An Electronic Payment Scheme based on Blockchain for VANETs

Xinyang Deng[1], Bing Guan[2], Tianhan Gao[1*]
[1]Northeastern university, Shenyang, China
xinyang1121@sina.com, gaoth@mail.neu.edu.cn
[2]Liaoning Information Security and Software Testing and Certification Center, Shenyang, China
17400957@qq.com

Abstract

As an important part of intelligent transportation system, VANETs can provide a variety of services for driving vehicles, where the payment is the most important one. However, most schemes focus on the services provided by VANETs and seldom involve payment, which makes it difficult for service providers to provide long-term and stable services. In this paper, taking the parking toll management system as a scenario, an electronic payment system based on blockchain is designed. Due to the tamper-resistant and non-repudiation of the blockchain, the proposed scheme can guarantee the interests of service providers and consumers. Through security analysis, the proposed scheme owns high security.

Keywords: VANETs, blockchain, electronic payment

1 Introduction

With the development of automotive industry and wireless network, vehicular ad-hoc networks (VANETs) show great potential in intelligent transportation system (ITS) for vehicle to provide network and communication services. In VANETs, vehicles on the road can communicate with each other (vehicle to vehicle, V2V) through opportunistic wireless links. In V2V communication, safety and entertainment messages are usually exchanged to obtain diverse application services like traffic safety and infotainment[4]. Meanwhile, vehicle-to-infrastructure (V2I) communication between vehicle and infrastructure like roadside unit (RSU) is also considered as an important part, which can provide more accurate application services for vehicles in VANETs.

Generally, the applications depending on VANETs can be divided into safety-related applications, efficiency-related applications, and entertainment-related applications[14]. Since great business opportunities are emerging, it is expected that more and more research attentions will be attracted in this area. However, when drivers and passengers enjoy the services by these applications, the necessary costs (such as human cost, infrastructure construction cost etc.) will be generated. Consequently, it is necessary to build an efficient payment scheme that satisfies the additional requirements associated with VANETs.

Now, the electronic payment is thought as an important part of the services provided by VANETs. Zhu et al.[16] proposes an anonymous smart-parking and payment(ASAP) scheme, in which privacy parking spots messages are provided and processed by drivers and server respectively. Blind signature is utilized to guarantee anonymous payment. Whereas high computation cost is done during authentication and payment, which causes inefficiency. Isaac et al.[12] proposes a payment scheme for VANETs based on symmetric cryptography, which allows client to send messages to issuer through merchant. During

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 5, Article No. 10 (November 30, 2019)
*Corresponding author: Tianhan Gao, Software College, Northeastern University, 195 Chuangxin Road, Hunnan District, Shenyang, Liaoning, 110169, China, Tel:+86-24-83678115, email: gaoth@mail.neu.edu.cn

payment process, the scheme can guarantee low computation cost and improves efficiency. Li et al. [7] proposes a self-certified key agreement based on payment scheme, in the scheme, the shared key is generated by two participants without additional message exchanges, and therefore, the computation cost is reduced. However, in the above schemes, each transaction between RSU and vehicle has to be handled by the payment server, which causes enormous communication and maintenance pressures for the payment server. Besides, how to store and maintain all transaction information is not negligible either.

Recently, blockchain is considered as a distributed ledger to participate and record transactions. Through blockchain, users can interact with each other without a trusted third party and all public ledgers are maintained by the participants. Consequently, central managers are removed. In addition, the use of cryptography algorithms and consensus mechanisms guarantees the stability and security of the application.

Generally, the transaction between vehicle and RSU is the main scenario for payment in VANETs. This paper takes the parking toll management system as a scenario to introduce an efficient electronic payment system. We combine blockchain to make the following contributions: (1) Smart contract is used to satisfy the scenarios of transactions between service providers and consumers. (2) In each transaction, the communication with the third party is removed, which reduces communication and computing pressure on third-party entity. (3)The scheme can effectively guarantee the non-tampering and non-repudiation of all transactions.

The remainder of this paper is organized as follows. In section 2, VANETs, DSRC, and blockchain are introduced. Section 3 elaborates the proposed scheme. In section 4, the security analysis of the core protocols are given. Finally, we draw the conclusion and introduce the future work in section 5.

