A Fair Blind Signature Scheme to Revoke Malicious Vehicles in VANETs

Xiaoliang Wang[1, *], Jianming Jiang[1, 2], Shujing Zhao[1] and Liang Bai[1]

Abstract: With the rapid development of IoT (Internet of Things), VANETs (Vehicular Ad-Hoc Networks) have become an attractive ad-hoc network that brings convenience into people's lives. Vehicles can be informed of the position, direction, speed and other real-time information of nearby vehicles to avoid traffic jams and accidents. However, VANET environments could be dangerous in the absence of security protection. Because of the openness and self-organization of VANETs, there are plenty of malicious pathways. To guarantee vehicle security, the research aims to provide an effective VANET security mechanism that can track malicious vehicles as necessary. Therefore, this work focuses on malicious vehicles and proposes an anonymous authentication scheme in VANETs based on the fair blind signature to protect vehicle security.

Keywords: VANETs, fair blind signature, trusted third-party, anonymous authentication.

1 Introduction

The rapid development of wireless communication technology has enabled mobile ad-hoc networks to be widely adopted in the ubiquitous Internet of Things, along with the rise of VANETs (Vehicular Ad-Hoc Networks).

As the infrastructureless and decentralized nature of VANET, it is easy to suffer from various malicious attacks. The smart vehicles can be classified into cooperative or malicious ones with the help of machine learning techniques, such as support vector machine [Wahab, Mourad, Otrok et al. (2016)], extreme learning machine [Xiang, Zhao, Li et al. (2018)], etc. But, privacy-preserving is a challenge and the main threat that VANETs face is also the issue of privacy. The previous research of VANETs mainly focus on authentication [Calandriello, Papadimitratos, Hubaux et al. (2007); Han, Sang and Bae (2017); Lin, Sun, Ho et al. (2007); Oulhaci, Omar, Harzine et al. (2017); Tian and Qiang (2012)] defense against Sybil attacks [Feng, Li, Chen et al. (2017); Hussain and Oh (2014); Wu (2017); Zhang, Liang, Lu et al. (2014)] along with DDoS attack prevention [Biswas, Mišić and Misic (2012); Hamieh, Ben-Otheman and Mokedad (2009); Hussein, Elhajj, Chehab et al. (2017)]. In 2011, hackers successfully invaded a vehicle through Bluetooth and wireless network technology. In July 2013, a company

[1] School of Computer and Communication Engineering, Hunan University of Science and Technology, Xiangtan, 411201, Hunan, China.

[2] School of Computer Science, University of Newcastle, Newcastle, 2308, New South Wales, Australia.

[*] Corresponding Author: Xiaoliang Wang. Email: fengwxl@hnust.edu.cn.

CMC. doi: 10.32604/cmc.2019.04088

engineer successfully caused a vehicle brake failure by controlling its speed and making the engine stop. In March 2014, a security consultant put forward inherent password security vulnerabilities in the 2014 Black Hat ASIA conference in Singapore, which would lead to the leaking of the personal information of the driver. Additionally, on February 9, 2015, Massachusetts Senator Ed Markey published a report about risks of VANETs, which disclosed although more and more vehicle manufacturers wanted to apply wireless sensor devices and applications in vehicles, they would be unable to prevent hackers from impairing vehicular security [Markey (2015)].

In VANETs, there are two main communication types: V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure). Hartong et al. [Hartong, Goel and Wijesekera (2007)] proposed an algorithm that was based on the geographic location concept [Denning and Macdoran (1996)], which used the vehicle location, the speed and travelling time information as factors to protect the communication of V2I. In 2008, Zhang et al. [Zhang, Lu, Ho et al. (2008)] presented a pseudonym application based on blind signature technology for vehicles between two Remote Sensing Utilities (RSUs), which can prevent infrastructure from peeking into the trails of vehicles, but unable to revoke a malicious vehicle. Feng [Feng (2010)] used Combined Public Key (CPK) and blind signature to propose a pseudonym generation scheme to satisfy security and privacy requirements, which is more efficient in computation and communication cost. Proxy Blind Signature Scheme (PBSS) [Tian and Qiang (2012)] proposed a signature scheme based on blind signature and proxy multi-signature certification technology, which solved authentication problems between the nodes. The use of two signature technologies realized onboard interactivity authentication and improved communication safety. Experimental results show PBSS can meet the on-board node mobility and complexity, as well as the authentication efficiency and offering good performance.

