International Journal of Sciences

Research Article Volume 7 – July 2018 (07)

WLAN Mesh Security Access Method Based on Blockchain Technology

Chen Yang[1,2]✎, Kun Yang[1,2], Xin Jiang[1,2]

[1]State Key Laboratory of Geohazard Prevention and Geoenvironment Protection, Chengdu University of Technology, Chengdu 610059, China
[2]College of Nuclear Technology and Automation Engineering, Chengdu University of Technology, Chengdu 610059, China

Abstract: As a brand-new network structure, WLAN Mesh network is a distributed network with large capacity, fast speed and wide coverage. However, the security problems caused by the characteristics of wireless connection are not negligible. This paper proposes a new blockchain-based WLAN Mesh design method, including user encryption module, blockchain authentication module and kernel space module. Using the blockchain technology, each user's access authentication request is treated as a transaction, and all authentication records in the mesh network are treated as public ledgers. This method based on blockchain enables secure access to the network and prevents malicious attacks.

Keywords: Block chain,WLAN Mesh, Public Ledgers, Access Method

1. Introduction

WLAN Mesh network is a wireless broadband access network technology that has been rapidly developed in recent years. It does not require a pre-built infrastructure such as a base station, but uses a distributed idea to construct a dynamic self-organized wireless multi-hop network. Users within the coverage can make high-speed wireless access to the Internet anytime and anywhere[1]. The wireless Mesh network inherits the characteristics of wireless Ad-hoc network without center, no infrastructure, multi-hop, self-organization, and it has developed a new architecture to provide IP broadband access. A wireless mesh network consists of two nodes: a Mesh router and a Mesh client[2-4].

In the wlan mesh network, the mesh ap nodes are connected wirelessly, and the data transmission can be forwarded by multiple hops, making the mesh network more vulnerable to active intrusion, passive eavesdropping, identity forgery and data tampering. Therefore, while improving routing and problems in the wlan mesh network, security issues are becoming more and more important[5].

2. Related Works

2.1. Blockchain

Blockchain technology is called distributed ledger technology. It is an Internet database technology[6]. It is characterized by decentralization, transparency and transparency, so that everyone can participate in database records. Blockchain is a new application mode of computer technology such as distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm[7-8]. The consensus mechanism is a mathematical algorithm for realizing trust and acquiring rights between different nodes in the blockchain system[9].

According to the characteristics of the blockchain identity authentication technology, the identity information of the applicant for the network needs to be encrypted. The encryption method used in this article is hash encryption[10]. After the incoming user is encrypted, a pair of keys representing their identity will be assigned. This is unique to the secret key and is divided into a public key and a private key.

2.2. WLAN Mesh

A wireless mesh network is a wireless network that is completely different from a traditional wireless network. It can connect wireless routers that are far away from each other and cannot be directly connected through some intermediate nodes. That means each node in the network can send and receive signals[11]. It is multi-hop, distributed, self-organizing, etc. It can achieve a wide range of wireless coverage through simple deployment. As a new form of network structure, Mesh networks have been incorporated into the 802.16, 802.16e and 802.1s standards[12-13].
Wlan Mesh can be seen as a fusion of wireless local area network (WLAN) and wireless Mesh networks, using

Published at: http://www.ijsciences.com/pub/issue/2018-07/
DOI: 10.18483/ijSci.1753; Online ISSN: 2305-3925; Print ISSN: 2410-4477

✎ Chen Yang (Correspondence)
✉ innerai @163.com
☎ +

wlan technology to achieve the transmission of each Mesh link. At the same time, the multi-hop networking method solves many problems such as poor scalability and poor robustness of the traditional wlan[14-15].

3. Wlan Mesh Manager Overview

Wlan Mesh Manager includes user space module,blockchain authentication module and kernel space module. User Space includes below components: information encryption, digital signature and login authentication. Blockchain authentication module includes Core chain, mysql public ledger and public chain. Kernel space module includes wifidriver and netlink. These three modules jointly implement the wlan mesh security access based on the blockchain. All distributed ledgers maintain the network access records of all authentications in the blockchain and make it safer for new users to access the network.The specific architecture of Wlan Mesh manager based on blockchain is shown in the following figure 1.