2 Preliminaries

2.1 VANETs

VANETs, as a particular type of mobile ad-hoc networks (MANETs), are considered as a new application of wireless communication technology in the field of vehicle control. Generally, VANETs are also called V2X (Vehicle to Everything), which mainly includes V2V and V2I [15]. As shown in Figure 1, In V2V communication, vehicles must work together to guarantee the dissemination of V2V service notification in time, such as congested road notification, post crash notification, road hazard condition notification, and road feature notification. In V2I communication, RSU is deemed to an important infrastructure to realize the communication with vehicles and helps vehicles access to safety, traffic management, and infotainment application [1]. Generally, V2X communication are required to adopt DSRC[5] and IEEE WAVE[13] in North American (ETSI ITS-G5[2] in Europe).

2.2 DSRC

DSRC is a vehicle wireless communication technology. It is based on IEEE 802.11 standard and allocated from 5.85 to 5.925 GHz of spectrum for dedicated short-range communication radio services in ITS. This band is segmented into 7 channels. Each channel is allocated 10 MHz, forming one CCH (control channel) and six SCHs (service channel), in which two 10MHz channels can also be combined into 20 MHz channels, such as channel 175 and channel 181. DSRC radio can only communicate on one channel at a time. To use multiple channels, it is necessary to switch radio dynamically among them.

Figure 2 shows layered architecture for DSRC communication in the US. In the physical layer and MAC layer, the standard of IEEE 802.11p is adopted. In the middle of the stack, WAVE (Wireless Access

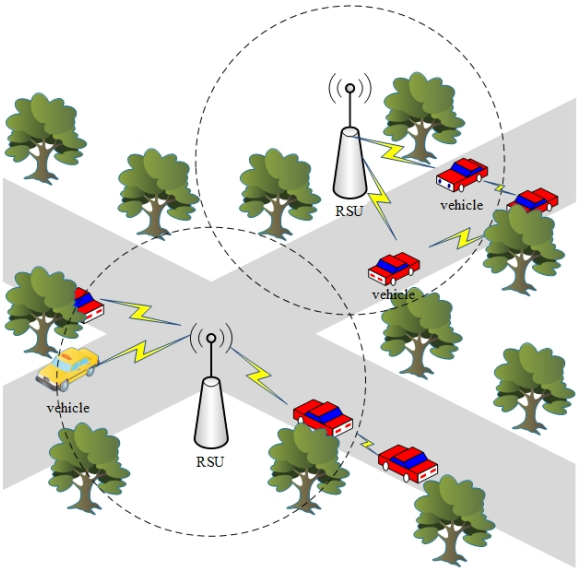


Figure 1: VANETs architecture.

for Vehicle Environment) is defined by the working group of IEEE 1609, which is mainly structured into four components (1609.2, 1609.3, 1609.4, 1609.6)[10].

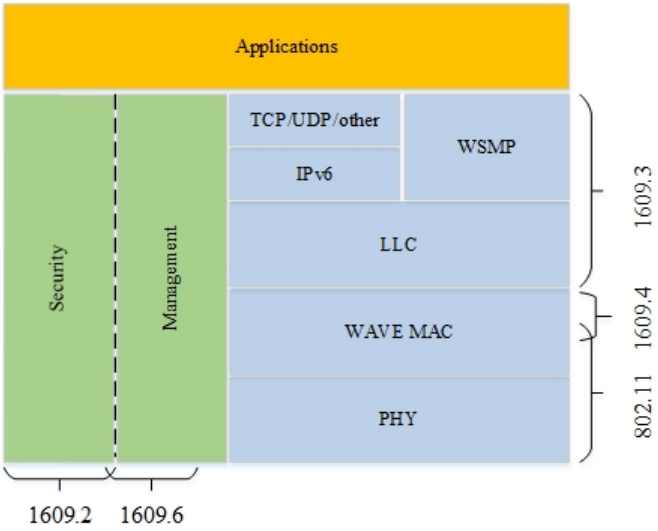


Figure 2: DSRC Channels.