However, these articles do not provide traceability capability for VANETs, especially when a vehicle abuses the blind signature. Essentially, the malicious vehicle can abuse the anonymity of the blind signature to commit an array of fraudulent behaviors. The question is how to constrain abusive behaviors in reality? It was never addressed in the abovementioned articles.

This work proposes a lightweight anonymous authentication scheme, which can be used to track anonymity abuse in VANETs. Comparing with previous anonymous authentication schemes in VANETs, the proposal is the only one that can achieve privacy protection, authentication and traceability.

2 Overview of fair blind signature

Conventional blind signature is that the signers of the document never know what they have signed, which may cause blind abuse. Some malicious users will use the feature of the blind mechanism to cheat the signer to sign unwilling contents. As opposed to blind signature, fair blind signature [Stadler, Piveteau and Camenisch (1995)] adds a trusted third party to avoid this phenomenon because the trusted third party is able to supervise the signing process. Upon finding the signed contents are tampered with, it can track the malicious user in a timely fashion. Compared to blind signature mechanism, the revocable anonymity is brought into the Fair blind signature mechanism, in which the authority can link an issuing session to the resulting signature and track a signature to the user who possesses it.

3 System architecture

Fig. 1 illustrates a communication scenario and mode between the vehicles, Trust Managers (TMs) and RSUs. Communication mode includes communication amongst the vehicles and between vehicles and infrastructures. In this figure, it mainly introduces the communication between the vehicles, infrastructure, TMs and information transmission mode.

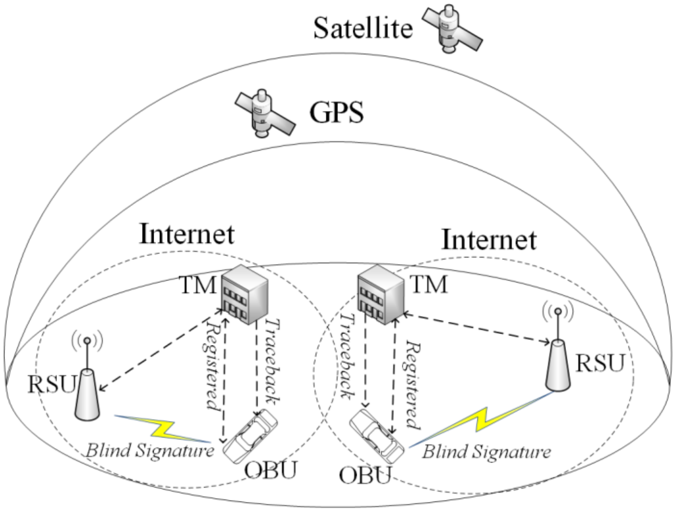


Figure 1: VANET communication model

Fig. 2 shows the communication relationship between vehicles and Trust Manager (TM), along with the RSU in the VANET. In our scheme, before a vehicle engages into daily traffic, it must register at the TM. In this process, firstly the vehicle signs the message using its own identity information, and then sends it to the nearby TM. The process generates the parameters of the signature process, transmission information and the signature algorithm. After the TM receives this information, it will verify whether the information is from the authentic vehicle.

Then the TM uses the same signature algorithm to sign information, and then sends it back to the vehicle. After the vehicle receives the returning information, it will check whether these messages have changed or not. If not, it will send this signature to the RSU, which the vehicle will keep for future use. The RSU then starts its verification if there is the true signature of TM, it will complete the blind signing, and transmit the final signature to the vehicle.

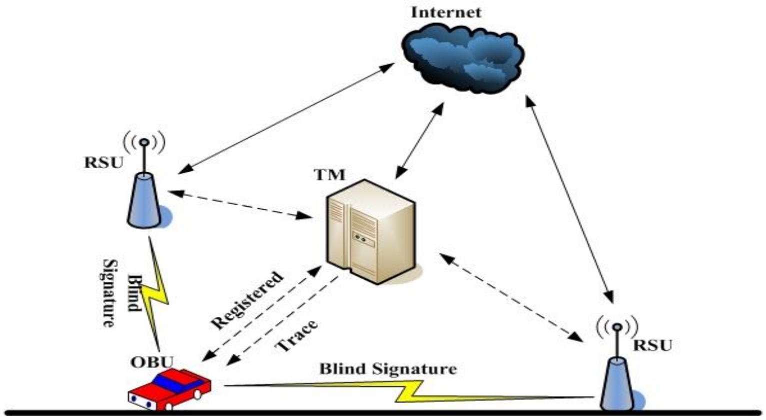


Figure 2: VANET architecture

Tab. 1 describes the meaning of the main symbolic parameters used in the communication process:

Table 1: Parameter table

Notation	Description
p, q	Random large prime number of RSU
e, n	Public key of RSU
d	Private key of RSU
H( )	Secure hash function
m	A message sent by a vehicle
r	Random parameter of OBU
TM	Trust manager
DSA( )	Signing algorithm of TM and OBU

4 Signing model

A transportation management department allocates different symbolic parameters (n, G, g) to every region, which represents local identification information. These parameters are embedded in the OBUs of vehicles. Every vehicle in the region is denoted as Vi, $i \in (1,...,n)$.The public key of vehicles in the region are disclosed during running. As per the above introduction, before vehicles connect with the RSU they must have a registration process, so that they can use signatures from a local TM to represent their identities to connect with the RSU. The registration process includes the two steps:

1. The vehicle will sign its own privacy information and send it to the local TM. Then the TM verifies and registers it. If successful, TM will sign the information and return it to the vehicle;

2. After the vehicle has received the TM's signature, it will check whether the signature is tampered with or not. If the information has not been tampered, the vehicle will use the TMs' signatures as its identity certificate to communicate with RSUs anonymously. In addition, the TM also distributes a different electronic license to each vehicle.

4.1 System initialization phase

Use a set R to denote these RSUs in the region, $Ri, i = \{1,2,...,n\}$

1. Ri randomly selects two large prime numbers p , q to calculate $N = pq$, $\varphi(N) = (p-1)(q-1)$;

2. Ri randomly selects a large integer e , which lets $0 < e < \varphi(N)$ and $\gcd(e, \varphi(N)) = 1$;

3. R uses the Euclidean algorithm to calculate d , which fulfills $ed = 1 \bmod(\varphi(N))$, namely $d \equiv (1/e) \bmod(\varphi(N))$. R stores the public key $PK(N, e)$, private key d as well as the two prime numbers p and q . Besides, R chooses a secure hash function H( ).

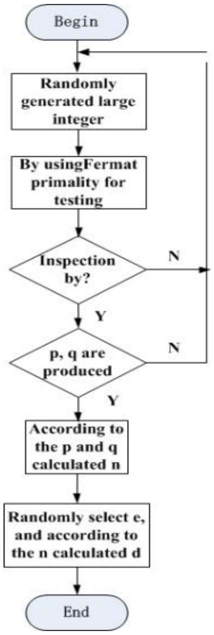

Begin
Randomly generated large integer
By usingFermat primality for testing
Inspection by?
N
Y
p, q are produced
N
Y
According to the p and q calculated n
Randomly select e, and according to the n calculated d
End

Figure 3: Key generation

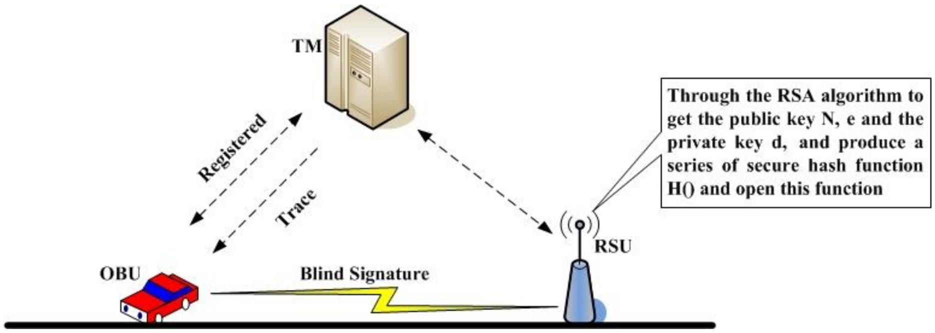

TM
Registered
Trace
OBU
Blind Signature
RSU
Through the RSA algorithm to get the public key N, e and the private key d, and produce a series of secure hash function H() and open this function

Figure 4: Initialization phase

4.2 Registration at TM of vehicles

In this process, the TM gives each vehicle a valid license before driving on-road and storing related information about the vehicle. Then the vehicle will sign its own information and send it to the local TM for registration. Assume the vehicle is denoted as Vi:

1. Vi randomly selects a number r, 1<r<N, and calculates $M = r^e h(m) \bmod N$, where M is the message to be transmitted, then sends the transmitted message M, random number r, electronic license ID and signature algorithm DSA(M) to the TM.

