Practical and Efficient Secure Communication in Autonomous Vehicle

Jiongen Xiao1,2, Yi Liu3,4*, Yi Zou5, Dacheng Li5,6 and Tao Leng7,8,9

Abstract

Internet of Vehicles can improve driving and riding experience, provide information needs, reduce environmental pollution, and improve transportation efficiency, thereby promoting the rapid development and application of intelligent transportation. Especially through the advantages of the rapidity of information exchange and the flexibility of real-time data processing, autonomous vehicle can provide barrier free, safe and sustainable transportation. At present, the rapid progress of the Internet of Things has promoted the continuous development of fully autonomous vehicle. However, autonomous vehicle network uses wireless communication technology, and the openness of its communication channel makes the communication process vulnerable to various security attacks. Therefore, this paper proposes a practical and efficient secure communication in autonomous vehicle. This scheme utilizes elliptic curve cryptography and signature, which can protect the security of multi-party communication between vehicle, cloud server, and user with lower computation and communication overhead. By analyzing the latest data obtained from cloud servers while securely accessing autonomous vehicle, user can transmit more reasonable driving strategies to autonomous vehicle while protecting communication security. This paper provides security verification for the scheme by using Scyther. Informal security analysis shows that this scheme can resist multiple attacks. Through comparative analysis and performance evaluation of the schemes, we found that the scheme improves security while maintaining efficiency.

Keywords Autonomous vehicle; Communication; Secure; Elliptic curve cryptography; Scyther

1. Introduction

The global road traffic safety situation is severe, with over one million traffic fatalities annually. The occurrence of road traffic accidents not only causes a large number of casualties, but also seriously affects economic development and social stability. The arrival of the intelligent era has provided many new ways to solve traffic problems, and autonomous vehicle that integrate emerging technologies such as the Internet of Vehicles, intelligent vehicles, and real-time communication are widely recognized as an effective solution to traffic problems. Autonomous vehicle is equipped with advanced onboard sensors and other devices, relying on high-precision digital maps, integrating modern communication and network technology, to achieve real-time interaction and sharing of data information between vehicles and surrounding intelligent transportation facilities [1-7]. It can effectively improve safety and traffic efficiency, reduce energy consumption, and is currentlya hot research topic internationally.

However, the deployment of autonomous vehicles in intelligent transportation systems faces some limitations and special needs[8]. On the one hand, autonomous vehicle can rely on multiple sensors to obtain accurate environmental information. These sensors play a crucial role in helping vehicles perceive the surrounding environment, detect objects, measure distance, determine direction and speed [9]. When faced with complex traffic conditions, harsh weather, and complex terrain and environmental conditions, the accuracy of sensors will be greatly affected[10]. This in turn affects the vehicle's ability to make accurate judgments and decisions, and cannot achieve the required safety level, posing huge challenges and risks to deploying autonomous vehicle. On the other hand,

the environmental information obtained by each vehicle through sensors is limited, and its own data collection and processing capabilities are also limited. Especially in complex and emergency situations, remote users need to control autonomous vehicle. This ensures that even if the user is not in the car, the autonomous vehicle can cope with complex road and environmental conditions through remote control. However, this also brings other challenges, increasing the risk of vehicles being maliciously invaded and making poor decisions [11-13].

In order to not only improve traffic conditions and optimize road conditions, but also achieve communication security and privacy protection in autonomous vehicle, it is necessary to research and design more secure, lightweight, security authentication and key agreement schemes for autonomous vehicle [14]. This scheme should strive to meet the requirements of anonymity and privacy protection, and not disclose the user's personal information, such as personal identity and communication objects, while also ensuring that some confidential information such as vehicle driving routes is also kept confidential [15-17]. This enables independent session keys to be obtained through authentication and key negotiation between the remote controller, cloud server, and autonomous vehicle, encrypting the information to be transmitted, ensuring communication security and privacy. Through this key, vehicle can timely upload environmental and driving data to cloud server, which will collect and process this information [18]. Remote users can not only better manage vehicles and plan paths through this data, but also analyze and obtain better and safer driving strategies and decision-making suggestions. Therefore, this study introduces an efficient authentication protocol specifically designed for autonomous vehicles. The key characteristics of this protocol include:

(1) Our protocol adopts elliptic curve cryptography technology and signature to en- sure the security of authentication, and uses three factor authentication to achieve user login, ultimately avoiding various security attacks.

