Unified Identity Authentication Based on D-S Evidence Theory

Jiawei Wang[1], Zhenjiang Zhang[2], Shih-Chen Wang[3], Sheng-Lung Peng[3], Yuqun Rui[4]

[1] School of Electronic and Information Engineering, Key Laboratory of Communication and Information Systems, Beijing Jiaotong University, China
[2] School of Software Engineering, Beijing Jiaotong University, China
[3] Department of Computer Science and Information Engineering, National Dong Hwa University, Taiwan
[4] Jingyou International Information Technology (Beijing) Co. LTD, China
18120131@bjtu.edu.cn, zhangzhenjiang@bjtu.edu.cn, 810621002@ndhu.edu.tw, slpeng@ndhu.edu.tw, ruiyuqun@jingyougroup.com

Abstract

Nowadays, the number of cases that executed cooperation with others in the world is increasing. Some major cases and some cases that are connected with several areas are settled in several courts. For the particularity of this kind of cases, coordinated command across regions and levels should play a more important role. Under this background, every law enforcer should be able to be authenticated anytime and anywhere, and can access to the system easily. In this case, establishing a kind of unified identity authentication is essential. This paper come up with a unified identity authentication based on D-S evidence theory, merging several kinds of authentication methods to complete the identity authentication.

Keywords: Unified identity authentication, Data fusion, D-S evidence theory

1 Introduction

Integrated coordinated command can bring great benefits on both economic and society. Through multi-cooperation, the command center can command the law enforcers dynamically and momentarily all over the country, to deal with the emergency. The enforcers do not need to travel back and forth, which saves both labor and the materiel, saves the time cost of the law enforcers, improves efficiency of enforcing at the scene, and also creates economic benefits indirectly.

Under the background of integrated coordinated, the law enforcers not only need to work indoor in the court, but also go to the scene, to finish the work of recording, collecting evidence, and then send the data back to the command center. In this mode of enforcement, every law enforcer should be able to access to the system easily. And it can make sure that all of the law enforcers can connect with the internal network to send data back and reply information, no matter where he is, in the court, in the scene, or in other courts.

At present, in the process of enforcement, only one main authentication mode is used, that all the people can only be authenticated in a certain way. And the account password authentication is used mainly. The single authentication greatly restricts the convenience and flexibility of working out. Especially in some environment that using account password is not very convenient. At this moment, other authentication methods, such as fingerprint authentication, can play an important role.

Based on the fact that multiple access modes can be used at the same time, the newly established unified identity authentication can implement the following functions. The same user, no matter in which way accessing into the system, he can log in to his account successfully, and can connect to the internal network to finish the work.

Under the unified identity authentication system, the enforces can be authenticated successfully in various ways, such as the account password, the fingerprint, and the USB key, to complete the unified identity authentication. All of these authentication methods above have advantages. However, they can make up for each other in terms of features and applications.

In such a single-point scenario, the unified identity authentication approach can be used smoothly. In addition, this authentication can also be used in the edge computing scenario in [1] and [2].

2 System Model

The process of identification is also the process of determining whether a user is legal. The most ordinary authentication method is the account password authentication. Some other complex authentications are also used. The users are authenticated by some other information, such as the fingerprint.

*Corresponding Author: Zhenjiang Zhang; E-mail: zhangzhenjiang@bjtu.edu.cn
DOI: 10.3966/160792642020032102021

For the convenience of authentication, a unified identity authentication is needed. Under the unified identity authentication, a user can be authenticated by any kind of method, and then can access to the system and get all the data he has.

The unified identity authentication needed should meet the following requirements. Every user decides his authentication by the environment he is in. No matter which one he chooses, he can be authenticated by the system, and can access it. Every authentication method has a same database, that has all the information a user has.

At present, there are three main kinds of authentication, the account password authentication, the fingerprint authentication, and the USB key authentication.

This paper comes up with a unified identity authentication based on D-S evidence theory. Figure 1 shows the schematic diagram of unified identity authentication [3-4]. A simple introduction of these authentication methods and the applications is given in the following subsections.

