SLIM: Secure and Lightweight Identity Management in VANETs with Minimum Infrastructure Reliance

Jian Kang[2], Yousef Elmehdwi[1], and Dan Lin[2](✉)

[1] Department of Mathematics and Computer Science, Emory University, Atlanta, USA
yousef.Elmehdwi@emory.edu

[2] Department of Computer Science, Missouri University of Science and Technology, Rolla, USA
{jkb7c,lindan}@mst.edu

Abstract. Vehicular Ad-hoc Networks (VANETs) show a promising future of automobile technology as it enables vehicles to dynamically form networks for vehicle-to-vehicle (V2V) communication. For vehicles to securely and privately communicate with each other in VANETs, various privacy-preserving authentication protocols have been proposed. Most of the existing approaches assume the existence of Road-Side Units (RSUs) to serve as the trusted party during the authentication. However, building RSUs is costly and may not be able to capture the speed of the deployment of the VANETs in the near future. Aiming at minimizing the reliance on the infrastructure support, we propose a Secure and Lightweight Identity Management (SLIM) mechanism for vehicle-to-vehicle communications. Our approach is built upon self-organized groups of vehicles which take turns to serve as captain authentication unit to provide temporary local identities for member vehicles. While ensuring the vehicles' identities are verifiable to each other, we also prevent any vehicle in VANETs including the captain authentication unit from seeing the true identities of other vehicles. The proposed authentication protocols leverage the public key infrastructure in a way that the key generation workload is distributed over time and hence achieve authentication efficiency during the V2V communication. Compared to the previous related work, the proposed SLIM mechanism is more secure in that it can defend more types of attacks in VANETs, and is more efficient in that it requires much shorter response time for identity verification between vehicles.

Keywords: VANETs · Privacy · Authentication · Lightweight
Vehicle-to-vehicle communication

1 Introduction

Vehicular Ad-hoc Networks (VANETs) are being touted as the crux of the future of automobile technology. In VANETs, vehicles can leverage onboard

X. Lin et al. (Eds.): SecureComm 2017, LNICST 238, pp. 823–837, 2018.
https://doi.org/10.1007/978-3-319-78813-5_45

computing and communication devices to form dynamic networks for vehicle-to-vehicle communication. This technology would foster a variety of new and interesting applications such as obtaining real-time road safety and traffic information from peer vehicles, and sharing files among neighboring vehicles similar to that in Internet. Almost all the major automobile manufacturers have invested heavily on research regarding VANETs. Current prototypes like NOW (Network on Wheel) [2] and SeVeCom [16] have already provided workable testing-models for real-world use.

Since many VANET applications are based on vehicle-to-vehicle (V2V) communication, it is critical to ensure the integrity and authenticity of the messages exchanged by vehicles. Meanwhile, it is also important to preserve the privacy of the vehicle owners during the communication. This is not only because people may not feel comfortable to disclose their true identities to strangers, but also because a series of attacks (such as impersonation) may be easily launched when true identities are disclosed. In order to achieve secure and private V2V communication, various privacy preserving authentication protocols have been proposed [6,9,23]. Most of the existing approaches assume the existence of Road-Side Units (RSUs) to serve as the trusted party during the authentication. However, building RSUs is costly and may not be able to capture the speed of the deployment of the VANETs in the near future.

Aiming at minimizing the reliance on the infrastructure support, we propose a Secure and Lightweight Identity Management (SLIM) mechanism for V2V communications. Specifically, the SLIM scheme has an initial registration phase where the vehicles only need to contact a central authority once the first time they log on VANETs to obtain a global identity. This global identity is tied to the vehicle's identification number (VIN) without explicitly revealing this information. Then as vehicles move around, they self-organize into groups of similar interest or destinations using our previously proposed moving-zone forming protocols [11]. Inside each moving zone, vehicles take turns to serve as the captain authentication unit (CAU) who will be in charge of generating a temporary local identity for each member vehicle to communicate with peers. The local identities are computed from the vehicle's global identity, and do not reveal the true identity of vehicles to the CAU or peer vehicles. Moreover, the SLIM mechanism also support traceability in that the true identity of a malicious vehicle can be recovered through the collaboration between other peer vehicles and the central authority. We have implemented our approach and compared the performance with the most related V2V-based authentication approach [22]. The experimental results show that the SLIM is much faster during the V2V authentication.