(2) We have provided formal security proof for the protocol using Scyther. Informal security analysis suggests that the protocol is capable of satisfying the required security criteria

(3)Throughcomparativeanalysisandperformanceevaluationofprotocols,we found that the protocol maintains efficiency while improving security.

2. Related Work

In recent years, extensive research has been conducted by scholars on the security aspects of the Internet of Vehicles . This research has led to the emergence of a multitude of authentication schemes for vehicle networks.

Bisbas et al. [19] introduced a message authentication scheme for vehicles. However, it is important to note that this scheme is vulnerable to impersonation attacks. KA Shim et al. [20] introduced across-layer scheme for vehicles. Nevertheless, this scheme has been found to be insecure when subjected to key recovery attacks. Zhong et al. [21] presented a comprehensive scheme that facilitates secure communication through the utilization of certificateless aggregated signatures. However, it is worth mentioning that this scheme is susceptible to security vulnerabilities when subjected to man-in-the-middle attacks. Kumar et al. [22] introduced a certificateless authentication scheme that strengthens the security of authentication through the utilization of a substantial number of bilinear pairs. Nonetheless, the scheme introduces significant computational overhead. In contrast, Cui et al. [23] introduced a scheme based on semi-trust authorization,

combining key distribution method with a certificateless signature in a semi-trust authoritative environment. This approach eliminates the need for the receiver to query the revocation list, resulting in storage space and computational cost savings. However,the security level of this scheme is relatively low. Zhou et al. [24] presented a lightweight protocol that relies on location services. However, the vehicle node of this scheme requires a large amount of blind information to be calculated, which will incur significant computation overhead. Jianget al. [25] presented a security authentication protocol for vehicles based on Physical Unclonable Functions. This protocol eliminates the need for devices to store any secret information, ensuring resistance against attacks. Bagga P et al. [26] developed a novel onboard network security authentication protocol specifically designed for the secure authentication scheme. This protocol establishes a secure session key and can be employed for safety certification among vehicles. The analysis and verification have demonstrated that the protocol exhibits robust security and operational efficiency. Jangirala S et al. [27] introduced a secure protocol. The scheme enhances security through the integration of biometric technology, user identity, and passwords. By employing robust security authentication measures, this protocol establishes a secure communication channel, ensuring the confidentiality and integrity of the exchanged data. Jiang et al. [28] introduced a cloudcentric protocol specifically designed for autonomous vehicle. This protocol enables secure access to autonomous vehicle through authentication mechanisms. The protocol facilitates key negotiation between users and the cloud, as well as between users and the autonomous vehicle. The establishment of a session key communication ensures the security of the entire system, preventing unauthorized control of the autonomous vehicle.

Srinivas et al. [29] presented an authentication protocol based on biometric hashing. It caters to the requirements of dynamic changes and local password modification for wireless sensor nodes. However, it is important to note that this protocol lacks resilience against privileged internal attacks and falls short in achieving both forward security and user anonymity. Ali R et al. [30] introduced a protocol, aimed at safeguarding the security and privacy of agricultural environments against various malicious attacks. Nonetheless, it is important to note that this protocol is vulnerable to offline dictionary guessing attacks, and it does not provide forward security. PS A et al. [31] introduced a patient monitoring protocol. It incorporates numerous security attributes, offering advancements over existing solutions. However, it is important to note that this protocol does not address node capture attacks, and forwarding security. On a separate note, Jiang et al. [32] introduced a novel scheme specifically designed for the remote control of autonomous vehicle.This solution effectively combined cloud computing technology, enabling access to resources stored in the cloud to meet their data storage and analysis needs, as well as obtaining relevant information from vehicle manufacturers and autonomous vehicle service providers.