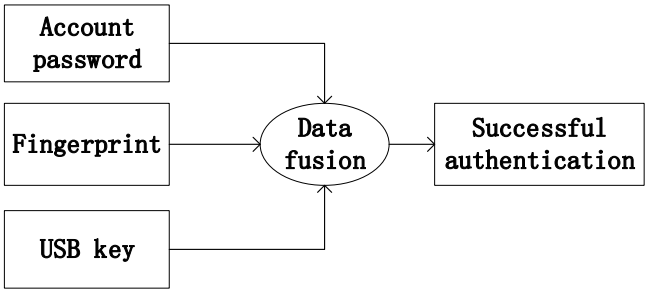

Figure 1. Schematic diagram of unified identity authentication

2.1 The Account Password Authentication

In an account password authentication, users perform the authentication by entering account password. In our unified identity authentication, the account password authentication is the most basic one. This authentication method can be used on the APP of mobile terminal, or the authentication on the website. Because of its simplicity and no need for any extra equipment, the account password authentication can be done with the lowest price. This is also the reason why the account password authentication is the most widely used one.

However, in the progress of working out sometimes, there may be some limitations. For example, the forgotten of password is possible. And in some occasions, it may be not very convenient to enter account and password. For these problems, some other authentications are needed [5].

2.2 The Fingerprint Authentication

Biological characteristics are unique and we can use them to identify individuals by identifying their physiological characteristics. Based on these characteristics, some technologies such as fingerprint identification, face identification are being used.

The biological identification technology has many advantages that the traditional identification methods cannot match. With the biological identification, the identity and attribute can be quickly identified, and the password is no longer used. It is more convenient.

Among these mentioned technologies, fingerprint authentication is most widely used now, and it has a broad prospect. At present, it is widely used in unlocking mobile phones, unlocking entrance guard and other fields [6].

For its feature of convenience, easily getting, and easily carrying, the fingerprint authentication can combine with wearable devices, playing an important role in assisting working. The fingerprint sensor is put on a wearable device, and is carried with the law enforce for authentication. When it is necessary to access to the system for some operations, the law enforces can be authenticated by the fingerprint authentication directly. With the direct authentication on the wearable devices, the law enforces do not have to enter their account and password in some inconvenient occasions. Meanwhile, the time that is saved can speed up the handling of cases and improve work efficiency greatly.

However, there are also some conditions that the fingerprint authentication is failed. When the law enforcers are working outside, there are some conditions that the finger is dirty or the fingerprint is out of shape. In this case, the fingerprint sensor cannot identify the fingerprint, which will cause the authentication failed.

2.3 The USB Key Authentication

The USB key, is a kind of little storage device, which can connect with the computer directly, and has a function of authentication. It is a great supplement of the existing network security system. The main feature of the USB key is high security, consistent technical specifications, good compatibility of operating system, and flexible using. Meanwhile, the operation with the USB key cannot be changed or denied [7].

In the unified identity authentication proposed in the paper, the USB key is an important one. It is a great supplement to the account password authentication. When using the USB key, the identity of a user and the USB key of his own can be ensured matched. With the USB, the security is guaranteed. And in the working of law enforces, there may be some data, that should be operated by some people of some certain status, and the process must be safe enough, and the USB key is a good thing to do it. It must be the one who owns the USB key and has the password of himself, can operate on the client, which achieve the goal of matching the users and the equipment.

On the other hand, the USB key authentication also

has some problems. The software is essential on the computer, and the USB key should be used with the computer too. In addition, as a hardware device, the USB key may break down. And the independent USB key should be carried with the user, which also brings inconvenience. For these reasons, the USB key is not suitable for general occasions.

3 Related Work

3.1 Methods of Unified Identity Authentication

With the development of the network, more systems and functions are produced. In order to ensure the system can work safely, it needs to be authenticated in an appropriate way. At the same time, more systems are accompanied by more and more complex security authentication. Combining various authentication methods to get a unified identity authentication will bring greater convenience to the use of the system. At present, there are several kinds of unified identity authentication methods being used in many fields.

