The Classic Security Application in M2M: the Authentication Scheme of Mobile Payment

Liang Hu[1], Ling Chi[1], Hong-tu Li[2], Wei Yuan[2], Yuyu Sun[2] and Jian-feng Chu[2]
[1] Software College, Jilin University, Changchun, China
E-mail: 164504108@qq.com
[2] College of Computer Science and Technology, Jilin University, Changchun, China
E-mail: chujf@jlu.edu.cn
*Corresponding author: Jian-feng Chu

Received August 29, 2011; revised December 13, 2011; accepted January 7, 2012; published January 31, 2012

Abstract

As one of the four basic technologies of IOT (Internet of Things), M2M technology whose advance could influence on the technology of Internet of Things has a rapid development. Mobile Payment is one of the most widespread applications in M2M. Due to applying wireless network in Mobile Payment, the security issues based on wireless network have to be solved. The technologies applied in solutions generally include two sorts, encryption mechanism and authentication mechanism, the focus in this paper is the authentication mechanism of Mobile Payment. In this paper, we consider that there are four vital things in the authentication mechanism of Mobile Payment: two-way authentication, re-authentication, roaming authentication and inside authentication. Two-way authentication is to make the mobile device and the center system trust each other, and two-way authentication is the foundation of the other three. Re-authentication is to re-establish the active communication after the mobile subscriber changes his point of attachment to the network. Inside authentication is to prevent the attacker from obtaining the privacy via attacking the mobile device if the attacker captures the mobile device. Roaming authentication is to prove the mobile subscriber's legitimate identity to the foreign agency when he roams into a foreign place, and roaming authentication can be regarded as the integration of the above three. After making a simulation of our proposed authentication mechanism and analyzing the existed schemes, we summarize that the authentication mechanism based on the mentioned above in this paper and the encryption mechanism establish the integrate security framework of Mobile Payment together. This makes the parties of Mobile Payment apply the services which Mobile Payment provides credibly.

Keywords: Authentication, mobile payment, M2M, security issues, wireless network

DOI :10.3837/tiis.2012.01.008

1. Introduction

As is known to all, the more rapidly the computer science develops, the more widely the internet spreads. The establishment of the internet requires a large number of computer terminals, hence there are a huge number of requirements of the cables, which give rise to a problem of the deployment of these computer terminals [1][2]. The deployment of the cables among the computer terminals limits that we have to reach the place where the computer terminal is, if we want to work on the network. It means that we cannot enjoy the services which computer terminals and the network provide anytime and anywhere. As a result, the wireless network was proposed and applied [3]. With the development of the wireless network, we have not satisfied with the network constituted by computer terminals, we wish that every machine could communicate with each other by the wireless network technology. This development trend leads to "machine-to-machine" communication, that we could call it "M2M" [4].

As is shown in **Fig. 1**, "M2M" is one of the four basic technologies of the IOT (Internet of Things) [5]. One of the "M" in "M2M" means the equipments with sensing capabilities and network capabilities; the other "M" means the intelligent applications and control system in various industries [6]. "M2M" technology is to achieve the human`s wish that establish the communication to communicate anytime and anywhere among "Man-to-Man", "Man-to-Machine", "Machine-to-Machine" [7]. Information infrastructures and physical infrastructure combine, then become intelligent by network, so that solve a series of problems such as "efficiency, security, cost" .etc.

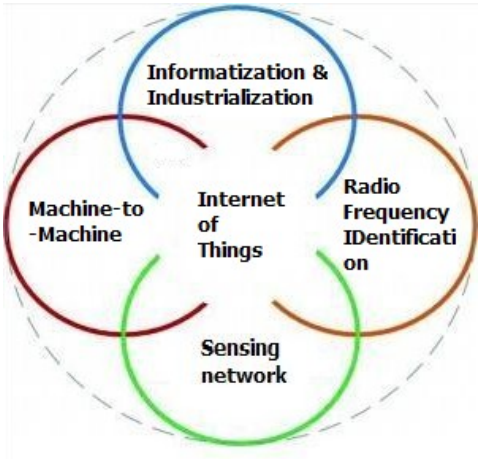

Fig. 1. The structure of Internet of Things

As is shown in As is shown in **Fig. 2**, the "M2M" industry is huge in this modern world, and the details of **Fig. 2** can be found in the reference [8]. In this paper, the main industry we discuss is Mobile Payment [9]. However, as a result of the wireless technical limitation, we can't ensure that the mobile device would not be cheated by the counterfeit center system, and we can't ensure that the privacy information would not be obtained completely, if the mobile device is captured [10]. Consequently, the solutions against the above problems are the prime discussions in this paper. One of the efficient solutions is authentication mechanism. The authentication mechanism in Mobile Payment includes: two-way authentication; roaming

authentication; re-authentication; inside authentication. The authentication mechanism based on the mentioned above in this paper and the encryption mechanism establish the integrate security framework of Mobile Payment together. This makes the parties of Mobile Payment apply the services which Mobile Payment provides credibly [11].