3. Preliminaries

The article outlines a system model involving three main entities: users, cloud servers, and autonomous vehicles. The cloud server is responsible for registering legitimate users and vehicles, storing necessary private keys and information, and facilitating operations for remote autonomous vehicles. Once registered, users can remotely access and control autonomous vehicles through cloud servers to continuously check their status. Autonomous vehicles, equipped with multiple sensor nodes and onboard units (OBU), interact wirelessly with cloud servers.

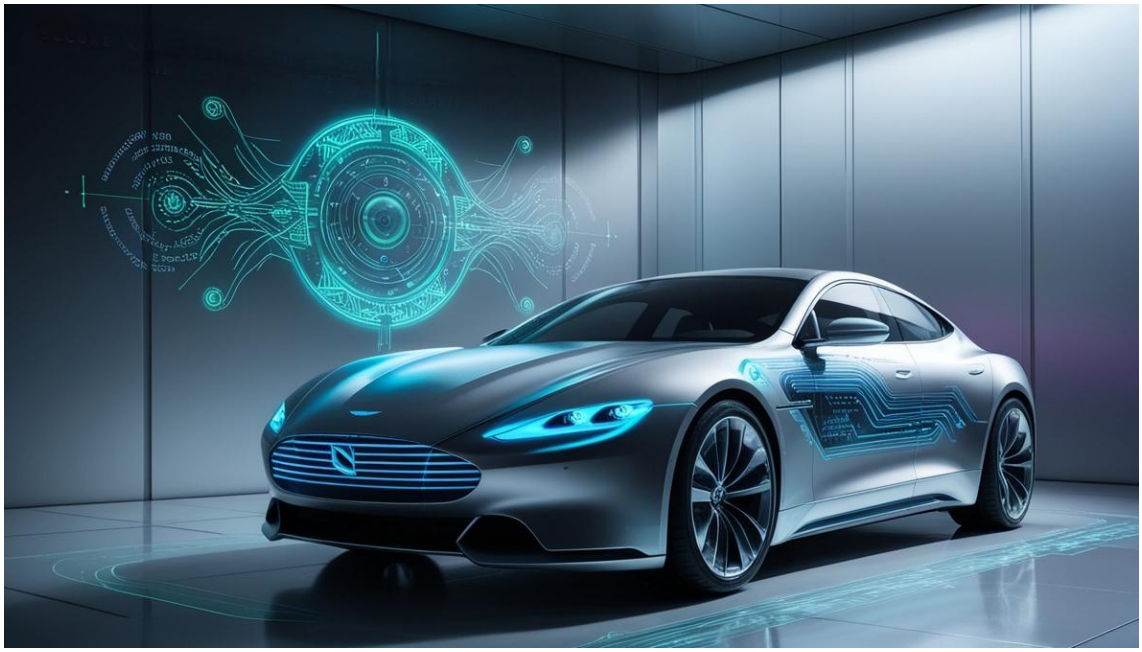
3.1. System Model

The proposed system model in this article is depicted in Figure 1, which includes the primary components of the system: users, cloud servers, and autonomous vehicles. In

this model, the cloud server plays a central role in managing the system's security and communication.

3.2. Threat Model

The threat model referenced in this article is the Dolev-Yao model. The adversary, denoted as A, is assumed to have various capabilities within the network. A can register as a vehicle in the network and is capable of manipulating, intercepting, eavesdropping on, and deleting messages transmitted over public channels. Additionally, A can access secret information stored within the vehicle's storage unit and attempt to guess the vehicle's true identity. A is also capable of launching various attacks, including internal attacks, impersonation attacks, and replay attacks.



3.2. Elliptic Curve Cryptography

Elliptic curve cryptography is a cryptosystem based on elliptic curves over finite fields. The elliptic curve can be defined on a finite field by a specific equation, where certain parameters belong to the finite field, and a particular condition must not be met to ensure the curve's validity.

4. The Proposed Protocol

The proposed protocol involves several steps and utilizes symbols defined in Table 1. The authentication process is illustrated in Figure 2. The protocol includes a system setup where the cloud server selects a cyclic group and a generator, chooses a main key, and calculates its corresponding public key. It also selects secure hash functions and publishes the system parameters while storing the master key secretly.