It proposes a kind of management system of unified identity based on SAML (Security Assertion Markup Language) in [8], and it also explains the main points of the unified authentication module and the single sign-on module of the system. A CPK-based (Combined Public Key) unified identity management method for the remote access user's identity is proposed in [9], and it can improve the security and manageability of secure remote access system. A newly designed plan for unified identity authentication based on university website portals is proposed in [10], and it is possible for different sections to share data effectively with this method. In [11] a unified desktop cloud-based authentication architecture is proposed based on the traditional single sign-on authentication technology and desktop cloud. In [12] it proposes a new interaction mode of indirect authentication exchange, to unify network access authentication with application level Single Sign-On (SSO) as an integrated one-step authentication and the system can be more easily and flexibly deployed and maintained. In [13] it presents an IFF identity authentication scheme of security and guarantee system based on elliptic curve encryption, and the scheme is suitable for the identification of the light weight mobile terminal in infinite network environment, which has the characteristics of high security, high efficiency and bandwidth saving. In [14] it presents a new design of bidirectional identity authentication solution which combines PKI (Public Key Infrastructure) with fingerprint features, provides the concrete structure of it and certification process, and this solution better overcomes security flaws in traditional authentication and improves the reliability of identity authentication. In [15] it proposes an efficient hash-based RFID grouping authentication protocol to provide missing tags detection.

3.2 The Content and Fusion Process of D-S Evidence Theory

D-S evidence theory is a commonly used data fusion technology, and it is come up in the 1960s by Dempster and Shafer. It is a theory of dealing with the uncertainty. The core of D-S evidence theory is the fusion rule that it fuses multiple objects. And the objects can be the predictions of different people, the data of different sensors, and so on.

Following is the advantage of D-S evidence theory. The priori data are easily to get. It does not need to meet the additivity of probability. It has ability of expressing the uncertainty directly, and these information is showed in the mass function and is kept during the process of evidence fusion [16-17].

Several basic concepts in the evidence theory are described as follows. Frame of identification is the range of the event that we need to judge. Basic Probability Assignment is also called BPA. It is the probability of each event in the basic framework from each people or each sensor. And the sum of the probabilities from all of the people or sensor is 1. Usually, the probability is called the mass function. The belief function of an event is the sum of all the probabilities of the event's subsets, and it is used to show the degree of trust of the event. Plausibility function of an event is the sum of all the probabilities of the condition that is intersected with it, and it is used to show the degree of trust of not denying the event.

The following is the Dempster combination rule of mass functions.

$$\begin{aligned}&(m_1 \oplus m_2 \oplus \cdots \oplus m_n)(A)\\&= \frac{1}{K} \sum_{A_1 \cap \cdots \cap A_n = A} m_1(A_1) * m_2(A_2) \cdots m_n(A_n)\end{aligned} \tag{1}$$

In the formula, K is called the normalization factor. And $1-K$ reflects the conflict of the evidence.

$$\begin{aligned}K &= \sum_{A_1 \cap \cdots \cap A_n \neq \varnothing} m_1(A_1) * m_2(A_2) \cdots m_n(A_n)\\&= 1 - \sum_{A_1 \cap \cdots \cap A_n = \varnothing} m_1(A_1) * m_2(A_2) \cdots m_n(A_n)\end{aligned} \tag{2}$$

After the fusion of every evidence, the following is a judgement rule.

Here, both A_1 and A_2 are the subsets of U, and the result meets

$$\begin{cases} m(A_1) = \max\{m(A_i),\ A_i \subset U\} \\ m(A_2) = \max\{m(A_i),\ A_i \subset U \text{且} A_i \neq A_1\} \end{cases} \tag{3}$$

If the following conditions hold,

$$\begin{cases} m(A_1) - m(A_2) > \varepsilon_1 \\ m(\Theta) < \varepsilon_2 \\ m(A_1) > m(\Theta) \end{cases} \quad (4)$$

then A_1 is judged as the result. Among the formula, ε_1 and ε_2 are two thresholds, and Θ is the uncertain set.

4 Progress of Fusion

4.1 Basic Probability Assignment

In the process of authentication, there are several methods such as the account, the fingerprint, and the USB key. And the first thing to do is to fuse these methods. In the process of fusing, the major problem is the basic probability assignment, which is the key of data fusion through the method of D-S evidence theory. Normally, the basic probability assignment should be determined by the actual situation.

The following is several commonly used methods to get the basic probability assignment. Determining the coefficient is according to the target type, according to the statistical data, according to the target identity, and according to the previous experience [18-19].

As mentioned above, the main difference between every kind of authentication is the frequency of using. On the App, on the client, or on the website, the account password method is widely used in these scenes. The fingerprint method is good for using outdoor, such as using on the wearable devices. And the USB key, which can provide a safe environment for the login and the next operation is used for some confidential processes.

In addition, another feature to distinguish between various ways is the success rate of authentication. Each of the above three ways of identity authentication exists some conditions that cannot be used. And all of these several kinds of accidents may cause a failure of authentication.

