Research and Design of Dynamic Migration Access Control Technology Based on Heterogeneous Network

Feng Wang, Weichuan Ni, Shaojiang Liu, Jia Lu, Zhiping Wan

Xinhua College of Sun Yat-sen University, Guangzhou, 510520, PR China

Abstract: With the continuous development of wireless networks, the amount of privacy services in heterogeneous mobile networks is increasing, such as information storage, user access, and so on. Access control security issues for heterogeneous mobile radio network, this paper proposes a dynamic migration access control technology based on heterogeneous network. Through the system architecture of the mutual trust system, we can understand the real-time mobile node failure or abnormal state. To make the service can be terminated for the node. And adopt the 802.1X authentication way to improve the security of the system. Finally, it by combining the actual running test data, the trust update algorithm of the system is optimized to reduce the actual security threats in the environment. Experiments show that the system's anti-attack, the success rate of access, bit error rate is in line with the expected results. This system can effectively reduce the system authentication information is illegally obtained after the network security protection mechanism failure and reduce the risk of user data leakage.

Keywords: Heterogeneous network; wireless network; mutual trust system; trust update algorithm

0. Introduction

The diversification of Internet services and the spread of communication technology services have led to the rapid development of mobile devices. This makes wireless network service demand more than ever before. Heterogeneous mobile wireless network access and network type are showing diversity. Different network implementation technology, transmission mechanism, organization, control mechanism there is a huge difference. Access Control Technology for Heterogeneous Mobile Wireless Networks, which need to request the user's network status based on the current visit. According to the user's location and business in a different way to smooth between the accesses that can to provide reliable access to support services.

Through different access network landing personal account information to access the service system on the mobile device, compared to a single access network to authenticate the way more convenient. As a result, more authentication processes are done on heterogeneous mobile wireless networks [1-2]. Heterogeneous mobile networks involved in the security-critical business, which the need for strong security access control technology as a support. To ensure that the only legitimate user account and other information will not be illegal access. Today's heterogeneous mobile wireless networks offer a variety of security services. On this basis, the relevant security

strategies are: encryption, authentication, access control, key management, certificate management, etc. [3-4]. Among them, the most widely used authentication mechanism for network security-sensitive services is authentication methods based on personal information such as ID / password and digital certificates. Personal information will be due to the user's own negligence, but also by other illegal means of invasion of technology, such as the loss or theft of smart cards, access to information is illegal tracking and collection. Even if the application layer and network layer at the same time the implementation of security certification, but due to the dependence between the network layer and the application layer. The application layer's security risks still exist [5]. Because heterogeneous network services are the interaction between users and service delivery systems, service security is based on mutual trust between them. The user terminal can access the service providing system simultaneously through a different access network. When the authentication information of the only legitimate user is illegally stolen by another person, the service providing system cannot distinguish whether the object to be accessed is a legitimate user. As a result, there is a security issue for the mutual authentication system of authentication between the user terminal and the service providing system.

This paper studies the security of heterogeneous mobile

wireless network access control. We proposed architecture consists of a client and a security service system installed on a trusted user node. It can make the security service system can obtain the real-time status of the mobile node. Make the system can be real-time understanding of mobile node failure or abnormal state, which can terminate the service for the node. And this paper is building the modeling method to analysis and comparison with safe access methods. It make the system finding a safer, more efficient access method. And we are use 802.1X authentication to improve the security of the system. And in the authentication process, the user's identity is used as a public key, so that the key management easier, and do not need to perform the key revocation of the certificate. Node are using a non-interactive computing a symmetric key, which can reduce communication overhead. Finally, after the actual operation of this test, the trust update algorithm to optimize the system to reduce the actual operation of the security threats in the environment.

1. Heterogeneous Network

Security issues as wireless heterogeneous network development process must pay attention to an important issue. As the expanding range of network applications and the diversification of access methods, it make a variety of means of attack growing, security plays a vital role in all key technical issues heterogeneous networks. As in all aspects of heterogeneous network routing, authentication, billing, node cooperation, intrusion detection, there are security vulnerabilities. At present, people have carried out relevant research work on some aspects of heterogeneous network security and achieved certain results. However, due to the extremely complex nature of heterogeneous networks, the need to address the security issues is still more.

Figure 1. isomorphic network overall architecture map

2. Article Algorithm

2.1 System Architecture Based on Mutual Trust System

Our proposed architecture consists of a client and a security service system installed on a trusted user node. The security service system realizes the user and assigns unique identifiers to each user. The client can manage multiple network interfaces. And the establishment of a mutual trust system to establish and maintain network links based on security services. And it can use security service system to send mobile conditions under the changing network status information, which including the connection status, network address dynamic changes.

The study of the mutual trust system in the system is the key to the design of the whole system architecture. The mutual trust system enables the secure service system to obtain the real-time status of the mobile node. It can make the system understand the fault or abnormal state of the mobile node. If the illegal node chooses not to send the state data to the security service system in order to hide its own abnormal state information, the mutual trust rule will be broken, and the security service system may terminate the service for the node.