4.1. System Setup

The cloud server initiates the system by selecting a cyclic group and a generator. It also randomly selects a main key and computes the corresponding public key. Two secure

hash functions are chosen for the system's security measures.

4.2. Registration

During the registration process, the cloud server assigns a real identity to the autonomous vehicle and calculates a temporary identity. It also selects a random secret value and computes a hash value. The information is saved, and messages are sent to the autonomous vehicles through a secure channel.

4.3. Login and Authentication

The login and authentication process involves the user entering their real identity, password, and biometric information. The user equipment then calculates temporary values and sends registration information to the cloud server through a secure channel. The cloud server checks the registration information and sends a response to the user equipment.

5. Security Evaluation

The security evaluation of the proposed protocol is conducted using both formal verification tools and informal security analysis.

5.1. Formal Verification With Scyther Tool

The Scyther tool is utilized for formal protocol analysis, providing clear termination for unrestricted sessions and supporting multi-protocol parallel analysis. It uses the Security Protocol Description Language (SPDL) to describe and analyze security protocols. The Dolev-Yao model is selected to check the security of the proposed scheme, allowing the attacker to execute various attacks. The Scyther analysis demonstrates that the scheme successfully detects and mitigates all tested attacks, showcasing its robustness against potential threats.

5.2. Security Analysis

The proposed scheme achieves several security objectives:

Mutual Authentication: The scheme ensures mutual authentication between communication entities, verifying each party's identity through signature verification.

Identity Privacy Protection and Anonymity: It protects the identity privacy of users, preventing unauthorized tracing by encrypting identity information and transmitting anonymous identities over public channels.

Unlinkability: Each session maintains independence, making it difficult for adversaries to trace information across different sessions.

Resistance to Replay Attacks: The protocol uses timestamps to ensure the freshness and independence of messages, preventing replay attacks.

Resistance to Impersonation Attacks: The requirement of accurate identity, password, and biometric information deters impersonation by potential attackers.

Resistance to Man in the Middle Attacks: The mutual authentication and the use of secret values in transmitted messages safeguard against manipulation by unauthorized entities.

Resistance to Internal Attacks: The encryption of the user's password by random numbers and a one-way hash function protect against internal attacks.

Resistance to Password Guessing Attacks: The combination of honeywords technology and fuzzy verification technology makes it challenging for attackers to guess correct identity and password values.

5.3. Security Comparison

A comparison of the safety and functional characteristics of the proposed scheme with existing schemes is presented in Table 2. The results indicate that the proposed scheme provides better security features than existing ones.

6. Performance Evaluation

The performance evaluation of the proposed scheme is demonstrated through comparison of overheads.

6.1. Computation Overhead

The computation overhead of the proposed scheme and other existing schemes is compared by calculating the time required for various cryptographic operations. The proposed scheme shows significant advantages in computation overhead due to the efficient use of elliptic curve operations and hash functions.

6.2. Communication Overhead

The communication overhead is compared by unifying the output lengths of various cryptographic operations across different schemes. The proposed scheme, despite having a slightly higher communication overhead compared to one of the comparative schemes, offers higher communication efficiency and security.

7. Conclusion

The article concludes that with the rapid development of autonomous vehicle networks, ensuring communication security and privacy is crucial. The proposed secure communication scheme for autonomous vehicles not only prevents unauthorized access but also protects the security of communications between vehicles, cloud servers, and users. The scheme meets security requirements and demonstrates good performance, making it a practical solution for autonomous vehicle networks.

References

1. Chattopadhyay A, Lam KY, Tavva Y. Autonomous vehicle: Security by design[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 22(11): 7015-7029.

2. Nanda A, Puthal D, Rodrigues JJ P C, et al. Internet of autonomous vehicles communications security: overview, issues, and directions[J]. IEEE Wireless

Communications, 2019, 26(4): 60-65.

3. Miao J, Wang Z, Miao X, et al. A secure and efficient lightweight vehicle group authentication protocol in 5G networks. Wireless Communications and Mobile Computing, 2021, 2021:1-12.

4. Jha S, Jha N, Prashar D, et al. Integrated IoT-based secure and efficient key management framework using hashgraphs for autonomous vehicles to ensure road safety[J]. Sensors, 2022, 22(7): 2529.