2. After the TM has received the above information, it calculates $M' = r^e h(m) \bmod N$, and then according to the ID provided by Vi, it finds the corresponding user signature algorithm DSA( ) for next verification. If M'=m, the TM records some information of the vehicle, such as r, m and M. Finally, TM adopts the same signature algorithm DSA( ) to sign them, and returns (m, DSA (m)) to the vehicle Vi.

3. After vehicle Vi has received (m, DSA (m)) from TM, it will verify whether its information has been modified or not. If the information has not been tampered with, the vehicle Vi sends (m, DSA (m)) to a certain RSU, which Vi will communicate in future.

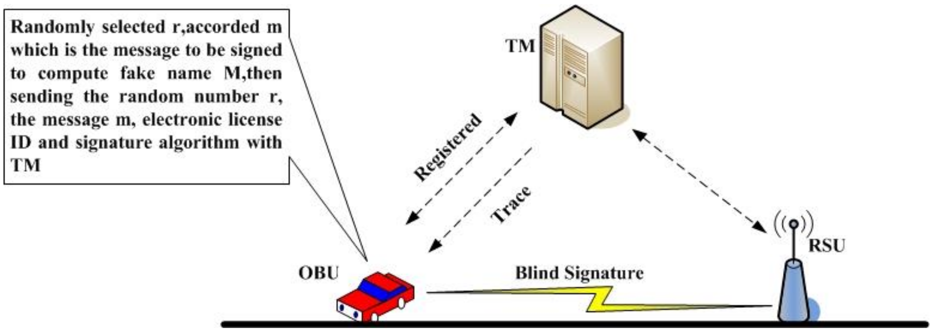
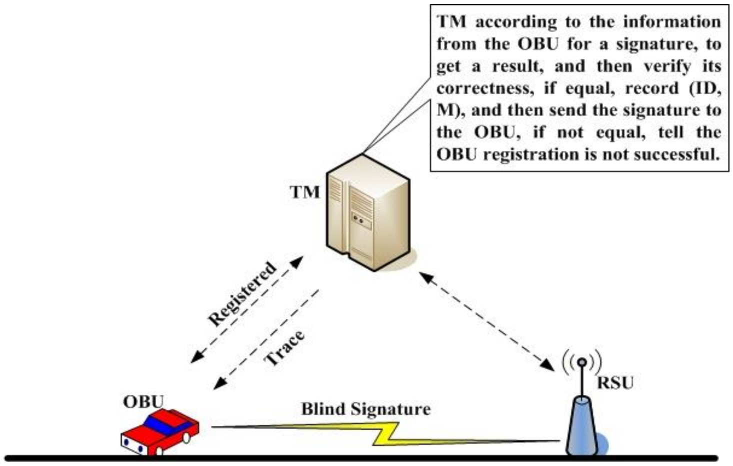
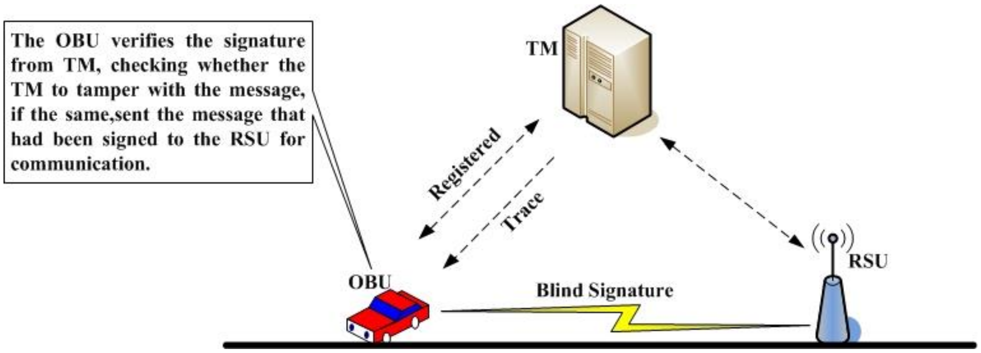