2.3 BlockChain

As depicted in Figure 3, blockchain is a synchronized and distributed ledger, which maintains a growing list of interconnected blocks. Due to the advantages of decentralization, openness, and information tamper-resistant, blockchain has attracted lots of attentions from academy. Blockchain consists of a set of nodes connected via the network like mesh and P2P topologies[6]. The nodes in blockchain can interact directly without any third trusted party. This trust-less infrastructure guarantee faster and

cheaper transactions[8]. Ethereum is thought to be an important encrypted currency that uses blockchain and support smart contracts[3]. In smart contract, the content is realized in the form of codes, which are stored on the blockchain. Through the tamper-resistant feature of the blockchain, the validity of the contract is guaranteed and all participants can not breach the contract from the beginning. These functions are very suitable for transactions in VANETs[11].

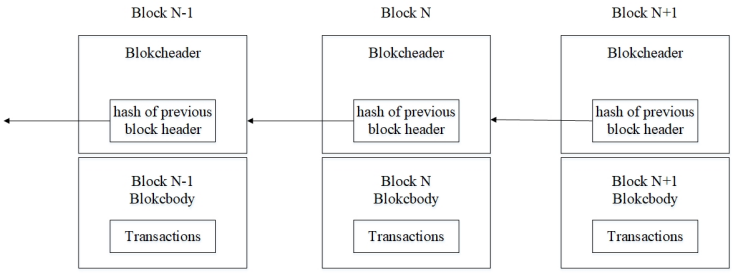


Figure 3: Logical representation of a blockchain.

3 The proposed scheme

3.1 System Model

In terms of on VANETs' payment model and blockchain technology, we design an electronic payment system model, as shown in Figure 4, which includes VANETs and blockchain layer.

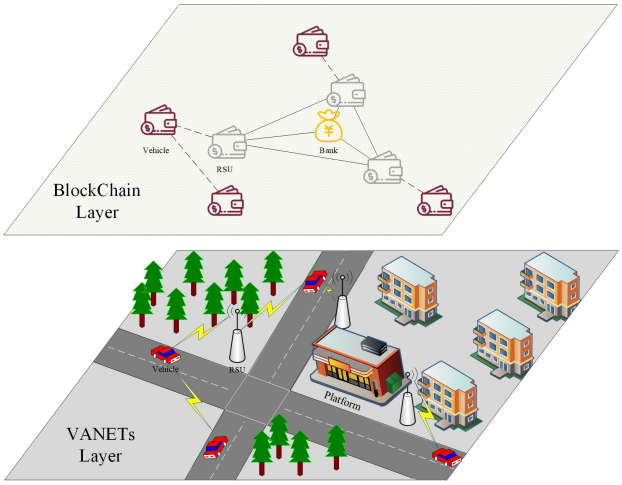


Figure 4: System model.

The entities involved in VANETs layer are divided into:RSU, vehicle, and payment platform. RSU broadcasts its application service in CCH. Then, RSU switches to SCH and communicates with vehicles interested in the service. During authentication, RSU can ensure the legality of the connected vehicle. Meanwhile, RSU and vehicle build a secure channel, which guarantees secure communication. Each vehicle can discover the service broadcasted by RSU in CCH and switch to the corresponding SCH channel to communicate with the RSU for transaction. At the end of the transaction, the vehicle is also allowed to obtain a receipt from RSU. Payment platform is considered as a trusted third-party, like

bank. Vehicles and RSUs are requested to register and apply corresponding accounts through payment platform.

In blockchain layer, the security of all transactions is maintained by the entities within blockchain. Generally, genesis block is generated by payment platform. All accounts of RSUs and vehicles are required to register and sent to blockchain through payment platform. When added to the blockchain, each vehicle need to deposit a certain amount of currency to guarantee that transactions are correctly executed and corresponding services are obtained. In addition, RSUs and vehicles have different rights in the blockchain layer. RSUs are responsible for maintaining all accounts in the blockchain and adopting a unified consensus mechanism to fight for accounting. Meanwhile, RSU is also allowed to trade with vehicles through blockchain. Vehicles do not participate in the maintenance of blockchain due to discontinuity and instability of network connections. However, all vehicles have the right to acquire all blocks in the blockchain from RSU. After finishing the transaction with RSU, vehicles can request receipt from the RSU.