Thus, we combine the frequency of usage and the probability of the authentication success together, and regard the result as the basic probability assignment. We take the probability of the authentication success as the parameter, and set a weight for each parameter, which is the frequency of using each method.

Let us take the account password authentication as an example. Set the frequency of usage to f_1, the probability of the authentication success is s_1. Thus, the parameter of this kind of authentication is as follows:

$$P_1 = f_1 * s_1 \quad (5)$$

That means the probability of using the account password authentication and getting authentication successfully is P_1. Similarly, the parameters of the fingerprint and the USB key authentication are as follows:

$$P_2 = f_2 * s_2 \quad (6)$$

And

$$P_3 = f_3 * s_3 \quad (7)$$

Table 1 shows the result of the probability of the evidence.

Table 1. The probability of the evidence

The result	Account password (1)	Fingerprint (2)	USB key (3)
Authentication success (A)	P_1	P_2	P_3
Authentication failure (B)	1 - P_1	1 - P_2	1 - P_3

4.2 The Progress of Fusion

The progress of fusion is shown in Table 2.

Table 2. The progress of fusion

The progress of fusion
Get parameters of the three kinds of authentication. Calculate the normalization coefficient *K*.
Calculate the mass function of authentication success *m*(*A*).
Calculate the mass function of authentication failure *m*(*B*).
Get the final result by comparing *m*(*A*), *m*(*B*) and the threshold value. Get the result after judging.

4.3 The Result of Fusion

By applying the steps of Table 2, we can get some useful results. The normalization coefficient K is shown in the formula (8).

$$\begin{aligned} K &= \sum_{A_1 \cap A_2 \cap A_3 \neq \varnothing} m_1(A_1) * m_2(A_2) * m_3(A_3) \\ &= P_1 * P_2 * P_3 + (1 - P_1) * (1 - P_2) * (1 - P_3) \\ &= (f_1 * s_1) * (f_2 * s_2) * (f_3 * s_3) \\ &\quad + [1 - (f_1 * s_1)] * [1 - (f_2 * s_2)] * [1 - (f_3 * s_3)] \end{aligned} \quad (8)$$

The mass function of authentication success $m(A)$ is shown in the formula (9).

$$\begin{aligned} m(A) &= m_1 \oplus m_2 \oplus m_3(A) \\ &= \frac{1}{K} \sum_{A_1 \cap A_2 \cap A_3 = A} m_1(A_1) * m_2(A_2) * m_3(A_3) \\ &= \frac{P_1 * P_2 * P_3}{P_1 * P_2 * P_3 + (1 - P_1) * (1 - P_2) * (1 - P_3)} \\ &= \frac{(f_1 * s_1) * (f_2 * s_2) * (f_3 * s_3)}{(f_1 * s_1) * (f_2 * s_2) * (f_3 * s_3) + [1 - (f_1 * s_1)] * [1 - (f_2 * s_2)] * [1 - (f_3 * s_3)]} \end{aligned} \quad (9)$$

The mass function of authentication failure $m(B)$ is

shown in the formula (10).

$$\begin{aligned} m(B) &= m_1 \oplus m_2 \oplus m_3(B) \\ &= \frac{1}{K}\sum_{B_1\cap B_2\cap B_3=B} m_1(B_1)*m_2(B_2)*m_3(B_3) \\ &= \frac{(1-P_1)*(1-P_2)*(1-P_3)}{P_1*P_2*P_3+(1-P_1)*(1-P_2)*(1-P_3)} \\ &= \frac{[1-(f_1*s_1)]*[1-(f_2*s_2)]*[1-(f_3*s_3)]}{\left\{\begin{array}{l}(f_1*s_1)*(f_2*s_2)*(f_3*s_3)\\ +[1-(f_1*s_1)]*[1-(f_2*s_2)]*[1-(f_3*s_3)]\end{array}\right\}} \end{aligned} \quad (10)$$

Judge $m(A)$ and $m(B)$.

If

$$\begin{cases} \mathrm{m}(\mathrm{A})-\mathrm{m}(\mathrm{B})>\varepsilon_1 \\ \mathrm{m}(\Theta)<\varepsilon_2 \\ \mathrm{m}(\mathrm{A})>\mathrm{m}(\Theta) \end{cases} \quad (11)$$

then the authentication is successful. Otherwise, it fails. In the formula, ε_1, ε_2 are the thresholds, and Θ is the uncertain set.