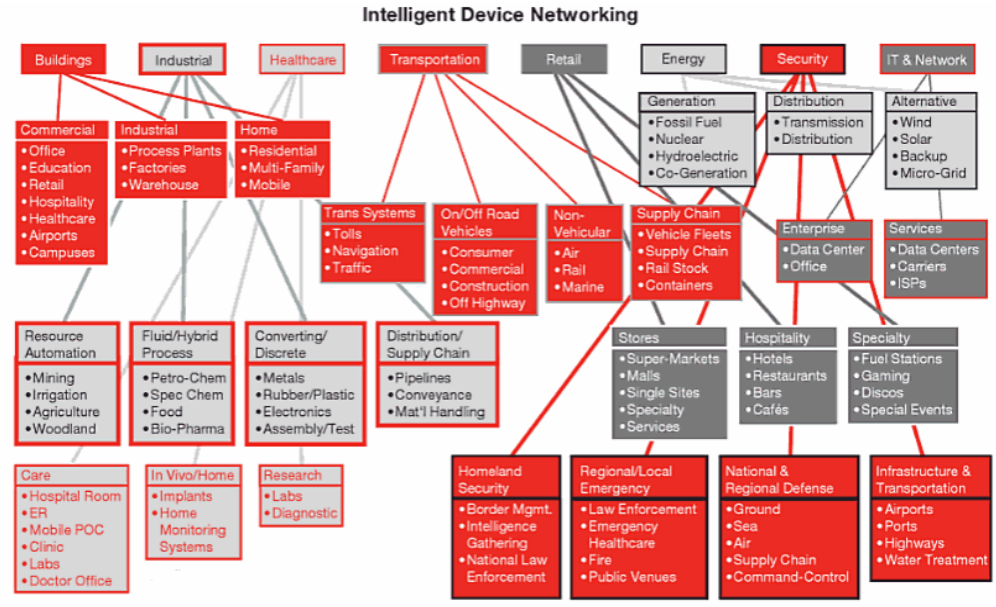

Fig. 2. The industies of M2M

2. Mobile Payment

With regard to Mobile Payment, we will think of the Point of Sales(POS machine) and Mobile Banking. But these applications are only the rudiment of the Mobile Payment actually. Mobile Payment doesn't only mean paying by mobile device when doing shopping, though it could achieve the same goal, the "mobile" in "Mobile Payment" is not same as the "mobile" in "mobile device". Also, mobile phone is not the only device of Mobile Payment, it is just a media, such as Personal Digital Assistant (PDA), Mobile terminal, Tablet PC .etc [12]. Indeed speaking, Mobile Payment describes a payment process, namely, any payment where a mobile device is used in order to initiate, activate, and/or confirm this payment can be considered a mobile payment. Obviously, Mobile Payment is a derivative of e-commerce. However, Mobile Payment possesses more advantages than e-commerce [13][14][15]: In e-commerce, commercial transactions carry out between human and human on multi-user machines, a task that eases anonymity and makes it difficult to provide services such as identification, security, and trust. In the mobile world this is different, as mobile devices are regarded as personal trust devices (PTD), which are generally considered to belong to, and be managed by, a single user, i.e. the owner [16][17][18].

A typical digital payment scenario is depicted in **Fig. 3** [19][20]. The customer is the party making the payment; the merchant is the party accepting the payment; the acquirer is the third party that has a relationship and interacts with the merchant; and the issuer is a third party that has a relationship and interacts with the customer. In any transaction the goal is the value transfer from the customer to the merchant. A typical procedure followed by credit card

companies is as follows. The customer "pays" a merchant for goods/services. Subsequently, the merchant sends the transaction details to the acquirer for clearing. The acquirer sends the transaction details to the financial network to which it belongs (e.g. VISA) which then forwards the details to the issuer. The issuer is informed to make the necessary fund reservation at the customer side. The scheme settles/pays the acquirer, the acquirer settles/pays the merchant, the issuer settles/pays the scheme, and the customer pays the issuer [21][22][23].

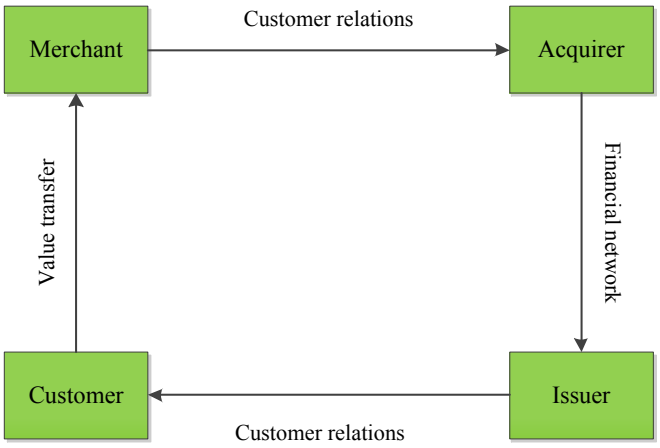

Fig. 3. A typical digital payment scenario

The main parties in the mobile payment mechanism are depicted in **Fig. 4** [24][25]: the customer (payer) and the merchant (payee). These transact with each other via the Mobile Payment process, whose main players also include the mobile network operators (MNO), the financial sector institutions (e.g. banks, credit card companies, payment processors), the government (legislation and regulation constraints), and, of course, the device, software, and service providers. There are many players in Mobile Payment, and the cooperation of the various players within such a framework is considered to be the key to success, while standalone efforts may have only limited local success [26][27].

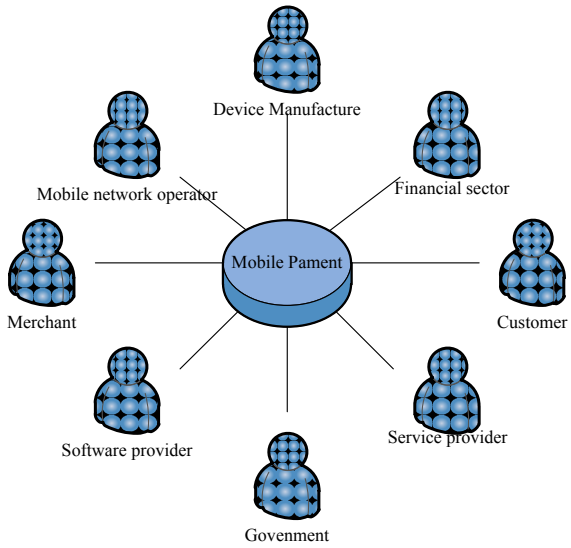

Fig. 4. The main parties in the mobile payment scheme

Generally speaking, the application field of the Mobile Payment is divided into two parts: inside application and outside application in Mobile Commerce. The Mobile Payment in inside application means: when a transaction is carrying out, at least, one of the two parties to the transaction has used electronic communications technology in transaction initiate, transaction service protocols and transaction submission process, namely, Mobile Payment is seen as an inherent payment of purchasing mobile service by the customers. On the other hand, the outside application in Mobile Payment means: the applications via Online shopping, Vending machine, Traditional stores and the transactions between person and person [28].

