IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON SECURITY AND PRIVACY FOR VEHICULAR NETWORKS

Received September 25, 2017, accepted October 20, 2017, date of publication October 31, 2017,
date of current version November 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2768499

A Privacy-Preserving Mutual Authentication Resisting DoS Attacks in VANETs

CONG SUN, (Member, IEEE), JIAO LIU, XINPENG XU, AND JIANFENG MA
School of Cyber Engineering, Xidian University, Xi'an 710071, China

Corresponding author: Cong Sun (suncong@xidian.edu.cn).

This work was supported in part by the Natural Science Basis Research Plan in Shaanxi Province of China under Grant 2016JM6034, in part by the National High Technology Research and Development Program (863 Program) of China under Grant 2015AA017203, and in part by the Special Research Foundation of MIIT under Grant MJ-2014-S-37, and in part by the China 111 Project B16037.

ABSTRACT Providing efficient anonymous authentication in vehicular ad hoc networks (VANETs) is a challenging issue. Identity-based signature schemes have been used to provide privacy-preserving authentication effectively for VANETs. In such scenario, mutual authentication between vehicles is critical to ensure only legitimate vehicles can involve in the inter-vehicle communication, and how to resist denial-of-service attack should be carefully addressed due to the regionally central signature verification in vehicle-roadside communications. In this paper, we propose a conditional privacy-preserving mutual authentication framework with denial-of-service attack resistance called MADAR. The authentication framework combines different identity-based signature schemes and distinguishes inner-region and cross-region authentications to increase efficiency. Beyond the privacy preservation and non-repudiation achieved by the existing framework, our authentication framework provides asymmetric inter-vehicle mutual authentication and strength-alterable computational DoS-attack resistance. We have formally proved the privacy preservation, unlinkability, mutual authenticity, and correctness of pseudonym with ProVerif, and analyzed other security objectives. The performance evaluations are conducted and the results demonstrate that our framework can achieve these security objectives with moderate computation and communication overheads.

INDEX TERMS Authentication, privacy, denial-of-service attack, security protocol, vehicular ad hoc networks.

I. INTRODUCTION

Vehicular ad hoc network (VANET) is a kind of mobile ad hoc network that provides communication between vehicles and roadside infrastructures. With the Dedicated Short Range Communication (DSRC) system, VANET can support both vehicle-to-vehicle and vehicle-to-infrastructure communications under a highly dynamic topology. Security is crucial to VANETs because the messages transmitted between vehicles are safety-critical but exposed over an open access environment. As one of the critical components of security, authentication plays an important role in the secure communication of VANETs. For VANET applications to operate safely, authentication is essential for us to identify valid participants, ensure participants are who they claim to be, and prevent attackers from tampering messages.

Privacy preservation is a long-standing issue for VANETs. Various private data, e.g. vehicle's identity, position, moving route, and other driver-specific information, should be protected properly. If these private data are exposed to attackers, they may easily use these data to profile user or launch different attacks, e.g. masquerading attack and impersonation attack. Moreover, a malicious vehicle may send fake messages to misguide other vehicles and cause harm to the road safety. Various approaches have been proposed to support the anonymity of vehicles. One of the most acknowledged mechanisms to ensure the privacy of vehicles for VANET security is privacy-preserving authentication [1]. In order to provide traceability and non-repudiation to each vehicle, conditional privacy-preserving authentications [2]–[8] leverage conditional tracking mechanism to ensure only trusted authorities can retrieve the real identity of vehicle from the message if a dispute appears. In these approaches, it has been realized that (pseudo-) identity-based (ID-based) signature schemes [3]–[6] are generally more efficient than centralized PKI-based authentication schemes [2], [7]. A recent improvement on PKI-based schemes has reduced the communication overhead by decentralizing the functionalities of certificate

authority (CA) [8]. To alleviate the computation overhead of regular ID-based signature schemes, recent approach combines ID-based signatures with ID-based online/offline signatures to reduce the verification overhead [6]. Because of the low overhead of ID-based signature schemes, they are more easily confronted with denial-of-service (DoS) attacks. Meanwhile, unilateral authentication may cause redirection or impersonation attack and fail to ensure that both involved peers are legitimate. However, both the DoS resistance and inter-vehicle mutual authentication have rarely been discussed on the ID-based conditional privacy-preserving authentication schemes.

As a strong security requirement of VANET, mutual authentication is critical to ensure that only legitimate vehicles or devices can involve in the communication of vehicular network. Recently, mutual authentication has been discussed for different principals, i.e. between the vehicle and roadside infrastructures [5], [9], [10], between different vehicles [11]–[13], or between in-vehicle components [14]. Compared with the vehicle-roadside mutual authentications which address the prevention of spurious infrastructure entities, vehicle-to-vehicle mutual authentications mainly concern that only benign vehicles can communicate and the traceability of abnormities. Céspedes et al. [11] proposed a lightweight mutual authentication between destination node and relay node for the multihop-authenticated proxy mobile IP scheme. The scheme does not focus on the privacy preservation thus is vulnerable to the malicious location tracking. Caballero-Gil et al. [12] developed a fully distributed and self-managed mutual authentication between a small number of vehicles using zero-knowledge proofs and certificate graphs supporting privacy protection. Each pair of vehicles verifies the validity of a shared secret key with zero-knowledge proof, and use this shared key for key exchange. Then the authenticity of the message is guaranteed by the exchanged keys. Vijayakumar et al. [13] proposed a batch authentication scheme which can be performed bidirectionally as the prerequisite of key distribution. Their approach does not distinguish the vehicle-to-vehicle authentications and the vehicle-roadside authentications. Compared with these work, we develop in this work a new inter-vehicle mutual authentication for a different communication scenario, which has no relay vehicle and does not need symmetric verification replication.

DoS attack has also been considered for long as one of the elementary attacks to the authentication in VANET [15]. DoS attack can be carried out by either insiders and outsiders of the network, and renders the vehicle-roadside authentication service unavailable to other vehicles by flooding or jamming with abundant artificially generated messages or dummy messages to the roadside units. Communications in the urban vehicular network are especially susceptible to DoS attacks due to the limited wireless bandwidth, the density of vehicles, as well as the computational or memory limit of vehicles and roadside units. Although authentication schemes using symmetric cryptography and delayed key disclosure have been proved to be resilient to computation-based DoS attacks [16], [17] or memory-based DoS attacks [17] in inter-vehicle communications, asymmetric cryptography based signature, e.g. ECDSA for 802.11p, is essential to provide non-repudiation, that causes the central nodes or roadside units vulnerable to DoS attacks, let alone the lightweight ID-based signature schemes. In several DoS-resistant schemes [18], [19], vehicles use different hash trees to generate a common public key for all their possible movements, and efficiently verify the authenticity of beacons and the sender's mobility by reconstructing this public key from the hash trees. The anonymity of vehicles has also been considered over TESLA-based DoS-resistant authentication frameworks [20], [21], as well as some lightweight message authentication resisting DoS by avoiding both symmetric and asymmetric key operations [8], but mutual authentication has not been equipped between vehicles in these schemes.