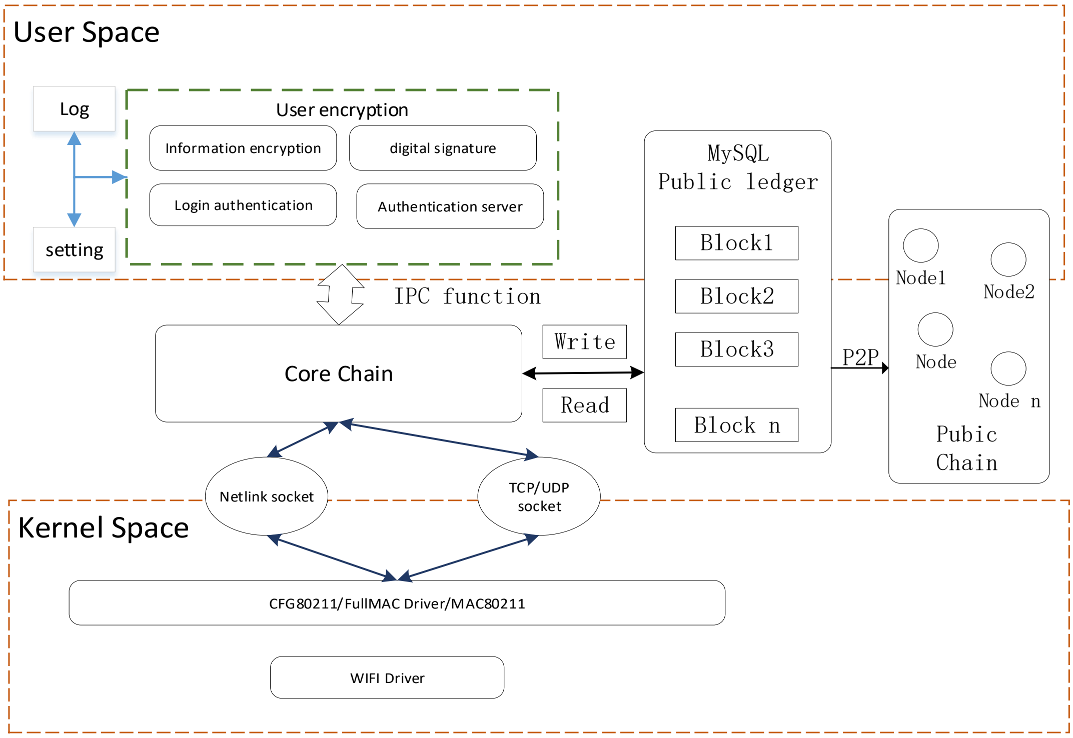

Figure 1 –Wlan Mesh Manager Based on Blockchain in System

3.1. User encryption module

The function of the user encryption module is to implement the maintenance of the application user login and setting up its own information. The user information encryption module encrypts the three scenarios of information encryption, digital signature and login authentication. After the user submits an application for network access, it will use asymmetric cryptography. The information encryption scenario is mainly caused by the information sender (network access user) encrypting the information using the public key of the recipient (corechain). And it will send the information to the core chain, at the same time the core chain decrypts the information by using its own private key. The digital signature scheme is sent by the sender (incoming network user) to the core chain with its own private key, and the core chain uses the public key of the incoming network to decrypt the information to ensure that the information is made by the network user. The login authentication scenario is performed by the core chain using the private key to encrypt the login information and then sending it to the server. After receiving, the latter uses the public key of the core chain to decrypt and authenticate the login information.

The information encryption scenario uses public key encryption and private key decryption to ensure the security of the information; the digital signature scenario is to use private key encryption and public key decryption to ensure the attribution of digital signature; the login verification scenario uses private key encryption and public key decryption . The asymmetric encryption mechanism of the user information encryption mechanism is shown in Figure 2.

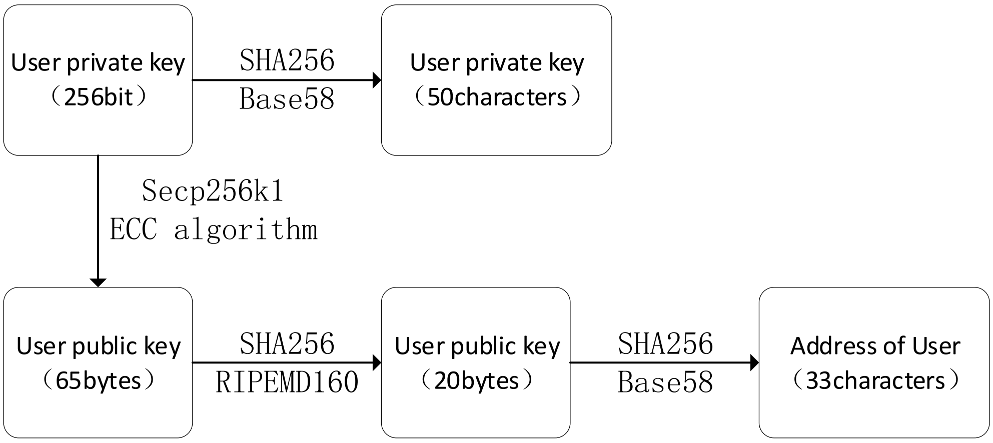
User private key （256bit）
SHA256
Base58
User private key （50characters）
Secp256k1
ECC algorithm
User public key （65bytes）
SHA256
RIPEMD160
User public key （20bytes）
SHA256
Base58
Address of User （33characters）

Figure 2 –Asymmetric Encryption Process for User Information

The authentication server generally generates a 256-bit random number as a private key by calling the underlying random number generator of the operating system. For easy identification, the 256-bit binary form of the private key will be converted by the SHA256 hash algorithm and Base58 to form a 50-character length of easy-to-recognize and write private key for incoming application users. The public key of the application user is generated by the private key first through the Secp256k1 elliptic curve algorithm to generate a random number of 65 bytes in length. The public key can be used for the address used in transaction authentication. The generation process is to first perform the SHA256 and RIPEMD160 double hash operation on the public key to generate a summary result of 20 bytes length (ie, the result of Hash 160), and then pass the SHA256 hash algorithm and the Base 58 converts the address of the incoming user identity of 33 characters. The public key generation process is irreversible, that is, the private key cannot be reversed by the public key, so the private key of the user is the most important, and only the network user knows. The encrypted information will be transmitted to the core chain by means of process communication.