3. Why is authentication important in Mobile Payment?

"Mobile" in Mobile Payment means that wireless network service is the foundation of Mobile Payment, consequently, the security goals, security challenges, threats and attacks in wireless network also exist in Mobile Payment [29][30]. Further speaking, a mobile device used in Mobile Payment also could be regarded as a special sensor node, it means, the compromises the sensor node has also exist in the mobile devices used in Mobile Payment. However, the security goal we need to achieve is authentication, others are my focuses in this paper. Consequently, we will mainly discuss the threats and attacks.

Security issues mainly come from attacks. These attacks can be classified as external attacks and internal attacks. In an external attack, the attacker node is not an authorized participant of the sensor network. External attacks can further be divided into two categories: passive and active. Passive attacks involve unauthorized 'listening' to the routing packets. Active external attacks disrupt network functionality by introducing some denial-of-service (DoS) attacks [31], such as jamming, power exhaustion.

Node compromise is the major problem in sensor networks that leads to internal attacks. With node compromise, an adversary can perform an internal attack. Compared with external attacks, internal attacks are hard to be detected and prevented, thus raising more security challenges. Compromised nodes can do the following attacks:

(1) Compromised node can steal secrets from the encrypted data which passed it;

(2) Compromised node can report wrong information to the network;

(3) Compromised node can report other normal nodes as compromised nodes;

(4) Compromised node can breach routing by introducing many routing attacks, such as selective forwarding, black hole, modified the routing data, etc., while systems are hard to notice these activities, and normal encryption methods have no effect to prevent them because they own the secret information such as keys;

(5) Compromised nodes may exhibit arbitrary behavior and may collude with other compromised nodes.

The schemes against the security issues can be solved by the encryption in communication and authentication of the identity. Because of the characteristics of the wireless network, we cannot prevent the occurrence of the eavesdropping, it means, an attacker can acquire all the information the mobile device sends by eavesdropping. Therefore, the encryption [32][33][34] in communication is indispensable. In this paper, the encryption [35][36][37] in communication isn`t our principal task but the authentication of the identity.

4. Authentication mechanism in Mobile Payment

In the section above, we have discussed the security issues in Mobile Payment, as the conclusion we obtained, the compromises the sensor node has also exist in the mobile devices. Hence, the authentication mechanism in wireless sensor network is the same in Mobile payment. Before discussing the authentication in Mobile Payment, we will firstly explain the constraints in authentication. E.g. power consumption and key management constraints.

Power consumption constraints: The cryptographic algorithms used by security protocols have an important computational cost that must be taken into account and analyzed. Traditionally, it has been considered that the power and energy limitations of usual WSN nodes make the use of public-key cryptosystems impractical [38][39]. However, this situation has changed in last few years and recent studies show that public-key approaches are now feasible [40][41], even in Radio Frequency Identification (RFID) tags [42][43]. In any case, symmetric- key cryptography and hash functions are still between two and four orders of magnitude faster than digital signatures, in such a way that those procedures become, in our opinion, the most practical choice for protecting WSN communications.

Key management constraints: Despite several proposals that can be found in the specialized literature on the subject, to date the only practical option for the distribution of keys to sensor node in large-scale WSN is key pre-distribution [44][45]. According to this scheme, keys would have to be installed in sensor nodes during the manufacturing process. This approach offers two inadequate solutions: either a single mission key or a set of separate n-1 keys, each being pairwise privately shared with another node, must be installed in every sensor node. The single mission key solution is inadequate because the capture of any sensor node may compromise the entire network. On the other hand, the pairwise private sharing of keys requires pre-distribution and storage of n-1 keys in each sensor node, and n(n-1)/2 in the whole network, which renders it impractical for large-scale networks.

Hence, to overcome the above drawbacks, we have to construct an integrity and secure authentication system. An integrity authentication system consists of four parts: two-way authentication, re-authentication, roaming authentication and inside authentication. Basically, two-way authentication is the foundation of the other three parts; re-authentication is an

indispensable for the authentication system; inside authentication is different from re-authentication and roaming authentication, it is used to prevent the privacy data from being obtained by the illegitimate users; basing on the above three, roaming authentication is an important application for the wireless transmission of data. Additionally, considerring with the constraits above, an essential requirement is that the authentication system has to be light-weight [46].

4.1 The two-way authentication

As the foundition of all the authentication mechanisms, the two-way authentication need to be designed carefully. Then, before the designing, we have to pay attention to these threat models: (1) The WSN cannot prevent an attacker from eavesdropping the data mobile subscribers send; (2) The WSN cannot prevent the identity of the mobile subscriber`s security from being stolen by an attacker.

To resist the above threat models, a possible challenge-response authentication protocol is proposed as follows. An identity of each mobile subscriber is denoted by id, and $f()$ is a symmetric-key encryption function. Based on a random challenge r sent from the authentication server on the network side, the mobile subscriber sends its identity id and the response $f(k,r)$ to the authentication server, where k is a secret key of the mobile subscriber shared with the authentication server beforehand. The authentication server finds the mobile subscriber`s secret key k in a database, and completes the authentication to the mobile subscriber by verifying $f(k,r)$. The session key can be also generated from both the secret key and the random challenge. The advantage of this scheme is that the computation of $f()$ can be easily performed by the mobile subscriber having the low computational power. However, it is not easy to protect and maintain the database containing the secret keys of the mobile subscribers.