In this work, we propose a new asymmetric vehicle-to-vehicle Mutual Authentication framework with DoS Attack Resistance, i.e. MADAR, to ensure privacy preservation, non-repudiation and traceability. To resist DoS attacks to the regionally central signature verification computationally, we utilize a weak authentication mechanism to raise the cost of attacks. The contributions of this work can be summarized as follows.

1) We propose a new vehicle-to-vehicle mutual authentication framework which leverages the combination of ID-based signature schemes and self-generated pseudonym to provide conditional privacy-preservation. The mutual authentication is asymmetrically performed for efficiency and partially supervised by roadside infrastructures.
2) We propose to use the strength-alterable message-specific puzzle to resist DoS attacks in vehicle-to-infrastructure communications. The strength of resistance can vary to balance the effectiveness of protection and the performance of authentication.
3) We have elaborated the conformance of our authentication framework to a variety of security requirements, and formally proved the privacy preservation, unlinkability, mutual authenticity and correctness of pseudonym with the ProVerif tool. We have also shown that our framework has moderate computation and communication overheads compared with the unilateral authentication.

The rest of this paper is organized as follows. Section II presents the network architecture, security requirements and the threat model. Section III describes the proposed MADAR framework in detail. Section IV gives the security analysis. Section V presents performance evaluations demonstrating the effectiveness of DoS-attack resistance and the performance overheads of our framework. Section VI concludes the paper and provides potential direction for future work.

II. NETWORK ARCHITECTURE AND SECURITY MODEL

A. NETWORK MODEL

VANETs are a kind of mobile ad hoc networks spontaneously organizing mobile vehicles and roadside infrastructures to communicate and exchange respective node information, e.g. the speed or location of the vehicle. The urban VANETs adapt the communications of VANETs to the environment with high-density nodes and frequently changing topology highly related to road layouts. In the urban environments of VANETs, the vehicular communication structure usually consists of three different kinds of principals: vehicle (V), roadside unit (RSU), and regional trusted authority (RTA). Vehicles are equipped with certain radio interface or On-Board Unit (OBU) that supports the construction and operation of wireless ad hoc networks. RTA is the certification authority, which may be served as a trusted third party by automobile manufacturers or administrative agency. A finite number of RSUs are registered along the roadside to facilitate the vehicle-roadside (V-R) communications. RSUs should cover the wireless vehicular communications and play a part of the connection between vehicles and RTA. Besides the vehicle-roadside communications, the vehicle-to-vehicle (V2V) communications equip each individual vehicle with the ability to monitor the ''hidden'' data, such as location and speed, of other vehicles on the street, so far as to automatically predict potential collisions. We also assume the wired communications between RSUs and between RSU and RTA are secure.

B. SECURITY REQUIREMENTS AND THREAT MODEL

1) PRIVACY-PRESERVATION

The real identity of vehicles should be hidden from the roadside infrastructures during the authentications as well as in the vehicle-roadside communication and V2V communication. Even when the RSUs are compromised, these real identities should never be obtained by the attacker. This requirement on anonymity is essential to avoid the revealing attacks on identity and location. Beyond the anonymity, the adversaries should never infer the identity of vehicles through the common properties from any number of messages, which we called *unlinkability* [8].

2) MUTUAL AUTHENTICATION

The V2V communication is available for interchanging safety data for predicting emergency situations. The prediction and alert should be built upon the mutual trust between vehicles. All vehicles are expected to achieve V2V mutual authentication in both inner-RSU and cross-RSU manners.

3) NON-REPUDIATION

A receiver node has the ability to prove to a third party that who is accountable for the message. An adversary cannot claim that the message is created by another party. Non-repudiation implies that the receiver can identify the sender and detect the manipulation of forged messages. In the scenario of VANETs, each vehicle should never deny a specific message generated and sent by itself, such as an ETC purchase.

4) TRACEABILITY

Although V2V and vehicle-roadside communications are anonymous and unlinkable, it is still essential to trace the real identity of vehicle in some controversial scenarios, e.g. the accident responsibility investigations. The trusted party RTA should be able to ensure vehicles' real identity through their registrations, even when the origin of message is in dispute.

5) DoS-ATTACK RESISTANCE

A limited amount of resources is required for the specific security mechanism such that other applications can operate smoothly. Due to the relatively high cost of digital signature verification in authentication, numerous invalid verification or authentication requests may be maliciously broadcast so that the receiver's processing power and the network bandwidth may be exhausted. Under this kind of attacks, this requirement implies the ability of RSUs to perform ordinary verification and authentication.

Correspondingly, we focus on the attacks related to the above security requirements. Firstly, an attacker may forge, modify or block some packets from senders. Secondly, an attacker may pretend to be another entity or use different vehicles' identities at the same time. Consequently, the attacker can capture the critical responses to another entity or launch false requests to the roadside infrastructures. Thirdly, an attacker may compromise some RSU and passively eavesdrop sensitive information, including the real identity of the vehicle, to infer some privacy of users. Forth, an attacker may deny the involvement in the procedure of communications. Moreover, an attacker may perform channel jamming or aggressive injection of dummy messages, verification requests or authentication requests. Due to the high density of vehicles, a DoS attack to RSU will be easily triggered.

III. PROPOSED AUTHENTICATION FRAMEWORK: MADAR

In this section, we describe the new Mutual Authentication framework with DoS-Attack Resistance mechanism, called MADAR. With regard to the different types of wireless communications in the VANET scenario, our authentication framework can be divided into two categories, vehicle-roadside authentication and V2V authentication. Similar to the existing work [6], our authentication framework combines ID-based signature (IBS) scheme [22] and ID-based online/offline signature (IBOOS) scheme [23] for the efficiency of authentication. Before applying the authentications, each vehicle should first register itself to the RTA directly using its real ID, and get a set of RSU IDs in response from the RTA. Then the mutual authentications can be operated according to the formalization given in Table. 1.

TABLE 1. Operations of MADAR protocol.

