Proceedings of 2011 International Conference on
Modelling, Identification and Control, Shanghai, China, June 26-29, 2011

A Novel Mutual Authentication Scheme for Internet of Things

Guanglei Zhao[1], Xianping Si[2], Jingcheng Wang[1]*, Xiao Long[1], Ting Hu[1]

Abstract—**This paper presents a novel mutual identity authentication scheme which can be applied securely in Internet of Things. Based on secure hash algorithm(SHA), feature extraction and elliptic curve cryptography(ECC), we propose an asymmetric mutual authentication scheme between the platform and the terminal node, which imposes light computation and communication cost, through security analysis it is also shown that the proposed scheme is secure and feasible for applications in the Internet of Things.**

I. INTRODUCTION

The Internet of Things(IOT) is the extension of the Internet, which refers to the interconnection and communication of everyday objects. It is generally viewed as a self-configuring wireless network of sensors whose purpose would be to interconnect all things[1][2]. During the past decade, many researchers have paid attention to the Internet of Things and the IOT has been successfully applied to some fields such as medical health, payment system, military affairs, security assurance and so on. The development of IOT is based on wireless network, whose basic function is to collect information for authorized users. Typically, the platform and terminal nodes communicate with each other, the platform sends instructions to terminal nodes, then the terminal nodes start working, gathering information and transmitting the gathered information to the platform. During the communication process, in order to operate properly, the platform and the terminal nodes should be authenticated mutually to guarantee the security of the network. Because if there is no identity authentication, the illegal adversaries can also use the network to collect information or to attack the network maliciously. In addition, the identity of the terminal nodes should also be authenticated by other nodes, otherwise, the attacker can insert invalid terminal nodes into the sensor networks to deceive the platform and other nodes. Therefore, the mutual identity authentication plays a significant role in security of the Internet of Things.

Many identity authentication schemes in wireless mobile com- munication and wireless sensor networks have been proposed. [3] proposed a identity authentication scheme for wireless sensor networks, which based on elliptic curve cryptography. [4] investigated a distributed user authentication scheme in wireless sensor networks, which is based on self-certified keys cryptosystem. however, only the user nodes are authenticated in both of the above schemes. [5] presented a four entity mutual authentication technique for mobile communications which demands much computation resource. In [6], mutual authentication for wireless sensor networks in healthcare is investigated and [7] provided a robust mutual two-factor user authentication protocol for wireless sensor networks by applying hash functions.

Due to the limited computation and memory resource of the terminal nodes in IOT, and also the insecure open environment, a new mutual identity authentication scheme is needed, which should be computation effective and secure enough. Most of the current secure authentication schemes are based on Hash functions or public key cryptography, however, [8] has shown that the existing Hash functions (MD5,SHA) are no longer absolute secure as before because of effective collision algorithm has been proposed, and the method based on public key cryptography needs much more computation and memory resources, which is not appropriate for the nodes in IOT.

In this paper we will develop a new asymmetry mutual authentication scheme which can guarantee security(the security will be present in this paper) and be used effectively in terminal nodes of IOT. Our scheme combines the Hash function method and feature extraction, the scheme can prevent collision attack for Hash functions and with some simple feature extraction method, the increased consumed resource which induced by feature extraction is very limited. Feature extraction is a technique often used in pattern recognition and image processing [9], it can transform the input data into the set of features in order to perform the desired task using this reduced representation instead of the full size input. The reasons which motivate us to use the feature extraction in our mutual authentication scheme are mainly in two aspects: firstly, the original quantity of information can be reduced by feature extraction, which means that lesser information will be transmitted over the wireless network, and the burden of the wireless network is lightened; secondly, because the feature extraction is irreversible, that is to say, the original information can not be recovered after feature extraction. Therefore, if we extract the feature of the information which computed from the Hash functions and then send this information to other nodes by wireless channel, even if the attacker intercepts the transmitted information, he does not know what it means.

The rest of this paper is organized as follows. Some basic concepts related to the mutual authentication and feature extraction are introduced in section II. The proposed scheme

1 Guanglei Zhao, Jingcheng Wang, Xiao Long and Ting Hu are with the Department of Automation, Shanghai Jiao Tong University, and Key Laboratory of Wireless Sensor Network & Communication, Chinese Academy of Sciences, Shanghai, 200240.(*Corresponding author: jcwang @sjtu.edu.cn).

2 Xianping Si is with the Fixed Network Testing Department, ZTE Corporation, Zhangjiang Hi-tech Park, Shanghai, 201203, China.

is presented in section III. Then in section IV, we analyze the attack-resistant performance of the proposed scheme. Finally, concluding remarks and future research directions are given in section V.

