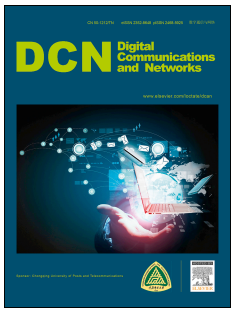


An efficient voting based decentralized revocation protocol for vehicular ad hoc networks

Miraj Asghar, Lei Pan, Robin Doss

PII: S2352-8648(19)30016-1

DOI: https://doi.org/10.1016/j.dcan.2020.03.001

Reference: DCAN 200

To appear in: *Digital Communications and Networks*

Received Date: 15 January 2019

Revised Date: 19 February 2020

Accepted Date: 28 March 2020

Please cite this article as: M. Asghar, L. Pan, R. Doss, An efficient voting based decentralized revocation protocol for vehicular ad hoc networks, *Digital Communications and Networks* (2020), doi: https://doi.org/10.1016/j.dcan.2020.03.001.

Digital Communications and Networks (DCN)

Journal Pre-proof

HOSTED BY

Available online at www.sciencedirect.com

ScienceDirect

Journal homepage: www.elsevier.com/locate/dcn

An efficient voting based decentralized revocation protocol for vehicular ad hoc networks

Miraj Asghar*[a], Lei Pan[b], Robin Doss[c]

[a] **Centre for Cyber Security Research and Innovation (CSRI), Deakin University, Geelong, 3220, Australia**
[b] **Centre for Cyber Security Research and Innovation (CSRI), Deakin University, Geelong, 3220, Australia**
[c] **Centre for Cyber Security Research and Innovation (CSRI), Deakin University, Geelong, 3220, Australia**

Abstract

Vehicular Ad-hoc NETworks (VANETs) enable cooperative behaviors in vehicular environments and are seen as an integral component of Intelligent Transportation Systems (ITSs). The security of VANETs is crucial for their successful deployment and widespread adoption. A critical aspect of preserving the security and privacy of VANETs is the efficient revocation of the ability of misbehaving or malicious vehicles to participate in the network. This is normally achieved by revoking the validity of the digital certificates of the offending nodes and by maintaining and distributing an accurate Certificate Revocation List (CRL). The immediate revocation of misbehaving vehicles is of prime importance for the safety of other vehicles and users. In this paper, we present a decentralized revocation approach based on Shamir's secret sharing to revoke misbehaving vehicles with very low delays. Besides enhancing VANETs' security, our proposed protocol limits the size of the revocation list to the number of the revoked vehicles. Consequently, the authentication process is more efficient and the communication overhead is reduced. We experimentally evaluate our protocol to demonstrate that it provides a reliable solution to the scalability, efficiency and security of VANETs.

KEYWORDS: VANETs, Security, Authentication, Public key infrastructure, Decentralized revocation

1. Introduction

Vehicular Ad-hoc NETworks (VANETs) are seen as a fundamental component of Intelligent Transportation Systems (ITSs) and connect vehicles through wireless communication technologies. The main objective of the ITS is to improve the safety and comfort of drivers and passengers. As a key part of the ITS, VANETs allow vehicles to communicate with other vehicles and roadside infrastructures. In terms of communication, both Vehicle-To-Vehicle (V2V) communication and Vehicle-To-Infrastructure (V2I) communication are envisaged and Fig. 1 depicts a typical VANET architecture with On-Board Units (OBUs) in vehicles broadcasting safety and traffic-related information. The wireless communication between vehicles or between vehicle and infrastructure is vulnerable to several security attacks and a fundamental requirement for mitigating such attacks and securing VANETs is the authentication of vehicles before allowing them to participate in the VANET. Public Key Infrastructure (PKI) based authentication is the most viable mechanism for securing VANETs. It can meet most of VANETs' security requirements. However, the PKI is unable to provide certain security requirements, such as location privacy, efficient authentication, and distributed and fair revocation [1]. A critical aspect of PKI-based authentication schemes is efficient revocation of certificates issued to misbehaving or malicious

vehicles in order to exclude them from the network. Traditionally, PKI schemes rely on the use of a centralized Certificate.

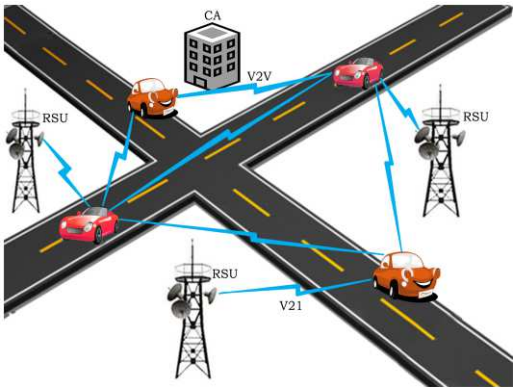


Fig. 1. VANETs Architecture

Revocation List (CRL) for checking the currency of a certificate and by associating the legitimacy of a vehicle.

In traditional PKI-based authentication, if an RSU or vehicle detects any misbehaving or malicious vehicle(s), it will report the incident to the Central Authority (CA). After confirming liability through investigation, the CA will add all certificates of the revoked vehicle into the CRL. Therefore, the CA is solely responsible for adding certificate information of the revoked vehicle to the CRL. The updated CRL is then broadcast by the CA to the Road Side Units (RSUs) and vehicles.

Centralized revocation involves considerable time delay caused by reporting, investigation and updating of the CRL with thousands of certificates and then finally broadcasting a CRL of enormous size. This totally centralized way of updating and broadcasting the CRL makes the revocation procedure inefficient. In practice, the revocation of misbehaving vehicles should take place as fast as possible to prevent these vehicles from participating in the network and jeopardizing the safety of other vehicles.

One practical solution to this problem is decentralized revocation. In the decentralized revocation, the vehicles are capable of revoking any malicious or misbehaving vehicle within their communication range. This can be achieved through a consensus based on a secure voting procedure.

The vehicles within the communication range of a misbehaving or malicious vehicle are regarded as neighbour vehicles. One or more neighbour vehicles can initiate a voting procedure to confirm the revocation of the malicious vehicle. If a threshold of required votes is met, all certificates of the malicious vehicle are added to the CRL. This restricts the ability of a malicious vehicle to send or receive information immediately.

Decentralized revocation is more efficient as the vehicles do not need to wait for a CA to take action and they can preserve their privacy and network security by revoking the privileges of a malicious vehicle straightaway. This prevents misbehaving vehicles from continuing to exploit the network until the CA updates and broadcasts the CRL as in the centralized revocation.

In traditional PKI-based authentication, each vehicle is assigned thousands of certificates and corresponding public–private keys by the CA. The network scale of VANETs is expected to be very large. Whenever a vehicle will be revoked, thousands of its certificates will be added to the CRL by the CA. Hence, the size of the CRL is expected to be enormous. Based on the Dedicated Short-Range Communications (DSRC) standard, each vehicle is required to broadcast a message every 300ms. These messages include the vehicle's current position, speed, and other telemetry information. In such a scenario, vehicles will receive a large number of signed messages every 300ms.

The receiving vehicles will have to verify each message before processing it. The verification process includes making sure that the sending vehicle is not revoked by the CA. To do so, the receiving vehicle will match the certificate in the message with those in the CRL. This checking process is expected to be time consuming due to the enormous amount of entries in the CRL. The ability for each vehicle to check the CRL and verify the sender's signatures on the received messages in a timely manner forms an inevitable challenge for the PKI. Other than the CRL check delay, the distribution of fairly sized CRLs is prone to have long delays. Also, during the early deployment of VANETs, it is expected that RSUs will be sporadically distributed in the network. This will also be unfavorable for the efficient dissemination of an updated CRL.

We address the above mentioned issues related to efficient certificate revocation in this paper. We limit the size of the CRL to the number of the revoked vehicles, i.e., $O(n)$ with a single entry for each revoked vehicle. The significant reduction in the size of CRL in return reduces the CRL processing time. The receiving vehicles will be able to verify messages quickly. The CRL is updated and distributed locally by the vehicles, therefore, the dissemination of CRL over the network is more effective.

