Design of the Identity Authentication and Key Management System Based on Wireless Community

Wang Linsheng, Zhou Ke

Henan Polytechnic Institute, Nanyang, 473000,China

Xuexi123@163.com

Keywords: Wireless community, Two-way authentication, Key management, Hash function, Random number, Energy consumption.

Abstract. With the rapid development of wireless communication technology, wireless community has brought a lot of convenience to people's life. However, in the open wireless network environment, the communication system has been attacked and threatened to be higher than the traditional wired network. In order to improve the reliability of the wireless community network identity authentication and the efficiency of the key management system, this paper proposes a bidirectional identity authentication scheme based on one-way hash function and one-time random number, the scheme realizes the two-way authentication between users and servers, and provides a secure key agreement for the server and users. Finally, the wireless community identity authentication and key management system are tested, we found that the authentication method based on the random number is lower than the energy consumption of common authentication mode, and the communication overhead is smaller, the system stability and reliability are also good.

Introduction

In recent years, with the rapid development of wireless communication technology, the arrival of 4G wireless communication eras as well as the promotion of Web 3.0, they integrate the mobile network, internet and video network [1-3]. With the development of mobile terminals, wireless community has become an everywhere in the mobile environment. Wireless community can provide online transactions, electronic government affairs, remote language, video calls and a series of services, which greatly facilitates the lives of community residents. [4,5] However, in the development of wireless network, it is an urgent problem to provide security for the network environment. Identity authentication and key management are the basis of ensuring the wireless communication security, it is important to ensure the security of the system, to study the identity authentication and key management in wireless network.

Wireless Sensor Networks Key Management Schemes and Protocols Classification

In recent years, the study of wireless network key management and identity authentication system have made great progress, in which the emphasis is different for the different authentication management scheme and protocol [6-8]. Through the district division of different protocols and key management, key management can be divided into three categories.

Symmetric and asymmetric key management. According to the different of key system, the management of wireless network key can be divided into symmetric key management and asymmetric key management [9]. For the symmetric key management, users and servers can use the same key and encryption algorithm. The key length is relatively short and the communication overhead is relatively small, which is the main research direction of wireless network key. In the aspect of asymmetric key management, the encryption and decryption keys of the nodes are different, however the storage and overhead of the communication are relatively high, and the optimization can be used in the wireless network security authentication system.

Distributed and hierarchical key management. According to the structure of wireless network, the key management can be divided into two types that are respectively distributed and hierarchical

[10,11]. Distribution is that key management node communication and computing power are the same, the key agreement is the use of the mutual authentication between neighboring nodes to complete, which has a strong distribution characteristics; hierarchical key management are lower for the computing power nodes and storage capacity requirements, but if the cluster head are loss, it will lead to a serious threat to the entire security authentication system.

Static and dynamic key management. According to whether the wireless network authentication keys need to be updated, the key management can be divided into static key management and dynamic key management [12]. The static key management needs a certain number of key pre distribution, and the key is to be formed through negotiation. In the whole process of authentication, the network part carries out updated and withdrawn. The characteristics of dynamic key management carries out periodic distribution, negotiation and withdrawal operation, and the communication overhead of dynamic key management is greater than the static key management.

Random and determination key management. According to the distribution method of wireless network node key, the key management can be divided into two kinds that are respectively the random key and derermine key, in which the node of the random key is obtained by random allocation, the user can randomly obtain a password in the password pool, and the determination of the key is to determine the way to get the password; the connectivity of random password is between 0 and 1, and the sum of derermine password connectivity is 1; the advantage of random password is that the distribution of nodes is not limited, but it may cause the distribution of the blindness and the waste of storage space; the determine key has better targeted, but the use of its storage space is not too good, which will reduce the flexibility of key management.

Wireless Community Two-way Identity Authentication and Key Management based on Random Number

In order to improve the reliability of wireless community identity authentication and the efficiency of the key management, this paper proposes a two-way identity authentication scheme based on random number, the scheme is composed of three parts, including sub protocol registration, sub protocol login and sub protocol two-way authentication [13-15].

