Winter 12-6-2018

Privacy-preserving Wi-Fi Access Scheme for VANETs

Tao Wan

Hongjie Zhang

Shengke Zeng

Wan, T., Zhang, H., & Zeng, S. (2018) Privacy-preserving Wi-Fi access scheme for VANETs. In *Proceedings of The 18th International Conference on Electronic Business* (pp. 461-469). ICEB, Guilin, China, December 2-6.

Privacy-preserving Wi-Fi Access Scheme for VANETs

(Full Paper)

Tao Wan, Xihua University, China, 996088955@qq.com
Hongjie Zhang, Xihua University, China, 18280418253@163.com
Shengke Zeng, Xihua University, China, zengshengke@gmail.com

ABSTRACT

Recently, great progress has been made in the study of Vehicular Ad Hoc Networks (VANETs) to solve road congestion and prevent traffic accidents. To pursue the life quality, driving comfort and entertainment requirements are necessary, such as surfing the Internet, searching nearby gas stations, restaurants, etc. Hence, vehicles have to access to the Internet via Wi-Fi hotspots provided by roadside units (RSUs). Obviously, the connection to RSUs reveals the driving routine. The location privacy of vehicles is seriously threatened. In this paper, we propose a novel approach to protect the location privacy while accessing to Wi-Fi hotpots (RSUs). We adopt the idea of 'off-the-record' communication to achieve the privacy property. In other words, the vehicle performs a deniable authentication with RSU while accessing to Wi-Fi hotpot and the participants should have the *deniability* capability. RSU provides the Internet service to the vehicle if authentication completes. On the other hand, this authentication conversation leaves no 'paper trail' and therefore, the vehicle can deny to a third party that the fact of the authentication occurred since the communication transcript could be produced (simulated) by others.

Keywords: Location privacy, Wi-Fi hotpots access, privacy-preserving authentication, deniability.

*Corresponding author

INTRODUCTION

With the development of society, the vehicles have become the essential for people to travel. The increase of vehicles also brings many problems such as traffic congestion, traffic accidents and so on. Vehicular Ad Hoc Networks (VANETs) emerge to solve above problems, and hence have been highly concerned by automobile manufacturers, research institutions and governments. VANETs are the new large-scale mobile ad hoc networks composed of On-board Units (OBUs) and Road-side Units (RSUs). The communication between the OBUs and RSUs can realize efficient accident warning, auxiliary driving, road traffic information query, Internet services and so on.

However, VANETs encounter the great threat of privacy leakage while improving the security, efficiency and convenience of the transportation system. The traffic information such as speed, location, direction and the regularity of vehicle movement are useful for VANETs, but sensitive for users privacy. As people pay more and more attention to personal privacy, the design of an effective privacy-preserving mechanism has become a key issue in the successful deployment of VANETs.

On the other hand, vehicles need Internet service while driving to improve the quality of driving experience, such as surfing the Internet, searching nearby gas stations, restaurants, etc. Most applications support RSUs to use WLAN access mode to provide the Internet service for vehicles. The IP/MAC address is necessary for the authentication during the access procedure. Obviously, connection to RSUs which play the role of Wi-Fi hotpots leaks the drive routines of vehicles. Therefore, location privacy of the vehicle is focused while accessing to Wi-Fi.

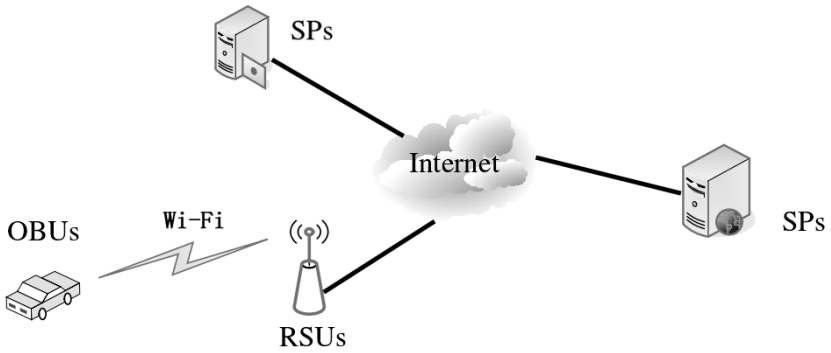

Figure 1: Vehicles Access to Wi-Fi Hotpots for Internet Service

Related Work

When the vehicle connects to a Wi-Fi hotpot to obtain the Internet service, this access point (AP) records vehicle information (e.g. IP/MAC address) from the authentication procedure. Since the AP location is fixed, this vehicle can be located obviously. Therefore, it is possible to pinpoint the location of a user to a particular depot, or a particular section of a square. Location privacy is necessary concerned while accessing to Wi-Fi for vehicles.