This paper makes the following contributions:

1. We propose a provably secure and efficient revocation protocol. The proposed Efficient Decentralized Revocation Protocol (EDRP) enables decentralized revocation in a secure and effective way. We address the security, scalability and efficiency issues of a PKI-based solution through this novel protocol.
2. The EDRP makes certificates of a vehicle linkable if it is revoked. All certificates of revoked vehicles are linkable through a linking public key. The CRL therefore has a single linking public key value against each vehicle, resulting in a reduced linear complexity and size of the CRL.
3. The EDRP makes the revocation procedure decentralized. The vehicles with secret shares from the CA can vote to revoke a misbehaving vehicle. The revocation does not involve the CA or RSUs. Also, the CRL is locally disseminated by vehicles. The EDRP not only improves the security of users but also significantly reduces the communication and computational overhead for VANETs.

In order to clarify the scope of this work, we state that this protocol is designed to revoke any misbehaving or malicious vehicle in a decentralized manner through a voting procedure. Regarding the voting procedure, we assume that the majority of the voting vehicles are honest and the malicious behaviors can be detected with simple statistics. So we do not consider the details of the malicious node detection system. Instead, we focus on the immediate revocation of a faulty node or the adversary. We refer to some examples of the malicious or misbehaving node detection systems in [2, 3, 4].

The rest of this paper is organized as follows: Section 2 lists the related work where we identify the research gaps. Section 3 introduces the system architecture and our design goals. Section 4 briefly lists the preliminary knowledge of secret sharing and elliptic curves, before Section 5 proposes the detailed protocol of EDRP. The security analysis is in Section 6. And the experimental studies are in Section 7. Finally, Section 8 concludes this paper.

2. Related Work

In literature, researchers adopted diverse approaches to provide security and privacy in VANETs. Group signature based schemes [5][6][7] allow vehicles in a group communicate anonymously as group members. Only the group manager is privileged to identify a vehicle if it behaves maliciously.

This keeps conditional anonymity in the system. The size of the CRL is linear to the revoked vehicles
but the CRL checking operation consists of two pairing operations. This adds significant computational overhead resulting in long delays and further leading high message loss [8].

J. Shao *et al.* in [9] proposed a group signature-based threshold anonymous authentication protocol. The protocol allows the disclosure of the identity of a vehicle who generates two different signatures on the same message. Each vehicle gets a group certificate from the RSU to communicate as an anonymous group member. As the RSU is checking the CRL before assigning a group certificate, therefore, each OBU needs not to retrieve the CRL from the Trusted Authority (TA).

The protocol proposed by J. Shao *et al.* will suffer
from delay in processing group certificate requests by enormous vehicles in dense traffic. The protocol also applies the requirement for evenly distributed RSUs to protect the privacy of users.

Group signatures achieve a certain level of security and privacy but pose challenges, such as group manager selection, dynamic group management and high dependency on infrastructure still prevails [10, 11].

Pseudonym-based authentication schemes [12, 13,
14, 15] use pseudonyms to protect the identity privacy of users and do not suffer the above-mentioned limitations. The pseudonyms are either preloaded in Temper Proof Device (TPD), assigned by RSUs or generated by OBUs themselves.

D. Huang *et al.* in [16] proposed a computationally
efficient pseudonym generation scheme in which vehicles generate pseudonyms by themselves. However, the high speed of vehicles obstruct the dynamic re-computation of pseudonyms.

U. Rajput *et al.* in [13] introduced a hierarchy of pseudonyms to protect the anonymity of the users. The primary pseudonyms are generated by the TA and assigned to a vehicle on registration, Whereas secondary pseudonyms (short term) are issued by RSUs on request. On each secondary pseudonym request, the RSU involves the TA for verification of the legitimacy of a vehicle which adds extra communication cost and significant computational overhead on the TA, although the revocation check is efficient due to the lesser amount of primary pseudonyms. Furthermore, in case of unavailability of a RSU, the vehicle has to use a secondary

pseudonym for a longer period, therefore threatening users' privacy.

Later, U. Rajput *et al.* [14] proposed a hybrid approach to elevate the burden of pseudonym generation from the TA and the dependency on RSUs. The new scheme manipulates useful features of both the pseudonym-based and group signature-based approaches. The authors introduced a region-based CA which is responsible for the generation, verification and management of pseudonyms. The pseudonym-based authentication schemes remarkably accelerate message authentication, however, the CRL check process causes high message loss ratio due to the enormous amount of pseudonyms [17].

Identity-Based Signature Verification (IBSV) schemes [18, 19, 20] utilize identity information of user to generate public-private keys. IBVS schemes in the literature mostly integrate pseudonyms which ensures conditional anonymity along with integrity and confidentiality of messages. N. W. Lo [20] proposed an IBVS scheme with batch verification. Batch authentication allows the verification of many messages simultaneously but always come with re-batch overhead if there is an invalid message or request in the batch. The authors introduced the trusted third party which assigns a master private key and a public key to the requesting vehicle. The scheme requires preloaded short-term pseudo-identities and private keys, which poses significant storage and CRL checking overhead.

Researchers also explored the Hash Message Authentication Code (HMAC) as a solution to the time consuming CRL check [21, 17, 22, 23]. X. Zhu *et al.* [23] utilized both group signatures and pseudonyms to reduce the overhead of CRL checking process. They used HMAC to replace the CRL checking and introduced cooperative authentication among vehicles.

Another recent approach based on HMAC was proposed by S. Jiang *et al.* [17], where different domains are considered to apply group key-based communication. On joining the new domain, RSUs authenticate vehicles by calculating the HMAC instead of checking the CRL. The protocol allows batch verification and removes the CRL check process, therefore, the message loss ratio is reduced significantly as compared with schemes in [18, 16, 21].

PKI-based authentication schemes for VANETs do not suffer from key escrow or group management constraints like in IBVS and group-based authentication schemes. These schemes apply digital signatures using mostly asymmetric cryptography to ensure data authentication and non-repudiation.

For user authentication, the CA generates thousands of certificates for each user to bind the user public key to its identity. These certificates can not reveal the real identity of the user, therefore, are anonymous. If a vehicle is revoked, all of its certificates are added to the CRL, which is checked before user authentication or message verification. Researchers claimed PKI as a most viable, comprehensive and promising solution for VANETs' privacy and security [21, 24, 25].

In PKI-based VANETs, the authentication of messages includes, first, checking CRL to find if the sender's certificate is revoked, and then verifying the certificate. Vehicles are assigned around 10,000 to 30,000 certificates to protect the privacy of the user. Fewer certificates force the user to use a certificate for a long period of time which can lead to privacy leakage. Therefore, the PKI enforces large number of certificates to protect user's privacy.

The scale of VANETs is expected to be very large due to day by day increase in different types of vehicles on roads. In 2016, there were around 537 million vehicles in the US according to United States Bureau of Transit Statistics [26]. Therefore, the size of CRL is expected to be reasonably large.

The authentication schemes based on traditional PKIs as in [27] are inadequate for time-critical safety applications offered by VANETs. VANETs based on WAVE standard requires requests and messages to be authenticated and verified in less than few 100ms, whereas future communication technology based on 5G will require a delay of less than 1ms.

The authors in [28, 29, 30, 31] adopted different strategies to deal with the CRL check overhead. Studer *et al.* [28] introduced a hierarchical system model consisting of a TA and regional authorities. Group signatures are applied to manage groups under different regional authorities. Vehicles sign their certificates, using the group key to update their certificates which are valid for a specific region. Regional authorities verify the group signature of vehicles and check the CRL before authentication. Each vehicle has to wait for a few seconds before being authenticated by the regional authority. It is unable to send messages when it reaches a new region until the regional authority authenticates the vehicle.

P. Papadimitratos *et al.* [29] distributes CRL as small pieces in the network. Haas *et al.* [30] broadcast just a single secret key into the network

and vehicles generate all certificates of the revoked vehicle using that secret key. Laber *et al.* [31] utilized V2V communication to disseminate CRL in the network.