The proposed SLIM mechanism has the public key infrastructure as the building block similar to many existing works. However, compared to the existing works, the SLIM has three major advantages:

1. The SLIM mechanism does not rely on infrastructure support during V2V communication.

2. The SLIM mechanism is more secure than other V2V-based authentications such as [22] in that the SLIM can defend more types of attacks as discussed in Sect. 5.
3. The SLIM mechanism is more efficient for V2V authentication by distributing the authentication workload such as the key generation over time.

The rest of the paper is organized as follows. Section 2 reviews related works on privacy-preserving vehicle authentication. Section 3 introduces the threat model, design goals and notations. Section 4 presents the details of the proposed SLIM scheme. Section 5 discusses the reaction of the SLIM scheme to various attacks in VANETs. Section 6 reports the experimental results. Finally, Sect. 7 concludes the paper.

2 Related Work

There have been lots of efforts in developing privacy-preserving authentication protocols in VANETs, which can be roughly classified into two main categories based on the fundamental techniques: (i) pseudonym-based and (ii) group-based approaches. An early work on pseudonym-based authentication protocol is by Raya and Hubaux [19]. They allow vehicles to randomly select a private key from a huge pool of certificates issued by the authority and use this private key to verify the vehicle's identity. However, the vehicles may need to check a long list of revoked certificates when verifying a received signed-message, which could be very time consuming. Raya et al. in [20] proposed efficient revocation schemes. However, these schemes do not preserve the location privacy [12] and are subject to a movement tracking attack. Later, more works [10,21,23,30] have been proposed to further improve the key revocation efficiency when using pseudonyms. Rajput et al. proposed a hierarchical privacy preserving pseudonym-based authentication protocol [18] that the primary pseudonyms were issued by a central authority, and the secondary pseudonyms were issued by RSUs. Yet another recent work called RAU (Randomized AUthentication) by Jiang et al. [8] proposed to use two cloud servers to generate any number of pseudonyms for vehicles.

The group-based protocols [5,14,26] may look more similar to our proposed scheme in the sense that they also group vehicles before authentication. Many group-based protocols leverage the group signature scheme, ring signature or blind signature [24,28,29]. Under the group signature scheme, vehicles can only verify that the messages are from a valid group member but do not know who is the actual sender. In our proposed SLIM scheme, message receivers know the anonymous ID of the sender vehicles and vehicles are also traceable in the case of dispute. More recently, Whyte et al. [27] presents a security credential management system for V2V communication by implementing a Public-Key Infrastructure (PKI) with additional new features. It issues digital certificates to vehicles to establish trust among them. Hasrouny et al. [7] also proposed a group-based V2V authentication and communication solution. They assume the mutual authentication were done by RSUs and decentralize their system via group leaders to make the system more efficient. Want et al. [25] proposed a two-factor lightweight privacy-preserving authentication scheme which employs the decentralized certificate authority (CA) and biological-password-based authentication. Their protocol depends on the RSUs which are responsible for message forwarding and key updating.

Most existing privacy preserving authentication schemes such as those discussed in the above, all heavily rely on some sort of infrastructure such as RSUs. However, RSUs would be expensive to deploy and are not expected to be widely available anytime soon. Very few works provide privacy preserving authentication based on pure V2V communication. One representative work could be the PAIM scheme proposed by Squicciarini et al. [22]. Since our work will be compared with PAIM, we provide more detailed review of this system as follows. The PAIM protocol dynamically constructs groups via pure vehicle-to-vehicle communication, and leverages Pedersen commitment and secret sharing scheme to achieve anonymously authentication of vehicles. The biggest drawback of the Pedersen commitment scheme is that it is malleable. A commitment scheme is non-malleable [1,3,4] if one cannot transform the commitment of another person's secret into one of a related secret. Unfortunately, this property is not achieved by Pedersen commitment scheme [17] because it is only designated to hide the secret. Compared to PAIM, the SLIM scheme also has the concepts of global identities and local identities. However, the protocols to generate the global and local identities are totally different, which makes the proposed SLIM scheme more secure and more efficient during the V2V authentication.

3 Threat Model and Design Goals

3.1 Threat Model

Our proposed SLIM scheme aims to defend the following attacks in VANETs as some are also pointed out in [13]:

- **Eavesdropping Attack:** The attacker can eavesdrop on any communication in the VANET.
- **Impersonate Attack:** Attackers may pretend to be another vehicle in the network to fool the others.
- **Movement Tracking:** An adversary who constantly eavesdrops messages exchanged in VANETs and therefore tracks other vehicles' travel routes.
- **Message Replay Attack:** Replay the valid messages to disturb the traffic.
- **Man-In-The-Middle Attack:** Attackers may relay and alter the messages during the transmission between two vehicles who believe they are communicating with each other directly.
- **Denial of Service (DoS) Attack:** The attacker may send a large amount of junk messages to prevent legitimate users from accessing other vehicles' computing and communication resources.