Randomly selected r,accorded m which is the message to be signed to compute fake name M,then sending the random number r, the message m, electronic license ID and signature algorithm with TM
TM
Registered
Trace
OBU
Blind Signature
RSU

Figure 5: Registration Phase



TM according to the information from the OBU for a signature, to get a result, and then verify its correctness, if equal, record (ID, M), and then send the signature to the OBU, if not equal, tell the OBU registration is not successful.

Figure 6: Validation phase



The OBU verifies the signature from TM, checking whether the TM to tamper with the message, if the same,sent the message that had been signed to the RSU for communication.

Figure 7: OBU Validation phase

4.3 Signing

1. When the roadside infrastructure R receives (m, DSA (m)), it will be verified. If successful, R signs it and calculates $S' = M^{d} \bmod N$, then returns the signature to vehicle Vi as well as storing the signature and (m, DSA (m)).

2. After receiving S' from R, the vehicle Vi will calculate $S = S'/r \bmod N$, where S is the signature of the transmitting information signed by R.

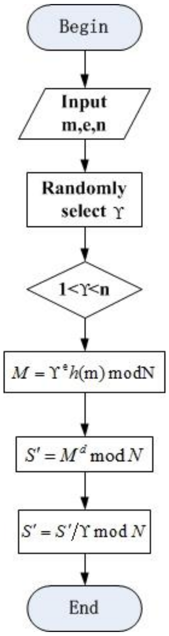
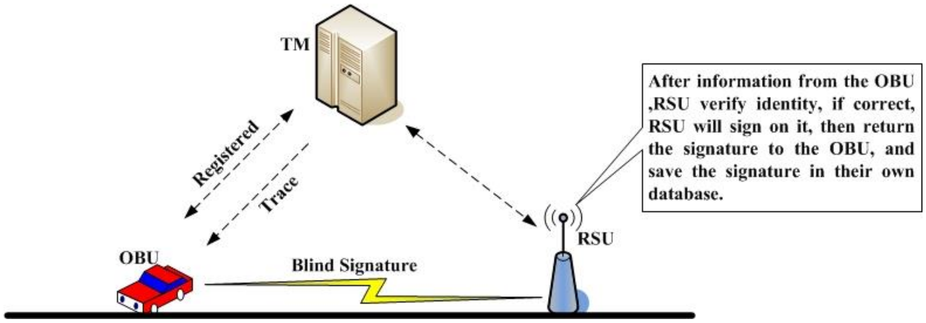

Begin
Input
m,e,n
Randomly select ϒ
1<ϒ<n
$M = \Upsilon^{e} h(\mathrm{m}) \,\mathrm{modN}$
$S' = M^{d} \bmod N$
$S' = S'/\Upsilon \bmod N$
End

Figure 8: Blind signature



After information from the OBU ,RSU verify identity, if correct, RSU will sign on it, then return the signature to the OBU, and save the signature in their own database.

Figure 9: RSU validation phase

4.4 Verification

The verification process begins by processing the blind factor γ to obtain the inverse of γ, then according to the blind factor γ to restore the message S. Next, the public key e is used to verify the signature. Finally, $S^{e} = h(m)$ is calculated to verify whether the information has been tampered or altered by an external party.

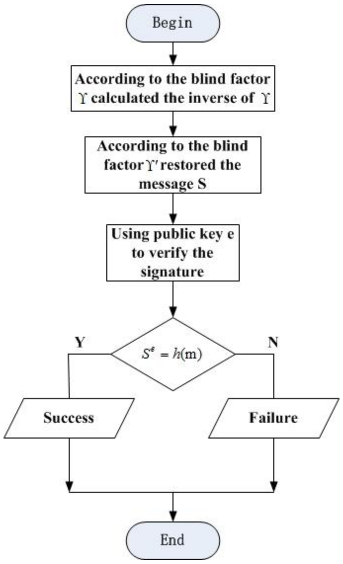
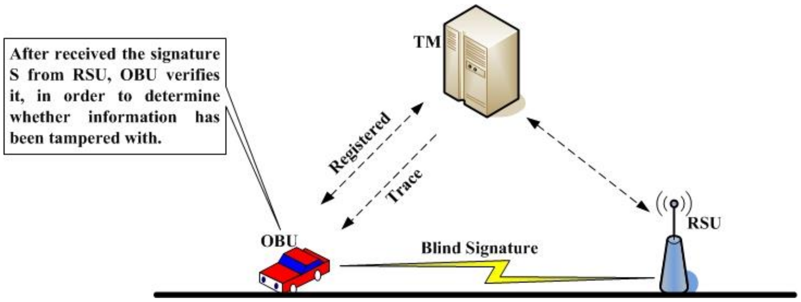

