A Two-Way Identity Authentication Scheme Based on Dynamic Password

Baohua Zhao[1,2,3], Ningyu An[2,3], Xiao Liang[2,3], Chunhui Ren[2,3(✉)], and Zhihao Wang[2,3]

[1] Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China
zbhl984_l@126.com
[2] Global Energy Interconnection Research Institute Co., Ltd., Beijing 102209, China
anningyu@foxmail.com, 33180900@qq.com, renll98997229@163.com, lanyiner2016@163.com
[3] Artificial Intelligence on Electric Power System State Grid Corporation Joint Laboratory (GEIRI), Beijing 100124, China

Abstract. In order to solve the security issues existed in RFID authentication in recent years. A mutual identity authentication scheme based on dynamic is proposed after describing and analyzing the problems that RFID authentication technology encounters, which can solve replay attack, man-in-the-middle attack and other security issues. In addition, this paper also describes the techno of Authentication technology. The method proposed refers to tags privacy level between Tag and Reader to achieve mutual authentication, it not only can enhance the privacy protection of the label carrier and protect the identity privacy of the Reader holder, but also has a certain effectiveness advantage.

Keywords: Mutual authentication · Internet of Things · Mobile RFID

1 Introduction

The Internet of Things (IoT) embeds or equips sensors into objects such as smart grids, railways, oil and gas pipelines to realize the integration of objects with the existing Internet, the integration of human society, information space, and physical systems [1]. The basic security facilities of the IoT are the key reasons that limit the continued development of the IoT. The authentication technology for "things" entering the network is the basis of IoT security. If this problem cannot be solved, it's meaningless to talk about the development of the IoT. The following is an authentication method for IoT.

For example, object A moves from area 1 to area 2. If object A wants to collect and transmit its information using the resources of area 2, it must get the permission of management organization of area 2. Therefore, object A needs to ask for identity authentication to management organization of area 2, which is used to prove that it is a legal and normal node in area 2.

This work is supported by the science and technology projects of SGCC (5455HJ170001).

M. Qiu (Ed.): SmartCom 2018, LNCS 11344, pp. 1–7, 2018.
https://doi.org/10.1007/978-3-030-05755-8_1

The characteristics of this identity authentication are as follows. First, the access to resources is random. In the future trends of IoT applications, such mobile roaming will be long-term and exist in large numbers. Second, the energy of nodes in the IoT, regardless they are dynamic or static, is limited, which indicates that their survivability is limited by their own power. Third, when the node joins the new access area and obtains the legal identity through identity authentication, it can obtain all the network resources provided by the access area. Finally, except to ensure the security of itself, the identity authentication protocol should not reduce the security of the access area and transport backbone network connected to it.

There are many authentication models for the network, such as PKI technology. After the emergence of the IoT, professionals applied them to the IoT. These technologies played a role in the initial, but with the development of the IoT technology, there are some problems as follows.

(1) In this type of model, the legitimacy of the central node is guaranteed by the certificate issued by the CA. Since the entity information in the certificate is not very clear, it is difficult to distinguish the entity with the same name in real world.
(2) They are too dependent on PKI, which result in poor scalability.
(3) The authentication process requires the intervention of third-party intermediaries, which complicates the authentication process.
(4) They are usually large computation, low efficiency, and high cost, etc.
(5) Existing methods do not involve random roaming, combined security, etc.

In order to solve these problems, professionals engaged in certification research have proposed many methods.

2 Research Status of IoT Authentication Technology

There are many authentication technologies in the IoT, such as hash-based, state-based, key-based encryption, key-based sharing, TinyPk, etc.

RFID authentication protocol based on hash function: The literature [2] proposed a hash function-based authentication protocol. The privacy and security of the protocol can be guaranteed because of the one-way feature of hash function. In addition, as we know, with a one-way hash function h(), let z = h (ID), it is easy to calculate z from the ID, but it is impossible to derive the ID from z. This irreversibility can fight against eavesdropping attacks. Furthermore, the Reader has a random number r generated in each communication. The literature [3] uses the CRC (Cyclic Redundancy Code) algorithm to design the hash function h(). Combined with the updated tag ID, the algorithm can effectively resist playback attack and location detection. However, once the attacker illegally terminates a session, it is easy to cause ID update which will suffer the asynchronous attack or the Tag location detection attack, and cannot effectively resist the fake attack.