Then, for preventing the identity of the mobile subscriber`s security from being eavesdropped, the authentication between the mobile subscriber and the authentication server has to be anonymous. Anonymity in the wireless mobile communication environment is to maintain the confidentiality of mobile subscriber`s identity, namely to prevent an eavesdropper from discovering a correspondence between a mobile subscriber and a particular subscriber registered in a certain mobile network. Anonymity can be provided to the mobile subscribers through either assigning a kind of alias or encrypting the real identity. Global system for mobile communications (GSM) protects the identity of the mobile subscriber through an alias known as temporary mobile subscriber identity (TMSI). The mobile subscriber utilizes the TMSI instead of its real identity to access the mobile network. However, since a particular mobile subscriber`s movement can be traced if a fixed alias is used several times, the alias should be changed at each session to make it untraceable. Therefore, an additional message flow between the mobile subscriber and the authentication server is required to update the alias within the corresponding session. Usually, the new alias is exchanged after encrypted symmetrically with the session key established during the session. In case of encrypting the real identity of the mobile subscriber, either symmetric-key encryption or the public-key encryption can be employed. If the real identity is encrypted using the public key of the authentication server, the corresponding mobile subscriber can be identified through decryption with the private-key of the authentication server. On the other hand, a common session key should be first established between the mobile subscriber and the authentication server to encrypt the real identity symmetrically. In Cellular digital packet data (CDPD), the mobile subscriber`s real identity and authentication- related information are symmetrically encrypted with the session key derived from a Diffie–Hellman key exchange

protocol.

4.2 The re-authentication

The re-authentication is used to guarantee that the whole authentication system works validly. Due to plenty of applications working with real-time feature in the Mobile Payment [47][48], we may face such a threat model as follows: During the mobile subscriber moving out of the coverage of currently associated access point, and then, there is a latency involved in the process during which the mobile subscriber is unable to send or receive any kind of the information, as a result, the attacker can eavesdrop all the information the mobile subscriber sends or the attacker could pretend to be the legitimate mobile subscriber communicating with the center system.

To solve the above threat, the important challenge lies in reducing the time devoted to executing the network access control when mobile subscriber moves out of the coverage of currently associated access point. By decreasing this time, active communications can be re-established faster and therefore the perceived quality by the end-user can be significantly improved. Consequently, the recent literatures all proposed, that one important factor is the authentication process required by network operators in order to control that only legitimate users are able to employ the operator's resources, and this authentication we call re-authentication. Consequently, the primary goal is fast re-authentication so that the handover stays unnoticed by the user. As pointed out in the precious literatures, the overall handover latency should not exceed 50 ms [49].

4.3 Inside authentication

In the authentication system, inside authentication performs as a protector of the security of hardware layer. The threat models that the inside authentication has to face to is showed as follows: The attacker could capture the mobile device. Then he can obtain the privacy kept in the mobile device via force attack.

Because of the portability of the mobile device, preventing the mobile device from being captured is not effective. Therefore, adding the authentication mechanism into the mobile device is essential. Taking the computation and storage capability into account, preventing the mobile device from being attacked by force attack is not valid. Generally speaking, one of the practical method is adding access control phase into the mobile device as one of the authentication mechanisms. Access control gives different users different rights. For implementing the privacy-preserving validly, the user of mobile device only has the right of using the mobile device, he cannot have the right of querying the privacy data held in the mobile devise; the maintainer of the mobile device only has the right of querying privacy data held in mobile device, he cannot tamper these data. Even so, this authentication mechanism still cannot prevent the data from being obtained by force attack perfectly. Therefore, the previous literatures show: when the number of the failure of the authentication attempts reaches the limitation, the formatting of the storage of the mobile device or memory lockout will be carried out so that the attacker cannot obtain anything in the mobile device.

4.4 Roaming authentication

Basing on the above three, the roaming authentication is one of the most important applications. Generally speaking, the roaming authentication will face to these threat models: (1) When a mobile device roams into another foreign network, the mobile device could be deceived by a counterfeit network service provider; (2) When a mobile subscriber is carrying

out the identity authentication in a foreign network, his location and identity could be traceable by the attacker.

If a mobile device wants to use the network service when it roams into a foreign network, the mobile device has to access the foreign agency. Then, a security challenge appears, the mobile device has to prove its legitimate identity to the foreign agency. In the previous literatures, challenge has been solved by Message Authentication Code (MAC) and timestamp, and these literatures show an authentication model: (1) If the MAC is identified to be correct and the timestamp is identified to be valid, the home agency would trust in the mobile device; (2) If the MAC is identified to be correct and the timestamp is identified to be valid, the home agency would trust in foreign agency; (3) If the MAC is identified to be correct and the timestamp is identified to be valid, the foreign agency would trust in home agency; (4) If foreign agency trusts in home agency and home agency trusts in mobile device, foreign agency would trust in mobile device; (5) If the timestamp is identified to be valid, mobile device would trust in foreign agency. The general process shows in **Fig. 5** as follows.

In the whole authentication process, another important issue is to ensure that the mobile device, foreign agency and home agency are anonymous. In this way, the attacker could not trace the identity and location by eavesdropping.

We summarized the popular schemes used for wireless roaming authentication to prove that our proposed classic execution process of roaming authentication is right. Also, we have maken a comparation of these schemes and a table to show the performance of these schemes in **Table. 1**.

Table 1. The performance of the popular roaming authenticaion schemes

	C.C.Lee's scheme in [50]			C.C.Wu's scheme in [51]			C.C.Chang's scheme in [52]		
	M	F	H	M	F	H	M	F	H
Hash operation	4	4	5	3	5	4	7	3	8
XOR operation	3	1	3	1	N/A	3	5	2	3
Symmetric encryption operation	2	2	1	1	N/A	2	N/A	N/A	N/A
Asymmetric encryption operation	N/A	N/A	N/A	N/A	2	N/A	N/A	N/A	N/A
	H.C.Hsiang's scheme in [53]			Hyeran Mun's scheme in [54]			T.Zhou's scheme in [55]		
	M	F	H	M	F	H	M	F	H
Hash operation	9	7	4	5	4	5	3	2	5
XOR operation	N/A	N/A	N/A	2	2	3	2	1	2
Symmetric encryption operation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Asymmetric encryption operation	N/A	N/A	N/A	1	1	N/A	N/A	N/A	N/A

Because the roaming authentication can be regarded as integration of the whole authentication mechanism, we will make a simulation about it in section 5.