3.2 Design Goals

Our proposed SLIM aims to achieve the following design goals:

- **Data Origin Authentication and Integrity:** Every exchanged message should be unaltered during the delivery and can be authenticated by the receiver. Authentication and integrity of the messages must be verified [15].
- **Anonymous User Authentication:** The process of authenticating the vehicle should not reveal the vehicle's real identity to other peer vehicles.
- **Vehicle Traceability:** In case there is any dispute, the authority should be able to reveal the real identity of the suspect vehicle.
- **Message Unlinkability:** Observers can not link messages observed in different groups to the same vehicle so that observers cannot track other vehicles.

We list the description of the notations used throughout this paper in Table 1.

Table 1. Notations and definitions

Notation	Definition
v_i	Vehicle i
ID_i	Vehicle's identity encrypted by DMV_{pubkey}
CAU^j	Captain authentication unit of zone j
GIT_i	Global identity token for vehicle i
LIT_i^j	Local identity token for vehicle i for a specific zone j
$\{...\}_{key}$	Encryption using key
$Sign(...)_{key}$	Generate signature using key
$key_{i,k}$	Session key between two vehicles v_i and v_k
R_i	Role of vehicles i (government car, emergence car, etc.)
r_i	Nonce generated randomly by CAU^j for vehicle v_i

4 Secure and Lightweight Identity Management Scheme

In this section, we present the details of the proposed Secure and Lightweight Identity Management (SLIM) scheme in VANETs. The SLIM scheme is built upon moving zones self-organized by vehicles using the zone forming protocols in [11]. Each self-organized moving zone is formed by a group of vehicles with similar movement patterns or social interest. These moving zones are dynamic and will change as vehicles move. Each zone has a captain vehicle which helps pass messages among member vehicles. In SLIM, we assign the captain vehicle a new task to serve as the authentication unit and name it captain authentication unit (CAU) similar to [22]. The SLIM scheme ensures that the vehicles' identities are verifiable to each other while preventing any vehicle in the VANET including the CAU from seeing the true identities of other vehicles.

Procedure 1. Registration

Each Vehicle v_i executes the following steps

Generate global key pair $Gpubkey_i$ and $Gprikey_i$

Encrypt $ID_i = \{Identity_i, VIN\}_{DMV_{pubkey}}$

Generate signature $rs_i = Sign(ID_i, Gpubkey_i)_{Gprikey_i}$

$v_i \xrightarrow{\{ID_i||Gpubkey_i||rs_i\}_{IDMC_{pubkey}}} IDMC$

IDMC executes the following steps

Decrypt using $IDMC_{prikey}$

Verify signature rs_i using $Gpubkey_i$

Verify v_i's identity ID_i with DMV

IF v_i's identity is verified

Generate a random number r_i

Generate signature $s_i = Sign(r_i, R_i, Gpubkey_i)_{IDMC_{prikey}}$

Generate $GIT_i = \langle r_i, R_i, Gpubkey_i, s_i \rangle$

$IDMC \xrightarrow{\{GIT_i\}_{Gpubkey_i}} v_i$

ELSE Reject Request

Each Vehicle v_i executes the following steps

Verify signature s_i using $IDMC_{pubkey}$ and obtain GIT_i

The SLIM scheme is composed of three phases: *Registration*, *Inner-zone Authentication* and *P*eer-to-Peer Communication. During the registration phase, a vehicle will contact Identity Management Center (IDMC) to be verified and then obtain a global identity that does not reveal the vehicle's real identity. During the authentication phase, vehicles will send its global identity to the CAU to obtain a local identity. This local identity is later used for communication among vehicles in the same moving zone. In what follows, we elaborate the detailed algorithms for generating the global and local identities.

4.1 Registration

Procedure 1 presents the registration phase of our proposed scheme. This phase is executed only once for each new vehicle joining the VANET. The first time that a vehicle v_i logs onto the VANET, it will communicate with the IDMC to obtain a global identity token GIT. Specifically, before logging onto the VANET, v_i need to generate a pair of global keys $Gpubkey_i$ and $Gprikey_i$, encrypt its ID_i using DMV_{pubkey} and generates a digital signature rs_i. The first time that v_i enters the VANET, it sends a encrypted registration request to IDMC.