Figure 2. Enhanced cell coverage model

Trusted Verification Security Formula 1: The system state v is to satisfy the trusted authentication security formula. iff for any allowed $(s, o, A, T) = \text{true}$. The following formula holds:

(1) 当 $A=r$ 时, $fc_c(s) \geq fo_c(o) \wedge fc_w(o) \geq fo_w(s) \wedge \text{Time}(\text{trans}, s) \leq T$;

(2) 当 $A=w$ 时, $fc_c(s) \leq fo_c(o) \wedge fc_w(o) \leq fo_w(s) \wedge \text{Time}(\text{trans}, s) \leq T$;

Trusted Verification Security Formula 2: system $\Sigma (R, D, W, v_0)$ is a security system. Each state of the system $(v_0, v_1, \dots, v_n)$ are safe.

Here s is the set of subjects in the system. o is the guest set. $A=\{r, w, a, e\}$ indicates that the subject requests access. They represent the read, write, append and execution. Trusted state set $Ts=\{\text{trusty}, \text{untrusty}, \text{wtrusty}\}$, which represents trusted entities, untrusted entities, and integrity trusted entities,

respectively. And it corresponds to a trusted area, an untrusted area, and a controlled area in the TNC structure.

2.2 Secure Access Model for Heterogeneous Mobile Networks

Through the modeling method [6], which can make all aspects of the system behavior in the early stages of development, is predicted, and thus easier to solve the problem. Therefore, we need to abstract the security access problem and establish the theoretical model at first. Through the model of the method to compare a variety of secure access methods to find a more secure, more efficient access method.

Figure 3. Secure access model for heterogeneous mobile networks

The network is abstracted into two levels. One for the user network plane, it is mainly represents the heterogeneous network topology and the behavior of the user in the network. The other for the abstract level of the context, it is mainly used to ensure the security of the transfer of context. There are multiple Diameter nodes in the fig.3.it is including AAA home server (AAAH), AAA local server (AAAL) and protocol conversion gateway. Among them, if the mobile node is only in the local mobile, then only need to pass AAAL certification, or in the context of the transfer process need to go through AAAH processing.

2.3 Secure Access Authentication Method for Heterogeneous Mobile Networks

In this paper, the network access authentication process, mainly including three levels:

Access control layer, is to control access [7]. Which allows users to access, when to allow access, to allow access to where and so on. It mainly adopts the way of Web authentication and 802.1X authentication.

The authentication control layer, which is the interactive rule that controls the authentication message [8-9]. Based on the key mechanism of the service system, the user responds to the authentication requirements of the service system according to

the authentication method and its parameters needed by the negotiation.

Authentication implementation layer, which completion of authentication based on in the selected access and authentication control. At present, commonly used authentication methods include account number / password, CHAP, AKA, etc. Authentication control and authentication implementations are usually combined to complete access authentication.

Figure 4. Identity encryption key mechanism

2.4 Key mechanism based on identity encryption

In the identity encryption mechanism, the user's identity is used as a public key [10-11]. This makes it easier to manage keys and does not need to perform a certificate for key revocation. The node uses noninteractive computing symmetric keys to reduce communication overhead. This model of minimizing PKC overhead is very appealing For mobile, resource-constrained heterogeneous mobile networks.

Compared with the traditional encryption algorithm, this article uses a symmetric key cryptography system. The elliptic curve encryption method based on signature (El-Jamal type) is used on the decryption key to avoid tampering with unauthorized attackers.

According to its use of the key only one, both parties use this key to encrypt and decrypt the data. This requires the decryption party to know the encryption key in advance. Symmetric encryption algorithm is characterized by open algorithm, small computation, fast encryption, high encryption efficiency.

2.5 Trust update algorithm

Through the system in the actual operating environment for a large number of security scenes testing, the average

number of times the security analysis information is obtained is q_{Δ} . Here Δ is a placeholder. Respectively, with BSD, HSD and RSD instead of the respective indicators of information on the average number of replacement. The frequency of each security is f_{Δ} [12-13].

$$f_{\Delta} = q_{\Delta}/T$$

The system's total update frequency can be calculated by the above formula:

$$f = f_{\text{BSD}} + f_{\text{HSD}} + f_{\text{RSD}} - f_{\text{BSD}} * f_{\text{HSD}} * f_{\text{RSD}}$$

In this paper, the network security threats are simply divided into three types: warnings, errors and attacks. The threat frequency is expressed as R_y . Here $y = 1, 2, 3$, which representing the three threat levels. The resulting attack frequency function is $g(f)$.

The replacement period T of the system can be calculated and the following equation is satisfied:

$$T = 1/f^*$$

Here f^* satisfies $\lim_{f \rightarrow f^*} g(f) = f^*$.

3. Simulation Experiment

The research group will build a heterogeneous mobile network platform based on NS2. And we using the MATLAB simulation platform to attack the system, the success rate of access, bit error rate and other parameters to simulate. By comparing the data with the traditional system and the literature [14], we can verify the anti-attack effect, the success rate and the data fidelity ability of the algorithm.