To address the location privacy issue in wireless environments, several approaches are proposed. Schilit, Hong and Gruteser (2003) proposed Wireless Location Privacy-preserving for the first time. This paper points out that with the development of Wi-Fi and location services, it will bring great challenges to user's location privacy. And assume some privacy risks, which now seems to exist. Then there are some K-anonymity schemes (Gruteser & Grunwald, 2003; Yang *et al.*, 2013) which are the most widely adopted. Such schemes attempt to fuzz the location resolution by hiding a mobile user from a certain range including k-1 other mobile users. However, considering the lightweight setup in Wi-Fi deployment sites, they are confronted with the challenge of lacking the trusted third party whose job is to relay the communication between the mobile users and the LBS provider. Titkov and Poslad (2003) realizes user anonymity through a Mediator Agent, either a user-controlled or a trusted-third-party mediator that separates mobile terminals from service providers on the fixed network. Raghunath and Narayanaswami (2007) works by examining each unique identifier that can be used to associate location information with a particular subscriber, and making each such identifier useless. Quigley *et al.* (2004) proposes location obfuscation: LBSs can only access a uniformly downscaled location information (with lower precision and lower geographical granularity) instead of exact client positions. Bellavista, Corradi and Giannelli (2005) presents the privacy-related extension of our proxy-based mobile agent middleware to support personalized service provisioning to Wi-Fi portable devices. Jiang, Wang and Hu (2007) obfuscate several types of privacy-compromising information revealed by a mobile node, including sender identity, time of transmission, and signal strength. Peng, Kaji and Kawaguchi (2014) presented an algorithm that determined the reliability of the user by considering the probability of both spatial and temporal to resolve the privacy problem in Wi-Fi based location estimation.

As far as we know, most of the existing schemes involve third party participation or fuzzy location based schemes. In a scheme with a third party, the assumption that a third party can be completely trusted is very strong. In the location based fuzzy scheme, SP can not get the exact location, thereby reducing the quality of service. In this paper, we propose a scheme that requires neither third party nor fuzzy location. This does not only protect the user's location privacy, but also does not reduce the quality of service.

Contribution

We propose a location privacy-preserving scheme while vehicles accessing to the Wi-Fi hotpots to obtain the Internet service. Different with the existing schemes, we adopt a novel idea to achieve the privacy property. We make use of the deniability to provide the conversations with 'off-the-record'. Technically, we employ the deniable authentication (Zeng *et al.*, 2018) as the building block to protect the location privacy of vehicles while connecting to the Wi-Fi hotpots. Vehicle submits its identity (i.e., IP/MAC address) to the server (RSU) to obtain the Internet service for the authentication. This is the evidence to disclosure its drive circuit and hence leak the location privacy. To meet the location privacy of OBUs, we require the authentication protocol satisfying the deniability. In the end of the execution of authentication, RSU can be convinced that OBU is the legal user to gain the Internet service. On the other hand, the deniability prevents that RSU to show the evidence to the third party as the conversation transcript can be simulated by anyone including RSU. Therefore, the location privacy of OBU is perfectly protected. We design this deniable authentication protocol by using the projective hash function (Zeng *et al.*, 2017).

Organization

This paper is organized as follows. We review the properties of projective hash function which is an essential tool to construct the protocols and the notion of deniable authentication in the section 2. We introduce the architecture of VANETs and the principle of Wi-Fi access in the model of VANETs in the section 3. We construct the deniable authentication based on the projective hash function and then instantiate this protocol to protect the location privacy while accessing to the Wi-Fi hotpots in the VANETs environment in the section 4. We analyze the security and performance of our proposed protocol in the following section and conclude this paper in the last section.