When receives the registration request, the IDMC decrypts it and verifies v_i's signature rs_i to make sure that the message is sent by v_i who owns $Gprikey_i$. Then the IDMC verifies the received encrypted identity information ID_i with DMV (Department of Motor Vehicles). Since the verification message can only be decrypted by DMV, the IDMC will only know whether v_i has a valid identity but don't know what this true identity is. In this way, the vehicles' privacy is

Procedure 2. Joining Existence Zone j

Each Vehicle v_i executes the following steps

Generate local key pair $Lpubkey_i^j$ and $Lprikey_i^j$

Generate signature $vs_i = Sign(GIT_i, Lpubkey_i^j)_{Gprikey_i^j}$

$v_i \xrightarrow{\{GIT_i||Lprikey_i^j||vs_i\}_{CAU^j_{pubkey}}} CAU^j$

CAU^j executes the following steps

Decrypt using CAU^j_{prikey}

Verify IDMC's signature on GIT_i

Verify signature vs_i using $Gpubkey_i^j$

IF verified

Generate timestamp T_c

Generate signature $cs_i = Sign(R_i, T_c, Lpubkey_i^j)_{CAU^j_{prikey}}$

Generate $LIT_i^j = \langle R_i, r_i, Lpubkey_i^j, cs_i\rangle$

$CAU^j \xrightarrow{\{LIT_i^j\}_{Lpubkey_i^j}} v_i$

ELSE Reject Request

Each Vehicle v_i executes the following steps

Verify timestamp T_c and signature cs_i using CAU_{pubkey}

Obtain LIT_i^j

also protected against the IDMC. Only if the validation result is true, for v_i, the IDMC generates a global identity token GIT_i. Upon receiving the GIT_i, v_i decrypts and verifies it to ensure that the GIT_i was issued by the IDMC and has not been altered. At this point, v_i has a global identity token that does not reveal any sensitive information about its actual identity.

4.2 Inner-Zone Authentication

After vehicle v_i obtains the global identity token, it can use this token to be authenticated in any moving zone that it belongs to during the movement. Specifically, when v_i joins a new moving zone Z_j, it will contact the captain authentication unit CAU^j to obtain a local identity token LIT_i^j. This local identity LIT_i^j will only be used within this zone. When v_i moves to another zone, it will need to seek another local identity so that it would not be easily tracked by observers. Procedure 2 illustrates how the local identity tokens are issued.

In Procedure 2, vehicle v_i first randomly generates a pair of local keys $Lpubkey_i^j$ and $Lprikey_i^j$ during any free time before v_i wants to enter a new zone so that the generation procedure would not affect the authentication time. Then, v_i computes a digital signature vs_i and sends a join request to CAU_j.

When receives the join request, the CAU^j decrypts it using its private key, extracts v_i's global identity token GIT_i and verifies IDMC's signature s_i in GIT_i

Procedure 3. Peer-to-Peer Communication (v_i, v_k) within Zone j

Vehicle v_i executes the following steps

$v_i \xrightarrow{LIT_i^j} v_k$

Vehicle v_k executes the following steps

Verify CAU^j's signature on LIT_i^j

IF Verified

Generate session key $key_{i,k}$

Generate signature $ts_k = Sign(LIT_k^j,\ key_{i,k})_{Lprikey_k^j}$

$v_k \xrightarrow{\{LIT_k^j,\ key_{i,k},\ ts_k\}_{Lpubkey_i^j}} v_i$

ELSE Reject Request

Vehicle v_i executes the following steps

Decrypt using $Lprikey_i^j$ and extract LIT_k^j

Verify CAU^j's signature on LIT_k^j

IF Verified

v_i and v_k authenticate each other and both share the session key $key_{i,k}$

ELSE Reject Request

to validate this global identity. The CAU^j also verifies v_i's signature vs_i to ensure that this GIT_i belongs to v_i. Only if the verification results are true, the CAU^j generates a randomized number r_i, issues a local identity LIT_i^j and sends this local identity to v_i.

Once receives the response from CAU^j, vehicle v_i will extract and verify the authenticity and integrity of this response. At this point, v_i has obtained a local identity token LIT_i^j until it leaves current moving zone.

4.3 Peer-to-Peer Communications

After vehicle v_i obtains the local identity LIT_i^j, it is now ready to securely communicate with any other vehicles in the same zone. As illustrated in Procedure 3, in particular, when v_i intends to establish a fresh session communication channel with another vehicle (say v_k), the first step is to generate a session key between them. For this, v_i first send a session request along with its local identity LIT_i^j to v_k. When receives this request, v_k first verify the validity of v_i's local identity by checking the CAU^j signature in LIT_i^j and generate a random session key $key_{i,k}$ and a signature ts_k. Then, encrypts the following message using v_i's local public key so that attackers can neither eavesdrop or modify it: $\{LIT_k^j, key_{i,k}, ts_k\}$. After that, sends it to v_i. Once receives this response, v_i will decrypt the message and verify the identity of v_k in the same way that v_k just did.