5. Algarni A, Thayananthan V. Autonomous vehicles: The cybersecurity vulnerabilities and countermeasures for big data communication[J]. Symmetry, 2022, 14(12): 2494.

6. Nayak B P, HotaL, Kumar A, et al. Autonomous vehicles: Resource allocation, security, and data privacy[J]. IEEE Transactions on Green Communications and Networking, 2021, 6(1): 117-131.

7. Cui J, Liew L S, Sabaliauskaite G, et al. A review on safety failures, security attacks, and available countermeasures for autonomous vehicles[J]. Ad Hoc Networks, 2019, 90: 101823.

8. Sun X, Yu F R, Zhang P. A survey on cyber-security of connected and autonomous vehicles (CAVs)[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 23(7): 6240-6259.

9. Kim S W, Seo S W. Cooperative unmanned autonomous vehicle control for spatially secure group communications[J]. IEEE Journal on selected areas in communications, 2012, 30(5): 870-882.

10. Raiyn J. Data and cyber security in autonomous vehicle networks[J]. Transport and Telecommunication, 2018, 19(4): 325-334.

11. Miao J, Wang Z, Wu Z, et al. A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things. Expert Systems with Applications, 2024, 237: 121329.

12. Passerone R, Cancila D, Albano M, et al. A methodology for the design of safety-compliant and secure communication of autonomous vehicles[J]. IEEE Access, 2019, 7: 125022-125037.

13. Sun J, Xu G, Zhang T, et al. Secure data sharing with flexible cross-domain authorization in autonomous vehicle systems[J]. IEEE Transactions on Intelligent Transportation Systems, 2022.

14. Khan F, Kumar R L, Kadry S, et al. Autonomous vehicles: A study of implementation and security[J]. International Journal of Electrical & Computer Engineering (2088-8708), 2021, 11(4).

15. Huang C, Lu R, Lin X, et al. Secure automated valet parking: A privacy-preserving reservation scheme for autonomous vehicles[J]. IEEE Transactions on Vehicular Technology, 2018, 67(11): 11169-11180.

16. KakkarR, Gupta R, Agrawal S, et al. Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G[J]. Journal of Information Security and Applications, 2022, 67: 103179.

17. Hataba M, Sherif A, Mahmoud M, et al. Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey[J]. IEEE Open Journal of the Communications Society, 2022, 3: 811-829.

18. Miao J, Wang Z, Ning X, et al. Practical and secure multifactor authentication protocol for autonomous vehicles in 5G. Software: Practice and Experience, 2022.

19. S. Biswas, J. Misic. A Cross-Layer Approach to Privacy Preserving Authentication in WAVE-Enabled VANETs. IEEE Transactionson Vehicular Technology, 2013, 62(5): 2182–2192.

20. K.-A. Shim. Comments on "A Cross-Layer Approach to Privacy Preserving Authentication in WAVE-enabled VANETs" by Biswas and Misic. IEEE Transactions on Vehicular Technology, 2017, 66(11): 10588–10589.

21. H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu. Privacy-Preserving Authentication Scheme with Full Aggregation in VANET. Information Sciences, 2019, 476: 211–221.

22. P.Kumar, S.Kumari, V.Sharma,X. Li,A. K.Sangaiah,and S.H.Islam. Secure CLS and CL-AS Schemes Designed for VANETs[J]. The Journal of Supercomputing, 2019, 75(6): 3076-3098.

23. J. Cui,D. Wu,J. Zhang, Y. Xu, and H. Zhong. An Efficient Authentication Scheme Based on Semi-Trusted Authority in VANETs. IEEE Transactions on Vehicular Technology, 2019, 68(3): 2972–2986.

24. J. Zhou, Z. Cao, Z. Qin, X. Dong, and K. Ren. LPPA: Lightweight Privacy-Preserving Authentication from Efficient Multi-Key Secure Outsourced Computation for Location-Based Services in VANETs. IEEE Transactions on Information Forensics and Security, 2020, 15: 420–434.

25. Jiang Q, Zhang X,Zhang N, et al. Three-factor authentication protocol using physical unclonable function for IoV[J]. Computer Communications, 2021(5).

