Proceedings of the Estonian Academy of Sciences,
2021, **70**, 1, 91–97
https://doi.org/10.3176/proc.2021.1.04
Available online at www.eap.ee/proceedings

Authentication mechanism of network communication nodes based on information safety of the Internet of Vehicles

Qiong Wu

José Rizal University, 80 Shaw Blvd., Mandaluyong, Philippines; Taiyuan University of Technology, No. 79 West Street Yingze, Taiyuan, Shanxi 030024, China; wuqiong_qw@yeah.net

Received 8 September 2020, accepted 27 November 2020, available online 28 January 2021

Abstract. The Internet of Vehicles (IoV) is an important part of intelligent traffic, and the problem of information safety is an essential task that has to be solved urgently. In this study, the main focus is on the authentication mechanism of communication nodes in the IoV. Based on elliptic curve cryptography, an authentication method was designed; the processes of system establishment, pseudonym generation and message authentication were introduced; and the safety of the system was analysed. The results indicate that the proposed method has passed the correctness verification and has significant advantages compared to SPECS and b-SPECS in terms of time cost and authentication delay. The experimental results verify the reliability of the method, which makes some contributions to the authentication of communication nodes in the IoV and is beneficial to the further improvement of information security of the IoV.

Key words: Internet of Vehicles, information security, elliptic curve cryptography, communication nodes, identity authentication.

1. INTRODUCTION

Volume capacity of automobiles has rapidly increased with the development of economy. Moreover, the problems of traffic jams and safety are becoming more and more prominent, which poses huge challenges to the society and economy. For the purpose of organizing the traffic system, the Internet of Vehicles (IoV) has emerged, which collects and combines data from different sectors. The Internet of Vehicles can help drivers obtain information about other vehicles and road condition [1] in order to effectively avoid traffic jams and accidents [2]. It can also provide office and entertainment services [3] to improve the driving experiment. It is a great revolution for the traffic system which has a very broad application prospect [4]. While releasing information, the IoV also needs to rapidly acquire relevant information in the network. Not only does it have to protect the information but it also needs to make safety certification on the received information. Bugs in information security will cause the loss of privacy and property, and may directly endanger the life of drivers. Therefore, information security is an important part of the IoV. To ensure the safe and stable development of the IoV, it is necessary to enhance its information security. Currently, studies on the IoV mainly concentrate on how to improve the operational efficiency of the IoV and the study on its information security issue is still slow to develop, but it has lately become the concern of an increasing number of researchers. The authentication of IoV communication nodes is an effective means of ensuring IoV information security. Cheng et al. [5] have proposed an authentication method which performed bilinear pairings on the elliptic curve and generated a signature through the vehicle node and roadside cell node. The analysis also verified that the scheme was unforgeable and had forward and backward security as well as high authentication efficiency. Wang et al. [6] have designed a two-factor lightweight privacy- preserving authentication scheme. Compared with other schemes, the computation cost of the scheme was 100–1000 times lower, the communication cost was 55.24–77.52% lower, and it had strong non-repudiation. Wang et al. [7] have used self-generated pseudo-identities to ensure privacy protection and then implemented message authentication codes to verify the messages. Compared with the public key based method, this particular method reduced the computational cost 102–103 times and the communication cost by 41.33–77.60%. Zhou et al. [8] have proposed an authentication method based on trust evaluation, which calculated the trustworthiness of vehicle nodes and detected malicious vehicles by the correlation coefficient. The simulation results showed that the method was effective. Currently, the authentication of IoV communication nodes has the problems of high time cost and poor real-time performance, which cannot satisfy the increasing demands for the IoV. In this study, a communication node authentication method based on elliptic curve cryptography was designed, and its correctness and time cost were analysed, proving the validity of the scheme. The present study provides some theoretical support for the application and promotion of the designed method for the IoV and makes some contributions to ensuring the information security of IOV.

2. IoV AND ITS INFORMATION SECURITY PROBLEM

The IoV achieves a comprehensive connection between people, vehicles, roads and the Internet, relying on information technology, so as to improve the level of automation and the intelligence of vehicles, and to enhance traffic efficiency and user experience [9]. The IoV is mainly composed of on-board units (OBU) on vehicles, roadside units (RSU) [10], trusted authority (TA) and a service provider (SP). There is cable communication between TA and SP and wireless communication between OBU and RSU, which is divided into Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). The IoV has the characteristics of predictability, different network density, fast network topology change, large network scale, and strong computing power. As the IoV uses wireless communication mode, it will inevitably be subject to many threats and attacks, as shown in Table 1.