After the above peer-to-peer authentication, v_i and v_k are able to communicate securely by encrypting the messages using the session key in the following form: $\{LIT_{v_i}^j, msg\}_{key_{i,k}}$. It is worth noting that as long as v_i and v_k stay communicating with each other, the peer-to-peer authentication between these two vehicles just need to conducted once. If more security is desired, the two vehicles can change the session keys over time.

To sum up, the SLIM scheme involves one-time communication between the IDMC and the vehicle, and vehicles can have different local identities in different moving zones for privacy preserving.

5 Security Analysis

In this section, we analyze the reactions of our proposed SLIM scheme to common attacks in the VANETs.

Eavesdropping Attack: With our SLIM scheme in place, any outside attacker cannot obtain any sensitive identity information of vehicles by eavesdropping the VANETs. When sending the registration request to IDMC, the vehicle's identity information was encrypted by DMV_{pubkey}, and the whole request was encrypted by $IDMC_{pubkey}$ too. It is impossible for any attacker to decrypt the registration message because they do not have the required private keys. For the same reason, outside attackers cannot eavesdrop any valuable private information during the peer-to-peer authentication and communication.

Considering inside attackers, the IDMC can only verify v_i's identity with DMV without knowing any detail personal information because only DMV can extract the private information from ID_i. Moreover, the $CAUs$ cannot eavesdrop their member vehicles' communication either. This is because CAUs do not know the session keys established between member vehicles.

Impersonation Attack: In SLIM, a vehicle v_i cannot be impersonated because no other vehicles knows v_i's $Gprikey_i$ or $Lprikey_i$. Thus, it is impossible for other vehicles to generate v_i's signature or decrypt the messages received by v_i. More specifically, during the peer-to-peer communication, suppose that an attacker knows v_i's LIT_i and plans to impersonate v_i. When the attacker sends this local identity to another vehicle v_k in the same moving zone, v_k will generate a session key encrypted using vehicle v_i's $Lpubkey_i$ and send it back to the attacker. Since the attacker does not possess vehicle v_i's local private key, it would not be able to decrypt the message received from v_k and hence cannot pretend to be v_i.

Movement Tracking: As previously mentioned, any outside attacker cannot see sensitive ID information by eavesdropping the network that is using the SLIM scheme. Thus, outsiders would not be able to find out the traveling routes of vehicles. Considering the insider attacks, we separate the cases of CAU and member vehicles. Any member vehicle only knows the local identities of vehicles in the same zone that communicates with it, but does not know the global identity of these vehicles. Thus, member vehicles may only be able to track the vehicles who are communicating with it within the same zone, but will not be able to keep tracking the same vehicle which has moved to another zone. Note that member vehicles even do not know if they are communicating with the same vehicle that they have met in the past since the same vehicle will use a different local identity in a different zone.

As for CAUs who know the global identities of its member vehicles, the CAU may be able to track the same vehicle whenever the vehicle enters its moving zone. However, this risk can be mitigated by a proper CAU election which forbids a vehicle to serve as a CAU continuously and frequently. This can be achieved since member vehicles know the CAU's global identity and they can verify if the same vehicle wants to serve CAU again when they move along together from one zone to another. On the other hand, a normal CAU may not want to serve as CAU frequently either since in that way it exposes its global identities for a long time for others to track.

Message Replay Attack: In our system, if an attacker replays a registration or inner-zone authentication request sent by vehicle v_i, it would not be able to decrypt the response messages from IDMC or CAU without knowing the private keys obtained by v_i. Also, if an attacker replays a message sent by v_i to v_j, it would not be able to know the content of the response sent back by v_j since the attacker does not know the session key used by v_i and v_j. As a result, the attacker would not be able to continue meaningful conversation with v_j further.

Man-In-The-Middle Attack: All the messages in our SLIM scheme are either signed or encrypted, which prevents attackers to modify or reuse. Specifically, the global identity GIT_i cannot be modified by other vehicles because it's signed by the IDMC. Vehicle v_i's inner-zone authentication request can only be verified by $Gpubkey_i$ which is included in GIT_i. Thus, any other entity cannot modify this request and regenerate the signature without knowing v_i's $Gprikey_i$. Also, attackers cannot put itself into the communication between vehicles. When v_i communicates with the IDMC, its message is encrypted using the IDMC's public key and hence only the IDMC can open it. When the IDMC responds to v_i, the message is encrypted using v_i's public key and hence only v_i can open the message. The case with the CAU is similar.