Vehicle-Roadside authentication		
Step 1	$RSU_r \Rightarrow *:$	$\langle ID_r, T, pk_c, nonce_r, SIG_r(ID_r\|\|T\|\|pk_c)\rangle$
Step 2	$V_v \rightarrow RSU_r:$	$\langle PS_v, ID_r, T, join, SIG_v(PS_v\|\|T), wa, nonce_r\rangle$, $wa = (i, k_i, p_i)$
Step 3	$RSU_r \Rightarrow *:$	$\langle ID_r, t, set_v(PS_v\|\|SIG_v^{\text{offline}}(PS_v)), SIG_r(ID_r\|\|t)\rangle$
V2V authentication		
Step 1	$V_v \Rightarrow *:$	$\langle PS_v, t, nonce_v, SIG_v^{\text{online}}(SIG_v^{\text{offline}}(PS_v)\|\|t)\rangle$
Inner-RSU V2V authentication		$(ID_r^i = ID_r^v)$
Step 2	$V_i \rightarrow V_v:$	$\langle PS_i, PS_v, t, nonce_v, SIG_i^{\text{online}}(SIG_i^{\text{offline}}(PS_i)\|\|t)\rangle$
Cross-RSU V2V authentication		$(ID_r^w \neq ID_r^v)$
Step 2'	$V_w \rightarrow RSU_u:$	$\langle PS_w, ID_u, T, q.y., SIG_w^{\text{online}}(SIG_w^{\text{offline}}(PS_w)\|\|T), nonce_w\rangle$
Step 3'	$RSU_u \rightarrow V_w:$	$\langle ID_u, PS_w, T, q.r., iden, SIG_u(q.r.\|\|ID_u\|\|T), SIG_u(iden\|\|ID_u), nonce_w\rangle$
Step 4'	$V_w \rightarrow V_v:$	$\langle PS_w, PS_v, t, ID_u, iden, SIG_w(PS_w\|\|t), SIG_u(iden\|\|ID_u), nonce_v\rangle$

Notation	Meaning
$*$	All the vehicles in the communication range of RSU or vehicle as broadcaster.
$\Rightarrow, \rightarrow$	The broadcast and unicast communication.
T	The time stamp for a specific time interval of vehicle-roadside authentication.
t	The time stamp for a specific time interval of V2V authentication.
$nonce$	A random number generated by a specific vehicle or RSU.
ID	The ID of RSU.
PS	The pseudonym of vehicle.
SIG	The ID-based signature generated by either RSU or vehicle.
SIG^{online}, SIG^{offline}	The online and offline signature generated with IBOOS
wa	Weak authentication mechanism.
$join$, $q.y.$, $q.r.$, $iden$	The join request, query message, query result, authentication evidence.
$set(\bullet)$	The message generated from PO information of each vehicle.
pk_c	The current public key of RTA for vehicle pseudonym encryption.

A. VEHICLE-ROADSIDE AUTHENTICATIONS

The vehicle-roadside authentications, as seen in the first part of Table 1, are performed as prerequisite of both inner-RSU and cross-RSU V2V authentication.

First, the RSU periodically broadcasts the public key pk_c of the RTA to all the vehicles in its communication range, along with its ID-based signature of current time interval and a nonce value for freshness to validate the authenticity of message. All vehicles in the range of this RSU use pk_c and other private information to generate or update its pseudonym, either intentionally or whenever the ID of this RSU is identified as a new one. The pseudonym PS_v of vehicle V_v, with respect to the current RSU RSU_r, can be denoted as $\langle Time||Enc_{pk_c}(ID_v)||ID_r\rangle$. *Time* is the current time interval and ID_v represents the real identity of vehicle hidden by the encryption against the RSU.

Then, each vehicle replies a message to the RSU, using its newly generated pseudonym in the signature for source authenticity. The join request *join* attached in this message informs the RSU for further acceptance on this vehicle and operations on the pseudonym/offline signature set. In order to resist DoS attacks, we resort to a weak authentication mechanism *wa* to increase the attack cost. *wa* consists of an index *i*, a key k_i indexed by *i* from a one-way key chain, and the solution p_i to the *i*th message-specific puzzle. Computation resource is consumed to find the solution p_i according to the current message and the k_i from *wa*, see Section III-C for more details.

After verifying the pseudonym-based signature in the received join-request message for its authenticity, the RSU stores the new pseudonym PS_v and reports it to RTA for the traceability of vehicle. Then the RSU uses the pseudonym PS_v to generate the off-line signature $SIG_v^{\text{offline}}(PS_v)$ for the vehicle V_v. Then the RSU generates a pseudonym/offline signature (PO) set containing all the active vehicles' pseudonyms as recorded, each of whose elements is in the form of $PS_v||SIG_v^{\text{offline}}(PS_v)$. The RSU broadcasts such a PO set to all the vehicles in its transmission range, along with a signature $SIG_r(ID_r||t)$ and a nonce. The signature verification is performed by each vehicle that receives this broadcast message. If the signature is valid and the receiver vehicle's pseudonym is found in the received PO set, the current PO set of this receiver vehicle will be updated.

B. V2V AUTHENTICATIONS

The V2V authentication is used for securing inter-vehicle communications. Consequently, the existing unilateral authentication [6] is insufficient to ensure both peers are legitimate. Our mutual V2V authentication can be divided into inner-RSU V2V authentication and cross-RSU V2V authentication, see the second part of Table 1. In both cases, a vehicle should first broadcast an authentication message to

show its willing of authenticated communication (Step 1). This authentication message contains an online signature derived from the offline signature of its pseudonym, i.e. $SIG_v^{\text{offline}}(PS_v)$, and a time stamp t. Each receiver vehicle verifies the authenticity of this message to the sender vehicle's pseudonym PS_v, and searches PS_v in its own PO set. If PS_v is found, the receiver vehicle may conduct an inner-RSU mutual authentication (Step 2), otherwise it will conduct a cross-RSU mutual authentication (Step 2' – Step 4').

In the inner-RSU mutual authentication, after authenticating V_v, each receiver vehicle, e.g. V_i, may feed back $SIG_i^{\text{online}}(SIG_i^{\text{offline}}(PS_i)||t)$ to V_v. V_v can then verify the online signature from each V_i using its PO set for searching the offline signature of each V_i.

In the cross-RSU mutual authentication, firstly, the vehicle V_w need to transmit a query message $q.y.$ to the nearest RSU, i.e. RSU_u. The query message $q.y.$ contains the pseudonym, online signature, and time stamp of V_v, and asks for authenticating V_v by the RSUs. Meanwhile, V_w also send its online signature $SIG_w^{\text{online}}(SIG_w^{\text{offline}}(PS_w)||T)$ to the nearest RSU in purpose of authenticating itself for V_v. Then, after receiving the query message, the nearest RSU first authenticates V_w by searching its PO set and verify the online signature of V_w. Then, it queries other RSUs or RTAs to check the validity of V_v. If V_v is valid and V_w itself is authenticated by RSU_u, a query result $q.r.$ which indicates the validity of V_v, as well as an evidence *iden* which indicates that V_w has been authenticated by RSU_u, are sent back to V_w, with proper signatures for the authenticity of message source and the evidence *iden*. Finally, the signed evidence *iden* is delivered from V_w to V_v, and V_v is able to verity through the authenticity of *iden* that V_w has been authenticated by RSU_u.

C. MECHANISM OF DoS-ATTACK RESISTANCE

In order to resist DoS attacks, we provide a weak authentication mechanism based on message-specific puzzle [24] in the vehicle-roadside authentication phase for each vehicle's reply. Under such mechanism, when digital signatures are used for authentication, the receiver node, i.e. RSU, does not have to verify the signature if the weak authenticator cannot be verified. One-way key chain is utilized to provide weak authentication, that can be generated by firstly selecting random value k_n as the last key in the key chain, and then repeatedly performing a one-way hash function F to compute all the previous keys, i.e. $k_i = F(k_{i+1}), 0 \leq i \leq n-1$. Given k_j in the key chain, it is easy to compute all the previous keys $k_i (0 \leq i < j)$, but computationally infeasible to compute any later key $k_i (j < i \leq n)$. If we know F and the initial key k_0, we can easily authenticate any key k_x by performing hash function operations.