In a certain communication using state-based RFID authentication protocol [4], if an attacker maliciously blocked the last session, it is likely to make flag = 0, and the Tag ID is not updated. While in the background database, the Tag ID was updated by the server, which will cause a non-synchronization problem.

The RFID authentication protocol based on key encryption [5] has the disadvantage that in an RFID system with a large number of tags, the calculation of authentication is very difficult. In every authentication, the authentication system needs to check the key of each Tag while for those low-cost RFID Tags, they usually have very limited storage space and computing power.

TinyPK Sensor Entity Authentication [6] requires a Trust Center (CA). Usually, base station can act as CA. Any external organization (EP) in the authentication protocol must have a public/private key pair to establish contact with the sensor node, and its legal identity can be proved by processing public key signed by CA. The TinyPK authentication protocol uses a request-response mechanism. First, the EP sends a request message which contains two parts: (1) its own public key signed by CA; (2) an information validity value and time stamp which are signed by the EP's private key. The integrity of the information is guaranteed by the information validity value, and the time stamp is used to resist the replay attack. After the request packet arrives at the node, the first part of the packet is verified using the CA's public key, which can confirm the identity of EP and obtain the public key of the EP at the same time. Then the EP's public key is used to verify the second part of the packet. After that, we can obtain the information validity value and time stamp, which can be used to verify the legal identity of the third party.

In addition, literature [7] uses a one-way hash chain to implement a broadcast authentication μTESLA. Literature [8] uses Merkle Tree to construct a certification path based on the public key mecha-nism to reduce the communication overhead of authentication. Literature [9] proposes a layered-based authentication management scheme. All of these authentication protocols are designed for the traditional static nodes of the sensor network, lightweight is an advantage. However, none of them consider about the roaming scenario and the combined security requirements for the IoT.

3 Mobile IoT Identity Authentication Based on Dynamic Password

Compared with the traditional static passwords, dynamic password is generally produced by a terminal device using dynamic password algorithm. The dynamic password produced is varied with dynamic parameters. The dynamic password generation algorithm generally adopts a double operation factors. One is the identification code of the user identity which is fixed, such as the user's private key; the other is a variation factor, such as time, random number, counter value, etc. Different dynamic factors adopt different dynamic password authentication techniques.

It is undeniable that the dynamic password-based identity authentication system brings the gospel to the mobile IoT, which can solve problems we mentioned in the second chapter of this article. Its advantages, such as dynamics, one-off, randomness, multiple security, etc. fundamentally repair some security risks of traditional identity authentication systems. For example, it can effectively prevent replay attacks, eavesdropping, guessing attacks, etc. However, as far as the current research results and usages are concerned, it also has deficiency and technical difficulties.

The existing dynamic password-based identity authentication system can only achieve one-way authentication, that is, the server authenticates the client, so attacks from the server side cannot be avoided. With the diversity of network applications, more and more network applications require two-way authentication to ensure the benefits of both parties. For example, in the registration phase of e-commerce, the client and server need to exchange their id and public key. In order to solve above problems, and further improve the security, reliability, flexibility and efficiency of mobile IoT, a dynamic mobile IoT identity authentication method is proposed in this paper. This method is based on the mechanism of public key infrastructure PKI and Privilege Management Infrastructure (PMI), and absorbs the essence of traditional trust model.

3.1 Scheme Design

Under the wireless network structure of mobile IoT, node authentication is usually divided into three stages:

The first stage is registration. Mobile node will register in the initial area A. The main purpose of this stage is to pre-deploy secret materials such as initial identification code, password and authentication information, etc.

Symbols and parameters involved in the scheme are as follows:

Qu: Indicates that the Reader has submitted an authentication request to the tag.

