Journal of Cyber Security
DOI: 10.32604/jcs.2022.028792
Article

Tech Science Press

Security Analysis for a VANET Privacy Protection Scheme

Yuzhen Liu[1,2], Xiaoliang Wang[1,2,*], Zhoulei Cao[1,2] and Frank Jiang[3]

[1]School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China
[2]Hunan Key Laboratory for Service Computing and Novel Software Technology, Xiangtan, 411201, China
[3]School of Engineering and IT, University of New South Wales, NSW,Australia
*Corresponding Author: Xiaoliang Wang. Email: fengwxl@163.com
Received: 05 March 2022; Accepted: 08 April 2022

Abstract: Vehicular ad hoc network (VANET) is a self-organizing wireless sensor network model, which is extensively used in the existing traffic. Due to the openness of wireless channel and the sensitivity of traffic information, data transmission process in VANET is vulnerable to leakage and attack. Authentication of vehicle identity while protecting vehicle privacy information is an advantageous way to improve the security of VANET. We propose a scheme based on fair blind signature and secret sharing algorithm. In this paper, we prove that the scheme is feasible through security analysis.

Keywords: Vehicular ad hoc network; anonymous authentication; fair blind signature; secret sharing algorithm; security analysis; BAN logic ideology

1 Introduction

Vehicle Ad Hoc Network (VANET) is a self-organizing multi-hop network. It establishes a traffic network with information sharing through wireless communication between vehicles and road infrastructure and between vehicles. It has the characteristics of openness, high-speed change of topology and so on.

Because of the limited communication radius of the vehicle, the vehicle node not only transmits its own message, but also forwards the message to other vehicle nodes as a wireless router node. In this open self-organizing network, in order to avoid unsafe communication environment, efficient, reliable inter-vehicle authentication scheme with less delay is essential. Therefore, efficient and reliable inter-vehicle authentication scheme is the focus of VANET research.

The IEEE 1609.2 standard [1] addresses security services for applications and management messages in wireless vehicular environment. It suggests the Secure Elliptic Curve Digital Signature Algorithm (ECDSA) [2] signatures should be used for wireless access. ECDSA ensures vehicular authentication and message integrity. However, it also brings huge signature verification overhead.

Due to this, Grover et al. [3] propose an efficient authentication scheme for highly dynamic VANET. They use probabilistic verification approach to reduce packet ratio in the highly dynamic traffic. They implement a complete solution in a realistic VANET scenario, which shows their scheme decreases message loss by an overall average of 68% compared to ECDSA.

To change the one by one verification way between vehicles, Lee [4] propose a batch authentication scheme for VANETs. They use a bilinear pairing to verify the vehicles' identities. At the same time, it can resist replay attacks and achieve non-repudiation effect. However, Bayat et al. [5] find the above scheme is vulnerable to the impersonation attack. That is to say, a malicious vehicle node can create a valid signature faking the identities of other vehicles. Therefore, they adopt a discrete logarithm problem to make malicious vehicles cannot compute the secret values of other vehicles. However, neither of the two Scheme's computational speed is fast enough to adapt to the real high-speed traffic environment.

Considering the requirement of quick verification when vehicles meet, Liu et al. [6] propose a proxy-based authentication scheme to assist roadside units in verifying a large number of vehicles simultaneously. They also present a novel key negotiation scheme for the transmitting of sensitive messages. Using such an authentication scheme, every RSU can verify more than 26000 signatures per second simultaneously with the assistance of some proxy vehicles.

To ensure certification service availability under the high dynamicity of VANETs, Oulhaci et al. [7] propose a distributed and secure certification system architecture for vehicular authentication. They use the concept of delegation and threshold cryptography to build collaborative-based certification approach in order to resist against compromised RSUs.

While some researchers focus on vehicle authentication, others begin to pay attention to vehicle privacy. For the driver, the identity and location information of the vehicle impacts his privacy rights and he does not want it to be disclosed.

Song et al. [8] address the advances in mobile networks and positioning technologies make vehicular location information leaked. Then, some adversaries will launch unauthorized tracking to a valid vehicle in VANET. They propose a vehicle density-based location privacy (DLP) scheme providing location privacy by utilizing the neighboring vehicle density as a threshold to change the pseudonyms. The proposed DLP scheme has a lower probability of successful tracking by an adversary than conventional schemes.