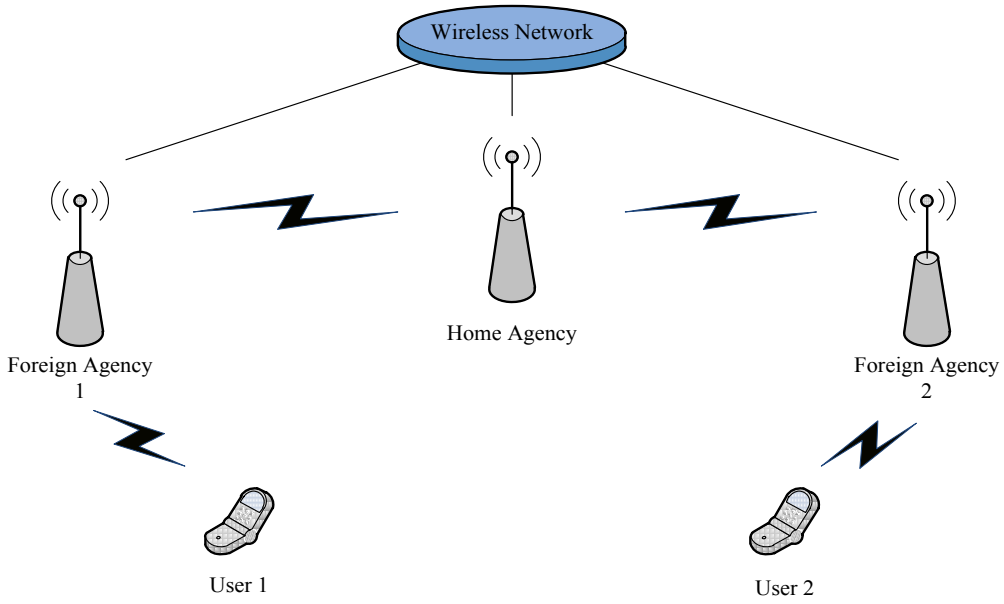

Fig. 5. The general process of roaming authentication

5. The simulation of the proposed authentication mechanism

In this section, we will make a simulation of our proposal and a analysis of the existed schemes. First, we construct a mobile subscriber B and an adversary A.

Inside authentication simulation: when B wants to use the mobile device, he will firstly face to the inside authentication for the using right of the mobile device. In this phase, B will input his password that is only shared between B and mobile device into the mobile device to obtain his using right. If A wants to using B's mobile device, he has to obtain B's password, otherwise, A only has little chance to obtain the using right of B's mobile device by guesing B's password.

Two-way authentication simulation: when B wants to get the service the wireless network service provider provides, he has to firstly pass the identity authentication between he and the wireless network service provider by two-way authentication. In this phase, A can eavesdrop all the information transmitted between B and wireless network service provider, but if A cannot obtain the value k and r, A cannot get B's right to use the service.

Re-authentication simulation: when B moves out of the coverage of currently associated access point, there are two situations to be consider with. The first situation: If B just moves out of the coverage of currently associated access point and does not move into other points, due to the complexity of the normal authentication, the most efficient method B need to do is re-authentication. This authentication is faster than the normal authentication and has the same security level. The second situation: B just moves out of the coverage of currently associated access point and moves into other points. This situation is the next simulation: roaming authentication simulation.

Roaming authentication simulation: when B moves into other points or networks, he will be requierd to carry out the roaming authentication to state his legitimate identity to the foreign agency. A can eavesdrop all the information transmitted among B, home agency and foreign agency. But A cannot obtain the key shared between B and home agency or the key shared between home agency and foreign agency. So A cannot obtain the B's right to access the

network. The whole process of the above simulation can summarized in a figure as showed in **Fig. 6**.

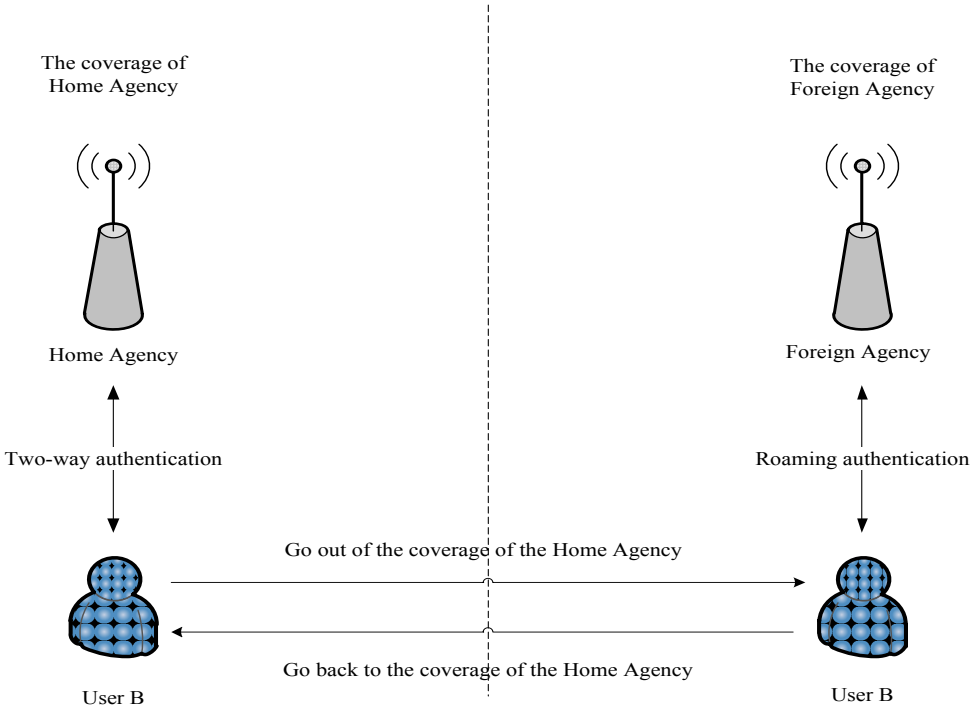

Fig. 6. The process of the proposed system.