PRELIMINARIES

Projective Hash Function

Projective hash functions were introduced by Cramer and Shoup (2002) and later formalized by Benhamouda *et al.* (2013). The properties (projection and smoothness) of projective hash functions are used to achieve the authentication in our scheme. We first review the original definition of projective hash functions.

Definition. Define a domain χ and an NP language L with $L \subset \chi$. The projective hash function is over L. For a word $c \in L$, the value of this function can be calculated by either a secret hashing key hk or a public projection key hp with a witness ω of the fact that $c \in L$. Specifically, a projective hash function over $L \subset \chi$ is defined as follows.

-- $HashKG(L)$: Use the L to generate a secret hashing key hk;

-- $projKG(hk, L)$: Use the hk generated in the previous step to generate a projection key hp, which is public;

-- $Hash(hk, L, c)$: Use the hashing key hk and the word $c \in L$ to calculate the value of this hash function.

-- $projHash(hp, L, c, \omega)$: output the value of this hash function by using the projection key hp, the witness ω for the word $c \in L$.

Projection. We say this hash function is $projective$ if $Hash(hk, L, c) = projHash(hp, L, c, \omega)$. That means the value of the hash function can be computed even without knowing the secret hashing key hk.

Smoothness. This projective hash function is smooth if $c \notin L$, then $Hash(hk, L, c)$ is statistically indistinguishable from a random value. That means it gives no information about the hash value of any point out of L.

Deniable Authentication

Deniable authentication is first formally introduced by Dwork, Naor and Sahai (1998, 2006), which provides a property to facilitate privacy-preserving communication. The receiver is convinced that sender's authentication to some message m, however, will not be able to convince any third party that the fact of this authentication occurred as this communication transcript can be produced without the knowledge of sender's secret. With the implementation of deniable authentication to our application, Wi-Fi hotpots (RSUs) accepts vehicles(OBUs)'s authentication to the identity (IP/MAC address) while RSUs cannot convince anyone else that the fact of this service has been requested by someone. Therefore, when vehicle connects to Wi-Fi for Internet service, its identity cannot be the evidence in the authentication. In other words, connection to some RSUs do not imply the vehicle routine and the location privacy follows.

A secure deniable authentication protocol must satisfy the following fundamental security requirements.

– Authentication. The receiver can be convinced of the source and accepts the intended sender if the two parties follow the authentication protocol honestly.

– Deniability. The sender can deny its involvement in an authentication. The receiver accepts the authentication while can not convince a third party the fact of this authentication occurred. Formally, this property is captured by simulation. We require that the simulator can produce a communication transcript without sender's secret and the simulated conversation can not be distinguished.

SYSTEM ARCHITECTURE

In this section, we briefly introduce the VANETs system model, the Wi-Fi access model and the privacy requirement.

VANETs

The common VANETs system with privacy protection mainly consists of four entities: the Transportation Regulation Center (TRC), the road-side units (RSUs) and the on-board units (OBUs) equipped on moving vehicles. With the increasing demand for network, SPs has become a very important part of VANETs. The model for VANETs is shown in Figure 2. Concretely.

•TRC. TRC is the top management of the system, with sufficient storage space and computing power, generally considered to be completely reliable. TRC in our scheme is an institution which is in charge of identity authentication, issuing and recycling certificate of each vehicle. Moreover, TRC can trace the target vehicle which involved in a traffic dispute.

•RSU. RSU is the Infrastructure of Vehicle Ad Hoc Network, with strong storage space and computing power, generally considered to be not completely credible. RSU is responsible for receiving a certificate application from OBU, forwarding the application to the local TRC, and forwarding the response of TRC to OBU. RSU broadcasts road information and security information received from other RSU or collected by themselves, as well as providing OBU with Wi-Fi hotspots and OBU connections to Wi-Fi hotspots to enjoy network services.

•OBU. OBU is the infrastructure of each vehicle, with weak storage space and computing power, which is generally considered untrustworthy. Each OBU should broadcast its routine safety messages when they are on the road, such as position, direction, speed, traffic conditions and traffic events. Thereout, the communication between two vehicles or vehicle to RSU can assist drivers

to get a better awareness of their environment and take action earlier. OBU can also access network services via RSU Wi-Fi to improve the driving experience.