We assume the vehicle has generated a one-way key chain consisting of $k_0, k_1, \ldots, k_n$, and distributed k_0 to all potential RSUs along its trace. The ith key k_i in this key chain is used for the weak authentication of the ith packet. We also assume there is a hash function F_p known to all the vehicles and RSUs.

Given the ith message $m_i = \langle PS_v, ID_r, T, join, nonce_r \rangle$ for $V_v \rightarrow RSU_r$ in vehicle-roadside authentication, V_v first generates the signature $sig = SIG_v(PS_v||T)$. Then V_v generates the ith message-specific puzzle which consists of the index i, the message m_i, the signature sig, and the ith puzzle key k_i. The solution to the ith message-specific puzzle, denoted as p_i, must satisfies the following condition:

- The puzzle key k_i is the ith key in the one-way key chain.
- After applying F_p to the ith message-specific puzzle and its solution p_i, the first ℓ bits of the result bit-vector are all "0". That is $F_p(i, m_i, sig, k_i, p_i) = \underbrace{0 \ldots 0}_{\ell \text{ bits}} x \ldots x$, where $x \ldots x$ can be any bit pattern and ℓ is called the strength of puzzle.

Before verifying the pseudonym-based signature in the join-request message, RSU should first ensure the index i is greater than the preceding index. Then, it verifies whether the received puzzle key k_i is on the hash chain by applying F finite times on k_i to derive k_0 or a previously verified puzzle key. After passing this verification, the puzzle solution p_i is verified. And then, RSU can verify the authenticity of join-request message using the signature. It takes 2^ℓ trials on average for vehicle to find a solution to the message-specific puzzle. The DoS attacker cannot force RSU to verify the signature of forged message before it can solve the message-specific puzzle. Thus, the DoS attack is computationally resisted.

IV. SECURITY ANALYSIS AND VERIFICATION

We take a symbolic approach to prove the conformance of our authentication framework to the security requirements presented in Section II-B. The automated tool used for symbolic analysis is ProVerif [25]. We implement the core phases of MADAR using ProVerif, and prove the security properties to the requirements. The primitives of ProVerif used for our analyses are listed as below:

- *choice* $[M, M']$: This primitive is used for the same process with different arguments, either M or M', to trigger the difference on behaviors caused by these arguments, and report a trace directing to the triggering point.
- *query attacker*(M): This primitive decides whether the attacker may have M in some phase of the protocol, i.e. whether the secrecy of M is preserved by the protocol.
- *query event* $: f(x_1, \ldots, x_n) ==> event : f'(x_1, \ldots, x_n)$: This primitive is a non-injective agreement deciding that the execution of $f(x_1, \ldots, x_n)$ can imply a previous execution of $f'(x_1, \ldots, x_n)$.
- *query inj-event* $: f(x_1, \ldots, x_n) ==> inj\text{-}event : f'(x_1, \ldots, x_n)$: This primitive decides that each occurrence of $f(x_1, \ldots, x_n)$ corresponds to a distinct previous occurrence of $f'(x_1, \ldots, x_n)$.
- $!Proc$: This primitive means repeatedly executing an unbounded number of copies of process *Proc* in parallel.

```
- Query ...
Starting query event(Vvverify(psi_10541)) ==>
event(Virespond(psv_10542, psi_10541, t_10543, nv_10544,
sig_10545))
RESULT event(Vvverify(psi_10541)) ==>
event(Virespond(psv_10542, psi_10541, t_10543, nv_10544,
sig_10545)) is true.
- Query ...
Starting query inj-event(Vvverify(psi_3210)) ==>
inj-event(Virespond(psv_3211, psi_3210, t_3212, nv_3213,
sig_3214))
RESULT inj-event(Vvverify(psi_3210)) ==>
inj-event(Virespond(psv_3211, psi_3210, t_3212, nv_3213,
sig_3214)) is true.
- Query ...
Starting query event(Viverify(psv_8099)) ==>
event(Vvbroadcost(psv_8099, t_8100, nv_8101, sig_8102))
RESULT event(Viverify(psv_8099)) ==>
event(Vvbroadcost(psv_8099, t_8100, nv_8101, sig_8102)) is
true.
- Query ...
Starting query inj-event(Viverify(psv_5655)) ==>
inj-event(Vvbroadcost(psv_5655, t_5656, nv_5657,
sig_5658))
RESULT inj-event(Viverify(psv_5655)) ==>
inj-event(Vvbroadcost(psv_5655, t_5656, nv_5657,
sig_5658)) is true.
```

(a)

```
- Query ...
Starting query event(Vvverify(psw_3136)) ==>
event(Vwrespond(psv_3137, psw_3136, t_3138, nv_3139,
sig1_3140, sig2_3141))
RESULT event(Vvverify(psw_3136)) ==>
event(Vwrespond(psv_3137, psw_3136, t_3138, nv_3139,
sig1_3140, sig2_3141)) is true.
- Query ...
Starting query inj-event(Vvverify(psw_86)) ==>
inj-event(Vwrespond(psv_87, psw_86, t_88, nv_89, sig1_90,
sig2_91))
RESULT inj-event(Vvverify(psw_86)) ==>
inj-event(Vwrespond(psv_87, psw_86, t_88, nv_89, sig1_90,
sig2_91)) is true.
- Query ...
Starting query event(Vwverify(psv_7774)) ==>
event(Vvbroadcost(psv_7774, t_7775, nv_7776, sig_7777))
RESULT event(Vwverify(psv_7774)) ==>
event(Vvbroadcost(psv_7774, t_7775, nv_7776, sig_7777)) is
true.
- Query ...
Starting query inj-event(Vwverify(psv_5456)) ==>
inj-event(Vvbroadcost(psv_5456, t_5457, nv_5458,
sig_5459))
RESULT inj-event(Vwverify(psv_5456)) ==>
inj-event(Vvbroadcost(psv_5456, t_5457, nv_5458,
sig_5459)) is true.
```

(b)

FIGURE 1. Verification results on the mutual authentication. (a) Inner-RSU. (b) Cross-RSU.

A. PRIVACY-PRESERVATION

The security requirement includes two sub-requirements, anonymity and unlinkability. In both vehicle-roadside communication and V2V communication, signature and message authentication depend on the vehicles' pseudonym. Through the registration of each vehicle to RTA, the RTA learns the vehicle's real ID. Contrarily, no RSU knows the vehicle's real ID and no attacker can infer it from the transmitted messages between RSU and vehicle, or between vehicles. To prove the anonymity, we specify `query attacker(idv)` where `idv` represents the real ID of vehicle. The result "`RESULT not attacker_ID(idv[]) is true`" is returned by ProVerif to show the real ID is hidden from the attackers. Unlinkability means the adversaries cannot infer the identity of vehicles through any amount of messages. In order to prove the unlinkability, we composite infinite number of sessions for each participant by adding replication notation `!` over the process of each participant. The result is still true, which means no matter how many messages the adversary collects, it still could not get any information about vehicles' real identity.