During the peer-to-peer communication, when v_k received the local identity LIT_i^j from v_i, a possible attack that it may conduct is to pass this local identity to another v_l and try to play a middle role in this communication. However, the v_l's response will be encrypted by $Lpubkey_i^j$. Since v_k does not know the local private key of v_i, v_k would not be able to decrypt the message sent back by v_l and obtain the session key inside the message. Also, v_k cannot generate new response to v_l since v_k is not able to produce v_i's signature.

Denial of Service (DoS) Attack: In the SLIM system, outside attackers' messages can be filtered because they do not have valid identity tokens. When they try to replay the registration or inner-zone authentication request, the IDMC or CAUs can reject those messages because the *Gpubkey* or *Lpubkey* have been used in the previous requests. The inside attackers also will eventually be caught as they have been authenticated and will leave all these malicious behavior in records.

6 Performance Study

We now move to evaluate SLIM's efficiency in the authentication process. We compare its performance with the most related V2V-based authentication scheme – PAIM [22]. The implementations are conducted using a machine equipped with an Intel Core i7 at 2.6 GHz with 16 GB of RAM running UNIX system. Each procedure in the program has been run 1000 times and the mean values are reported in milliseconds.

The network simulation was conducted using the Network Simulator NS-3 (version 3.26) and vehicular mobility simulator SUMO (version 0.23.0). Vehicles' movements along with the main roads of three real maps: Manhattan (4.5 km × 5.5 km), Chicago (6 km × 7 km) and Los Angeles (5 km × 4.5 km). Vehicles' speed ranging from 30 to 60 miles/h. In NS-3, the maximum transmission range is set to 100 m, the network delay is 10 ms, and the wireless transmission rate is 6 Mbps. Unless noted, otherwise we use the Manhattan map and set the number of vehicles to 800. The simulation was run for 15 s to insert all vehicles, then begin registration phase. After 60 s, at random time, each vehicle become group manager respectively, select up to 10 vehicles over a range of 80 m and start Inner-Zone Authentication. The simulation time is 120 s.

6.1 Registration Phase Performance

In the first round of experiments, we measure the average time needed for a vehicle to register at the IDMC using the SLIM and the PAIM scheme respectively. As shown in Fig. 1(a), the average registration time per vehicle under SLIM is about 40 ms, which was faster than PAIM's 80 ms. This could be attributed to the efficient protocol of SLIM which does not need extra rounds to establish a session key between the IDMC and the vehicle. Note that the vehicles' private/public key pairs in SLIM scheme can be generated during the vehicle's free time and hence would not affect any authentication performance.