6. Conclusion

As the four basic technologies of the Internet of Things, there is no doubt about the importance of the M2M. The Mobile Payment is one of the important applications of M2M. In my paper, we summarize and perfect the authentication framework of Mobile Payment. As a part of security system, the authentication mechanism can prevent the mobile subscriber's privacy and data security from being attacked. Our research achievement is novel and has the vital significance in the field of Mobile Payment.

Though this review introduces many solutions proposed by the previous literatures against the drawbacks and compromises existing in Mobile Payment, it still has many a drawback and compromise as M2M has. Some of these drawbacks and compromises still could not be availably solved. The computation, storage capability and restricted energy of the mobile device still limit the development of the security scheme in wireless network; the mobile device still could be captured; because of the characteristics of the wireless communication, we still cannot prevent the attacker from eavesdropping.

Take a broad view of the development of the modern technology, the limitation of computation, storage capability and restricted energy is most probable the first security issue being solved. Then, in the near future, we will solve the eavesdropping issue via improving the way of wireless communication schemes and the capture of the mobile device via improving the anti-theft measures.

References

[1] X.Y. Zhou and J.M. Schoenung, "An integrated impact assessment and weighting methodology: Evaluation of the environmental consequences of computer display technology substitution," in *Proc. of Journal of Environmental Management*, vol. 83, no. 1, pp. 1-24, 2007.
Article (CrossRef Link)
[2] Abidi. B.R, Aragam. N.R, Yao. Y and Abidi. MA, "Survey and analysis of multimodal sensor planning and integration for wide area surveillance," in *Proc. of ACM Computer Surveys*, vol. 41, no. 1, 2008. Article (CrossRef Link)
[3] Mendes. LDP and Rodrigues. JJPC, "A survey on cross-layer solutions for wireless sensor networks," in *Proc. of Journal of network and computer applications*, vol. 34, no. 2, pp. 523-534, 2011. Article (CrossRef Link)
[4] Axel. Glanz and Oliver. Jung, "Machine-to-machine kommunikition," in *Proc. of Campus Verlag*, pp. 7-14, 2010.
[5] Cha. Inhyok, Shah. Yogendra and Schmidt. Andreas U, "Trust in M2M communication," in *Proc. of IEEE Vehicular Technology Magazine*, vol. 4, no. 3 pp. 69-75, 2009.Article (CrossRef Link)
[6] Chang. Kim, Soong. Anthony and Tseng. Mitch, "Global wireless machine-to-machine standardization," in *Proc. of IEEE Internet Computing*, vol. 15, no. 2, pp. 64-69, 2011.Article (CrossRef Link)
[7] Dai. GuoHua, LI. BaoRong and L1U. ZhaoYuan, "M2M industry development status and problems," *Guangzhou Research Institute of China Telecom* Co. L TD.2008.
[8] Ramfos. A, Karnouskos. S and Vilmos. A, "SEMOPS: Paying with mobile personal devices," in *Proc. of International Federation for Information Processing*, vol. 146, pp. 247-261, 2004. Article (CrossRef Link)
[9] Au. Yoris. A and Kauffman. Robert. J, "The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application," in *Proc. of Electronic Commerce Research and Applications*, vol. 7, no. 2, pp. 141-164, 2008. Article (CrossRef Link)
[10] Stamatis. Karnouskos, Anna. Hondroudaki, András. Vilmos and Balázs. Csik, "Security, trust and privacy in the secure mobile payment service," in *Proc. of 3rd International Conference on Mobile Business*, 2004.
[11] Li. Xinghua, Lu. Xiang and Ma. Jianfeng, "Authentications and key management in 3G-WLAN interworking," in *Proc. of Mobile Network & Applications*, vol. 16, no. 3, pp. 394-407, 2011.Article (CrossRef Link)
[12] Karnouskos. S and Vilmos. A, "The european perspective on mobile payments," in *Proc. of Joinst IST Workshop on Mobile Future & Symposium of Trends in Communications,* pp. 185-198, 2004.
[13] Leavitt. Neal, "Payment applications make e-commerce mobile," in *Proc. IEEE of Computer*, vol. 43, no. 12, pp. 19-22, 2010.Article (CrossRef Link)
[14] Gu. Ruijun, Yao. Juan and Wang. Jiacai, "Research on mobile payment technology and business models in China under e-commerce environment," in *Proc. of Future Generation Information Technology*, vol. 6485, pp. 334-343, 2010.Article (CrossRef Link)
[15] Chen. Xin, "The applications of mobile payment," in *Proc. of High Performance Networking, Computing, Communication Systems and Mathematical Foundations*, vol. 66, pp. 62-67, 2010.
Article (CrossRef Link)
[16] Rad. Habibollah. Arasteh, Tehrani. Mohamad. Bagher and Samsudin. Khairulmizam, "A simple and highly secure protocol for POS termina," in *Proc. of 2nd International Conference on Environmental and Computer Science*, pp. 204-207, 2009
Article (CrossRef Link)
[17] Shin. Dong-Hee, "Modeling the interaction of users and mobile payment system: Conceptual framework," in *Proc. of International Journal of Human-Computer Interaction*, vol. 26, no. 10, pp. 917-940, 2010.Article (CrossRef Link)
[18] Manvi. S. S, Bhajantri. L.B and Vijayakumar.M.A.l, "Secure mobile payment system in wireless environment," in *Proc. of International Conference on Future Computer and Communication,* pp. 31-35, 2009.Article (CrossRef Link)