A. Wasef *et al.* [21] used the HMAC to replace the CRL checking process in VANETs. The proposed system model is based on a PKI system, where each OBU is preloaded with certificates, secret keys, and corresponding public keys. The secret keys are used to calculate HMAC of a message and are shared among the non-revoked vehicles. In case of key compromise, the OBUs can update keys corresponding to the compromised keys. The message loss ratio is significantly less than the linear and binary search. The protocol achieves an average authentication delay of 710ms when 200 vehicles are in communication range.

The authentication schemes we have discussed so far deals with mandatory security and privacy-related issues in VANETs. One of the major security and privacy concerns left behind is raised in a situation when any misbehaving or malicious user gets enough time span to abuse the network until it is revoked by CA. VANETs pose real-time requirements not only for user authentication and message verification but also for the revocation. This inevitable problem grabbed the attention of just few authors [32, 33, 34] so far.

Raya *et al.* [32] introduced a node eviction scheme consisting of two components, localized Misbehavior Detection System (MDS) and Local Eviction of Attackers by Voting Evaluators (LEAVE). These components make the misbehaving node secluded by neighboring vehicles until the CA issues a centralized revocation for the vehicle. LEAVE allows vehicles to detect an attacker or malicious user in the neighborhood and the outcome can also be served as an input to MDS.

The Raya *et al.* scheme also reduced both the CRL checking time and the size of CRL by using Bloom filters. However, according to the probabilistic nature of Bloom filters, there are chances of innocent vehicles to be revoked as well. Additional computational overhead is involved as each vehicle has to update the Bloom filter on receiving revocation information of newly revoked vehicles from RSUs. Raya *et al.* [33] employed a game theory method to model the localized certificate revocation process.

An Efficient Decentralized Revocation (EDR) protocol is proposed in [34]. The Authors used a pairing-based threshold scheme to revoke any malicious certificate in a decentralized manner. The revoked certificate is disseminated in the neighborhood so that legitimate vehicles do not accept messages containing a revoked certificate. The protocol only revokes a single certificate from the malicious user, if the vehicle changes the certificate, it can again pretend as a legitimate vehicle.

There are many different studies which aim to reduce the computational and communication complexities related to the CRL [21, 29, 30]. However, they do not address the security and privacy challenges of a centralized revocation system. There are very few approaches to efficient revocation where neighbouring vehicles are capable of revoking a misbehaving or malicious vehicle [32, 34]. These schemes are capable of revoking a single certificate of a vehicle. If the vehicle changes its certificate, again it is able to threaten the security of the network and the privacy of users. Our scheme not only addresses the complex issues related to CRL management but also achieves higher security and privacy levels through a decentralized revocation.

3. System architecture and design goals

3.1. System architecture

We consider VANETs architecture based on the following three entities:

- CA: We assume the CA as a fully trusted authority having sufficient storage and computational capabilities. It generates cryptographic materials for each vehicle. The CA can uniquely identify a vehicle on the basis of vehicle model number, user identity, etc. It has secured connection with RSUs, therefore, it can pass on secret information to RSUs and vice versa.
- RSUs: The RSU authenticates the OBUs to legitimately receive safety and value-added services on entering its domain. RSUs are equipped with a device embedded with a wireless communication module based on the IEEE 802.11p standard. RSUs communicate with OBUs through wireless insecure connection whereas connecting to the CA securely through wired connection. Hence the RSU can send and receive the updated CRL to and from the CA securely. THe RSU plays no active role in the revocation process as the revocation procedure is totally decentralized.

- OBUs: The OBU is responsible for broadcasting safety and traffic management related information periodically. OBUs support IEEE 802.11p standard for communication. The CA assigns a secret share to each vehicle which enables the vehicle to participate in the voting procedure. The OBU has a Temper Proof Device (TPD) which securely stores the vehicle's certificates and secret share.

3.2. Our design goals

1. Enhancing Security of VANETs: Conventionally, the PKI-based authentication depends on a centralized revocation system. The CA is a single authority entitled to revoke a malicious user. When any malicious vehicle is revoked, the CA adds all of its certificates to CRL and broadcasts the updated CRL. The malicious user keeps on abusing the network until the updated CRL is disseminated to all entities in the network. This delay makes other users' security and privacy at a high risk.
   The EDPR allows immediate revocation of misbehaving or malicious vehicles. The updated CRL is instantly disseminated to the neighborhood vehicles in a local manner. Neighborhood vehicles then stop processing messages from the revoked vehicle. This restricts the revoked vehicle to continue exploiting the network, hence, enhancing the security and privacy of users in the VANETs.
2. Reducing communication overhead: The scalability of VANETs is always challenging for the PKI-based authentication system. Thousands of certificates of each revoked vehicle will immensely increase the size of CRL. The huge size of the CRL will add significant communication overhead for the network.
   In our proposed protocol, the large-sized CRL is replaced with a linearly sized CRL. No matter how many certificates a revoked vehicle owns, the CRL will have a single linking public key for that revoked vehicle. This will significantly reduce the communication overhead and makes the PKI feasible for a scalable VANET system.
3. Improving authentication efficiency: Normally, to find the authenticity of an authentication request, the authenticating entity (vehicle or RSU) checks the CRL. If the certificate attached with message exists in the CRL, the message is discarded; otherwise, it is processed. The efficiency of authentication therefore heavily depends on the CRL checking process.
   The conventional CRL is expected to have innumerable certificates. The CRL checking process consequently causes extra delay for the authentication of request. In the EDRP, the entries in the CRL are linear to the revoked vehicles. Therefore, the authentication process is very efficient.

Table 1. Notations

Notations	Descriptions
$\|\|$	Message Concatenation
n	The vehicle n
Pub_n/Pr_n	Public and private key pair of vehicle n
g	A large prime number
$S\ hares$	K shares distributed by CA
K	Minimum number of shares required for revocation
SrT_n	Unique secret generated by CA for vehicle n
S	The secret share of CA
CN	The certificate number
$pubL_n/prL_n$	Public and Private linking keys of vehicle n
$EnPubL_n$	Encrypted public linking key of vehicle n
$Cert_n$	The certificate that belongs to vehicle n
TS	The current time stamp
M	The message

M_r	The revocation message
Sig_n	Signature of vehicle n

4. Preliminaries

4.1. Shamir secret sharing scheme

The Shamir's Secret Sharing Scheme (SSSS) for cryptography was introduced by Adi Shamir. In SSSS, the shares of a unique secret are distributed among n users. To recover a particular, secret at least k unique shares from users are required. Note that $k \leq n$. Therefore, not all the shares of secret are required to recover the actual secret. The SSSS has information-theoretic security, which means an attacker cannot break the cryptosystem. The attacker cannot get sufficient information to threaten the security even if it has unlimited computational power.

4.2. Elliptic Curve Cryptography (ECC)

The ECC proposed by Neil Koblitz and Victor Miller in 1985 is based on the algebraic structure of elliptic curves over the finite fields. The ECC is a more efficient alternative to other cryptographic systems as it provides the same security using smaller keys.

The security of ECC depends on the computation of discrete logarithm in a group of points over an elliptic curve. The difficulty of solving the Elliptic Curve Discrete Logarithmic Problem (ECDLP) depends on the size of n, where n is the number of points in the specified group. A reasonable size of n takes a very long period of time for solving the ECDLP [35]. The investigation shows that the discrete logarithm problem in the elliptic curve is as hard as in any other groups [36].

5. EDRP

In VANETs, vehicles frequently broadcast safety related messages. Vehicles attach signed certificates with the safety messages they broadcast, which allow the receiver of the message to verify the sender. In our scheme, the CA assigns these certificates to vehicles in the registration process. The CA keeps the identity information of vehicles so that later, if needed, the CA can track the vehicle.

During the registration process, the CA also distributes the secret shares among the registered vehicles. These shares allow vehicles to take part in the decentralized revocation though voting. We explain system initialization, message authentication and decentralized revocation procedures in this section. Table 1 lists the notations that we use for explaining the proposed algorithms.