Sub protocol registration. When a user U_i is registered in the server S, the system will generate a random number after selecting user identity ID_i and login password, and its expression is

$$RPW = h(r\|pw_i) \tag{1}$$

Among then, h represents the hash function, the user will send ID_i and RPW to the server, the server carries out the following operations:

$$\begin{aligned} e &= h(ID_i\|x) \\ V_1 &= h(e\|RPW) \\ Y &= (ID_i \oplus RPW \oplus y) \\ q &= e \oplus RPW \end{aligned} \tag{2}$$

Among then, x shows the remote server login password, q, V_1, Y and h will be written to the smart card by server, and then the use of the security channel is presented to the user, completing the sub protocol registration procedures.

Sub protocol login. When the user needs to log on the server, the smart card will be connected by reader and network, and then smart card begins to calculate.

$$\begin{aligned} e &= q \oplus h(r\|pw_i) \\ V_1' &= h(e\|h(r\|pw_i)) \end{aligned} \tag{3}$$

If server detection V_1' and intelligent card V_1 are the same, the verification goes through, and then the server carries out the following operations:

$$y = Y \oplus ID_i \oplus h(r \| pw_i) \tag{4}$$

Through the calculation, it can generate random numbers N_u.

$$\begin{aligned} A_1 &= e \oplus N_u \\ A_2 &= h(ID_i \oplus y \oplus N_u) \\ A_3 &= h(y \oplus N_u) \\ A_4 &= h(A_2 \oplus A_3) \end{aligned} \tag{5}$$

Finally, the user sends the authentication message $\{ID_i, A_1, A_2, A_4\}$ for the server, and the sub protocol login is completed.

Sub protocol authentication. When the user sends the login message, the server performs the following actions:

$$\begin{aligned} N_u' &= A_1 \oplus h(ID_i \| x) \\ A_2' &= h(ID_i \oplus y \oplus N_u') \\ A_3' &= h(y \oplus N_u') \end{aligned} \tag{6}$$

If the detected A_4 and $h(A_2' \oplus A_3')$ by server are equal, the verification completes; if not same, the verification terminates; if the verification goes through, then the server performs the following operations:

$$\begin{aligned} A_5 &= h(ID_i \| x) \oplus N_s \\ A_6 &= h(h(y \oplus N_u \oplus N_s) \oplus h(ID_i \| x)) \end{aligned} \tag{7}$$

Among then, N_s represents the number of random generated by the servers. In order to achieve the two-way authentication of wireless community, the server is also sent to the user authentication message $\{A_5, A_6\}$, requesting users to authenticate, and then the user performs the following operations:

$$N_s' = A_5 + h(ID_i \| x) \tag{8}$$

Detecting A_6 and $h(h(y \oplus N_u \oplus N_s') \oplus h(ID_i \| x))$ is equal to complete the certification, if not equal, the certification is terminated, and then the user and the server share session key after two way authentication.

$$SK = h(h(ID_i \| x) \oplus y \oplus N_u \oplus N_s) \tag{9}$$

The key is used to encrypt the session information.

The Security and Efficiency Test of Identity Authentication and Key Management System

In order to verify the reliability of wireless community identity authentication and key management system designed in this paper, the use of the simulation experiments verifies the performance of identity authentication and key management system [16-18]. The simulation experiment uses the wireless network topology, in which the area size is 600m*600m, this area are arranged 500 nodes, the communication radius is 20m, and its structure is shown in Figure 1.