Table 1. Main threats faced by the IoV

Availability threat	Denial-of-Service attacks: Attackers make users unable to use the network, normally through flooding, and prevent nodes from processing information.
	Black hole: Attackers refuse to join or maliciously withdraw from the network, causing the network link to be interrupted.
	Broadcast intervention: Attackers publish false information in the network, affecting user judgment.
Authenticity threat	Replay attack: Attackers redistribute previous information to the network, destroying the routing strategy of the mobile node.
	Information tampering: Attackers modify the information between V2V and V2I, causing network damage.
	Location spoofing: Attackers modify or forge their location and send it to the network to destroy the network.
Confidentiality threat	Attackers eavesdrop and steal user information without the user's consent.

Network threats will lead to the development of security incidents. IoV security incidents can be roughly divided into (1) control of automotive power system: the attacker may invade the automobile system through IoV vulnerability, modify the instructions, and control the steering and braking of the automobile, which will seriously threaten the safety of the driver; (2) intrusion into driver's account: attackers may use IoV vulnerabilities to illegally obtain vehicle information, locate and unlock vehicles, as well as steal vehicles, resulting in property loss to the owners. Alternatively, they may even obtain owner information through monitoring and tracking.

3. ELLIPTIC CURVE CRYPTOGRAPHY BASED AUTHENTICATION MECHANISM OF COMMUNICATION NODES

3.1. Elliptic curve cryptography

The elliptic curve $E\left(F_q\right)$ is the union set of the solution of the equation $y^2 = x^3 + ax + b$ on the finite field F_q and the point at infinity, which can be expressed as: $E\left(F_q\right) = \left\{\left(x, y\right) | \, y^2 = x^3 + ax + b, \left(x, y\right) \in F_q\right\} \cup \left\{0\right\}$, where q stands for a prime number. The set of points whose order on E is q and the generating element P is represented by the group G_p. The operations on the elliptic curve include:

(1) Addition of points. Let us suppose that there are $P_1 = \left(x_1, y_1\right)$, $P_2 = \left(x_2, y_2\right)$ and $P_1, P_2 \in E\left(F_p\right)$, then $P_1 + P_2 = \left(x_3, y_3\right) \in E\left(F_p\right)$.

(2) Scalar-multiplication of points: If $P = \left(x, y\right) \neq 0$ and k is an integer, then $kP = P + P + P + \cdots + P$, i.e. k-points are added up.

In elliptic curve cryptography, the point $P = \left(x, y\right)$ on $E\left(F_p\right)$ is taken as the public base point. The cryptosystem is established based on an Abelian group.

3.2. System establishment

TA is defined as: $E : y^2 = x^3 + ax + b \bmod p$, a,b $\in Z^*_{\mathrm{q}}$. The group G_p is selected on E. $S_1, S_2 \in Z^*_{\mathrm{q}}$ is randomly selected as the private key. Then the public key $P_{pub_1} = s_1 P$, $P_{pub_2} = s_2 P$ is calculated. Next, four hash functions are selected by TA: $h_1 : G \rightarrow Z_{\mathrm{q}}$, $h_2 : G = \left\{0,1\right\}^* \times \left\{0,1\right\}^* \rightarrow Z_{\mathrm{q}}$, $h_3 : G \times \left\{0,1\right\}^* \times \left\{0,1\right\}^* \rightarrow Z_{\mathrm{q}}$, $h_4 : \left\{0,1\right\}^* \times \left\{0,1\right\}^* \times G \times G \times \left\{0,1\right\}^* \rightarrow Z_{\mathrm{q}}$. The system parameter is $Paras = \left\{p, q, a, b, p_{pub_1}, p_{pub_2}, h_1, h_2, h_3, h_4\right\}$. A vehicle node needs to submit the identity RID and the password PWD. TA allocates a tamper-proof device (TPD) for the vehicle node. RID, PWD, the system private key s_1, s_2 and $Paras$ are stored in TPD.