5.1. System initialization

5.1.1. Shares Calculation and Distribution

In the system initialization phase, the CA performs some computations to calculate shares to distribute into the network. Suppose, n is total number of vehicles want to register with the CA to use the VANET's services. The CA calculates k number of shares $S\ hare_k$, which are used to derive the secret $S\ rT_n$ for each vehicle n. The $S\ rT_n$ is unique for each vehicle n. Disclosure of secret $S\ rT_n$ will allow vehicles to link all of the certificates belonging to vehicle n in case of revocation. Each share $S\ hare_k$ is distributed into the network and any legitimate vehicle with $S\ hare_k$ can initiate or participate in the decentralized revocation procedure. Note that the shares will be repeated on a random assignment, therefore more than one vehicle can have the same share.

5.1.2. Certificate assignment

To generate certificates for each vehicle n, the CA performs the following steps:

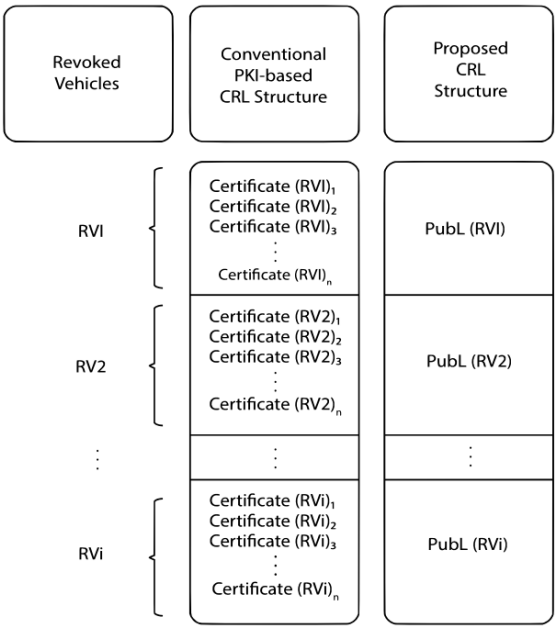


Fig. 2. The proposed CRL v.s. a conventional PKI CRL

- the CA generates a linking public/private key pair $pubL_n = prL_n$.
- The CA calculates the unique secret share s_n for itself.

- The CA then derives a unique secret $S\,rT_n$ using s_n and $S\,hares_k$ shares.
- The vehicle n is assigned a single share $S\,hare_k$ out of total K shares.
- The CA generates a large prime number g_n to calculate

$$g_n^{S_n} \tag{1}$$

and

$$g_n^{SrT_n} \tag{2}$$

- The CA encrypts the vehicle's linking public key $pubL_n$ with $gS\,rT_n$ to get $EnPubL_n$.
- The CA generates a pseudo-random unique certificate number CN_n^i for each certificate of the vehicle.
- The CA generates the public/private key pair Pub_n^i/Pr_n^i. Pub_n^i/Pr_n^i denotes the i^{th} public/private key pair for the nth vehicle.
- The CA uses the private linking key prL_n to sign the certificate number CN_n. $S\,igL_n$ stands for the linking signature which reveals the revocation status of the specific certificate.
- the CA attaches its share in form of g_n s with the certificate.
- The CA signs the certificate number CN_n^i, base g_n, encrypted linking value $EnPubL_n$, linking signature $S\,igL_n$ and public linking key Pub_n^i with its private key.

5.1.3. Certificate structure

Table 2 shows the structure of each certificate of a vehicle n. The certificates consist of the following fields:

- Certificate number CN_n: A pseudo-random, unique number for the certificate.
- Base g_n: A large prime used for Shamir's secret sharing calculations.
- Encrypted linking value $EnPubL_n$: A public key value common to all certificates issued to a user. It is encrypted using a key protected by Shamir's secret sharing.
- Linking signature $S\,igL_n$: The signature on the certificate number CN_n using the linking private key PrL_n.
- CA share g_n^s: CA's share s_n represented in form of g_n^s.
- A public key Pub_n^i of vehicle v_n.
- CA signature on all of the above fields.

Any certificate $Cert_n$ belonging to vehicle v_n can be represented as follows:

$$Cert_n = SigCA(CN_n, g_n, EnpubL_n\ \ SigL_n, g_n^s, Pub_n^i) \tag{3}$$

5.2. Message authentication

Let us consider a scenario where a vehicle n wants to broadcast a message M to the RSU and other vehicles in the range. We refer the receiving RSU or vehicle as R_j. The message broadcasting vehicle n will attach any randomly selected a certificate $Cert_n$ with the message M along with the current timestamp TS before broadcasting it into the network.

$$(SigCA(CN_n, g_n, EnPubL_n, S\,igL_n, g_n^s, Pub_n^i) \parallel (Sig_n^i(M \mid TS)) \tag{4}$$

Here $Sig_n^i(M \mid TS)$ refers to the signature of vehicle n using its private key Pr_n^i. The receiver of the message then verifies the received broadcast message by executing Algorithm 1.

Algorithm 1 Verification of Message

Require: $SigCA(CN_n, g_n, EnPubL_n, SigL_n, g_n^s, Pub_n^i) \parallel (Sig_n^i(M \mid TS))$

Check validity of time stamp TS
if *invalid* **then**
  Discard the message
else
  Verify the CA signature on $Cert_n$
  if *invalid* **then**
    Discard the message
  else
    Verify the Signature $(Sig_n^i(M \mid TS))$
    if *invalid* **then**
      Discard the message
    else
      Decrypt $S\,igL_n$ with each value in CRL
      if Decrypted value = CN_n **then**
        Discard the message
      else
        Process the message
      end if
    end if
  end if
end if

5.3. Decentralized revocation

A misbehaving or malicious vehicle refers to an internal or external attacker. An adversary or misbehaving node detection system can identify a message as a fake or deceiving message. In case a fake message is sent by vehicle A to vehicle B, and vehicle B identifies the message as coming from a malicious or misbehaving vehicle. Then vehicle B can initiate a voting procedure against vehicle A. We refer the malicious or misbehaving vehicle as the target vehicle for simplification.

In order to revoke a target vehicle, there must be a consensus of K neighborhood peers, each of which
possesses a Shamir's secret sharing share assigned by the CA. We explain the voting procedure based on SSSS as follows.

5.3.1. Voting procedure

We assume that there are at least $k + 1$ vehicles in the communication range of an RSU and vehicle v_t is the target vehicle. A legitimate vehicle v_x receives a message M_t with $cert_t$ from the target vehicle V_t.

$$M_t = (SigCA(CN_t, g_t, EnPubL_t, g_t^s, Pub_t^i) \| (Sig_t^i(M_m \mid TS)) \quad (5)$$

Note that v_t != v_x and x <= K. The following steps describe the voting procedure initiated by vehicle v_x.

- Vehicle v_x extracts the base g_t and g_{ts} from M_t. Then v_x uses its own share to compute a vote result value p, where p is the aggregate value that a vehicle has after adding its share. It subsequently broadcasts this value with the actual message from the target vehicle so that other vehicles can pursue the process.

$$p = g^{\prod_{\forall j \in K | j \neq i}(S_x)} * g_t^s \quad (6)$$

- Vehicle v_x broadcasts a revocation message M_r1
consisting of the original message M_t from v_t signed by v_x. Vehicle v_x attaches its certificate with M_r.

$$M_{r1} = Sig_x^i(M_t, P) \| (SigCA(CN_x, gx, EnpubL_x, SigL_x, g_x^s, Pub_x^i)) \quad (7)$$

- If vehicle v_y has received M_r and then decides to
participate in the voting procedure against vehicle v_t, vehicle v_y then calculates a vote result q using its own secret share.

$$q = g^{\prod_{\forall j \in K | j \neq i}(S_y)} * p \quad (8)$$

- Vehicle v_y (where y <= K) broadcasts a new revocation message M_{r2} consisting of message M_{r1} from v_x. Vehicle v_y attaches its certificate alongside with M_{r2}.

$$M_{r2} = Sig_y^i(M_{r1}, q) \| (SigCa(CN_y, g_y, EnPubL_y, g_y^s, Pub_x^i)) \quad (9)$$

- The vehicles continue this procedure of computing the voting result using their own shares and keep broadcasting the revocation message until the vehicles with K unique shares contribute in the voting.

In the above voting procedure, a vehicle may receive a revocation message where its share has already been contributed. The vehicle will then ignore the message. Any vehicle getting revocation message M_{r1} from vehicle v_x will execute Algorithm 2.