II. PRELIMINARIES

A hash function is any well-defined procedure or mathematical function that converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index to an array. The values returned by a hash function are called hash values. The cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, such that an accidental or intentional change to the data will significantly change the hash value, and the hash value is sometimes called the message digest or simply digest.

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. Two typical cryptographic hash functions which are widely used currently in many applications are MD5(Message Digest) and SHA1(Secure Hash Algorithm), they are considered to be absolute secure before [8] presents their research results that collision examples have been found for MD5 and SHA1, therefore, considering the future development of IOT as well as its requirement for security, the authentication scheme with MD5 or SHA1 can not guarantee the security of the IOT. In this paper, we will combine SHA1 and feature extraction, which is introduced below, to propose a novel mutual authentication scheme that can avoids the collision attack for SHA1 and guarantee the security of the scheme.

With any information with its length less than $2^{\wedge 64}$ bits, SHA1 can be used to generate a digest with fixed 160 bits. We haven't use the authentication scheme based on public key system, because the computation related to public/private key needs much resource, which is not suitable for terminal nodes in IOT. We use ECDSA(Elliptic Curve Digital Signature Algorithm) and SHA1 respectively to compute the digest for the same information on personal PC, and the time cost is about 1ms and 0.005ms respectively, which proves that the SHA1 is more suitable

Feature extraction is often used in pattern recognition and image processing, it is a special form of dimensionality reduction. To the best of the author's knowledge, this is the first time the concept of feature extraction is introduced into the identity authentication. There are two main reasons that we combine the feature extraction and SHA1 in our authentication scheme: firstly, feature extraction involves simplifying the amount of resources required to describe a large set of data accurately, which means that after feature extraction process, less information will be transmitted over the wireless network; secondly, feature extraction is an irreversible process, which means that even if the attacker get the extracted information, he can not compute the original information.

For simplicity, we only consider two class of features: variance and energy, that can be represented as follows:

$$\text{Variance: } \sigma^2 = \sum_{i=0}^{L-1} (i-\mu)^2 H(i) \tag{1}$$

$$\text{Energy: } \mu_N = \sum_{i=0}^{L-1} H(i)^2 \tag{2}$$

where $\mu = \sum_{i=0}^{L-1} iH(i)$, $H(i) = \frac{n_i}{N}, i = 0,1,\cdots,L-1$, $L = 16$, n_i denotes the number of matrices whose size is i , N denotes the total number of matrices. In our authentication scheme, after the message digest is obtained by SHA1, we view the digest as nonobjective image and compute its variance and energy by the above expressions. The detailed description will be presented in next section.

III. PROPOSED AUTHENTICATION SCHEME

We will focus on the mutual identity authentication between the platform and terminal node, mutual authentication between terminal nodes can be easily deduced from the proposed scheme, and in the case of large amount of terminal nodes, we can use the hierarchical processing method according to the capability of the platform. The main contribution of this paper is combining the SHA1 and feature extraction in the proposed authentication scheme. By means of the properties of feature extraction, on the one hand, we can improve the security of the IOT, on the other hand, the quantity of information which is transmitted over the wireless network can be reduced.

The proposed mutual authentication scheme, which can be used in IOT, is shown in fig.1, we can see that the scheme is composed of three parts. The differences between our scheme and the existing ones are mainly in the first and third part, in part 2(CA verification), we assume that there is a CA center that can be securely used to verify the certificates, we will not pay much attention to this part. According to the practical applications, the control information, which is sent from the platform to terminal node, needs higher-level security than the collected information which is sent from terminal node to platform. Therefore, when the platform sends control information to terminal node, we need to use the key agreement scheme to establish a session key for the control information transmission. Now we are in a position to describe the proposed mutual authentication scheme.

Mutual Authentication Scheme

1. *Initialization*

In the phase of initialization, some necessary factors are pre-distributed to the platform and terminal node. From fig.1 we can see that the factors in the terminal node's side including ID, account, matrix password card, public key, residual private key, second public/private key, random number R_T and other necessary information. And the factors in the platform's side including all information regarding the

terminal node. In order to clearly understand the scheme, we need to make some explanations.

(1).The ID and account are used to identify the terminal node. The matrix password card is used to increase the randomicity of password. According the received matrix password identifier, then the terminal node selects the corresponding matrix password and uses this password as an authentication factor.

