A Privacy-preserving and Cross-domain Group Authentication Scheme for Vehicular in LTE-A Networks

Cheng Xu[1], Xiaohong Huang[1], Maode Ma[2], and Hong Bao[3]
[1] Institute of Network Technology，Beijing University of Posts and Telecommunications, Beijing and 100876, China
[2]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore
[3] Beijing Key Laboratory of Information Service Engineering, Beijing and 100101, China
Email: xc-f4@163.com

Abstract —In order to improve road traffic safety, reduce congestion, improving driving experience, intelligent transportation systems and vehicular networking concepts arises at the historic moment. In vehicle larger density scene, can’t guarantee safe reliable and information transmission timely, sometimes can also cause problems such as the broadcast storm. Represented by LTE-A evolution of new generation of mobile communication network rapid development. It performance optimization in the system capacity, the peak rate, transmission delay and other key. In this paper, we proposed a privacy-preserving and cross-domain group authentication scheme. It can effectively solve the security problems. Theoretical analysis and simulation results are shown that compared with other authentication protocol, our scheme has more security properties and better performance.

Index Terms—LTE-A, vehicular network, cross-domain, group authentication, key agreement

I. Introduction

Vehicle Ad hoc Networks (VANET) is the important basis of intelligent transportation services, as well as the most critical vehicular networking technology.

At present, the main countries and regions in the world based on IEEE802.11p technology have establishment Dedicated Short Range Communications (DSRC) technical standard. It has formed the US IEEE/ASTM, European CEN/TC278, Japan IOS/TC204 standardization system and China LET-V standard of technology path. The LTE wireless services have found new application space. As the extension of the LTE to new services, 3 rd Generation Partnership Project (3GPP) has been providing vehicular communication enhancements, including vehicle to vehicle (V2V), vehicle to pedestrian (V2P) and vehicle to infrastructure (V2I) communications. And based on the 802.11 wireless LAN standards of 802.11p, the evolution of the future path is not clear. In the next period of time restricts the development of V2X.

The evolution of LTE-V is based on the LTE technology, it optimized in time delay, reliability, etc. LTE-V is in line with the vehicular networking application scenario for the demand, it can be seen as LTE-Advanced. Obviously, 5G is the evolution of its future direction. Relative to the 4G and LTE, it has reliability improved, such as multiple access, super dense network and full spectrum access [1].

Technology evolution path is very clear, therefore, how to solve a large number of vehicle terminal high frequency caused by the access to the mobile network at the same time the content of the resources and capacity problems becomes urgent. With the development of LTE-A technology and wireless communication capabilities, greatly improve the support vehicular networking technology in the process of communication related bottlenecks and deficiencies will be improved and solved.

Due to hundreds of vehicle devices in the VANET access and management, the huge amounts of data and information, a large number of heterogeneous networks. The application of many complex business and user group of the existence, these demands and vehicles make network security is facing more serious challenges. Thus, a heterogeneous network security communication and real-time and efficient cross-realm authentication information sharing at the same time are the key and difficult problem to solve. One of the most important is the transmission data effectively protect users' private information [2].

There are also some research works on group authentication and key agreement protocol in LTE-A networks. A series of authentication scheme in [3] based on privacy protection, these solutions are used to handle traffic information sharing problems in VANET, and they all adopt direct information interaction on V2V to communicate. This way not only caused by repeated authentication information, and vulnerable to denial of service attacks and other problems. In order to solve this problem, use such as Group Signature (GS) and identity-based Signature (IS) method in [4] to construct privacy protection and certification scheme. Group signature method which make use of the sender's private key to anonymous signature of the message, the receiver is using the group public key to verify the message.