Figure 5. system of anti-attack data curve

In this paper using 10 groups of commonly used network attacks (including message tampering, MitM attacks, etc.) in the actual network environment. And each group we carried out 100 attacks. The experiment to obtain FIG. 5 system against attacks graph data, we can see that the system can effectively detect and block these network attacks. It can

guarantee the safety of the system, and each group of anti-attack success rate of more than 75%.

Figure 6. System access success rate change data curve

By observing the data rate of the success rate is not difficult to find that The success rate of its authorized users to access gradually become smaller with the system of malicious users continue to increase. But compared with the traditional algorithm, we can that success rate of this algorithm is always guaranteed to be above the traditional algorithm data curve. Article System Access success rate gradually stabilized with the gradual increase of malicious users. It can effectively prove the stability of the system.

In order to better verify the accuracy of the algorithm. We compare the error rate between the algorithms in the equalizer in the same environment. The data is shown below.

Figure 7. error rate curve of each algorithm

Looking at Figure 7 we can see that the error rate of this algorithm has high stability. The bit error rate remains essentially unchanged, after the number of iterations is 300. But the traditional algorithm has been growing from beginning to end. By comparison, although the algorithm can have a more stable bit error rate, But the steady-state error rate is higher

than this algorithm. Therefore, it can be proved that the algorithm has high accuracy.

4. Conclusion

This article proposed a system architecture based on mutual trust system. The service is terminated for the node by detecting the fault or abnormal state of the mobile node in real time. In the process of system authentication using 802.1X authentication to improve the security of the system. And it combines the actual running test data to optimize the trust update algorithm. It will be reduce the actual operational security threats in the environment. The experimental results show that the experimental results are in accordance with the expected results by testing the system's anti - attack, the success rate of access and the bit error rate. It shows a good anti-jamming capability with data fidelity. And it can effectively reduce the risk of user data leakage, with a certain practical value.

Acknowledgements

The paper is subjected by the following project funding:

Guangdong Provincial Department of Education of young creative talents of Natural Science Fund Project (2015KQNCX227)

References

- [1] Zhu L, Zhan Z. A random key management scheme for heterogeneous wireless sensor network[C]// Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on. IEEE, 2015:1-5.
- [2] Kumar P, Ylianttila M, Gurtov A, et al. An Efficient and Adaptive Mutual Authentication Framework for Heterogeneous Wireless Sensor Network-Based Applications[J]. *Sensors*, 2014, 14(2):2732-2755.
- [3] Yu X. Security Key Management Scheme in Heterogeneous Wireless Sensor Networks Based on Clustering Strategy[J]. *Journal of Networks*, 2013, 8(9): 2114-2120.
- [4] Turkanović M, Brumen B, Hölbl M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion[J]. *Ad Hoc Networks*, 2014, 20(2):96–112.
- [5] Deebak B D. Secure and Efficient Mutual Adaptive User Authentication Scheme for Heterogeneous Wireless Sensor Networks Using Multimedia Client–Server Systems[J]. *Wireless Personal Communications*, 2015:1-23.
- [6] Jiang JM, Peng MG, Zhang KC, Li L. Energy-efficient resource allocation in heterogeneous network with cross-tier interference constraint[J]. *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*. 2013.9:168-172
- [7] Samuel H, Zhuang W. Preventing Unauthorized Messages and Achieving End-to-End Security in Delay Tolerant Heterogeneous Wireless Networks[J]. *Journal of Communications*, 2010, 5(2):152-163.
- [8] Mahshid M K, Eslamipoor R. An efficient and secure authentication for inter-roaming in wireless heterogeneous network[J]. *Social Network Analysis & Mining*, 2014, 4(2):1-10.
- [9] Hou H F, Xin-Sheng J I, Liu G Q. Identity-based anonymity authentication protocol in the heterogeneous wireless network[J]. *Journal on Communications*, 2011, 32(5):153-161.
- [10] Liu G Q, Hou H F. Research on access authentication mechanisms for 3G and WLAN and integrated wireless network between them[J]. *Application Research of Computers*, 2009, 26(11):4023-4026.
- [11] Shrestha AP, Choi DY, Kwon GR, Han SJ. Kerberos based authentication for inter-domain roaming in wireless heterogeneous network[J]. *Computers and Mathematics with Applications*. 2010,60(2):245-255.
- [12] Deng Y, Wang G, Cao J. Trust-Based Fast Inter-Domain Secure Handoff over Heterogeneous Wireless Networks[C]// *Wireless Communications, Networking and Mobile Computing (WiCOM)*, 2011 7th International Conference on. IEEE, 2011:1-5.
- [13] Durresi A, Durresi M, Barolli L. Secure authentication in heterogeneous wireless networks.[J]. *Mobile Information Systems*, 2008, 4(2):119-130.
- [14] Yoon SHY, Lee SS, Kim, SH. Robust mutual trust architecture for safety critical service in heterogeneous mobile network environment[J]. *Telecommunication Systems*. 2015,60(2): 275-284.