3.3. Pseudonym generation

In the process of pseudonym generation, the vehicle node V_i first inputs RID_i and PWD_i into TPD. Then TPD tests them. The next step is taken only if they pass the test; otherwise, the operation stops. After testing, TPD generates two random numbers r_i, u_i and the timestamp T_i. $R_i = Pr_i$, $U_i = Pu_i$, $PID_i = RID_i \oplus h_i\left(r_i \cdot p_{pub_1}\right)$, $h_{r_{\mathrm{i}}} = h_2\left(PID_i, T_i, R_i\right)$, $h_{u_{\mathrm{i}}} = h_3\left(PID_i, T_i, U_i\right)$, $SK_i^1 = s_1 h_{r_{\mathrm{i}}} + r_i \bmod q$ and $SK_i^2 = s_2 h_{u_{\mathrm{i}}} + u_i \bmod q$ are calculated. Finally, $\left\{PID_i, R_i, U_i, SK_i^1, SK_i^2, T_i\right\}$ is obtained and sent to an OBU node.

The OBU node signs the message M_i. The abstract $h_i = h_4\left(M_i, PID_i, T_i, R_i, U_i\right)$ and the signature $\delta_i = SK_i^1 + h_i SK_i^2 \bmod q$ are calculated. The vehicle node V_i sends M_i by pseudonym. The signature information at that time is $\tau_i = \left\{U_i, R_i, \delta_i\right\}$. Then the above information is broadcast by the vehicle node.

3.4. Message verification

The message $\left\{M_i, PID_i, T_i, \tau_i\right\}$ needs to be verified after being received. First, it is verified whether T_i is fresh or not. If it is not, then the message is abandoned; if it is, the message is added to the batch authentication queue. To prevent an attack, a random small factor testing technique is introduced and the small integer sequence $\lambda = \{\lambda_1, \lambda_2, \cdots, \lambda_i, \cdots \lambda_n\}(\lambda_i \in [1,2^{\varsigma}])$, where ς refers to the safety parameter of the random small factor, is taken as the random small factor. The following equation is used for verification:

$$P \cdot \left(\sum_{i=1}^{n} \lambda_i \delta_i\right) = P_{pub_1}\left(\sum_{i=1}^{n} \lambda_i h_{r_i}\right) + P_{pub_2}\left(\sum_{i=1}^{n} \lambda_i h_{u_i} h_i\right) + \left(\sum_{i=1}^{n} \lambda_i h_i U_i\right) + \left(\sum_{i=1}^{n} \lambda_i R_i\right). \tag{1}$$

If the equation stands, then the signature is effective, and the received information can be accepted; otherwise, the signature is ineffective, and the message is abandoned.

4. PERFORMANCE ANALYSIS OF AUTHENTICATION MECHANISM

4.1. Correctness analysis

It is obtained according to the parameters set in this paper that $P_{pub_1} = s_1 P$, $P_{pub_2} = s_2 P$, $R_i = Pr_i$, $U_i = Pu_i$, $SK_i^1 = s_1 h_{r_1} + r_i \bmod p$, $SK_i^2 = s_2 h_{u_i} + u_i \bmod p$, and $\delta_i = SK_i^1 + h_i SK_i^2 \bmod q$.

The equation of message verification is deduced as follows:

$$\begin{aligned} P \cdot \left(\sum_{i=1}^{n} \lambda_i \delta_i\right) &= P \cdot \left(\sum_{i=1}^{n} \lambda_i \left(SK_i^1 + h_i SK_i^2\right)\right) \\ &= P \cdot \left(\sum_{i=1}^{n} \lambda_i \left(s_i h_{r_i} + r_i + h_i \left(s_2 h_{u_i} + u_i\right)\right)\right) \\ &= \sum_{i=1}^{n} \lambda_i \left(h_{r_i} P_{pub_1} + R_i + h_i h_{u_i} P_{pub_2} + h_i U_i\right) \\ &= P_{pub_1}\left(\sum_{i=1}^{n} \lambda_i h_{r_i}\right) + P_{pub_2}\left(\sum_{i=1}^{n} \lambda_i h_{u_i} h_i\right) + \left(\sum_{i=1}^{n} \lambda_i h_i U_i\right) + \left(\sum_{i=1}^{n} \lambda_i R_i\right). \end{aligned} \tag{2}$$

The equation of message verification stands, which means that the authentication mechanism is correct.