Begin
According to the blind factor Υ calculated the inverse of Υ
According to the blind factor Υ' restored the message S
Using public key e to verify the signature
$S^e = h(m)$
Y
N
Success
Failure
End

Figure 10: Verification process



After received the signature S from RSU, OBU verifies it, in order to determine whether information has been tampered with.

Figure 11: OBU Validation phase

5 Proof and security analysis

1. The vehicle Vi uses the secure hash function to make the message M anonymous. It calculates M and makes the message M blind. Because the message M is blinded, but carries the signature of Vi, this process makes other vehicles unable to impersonate the identity of Vi to cheat the TM. The difficulty of faking Vi is equal to attacking the DSA( ) algorithm.
2. The vehicle manager TM can only register the message M sent by vehicle Vi, but not modify it. Otherwise it will fail to pass the verification of Vi. If the TM wants to modify the message M, it must find a random parameter to meet the verification equation of M, which is equivalent to attacking the RSA algorithm.
3. The information that vehicle Vi sends to the infrastructure R is verified by TM, so it cannot be arbitrarily modified by Vi. The difficulty of vehicle Vi tampering the message is equal to the difficulty of breaking the DSA( ) algorithm.

4. Once the infrastructure R finds the transmitted message is incorrect, it can track the real vehicle with the help of the TM.

6 Analysis of experimental results

In order to verify the validity of the scheme, the simulation experiment was carried out. C++ language is used to develop experiments on a Microsoft Windows 7 system with a 2.6 Ghz Intel Core i5 processor and 4 GB memory. The experimental data set is generated by the algorithm of Thomas Brink [Brinkhoff (2002)] and widely recognized by the mobile data management industry. Oldenburg mobile network (5*5km) is used as the input to generate mobile data sets and communication node objects.

According to the VANET security standard of IEEE 1609.2 [IEEE Standard (2006)], the definition of message format is described in Tab. 2.

Table 2: Message format for vehicle

Parameter	Default Value
MID	2B
MData	100B
TTL	1B
Sign	136B

In Tab. 2, MID is message identifier defining the different message types in the scheme. MData carries valid data for the message including the relevant information of the vehicle, such as vehicle speed, location, direction and so on. TS is timestamp recording the time of message generation to prevent invalid packets and replay attacks. Sign is the blind signature. TTL is the survival time that is used to terminate the transmission of messages to prevent the flooding of messages.

Consider the use of a blind signature in a communication cycle. If all messages are carried with this blind signature, the communication cost is huge. If only the previous single messages have blind signatures and the later messages no longer contain the blind signatures, the success rate of message authentication is low. Therefore, we want to find that how many messages containing this blind signature are suitable. It is assumed that the number of messages in a communication cycle is y and z is the number of messages containing blind signatures. Using the receiving ratio model of data packet provided in the literature [Calandriello, Papadimitratos, Hubaux et al. (2007)], $P_{recv}(d) = -0.04d + 1/7 * \sin(\pi/125 * d) + 1$, where d is message transmission distance and $P_{recv}(d)$ is message receiving rate. The success rate of message authentication is defined as $P_{auth} = 1 - (1 - P_{recv})^z$. Fig. 12 shows the impact of the message transmission distance to the receiving rate. As transmission distance increases, the success rate of messages decreases.

