A Blockchain Based Authentication Mechanism in Wireless Local Area Network

Yuan Yao[1, a], Tao Xie[2, b]

[1]School of Computer, University of Defense Technology, Changsha 410073, China;

[2]School of Computer, University of Defense Technology, Changsha 410073, China;

[a]yaoyuan17@nudt.edu.cn, [b]hamish@vip.sina.com

Abstract. Considering the security of the widely used WLAN technology, a secure, flexible and reliable authentication scheme is definitely necessary. Most of the existing schemes adopt centralized authentication process, making it vulnerable to DDoS attack, faked AP and the leak of shared secrets. We propose a blockchain based authentication system in the WLAN scenario, taking advantage of the decentralization and tamper resistant characteristics of the blockchain, to make everyone know the exactly information about the WLAN and have the opportunity to authenticate other's access request. Our analysis and comparison show that it's more convenient and has better security properties.

Keywords: WLAN, Security, Decentralized, Authentication, Blockchain, Smart Contract.

1. Introduction

With the development of Internet technology, it has greatly facilitated people's lives and work. Compared with connecting desktops and laptops to the Internet with a cable, in public places like schools, parks, stations and restaurants, more and more people prefer to network their laptops, smart phones, and other devices by Wi-Fi, which is one kind of technology using IEEE 802.11 protocol in WLAN and allows Wi-Fi capable devices to receive and transmit data using radio frequencies when they are in range of a Wi-Fi network.

However, more and more attacks against devices in WLAN have been launched due to the openness and flaws of the network using 802.11 protocols. They found that some users can access the network without permission and often launch attacks using technologies like fake APs, password cracking, denial of service to occupy network traffic maliciously, or even steal user's private data. Therefore, a reliable and secure authentication mechanism are in great demand to prevent unauthorized access to any resources , and provide users with more convenient, fast, and secure WLAN services.

Many authentication systems have been used in schools, stations and other public places when devices try to be connected to the Internet through an access point, denoted as AP. But there are some defects in existed systems: (1) A server often is needed to store and check authentication information and security preference. (2) Switching and re-authenticating is necessary for small-scale movement between different APs' ranges. (3) Authentication between devices and AP requires several steps of interaction. In this paper, we propose a blockchain based solution for the access and authentication process of WLAN devices to solve these problems.

The remainder of our paper is organized as follows. In section 2, we introduce several existing authentication solutions in WLAN. In section 3, we propose our blockchain based authentication mechanism. A comparison between our work and others is also introduced in section 4 to prove the convenience and security of our proposed solution. In section 5, we provide conclusions and future work.

2. Authentication in WLAN Access

Authentication is an important technology to prevent active attacks in modern cryptography. It's crucial to the security of various information systems in an open environment. The main purpose of authentication is to provide the authenticity, integrity and non-repudiation of information in order to resist active attacks such as forgery, tampering and replay [1]. That's to say, authentication is a kind of mechanism ensuring that the sender of the message is the person I want to communicate with, and the received message is the message the sender wants to transmit. That's just what we need in the open access in WLAN. Authentication mechanism in wireless network can be divided into two categories according to whether a password is used in the process.

2.1 Existing Mechanisms

Unencrypted authentication is mainly implemented by setting SSID and filtering MAC address.

(1) Schemes based on SSID. SSID is short for Service Set Identifier, which contains some information about the AP. SSID is usually broadcasted by an AP and scanned by devices in the range of an AP. We can divide the network of an AP into multiple subnets with different SSIDs and permissions. When necessary, we can also hide the SSID broadcast in order to avoid detection by others.

(2) Schemes based on MAC address. An AP can determine whether devices are allowed or denied to access the AP by filtering their MAC addresses. Only if a device's MAC address has been registered to the AP can it be allowed to access the AP.

Encrypted authentication is more common in practical situations. We can use different encryption method in different scenarios

(3) Schemes based on encryption method. Before trying to access the WLAN, the user's device should provide the correct key of the AP. According to the way the key works, there are some protocols including WEP, WPA/WPA2-PSK, WPA/ WPA2-Enterprise. Since WEP protocol has been cracked, WPA style protocols require a four-way handshake process. A pairwise master key (PMK) is generated by combining the pre-shared key and a SSID. After PMK is distributed to a AP and user's devices, they begin to negotiate a pairwise transient key (PTK), which is generated dynamically in every connection and used to guarantee the confidentiality of messages in communication [2].