In addition to location privacy, identity privacy is also important. Hwang et al. [9] use Identity-Based Encryption (IBE) to design a secure message-broadcasting method in VANET, which can protect vehicular privacy and trail. Their proposal has some functionality such as integrity, authentication, non-repudiation, confidentiality, forward secrecy, anonymity, untraceability. It is more able to meet the needs of VANET communication.

However, a large number of malicious attacks are accompanied by the development of privacy preserving.

As presented in Bouali et al. paper [10], it regards that there are a large number of malicious users in existing VANET. They divided conventional methods into two categories. One is that the central authority (CA) uses CRL to discover compromised certificates to revoke users' certificates, and the other is to use intrusion detection methods to discover malicious users. The former approach with high overhead is not practical. The latter is a passive approach and cannot predict malicious behavior. They design a classification method to divide vehicles into three lists, namely black list, gray list, and white list. This classification offers the possibility for the system to predict an attack before it happens by detecting vehicles in the gray list in the routing process.

In many privacy protection schemes, the identity information of vehicles is completely hidden, so it is not practical to use the above anti-malicious attack scheme based on real identity.

Recently, some schemes protecting vehicular privacy in VANET, which focuses on conditional anonymous authentication based on anonymous certificates and signatures. Common techniques used in these schemes include group or ring signature scheme [11,12], ID-based encryptionscheme [13–16], blind signature [17] or commitment zero-knowledge proof and so on [18].

Wang et al. [12] point out that most of privacy-preserving authentication schemes depend on central certificate and has the single point failure problem, and then propose a VANET privacy protection scheme without a trusted third party. The proposal satisfies the most of security requirements, such as authentication security, good anonymity, and anti single point attack.

Tzeng et al. [15] regard that the conventional IBV scheme has some security risks and cannot be proved in the random oracle model. Therefore, they propose an identity-based batch verification for VANETs. Using a small constant number of pairing and point multiplication computations, their proposal has lower computation delay and transmission overhead because the verification processing is dependent on the number of messages.

But the above methods cannot resist collusion attack.

Recently, we proposed an anonymous identity authentication scheme, which not only guarantees users' privacy but also achieves anonymous identity authentication.

In recent years, there are some authors put forward some methods for privacy protection [24–30]. In [24], the authors design a novel anonymous authentication scheme based on edge computing in internet of vehicles. In [25], the authors put forward a location prediction method based on ga-lstm networks and associated movement behavior information. In [26], the authors research on copyright protection method of material genome engineering data based on zero-watermarking. In [27], the authors plan a plc protection system based on verification separation. H. Geng etc. design an efficient routing protection algorithm in large-scale networks [28]. In [29], the authors design a mutual authentication and key agreement protocol for wbans. In [30], X. Jin etc. design a reversible data hiding algorithm based on secret sharing.

As we mentioned above, there are also some weaknesses existing in current studies, such as single point failure, anonymity abuse. So we propose a novel mechanism based on fair blind signature and secret sharing algorithm to improve them [19].

2 Preliminary Knowledge

2.1 Fair Blind Signature

Blind Signature [20] is a signature approach that can be completed on the premise that the signer does not know the content of the signature. The blind signature scheme is extensively used in anonymous payment systems. However, the conventional blind signature schemes provide total unlinkability and sometimes it will give some attackers the opportunity to abuse anonymity. Therefore, Stadler et al. [21] propose a novel blind signature scheme to prevent anonymity abuse, which is called Fair Blind Signature Scheme. When anonymity abuse happens, this scheme can link a message signature pair with the corresponding protocol view of the signer.

2.2 Shamir Secret Sharing

Shamir's secret sharing [22] is an algorithm proposed by Adi Shamir. It is designed for preserving a secret. The secret is divided into different parts and distributed to different members. To reconstruct the original secret, a certain number of parts need to be collected. In this scheme, as long as parts larger than a certain threshold are collected, the secret can be restored. The threshold value is often less than the number of all parts.

3 Review of the Previous Scheme

3.1 Pseudonym Issue Based on a Fair Blind Signature

Initialization

AC denotes the authentication, PAC denotes pseudonym authentication center, TC denotes tracking center respectively. All entities generate their respective public/private key pair. V generates the private key dV and public key (NV, e_V). AC generates the private key dAC and public key (NAC, eAC). PAC generates the private key $dPAC$ and public key $(NPAC, ePAC)$. TC generates private key dTC and public key (NTC, eTC). Public keys of AC, PAC and TC will be sent to the vehicle that wants to take part in this communication network by the system.