5 The Experimental Results

In this section, an example is given to compare the unified identity authentication with the other three. Assume that the frequencies of using the three methods are 90%, 80%, and 70%, respectively, and the probabilities of the authentication success are 70%, 80%, and 90%, respectively.

So f_1=90%, f_2=80%, and f_3=70%. Similarly, s_1=70%, s_2=80%, and s_3=90%.

From formula (5), (6) and (7), we can get the result of the probabilities that P_1 is 63%, P_2 is 64%, and P_3 is 63%.

The basic probability assignment is calculated as follows. Here the mass value of account password is 63%, the mass value of fingerprint is 64%, and the mass value of USB key is 63%. It can be expressed as $m_1(A_1)$=63%, $m_2(A_2)$=64%, and $m_3(A_3)$=63%.

The result is shown in Table 3. It shows the probability of successful authentication with all of the three methods mentioned above together and the probability of successful authentication with only one of them.

Table 3. The result of the authentication

The result	Without account password	Without fingerprint	Without USB key
Account password	None	63%	63%
Fingerprint	64%	None	64%
USB key	63%	63%	None
Unified identity authentication	75.2%	74.4%	75.2%

From the result above, we can get that the result of the unified identity authentication has the highest probability comparing with the other methods. Thus it is the best method of authentication.

To get the relationship between the result of the authentication and the change of three probabilities, we select one of the probability and fix the value of the other two to get the graph of mass function of authentication success and authentication failure changing with a single one.

First, we keep P_2 and P_3 the same, and both P_2 and P_3 are 0.4. Then we change P_1 from 0.2 to 0.7, and the graph is shown in Figure 2. In the figure, the red one is $m(A)$, and the blue one is $m(B)$. From the last part, we can get that $m(A)$ is the mass function of authentication success, and $m(B)$ is the mass function of authentication failure. If we choose the bigger one as the server of the task, then we can see that in this range that usually used, $m(A)$ is always bigger than $m(B)$, and the authentication can always be succeed.

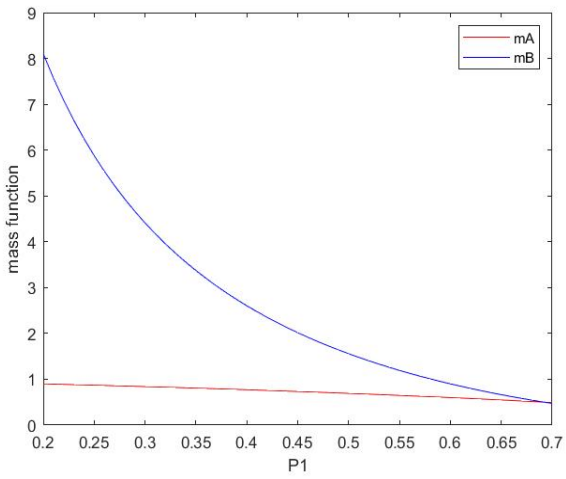

Figure 2. Graph of P_1 and mass function

Then, we change P_2 from 0.2 to 0.7 respectively and keep P_1=0.5 and P_3=0.4, and change P_3 from 0.2 to 0.7 respectively and keep and P_1=0.5, P_2=0.3. We can get the two graphs shown as Figure 3 and Figure 4, respectively. By Figure 3, we can see that when P_2 is less than 0.6, $m(A)$ is bigger than $m(B)$, and the authentication is successful, while P_2 is bigger than 0.6, the authentication is failure. In the actual scenario, due to the low frequency of use of the second method, the coefficient P_2 is usually less than 0.5, and it hardly exists a large coefficient. Therefore, we can consider that the authentication is successful within its normal working range. And it is the same for P_3 in Figure 4. We can think that in the normal working range, the authentication is always successful.