5.3.2. Linkability of revoked certificates and linearity of CRL

The last participating vehicle v_k which will contribute the K-th share in the voting procedure gets a final vote result f. This vote result f is actually the secret with which the public key of vehicle v_t is encrypted. Vehicle v_k decrypts the $EnPubL_t$ and adds it to the current CRL. The verification of the message includes CRL checking as presented in Algorithm 1.

Fig. 2 gives a comparison of the conventional PKI based CRL structure with the proposed CRL structure. RV_1, RV_2,……, RV_i are any i number of revoked vehicles. The conventional CRL will contain all n number of certificates belonging to each revoked vehicle.

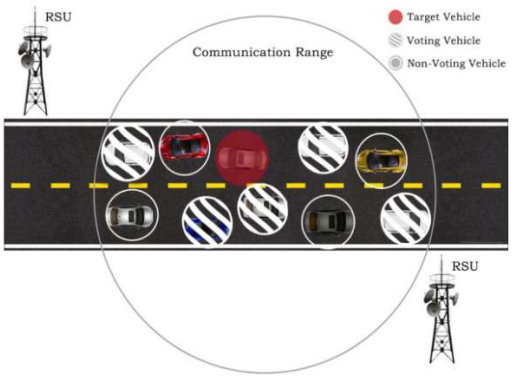


Fig. 3. A scenario of the voting procedure

Algorithm 2 The Voting Procedure

Require:
$\boldsymbol{v_y \leftarrow Sig_x^i(M_t, p)} \parallel$
$\boldsymbol{(SigCA_x(CN_x, g_x, EnPubL_x, SigL_x, g_x^s, PUB_x^i))}$

Verify CA signature S igCA$_x$
if *invalid* **then**
  Discard the message
else
  Verify $S\ ig_x^i(m_t, p)$
    if *invalid* **then**
      Discard the message
    else
      if declining to vote or its secret share is already contributed **then**
        Discard the message
      else
        Compute $p = g^{\prod \forall j \in K | j \neq i (s_y)} * p$
          if secret share is the K_{th} share **then**
            Add $EnPubL_t$ to CRL
          else
            Broadcast
$Sig_y^i(M_{r1}, q) \parallel$
            $(SigCA_y(CN_y, g_y, EnPubL_y, SigL_y, g_y^s, Pub_x^i))$
          endif
      endif
    endif
endif

Where as in the proposed CRL, there is a single public linking key *PubL* entry for each revoked vehicle.

When vehicle *s* sends a message to other vehicles or an RSU, the receiving vehicle or RSU will get *S igL$_s$* on certificate number *CN* from the certificate. The receiving entity will try to verify the linking signature *S igL$_s$*, using each linking public key *PubL* in the CRL. If any public key successfully decrypts the signed *CN* of the sender, then the sender is already revoked. Therefore, the receiving entity will discard the message.

6. Security analysis

6.1. Anonymous authentication and non-repudiation

The protocol is based on PKI, so all entities of the network use anonymous certificates signed by the CA for anonymity and authentication. The CA uses its private key to sign certificates of vehicles. Deriving the private key of the CA from its public key is an instance of the ECDLP. The similar analogy applies to private and public keys Pub_n=Pr_n of vehicles.

The EDRP applies digital signatures to achieve nonrepudiation. The vehicle signs the messages before broadcasting. The vehicle *n* signs the revocation message $S\ ig_n(M_r{=}TS)$ along with its certificate signed by the CA $S\ igCA(CN_n, g_n, EnPubL_n, SigL_n, g_n^s, Pub_n$. The security of the private key of the CA has a similar level as solving the ECDLP.

6.2. Resistance to colluding attacks

The EDRP requires each vehicle to pass a revocation check to participate the revocation process. If the candidate vehicle's public linking key *PubL* is found in the revocation list, the revocation message will be discarded by the next participating vehicle regardless of the share's validity it holds.

A fake revocation process can be initiated against any innocent target vehicle by a revoked vehicle. However, the success of such revocation needs at least *K* revoked vehicles or attackers with valid shares to collude. The probability of such a situation is very small. Because only a single legitimate vehicle in the range can abort such a fake revocation process.

6.3. Resistance to forgery attacks

To participate illicitly in the revocation process, the attacker needs to have a valid secret share *S hare$_k$* and the current private key Pr_n. Finding Pr_n and *S hare$_k$* has complexity of solving the ECDLP. The ECDLP is intractable, which means the security of ECDLP cannot be broken in a polynomial time.

The attacker can participate in the revocation process by stealing a single share of any legitimate vehicle. However, the attacker will not be able to find the secret *S rT$_n$*, which lets the attacker

disclose the public linking key $PubL_n$ of the target vehicle. To do so, the attacker needs all of the minimum K shares which are distributed among legitimate vehicles by the CA. The means Shamir's secret sharing algorithm can be forged if the attacker knows all of the shares which must be contributed to disclose a particular secret. In other words, the attacker needs to break the theoretical information security of Shamir's secret sharing algorithm.

6.4. Forward secrecy

During the revocation process, each vehicle broadcasts a revocation message M_i where i denotes the i-th participating vehicle. The message M_i has an aggregate vote result of all previous share contributions by vehicles. From this aggregate value, it is impossible to retrieve the previously contributed votes. Therefore, if a vehicle gets a revocation message, it cannot forward the information about the shares of other vehicles.

6.5. Resistance to replay attacks

Each vehicle n adds a current timestamp with the message and sign it $S\ ig_n(M{=}TS\ )$ before broadcasting. The timestamp is also attached with the revocation message $sig_n(M_r, q) \parallel (SigCA((CN_n, g_n, EnPubL_n, SigL_n, g_n^s, Pub_n))$, which a vehicle broadcasts after calculating the new vote result q.

We assume that revocation message M_r has a current timestamp TS . Therefore, no attacker can replay a message or revocation message from another vehicle later.

7. Performance evaluation

We compare the performance of the EDRP with two efficient revocation protocols: ABAH [17] and EMAP [21]. ABAH and EMAP use the HMAC verification to replace the time-consuming CRL checking used in pseudonym-based authentication schemes. ABAH offers batch verification as well. EMAP and ABAH apply Elliptic Curve Digital Signatures (ECDS) for protection against forgery as in the EDRP. Table 3 shows the simulation parameters used for evaluation of EDRP.

7.1. Computational complexity

7.1.1. Average authentication delay

The computational overhead of authentication consists of the revocation status check of the requesting OBU, the certificate verification, and the signature verification. The request or message is valid if all of the three verifications are valid. Fig. 4 compares the authentication delays caused by ABAH, EMAP and EDRP. For ABAH and EMAP, the CRL checking delay is excluded in comparison due to the HMAC verification delay. We do not consider the re-batch authentication delay for ABAH.

We evaluated the authentication delay caused by the EDRP for a wide range of messages, that is, from 10 to 250 messages. As the number of messages increases, each protocol takes more time to authenticate them. We show performance curves of the EDRP without and with the CRL check. We consider 1,000 revoked vehicles in the CRL in the latter case. In both cases, the EDRP outperforms ABAH and EMAP. For example, to authenticate 200 requests, ABAH takes 300*ms*, EMAP takes 476*ms* and EDRP 176*ms*.