Vehicle registration phase

1) V registers at AC.

V furtively passes $IDV||n||SV||CertV$ to AC. SV is the signature signed by V and equal to $(IDV||n)^{dV} mod/NV$, n is the number of pseudonyms.

2) AC verifies pseudonym and issues it.

AC checks the signature $(IDV||n)^{dV} mod/NV$. If it passes verification, AC issues a pseudonym and sends $IDAC||IDV||ts||SAC$ to V, in which SAC is the signature $[(IDAC||IDV||ts)^{dAC} \bmod NAC]^{eV} modNV$ by AC, and ts is a time stamp.

3) AC's signature is verified by V.

V decrypts $[(IDAC||IDV||ts)^{dAC} \bmod NAC]^{eV} modNV$ and obtains $(IDAC||IDV||ts)^{dAC} \bmod NAC$ and then checks AC's signature. If the signature is valid, two random numbers Ai, $Bi(1 \leq i \leq n)$ is selected by V and the blind value $Bi^{e_{AC}}Ai$ will be sent to AC from V.

4) AC computes $Ci = (Bi^{eAC}Ai \bullet (i||IDV||ts))^{dAC}$, $Di = ((i||IDV||ts)^{eTC})^{dAC}$ and sends the both to V.
5) V verifies $Di^{eAC} = (i||IDV||ts)^{eTC}$.

If passed, it will be gotten rid of blind factor and become $Ei, 1 = Ci/Bi$, $Ei, 2 = (Ei, 1^{eTC})/Di$. The pseudonym ID is denoted as $IDPVi = Ai{\bullet}(i||IDV||ts)||Ai^{eTC}$ $(IDAC||\{IDPVi||Ei, 1||Ei, 2||ePVi||NPVi||SPVi\})^{ePAC}$ is sent by V to PAC, where $1 \leq i \leq n$, and $SPVi$ is the signature signed by V using the temporary private key $dPVi$.

6) PAC verifies the signature and issues certificate.

PAC verifies the signature of V. If successful, it extracts $IDPVi$, namely $Ai \bullet (i||IDV||ts)$, Ai^{eTC}, $Ei, 1$ and $Ei, 2$. Then PAC checks whether $Ei, 1^{eAC} = (Ci/Bi)^{eAC} = (Ai \bullet (i||IDV||ts)^{dAC})^{eAC} = Ai \bullet (i||IDV||ts)$, $Ei, 2^{eAC} = (Ei, 1^{eTC}/Di)^{eAC} = \dfrac{(Ai \bullet (i||IDV||ts))^{eTC}}{(i||IDV||ts)^{eTC}} = Ai^{eTC}$. If the two equations pass verification, PAC sends $(Certpvi)^{eV} = (IDPAC||IDPVi||ts||ePVi||NPVi||SPAC)^{eV}$ to V.

3.2 *Anonymous Communication*

The vehicle V selects $Certpvi(1 \leq i \leq n)$ from n pseudonyms, and then sends anonymous message set $\{Mj\}$ $(1 \leq i \leq m$, m is the number of messages in this set) signed by temporary private signing key $dPVi$ to nearby vehicles. After passing the verification of nearby vehicle, $\{Mj\}$ will be accepted and used as anonymous communication.

3.3 *Threshold Sharing*

After the signing process ends, the TC preserves the private key dTC. In order to resist single point failure, the private key dTC is distributed to a group of other TCs called tracking group by Shamir secret sharing concept. It means that at least $n(n \leq m)$ members are needed to recover the private key dTC, where m is the number of members in this tracking group.

3.4 *Distributed Tracking Illegal Vehicle*

When the anonymous illegal behavior happens, authority system will require the tracking group to recover the pseudonym of the malicious vehicle and get its real identity.

The main steps are as follows:

1) PAC gets the pseudonym certificate $CertPV$ from the malicious packet and requires the corresponding tracking group to recover the private key dTC.
2) The tracking group members use the Lagrange interpolation formula and get a polynomial $f(x) = \sum_{i=1,i\neq j}^{n} yi \prod_{i\neq j} \frac{x-xj}{xi-xj}$. TC gets $dTC = f(0) = \sum_{i=1,i\neq j}^{n} yi \prod_{i\neq j} \frac{-xj}{xi-xj}$. After dTC is extracted, the real identity of the malicious vehicle is easy to be obtained.