2.2 Deficiencies and Attacks

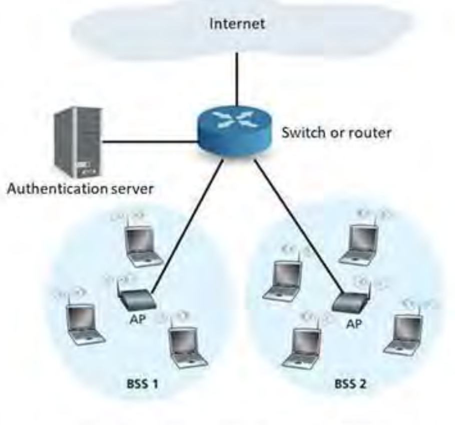

Fig. 1 A normal authentication mechanism with a third-party authentication server

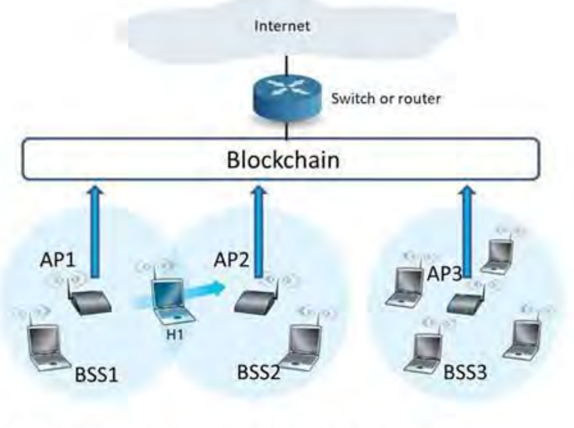

Fig. 2 A blockchain based decentralized authentication mechanism without a server

In fact, methods in 2.1 lack the features of authenticating APs, and give more opportunities for attackers to launch password cracking, DDoS attacks and attacks against handshakes in the authentication process between devices and the AP or the server. WPA-Enterprise uses a server to store correct identity information and check whether devices trying to connect the AP matches these conditions, as shown in Fig. 1. In the personal version of WPA (also called WPA-PSK), the AP play a similar role like what the server does. There is no doubt that APs and servers are the bottleneck of the system. These schemes are neither safe nor convenient.

Inspired by blockchain and smart contract technology, we propose a decentralized authentication mechanism. Fig. 2 illustrates the architecture of our authentication scheme, which has a blockchain system containing several devices as nodes and devices information packed as blocks. Unlike the schemes discussed above, our novel method offers a decentralized authentication scheme for devices'