•SP. SP provides information services for registered OBU, such as location services, mail services, network services, etc. Although most of the SP does not depend on the vehicle ad hoc network, it is also a very important object in the vehicle network communication. So, the service provider is also an indispensable role in the model system model of the VANETs.

Wi-Fi access model

Wi-Fi (Wireless Fidelity), a short-range wireless transmission technology, enables users to access to the Internet within hundreds of meters and provides users with network services. The Wi-Fi access model is shown in Figure 3, and the Wi-Fi network structure is as follows:

•Station.The most basic component of the network.

•BSS. BSS(Basic Service Set) is the most basic service unit of the network. The simplest service unit can consist of only two sites. The site can dynamically associate to the basic service unit.

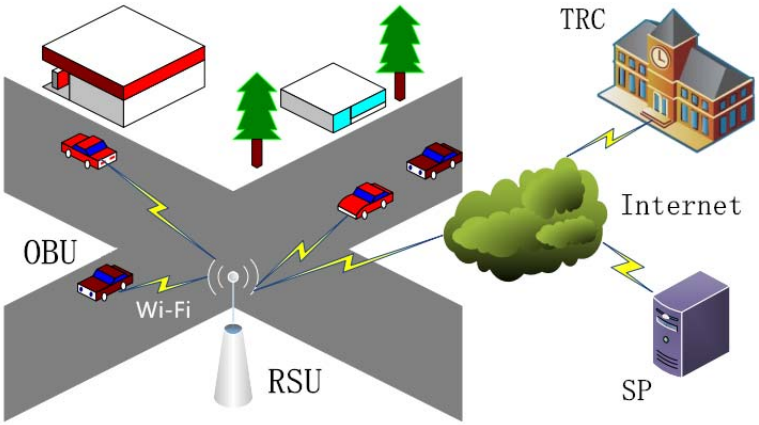

Figure 2: Vanets system model

•DS. The DS(Distribution System) is used to connect different basic service units.

•AP. The AP(Access Point) has the identity of the ordinary site and the function of accessing the distribution system.

•ESS. ESS(Extended Service Set) is composed of Distribution System and Basic Service Set. This combination is logical, not physical.

•Portal. It is also a logical element. Used to associate WLAN with wired local area networks or other networks.

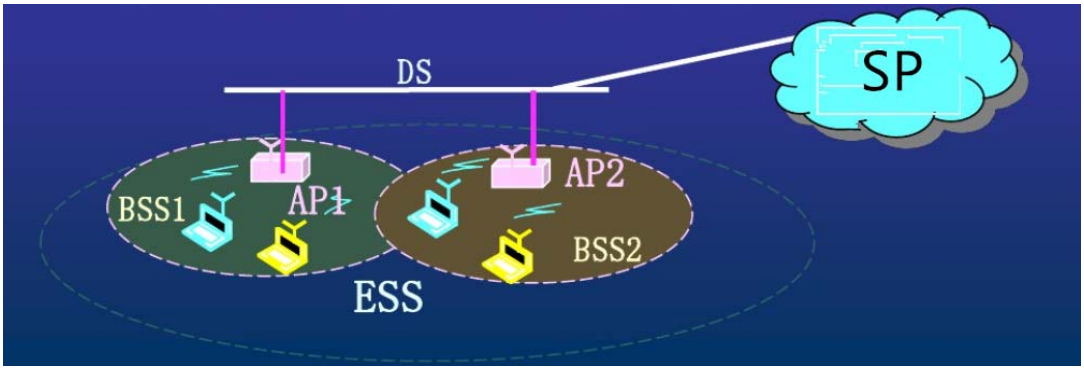

Figure 3: Wi-Fi access model

For the VANETs environment, the on-board Internet access mechanism can meet the needs for Internet access during travel, but it suffers the threat of location privacy. When vehicles access to RSU for Internet service, some regular access records(i.e., IP/MAC address, access duration, link bandwidth, and time between last visit, etc.) imply the footprints of vehicles. Since the RSU location is open and fixed. The vehicle location is also revealed if it has access to some RSU.