4 Semi-formal Validity Proof for this Scheme

In this section, we use similar BAN logic ideology [23] to briefly demonstrate the validity of the proposed scheme. Although BAN logic has some limitations, it is still a widely used tool for the analysis of security-sensitive schemes and applications.

We transform the process of our protocol to the following idealized form (including plaintext).

Msg 1: $V \rightarrow AC: \; \{IDV, n, \{IDV, n\}_{d_V}, CertV\}$.

Goal 1: $AC \mid\equiv V \mid\sim \{IDV, n\}$.

Proof: According to Msg 1, we could get the following statement by applying the Message Meaning Rules of BAN logic:

$$\frac{AC \mid\equiv \overset{e_V}{\mapsto} V,\; AC \triangleleft \{IDV, n\}_{d_V}}{AC \mid\equiv V \mid\sim \{IDV, n\}}$$

Msg2:$AC \rightarrow V: \; \{ID_{AC}, IDV, \; ts, \{ID_{AC}, IDV, \; ts\}_{d_{AC}}\}$

Initial assumption 2: $V \mid\equiv \#\,(\mathrm{ts})$

Goal 2: $V \mid\equiv AC \mid\equiv \{ID_{AC}, IDV, \; ts\}$.

Proof: According to assumption 2, we could get the following statement by applying the Freshness Rules of BAN logic:

$$\frac{V \mid\equiv \#\,(\mathrm{ts})}{V \mid\equiv \#\,\{ID_{AC}, IDV, \; ts\}} \tag{1}$$

Then, we could get the following statement by applying the Nonce Verification Rules to (1):

$$\frac{V \mid\equiv \#\{ID_{AC}, IDV,\ ts\},\ V \mid\equiv AC \mid\sim \{ID_{AC}, IDV,\ ts\}}{V \mid\equiv AC \mid\equiv \{ID_{AC}, IDV,\ ts\}} \tag{2}$$

Finally, we could get the following statement by applying the Jurisdiction Rule to (2):

$$\frac{V \mid\equiv AC \mid\Rightarrow \{ID_{AC}, IDV,\ ts\},\ V \mid\equiv AC \mid\equiv \{ID_{AC}, IDV,\ ts\}}{V \mid\equiv \{ID_{AC}, IDV,\ ts\}}$$

Msg 3: $V \rightarrow AC:\ B_i^{e_{AC}} A_i$.

Goal 3: $AC \triangleleft B_i$.

Proof: According to Msg 3, we could get the following statement by applying the Seeing Rules of BAN logic:

$$\frac{AC \mid\equiv\mapsto^{e_{AC}} AC,\ AC \triangleleft \{B_i\}_{e_{AC}}}{AC \triangleleft B_i}$$

Msg 4: $AC \rightarrow V:\ \left\{\{\{Bi\}_{e_{AC}} Ai \bullet (i, IDV, ts)\}_{dAC}, \left\{\{i, IDV, ts\}_{e_{TC}}\right\}_{dAC}\right\}$

Goal 4-1: $AC \mid\equiv V \mid\sim \{\{Bi\}_{e_{AC}} Ai \bullet (i, IDV, ts)\}$

Goal 4-2: $AC \mid\equiv V \Big|\sim \{i, IDV, ts\}_{e_{TC}}$

Proof: According to Msg 4, we could get the following statement by applying the Seeing Rules of BAN logic:

$$\frac{V \triangleleft \left\{\{\{Bi\}_{e_{AC}} Ai \bullet (i, IDV, ts)\}_{dAC}, \left\{\{i, IDV, ts\}_{e_{TC}}\right\}_{dAC}\right\}}{V \triangleleft \{\{Bi\}_{e_{AC}} Ai \bullet (i, IDV, ts)\}_{dAC}} \tag{3}$$

Then, we could get the following statement by applying the Message Meaning Rules to (3):

$$\frac{V \mid\equiv\mapsto^{e_{AV}} AC,\ V \triangleleft \{\{Bi\}_{e_{AC}} Ai \bullet (i, IDV, ts)\}_{dAC}}{V \mid\equiv AC \Big|\sim \{\{Bi\}_{e_{AC}} Ai \bullet (i, IDV, ts)\}_{dAC}}$$

Similarly, we could get another goal: $AC| \equiv V \Big|\sim \{i, IDV, ts\}_{e_{TC}}$