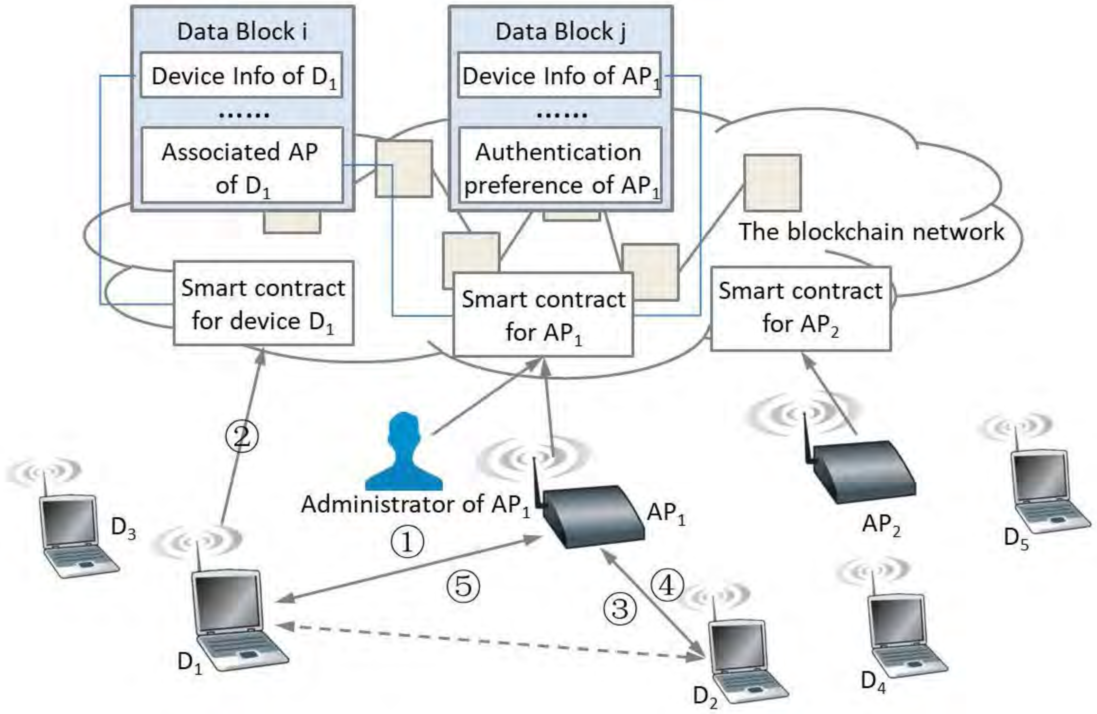

Fig. 3 The main communication flow of the blockchain based authentication mechanism

access to the AP without relying on a centralized authority storing users' information. Once a device try to access an AP, one of the devices having been in the system packs its authentication message together with AP information into blocks and broadcast it to the blockchain system.

3. System Implementation

3.1 Overview.

A blockchain is a distributed, append-only log of time-stamped records that is cryptographically protected from tampering and revision [3]. After nine years since the concept has been proposed, many work and applications have been improved by the blockchain approach. In [4], the author designed a secure dynamic spectrum access in moving cognitive radio networks based on the idea of blockchain. In [5], there is a blockchain based gateway to manage IoT devices. Smart contract technology is also used in medical data share, copyright manage, electricity trade, etc. These efforts attempt to use blockchain in different distributed scenarios and give me some original ideas for creating this system.

3.2 Blockchain Design

Each block of the original Bitcoin system contains data such as timestamp, previous block header hash, transaction details, transaction counter, block size, etc [6]. In our system, a transaction means that there is a device trying to access to an AP. In this way, our transaction message includes information of the devices and the AP we trying to access, as we have illustrate in figure 3.The AP's information is receiving from the blockchain system after our device runs a client to download all the blocks we need.

Although our scheme is a decentralized system, the privilege of managing the authentication preference is given to some users. These preferences include the schemes we have discussed in 2.1, which would determine whether a device can pass the authentication by match the correct MAC, SSID, password or other messages. Every device act as a node in the blockchain system. Devices connecting to the same AP make up a Basic Service Set, denoted as BSS, and have a SSID. Devices in one BSS have the opportunity to authenticate a new device's access after it receiving the requesting information through P2P communication.

3.3 Authentication Process

The main communication flow has been presented in Figure 3 and will be illustrated as follows:

1) Initialization: All of the available and secure APs' information have been registered and recorded in the blockchain by administrators. In step ①, AP_1 broadcast its SSID to the network and device D_1 receive it. D_1 try to pass the authentication and connect to AP_1 and this is just the transaction we are going to deal with. After D_1 runs a client program, it receives all the information on the blockchain. By looking up the corresponding block about AP_1, D_1 gets the correct authentication message of AP_1. Then D_1 pack the message with its own device information into a message *msg* and send the block to the blockchain system in step ②.

$$msg = F\ (\text{information of } D_1, \text{information of } AP_1)$$

(*F is a encryption function that can be used to pack some message into blocks. In Bitcoin system, F is a Hash function. Here we can use different kind of encryption function we can.*)

2) Authentication: As a BSS, there is already several devices connecting to AP_1. Suppose that D_2 and D_3 have been in the BSS. When they receive *msg* by broadcast in the blockchain system in step ③, they know there is a transaction about D_1's connecting to AP_1 to validate. Randomly, one of the devices is chosen for the validation, and now we suppose D_2 is chosen. In the authentication process, D_2 validates whether AP_1's message kept in block i is the same with what has been kept by D_2 about AP_1. Once the two matches, they will calculate a new message based on *msg* and D_2's information. This message will be appended to the previous block and become the data block i after broadcasting it to the system in step ④.

$$\text{Data block i} = F\ (\text{information of } D_1, \text{information of } AP_1, \text{information of the validator: } D_2)$$

3) Communication: From the updated information in the blockchain, AP_2 knows that D_1 has passed the authentication of a connection request from D_1 to AP_1. Then AP_1 send a reply to D_1 in step ⑤. As long as AP_1 can find a block contains the correct information about itself, it provides access to the device with the information.