3.2. Blockchain authentication module and kernel space module

Blockchain authentication module includes Core chain, mysql public ledger and public chain. After the Core chain receives the user application information (public key and network access basic information) sent by user space through the Inter-Process Communication（IPC）, the Core chain verifies the public key and the private key provided by the users. If the verification succeeds, the node of the network access user is confirmed as a legal node. Otherwise, it directly refuses to access the wireless LAN. After the verification is passed, the Core chain encrypts the authentication record of each incoming network user into a block, and stores the formed block in the MySQL public ledger to form a blockchain for successive authentication. The public ledger will use P2P technology to distribute all the information of the newly added block to each node in the blockchain, and all nodes store and protect their information. In this way, all nodes jointly maintain all the authentication records on the ledger, improve the security of the network access and prevent illegal tampering and hacking.

Kernel space module includes Netlink socket, TCP/UDP socket and WIFI Driver. Netlink sockets are a special kind of interprocess communication (IPC) used to communicate user processes with kernel processes. They are also the most common interface for network applications to communicate with the kernel. Cfg80211 is used for configuration management of wireless devices. Mac80211 is a framework that driver developers can use to write drivers for SoftMAC wireless devices. After the kernel is verified, the kernel chain calls the kernel's WiFi driver module through the netlink socket or TCP/UDP socket and the routing algorithm to complete the user's network application and the user's WiFi connection, thereby realizing its safe Internet access function.

4. Conclusion

This paper first introduces the structure and characteristics of the wireless mesh network, and introduces the decentralized and non-tamperable nature of the blockchain. Due to its multi-hop network topology, WLAN Mesh networks bring high-capacity, high-speed, easy-to-expand, and unimpeded features, as well as wireless LAN security threats. Since the router nodes in the WLAN mesh network are connected by wireless multi-hop links, it is necessary to study the security scheme for accessing the wireless mesh network.

The focus of this paper is to combine a secure access network with a blockchain. It uses the user's authentication requirements to conduct transactions. All authentication records in the mesh network are treated as public ledgers to securely access the network and prevent intentional attacks. Therefore, accessing the

WLAN mesh network is more secure.

Reference

1. Abujoda, A.; Dietrich, D.; Papadimitriou, P.; Sathiaseelan, A. (2015): Software-defined wireless mesh networks for internet access sharing. Computer Networks, vol. 93, no. P2, pp. 359-372.
2. Choumas, Kostas, S. I. K. T. a. L. (2014): Video-aware multicast opportunistic routing over 802.11 two-hop mesh networks. In Eleventh IEEE International Conference on Sensing, Communication, and NETWORKING, pp. 486-494
3. Dobbertin, H.; Bosselaers, A.; Preneel, B. (1996): Ripemd-160: A strengthened version of ripemd. Fast Software Encryption Fse, vol. 1039, pp. 71-82.
4. Majumder, A.; Roy, S. (2017): Implementation of enhanced forward pointer-based mobil- ity management scheme for handling internet and intranet traffic in wireless mesh network. Telecommunication Systems, pp. 1-24.
5. Hiertz G R, Denteneer D, Max S, et al. IEEE 802.11S: the WLAN mesh standard[J]. Wireless Communications IEEE, 2010, 17(1):104-111.
6. Kosba A, Miller A, Shi E, et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts[C]// Security & Privacy. IEEE Computer Society, 2016:839-858.
7. Pilkington M. Blockchain Technology: Principles and Applications[J]. Social Science Electronic Publishing, 2016.
8. Pass R, Seeman L, Shelat A. Analysis of the Blockchain Protocol in Asynchronous Networks[C]// International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2017:643-673.
9. Vukolić M. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication[C]// International Workshop on Open Problems in Network Security. Springer, Cham, 2015:112-125.
10. Ylihuumo J, Ko D, Choi S, et al. Where Is Current Research on Blockchain Technology?—A Systematic Review[J]. Plos One, 2016, 11(10):e0163477.
11. Bahr M. Proposed routing for IEEE 802.11s WLAN mesh networks[J]. 2006:5.
12. Rajakumar V, Smadi M N, Ghosh S C, et al. Interference Management in WLAN Mesh Networks Using Free-Space Optical Links[J]. Journal of Lightwave Technology, 2008, 26(13):1735-1743.
13. Zhu R. Intelligent rate control for supporting real-time traffic in WLAN mesh networks[M]. Academic Press Ltd. 2011.
14. Sherman I, Kangude S. Apparatus for and method of synchronization and beaconing in a WLAN mesh network[J]. 2009.
15. Bari S M S, Anwar F, Masud M H. Performance study of hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s WLAN mesh networks[C]// International Conference on Computer and Communication Engineering. IEEE, 2012:712-716.