Privacy Definitions for VANETs

The privacy protection is the main challenge for VANETs. The sensitive information for users is the identity, the position and the requested service. The user has to show his identity when performs the authentication protocol. The identity protection requires the user identity is anonymous to anyone. The position and requested service belong to data privacy. When performs the VANETs authentication protocol, such information should be confidential to outsiders. Informally, the privacy requirements are stated as the following aspects:

Data privacy. Data privacy, is to protect the content of the communication itself is not known by entities outside the communication scene. For example, in Wi-Fi access, the RSU acts as a communication gateway, and the vehicle connects the Wi-Fi provided by RSU to communicate with SP. The vehicle is informed of the contents of its upload or download from SP, but in the process of communication, the transcript of the communication between the vehicle and SP does not wish to be obtained by a third party.

Identity privacy. Identity privacy, is to protect the identity of the communication entity is not known by a third party. Identity may be practical, but it can also be a e-mail address, employee number, etc. For example, when a vehicle accesses a email server via Wi-Fi, it does not want a third party to know its email address.

Location privacy. Location privacy, which protects the current or past communication location of the entity from being known outside the communication scene. For example, in Wi-Fi access, vehicles do not want SP to know where they are. If the communication location of the vehicle appears many times in the same family house, it can be speculated that the communication entity may be a member of the family, thus destroy the identity privacy of the entity.

By comparison, the challenge of location privacy protection is more prominent. The reasons mainly come from three aspects: (1) The quantity of location information is very large and it is very frequent to publish; (2) The change of location information is in accordance with the regularity of vehicle movement, and a very small amount of information leakage may give an attacker space for data mining. (3) Location correctness is the cornerstone of many vehicle applications and limits privacy protection.

OUR PROTOCOLS

In the process of the vehicle accessing to Wi-Fi hotpots, say RSUs, the IP/MAC address is the critical information submitted to RSUs. Therefore, the connection to RSU implies vehicle location. We adopt a novel idea to realize the location privacy while accessing to Internet via Wi-Fi hotpots. Since RSU knows the IP/MAC address of vehicle during authentication, the location privacy is preserved by deniability. The vehicle submits its identity (i.e., IP/MAC address) to RSU for authentication. RSU returns the Internet service to the corresponding vehicle if the authentication is valid. On the other hand, vehicle can deny the involvement in this authentication to the third party as this authentication is with 'off-the-record', RSU can not convince anyone else that the vehicle's connection.

In this section, we first construct a deniable authentication protocol based on the projective hash function. Then we instantiate this deniable authentication to construct a privacy-preserving Wi-Fi access scheme for VANETs.

Deniable Authentication based on Projective Hash Function

We give a generic construction of authentication protocol with deniability based on projective hash function. For each participant P in the system, it obtains the key pair (SK , PK) by invoking the hashing key generation algorithm $HashKG(L)$ and the projection key generation algorithm $projKG(hk, L)$ respectively. The public key of P is $PK = hp$ and the private key of P is $SK = hk$. The sender S authenticates a message $m \in M$ to the receiver R and S wishes to deny its involvement after executing the authentication. S sends its public key PK to the receiver R . Upon the receipts of PK from S , R begins to interact with S to execute the authentication.

Key Generation.

This algorithm is done by each participant P itself. The private/public keypair of each P is (SK , PK) = (hk , hp), where hk is the hashing key and the projection key hp is the projection key.

Deniable Authentication Protocol.

With PK , message $m \leftarrow M$ and NP language L . R picks a word $c \in L$ with the witness ω , sends $flow_1 = (m, c)$ to S .

Upon the receipt of (m,c) from R, S first computes the hash value by using the private hashing key hk and the word c, then hides this hash value by a secure commitment scheme COM. S does as following:

-- compute $\sigma = Hash(hk, L, c; m)$ with the word c, the message m and its private key $SK = hk$;

-- choose r randomly, compute $C = COM(\sigma; r)$;

-- send $flow_2 = C$ to the receiver R.

Upon the receipt of the commitment C, R reveals ω and sends $flow_3 = \omega$ to S.