3.2 V-R transaction

V-R transaction refers that the transaction is executed by vehicle and RSU. We present a parking toll management system as the scenario of V-R transaction. As shown in Figure 5, when getting ready to enter a carpark, vehicle can receive the parking service from RSU in the form of CCH. Then, the vehicle changes to SCH and communicates with RSU to send parking requests. The smart contract about parking toll is executed and the transaction begins. When the vehicle leaves the carpark, the vehicle sends out a departure request. Once the contract is completed, vehicle pays with RSU and obtains the receipt, the transaction ends. The details are depicted as following.

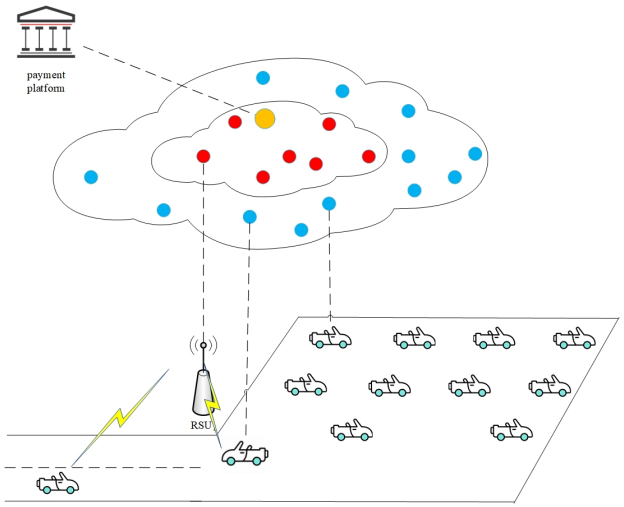


Figure 5: Park toll management system.

3.2.1 Transaction initiation

Before transaction, RSU needs to create a smart contract *Contract*, which mainly includes regulation of tolls and payee identity. When a vehicle enter a carpark, transaction initiation is performed as shown in Figure 6.

(1) RSU broadcasts parking service regularly and reports the service channel and it's identity.

(2) Vehicle turns to the appropriate channel and responds the parking service.

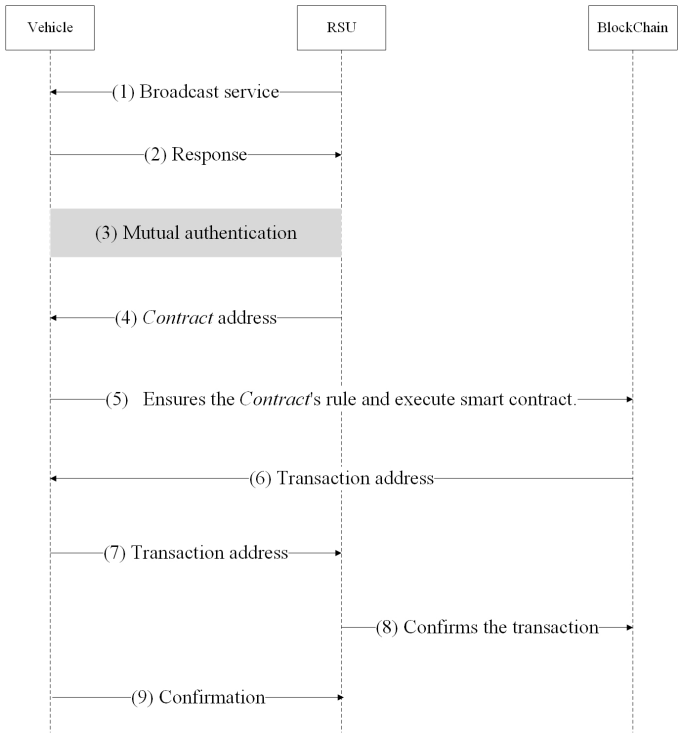


Figure 6: Transaction initiation.

(3) During mutual authentication, vehicles need to verify RSU, while RSU should determine whether the balance of the vehicle's claimed account in the blockchain meets parking fee standard. If the balance is enough, the protocol continues to execute.Otherwise RSU rejects the vehicle's parking request.