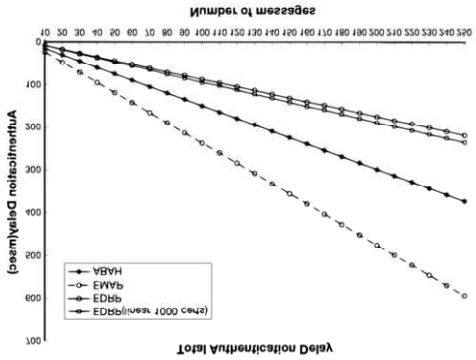


Fig. 4. Total authentication delay

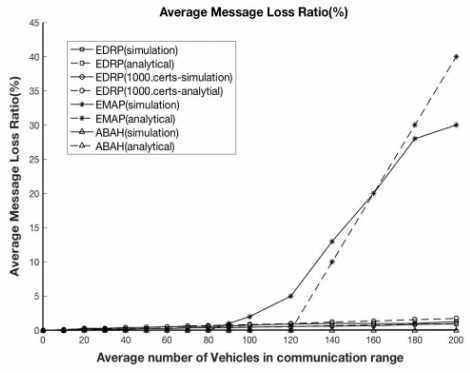


Fig. 5. Average message loss ratio

7.1.2. Message loss ratio

We simulate and analyze the message loss ratio for the range from 20 to 200 vehicles. Fig. 5 presents the comparison of messages loss ratios caused by the EDRP, ABAH, and EMAP. We consider both simulation results and analytical analysis. ABAH and EMAP consider the HMAC verification delay to compute the message loss ratio. ABAH needs a T_{hash} function to compute HMAC, which does not need $O(n)$ for a prior hash map construction or T_{str} for a string comparison as in EMAP. Therefore, the message loss ratio remains around zero. For the EDRP, we present results

Table 2. Certificate format

ID	Base	Link Val	linkSig	Share	Sig
4 bytes	4 bytes	12 bytes	4 bytes	4 bytes	28 bytes

Table 3. Simulation parameters

Simulation area	2500m x 2500m
Simulation time	100s
Speed of vehicle	20-30m/s
Wireless protocol	802.11p
Network Simulation tool	OMNET++
Vehicle information and dissemination interval	300ms
Wireless channel capacity	6Mbps

with and without the CRL check. For the 200 vehicles the message loss ratio with 1000 entries in the CRL is 1:2%. But, the ratio without the CRL check is 0:9%. It is evident from the graph that there is a slight increase in message loss ratio if the average number of vehicles in the communication range increases. The simulation result closely follows the analytical result. For analytical analysis, we denote T_{max} to be the total time consumed for processing a received message.

$$T_{max} = T_{cert} + T_{CRL} \quad (10)$$

Here T_{cert} is the time taken for validity check of a certificate. It includes a timestamp and signature validation. And T_{CRL} is the time consumed for checking the whole CRL. Let T_s be the time delay caused by checking one entry in the CRL and we have the following equation:

$$T_{CRL} = T_S * CRL_{size} \quad (11)$$

For simulatiom we set T_{cert} = 0.024ms. For CRL_{size} = 1000, the maximum computational complexity of a message authentication is T_{max} = 0.04ms.

The message loss ratio evaluated through simulation and analytical analysis for EDRP is almost identical.

7.2. Communication overhead

The communication overhead is the additional communication overhead caused by the increment of certificates and signature sizes. The additional message sizes for ABAH and EMAP are 92 bytes and 181 bytes, respectively. The additional size of the message for the EDRP is 52 bytes. Fig. 6 quantifies the impact of decreased message size on transmission delay for different numbers of

vehicles in the range. We compare the transmission delays for ABAH, EAMP and the EDRP. Four speeds of vehicles are considered — 0m/s, 10m/s, 20m/s and 30m/s. Graphs show that the transmission delay slightly varies under the various speeds. In particular, under all speeds and for an average number of vehicles in the range, the transmission delay for the EDRP is significantly less than ABAH and EMAP. For instance, the average transmission for ABAH is 0.69ms, 1.3ms for EMAP and 0.4ms for EDRP.

7.3. Decentralized revocation delay and success probability

7.3.1. Voting procedure delay

We investigate the cost in time and computations required for the immediate revocation procedure. The total time consumed for the calculation of all shares contributed by the neighborhood depends on the number of *K* shares. The voting procedure time for different numbers of *K* shares is given in Fig. 7. The cost grows linearly with respect to *K*. For example, it takes 29.7ms to calculate the vote result with 10 contributed shares, and 68.5ms for 20 shares.

7.3.2. Revocation success probability

The immediate revocation of any target vehicle requires the participation of vehicles with at least *K* unique shares. The probability of finding these shares in the neighborhood may vary with the number of vehicles in neighborhood *N*.

In Fig. 8, we observe the relations among the revocation success probability $P_{N,K}$, the number of vehicles in the range *N* and the required shares *K*. If the required number of shares *K* is less, there is a high possibility of finding *K* shares in the neighbourhood, resulting in a high success probability of revocation. Similarly, the large number of vehicles in the neighbourhood increases the chances of getting required *K* shares and helps achieve high revocation success probability. With $K = 5$, the success probability is 1 if there are 20 vehicles in the neighbourhood; whereas for $K = 10$, 45 vehicles should be in the communication range. Fig. 8 shows the general trend that a high rate of successful revocation associates with a large number
of shares and vehicles.