The earlier schemes in [4], [5] that are unlikely to provide user anonymity due to inherent design flaws are also susceptible to playback and simulated attacks. They

Manuscript received June 25, 2017; revised November 16, 2017.
This work was supported by the National Natural Science Foundation of China (Grant No.91420202 and No.61602055).
Corresponding author: xc-f4@163.com
doi:10.12720/jcm.12.11.604-610

then built a powerful user authentication scheme for a wireless smart card. However, a group-based security protocol for machine-type communications in [6] show that the scheme lacks user friendliness and cannot provide user anonymity and unfairness in key agreement. Reanalyzed the authentication scheme in [7], it point out that their scheme also fails to achieve user anonymity and perfect forward secrecy, and discloses a legitimate user's password. They then proposed an enhanced anonymous authentication scheme for a roaming service in global mobile networks. A pseudo random and group signature scheme in [8] with the combination. The scheme assigned each vehicle is a group signature private key, it load to reduce the message authentication, but there is still a huge problem in the verification certificate revocation list of group signature. A data fusion method in [9] can improve the efficiency of traffic information sharing problems in VANET, but for security issues such as privacy, it is still a lack of proper solutions.

Above all scheme is initiated by the vehicle itself and to self-validation of traffic information. These solutions directly or indirectly using the digital signature technology when the message signature and authentication. Thus, the solution there are some defects as follows: (1) In the face of very large scale of VANET applications, there is not enough effective solution to such a large number of message authentication. (2) Repeat send and validation of a large number of traffic information, network communication under the heavy load, the efficiency is not high. Through careful review and analysis, we find that earlier schemes are vulnerable to impersonation and insider attacks, and cannot provide user friendliness, and proper mutual authentication, and, in addition, lack backward security and local verification [10]. To remedy these weaknesses, we propose a privacy-preserving and cross-domain group authentication scheme in LTE-A network based on the elliptic curve public key cryptography algorithm.

We have designed a privacy-preserving and cross-domain group authentication protocol that implements safe and efficient for vehicular in LTE-A network. The outstanding features of the scheme are the following: (1) Simplification of the generation of session keys in a LTE-A system; use of elliptic curve cryptography realizes safe and efficient cross-domain group authentication. (2) For LTE-A vehicular networks, the proposed scheme conforms to the demand for basic security and can protect privacy. (3) Efficient reduction of the computational and communication costs. Compared to other related schemes, the proposed scheme has relatively good performance and can be applied to vehicular networks.

In Sec. 1 of this paper, we discuss privacy-preserving and cross-domain group authentication protocol security and efficiency requirements. We review earlier proposals, discuss their security vulnerabilities, and how to overcome their efficiency problems. In Sec. 2, we provide network architecture and goals to support our security analysis. In Sec. 3, we provide a detailed description of the proposed scheme in LTE-A network. In Sec. 4, we analyze the security of the scheme. In Sec. 5, we compare the performance of the scheme to other related schemes. We present our conclusions in Sec. 6.

II. Network Architecture

A. Network Model

As shown in Fig. 1 is based on the LTE-A network model of vehicle ad-hoc network mainly contain three entities: the on-board unit (OBU), road side unit (RSU) and Trusted Authority (TA).

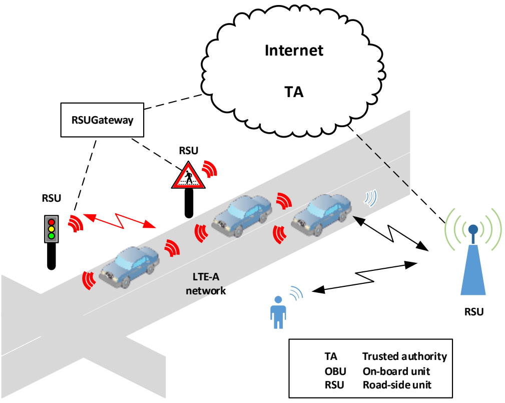


Fig. 1. Based on the LTE-A vehicle ad-hoc network model.