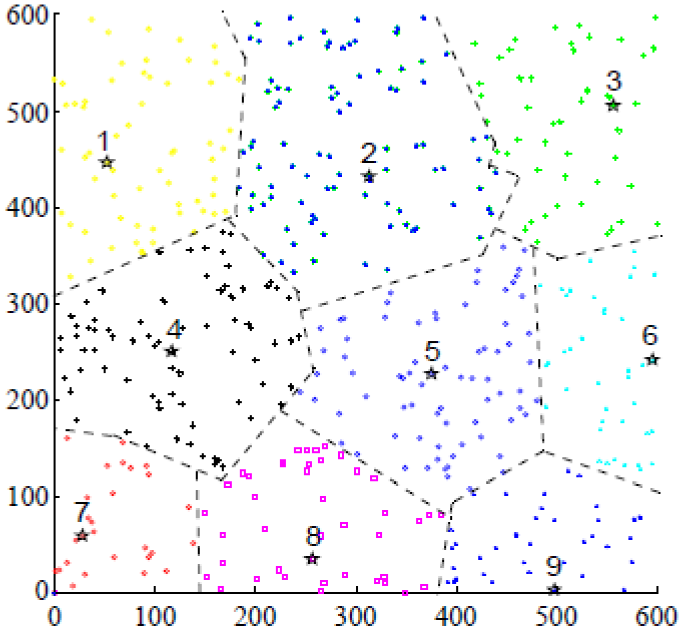

Fig. 1 Simulation experiment network topology structure

In the topology structure of the simulation experiment, the storage complexity degree of each node is at most $(m+1)\log q$, the complexity degree of the latter part $j-th$ is $(m-j+2)\log q$. In $j-th$ session, the complexity degree of the wireless communication is $(t+1+j)\log q$. Users ID can choose in the cell domain, assuming q is 64 bits, the communication overhead is shown in Figure 2.

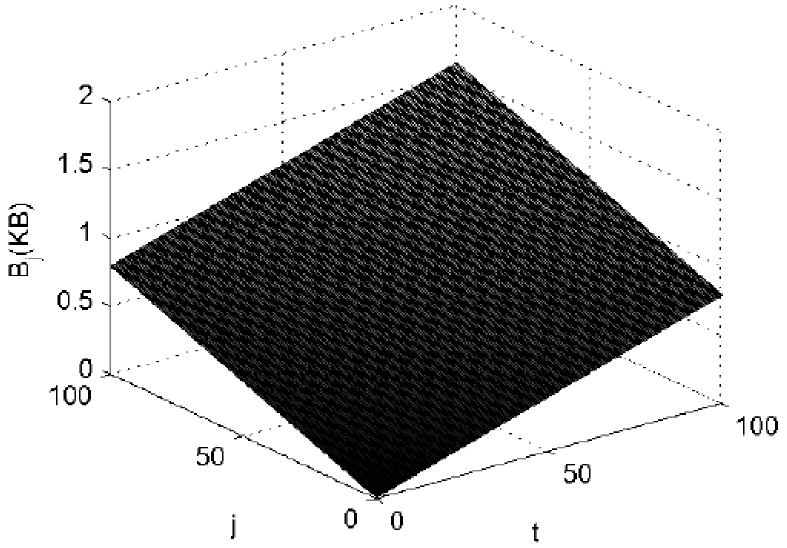

Fig. 2 The relationship between the communication overhead and the number of sessions and the delete user

Figure 2 shows the relationship between the communication overhead and the number of sessions and delete users, it can be seen that in the case of delete users, the communication overhead increases linearly with the increase of the number of sessions; when the number of sessions is constant, the communication overhead will increase linearly with the increase of the number of users.

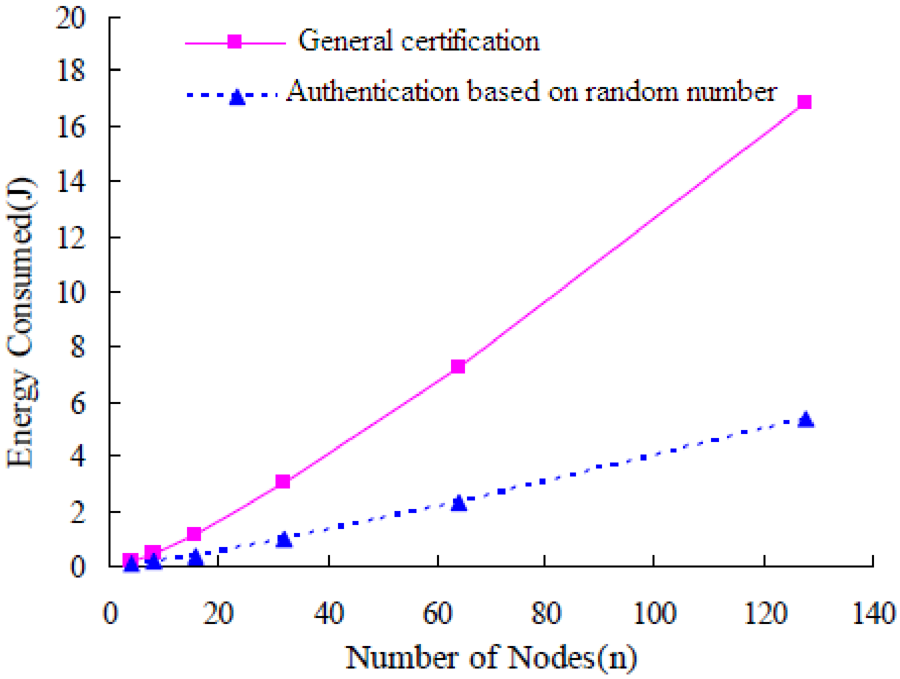

Fig. 3 The consumption contrast between the traditional authentication methods and the design of the authentication mode energy