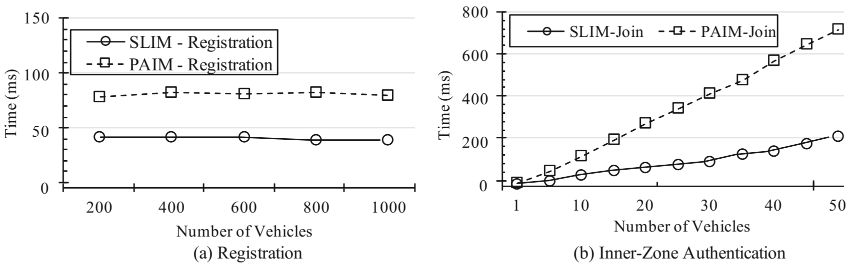

Fig. 1. Time performance

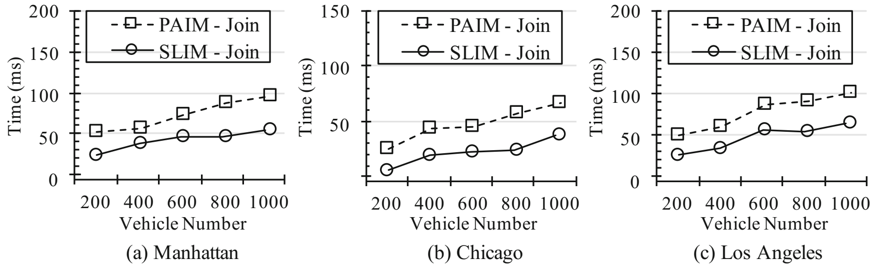

Fig. 2. Time performance during inner-zone authentication on three maps

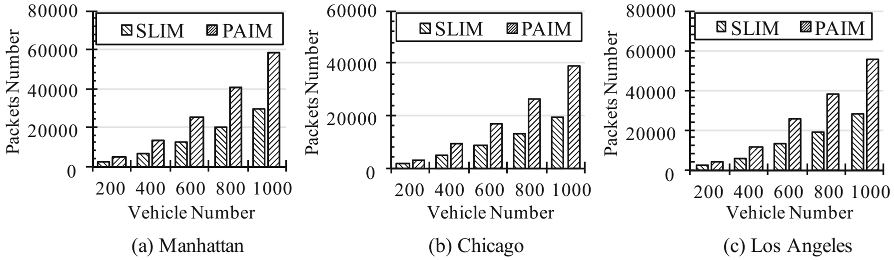

Fig. 3. Communication cost during inner-zone authentication

6.2 Inner-Zone Authentication Phase Performance

Next, we measure the performance of the inner-zone authentication for both the SLIM and the PAIM schemes. Figure 1(b) shows the total inner-zone authentication time at the CAU side when the number of vehicles in its zone varies from 1 to 50. Observe that SLIM is clearly faster than the PAIM. With the increase of the number of vehicles in the zone, the performance gap between the two approaches widened. Specifically, when there are 50 vehicles, our proposed SLIM scheme is more than 3 times faster than PAIM. In Fig. 2, with the increasing of the number of vehicles, the time raises due to more packets, larger network delay and heavier workload, and our SLIM protocol is obviously performs better than PAIM. This is because the SLIM scheme requires much fewer rounds of message exchanges to generate a local identity for a vehicle as shown in Fig. 3.

6.3 Peer-to-Peer Communication Performance

Finally, we compare the efficiency of the two approaches in terms of peer-to-peer communication. Figure 4 presents the time performance of these two protocols on three maps. In SLIM scheme, the time taken for two vehicles to mutually validate each other's local identity is only 3.5 ms excluding network delay. However, in PAIM, since two vehicles need to conduct the zero-knowledge proof which could take as long as 13.6 ms, it is clearly much slower than the SLIM scheme.

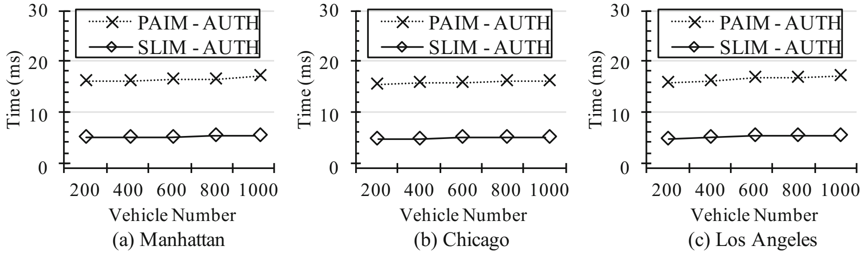

Fig. 4. Communication cost during peer-to-peer communication

7 Conclusion

In this paper, we proposed a lightweight privacy preserving vehicular authentication protocol SLIM, which alleviates the reliance on infrastructure support. The SLIM scheme leverages the PKI in an efficient way to create anonymous global identity and then local identities for vehicles to preserve their privacy when communicating with other vehicles. The SLIM is not only robust against various types of attacks but also very efficient as compared to the state-of-the-art.

Acknowledgement. This work is partially supported by National Science Foundation under the project DGE-1433659.

References

1. Di Crescenzo, G., Katz, J., Ostrovsky, R., Smith, A.: Efficient and non-interactive non-malleable commitment. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 40–59. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44987-6_4
2. Festag, A., Noecker, G., Strassberger, M., Lübke, A., Bochow, B., Torrent-Moreno, M., Schnaufer, S., Eigner, R., Catrinescu, C., Kunisch, J.: Now-network on wheels: project objectives, technology and achievements. In: Proceedings of 6th International Workshop on Intelligent Transportations (WIT), Hamburg, Germany (2008)
3. Fischlin, M., Fischlin, R.: Efficient non-malleable commitment schemes. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 413–431. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-44598-6_26
4. Fischlin, M., Fischlin, R.: Efficient non-malleable commitment schemes. J. Cryptol. **24**(1), 203–244 (2011)
5. Hao, Y., Yu, C., Zhou, C., Song, W.: A distributed key management framework with cooperative message authentication in VANETs. IEEE J. Sel. Areas Commun. **29**(3), 616–629 (2011)
6. Harsch, C., Festag, A., Papadimitratos, P.: Secure position-based routing for VANETs. In: Vehicular Technology Conference, pp. 26–30. IEEE (2007)
7. Hasrouny, H., Bassil, C., Samhat, A.E., Laouiti, A.: Group-based authentication in V2V communications. In: Digital Information and Communication Technology and its Applications (DICTAP), pp. 173–177. IEEE (2015)