(4) After successful authentication, RSU sends the address of *Contract* to the vehicle.

(5)Then vehicle ensures the *Contract*'s rule and invokes the functions written in *Contract* to execute smart contract. the block system sets the nounce, start time, the address of payer, the address of payer and meanwhile vehicle's signature is also added to the transaction.

(6) The address of the transaction is sent back to the vehicle.

(7) vehicle sends the transaction address to RSU.

(8) When receiving the message from vehicle, RSU can find transaction from blockchain system. Then RSU confirms the transaction.

(9) Finally, RSU sends confirmation to vehicle.

3.2.2 Transaction confirmation

When vehicle gets ready to leave the parking lot and enters RSU communication range, transaction confirmation is required to execute. The details is shown in Figure 7.

(1-2) The execution process is the same as transaction initiation (1-2).

(3) Vehicle sends request to settle account.

(4) When receiving the request from vehicle, RSU helps the vehicle to connect blockchain network and the vehicle updates the transaction in blockchain where the end time is set, and meanwhile the vehicle need to use its private key to signs the transaction. Then, the blockchain system confirms the legality of the transaction and transfer parking fees from vehicle accounts to RSU accounts. Right now, the transaction is added to the blockchain. The address of the transaction is thought as evidence of the

transaction.

(5) vehicle sends response that the transaction has been update to RSU.

(6) RSU confirms the transaction through the address of the transaction and ends the service.

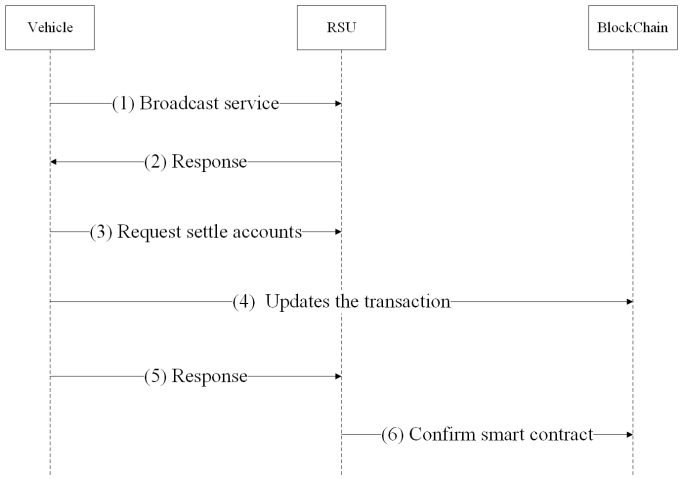


Figure 7: Transaction initiation.

4 Security Analysis

A brief security analysis is discussed in this section, which includes mutual authentication between RSU and vehicle, confidentiality and non-tampering of contracts, and non-repudiation of transactions.

Mutual authentication: During the mutual authentication between vehicle and RSU, RSU only needs to determine whether the vehicle account balance is adequate. When the vehicle is ready to leave the parking lot and confirm the transaction content, the blockchain system will automatically execute the vehicle payment to RSU. If the vehicle refuses to confirm the contract, RSU will prevent the vehicle from leaving. However, the RSU must be verified. Since RSU acts as the payee, once the vehicle pays to the compromised RSU, the property loss of the vehicle will be difficult to recover.

Confidentiality and Non-tampering: The confidentiality of the contracts mainly depends on blockchain. Now, some blockchain systems can adopt zero-knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARKs) [9] to ensure the confidentiality of contracts. Consequently, other nodes only know that the contracts are legal, but can't understand the content of the contracts. Meanwhile, relying on the blockchain, the content of the contracts can not be tampered with.

Non-reputation: During creating the contract and settling the account, vehicles must add their signatures to the transaction for ensuring the validity of the transaction, and the transaction is belong to the contract generated by RSU . Therefore, vehicles and RSU can not deny the transaction they have made.

5 Conclusion

In VANETs, payment is considered indispensable among service providers and consumers, this paper proposes an electronic payment scheme based on blockchain in VANETs. The transaction between vehicle and RSU is described in detail. The analysis shows that the proposed scheme can meet the security requirements of payment service.