On-board unit: in vehicle ad-hoc network, each vehicle is equipped with OBU used for sending traffic information, storage and handling basic operation and basic algorithm of cryptography. OBU and RSU based on LTE-A network communication, vehicle by using the OBU can be generated for every 100-300ms a traffic information data, and put the data sent to adjacent vehicle and RSU.

Road side unit: RSU is a kind of infrastructure that is set on the side of the road. It can be with TA and OBU within the scope of the communication allows direct communication. However, RSU not fully trusted entities, it is easy attack by the attacker. RSU has a strong ability of communication, it can transmission data for vehicle within 3km. All of the RSU can form a huge network, to cover all of the feasible region. At the same time, the RSU has a strong computing power and storage space, it can be used for information collection and dissemination of traffic jams.

Trusted authority: TA is fully trusted entities, have very strong computing power and storage space. It is mainly responsible for RSU and all vehicle registration work. Besides, TA can verify the RSU and OBU information, and transmission congestion information, etc.

B. Attack Model

In the safety analysis, it was assumed that the attacker can control the LTE-A network of communication channel, monitoring and interrupt the transmission of data, discarding the transmission of packets and replace the original data [11]. In addition, the attacker can also be compromised or capture a small part of the vehicle OBU in group. For the captured vehicle, the attacker can collection data and analyze it.

The attacker's purpose is to make a legal and imperceptible case to captured OBU group. It make vehicle receiving the wrong and harmful information. Common attack model include: the tampering of location information, communication interference, cheat near traffic, node identity attack, forgery and spreading false information, and spy out legitimate user privacy, etc.

C. Security Requirements and Goals

Security for VANET system has very important meaning to stable and efficient operation. Based on LTE-A network model and the attack model analysis, we can clear that VANET for intelligent transportation services, at the same time, more susceptible to kinds of attacks by attacker. The attacker to get more conducive to their own traffic in network resources. So as to use illegal means to interfere with the normal traffic. Some malicious attacks by the attacker will be launched the initiative, its purpose lies in the destruction of normal running of VANET. Therefore, we propose a protocol scheme needs to meet all security requirements are:

- Message authentication and integrity requirements.

In the VANET system, all the Message of the transmission should be certified. The correctness of the information transmission and source in is crucial for certification. It is ensure that the message is indeed, made by a legal entity and has not been changed. If the received message were modified, the receiver should be able to detect.

- The node authentication requirements.

Scheme should guarantee nodes (including the OBU and RSU) can conduct mutual authentication. It should be efficiently and avoid possible performance bottlenecks. Also can be resist attacks, avoid attackers forge or tamper with the identity information to attacks the system.

- Privacy protection.

Vehicles in VANET has corresponding relationship with nodes directly. The vehicle's identity needs to be protected. So that the attacker can't get any real information regarding the status of vehicles. And the session can’t be traced, communication between the vehicle and the vehicle should be anonymous. Only credible institutions and RSU can get real identity of the vehicle.

- Audit requirements.

For the vehicle, the mutual communication is anonymous and unlinkability, but TA have the right to verify the original information. The TA could ensure the vehicle on its own information non-repudiation. When the information is in a state of controversy, TA can audit vehicle nodes send important information.

Our goal is to design a cross-domain authentication key agreement scheme, group can not only verify the integrity of the vehicle passing messages, but also can resist denial of service attack. The identity information of the vehicle can be more privacy. In addition, the scheme has unlinkability and traceability. It can achieve cross-domain vehicular networking information sharing and mutual authentication.

III. The Proposed Scheme

We propose a group of cross-domain authentication key agreement protocol can be divided into: system initialization, group authentication phase, OBU and RSU key agreement phase. The overall structure of the scheme as follows.

A. System Initialization

In this phase, the trusted institutions through the system parameters to create a master key. In order to get the corresponding key secret identity, RSU and OBU must use its identity on the TA for registration.