Msg 5: $V \rightarrow PAC:\ \{IDAC, \{IDPVi, Ei, 1, Ei, 2, ePVi, NPVi, SPVi\}\}\ _{e_{PAC}}$

Goal 5: $PAC \triangleleft \{IDAC, \{IDPVi, Ei, 1, Ei, 2, ePVi, NPVi, SPVi\}\}$

Proof: According to Msg 3, we could get the following statement by applying the Seeing Rules of BAN logic:

$$\frac{PAC \mid\equiv\mapsto^{e_{PAC}} PAC,\ AC \triangleleft \{IDAC, \{IDPVi, Ei, 1, Ei, 2, ePVi, NPVi, SPVi\}\}\ _{e_{PAC}}}{AC \triangleleft \{IDAC, \{IDPVi, Ei, 1, Ei, 2, ePVi, NPVi, SPVi\}\}}$$

Msg 6: $PAC \rightarrow V:\ \{IDPAC, IDPVi, ts, ePVi, NPVi, SPAC\}\ _{eV}$

Goal 6: $V \triangleleft \{IDPAC, IDPVi, ts, ePVi, NPVi, SPAC\}$.

Proof: According to Msg 3, we could get the following statement by applying the Seeing Rules of BAN logic:

$$\frac{V \mid\equiv\mapsto^{eV} V,\ V \triangleleft \{IDPAC, IDPVi, ts, ePVi, NPVi, SPAC\}\ _{eV}}{V \triangleleft \{IDPAC, IDPVi, ts, ePVi, NPVi, SPAC\}}$$

It must be noted that the BAN logic is to achieve the trustworthiness of each other. In view of the number of relative entities in this scheme and the limited length of the paper, we only give and prove the local goal of each step in the certificate generation process. However, from these goals, the trustworthiness of each other can be further deduced.

5 Conclusion

In this paper, we use BAN logic ideology to prove our previous algorithm. Further experiments will be carried out in future work. By security analysis, the scheme has been proved to be available.

Funding Statement: This work was supported by Key project of Hunan Provincial Education Department (20A191), Hunan teaching research and reform project (2019-134), Cooperative Education Fund of China Ministry of Education (201702113002, 201801193119), Hunan Natural Science Foundation (2018JJ2138), Hunan teaching research and reform project (2019).

Conflicts of Interest: The authors state that they have no conflicts of interest related to this study to report.

References

[1] I. Transportation and S. Committee, “IEEE Trial-Use Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages,” *IEEE Standards*, vol. 1, pp. 1–105, 2006.

[2] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ECDSA),” *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[3] K. Grover, A. Lim, and S. Lee, “Efficient authentication approach for highly dynamic vehicular ad hoc networks,” (in English), *International Journal of Ad Hoc and Ubiquitous Computing*, Article vol. 19, no. 3–4, pp. 193–207, 2015.

[4] C. C. Lee, “Toward a secure batch verification with group testing for VANET,” *Wireless Networks*, vol. 19, no. 6, pp. 1441–1449, 2013.

[5] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, “A secure authentication scheme for VANETs with batch verification,” (in English), *Wireless Networks*, Article vol. 21, no. 5, pp. 1733–1743, 2015.

[6] Y. L. Liu, L. M. Wang, and H. H. Chen, “Message authentication using proxy vehicles in vehicular Ad Hoc networks,” (in English), *IEEE Transactions on Vehicular Technology*, Article vol. 64, no. 8, pp. 3697–3710, 2015.

[7] T. Oulhaci, M. Omar, F. Harzine, and I. Harfi, “Secure and distributed certification system architecture for safety message authentication in VANET,” (in English), *Telecommunication Systems*, Article vol. 64, no. 4, pp. 679–694, 2017.

[8] J. H. Song, V. W. S. Wong, and V. C. M. Leung, “Wireless location privacy protection in vehicular Ad-hoc networks,” (in English), *Mobile Networks & Applications*, Article vol. 15, no. 1, pp. 160–171, 2010.

[9] R. J. Hwang, Y. K. Hsiao, and C. Y. Hwang, “Privacy protection on vehicular Ad hoc NETworks,” (in English), *International Journal of Ad Hoc and Ubiquitous Computing*, *Article* vol. 7, no. 4, pp. 261–271, 2011.

[10] T. Bouali, S. M. Senouci, and H. Sedjelmaci, “A distributed detection and prevention scheme from malicious nodes in vehicular networks,” (in English), *International Journal of Communication Systems*, Article vol. 29, no. 10, pp. 1683–1704, 2016.