Upon the receipt of ω, S first checks that the value ω is indeed the witness for $c \in L$:

-- check $projHash(hp, L, c, \omega; m) \stackrel{?}{=} \sigma$;

If this equation holds, S is sure that it can deny successfully later. Then, S reveals r to R. R calculates $\sigma = projHash(hp, L, c, \omega; m)$ and $C' = COM(\sigma; r)$. R is convinced S's authentication to m if $C' = C$.

Authentication. If the sender returns the right σ implies the sender knows the corresponding private key of PK due to the smoothness of projective hash function. The soundness of the commitment scheme COM implies σ is calculated before R's disclosure. The authentication follows.

Deniability. Since R reveals the witness ω in the step 3, anyone can generate the authentication transcript as the sender. Therefore, S can deny its authentication.

Privacy-preserving Wi-Fi Access Protocol based on Deniable Authentication

With the property of deniable authentication, we propose a novel approach to protect the location privacy while accessing to Wi-Fi hotpots in VANETs. In our construction, the vehicle submits its identity (IP/MAC address) to RSU to run the deniable authentication. We instantiate our construction by employing a concrete projective hash function. The notations of our scheme are listed in Table 1.

Table 1. Some Notations about Our Scheme

U_i	The vehicle i.
id_i	The identity of U_i.
IP	The user's IP address.
MAC	Media Access Control address.
(s_i, v_i)	The private/public key pair of U_i.
COM	A public commitment scheme

Let $\mathbb{G}$ be a group of primer order p and $g, h \in \mathbb{G}$ the generators of $\mathbb{G}$. H is a collision-free hash function: {0,1}*→ $\mathbb{Z}p$. The system parameter para=($\mathbb{G}$, p, g, h, H).

Key Gen. Each U_i chooses $x_i, y_i \leftarrow \mathbb{Z}p$, sets $h_{k_i} = (x_i, y_i)$, $h_{p_i} = g^{x_i} h^{y_i}$. U_i's keypair is $(s_i, v_i) = (h_{k_i}, h_{p_i})$.

1. $U_i \rightarrow RSU$: U_i submits $m = id_i \| IP \| MAC$ to RSU to request the Internet service.

2. $RSU \rightarrow U_i$: Upon the receipt of message $flow_1 = m$, RSU chooses a random $\omega \leftarrow \mathbb{Z}p$ and computes $c = (g^{\omega}, h^{\omega})$. RSU sends $flow_2 = (m, c)$ to U_i.

3. $U_i \rightarrow RSU$: Upon the receipt of (m, c) from RSU, U_i first computes the hash value by using its private key s_i and the word c, then hides this hash value by a secure commitment scheme COM. U_i does as follow:

-- compute $\sigma = H(s_i, L, c; m) = g^{\omega x_i} h^{\omega y_i} g^{H(m)}$ with the word $c = (g^{\omega}, h^{\omega})$ the message m and its private key s_i;

-- choose r randomly, compute $C = COM(\sigma; r)$;

-- send $flow_3 = C$ to the receiver RSU.

4. $RSU \rightarrow U_i$: Upon the receipt of the commitment C, RSU reveals ω and sends $flow_4 = \omega$ to the U_i.

5. $U_i \rightarrow RSU$: Upon the receipt of ω, U_i first checks that the value ω is indeed the witness for $c \in L$:

-- check $(g^{x_i} h^{y_i})^{\omega} g^{H(m)} \stackrel{?}{=} \sigma$;

If this equation holds, U_i is sure that it can deny successfully later. Then U_i reveals r to RSU. RSU is convinced U_i's authentication to m by calculating $\sigma = (g^{x_i} h^{y_i})^{\omega} g^{H(m)}$, $C' = COM$（$\sigma; r$）and checks $C' = C$ or not.

Remark. With the development of vehicle networking industry, 5G network technology develops rapidly. (5G network has the characteristics of high transmission rate, low delay, high stability, flexible network architecture and so on.) Vehicle networking based on 5G is developing more and more rapidly in recent years, which provides a better network environment for the realization of our scheme.

SECURITY AND PERFORMANCE

We analyze the security and performance of our proposal in this section. We mainly discuss that how does our protocol achieve the privacy protection. Then we focus on the performance of this protocol execution.