Assume that all the OBU and RSU support LTE-A. Each vehicle OBU have an identity ID_{Vi}, it is installed in the vehicle directly by the supplier, used as a registered LTE-A network of a unique identifier. Based on the LTE-A group of cross-domain authentication key agreement involving symbolic description as shown in Table I.

Table I: Definition of Notations in the Scheme

Notation	Definition
TA	Trusted authority
RSU_i	Number i of roadside units
V_i	Number i of vehicle group
G	Additive cyclic group
V	Multiplication cyclic group
ID_{Vi}	The real identity of the vehicle Vi
ID_{Ri}	The real identity of the RSU_i
ID_{TA}	The real identity of the TA
PID	Fake identity

Initialization of TA:

G is rank for q addition cyclic group, in which P is the generation of the cyclic group, let $e:G\times G\rightarrow V$ bilinear mapping satisfy the following conditions.

Bilinear as in (1) and (2).

$$e(x_1+x_2,y)=e(x_1,y)e(x_2,y) \quad (1)$$

$$e(x,y_1+y_2)=e(x,y_1)e(x,y_2) \quad (2)$$

Non-degeneracy as in (3) exist $x\in G$, $y\in G$.

$$\forall x, y, e(x, y)\neq 1 \quad (3)$$

TA through the system parameters to generate the master key:

TA random integer $\alpha \in Z_q^*$ as system master key, and calculate $\beta=\alpha P$ as a public key system.

TA use the identity and master key private key to calculate its identity $s_{TA}=\alpha H（ID_{TA}）$ by hash function.

Message $\{\beta, ID_{TA}\}$ can openly, while message $\{\alpha, s_{TA}\}$ must be kept confidential.

OBU and RSU in TA through the following ways to register:

For vehicle V_i, it put its true identity ID_{Vi} and vehicle information to TA together. TA calculate V_i private key as in (4), and pass it to V_i.

$$s_{TA}=\alpha\ H(ID_{Vi}) \tag{4}$$

RSU sends its true identity and information to TA. And TA as in (5) obtained the identity of the private key, and pass the private key to Vi

$$s_{Ri}=A\ h(ID_{Ri}) \tag{5}$$

TA save the OBU and RSU sends information and the corresponding private key.

B. Group Authentication Phase

According to the first group of each member in the communication ability, storage capacity and the battery status information. When a group of OBU try to access networks at the same time, it needs elected a leader of the group to lead representatives and all other members for mutual authentication with RSU. Confirm its identity on both sides, by a group of each OBU to generate a session key. It is ensure that the OBU and RSU of communication security.

Step 1: Select an OBU behalf of all members in the group and ti communication with the RSU. It will be the device named as leader.

Step 2: Leader received from each member's EID and MAC. Verification for MAC, after validation through computing group of MAC, sent to the RSU.

Step 3: RSU and TA to transmit data to prove the validity of the MAC, then generate a shared secret, feedback to the RSU.

Step 4: RSU generation key feedback to the leader and the group OBU.

When need with other LTE-A vehicular networking communication, every private networks randomly selected from an OBU in an area as representatives for information sharing with other special networking. Each RSU if want to information sharing, must validation and signature by each private network within the TA. It has been made to broadcast message by TA. This way protect the confidentiality and integrity of data, and can be synchronized, efficiency is higher. In the end, each RSU collects information for networking, then summarize and verify. It is achieve the various special networking of information sharing and real-time communication.

C. OBU and RSU key Agreement Phase

In our proposed scheme, each RSU to undertake communication within the scope of the traffic information collection and detection work. Once the vehicle into a RSU can communication range. In order to maximize the protection of the privacy information of the vehicle. It is the important to key agreement with the RSU. Used the private key and forge the vehicle status information. The process of key exchange protocol as follows:

Step 1: The first vehicle V_1 select a random number $r_1 \in Z_q^*$, with TA identity information for their own identity. And joining random number r_1 to encrypt as in (6). At the same time with the private key the s_{Vi} of the identity of V_i, calculation signature as in (7). Then , V_i send message $\{c_1, \sigma_1\}$ to road side unit R_x.