4.2. Time-cost analysis

T_p is set as the operation time of a pair, T_{mul} is set as the operation time of point multiplication, and T_{mlp} as the operation time of MapToPoint hash function. The authentication mechanism is compared with the SPECS algorithm [11] and the b-SPECS algorithm [12]. The SPECS algorithm adopts batch certification, i.e. any vehicle is allowed to identity authentication with group members but cannot resist impersonation attack and needs extra cost because of the one-time pad mode. The b-SPECS algorithm is an improvement of the SPECS algorithm, but it also adopts the one-time pad mode, has low signature generation efficiency, and requires a high time cost because of performing pair operation two times in batch certification. The results of the algorithm comparison are given in Table 2.

Table 2. Comparison of calculation time between different methods

Algorithm	SPECS	b-SPECS	Method proposed in this study
Generation of signature	$4T_{mul} + 2T_{mlp}$	$5T_{mul} + 2T_{mlp}$	$4T_{mul} + 2T_{mlp}$
Verifying one signature	$2T_p + 2T_{mul} + 2T_{mlp}$	$2T_p + 2T_{mul} + 2T_{mlp}$	$2T_{mul} + T_{mlp}$
Verifying n signatures	$2T_p + 2nT_{mul} + 2T_{mlp}$	$2T_p + 2nT_{mul} + 2T_{mlp}$	$2nT_{mul} + nT_{mlp}$

Table 2 shows that the three methods have no significant difference in the signature generation, although the time consumed by the b-SPECS algorithm was slightly longer. In the verification of one signature, the time consumed by the SPECS and b-SPECS algorithms was the same, but the method proposed in this study did not need pair operation and less time was spent in the calculation of T_{mlp}. In the verification of n signatures, the time consumed by the SPECS and b-SPECS algorithms was the same, and the verification time of the method proposed in this study was significantly shorter. Overall, the method presented in this study has a significant advantage in time cost, and thus can meet the authentication requirement of IoV communication nodes.

4.3. Analysis of authentication delay

To further analyse the performance of the method proposed in this study, the average time delay of the three algorithms is compared under different number of vehicles and speeds, and the results are shown in Tables 3 and 4.

Table 3 illustrates that the communication time delay shows an increasing tendency with the increase of the number of vehicles, but the average time delay of SPECS and b-SPECS is similar. By the example of b-SPECS one can observe that when the number of vehicles was 25, the average time delay was 0.035 s; when the number of vehicles was 150, the average time delay was 0.114 s, which was three times higher than before. By following the method proposed in this study one can notice that when the number of vehicles was 25, the average time delay was 0.031 s; when the number of vehicles was 150, the average time delay was 0.064 s, which was two times higher than before. It shows that the method presented in this study can effectively reduce the calculation process and time delay in the case of the increasing number of vehicles. Table 4 demonstrates that the change in the average time delay under different methods was small in relation to the change in the vehicle speed. When the vehicle speed increased from 0 m/s to 25 m/s, the average time delay of all the three methods increased by 0.004 s. However, the comparison of the three methods under the same speed shows that the average time delay of the method proposed in this study always maintained a gap of 0.02 s over the other two methods, which indicates the reliability of the above-mentioned method.

5. DISCUSSION

With the continuous development of the IoV, more and more vehicles are connected to the network [13]. The degree of intellectualization and networking of the IoV is constantly improving. The IoV can quickly obtain real-time traffic information through the Internet, share data, allocate road resources reasonably, improve traffic

Table 3. Influence of the number of vehicles on the average time delay

Number of vehicles/n	25	50	75	100	125	150
Average time delay of SPECS/s	0.033	0.048	0.051	0.068	0.073	0.112
Average time delay of b-SPECS/s	0.035	0.047	0.052	0.069	0.072	0.114
Average time delay of the method proposed in this study	0.031	0.035	0.042	0.045	0.051	0.064