26. Bagga P, Das A K,Wazid M, et al. On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System[J]. IEEE Transactions on Vehicular Technology, 2021, PP(99):1-1.

27. Jangirala S,Das A K, Wazid M, et al. Designing Secure User Authentication Protocol for Big Data Collection in IoT-Based Intelligent Transportation System[J]. IEEE Internet of Things Journal, 2020, PP(99):1-1.

28. Jiang, Zhang, Ning, et al. Unified Biometric Privacy Preserving Three-Factor Authentication and Key Agreement for Cloud-Assisted Autonomous Vehicles.

29. Srinivas J ，Mukhopadhyay S ，Mishra D. Secure and efficient user authentication scheme for multi-gateway wireless sensor networks. Ad Hoc Networks ， 2017 ， 54（A）：147-169

30. Ali R ，PalAK ，KumariS ，KaruppiahM ，Conti M. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. Future GenerationComputer Systems ， 2018 ， 84（C）：200-215

31. Ps A,Akp A,Shi B . An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system[J]. Computer Methods and Programs in Biomedicine, 182:105054-105054.

32. Jiang Q, Zhang N, Ni J, et al. Unified biometric privacy preserving three-factor authenti-cation and key agreement for cloud-assisted autonomous vehicles[J]. IEEE Transactions on Vehicular Technology, 2020.

33. Cui J, Yu J, Zhong H, et al. Chaotic map-based authentication scheme using physical unclonable function for internet of autonomous vehicle[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 24(3): 3167-3181.

34. Jiang Q, Zhang N, Ni J, et al. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles[J]. IEEE Transactions on Vehicular Technology, 2020, 69(9): 9390-9401.

35. Miao J, Wang Z, Xue X, et al. Lightweight and secure D2D group communication for wireless IoT. Frontiers in Physics, 2023, 11: 121329.

36. NyangaresiV O. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography[J]. Journal of Systems Architecture, 2022, 133: 102763.

37. Saqib M, Jasra B, Moon A H. A lightweight three factor authentication framework for IoT based critical applications[J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(9): 6925-6937.

38. Ever, Yoney Kirsal. A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. Computer Communications, 2020, 155:143-149.(39)

39. Jia,Xiaoying,etal.Authenticated key agreement scheme for fog-driven IoT healthcare system. Wireless Networks,2019, 25:4737-4750.(48)

Author Biographies

Jiongen Xiao1,2, Yi Liu3,4*,Yi Zou5, Dacheng Li5,6 and Tao Leng7,8,9

1 International Business School,Guangdong University of Finance and Economics, Guangzhou, 510320, China; 20191068@gdufe.edu.cn

2 Electronic forensics laboratory,Guangzhou Software Application Technology Research Institute (for- merly known as Guangzhou Chinese Academy of Sciences Software Application Technology ResearchInstitute), Guangzhou, 510320, China;

3 Computer Network Center, Guangdong University of Finance and Economics, Guangzhou, 510320, China; gdym@gdpassword.cn

4 Guangdong Password Technical Service Co., LtdGuangzhou, 510320, China

5 School of Microelectronics, South China University of Technology, Guangzhou, 510320, China; zouyi@scut.edu.cn

6 Gosuncn technology group Co., Ltd, Guangzhou, 510320, China; 202311092404 @mail.scut.edu.cn

7 Intelligent Policing Key Laboratory of Sichuan Province,Sichuan Police College, Luzhou,646000,China

8 Institute of Information Engineering，Chinese Academy of Sciences,Beijing,10 0085,China

9 School of Cyber Security, University of Chinese Academy of Sciences, Beijing, 100049,China; lengtao@iie.ac.cn

* Correspondence: gdym@gdpassword.cn;

Author Contributions: Conceptualization, Jiongen Xiao and Yi Liu; methodology, Jiongen Xiao and Yi Liu; software, Yi Zou and Dacheng Li; validation and formal analysis, Yi Liu and Dacheng Li; writing—original draft preparation, Jiongen Xiao and Tao Leng. All authors have read and agreed to the published version of the manuscript.