In the future, we will simulate and analyze the performance of the scheme. Meanwhile, an efficient mechanism will be designed to achieve anonymous authentication.

Acknowledgment

This work was supported by China Fundamental Research Funds for the Central Universities under Grant No. N180716019 and Grant No.N182808003.

References

[1] A. Boualouache, S. Senouci, and S. Moussaoui. A survey on pseudonym changing strategies for vehicular ad-hoc networks. *IEEE Communications Surveys & Tutorials*, 20(1):770–790, Firstquarter 2018.

[2] C. Campolo, A. Molinaro, and R. Scopigno. *Vehicular ad hoc Networks: Standards, Solutions, and Research*. Springer International Publishing, June 2015.

[3] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor. Evaluation of logic-based smart contracts for blockchain systems. In *Proc. of the 10th International Symposium on Rule Technologies. Research, Tools, and Applications (RuleML'16), Stony Brook, New York, USA*, Lecture Notes in Computer Science, pages 167–183. Springer, Cham, July 2016.

[4] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Communications Surveys & Tutorials*, 13(4):584–616, December 2011.

[5] J. B. Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, July 2011.

[6] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal*, 4(6):1832–1843, December 2017.

[7] W. Li, Q. Wen, Q. Su, and Z. Jin. An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network. *Computer Communications*, 35(2):188–195, January 2012.

[8] S. Rouhani and R. Deters. Performance analysis of ethereum transactions in private blockchain. In *Proc. of the 8th IEEE International Conference on Software Engineering and Service Science (ICSESS'17), Beijing, China*, pages 70–74. IEEE, November 2017.

[9] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *Proc. of the 2014 IEEE Symposium on Security and Privacy (S&P'14), San Jose, California, USA*, pages 459–474. IEEE, May 2014.

[10] I. V. T. Society. IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture - Redline. Technical report, IEEE, March 2019.

[11] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran. Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment. *IEEE Internet of Things Journal*, 6(3):5791–5802, June 2019.

[12] J. Téllez Isaac, S. Zeadally, and J. C. Sierra. Implementation and performance evaluation of a payment protocol for vehicular ad hoc networks. *Electronic Commerce Research*, 10(2):209–233, June 2010.

[13] R. A. Uzcategui, A. J. De Sucre, and G. Acosta-Marum. Wave: A tutorial. *IEEE Communications Magazine*, 47(5):126–133, May 2009.

[14] A. M. Vegni and V. Loscrí. A survey on vehicular social networks. *IEEE Communications Surveys & Tutorials*, 17(4):2397–2419, July 2015.

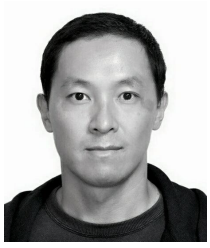
[15] Q. Wang, S. Leng, H. Fu, and Z. Yan. An ieee 802.11p-based multichannel mac scheme with channel coordination for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 13(2):449–458, June 2012.

[16] L. Zhu, M. Li, Z. Zhang, and Z. Qin. Asap: An anonymous smart-parking and payment scheme in vehicular networks. *IEEE Transactions on Dependable and Secure Computing*, page 1, June 2018.

Author Biography

Xinyang Deng received the BE in Software College from Dalian University of Foreign Languages in 2014, the ME in Software College from Northeastern university in 2018, respectively. Now he studies in Software College of Northeastern University. His primary research interests are next generation network security, PMIPv6 security and Identity-based Cryptography.

Bing Guan received his master degree in Software Engineering in Dalian University of Technology, Dalian, China, in 2015. He is currently working in Liaoning Information Security and Software Testing and Certification Center. His current research focuses mainly on network security, data security and information security management system.



Tianhan Gao received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2006, respectively. He joined Northeastern University in April 2006 as a lecture of Software College. He obtained an early promotion to an associate professor in January 2010. He has been a visiting scholar at department of Computer Science, Purdue, from February 2011 to February 2012. He obtained the doctoral tutor qualification in 2016. He is the author or co-author of more than 50 research publications. His primary research interests are next generation network security, wireless mesh network security, security and privacy in ubiquitous computing, as well as virtual reality.