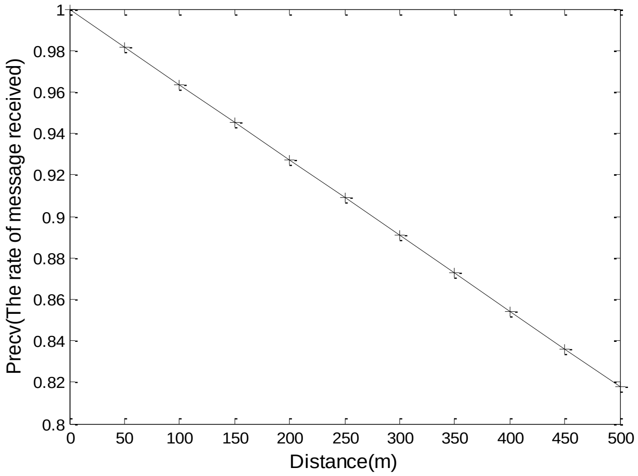


Figure 12: Impact of distance d

Fig. 13 depicts the relationship between the number of messages of a blind signature Z, message transmission distance d and the success receiving rate of messages P_{auth}. With the decrease of distance d , the message receiving rate is improved. When d is fixed, the success receiving rate of messages increases correspondingly with the increase of the number of messages containing a blind signature. It can be seen from the figure that when $P_{recv} \geq 95\% (d \leq 150m), z \geq 4$, the success receiving rate of messages is greater than 90%. Therefore, we take the number of messages contain a blind signature z=4. Under this condition, system is able to meet the verification requirements of most of the vehicle authentications.

Tab. 3 compares our scheme with the PBSS [Tian and Qiang (2012)] in anonymity, authentication and trace-ability. PBSS adopts the distributed proxy blind signature, which can avoid forgery attacks and meet authentication security, but not considering privacy protection and traceback of anonymous abusers.

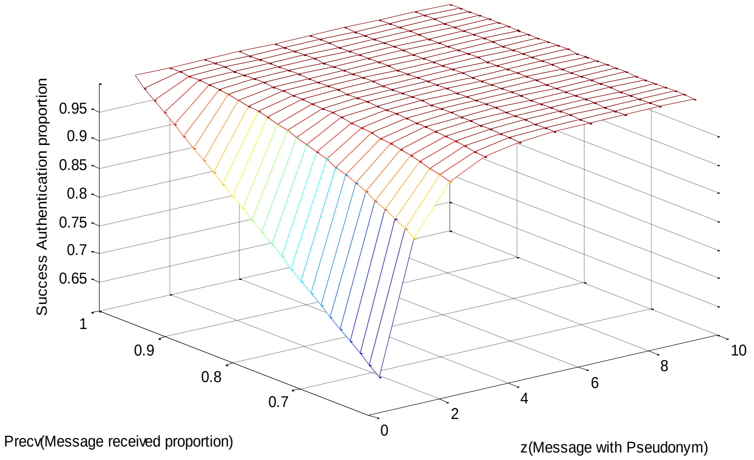


Figure 13: Success authentication for different $P_{recv\cdot z}$

Table 3: Scheme feature comparison

Attributes	PBSS	Our Proposal
Integrity	Yes	Yes
Authentication	Yes	Yes
Anonymity	Yes	Yes
Privacy Protection	No	Yes
Conditional Traceback	No	Yes

7 Conclusions

In this paper, an anonymous authentication scheme based on the fair blind signature is proposed for communication between vehicles and RSU in VANETs, along with the relative merits of the scheme against alternative communication approaches. A simulation experiment was then conducted to assess the merits of the Fair blind signature scheme, which includes an evaluation of the success receiving rate of messages. From the security analysis and experimental results, the proposed scheme is proven to possess anonymity, traceability and authentication functionalities. In the future, it should be an interesting issue to transmit the signature by steganography [Zhang, Qin, Zhang et al. (2018)] because of its excellent imperceptible in human sense system and statistic [Yang, Luo, Lu et al. (2018)].

Acknowledgments: This project is supported by Internet innovation and open platform base of the education Ministry of China (No. KJRP1401), the cooperative education project of the education Ministry of China (No. 201702113002), US-China Computer Science Research Centre of Nanjing University of Information Science and Technology (No. KJR16059), Hunan Natural Science Foundation (No. 2018JJ2138), Education Department of Hunan Province (No. 17B096).

References

Biswas, S.; Mišić, J.; Misic V. (2012): DDoS attack on WAVE-enabled VANET through synchronization. *Global Communications Conference*, pp. 1079-1084.