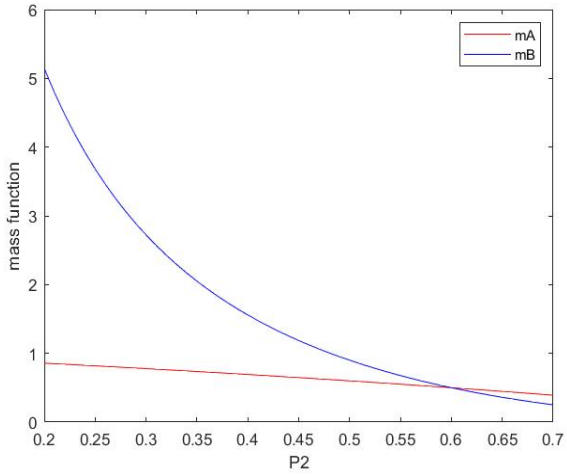

Figure 3. Graph of P_2 and mass function

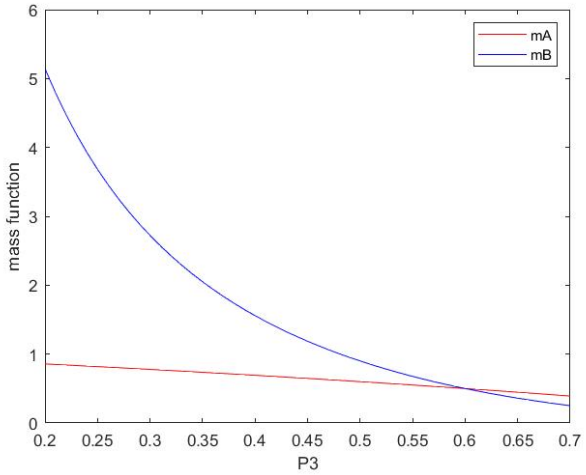

Figure 4. Graph of P_3 and mass function

6 Future Prospects

From the result of the experiment, the unified identity authentication in the paper is a good complement to the single identity authentication in existence. The scheme in the paper is based on the D-S evidence theory, and it fuses three different authentications: the account password, the fingerprint, and the USB key. Through the probabilities that the authentication of these three methods is successful, the mass functions of success and failure are counted separately. And the result of unified identity authentication is got by a further judgment.

The unified identity authentication makes the law enforces be more convenient in the process of handling cases, and be not affected by environment and surrounding conditions. They can use the more suitable authentication, which can greatly improve the efficiency of case handling. Besides, it plays an important role in the process of coordinate case handling.

For the unified identity authentication method, a prospect of future research is as follows. More single-point authentications can be involved. The three authentication methods used in this paper are simple and common authentication methods. Although they can meet the used requirements in most scenarios, there are still some specific scenarios and special needs that require the addition of other authentication methods. For example, when a method of authentication is very confidential and it is used in large quantities, the coefficient will be very large in the calculation process. At this time, the unified identity authentication method based on D-S evidence theory proposed in this paper will be invalid. Therefore, a more optimized and improved data fusion mode is needed to meet the usage requirements in more scenarios.

Acknowledgements

This work is supported by The National Key R&D Program of China (2018YFC0831900), the research on Intelligent Assistive Technology in the Context of Judicial Process Involving Concerned Civil and Commercial Cases.

References

[1] W. Zhang, Z. Zhang, S. Zeadally, H. Chao, V. C. M. Leung, MASM: A Multiple-algorithm Service Model for Energy-delay Optimization in Edge Artificial Intelligence, *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 7, pp. 4216-4224, July, 2019.

[2] Z. Zhang, W. Zhang, F.-H. Tseng, Satellite Mobile Edge Computing: Improving QoS of High-speed Satellite-terrestrial Networks Using Edge Computing Techniques, *IEEE Network*, Vol. 33, No. 1, pp. 70-76, January, 2019.

[3] Y. Yang, The Design of Unified Identity Authentication and Single Point Login System, *Applied Mechanics and Materials*, Vol. 391, pp. 155-156, February, 2012.

[4] H. Wang, C. Gong, Design and Implementation of Unified Identity Authentication Service Based on AD, *2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)*, Tehri, 2016, pp. 394-398.

[5] T. Acar, M. Belenkiy, A. Küpçü, Single password Authentication, *Computer Networks*, Vol. 57, No. 13, pp. 2597-2614, September, 2013.

[6] C. Yuan, X. Sun, Fingerprint Liveness Detection Using Histogram of Oriented Gradient Based Texture Feature, *Journal of Internet Technology*, Vol. 19, No. 5, pp. 1499-1507, September, 2018.

[7] J. Yu, The Program Design for the Network Security Authentication Based on the USB Key Technology, *Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology*, Harbin, 2011, pp. 2215-2218.

[8] Z. Tu, Q. Li, Design and Implementation of Unified Identity Management System Based on SAML, *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang, 2012, pp. 3178-3181.