[11] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, “Efficient and robust pseudonymous authentication in VANET,” in *Int. Workshop on Vehicular Ad Hoc Networks, Vanet 2007*, Montréal, Québec, Canada, pp. 19–28, September 2007.

[12] X. Wang, S. Li, S. Zhao, Z. Xia, and L. Bai, “A vehicular ad hoc network privacy protection scheme without a trusted third party,” *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, pp. 12–15, 2017, Art. no. 1550147717743696.

[13] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, “An identity-based security system for user privacy in vehicular Ad Hoc networks,” *IEEE Transactions on Parallel & Distributed Systems*, vol. 21, no. 9, pp. 1227–1239, 2010.

[14] D. J. Huang, S. Misra, M. Verma, and G. L. Xue, “PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs,” (in English), *IEEE Transactions on Intelligent Transportation Systems*, Article vol. 12, no. 3, pp. 736–746, 2011.

[15] S. F. Tzeng, S. J. Horng, T. R. Li, X. Wang, P. H. Huang, and M. K. Khan, “Enhancing security and privacy for identity-based batch verification scheme in VANETs,” (in English), *IEEE Transactions on Vehicular Technology*, Article vol. 66, no. 4, pp. 3235–3248, 2017.

[16] C. Y. Chen, T. C. Hsu, H. T. Wu, J. Y. Chiang, and W. S. Hsieh, “Anonymous authentication and Key-agreement schemes in vehicular Ad-hoc networks,” (in English), *Journal of Internet Technology*, *Article* vol. 15, no. 6, pp. 893–902, 2014.

[17] X. Tian and S. Qiang, “Research of an authentication scheme based on the proxy blind signature scheme for the vehicular Ad-hoc networks,” *Bulletin of Science & Technology*, 2012.

[18] A. Singh and H. C. S. Fhom, “Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection,” (in English), international journal of information security,” *Article*, vol. 16, no. 2, pp. 195–211, 2017.

[19] X. Wang and S. Li, “A VANET privacy protection scheme based on fair blind signature and secret sharing algorithm,” *Automatika*, vol. 58, no. 3, pp. 287–294, 2017.

[20] D. Chaum, “Blind Signatures for Untraceable Payments,” in *Presented at the Advances in Cryptology-Crypto 1982*, Santa Barbara, CA, USA, Springer, 1982.

[21] M. Stadler, J. -M. Piveteau, and J. Camenisch, “Fair blind signatures,” *Lecture Notes in Computer Science*, vol. 921, pp. 209–219, 1995.

[22] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[23] M. Burrows, M. Abad, and R. M. Needham, “R.M.: A logic of authentication,” *Proceedings of the Royal Society A Mathematical Physical & Engineering Sciences*, vol. 426, no. 1871, pp. 1–13, 1989.

[24] X. Wang, X. She, L. Bai, Y. Qing and F. Jiang, “A novel anonymous authentication scheme based on edge computing in internet of vehicles,” *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3349–3361, 2021.

[25] X. Cao, L. Jiang, X. Wang and F. Jiang, “A location prediction method based on ga-lstm networks and associated movement behavior information,” *Journal of Information Hiding and Privacy Protection*, vol. 2, no. 4, pp. 187–197, 2020.

[26] L. L. Cui and Y. B. Xu, “Research on copyright protection method of material genome engineering data based on zero-watermarking,” *Journal on Big Data*, vol. 2, no. 2, pp. 53–62, 2020.

[27] X. Pan, H. Li, X. Li, L. Xu and Y. Sun, “Plc protection system based on verification separation,” *Computers, Materials & Continua*, vol. 71, no. 2, pp. 2401–2417, 2022.

[28] H. Geng, H. Zhang and Y. Zhang, “Efficient routing protection algorithm in large-scale networks,” *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1733–1744, 2021.

[29] X. Meng, J. Xu, X. Wu and Z. Wang, “Design of a mutual authentication and key agreement protocol for wbans,” *Journal of Information Hiding and Privacy Protection*, vol. 2, no. 3, pp. 107–114, 2020.

[30] X. Jin, L. Su and J. Huang, “A reversible data hiding algorithm based on secret sharing,” *Journal of Information Hiding and Privacy Protection*, vol. 3, no. 2, pp. 69–82, 2021.