$$c_1=IBEnc_{IDTA}(r_1||ID_{Vi}) \tag{6}$$

$$\sigma_1=Signs_{Vi}(r_1) \tag{7}$$

Step 2: When received messages $\{c_1, \sigma_1\}$, roadside unit R_x select a random number $r_1 \in Z_q^*$, calculate signature as in (8). Then send the message $\{r_2, ID_{Rx}, \sigma_1, c_1, \sigma_2\}$ to TA.

$$\sigma_2=Signs_{Vi}(r_2) \tag{8}$$

Step 3: TA decrypting C_1 restore message $\{r_1, ID_{Vi}\}$. then through the Verify ID_{Vi} (c_1, σ_1) and Verify ID_{Rx} (c_2, σ_3) to verify the signature is valid. If the signature of the two validation is effective, means that the demand is legal by vehicles and roadside units.

Therefore, TA with its own private key splicing the message of the $r_1||ID_{Rx}$, and computing signature as in (9). Then send a new signature σ_3 to roadside unit Rx

$$\sigma_3=Signs_{TA}(r_1||ID_{Rx}) \tag{9}$$

Step 4: Once received signature σ_3, the R_x send identity information ID_{Rx} and signature to vehicle V_i.

Step 5: When messages are received, V_i verify whether σ_3 is valid signature. If it is effective, this entity authentication process is complete. Then, V_i select a random number $a \in Z_q^*$. Use R_x and the identity of the private key as the secret key computing as in (10), then forwarding message c_2 to R_x.

$$c_2=IBEnc_{IDRx}(aP||ID_{Vi}) \tag{10}$$

Step 6: R_x decryption c_2 and use $IBEnc_{IDRx}$ (c2) to decrypt the $aP||ID_{Vi}$. If verification through, then select a random number $b \in Z_q^*$, computing signature as in (11). then sends the message $\{bP, \sigma_3\}$ to V_i.

$$\sigma_3=Signs_{Rx}(aP||bP) \tag{11}$$

Step 7: V_i verify $ID_{Rx}(aP||bP, \sigma_3)$ to verify the signature is valid. Pass the verification, using its private key s_{Vi} calculation aP||bP's status message signature as in (12). Then send to roadside unit R_x.

$$\sigma_3=Sign_{sVi}(aP||bP) \tag{12}$$

Step 8: Roadside unit R_x validate signatures Verify ID_{Vi} $(aP||bP, \sigma_4)$ is valid. If the signature verification is effective, the V_i and R_x private key is as in (13). After that, the R_x calculate forged identity PID_1, PID_2,...PID_n, and the ciphertext c3 as in (14) sent to the V_i.

$$s = abP \tag{13}$$

$$c_3=EncabP(PID1||PID2||\cdots\cdots||PIDn) \tag{14}$$

Step 9: According to the *s* is produced by V_i and R_x, therefore, V_i can decrypt the c_3, and restore the PID_1, PID_2,..., PID_n. And fake identity as traffic information anonymous report by vehicles V_i.

At this point, the key agreement process is complete. Roadside unit and vehicle can negotiate the session key and secret communication.

IV. Safety Analysis

According to the definition of security requirements, mainly in the safety of the section with the two classic scheme ABAKA [6] and LGTH [8], this section compares and analyzes the results are shown in Table II.

TABLE II: PERFORMANCE COMPARISON OF DIFFERENT SCHEME

	ABAKA[10]	LGTH[4]	Our scheme
Certification	YES	YES	YES
Resist attacks	NO	YES	YES
Privacy protection	YES	YES	YES
Unlinkability	NO	YES	YES
Traceability	NO	NO	YES

- Certification

Message authentication codes used in information collection stage. As the message authentication code is based on one-way function to operation. If without knowing the private key, it is difficult to forge valid message authentication code. According to the difficult CDH assumption, under the condition of without knowing the private key entities, it is hard to forge the signature of the effective. Therefore, certification can be ensure the vehicle receives the message is sent by a legal entity. And ensure that in the process of message transmission without tampered.