B. MUTUAL AUTHENTICATION

In the inner-RSU V2V authentication, the receiver vehicle sends its online signature to the sender vehicle if the sender's online signature is valid. To prove the inner-RSU mutual authentication, we check whether querying on both `event(Vvverify(psi)) ==> event(Virespond(psv,psi,t,nv,sig))` and `event(Viverify(psv)) ==>event(Vvbroadcost(psv, t,nv,sig))` can derive true result, that means vehicle `v` and vehicle `i` completed the certification of each other. In addition, the freshness of authentication messages can be ensured by applying `inj-event` for each query. The verification results are shown in Fig. 1a. On the other hand, in the cross-RSU V2V authentication, the vehicle V_w sends its online signature to RSU for an evidence *iden* on behalf of its authenticity, and then transmits *iden* to vehicle V_v when the online signature of V_v is valid. In order to reduce the number of requests, V_w is responsible for launching the authentication request. To prove the cross-RSU mutual authentication, we query whether `event(Vwverify(psv))==>event(Vvbroadcost(psv,t,nv,sig))` and `event(Vvverify(psw))==>event(Vwrespond(psv,psw,t,nv,sig1,sig2))` can derive true result for ensuring the vehicle `v` and vehicle `w` have completed the certification of each other. The verification results are shown in Fig. 1b.

C. NON-REPUDIATION

Each message from vehicle is integrated with its pseudo-identity, which consists of the ID of current RSU, the real ID of vehicle encrypted with public key pk_c, and the time stamp. No vehicle can know the real identity of another vehicle except the RTA. Due to the encrypted component of each pseudonym, a vehicle can never deny the action of generating and sending the message. Due to the time stamp, it can never deny the time of generating and sending the message. Thus, non-repudiation is guaranteed.

D. TRACEABILITY

With V2V and vehicle-roadside communications being anonymous and unlinkable, only the RTA can retrieve a vehicle's real ID when the message is in dispute, and verify the non-repudiation of each message to ensure that no vehicles or drivers can deny the message generated by itself. Because the attacker on RSU is assumed to be passive, we can ensure

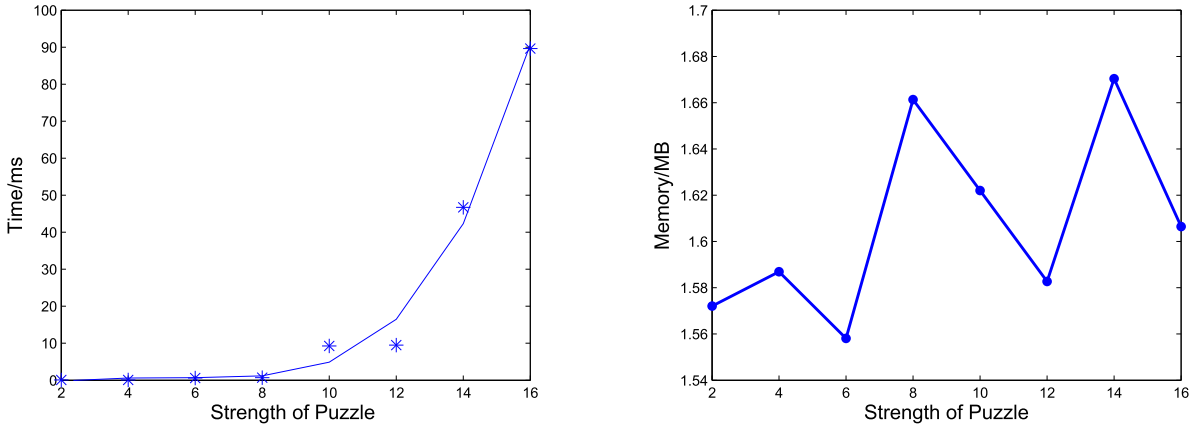


FIGURE 2. Cost variation on different strengths of message-specific puzzle. (a) Time cost. (b) Memory cost.

the vehicles can update their pseudonym with the correct pk_c. Then each message from vehicle is always traceable by RTA as it holds the sender's pseudo identity.

E. DoS-ATTACK RESISTANCE

A pre-authentication procedure before signature verification is developed with weak authentication mechanism to deal with DoS attack in vehicle-roadside communications. Sender should solve a message-specific puzzle according to the current information before it sends the join request to an RSU. The weak authenticator for the solution of puzzle cannot be easily forged, precomputed or reused. Thus, such weak authentication mechanism increases the computation cost of producing a valid join request to RSU, and launching DoS attacks against authentication becomes more difficult. The effectiveness of resistance is shown in Section V-A.

F. CORRECTNESS OF PSEUDONYM

Beyond the proof and analysis of the above security requirements, we can also work out the correctness of pseudonym, which means that operating the same processes with real identities instead of pseudonyms will only fail the anonymity of vehicle but will not influence the functionality of authentication. This property is proved by adding a primitive `choice[idv',psv]` to the protocol and getting "`RESULT Observational equivalence is true (bad not derivable)`" returned from ProVerif.

V. PERFORMANCE EVALUATION

In this section, we first evaluate the effectiveness of DoS-attack resistance mechanism. Then we perform an evaluation on the efficiency of our authentication framework. The experimental environment is Intel Core i5-4200U 1.60GHz×4 CPU and 4GB RAM.

A. EFFECTIVENESS OF DoS-ATTACK RESISTANCE

According to Section III-C, the solutions of a message-specific puzzle have equal probability distribution over a solution space with size 2^{ℓ}. To evaluate the computation cost for the solutions on different strengths of puzzle, we conduct an experiment on the time and memory cost to find p_i with different strengths of ℓ. The results are illustrated in Fig. 2. We can see the time cost increases exponentially for the attacker to launch a DoS attack (Fig. 2a). Meanwhile, the memory cost fluctuates in a narrow range, that indicates insignificant variation on the memory cost of vehicles (Fig. 2b).

Then we evaluate the effectiveness of our DoS resistance mechanism. We perform the simulation of network under DoS attacks using NS2. We set the strength of puzzle $\ell = 16$ and conduct our evaluation under different numbers of attackers ($N = 14, 28, 56$) respectively. In normal cases, we assume the benign vehicles send the join request to RSU every 500ms, whereas for the DoS attackers, they launch join request continuously with no idle time interval. Our experimental results in Fig. 3 show both the overheads and benefits of the weak authentication mechanism by measuring the traffic overhead of the RSU in a period of time. In each sub-figure for different number of vehicles/attackers, we can see that equipping the vehicle-roadside phase of protocol with the weak authentication mechanism puts extra overhead on both benign vehicles and attackers, thus the number of join requests is reduced and the burden on RSU service is eased. Meanwhile, from the gaps between the cases with and without resistance, we know that the weak authentication mechanism has much more significant effect on the attackers than on the normal vehicles.