(2).Muti-keys pre-distribution scheme is very common in practical applications. An innovation in our scheme is that we don't store integrated private key, as can be seen from fig.1, we name it residual private key. The integrated private key is completed in the process of key agreement before the platform sends control information to the terminal node, and a session key will be established. The public key is used to encrypt collected information. The second public/private key is used to encrypt/decrypt residual private key in the process of key agreement. The random number R_T is another authentication factor and variable, which can be used to prevent replay attack.

(3).The platform holds all information regarding the terminal node(ID, account, corresponding public/private key, etc.), and the information is used to authentication the identity of the terminal node.

2. *CA verification*

As we have explained in previous part, there is a CA center can be used securely to verify the certificates of both of the platform and the terminal node. The certificate authentication method is the same as the existing ones.

3. *Mutual authentication*

The proposed mutual authentication scheme is asymmetric for platform and terminal node. Generally speaking, the platform has relatively more complex structures and higher process capability compared with the terminal node, therefore it is very difficult for the attacker to pretend to be a false platform to communicate with terminal node.

(1). Platform identity authentication

As we presented above, the platform is relatively secure compare with the terminal node, hence, we use a simple way to authenticate the platform's identity. From fig.1, we can see that the information, which is sent from the platform to the terminal node, including matrix password identifier, R_T and $SHA1(R_{T-1} \| AN)$, where the identifier and R_T are used to enhance security by increasing randomicity. R_{T-1} is the random number generated in last authentication process. AN is the account which is secret and only known for the platform and the terminal node.

When the terminal node receives the authentication request, it will use SHA1 to compute $SHA1(R_{T-1} \| AN)$ and compare the result with the received authentication information, if they are equal, the platform is legitimate, otherwise, the platform is considered to be illegal and the mutual authentication process ends.

(2). Terminal node identity authentication

If the identity of the platform is confirmed, firstly, the R_{T-1} in terminal node's side is updated as R_T, and then we use SHA1 and feature extraction together to transform the authentication information.

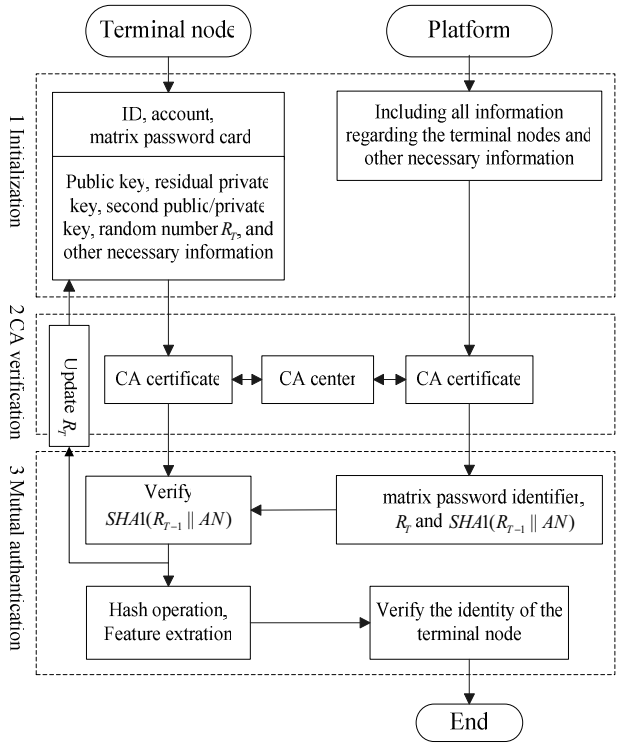

Fig.1. Mutual Authentication Scheme

We firstly use SHA1 to transform the authentication information(ID, account, etc.) to several messages with fixed length, and we regard these messages as a nonobjective image. Then we use the feature extraction expressions (1)(2) to compute corresponding variance and energy, and the variance and energy will be transmitted over wireless network. Meanwhile, the ID of the terminal node will be sent to the platform together with the variance and energy.

When the platform receives the authentication information, it knows which terminal node want to be authenticated according to the ID, and then the platform search for corresponding information about this terminal node in its database. With respect to this information, the platform computes the result with the same procedure as in the terminal and compares the result with received authentication information. If they are equal, the terminal node is legitimate, then the link between platform and terminal node is established and the authentication process ends. Otherwise, the terminal node is considered to be illegal and the authentication process ends without any link being established.

Key Agreement

In many applications, it doesn't matter even if some others know what the information sent from platform to terminal node is. For example, for the sensor nodes being used in healthcare to collect corresponding patient's information, and then it sends the information to management platform, it is indifferent that who knows the collected information. However, the control information sent from platform to sensor nodes must be secret and it needs high security. Therefore, key agreement is needed before sending control information to generate a session key to guarantee the security.