- Resist attacks

After completion of the OBU and RSU key agreement. Roadside units in charge of traffic information collection, vehicles are no longer alone to collect traffic information. As a result, the computational cost and storage cost will be moved. They would move from the vehicle to the roadside unit with stronger storage and computing ability.

- Privacy protection

Once the communication range of vehicles into a roadside units, trying to conduct key agreement. In the process of negotiation, the vehicle's identity can only be credible institutions authorized legal RSU of TA. As a result, the vehicle don't know other information such as the identity of another vehicle. Therefore, even if the attacker monitoring under the network environment, as to the identity of the vehicle privacy information can still get good protection.

- Unlinkability

Each vehicular in communication the identity of the traffic information are randomly. It selected from the collection of identity forged identity, and forged identity use the limited time. This will cause the attacker to multiple messages are associated with a specific vehicle. Because each vehicular traffic information is released by using negotiated key encrypted before, the attacker can't from the encrypted information transmission process for any positive information. It help them establish a contact between the vehicle and information.

- Traceability

Only TA and legal authorization of RSU can take the identity information of the vehicle. In order to get a message with the relationship between the real sender information, the credible agency can ask roadside units. Traceability can not only help trace message sender real credible institutions, at the same time help trusted institutions detect malicious vehicles.

V. Performance Analysis

To evaluate our scheme, we adopt a named Tate pairing method. Let G indicate cyclic group, its rank is q. the rank order of units is 160. The scheme using decryption algorithm is AES-128, message authentication codes algorithm is HMAC, hash algorithm is H(•). T_{mul} means calculation point multiplication operation time. T_{par} means performs a matching operation time. T_h means hash operation performed time. T_{mac} means performs a message authentication code computing time. T_{enc} means executed an encryption operation time. T_{dec} means performs a decryption operation time. T_{mul} T_{par}, T_h, T_{mac}, T_{enc}, T_{dec} etc. are the main part of the solution in computing performance. Therefore, we only compute send or collection operation of traffic information. And compute traffic information dissemination and validation in evaluate operation.

The experiment hardware equipped with Intel Core 2 Duo (TM) CPU@2.4GHz processor. After 100 times in operation of the experiment, to obtain the average of these operations, T_{mul} T_{par}, T_h, T_{mac}, T_{enc}, T_{dec} operations such as the average length of 5.5ms and 41.1ms, 8us, 19.3us, 18.5us, 43.6us. All of the following simulation operations are conducted on the basis of the results.

TABLE III: PERFORMANCE COMPARISON OF DIFFERENT SCHEME

	ABAKA[10]	LGTH[4]	Our scheme
Message sent	T_{mac}+T_{mul}	T_{mac}	T_{mac}+T_{enc}
Message transmission	2T_{mac}+2T_{mul}	T_{mac}+T_h	T_{mac}+T_{dec}

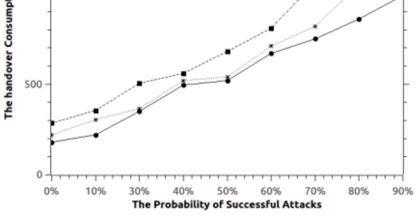


Fig. 2. The handover consumption compare.

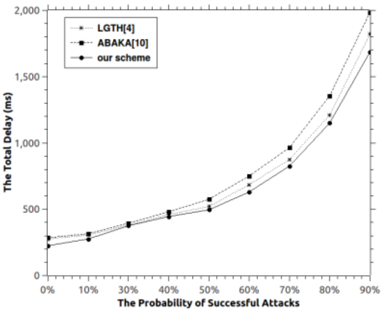


Fig. 3. The total delay compare.