B. EFFICIENCY OF PROTOCOL

We demonstrate the efficiency of our mutual authentication framework by comparing our protocol with ACPN [6]. Here we use signature system ECDSA-512 to generate the digital signatures for IBS scheme. We choose the strength $\ell = 16$ and $\ell = 8$ respectively for the message-specific puzzle. The time measures in Table 2 for different operations are utilized to estimate the computation overhead of the protocols. Differently from ACPN, which takes the computation delay of V2V

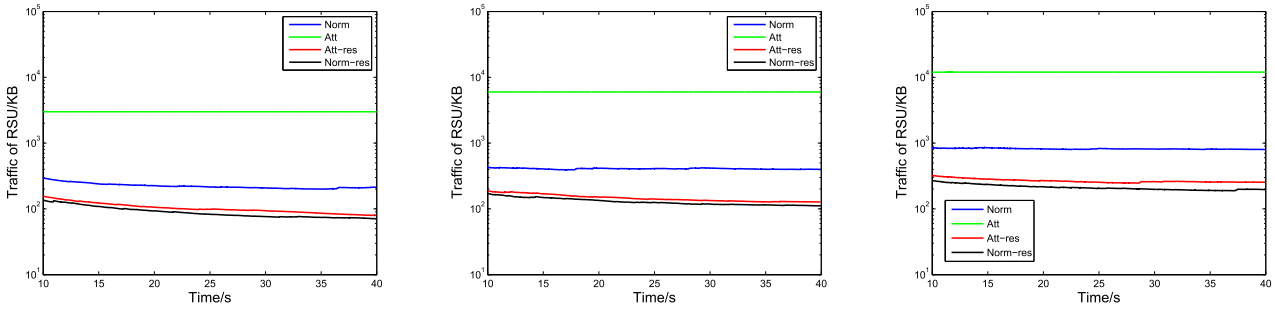


FIGURE 3. Effectiveness of DoS-Attack Resistance Mechanism (`Norm` - normal vehicles without resistance; `Att` - attackers without resistance; `Norm-res` - normal vehicles with resistance; `att-res` - attackers with resistance). (a) $N = 14$. (b) $N = 28$. (c) $N = 56$.

TABLE 2. Time measures of operations for evaluation.

Scheme	Operation	Time(ms)
ECDSA [26]	Sign	1.24
	Verify	2.33
IBOOS	Sign/Verify(online) [6]	0.19
	Sign(offline) [27]	0
Puzzle($\ell = 16$)	Solution	89.64
	Verify	0.06
Puzzle($\ell = 8$)	Solution	0.70
	Verify	0.05

authentication as primary metric of performance evaluation, we compare MADAR with ACPN on computation overhead and communication costs respectively.

1) COMPUTATION OVERHEAD

In the procedure of vehicle-roadside communication, RSU generates signature twice for broadcasting information, and produces an offline signature for vehicle. Vehicles verify the two signatures from RSU, and respond to RSU a join message with signature. Also the message-specific puzzle solving and verification are respectively performed by vehicle and RSU. The computation delay $T_{\text{V-R}}$ is calculated as:

$$T_{\text{V-R}} = 2T_{\text{RSU\_sign}} + 2T_{\text{V\_verify}} + T_{\text{V\_sign}} + T_{\text{RSU\_verify}} + T_{\text{RSU\_offSign}} + T_{\text{V\_Spi}} + T_{\text{RSU\_Vpi}}$$

In the procedure of inner-RSU V2V authentication, vehicles can verify online signature without the supervision of RSU. The online signature is verified by comparing the pseudonym in the message and the offline signature extracted from online signature with the elements from the PO set in its memory. Therefore, the computation delay is mainly caused by online signature and its verification. For the inner-RSU V2V authentication, the computation delay T_{inner} is calculated as:

$$T_{\text{inner}} = T_{\text{sender\_onSign}} + T_{\text{receiver\_onVerify}} + T_{\text{receiver\_onSign}} + T_{\text{sender\_onVerify}}$$

In the procedure of cross-RSU V2V authentication, because the sender vehicle V_v and receiver vehicle V_w are under the supervision of different RSUs, they do not have the current pseudonym of each other in their own PO set. Thus, they have to rely on the corresponding RSUs for the mutual authentication. The computation delay is made up of three parts. First, the sender V_v generate its online signature for broadcasting. This part of computation delay is $T_{\text{sender\_onSign}}$. Second, after receiving the online signature from the sender, the receiver sends query message including the sender's online signature to RSU, and asks RSUs for help to complete the online signature verification. RSUs verify two online signatures by using IBOOS scheme. Then, the nearest RSU generates two signatures separately with IBS scheme, and delivers them to the receiver. The receiver verifies one of these signatures before forwarding the other to the sender. This part of computation cost involves the actions between the receiver and the RSUs:

$$T_{\text{query}} = T_{\text{receiver\_onSign}} + 2T_{\text{RSU\_onVerify}} + 2T_{\text{RSU\_sign}} + T_{\text{receiver\_verify}}$$

Third, the receiver generates a new signature for the authenticity of the message, and forward the one he gets from the RSU. The sender then verifies the two signatures. In summary, the computation delay T_{cross} is calculated as:

$$T_{\text{cross}} = T_{\text{sender\_onSign}} + T_{\text{query}} + T_{\text{receiver\_sign}} + 2T_{\text{sender\_verify}}$$

The differences on operations between our approach and ACPN are summarized in Table 3, Table 4, and Table 5. Because there are two different V2V authentications in our approach, and they have different computation delays, the ratio of vehicles who participate in inner-RSU or cross-RSU V2V authentication may have impact on the overall computation costs. Let u denote the ratio of vehicles who participate in inner-RSU authentication. The value of u can be calculated by $N_{\text{inner}}/(N_{\text{inner}} + N_{\text{cross}})$, and the ratio of vehicles who use cross-RSU authentication is $1 - u$. Then, the average computation delay of V2V authentication is calculated as:

$$T_{\text{V2V}} = u \cdot T_{\text{inner}} + (1 - u) \cdot T_{\text{cross}}$$

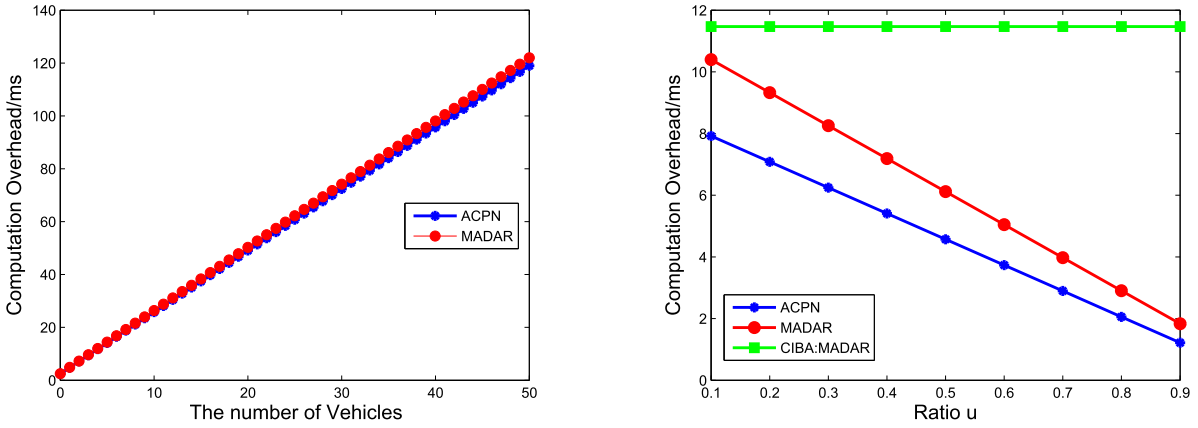


FIGURE 4. Comparison on Computation Overhead between MADAR and ACPN. (a) V-R. (b) V2V.

TABLE 3. Difference on operations between MADAR and ACPN (V-R).

Protocol	Subject	IBOOS Sign/Verify	IBS Sign/Verify	Solve/Verify p_i	Time(ms)
MADAR	V	0/0	1/2	1/0	95.54
($\ell = 16$)	RSU	1/0	2/1	0/1	4.87
MADAR	V	0/0	1/2	1/0	6.60
($\ell = 8$)	RSU	1/0	2/1	0/1	4.86
ACPN	V	0/0	1/2	0/0	5.90
	RSU	1/0	2/1	0/0	4.81

TABLE 4. Difference on Operations between MADAR and ACPN (inner-RSU V2V).

Protocol	Subject	IBOOS Sign/Verify	Time(ms)
MADAR	V_v	1/1	0.38
	V_i	1/1	0.38
ACPN	V_v	1/0	0.19
	V_i	0/1	0.19

TABLE 5. Difference on Operations between MADAR and ACPN (cross-RSU V2V).

Protocol	Subject	IBOOS Sign/Verify	IBS Sign/Verify	Time(ms)
MADAR	V_v	1/0	0/2	4.85
	V_w	1/0	1/1	3.76
	RSU	0/2	2/0	2.86
ACPN	V_v	1/0	0/0	0.19
	V_w	0/1	2/1	5.00
	RSU	0/0	1/1	3.57

In Fig. 4, we illustrate the difference on the computation overhead between different protocols. Because the weak authentication mechanism is equipped in the phase of vehicle-roadside authentication, we first assume the operations of RSU is single-threaded and evaluate the computation overhead on roadside infrastructures. When we choose $\ell = 16$ for the strength of message-specific puzzle, we can see our protocol brings insignificant computation overhead on the roadside of vehicle-roadside authentication procedure compared with ACPN (Fig. 4a). We also know from Fig. 2a that by choosing different strengths of message-specific puzzle, we can decide to trade off between the computation overhead on the vehicle and the strength of DoS-attack resistance. For instance, the computation overhead of an individual vehicle will be 16.19 times for $\ell = 16$ and only 1.12 times for $\ell = 8$ as much as ACPN.

When we compare the V2V authentication only, the computation overhead will be $0.31 \sim 1.00$ times more than ACPN (Fig. 4b). Similar to [6], we also investigate the benefit brought by the inner-RSU V2V authentication. The *conventional infrastructure-based authentication* (`CIBA` in Fig. 4) refers to a specific condition that all vehicles resort to the cross-RSU V2V authentication for the V2V authentication. It is clear that inner-RSU V2V authentication can reduce the computation cost. The decline of curves indicates that when the vehicles are with lower mobility, i.e. more vehicles are using inner-RSU V2V authentication and u becomes larger, the computation cost will decrease.

2) COMMUNICATION COST

We assume the vehicles and RSUs have the same communication speed. Then the communication overhead can be estimated by the length of messages. The default length of elements in our protocol are listed in Table 6. We know

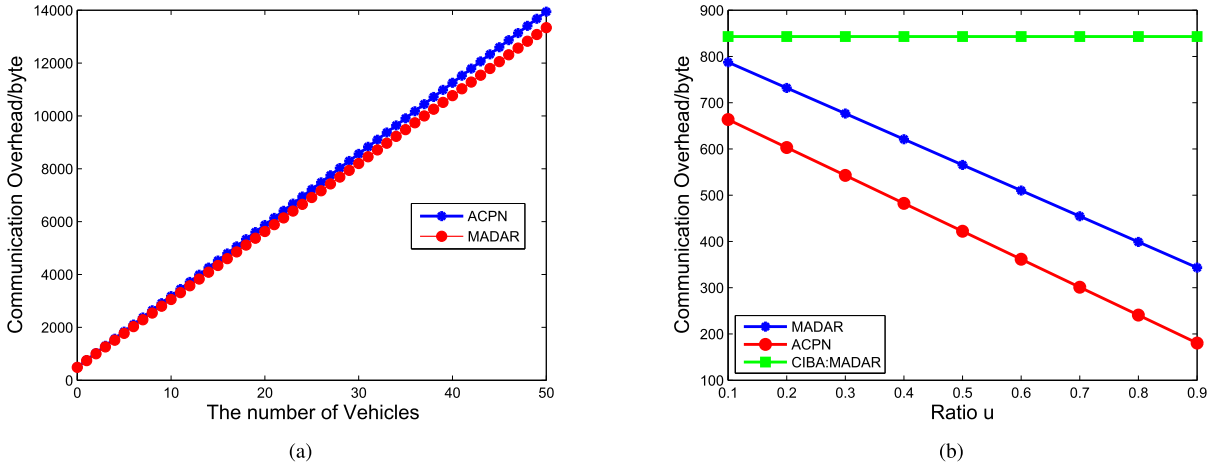


FIGURE 5. Comparison on Communication Overhead between MADAR and ACPN. (a) V-R. (b) V2V.

TABLE 6. Length of elements.

Element	Length(byte)
ID_{RSU}	20
ID_V	17
Time stamp	8
$nonce$	4
$q.y.$ (MADAR)	116
$q.y.$ (ACPN)	192
$join, iden$	1
$q.r.$ (MADAR)	1
$q.r.$ (ACPN)	128
PS_V	48

ECDSA-512 can generate 64-byte IBS signature. We adopt the serial number of X.509 certificate [28] as the ID of RSU, whose length is 20 bytes. We use the *vehicle identification number* (VIN) [29] as the ID of vehicle, whose length is 17 bytes. The length of pseudonym is 48 bytes when we use ECC to encrypt real ID of vehicle for pseudonym. $q.y.$ contains a 60-byte online signature [27], a 48-byte pseudonym, and a 8-byte time stamp.