In the proposed scheme, we only store a residual private key K_r (e.g. it is 100bits with the integrated private key 160bits) in the terminal node's side, it is decided by the platform what the other part of the private key K_c is. The platform can use random method or elliptic projection to generate K_c, and then send K_c to the terminal node, with the received K_c, the terminal node computes the integrated session private key $K_I = K_r + K_c$.

With this key agreement scheme, on the one hand, it can saves memory space; on the other hand, the platform can adopt different methods to generate K_c, which improves the security by increase randomicity.

IV. SECURITY ANALYSIS

In the proposed mutual authentication scheme, the related theories including Elliptic Curve Cryptography(ECC), SHA1 and feature extraction, the security is based on elliptic curve discrete logarithm problem and the irreversibility of the hash function and feature extraction algorithm. The following analysis results demonstrate that the proposed scheme is secure for application in IOT.

1. The session key $K_I = K_r + K_c$, where K_r is stored in the terminal node, K_c can be controlled to be different every time by the platform to prevent replay attack. Moreover, K_c is encrypted through ECC and it is only effective in finite time, hence it is impossible for the attacker to crack in current technical conditions.
2. Suppose that the attacker has obtained some old session keys, because the platform can use different methods to generate the residual key K_c, that guarantees the session key K_I is different every time and the attacker can not derive the new session key by the old session keys. The old session keys will be useless after a short time, so the attacker can't use them to communicate with the terminal node.
3. If the attacker intercepts the authentication information which is sent from the platform to terminal node, the replay attack is useless because there is a random factor R_T in the authentication information, which guarantees that the authentication information is just once-effective. The same analysis result can be obtained for the process of terminal node identity authentication.
4. Due to the privacy of the account AN, even if the attacker intercept the random number R_T, he can't compute the $SHA1(R_T \| AN)$, hence the man-in-the-middle attack is useless. If the attacker intercept authentication information which is sent from the terminal node to the platform, he can't compute the original information due to the irreversibility of the SHA1 and feature extraction, hence he can't pretend to be a terminal node and run man-in-the-middle attack.

V. CONCLUSION AND FUTURE WORK

In this paper we have proposed an efficient mutual authentication scheme, which, by the detailed description of the authentication process and the security analysis, we can see that the scheme is secure for application and consumes low computation and memory resource. Though the scheme has been shown to be secure by theoretical analysis, further work should focus on the realization of the proposed scheme on practical hardware nodes, and this issue is being currently studied.

ACKNOWLEDGMENT

This work was supported by Open Project of Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, National Natural Science Foundation of China (No. 60934007), Program for New Century Excellent Talents (No. NCET-08-0359), Shanghai RisingStar Tracking Program (No. 11QH1401300), National 863 Plan of China (No. 2009A A04Z162).

REFERENCES

[1] R. Kranenburg, "The Internet of Things: A critique of ambient technology and the all-seeing network of RFID," *http://www.net workcultures.org/ networknotebooks*, 2008.

[2] G. Zhao, J. Wang, J. Luo, X.. Long, "Applicability of elliptic curve cryptography on Internet of Things," *International Conference on Computer and Automation Engineering*, 2011, vol.1, pp.174-177.

[3] Z. Benenson, N. Gedicke, O. Raivio, "Realizing robust user authentication in sensor networks," *in: Real-World Wireless Sensor Networks(REALWSN),* 2005.

[4] C. Jiang, B. Li, H. Xu, "An efficient scheme for user authentication in wireless sensor networks," *in:21st International Conference on Advanced Information Networking and Applications Workshops*, 2007, pp.438-442.

[5] C. Koner, P. Bhatacharjee, C. T. Bhunia, "A novel four entity mutual authentication technique for 3-G mobile communications," *International Journal of Recent Trends in Engineering*, 2009, vol.2, no.2, pp.111-113.

[6] X. Le, M. Khalid, R. Sankar, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare," Journal of Networks, 2009, vol.6, no.3, pp.355-364.

[7] T. Chen, W. Shih, "A robust mutual authentication protocol for wireless sensor networks," *ETRI Journal*, 2010, vol.32, no.5, pp.704-712.

[8] X. Wang, H. Yu, "How to break MD5 and other Hash functions," *24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2005, pp.19-35.

[9] I. Guyon, S. Gunn, M. Nikravesh, L. A. Zadeh, *Feature extraction: foundations and applications*, Springer, 1 edition, 2006.