Security Analysis

Vehicles in VANETs connect to Wi-Fi hotpots to obtain the Internet service. Obviously, this connection leaks vehicle location through authentication. Thus, we analyze that how does the user obtains the Internet service (Authentication) from accessing to Wi-Fi hotpots without privacy leakage (Location Privacy).

Authentication. Wi-Fi access requires user's authentication. The vehicle is authenticated by RSU if it can calculate σ. This value can be computed only by SK. Due to the computational binding of the commitment scheme and the smoothness of the projective hash function, no one other than U_i can forge the authentication. Concretely, U_i computes $\sigma = H(s_i, L, c; m) = g^{\omega x_i} h^{\omega y_i} g^{H(m)}$ by using its private key $h_{k_i} = (x_i, y_i)$. This value σ is accepted by RSU as it can produce the same σ by using the witness ω and U_i's public key. Since the commitment scheme is sound, the committed value can not be modified to σ after the disclosure of ω.

Location Privacy. Our location privacy is achieved by the deniability. The tuple (id, IP, MAC) is submitted for authentication. However, it is the sensitive information for vehicles. The record of each connection to RSU with fixed location reveals vehicle location. If the user (vehicle) has the deniability property, the record of each authentication is not the evidence that this vehicle has been here before. Therefore, we require that this conversation transcript between U_i and RSU can be perfectly simulated and this simulation cannot be distinguishable. This is achieved by that RSU reveals the witness ω in the step 4. With ω, anyone can produce the right σ by $\sigma = (g^{x_i} h^{y_i})^{\omega} g^{H(m)}$. Therefore, there is no evidence that U_i has access to RSU. The location privacy of vehicle U_i follows.

Performance

Our proposal is a kind of cryptographic-based approach to protect user privacy in VANETs. The fundamental disadvantage of this category is the high computation and communication complexity. However, the main advantage of cryptographic-based approach is the strong privacy and security. It is inevitable to use cryptographic algorithms in order to preserve security.

We simulate the process of our scheme. We employ Inter Core i5 2.70GHz with 8GB RAM and the result is shown in Figure 4. We calculate the time it takes for OBU to authenticate under the security parameters K1=256 and K2=512, respectively. Obviously, the larger the security parameters, the longer the authentication time. In order to estimate the performance of our scheme accurately, as shown in figure 4, we have run the experiments several times under both security parameters. When the security parameter is K1=256, the first running-time is 1.971ms, the second running-time is 2.063ms, the third running-time is 2.153ms.... The average running-time under K1 is 2.095ms. When the security parameter is K2 = 512, the first running-time is 6.796ms, the second running-time is 7.326ms, the third running-time is 7.126ms.... The average running-time under K2 is 7.153ms.

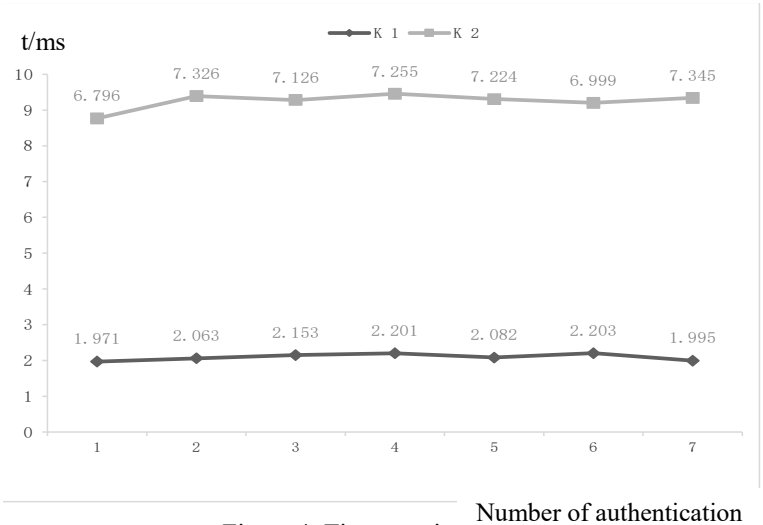

Figure 4: Time cost in authentication

CONCLUSION

In this work, we propose a novel approach that enables the user to access the Wi-Fi hotpots without location privacy leakage for vehicles in VANETs. We employ the deniable authentication to construct the protocol to provide the strong privacy. Although RSU obtains the user's identity from the authentication, it cannot convince anyone else that this user has connected to RSU, thus it has no evidence to locate this vehicle. More importantly, the 5G era is fast approaching. The 5G network technology will meet the need of high transmission rate and large capacity data processing in the vehicle network. We will consider this scheme based on 5G network in the future research.