In Fig. 5, we illustrate the difference on communication overhead between MADAR and ACPN. In the phase of V-R authentication, we know our DoS-attack resistance mechanism delays the time vehicle sends each packet by increasing the vehicle's computation overhead. Contrarily, the size of packages is reduced by our protocol in that the PO set broadcasted by RSU does not contain RSU ID as contained in the POI set of ACPN. Because the size of PO set depends on the number of vehicles supervised by a specific RSU, we can see the overhead reduction in Fig. 5a. In Fig. 5b for V2V authentication, different radio numbers of u are still considered comparing the overheads under different mobilities of vehicles. We observe that our protocol has $0.16 \sim 1.4$ times communication overhead more than ACPN, because we bring in one more message to our protocol for the mutual authentication. On the other hand, by comparing our approach with the `CIBA` cases, we can also ensure the usage of inner-RSU V2V authentication can reduce the communication overhead.

VI. CONCLUSION

In this paper, we have proposed MADAR authentication framework, which employs the existing combination of identity-based signature schemes and pseudonym mechanism for the privacy preservation and non-repudiation, and provides asymmetric inter-vehicle mutual authentications and strength-alterable DoS-attack resistance for the regionally central signature verification. Through comprehensive security analysis and formal automated proof, we prove that our framework provides conformance towards various security requirements, including privacy preservation, mutual authenticity, non-repudiation, traceability, and DoS-attack resistance. Experimental and analytic results show that our framework is feasible to achieve the security features with moderate computation and communication overheads compared with the unilateral authentication scheme [6]. In our framework, the strength of message-specific puzzle relies on the length of all-zero heading bit vector of the solution, which is alterable to meet a balance between the effectiveness of protection and the performance of authentication. As future work, we will use infinitely repeated game-based approach [30] to find the optimum history-dependent defense strategies against rational DoS attackers.

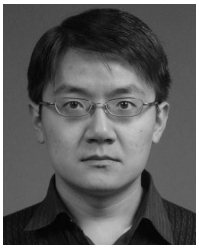
REFERENCES

[1] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.

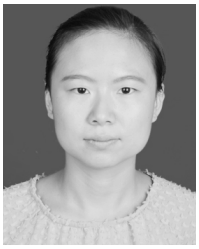
[2] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010.

[3] K.-A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874–1883, May 2012.

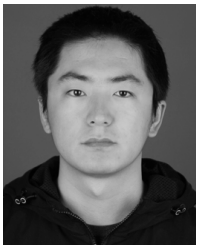
[4] S. Biswas and J. Mišić, "A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2182–2192, Jun. 2013.
[5] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.
[6] J. Li, H. Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 4, pp. 938–948, Apr. 2015.
[7] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711–1720, Mar. 2016.
[8] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET," *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, pp. 896–911, Feb. 2016.
[9] L.-Y. Yeh and Y.-C. Lin, "A proxy-based authentication and billing scheme with incentive-aware multihop forwarding for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1607–1621, Aug. 2014.
[10] N. Saxena and B. J. Choi, "Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1438–1452, Jul. 2016.
[11] S. Cespedes, S. Taha, and X. Shen, "A multihop-authenticated proxy mobile IP scheme for asymmetric VANETs," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3271–3286, Sep. 2013.
[12] C. Caballero-Gil, P. Caballero-Gil, and J. Molina-Gil, "Mutual authentication in self-organized VANETs," *Comput. Standards Interfaces*, vol. 36, no. 4, pp. 704–710, 2014.
[13] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Cluster Comput.*, vol. 20, no. 3, pp. 2439–2450, 2017.
[14] K. Han, S. D. Potluri, and K. G. Shin, "On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks," in *Proc. ACM/IEEE 4th Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Philadelphia, PA, USA, Apr. 2013, pp. 160–169.
[15] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.
[16] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, 2001, pp. 1–12.
[17] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *J. Commun. Netw.*, vol. 11, no. 6, pp. 574–588, Dec. 2009.
[18] H.-C. Hsiao *et al.*, "Flooding-resilient broadcast authentication for VANETs," in *Proc. 17th Annu. Int. Conf. Mobile Comput. Netw. (MOBICOM)*, Las Vegas, NV, USA, Sep. 2011, pp. 193–204.
[19] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: Prediction-based authentication for vehicle-to-vehicle communications," *IEEE Trans. Depend. Sec. Comput.*, vol. 13, no. 1, pp. 71–83, Jan. 2016.
[20] X. Lin, X. Sun, X. Wang, C. Zhang, P. H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4987–4998, Dec. 2008.
[21] B. Ying, D. Makrakis, and H. T. Mouftah, "Privacy preserving broadcast message authentication protocol for VANETs," *J. Netw. Comput. Appl.*, vol. 36, no. 5, pp. 1352–1364, 2013.
[22] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 1984, pp. 47–53.
[23] A. Shamir and Y. Tauman, "Improved online/offline signature schemes," in *Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 2001, pp. 355–367.
[24] P. Ning, A. Liu, and W. Du, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 1, pp. 1:1–1:35, 2008.
[25] B. Blanchet, "Automatic verification of correspondences for security protocols," *J. Comput. Secur.*, vol. 17, no. 4, pp. 363–434, Jul. 2009.
[26] N. Ghanmy, L. C. Fourati, and L. Kamoun, "Enhancement security level and hardware implementation of ECDSA," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Split, Croatia, Jul. 2013, pp. 423–429.
[27] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong, "Efficient online/offline identity-based signature for wireless sensor network," *Int. J. Inf. Secur.*, vol. 9, no. 4, pp. 287–296, 2010.
[28] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, document RFC 5280, May 2008.
[29] *Road Vehicles—Vehicle Identification Number (VIN)—Content and Structure*, document ISO 3779, 2009.
[30] M. Fallah, "A puzzle-based defense strategy against flooding attacks using game theory," *IEEE Trans. Depend. Sec. Comput.*, vol. 7, no. 1, pp. 5–19, Jan./Mar. 2010.



CONG SUN received the B.S. degree in computer science from Zhejiang University, in 2005, and the Ph.D. degree in computer science from Peking University, in 2011. He is currently an Associate Professor with the School of Cyber Engineering, Xidian University. His research interests include information flow security and cyber-physical system security.



JIAO LIU received the B.S. degree in applied mathematics from Changán University in 2016. She is currently pursuing the degree with the School of Computer Science and Technology, Xidian University. Her research interests include security of vehicular network and systems.



XINPENG XU received the B.S. degree in computer science from Xidian University in 2017. He is currently a pursuing the degree with the School of Computer Science and Technology, Xidian University. His research interests include embedded system security, and wireless network.

JIANFENG MA received the B.S. degree in computer science from Shaanxi Normal University in 1982, and M.S. degree in computer science from Xidian University in 1992, and the Ph.D. degree in computer science from Xidian University in 1995. He is currently a Professor with the School of Cyber Engineering, Xidian University. He has published over 150 journal and conference papers. His research interests include information security, cryptography, and network security.