[19] Nami. Mohammad. Reza, "E-Banking: Issues and challenges," in *Proc. of 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel Distributed*, pp. 263-266, 2009Article (CrossRef Link)
[20] Wang. Yan, Wong. Duncan. S and Wang. Huaxiong, "Employ a mobile agent for making a payment," in *Proc. of Journal Mobile Information Systems*, vol. 4, no. 1, pp. 51-68, 2008.Article (CrossRef Link)
[21] Tomi. Dahlberg, Niina. Mallat, Jan. Ondrus and Agnieszka. Zmijewska, "Past, present and future of mobile payments research: A literature review," in *Proc. of Electronic Commerce Research and Applications*, vol. 7, no. 2, pp. 165-181, 2008.Article (CrossRef Link)
[22] Li. Yunhong and Luo. Siwen, "Research on mobile payment in the e-commerce," in *Proc. of International Conference on Management of E-commerce and E-government*, pp. 100-103, 2008.Article (CrossRef Link)
[23] Zhang. Qinghua, "Mobile Payment in Mobile E-commerce," in *Proc. of 7th World Congress on Intelligent Control and Automation*, vol. S, pp. 1-23, 2008.
Article (CrossRef Link)
[24] Ayo. Charles K, Ekong.Uyinomen.O and Fatudimu. Ibukun. T, "The prospects of m-Commerce implementation: Issues and trends," in *Proc. of Information Management in The Networked Economy: Issues & Solutions*, pp. 210-217, 2007.
[25] Kaland. Kjell Olav, Rong. Chunming and Geng. Yang, "An e-wallet system with decentralized management," in *Proc. of Management of E-Commerce and E-Government*, pp. 35-50, 2007. Article (CrossRef Link)
[26] Manochehri. Naser-Nick, AlHinai. Yousuf, "Mobile phone users attitude towards mobile commerce (m-commerce) and mobile services in oman," in *Proc. of 2nd IEEE/IFIP International Conference in Central Asia on Internet*, pp. 164-169, 2006. Article (CrossRef Link)
[27] Vanneste. P, "Mobile payment transactions," in *Proc. of Securing Electronic Business Processes*, pp. 155-163, 2004.
[28] Jiang. Hua, "Study on mobile e-commerce security payment aystem," in *Proc. of The International Symposium on Electronic Commerce and Security*, pp. 745-757, 2008. Article (CrossRef Link)
[29] Tabandehjooy. Ali Akbar and Nazhand. Navid, "A lightweight and secure protocol for mobile payments via wireless internet in m-commerce," in *Proc. of 2010 International Conference on E-education, E-business, E-management and E-learning: IC4E 2010,* pp. 495-498, 2010
[30] Harb. Hany, Farahat. Hassan and Ezz. Mohamed, "SecureSMSPay: Secure SMS mobile payment model," in *Proc. of 2nd International Conference on Anti-counterfeiting, Security and Identification,* pp. 11-17, 2008
Article (CrossRef Link)
[31] W. Stallings, "Cryptography and Network Security- Principles and Practices," *Upper Saddle River, NJ: Prentice Hall*, 2003.
[32] Fan. Rong, He. Dao-jing and Pan. Xue-zeng, "An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks," in *Proc. of Journal of Zhejiang University-science C-computers & Electronics*, vol. 12, no. 7, pp. 550-560, 2011. Article (CrossRef Link)
[33] Y. W. Law, J. Doumen, and P. Hartel, "Benchmarking block ciphers for wireless sensor networks," in *Proc. of IEEE International Conference Mobile Ad-hoc Sensor Systems*, 2004, pp. 447–456. Article (CrossRef Link)
[34] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyOS based on elliptic curve cryptography," in *Proc. of 1st IEEE International Conf. Sensor Ad Hoc Communucatuib Networks*, pp. 71-80, 2004. Article (CrossRef Link)
[35] G. Gaubatz, J.-P. Kaps, and B. Sunar, "Public key cryptography in sensor networks-revisited," in *Proc. of 1st European Workshop Security Ad-Hoc Sensor Networks (ESAS)*, 2004. Article (CrossRef Link)
[36] M. Bohge and W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks," in *Proc. of ACM Workshop Wireless Security*, pp. 79-87, 2003.Article (CrossRef Link)
[37] S. Schmidt, H. Krahn, S. Fischer, and D. Watjen, "A security architecture for mobile wireless sensor networks," in *Proc. of 1st European Workshop Security Ad-Hoc Sensor Networks (ESAS)*, 2004.