There are two smart contract, one for user's device and one for the AP. Smart contract can be used to interact with the AP and user's device. For example, when SSID of an AP changes, a new block with the new information will be created. We can see from the authentication process that there doesn't need a server any more. All devices in the system have a copy of block information containing the information we can use to validate the authentication.

In the DDoS scenario, large quantities of devices try to access one server and collapse the network. But in our scheme, the authentication scheme is assigned to different devices and there is not a server. So DDoS attack is avoided. The same comes to faked AP : information of trusted APs is added to the blockchain system by the administrator, so faked AP can't be connected by devices in our system.

4. Performance Comparison

In some previous researches [7], 4 metrics have been proposed to compare different authentication mechanism in WLAN, which include scalability, safety, convenience and maintenance difficulty. Each technology has strengths and weaknesses and we should strike a balance between them.

Although our work hasn't been finished yet, we can get some intuitive result from the designing of our scheme. As our system is decentralized, new devices and APs can join the authentication system in a more secure and convenient way. In the table below, scheme 1-3 represent the corresponding three authentication method in 2.1. Scheme 4 is for the blockchain based mechanism we proposed in 3.3. Obviously, our scheme is a little more complex than others. But it can do better in safety, scalability and Convenience. More work need to do in the future to develop the performance of this scheme.

Table 1 Five Scheme comparing

Scheme	Scalability	Safety	Convenience	Maintenance
1	Small	Small	Medium	Poor
2	Small	High	Poor	Medium
3	Small	Medium	Poor	Medium
4	Large	High	High	High

5. Conclusion and Future Work

Blockchain technology is currently in a nascent state and would not be evaluated in a general way to determine whether one application is superior to previous schemes. But many scenario provide schemes to solve practical problems. Our novel authentication mechanism based on blockchain intends to function in a scenario without a centralized sever. Authentication tasks are randomly assigned to a node in the blockchain system. When a device has been authenticated by the system, its information is stored into a block by the randomly assigned node. Only if the information in the block matches the AP's authentication message can the device pass the access to the AP. In this way, we can avoid some kind of attacks that attempt to destroy the server and steal important data stored in the server. Smart contracts are used to configure the authentication preference and looking for corresponding information in the process.

The proposed mechanism can do better in some aspects from our comparison. First, we should design an appropriate function to pack APs and devices' information. In [8], the function can identify there exists the correct information but don't let anyone know what is in the block. Second, we should reduce the storage by technology like blockchain sharding. Third, there still are some details we must take into consideration: (1) since several APs are in the blockchain system, we can reduce the authentication process when our device switches from an AP to another; (2) some work should be done when devices are out of the network, information of APs, devices and passwords are changed, and some other aspects.

Acknowledgements

Supported by National Natural Science Foundation of China (61472476).

References

[1]. Xiaohang Li, Hongxia Wang, Wenfang Zhang. Authentication Theory and Application[M]. Tsinghua University Press, 2009, p. 2-4.

[2]. LI An-huai, JING Ji-wu. Distributed WLAN access system[J]. Computer Engineering and Design. Vol. 28 (2007) No. 1, p. 62-65.

[3]. Information on: https://zh.wikipedia.org/wiki/%E5%8C%BA%E5%9D%97%E9%93%BE

[4]. Kotobi K, Bilen S G. Secure Blockchains for Dynamic Spectrum Access : A Decentralized Database in Moving Cognitive Radio Networks Enhances Security and User Access[J]. IEEE Vehicular Technology Magazine. (2018), p. 1-1.

[5]. Cha S C, Chen J F, Su C , et al. A Blockchain Connected Gateway for BLE-based Devices in the Internet of Things[J]. IEEE Access. (2018), p 1-1.

[6]. Ryan H, Amir H, Aniket K . Blockchain Access Privacy: Challenges and Directions[J]. IEEE Security & Privacy. Vol. 16 (2018) No. 4, p. 38-45.

[7]. Peng Xu, Xuefeng Yu. Analysis and Research on Access Authentication Mechanism in WLAN[J]. Information Security and Technology. Vol. 6 (2015) No. 7, p. 42-44.

[8]. KOSBA A, MILLER A, SHI E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[C]. 2016 IEEE Symposium on Security and Privacy (SP). San Jose, CA, USA, May 22-26, 2016.