[9] X. Li, CPK Unified Identity Based Secure Remote Access System for Mobile Terminal, *2012 Fifth International Symposium on Computational Intelligence and Design*, Hangzhou, 2012, pp. 493-496.

[10] W. Wang, S. Yuan, H. He, Design of Portal-Based Uniform Identity Authentication System in Campus Network, *2010 International Conference on Multimedia Communications*, Hong Kong, China, 2010, pp. 112-115.

[11] Y. Sun, X. Zou, Desktop Cloud-Based Research on Unified Authentication Architecture, *2012 Spring Congress on Engineering and Technology*, Xian, China, 2012, pp. 1-4.

[12] J. Jiang, H. Duan, T. Lin, F. Qin, H. Zhang, A Federated Identity Management System with Centralized Trust and Unified Single Sign-On, *2011 6th International ICST Conference on Communications and Networking in China (CHINACOM)*, Harbin, China, 2011, pp. 785-789.

[13] J. Deng, Y. Ren, Y. Li, An IFF Identity Authentication Scheme of Security and Guarantee System, *2017 IEEE 17th International Conference on Communication Technology (ICCT)*, Chengdu, China, 2017, pp. 1529-1532.

[14] X. Xie, H. Chen, H. Zhang, Y. Wu, P. Wu, New Design of Dual and Biderectional Identity Authentication System, *2010 International Conference on Optics, Photonics and Energy Engineering (OPEE)*, Wuhan, China, 2010, pp. 207-210.

[15] H. Tan, D. Choi, P. Kim, S. Pan, I. Chung, An Efficient Hash-based RFID Grouping Authentication Protocol Providing Missing Tags Detection, *Journal of Internet Technology*, Vol. 19, No. 2, pp. 481-488, March, 2018.

[16] W. Zhang, X. Ji, Y. Yang, Data Fusion Method Based on Improved D-S Evidence Theory, *2018 IEEE International Conference on Big Data and Smart Computing (BigComp)*, Shanghai, 2018, pp. 760-766.

[17] Y. Meng, L. Xu, J. Yi, Y. Wang, Evidence Fusion Algorithm Based on Correction Conflict, *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, Hangzhou, China, 2018, pp. 799-803.

[18] S. Mahadevan, Y. Deng, P. Xu, A New Method to Determine Basic Probability Assignment from Training Data, *Knowledge-Based Systems*, Vol. 46, pp. 69-80, 2013.

[19] W. Jiang, J. Zhan, D. Zhou, A Method to Determine Generalized Basic Probability Assignment in the Open World, *Mathematical Problems in Engineering*, Vol. 2016, pp. 1-11, 2016.

Biographies

Jiawei Wang received the bachelor's degree in the School of Electronic and Information Engineering, Beijing Jiaotong University in 2018. He is currently pursuing his master degree in communication engineering at the same university.

Zhenjiang Zhang, received the Ph.D. degree in communication and information systems from Beijing Jiaotong University (BJTU), Beijing, China, in 2008. He has been a Professor in the same university in 2014. He is currently served as the vice dean of School of Software Engineering in BJTU. Prof. Zhang has published about 70 professional research papers. His research interests include cognitive radio, communication protocols, and wireless sensor networks.

Shih-Chen Wang, technical director of Yesee International Information Technology (Taiwan) Co., Ltd., has been engaged in software-defined networking (SDN) product development and management for 7 years. He has been integrated in the field of artificial intelligence (AI) science and technology for the past 4 years.

Sheng-Lung Peng is a Professor of the Department of Computer Science and Information Engineering at National Dong Hwa University, Taiwan. He received the BS degree in Mathematics from National Tsing Hua University, and the M.S. and Ph.D. degrees in Computer Science from the National Chung Cheng University and National Tsing Hua University, Taiwan, respectively. He is an honorary Professor of Beijing Information Science and Technology University of China and a visiting Professor of Ningxia Institute of Science and Technology of China. His research interests are in designing and analyzing algorithms for Bioinformatics, Combinatorics, Data Mining, and Networks. He published over 100 international conferences and journal papers.

Yuqun Rui, technical director of Jingyou International Information Technology (Beijing) Co., Ltd., has been engaged in software product development and management for 14 years. He has been serving in the field of judicial science and technology for the past 5 years and has participated in the drafting of the industry standards of the People's Republic of China.