8. Jiang, W., Lin, D., Li, F., Bertino, E.: No one can track you: randomized authentication in vehicular ad-hoc networks. In: IEEE International Conference on Pervasive Computing and Communications (PerCom). IEEE (2017)
9. Jung, C.D., Sur, C., Park, Y., Rhee, K.-H.: A robust conditional privacy-preserving authentication protocol in VANET. In: Schmidt, A.U., Lian, S. (eds.) MobiSec 2009. LNICST, vol. 17, pp. 35–45. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04434-2_4
10. Li, J., Lu, H., Guizani, M.: ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Trans. Parallel Distrib. Syst. **26**(4), 938–948 (2015)
11. Lin, D., Kang, J., Squicciarini, A., Wu, Y., Gurung, S., Tonguz, O.: MoZo: a moving zone based routing protocol using pure V2V communication in VANETs. IEEE Trans. Mob. Comput. **PP**(99), 1 (2016)
12. Lin, D., Bertino, E., Cheng, R., Prabhakar, S.: Location privacy in moving-object environments. Trans. Data Priv. **2**(1), 21–46 (2009)
13. Lin, X., Sun, X., Ho, P.H., Shen, X.: GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans. Veh. Technol. **56**(6), 3442–3456 (2007)
14. Lu, R., Lin, X., Zhu, H., Ho, P.H., Shen, X.: ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In: Proceedings of IEEE Conference on Computer Communications, pp. 1229–1237 (2008)
15. Mohanty, S., Jena, D., Panigrahy, S.: A Secure RSU-Aided Aggregation and Batch-Verification Scheme for Vehicular Networks (2012)
16. Papadimitratos, P., Hubaux, J.: Report on the "secure vehicular communications: results and challenges ahead" workshop. IEEE Commun. Mag. **12**(2), 53–64 (2008)
17. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (1992). https://doi.org/10.1007/3-540-46766-1_9
18. Rajput, U., Abbas, F., Oh, H.: A hierarchical privacy preserving pseudonymous authentication protocol for VANET. IEEE Access **4**, 7770–7784 (2016)
19. Raya, M., Hubaux, J.P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**, 39–68 (2007)
20. Raya, M., Jungels, D., Papadimitratos, P., Aad, I., Hubaux, J.P.: Certificate revocation in vehicular networks. Laboratory for Computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL (2006)
21. Shim, K.A.: CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. IEEE Trans. Veh. Technol. **61**, 1874–1883 (2012)
22. Squicciarini, A., Lin, D., Mancarella, A.: PAIM: peer-based automobile identity management in vehicular ad-hoc network. In: 2011 IEEE 35th Annual Computer Software and Applications Conference (COMPSAC), pp. 263–272. IEEE (2011)
23. Sun, J., Zhang, C., Zhang, Y., Fang, Y.: An identity-based security system for user privacy in vehicular ad hoc networks. IEEE Trans. Parallel Distrib. Syst. **21**(9), 1227–1239 (2010)
24. Tan, Z.: A lightweight conditional privacy-preserving authentication and access control scheme for pervasive computing environments. J. Netw. Comput. Appl. **35**(6), 1839–1846 (2012)
25. Wang, F., Xu, Y., Zhang, H., Zhang, Y., Zhu, L.: 2FLIP: a two-factor lightweight privacy-preserving authentication scheme for VANET. IEEE Trans. Veh. Technol. **65**(2), 896–911 (2016)

26. Wang, Y., Zhong, H., Xu, Y., Cui, J.: ECPB: efficient conditional privacy-preserving authentication scheme supporting batch verification for VANETs. IJ Netw. Secur. **18**(2), 374–382 (2016)
27. Whyte, W., Weimerskirch, A., Kumar, V., Hehn, T.: A security credential management system for V2V communications. In: 2013 IEEE Vehicular Networking Conference (VNC), pp. 1–8. IEEE (2013)
28. Yeh, L., Chen, Y., Huang, J.: PAACP: a portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks. Comput. Commun. **34**(3), 447–456 (2011)
29. Zeng, S., Huang, Y., Liu, X.: Privacy-preserving communication for VANETs with conditionally anonymous ring signature. Int. J. Netw. Secur. **17**(2), 135–141 (2015)
30. Zhang, C., Ho, P.H., Tapolcai, J.: On batch verification with group testing for vehicular communications. Wirel. Netw. **17**(8), 1851–1865 (2011)