Brinkhoff, T. (2002): A framework for generating network-based moving objects. *Geoinformatica*, vol. 6, no. 2, pp. 153-180.

Calandriello, G.; Papadimitratos, P.; Hubaux, J.; Lioy, A. (2007): Efficient and robust pseudonymous authentication in VANET. *International Workshop on Vehicular Ad Hoc Networks*, pp. 19-28.

Denning, D. E.; Macdoran, P. F. (1996): Location-based authentication: grounding cyberspace for better security. *Computer Fraud & Security*, vol. 1996, no. 2, pp. 12-16.

Feng, X.; Li, C. Y.; Chen, D. X.; Tang, J. (2017): A method for defensing against multi-source Sybil attacks in VANET. *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 305-314.

Feng, Y. (2010): Efficient anonymous authentication scheme in VANETs. *Computer Engineering & Applications*, vol. 46, no. 23, pp. 126-128.

Hamieh, A.; Ben-Othman, J.; Mokdad L. (2009): Detection of radio interference attacks in VANET. *Global Telecommunications Conference*, pp. 1-5.

Han, M. S.; Sang, J. L.; Bae, W. S. (2017): A secure and efficient V2V authentication method in heavy traffic environment. *Wireless Personal Communications*, vol. 93, no. 1, pp. 245-254.

Hartong, M.; Goel, R.; Wijesekera, D. (2007): Key management requirements for PTC operations. *Vehicular Technology Magazine IEEE*, vol. 2, no. 2, pp. 4-11.

Hussain, R.; Oh, H. (2014): On secure and privacy-aware sybil attack detection in vehicular communications. *Wireless Personal Communications*, vol. 77, no. 4, pp. 2649-2673.

Hussein, A.; Elhajj, I. H.; Chehab, A.; Kayssi, A. (2017): SDN VANETs in 5G: An architecture for resilient security services. *International Conference on Software Defined Systems*, pp. 67-74.

Lin, X.; Sun, X.; Ho, P. H.; Shen, X. (2007): GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442-3456.

Markey, E. J. (2015): Markey report reveals automobile security and privacy vulnerabilities. http://www.markey.senate.gov/news/press-releases/markey-report-reveals-automobile-security-and-privacy-vulnerabilities.

Oulhaci, T.; Omar, M.; Harzine, F.; Harfi, I. (2017): Secure and distributed certification system architecture for safety message authentication in VANET. *Telecommunication Systems*, vol. 64, no. 4, pp. 679-694.

Stadler, M.; Piveteau, J. M.; Camenisch, J. (1995): Fair blind signatures. *International Conference on Theory and Application of Cryptographic Techniques*, pp. 209-219.

IEEE Standard (2006): *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages 1609.2-2006*, pp. 1-116.

Tian, X.; Qiang, S. (2012): Research of an authentication scheme based on the proxy blind signature scheme for the vehicular Ad-hoc networks. *Bulletin of Science and Technology*, vol. 2012, pp. 10-16.

Wahab, O. A.; Mourad, A.; Otrok, H.; Bentahar, J. (2016): CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks. *Expert Systems with Applications*, vol. 50, pp. 40-54.

Wu, W. C. (2017): A secret push messaging service in VANET clouds. *Journal of Supercomputing*, vol. 73, no. 7, pp. 3085-3097.

Xiang, L.; Zhao, G.; Li, Q.; Hao, W.; Li, F. (2018): TUMK-ELM: a fast unsupervised heterogeneous data learning approach. *IEEE Access*, vol. 6, pp. 35305-35315.

Yang, C.; Luo, X.; Lu, J.; Liu, F. (2018): Extracting hidden messages of MLSB steganography based on optimal stego subset. *Science China Information Sciences*, vol. 2018, pp. 1-4.

Zhang, C.; Lu, R.; Ho, P. H.; Chen, A. (2008): A location privacy preserving authentication scheme in vehicular networks. *IEEE Wireless Communications and NETWORKING Conference*, pp. 2543-2548.

Zhang, K.; Liang, X.; Lu, R.; Shen, X. (2014): Sybil attacks and their defenses in the Internet of Things. *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372-383.

Zhang, Y.; Qin, C.; Zhang, W.; Liu, F.; Luo, X. (2018): On the fault-tolerant performance for a class of robust image steganography. *Signal Processing*, vol. 146, pp. 99-111.