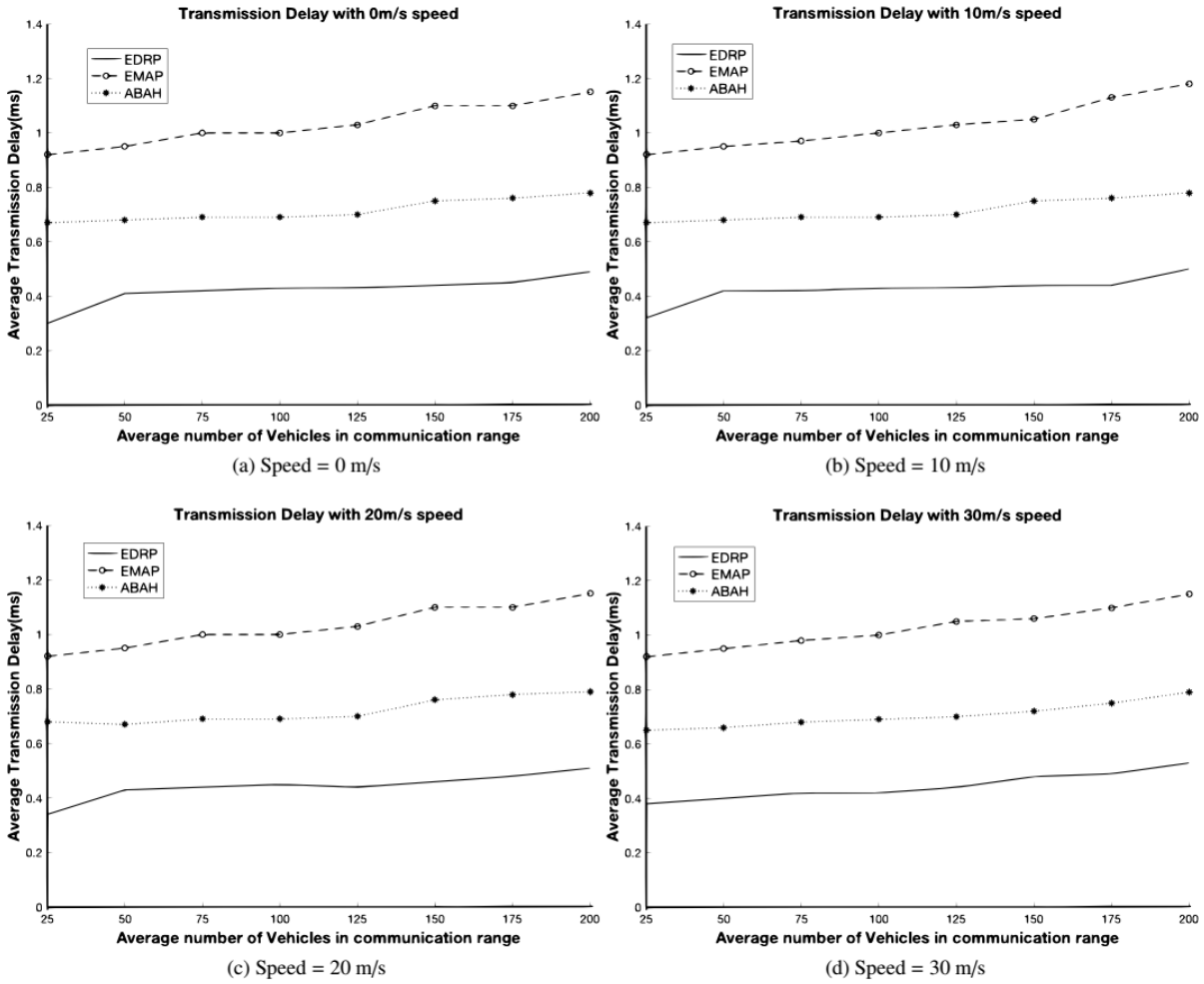


Fig. 6. Transmission delay at different speeds

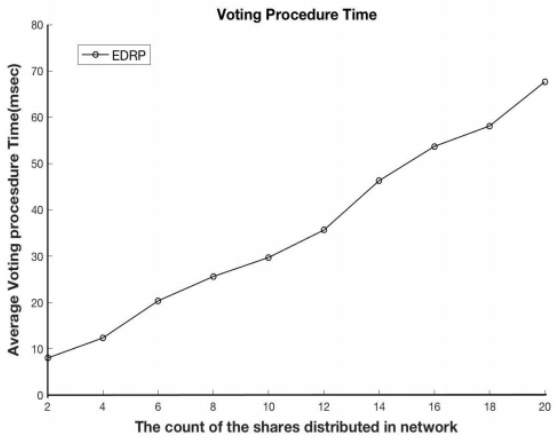


Fig. 7. Voting procedure delay

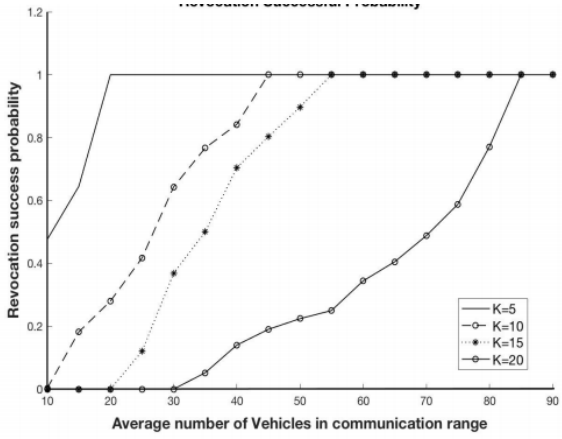


Fig. 8. Revocation success probability

The number of vehicles in the range, the number of shares required and the message loss ratio are the three important factors affecting the probability of successful revocation. That is, the revocation success decreases with the increment in the number of lost voting messages. The revocation success probability increases when it is easy to gather the number of required shares in the dense traffic. The revocation success may also increase when the number of required shares decreases in the neighborhood. Formally, we consider the traffic situation with N vehicles in the communication range. The voting procedure requires a contribution of K shares. The revocation success probability is denoted as $P_{N,K}$. On the other hand, the message loss ratio probability P_{Mlr} affects the revocation success probability $P_{N,K}$. Therefore the actual revocation success probability P_{Actual} is a combination of $P_{N,K}$ and P_{Mlr}, such that:

$$P_{Actual} = P_{N,K} * (1 - P_{Mlr}) \quad (12)$$

In Fig. 9, we investigate the effect of the message loss ratio, the number of vehicles in the range and the number of required shares on the revocation success probability. P_{Actual} achieves the highest value of 1 for approximately 30 vehicles in the range, even with the high message loss ratio of 30%, if the required shares are less than 5. The number of vehicles increases with the number of required shares. That is, if K = 20, 90 vehicles will be required in the range for success even if the message loss is 10%. There is a trade-off between success probability and the number of shares distributed into the network. Similar is the trade-off between success probability and message loss ratio. That is, more vehicles in range increase the probability of successful revocation.

8. Conclusions

We propose a novel protocol named as EDRP for vehicle authentication and digital certificate revocation of vehicles. The revocation of a digital certificate is achieved in the EDRP by quickly informing the neighboring vehicles about the misbehaving vehicle. The revocation is based on the voting results aggregated by the vehicles' valid secret shares assigned by the CA. Moreover, the revocation procedure does not involve any third party or authority such as the CA or the RSU. This takes off the extra burden of adding thousands of revoked certificates from the CA. The EDRP adds a single entry against each revoked vehicle. Therefore, it achieves a significant reduction in communication overhead due to the linearly sized CRL. The authentication delay is also significantly reduced. Our theoretical analysis and empirical studies show substantial improvements in the EDRP in terms of vehicle authentication and certificate revocation. Based on our security analysis and experiments, we argue that the EDRP achieves an essential milestone for developing the secure, efficient and scalable VANETs.

References

[1] M. Asghar, R. R. M. Doss, L. Pan, A scalable and efficient pki based authentication protocol for vanets, in: 2018 28th International Telecommunication Networks and Applications Conference, IEEE, 2018, pp. 1–3.

[2] R. Doss, M. Alajeely, S. F. Al Rubeaai, et al., Packet integrity defense mechanism in oppnets, Computers and Security 74 (2018) 71–93.

[3] E. Eziama, K. Tepe, A. Balador, K. S. Nwizege, L. M. Jaimes, Malicious node detection in vehicular ad-hoc network using machine learning and deep learning, in: IEEE Globecom Workshops, 2018, pp. 1–6.

[4] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan,M. Rajarajan, Host-based intrusion detection for vanets: a statistical approach to rogue node detection, IEEE transactions on vehicular technology 65 (8) (2015) 6703–6714.

[5] J. Guo, J. P. Baugh, S. Wang, A group signature based secure and privacy-preserving vehicular communication framework, in: IEEE International Conference on Mobile Networking for Vehicular Environments, 2007, pp. 103–108.

[6] X. Sun, X. Lin, P.-H. Ho, Secure vehicular communications based on group signature and id-based signature scheme, in: IEEE International Conference on Communications, 2007, pp. 1539–1545.

[7] X. Lin, X. Sun, P.-H. Ho, X. Shen, Gsis: A secure and privacy-preserving protocol for vehicular communications, IEEE Transactions on vehicular technology 56 (6) (2007) 3442–3456.

[8] M. K. K. Kishore, M. Suvitha, An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications, International Journal of Emerging Trends in Science and Technology 2 (02).

[9] J. Shao, X. Lin, R. Lu, C. Zuo, A threshold anonymous authentication protocol for vanets, IEEE Transactions on vehicular technology 65 (3) (Mar. 2016) 1711–1720.

[10] H. Zhong, J. Wen, J. Cui, S. Zhang, Efficient conditional privacy-preserving and authentication scheme for secure service provision in vanet, Tsinghua Science and Technology 21 (6) (2016) 620–629.

[11] A. Tomandl, H. Federrath, F. Scheuer, Vanet privacy by defending and attacking, in: International Conference on Wireless and Mobile Networking, 2013, pp. 1–7.