It is clear that from Fig. 2 and Fig. 3. The handover consumption and total delay compare indicate that our scheme is has more security properties and better performance. Under a 50% probability of successful attacks, the proposed scheme's time consumption is obviously less than that for ABAKA [10] and LGTH [4].

VI. Conclusions

We proposed a privacy and efficient communication protocol scheme, constructed to implement the cross-domain authentication communication between heterogeneous vehicular networking complex authentication scheme, theoretical analysis and simulation results show that compared with other authentication protocol, put forward the agreement to meet more security properties, has better performance.

Acknowledgment

This work has been supported by the Major Research Plan of the National Natural Science Foundation of China (Grant No. 91420202) and National Natural Science Foundation of China (Grant No.61602055).

References

[1] J. Cao, H. Li, and M. Ma, "GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks," in *Proc. IEEE International Conference on Communications*, 2015.

[2] B. T. Sharef, R. A. Alsaqour, and M. Ismail, "Vehicular communication ad hoc routing protocols: A survey," *Journal of Network & Computer Applications*, vol. 40, pp. 363-396, 2014.

[3] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *Communications Surveys & Tutorials IEEE*, vol. 16, pp. 283-302, 2014.

[4] Lai, H. Li, R. Lu, and R. Jiang, "LGTH: A lightweight group authentication protocol for machine-type communication in LTE networks," in *Proc. GLOBECOM 2013 - 2013 IEEE Global Communications Conference*, 2013, pp. 832-837.

[5] J. Cao, M. Ma, and H. Li, "GBAAM: group‐based access authentication for MTC in LTE networks," *Security & Communication Networks*, 2015.

[6] Choi, H. K. Choi, and S. Y. Lee, "A group-based security protocol for machine-type communications in LTE-advanced," *Wireless Networks*, vol. 21, pp. 405-419, 2015.

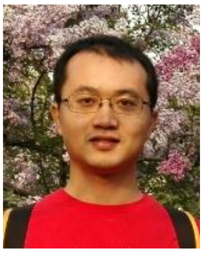
[7] Lai, H. Li, R. Lu, and X. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Computer Networks*, vol. 57, pp. 3492-3510, 2013.

[8] T. M. Lin, C. H. Lee, J. P. Cheng, and W. T. Chen, "PRADA: Prioritized random access with dynamic access barring for MTC in 3GPP LTE-A networks," *IEEE Transactions on Vehicular Technology*, vol. 63, pp. 2467-2472, 2014.

[9] R. Jiang, C. Lai, J. Luo, X. Wang, and H. Wang, "EAP-Based group authentication and key agreement protocol for machine-type communications," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[10] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 60, pp. 248-262, 2011.

[11] A. Fu, N. Qin, Y. Wang, Q. Li, and G. Zhang, "Nframe : A privacy-preserving with non-frameability handover authentication protocol based on (t, n) secret sharing for LTE/LTE-A networks," *Wireless Networks*, 2016, pp. 1-12.



Cheng Xu, is currently a Ph.D. at the State Key Laboratory of networking and switching technology in Beijing University of Posts and Telecommunications (BUPT), China. His research interests include wireless security and internet of vehicle.

Xiaohong Huang, corresponding author, received her Ph.D. degree from School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. She is an Associate Professor in Institute of Network Technology in BUPT. Her current research interests are future Internet architecture, network security.

Maode Ma, received his PhD degree from Hong Kong University of Science and Technology. Dr. Ma is an IET Fellow, a senior member of IEEE Communication Society and IEEE Education Society, and member of ACM. He is the Chair of the IEEE Education Society, Singapore Chapter and chair of ACM, Singapore Chapter, He is also an IEEE Communication Society Distinguished Lecturer.

Hong Bao, received his Ph.D. degree from school of computer and information technology, Beijing Jiao tong University Beijing, China. He is a professor of Beijing Union University. His current research interests include intelligent control and intelligent vehicle.