PWx: Indicates the access cipher group generated by the server. It is a 32-bit binary number that can represent the password stored in the Tag (when x is t) and the password stored in the back-end server (when x is i).

UIx: Indicates the identification code assigned by the server to the tag. It is a 32-bit binary number, which can respectively represent the identification code stored in the label (when x is t) and the identification code stored in the back-end server (when x is (i).

Rt: Indicates the random number generated by the tag, which is a 16-bit binary number.

Rr: Indicates the random number generated by the reader, which is a 16-bit binary number.

H(): indicates a one-way hash function, !!: Cascade operator, ==: compares whether the two are equal, →: send (Fig. 1).

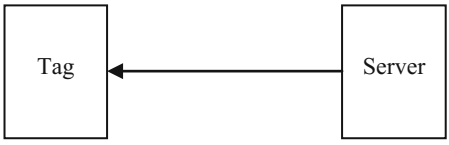

Fig. 1. Node registration

During the registration stage, the server assigns a unique identification code (USER ID) and password to the electronic tag, and stores them both in the Tag and back-end database e. In the process of system authentication, the password stored in the Tag is compared with the password stored in the database. If they are equal, it means the node

belongs to the system. Since PWi, UIi, PWt and UIt are generated by the server (or manufacturer) when the system is established, and they are encrypted and then distributed by the secure channel and stored in the corresponding tag and back-end database, they are considered to be safe and confidential.

The second stage is the authentication of the mobile node in the registration area.

The specific steps of the RFID system password authentication scheme are as follows:

(1) Reader → Tag: The Reader generates a random number Rr and then sends an authentication request Qu and Rr to the tag.
(2) Tag → Reader → Server: After receiving the authentication request Qu and the random number Rr, the Tag generates a random number Rt, and calculates PUIt = H(UIt!!PWt!!Rt!!Rr), and then sends (PUIt, Rt)to the reader. After the Reader receives it, it forwards (PUIt, Rt, Rr) to the server.
(3) Server: After receiving the (PUIt, Rt, Rr) sent by the reader, the local authentication server searches for UIi and PWi ($1 < i < n$) that satisfies PUIi == PUIt in the backend database, where PUIi = H(UIi!!PWi!!Rt!!Rr). If there exists such UIi and PWi, the authentication is passed and the process proceeds to step (4); otherwise, the authentication fails and the operation will be terminated. So the Tag can be identified by Reader through above process.
(4) Server → Reader → Tag: The server calculates PUIi = H(UIi!!PWi!!Rt) with UIi, PWi, Rt, and sends the calculated PUIi to the Reader. After the Reader receives it, it will forward it to the Tag.
(5) Tag: After the Tag receives the PUIi forwarded by the reader, it first calculates PUIt = H(UIt!!PWt!!Rt), and then verifies whether the PUIt is equal to PUIi. If they are equal, the authentication to the Reader is successful; otherwise, the authentication is failed. So the Reader can be identified by the Tag through above process (Fig. 2).

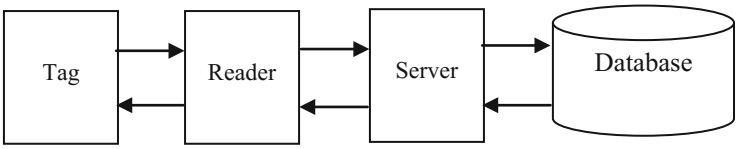

Fig. 2. Identification scheme

The third stage is to roam to the new area B (the visited area). How does the mobile node complete the authentication in the visited area with the assistance of the transmission backbone network? In this paper we assume that the static sensing network has been deployed, and there exists secure links among the sensor arears which are built on transmission backbone.

The mobile node A in the area A enters the area B through a period of time movement. Only node A accepts and passes the authentication from the manager of area B, it can enjoy the network service from the area B. The execution process of the roaming authentication protocol is shown in Fig. 3. The difference between it and the

previous stage is that when the authentication server cannot find the node in the local database, it will issue a collaborative authentication request to the remote server cluster, and the remote server cluster will authenticate the node. If it still cannot be found in remote server cluster's database, the node will be considered to be an illegal node and be added to the blacklist, then refused to pass the authentication (Fig. 3).