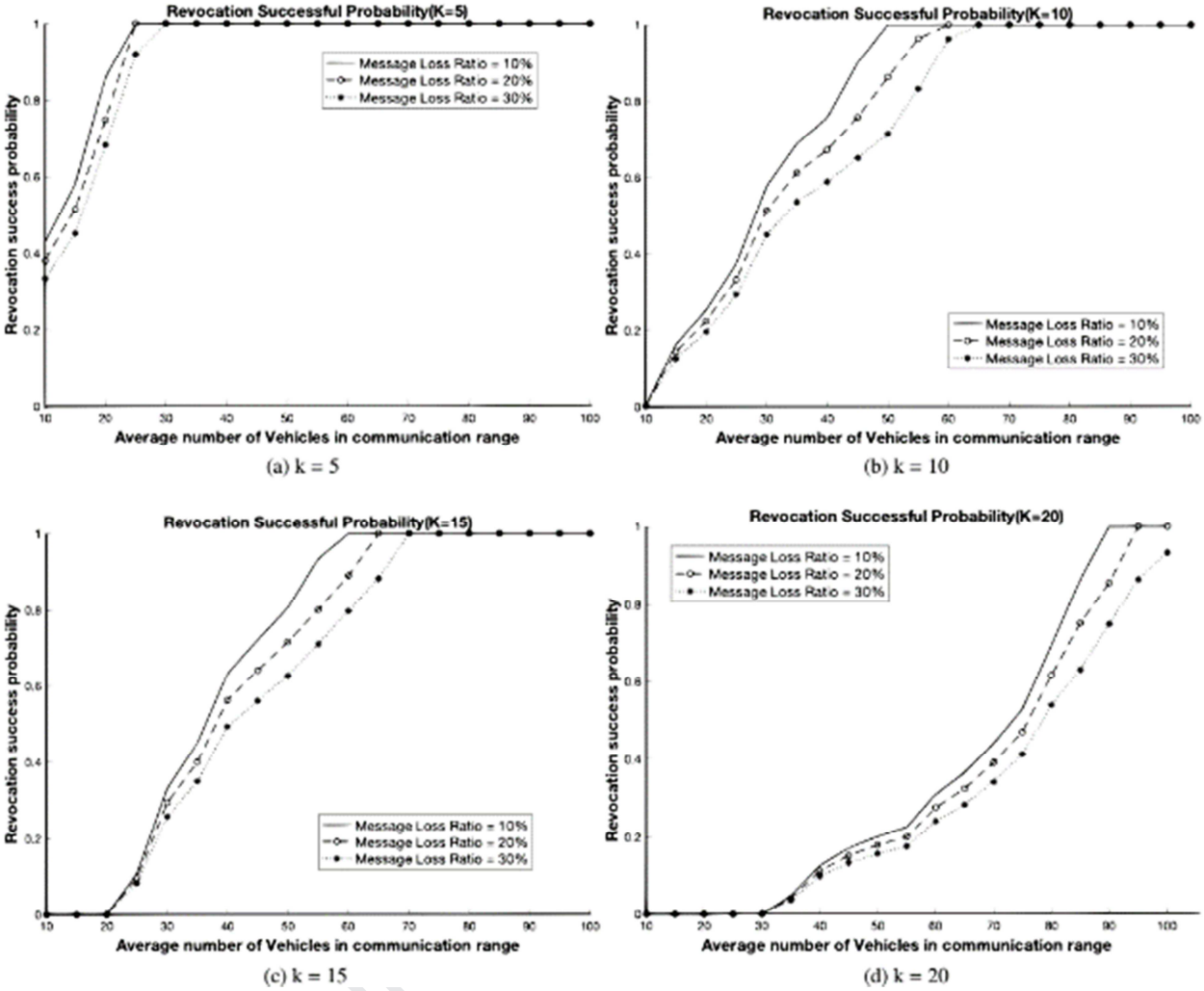
[12] Y. Sun, R. Lu, X. Lin, X. Shen, J. Su, An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications, IEEE Transactions on Vehicular Technology 59 (7) (Jun. 2010) 3589–3603.

[13] U. Rajput, F. Abbas, H. Oh, A hierarchical privacypreserving pseudonymous authentication protocol for vanet, IEEE Access 4 (Oct. 2016) 7770–7784.

[14] U. Rajput, F. Abbas, H. Eun, H. Oh, A hybrid approach for efficient privacy-preserving authentication in vanet, IEEE Access 5 (Jun. 2017) 12014–12030.

[15] R. Lu, X. Lin, H. Zhu, P.-H. Ho, X. Shen, Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications, in: IEEE International Conference on Computer Communications, 2008, pp. 1229–1237.

[16] D. Huang, S. Misra, M. Verma, G. Xue, Pacp: An efficient pseudonymous authentication-based conditional privacy protocol for vanets, IEEE Transactions on Intelligent



Transportation Systems 12 (3) (Oct. 2011) 736–746.

Fig. 9. Effect of the message loss ratio on revocation success probability (analytical).

[17] S. Jiang, X. Zhu, L. Wang, An efficient anonymous batch authentication scheme based on hmac for vanets, IEEE Transactions on Intelligent Transportation Systems 17 (8) (Mar. 2016) 2193–2204.

[18] C. Zhang, R. Lu, X. Lin, P.-H. Ho, X. Shen, An efficient identity-based batch verification scheme for vehicular sensor networks, in: IEEE International Conference on Computer Communications, 2008, pp. 246–250.

[19] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, M. K. Khan, Enhancing security and privacy for identity-based batch verification scheme in vanets, IEEE Transactions on Vehicular Technology 66 (4) (Apr. 2017) 3235–3248.

[20] N.-W. Lo, J.-L. Tsai, An efficient conditional privacy preserving authentication scheme for vehicular sensor networks without pairings, IEEE Transactions on Intelligent Transportation Systems 17 (5) (May 2016) 1319–1328.

[21] A. Wasef, X. Shen, Emap: Expedite message authentication protocol for vehicular ad hoc networks, IEEE transactions on Mobile Computing 12 (1) (Jan. 2013) 78–89.

[22] S. Jiang, X. Zhu, L. Wang, A conditional privacy scheme based on anonymized batch authentication in vehicular adhoc networks, in: IEEE International Conference on Wireless Communications and Networking, 2013, pp. 2375–2380.

[23] X. Zhu, S. Jiang, L. Wang, H. Li, Efficient privacy-preserving authentication for vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 63 (2) (Feb. 2014) 907–919.

[24] A. Wasef, R. Lu, X. Lin, X. Shen, Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks], IEEE Wireless Communications 17 (5).

[25] I. Committee, et al., Ieee trial-use standard for wireless access in vehicular environments security services for applications and management messages, IEEE Vehicular Technology Society Standard 16092.

[26] U. B. of Transit Statistics, US Department of Transportation, http://en.wikipedia.org/wiki/Passenger_vehicles_in_the_United_States, [online; access 2006] (2006).

[27] J.-P. Hubaux, S. Capkun, J. Luo, The security and privacy of smart vehicles, IEEE Security and Privacy 2 (3) (2004) 49–5.

[28] A. Studer, E. Shi, F. Bai, A. Perrig, Tacking together efficient authentication, revocation, and privacy in vanets, in: IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2009, pp. 1–9.

[29] P. P. Papadimitratos, G. Mezzour, J.-P. Hubaux, Certificate revocation list distribution in vehicular communication systems, in: Proceedings of the fifth ACM international workshop on Vehicular Inter-NETworking, 2008, pp. 86–87.

[30] J. J. Haas, Y.-C. Hu, K. P. Laberteaux, Design and analysis of a lightweight certificate revocation mechanism for vanet, in: Proceedings of the sixth ACM international workshop on Vehicular InterNETworking, 2009, pp. 89–98.

[31] K. P. Laberteaux, J. J. Haas, Y.-C. Hu, Security certificate revocation list distribution for vanet, in: Proceedings of the fifth ACM international workshop on Vehicular Inter-NETworking, 2008, pp. 88–89.

[32] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, J.-P. Hubaux, Eviction of misbehaving and faulty nodes in vehicular networks, IEEE Journal on Selected Areas in Communications 25 (8).

[33] M. Raya, M. H. Manshaei, M. Félegyházi, J.-P. Hubaux, Revocation games in ephemeral networks, in: Proceedings of the 15th ACM conference on Computer and communications security, 2008, pp. 199–210.

[34] A. Wasef, X. Shen, Edr: Efficient decentralized revocation protocol for vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 58 (9) (2009) 5214–5224.

[35] P. G. Shah, X. Huang, D. Sharma, Analytical study of implementation issues of elliptical curve cryptography for wireless sensor networks, in: IEEE International Conference on Advanced Information Networking and Applications, 2010, pp. 589–592.

[36] V. S. Miller, Use of elliptic curves in cryptography, in: Conference on the theory and application of cryptographic techniques, 1985, pp. 417–426.

Conflict of Interest Statement

Manuscript title: **An Efficient and Decentralized Voting Based Revocation Protocol for Vehicular Ad Hoc Networks**

The authors whose names are listed below certify that they have no affiliations with or involvement in any organization or entity with any financial interest (such as honoraria; educational grants; participation in speakers' bureaus; membership, employment, consultancies, stock ownership, or other equity interest; and expert testimony or patent-licensing arrangements), or non-financial interest (such as personal or professional relationships, affiliations, knowledge or beliefs) in the subject matter or materials discussed in this manuscript.

Author's name	Affiliation
Miraj Asghar	Deakin University, Geelong, 3220 Australia
Lei Pan	Deakin University, Geelong, 3220 Australia
Robin Doss	Deakin University, Geelong, 3220 Australia