Table 4. Influence of vehicle speed on the average time delay

Speed of vehicle (m/s)	0	5	10	15	20	25
Average time delay of SPECS/s	0.071	0.072	0.072	0.073	0.074	0.075
Average time delay of b-SPECS/s	0.071	0.073	0.073	0.074	0.074	0.075
Average time delay of the method proposed in this study/s	0.051	0.052	0.052	0.053	0.055	0.055

conditions [14], and effectively avoid traffic jams through traffic light regulation. However, due to the mobility, openness and complexity of the IoV, its information security problem is becoming ever more serious [15]. Moreover, the information security issue will not only incur loss of information and property but will also endanger people's lives. Therefore, the study of the information security of IoV has important practical values. Public key cryptography plays a crucial role in information security [16]. Elliptic curve cryptography is one of the public key cryptographies [17] which has been applied in many fields [18]. For example, in the smartphone network, elliptic curve cryptography can realize secure communication with limited resources [19]; in the electronic payment system, elliptic curve cryptography can encrypt through identity authentication to improve the security of payment [20]. Compared with these applications, the complexity and openness of the IoV set higher requirements for encryption. Therefore, the application of elliptic curve cryptography in the IoV is more challenging. In this study, elliptic curve cryptography was applied to the authentication of IoV communication nodes, which provides a safe and efficient authentication scheme for the IoV, is conducive to the large-scale application of the IoV, and can play a role in dispersing traffic and reducing traffic accidents.

The security authentication of communication nodes is mainly designed for vehicle nodes. It is difficult to authenticate vehicles as vehicles are in a state of high-speed movement in the network. Among the commonly used current authentication technologies, such as anonymous authentication, group signature authentication and so on, the time cost of the algorithm is a major difficulty. Therefore, in the design of the authentication scheme it is necessary to reduce the time cost as much as possible. First, elliptic curve cryptography is analysed, then it is applied to the identity authentication of IoV communication nodes, i.e. vehicle nodes, and finally the processes of system establishment, pseudonym generation and message verification are analysed. The results show that the authentication scheme designed in this paper can pass the correctness analysis and the message verification formula is valid. As regards the comparison of computing time, there is no significant difference in the signature generation time among the three methods. However, the computing time for signature verification by the method proposed in this study is significantly shorter than that of SPECS and b-SPECS, which proves the advantage of that method in computing time and shows that it produces faster computing compared to the other two methods. Therefore, the presented method has a greater advantage in the authentication of IoV communication nodes and can better meet the actual needs of the IoV. The analysis results of authentication time delay (Tables 3 and 4) reveal that the authentication time delay of the proposed method is always smaller than that of SPECS and b-SPECS with the change in the vehicle number and speed, which proves the reliability of the method.

Though the study of IoV communication nodes has some achievements, further study is still needed, particularly in the following aspects:

(1) RSU nodes need further optimization;
(2) The authentication mechanism requires further study to reduce encryption and decryption steps, and a more efficient authentication scheme should be searched for;
(3) Application in real IoV environment.

6. CONCLUSIONS

In view of the current information security problem of the IoV, this study has mainly analysed the authentication mechanism of communication nodes, applied the elliptic curve cryptography method to the IoV, introduced its authentication process, and made a performance analysis. It was established that the method proposed in this study could meet the correctness criterion, had low time cost, and could maintain a small time delay in the case of a large number of vehicles and high vehicle speed. The results of the performance analysis have verified the reliability of elliptic curve cryptography in communication node authentication. Therefore, it can be popularized and applied in practice.

ACKNOWLEDGEMENT

The publication costs of this article were partially covered by the Estonian Academy of Sciences.