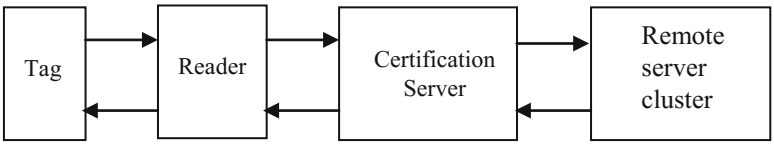

Fig. 3. Roaming authentication

4 Security Analysis

In order to verify the authentication scheme designed in this paper, a security analysis is carried out.

(1) Anti-replay attack: Whether password is sent from server or to server, it is one-time and irrelevant, namely, you can't deduce next password from the previous password. Therefore, it can resist the replay attack.
(2) Anti-man-in-the-middle attack: The protocol is two-way authentication, that is, user and server can authenticate each other. Generally, man-in-the-middle attack can break any protocol without encryption. Therefore, the public key encryption method is adopted in the transmission process. Even if the middleman can intercept the data transmitted between the server and the client, he still can't get the correct password because of lacking private key.
(3) High authentication strength: In this scheme, decryption, signed information verification, one-time password authentication are all used. So it has high security.
(4) Simple protocol structure: The whole authentication process can be completed by two communication parties and no third party is required. So the solution is easy to implement.
(5) Small interaction: Due to the use of one-time password generation mode in event synchronization, the number of communication times in the authentication process is small. And the amount of information exchange between two parties is small. Only two communications are required to achieve mutual authentication.
(6) Fractional attack vulnerability: The protocol adopts an event-based one-time password generation algorithm, which is different from the asynchronous one-time password generation mechanism used in challenge-response mode, so there is no fractional attack vulnerability.

5 Conclusion

With the increasingly growing applications of Internet of Things and RFID technologies, more security vulnerabilities are appearing in the RFID authentications, the requirements for its security are getting higher and higher. In order to solve the issue related to identity authentication existed in RFID applications in recent years. A mutual identity authentication scheme based on dynamic is proposed in this paper, which can better resist replay attack, man-in-the-middle attack, and has Simple protocol structure and small interaction. Therefore, the protocol can better satisfy the security requirements for mobile RFID applications. It has an effectiveness advantage and can make a positive contribution to the future RFID authentication applications.

References

1. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
2. Cbien, H., Chen, C.: Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards. Comput. Stan. Interfaces **29**(2), 254–259 (2016)
3. Dimitriou, T.: A lightweight RFID protocol to protect against traceability and cloning attacks. In: International Conference on Security and Privacy for Emerging Areas in Communications Networks, pp. 59–66. IEEE Press (2005)
4. Kang, S.Y., Lee, D.G., Lee, I.Y.: A study on secure RFID mutual authentication scheme in pervasive computing environment. Comput. Commun. **31**(18), 4248–4254 (2008)
5. Kaya, S.V., Sava, E.: Public key cryptography based privacy preserving multi-context RFID infrastructure. Ad Hoc Netw. **7**(1), 136–152 (2009)
6. Watro, R., Kong, D., Cuti, S.F., et al: TinyPK: securing sensor networks with public key technology. In: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 59–64. ACM (2004)
7. Perrig, A., Szewczyk, R., Tygar, J.D., et al.: SPINS: security protocols for sensor networks. Wirel. Netw. **8**(5), 521–534 (2002)
8. Du, W., Wang, R., Ning, P.: An efficient scheme for authenticating public keys in sensor networks. In: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Urbana, pp. 58–67 (2005)
9. Ibriq, J., Mahgoub, I.: A hierarchical key establishment scheme for wireless sensor networks. In: Proceedings of 21st International Conference on Advanced Networking and Applications (AINA 2007), Niagara Falls, pp. 210–219 (2007)