[38] D. D. Hwang, B.C.C. Lai and I. Verbauwhede, "Energy-memory-security tradeoffs in distributed sensor networks", in Proc. of *Lecture Notes in Computer Science on Ad-Hoc, Mobile, and Wireless Networks*, vol. 3158, 2004. Article (CrossRef Link)
[39] N. R. Potlapally, S. Ravi, A. Raghunathan and N.K. Jha, "Analyzing the energy consumption of security protocols," in *Proc. of the 2003 International Symposium on Low Power Electronics and Desig*, pp. 30–35, 2003.Article (CrossRef Link)
[40] J. Lopez, "Unleashing public-key cryptography in wireless sensor networks," in *Proc. of Journal of Computer Security*, vol. 14, no. 5, pp. 469–482, 2006
Article (CrossRef Link)
[41] A. S. Wander, N. Gura, H. Eberle, V. Gupta, S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proc. of the Third IEEE International Conference on Pervasive Computing and Communication*, pp. 324–328, 2005.Article (CrossRef Link)
[42] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls and I. Verbauwhede, "Public-key cryptography for RFID-tags," *in Proc. of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 217–222, 2007.Article (CrossRef Link)
[44] Y. Oren and M. Feldhofer, "A low-resource public-key identification scheme for RFID tags and sensor nodes," in *Proc. of the Second ACM Conference on Wireless Network Security*, pp. 59–68, 2009.Article (CrossRef Link)
[45] H. Chan, A. Perrig and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. of Symposium on Security and Privacy 2003*, pp. 197–213, 2003
Article (CrossRef Link)
[46] W. Du, J. Deng, Y.S. Han and P.K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks,", in *Proc. of 10th ACM Conference on Computer and Communications Security*, pp. 42–51, 2003.Article (CrossRef Link)
[47] Delgado-Mohatar. Oscar,Fuster-Sabater. Amparo and Sierra. Jose. M, "A light-weight authentication scheme for wireless sensor networks," in *Proc. of Journal Ad Hoc Networks*, vol. 9, no. 5, pp. 727-735, 2011.Article (CrossRef Link)
[48] Ahmed. Adel. Ali and Fisal. Norsheila. Fisal, "Secure real-time routing protocol with load distribution in wireless sensor networks," in *Proc. of Security and Communication Networks*, vol. 4, no. 8, pp.839-859, 2011.Article (CrossRef Link)
[49] Guangsong. Li, Jianfeng. Mab, Qi. Jiang and Xi. Chenb, "A novel re-authentication scheme based on tickets in wireless local area networks," in *Proc. of Journal Parallel and Distributed Computing*, vol. 71, no. 7, pp. 906-914, 2011.Article (CrossRef Link)
[50] C.C. Lee, M.S. Hwang and I.E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," in *Proc. of IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683-1687, 2006.Article (CrossRef Link)
[51] C.C. Wu, W.B. Lee and W.J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," in *Proc. of IEEE Communications Letters*, vol. 12, no. 10, pp. 722-723, 2008.Article (CrossRef Link)
[52] C.C. Chang, C.Y. Lee and Y.C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," in *Proc. of Journal Communications*, vol. 32, no. 4, pp. 611-618, 2009.
Article (CrossRef Link)
[53] H.C. Hsiang and W.K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," in *Proc. of Joucnal Computer Standards & Interfaces*, vol. 31, no. 6, pp. 1118-1123, 2009.Article (CrossRef Link)
[54] Mun Hyeran, Han Kyusuk and Lee Yan Sun, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," in *Proc. of Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp. 214-222, 2012.Article (CrossRef Link)
[55] Tao. Zhou and Jing. Xu, "Provably secure authentication protocol with anonymity for roaming service in global mobility networks," in *Proc. of Computer Networks*, vol. 55, no. 1, pp. 205-213, 2011.
Article (CrossRef Link)

Liang Hu was born in 1968. He has his BS degree on Computer Systems Harbin Institute of Technology in 1993 and his PhD on Computer Software and Theory in 1999. Currently, he is the professor and PhD supervisor of College of Computer Science and Technology, Jilin University, China. His main research interests include distributed systems, computer networks, communications technology and information security system, etc. As a person in charge or a principal participant, Dr Liang Hu has finished more than 20 national, provincial and ministerial level research projects of China

Ling Chi was born in Changchun of Jilin, China on Aug. 24 1986. In 2006, Ling Chi began the study of mathematics science at Jilin University in Jilin, Changchun, China. And in 2010, Ling Chi got bachelor's degree of computer science. In the same year, Ling Chi began the master's degree study in network security at College of Software in Jilin University. After 3 years study, Ling Chi will get his master's degree in 2012. From then on, Ling Chi will begin the doctor's degree in the same field of study at the same University.

Li Hongtu was born in Siping of Jilin, China on Mar. 17 1984. In 2002, Li Hongtu began the study of computer science at Jilin University in Jilin, Changchun, China. And in 2006, Li Hongtu got bachelor's degree of computer science. In the same year, Li Hongtu began the master's degree study in network security at Jilin University. After 3 years study, Li Hongtu got his master's degree in 2009. From then on, Li Hongtu began the doctor's degree in the same field of study at the same University.

From 2009, he has got a fellowship job. He worked in grid and network security laboratory as an ASSISTANT RESEACHER at Jilin University. From 2006 to now, he has published several papers. The list of published articles or books is as follows:

Wei Yuan was born in Chengde of Hebei province of China in 1984. He began the study of computer science at Jilin University in 2003 and got his bachelor degree in 2007. Then he continued his research on information security and received his master degree in 2010. Now he is a PhD candidate of the college of computer science and technology of Jilin University.

His main research interests include cryptography and information security. he have participated in several projects include two National Natural Science Foundations of China and one National Grand Fundamental Research 973 Program of China and published more than 10 research papers from 2007.

Yuyu Sun, female, born in 1977,Lecturer, Ph.D. of Jilin University. She graduated from the Department of Computer Science and Technology of Jilin University in 2005,and obtained an MA degree. From 2008,she began to start her doctorate in computer in Jilin University, now she is working in Changchun University. Her current research interests include network and information security. She mainly engaged in Teaching and research on information security and Application software development. She has participated in one National Natural Science Foundation of China, one Major Project of Chinese National Programs for Fundamental Research and Development (973 Program), five Science and technology support key project plan of Jilin Provincial Science and technology Department , three S&T plan projects of Jilin Provincial Education Department .She has Wrote 4 textbooks as yet. She has published 14 academic articles in English and Chinese, four of that has been retrieved by EI.

Jianfeng Chu, corresponding author, was born in 1978, Ph.D. , Now he is the teacher of the College of Computer Science and Technology, Jilin University, Changchun, China. He received the Ph.D. degree in computer structure from Jilin University in 2009. His current research interests focus on information security and cryptology.

An important objective of the projects is to probe the trend of network security, which can satisfy the need of constructing high-speed, large-scale and multi-services networks. Various complex attacks can not be dealt with by simple defense. And to add mechanisms to network architecture results in decreasing performance. In a word, fundamental re-examination of how to build trustworthy distributed network should be made.

.