REFERENCES

1. Punitha, A. and Manickam, J. M. L. Privacy preservation and authentication on secure geographical routing in VANET. *J. Exp. Theor. Artif. Intell*., 2017, **29**(3), 617–628.
2. Zhang, W. and Xi, X. The innovation and development of Internet of Vehicles. *China Commun*., 2016, **13**, 122–127.
3. Vijayakumara, P., Chang, V., Deborah, L. J., Balusamy, B., and Shynu, P. G. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. *Future Gener. Comput. Syst*., 2018, **78**(3), 943–955.
4. Cirne, P., Zúquete, A., and Sargento, S. TROPHY: Trustworthy VANET routing with group authentication keys. *Ad Hoc Netw*., 2018, **71**, 45–67.
5. Cheng, S., Zhang, M. Y., and Peng, W. P. Efficient pairing-based batch anonymous authentication scheme for VANET. *J. China Univ. Posts Telecommun*., 2018, **25**, 85–94.
6. Wang, F., Xu, Y. J., Zhang, H., Zhang, Y. J., and Zhu, L. 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. *IEEE* Trans. Veh. Technol., 2016, **65**(2), 896–911.
7. Wang, M. Z., Liu, D., Zhu, L. H., Xu, Y. J., and Wang, F. LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication. *Computing*, 2016, **98**, 685–708.
8. Zhou, A., Li, J., Sun, Q., Fan, C., Lei, T., and Yang, F. C. A security authentication method based on trust evaluation in VANETs. *EURASIP J. Wirel. Comm. Netw*., 2015, **2015**, 59.
9. Sun, Y. C., Wu, L., Wu, S. Z., Li, S. P., Zhang, T., Zhang, L., et al. Attacks and countermeasures in the internet of vehicles. *Ann. Telecommun*., 2017, **72**, 283–295.
10. Ruan, N., Li, M. Y., and Li, J. A novel broadcast authentication protocol for internet of vehicles. *Peer Peer Netw. Appl*., 2017, **10**, 1331–1343.
11. Chim, T. W., Yiu, S. M., Hui, L. C. K., and Li, V. O. K. SPECS: Secure and privacy enhancing communications schemes for VANETs. *Ad Hoc Netw*., 2011, **9**(2), 189–203.
12. Horng, S. J., Tzeng, S. F., Pan, Y., Fan, P. Z., Wang, X. M., Li, T. R., et al. b-SPECS+: Batch verification for secure pseudonymous authentication in VANET. *IEEE Trans. Inf. Forensics Secur*., 2013, **8**(11), 1860–1875.
13. Guo, L. H., Dong, M. X., Ota, K., Li, Q., Ye, T. P., Wu, J., et al. A secure mechanism for big data collection in large scale Internet of Vehicle. *IEEE Internet Things J*., 2017, **4**(2), 601–610.
14. Wu, H. T. and Horng, G. J. Establishing an intelligent transportation system with a network security mechanism in an Internet of Vehicle environment. *IEEE Access*, 2017, **5**, 19239–19247.
15. Zhong, H., Wen, J. Y., Cui, J., and Zhang, S. Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET. *Tsinghua Sci. Technol*., 2016, **21**(6), 620–629.
16. Pandey, J. G., Mitharwal, C., and Karmakar, A. An RNS implementation of the elliptic curve cryptography for IoT security. In *Proceedings of the 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), December 12–14, 2019, Los Angeles, CA, USA*. IEEE, 2020, 66–72.
17. Chandrasekher, A., Scholar, P. G., and Vanaja, R. Single sign-on in distributed networks using elliptic curve cryptography. *Int. J. Appl. Eng. Res*., 2019, **10**(70), 206–215.
18. Bayat, M., Atashgah, M. B., Barari, M., and Aref, M. R. Cryptanalysis and improvement of a user authentication scheme for Internet of Things using elliptic curve cryptography. *Int. J. Netw. Secur*., 2019, **21**(6), 897–911.
19. Fujdiak, R., Masek, P., Hosek, J., Mlynek, P., and Misurec, J. Efficiency evaluation of different types of cryptography curves on low-power devices. In *Proceedings of the 2015 7th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), October 6–8, 2015, Brno, Czech Republic.* IEEE, 2016, 269–274.
20. Kumar, R., Pal, S. K., and Yadav, A. Elliptic curve based authenticated encryption scheme and its application for electronic payment system. *Int. J. Comput. Sci. Math*., 2018, **9**(1), 90.

Sõidukite Interneti infoturbepõhine kommunikatsioonisõlmede autentimismehhanism

Qiong Wu

On keskendutud Sõidukite Interneti (IoV) kommunikatsioonisõlmede autentimismehhanismile. Elliptiliste kõverate krüptosüsteemil põhinedes on välja töötatud autentimismeetod; tutvustatud süsteemi rajamise, pseudonüümi loomise ja sõnumite autentimise protsesse ning analüüsitud süsteemi ohutust. Tulemused näitavad, et pakutud meetod on läbinud õigsuse kontrolli ja SPECS-i ja b-SPECS-iga võrreldes on sellel ajakulude ning autentimise viivituse osas olulised eelised. Eksperimentaalsed tulemused kinnitavad meetodi usaldusväärsust, mis annab teatava panuse IoV kommunikatsioonisõlmede autentimisse ja on kasulik infoturbe edasiseks parandamiseks.