ACKNOWLEDGMENT

This work is supported by Chunhui project of the Ministry of Education of China (Z2016150) and the National Key R & D Program of China (2017YFB0802300, 2017YFB0802000).

REFERENCES

[1] Bellavista, P., Corradi, A., & Giannelli, C. (2005). Efficiently managing location information with privacy requirements in Wi-Fi networks: a middleware approach. In Proceedings of International Symposium on Wireless Communication Systems (pp.91-95). ISWCS, Siena, Italy, Sep 5-7.

[2] Benhamouda, F., Blazy, O., Chevalier, C., Pointcheval, D., & Vergnaud, D. (2013). New Techniques for SPHFs and Efficient One-Round PAKE Protocols. In Proceedings of Cryptology Conference (Vol.8042, pp.449-475). Springer, Berlin, Heidelberg, August 18-22.

[3] Cramer, R., & Shoup, V. (2002). Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. In Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology (Vol.2332, pp.45-64). Springer, Queenstown, NewZealand, December 1-5.

[4] Dwork C., Naor M., & Sahai A. (1998). Concurrent zero-knowledge. Journal of the ACM, 51(6), 851-898.

[5] Dwork C., Naor M., & Sahai A. (2006). Concurrent zero-knowledge. Springer Berlin Heidelberg.

[6] Gruteser, M., & Grunwald, D. (2003). Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In Proceedings of International Conference on Mobile Systems, Applications, and Services (pp.31-42). MobiSys, Taipei, Taiwan, June 25-28.

[7] Jiang, T., Wang, H. J., & Hu, Y. C. (2007). Preserving location privacy in wireless lans. In Proceedings of International Conference on Mobile Systems, Applications, and Services (pp.246-257). MobiSys, San Juan, Puerto Rico, June 11-14.

[8] Peng, Z., Kaji, K., & Kawaguchi, N. (2014). Privacy protection in WiFi-based location estimation. In Proceedings of International Conference on Mobile Computing & Ubiquitous NETWORKING (pp.62-67). ICMU, Singapore, Jan 6-8.

[9] Quigley, A., Ward, B., Ottrey, C., Cutting, D., & Kummerfeld, R. (2004). BlueStar, a privacy centric location aware system. In Proceedings of Position Location and Navigation Symposium (pp.684-689). PLANS, Monterey, California, Apr 26-29.

[10] Raghunath, M. T., & Narayanaswami, C. (2007). A practical approach to location privacy in public wifi networks. Ibm Corporation.

[11] Schilit, B., Hong, J., & Gruteser, M. (2003). Wireless location privacy protection. Computer, 36(12), 135-137.

[12] Titkov, L., & Poslad, S. (2003). Privacy conscious brokering in personalised location-aware applications. In Proceedings of International Joint Conference on Autonomous Agents & Multiagent Systems (pp.1138-1139), AAMAS, Melbourne, Victoria, Australia, July 14-18.
[13] Yang, D., Fang, X., & Xue, G. (2013). Truthful incentive mechanisms for k-anonymity location privacy. In Proceedings of IEEE INFOCOM (Vol.12, pp.2994-3002). IEEE, Turin, Italy, Apr 14-19.
[14] Zeng, S., Mu, Y., He, M., & Chen, Y. (2018). New approach for privacy-aware location-based service communications. Wireless Personal Communications, 101(2), 1057-1073.
[15] Zeng, S., Mu, Y., Yang, G., & He, M. (2017). Deniable Ring Authentication Based on Projective Hash Functions. In Proceedings of International Conference on Provable Security 2017, (Vol. 10592, pp.127-143). ProvSec, Xi'an, China, Oct 23-25.