Figure 3 shows the consumption contrast between traditional authentication mode and the authentication mode energy based on random number, it can be seen that with the increase of the number of nodes, the energy consumption of certification is linear growth, in which the designed authentication method based on the random number by this paper is significantly lower than the ordinary energy consumption, the energy saving effect is good, the calculation of the cost is small, the stability and reliability of the system is also good.

Summary

Based on one-way hash function and one - time random number theory, this paper proposes a new dual - way wireless networks authentication scheme, which can achieve the dual - way authentication between user and server, but also provide the security key management function. The security authentication scheme is tested and found that in the case of delete users, the communication overhead increases linearly with the increase of the number of session authentication; when the number of sessions is constant, the communication overhead will increase linearly with the increase of the number of users. With the increase of the number of nodes, the energy consumption of the certification is linear increasing, in which the designed authentication method based on random number is obviously lower than the ordinary energy consumption, this method has obvious advantages.

References

[1] S.G. Yan, H. Wu, S.X. Xue. Design and implementation of Ethernet data transmission system based on W5300. Electronic design engineering, 2012, 13(9): 92-94.

[2] M.X. Yao. Research and implementation of encryption algorithm in network information security. Computer knowledge and technology, 2014,12 (28): 25-29.

[3] L.S. Liu. On the basis of RSA encryption algorithm. Computer knowledge and technology, 2014, 3 (21): 20-23.

[4] Y. Liu. Research on enterprise private cloud platform construction technology. computer time. Computer ear, 2014(6): 38-41.

[5] Q.Y. Ou, K. Zhao. The application of cloud software platform in multimedia classroom. Chinese information technology, 2014(16): 242-243.

[6] G.H. Cui, L.P. Zhang, J.Y. Lei, J.F. Xu. A new group key agreement protocol in dynamic collaborative peer group. Computer application, 2014, 28 (7): 1798-1801.

[7] X.Y. Huang. Wireless sensor network key management overview. Computer application research, 2013, 23 (4):10-15.

[8] Z.G. Qin, Z.J. Li, J.H. Wang. Research on wireless sensor network key distribution protocol. Computer science, 2014, 33(2): 87-91.

[9] G. Yang, J.T. Wang, H.B. Cheng. Wireless sensor network key distribution method based on identity encryption. Chinese Journal of electronics, 2014, 35(1): 184-188.

[10] H.Z. Zhang, X.L. Dan, P.C. Yu. Research on wireless sensor network key management based on clustering. Computer engineering and design, 2013, 28(20): 1608-1616.

[11] L.P. Zhang, P. Xu, G.H. Cui, J. Chen. Wireless sensor network key pre distribution protocols based on hierarchical grids. Computer science, 2013, 35(11): 49-53.

[12] R. Xue, D.G. Feng. The security protocol formal analysis of technology and method. Journal of computer, 2013, 29(1):1-17.

[13] L.P. Zhang, G.H Cui. A new group key agreement protocol in Ad Hoc network. Computer Engineering, 2014, 34(12): 123-125.

[14] L.P. Zhang, G.H Cui. An efficient group key agreement protocol in the large scale Hoc Ad networks. Computer application research, 2014, 25(6): 1817-1821.

[15] K. Lu. The design of embedded media player based on STM32F103VCT. Journal of Hunan Industrial Vocational and technical college, 2013, 18(5): 34-39.

[16] Y.F. Pu, W. Zhang, S.H. Teng, H.L. Du. collaborative network intrusion detection based decision tree. Journal of Jiangxi Normal University, 2014, 34(3): 302-307.

[17] F. Wang, H.Q. Lu, F. Song x, et al. Damage assessment system based on combat simulation. Journal of PLA University of Science and Technology, 2013, 10(2): 139-143.

[18] H.M. Wang, Y. Zhang. Research on joint operations simulation model. System simulation, 2008, 20(15): 4186-4188.