 CMC, vol.58, no.1, pp.45-59, 2019

A Blockchain-Based Authentication Protocol for WLAN Mesh Security Access

Xin Jiang[1], Mingzhe Liu[1, *], Chen Yang[1], Yanhua Liu[1] and Ruili Wang[2]

Abstract: In order to deploy a secure WLAN mesh network, authentication of both users and APs is needed, and a secure authentication mechanism should be employed. However, some additional configurations of trusted third party agencies are still needed on-site to deploy a secure authentication system. This paper proposes a new block chain-based authentication protocol for WLAN mesh security access, to reduce the deployment costs and resolve the issues of requiring key delivery and central server during IEEE 802.11X authentication. This method takes the user's authentication request as a transaction, considers all the authentication records in the mesh network as the public ledger and realizes the effective monitoring of the malicious attack. Finally, this paper analyzes the security of the protocol in detail, and proves that the new method can solve the dependence of the authentication node on PKI and CA.

Keywords: WLAN mesh, block chain, authentication protocol, public ledger.

1 Introduction

WLAN mesh network is a kind of multi-hop, self-organizing and self-healing broadband wireless distributed network structure. The emergence of WLAN mesh network and its unique network structure features can solve the constant ubiquity of high-speed internet access. As the WLAN mesh network extends the range of traditional wireless networks, it is known as the Wireless Broadband Future [Yu and Wong (2015)] and the economic broadband world's driving [Hung and Bensaou (2014)].

The security technology in WLAN network structure cannot be directly applied to the WLAN mesh network. In WLAN mesh network, the mesh AP nodes are connected wirelessly, the data transmission can make mesh network more susceptible to active intrusion, passive eavesdropping, identity forgery, data tampering and other attacks by multi-hop forwarding [Niizuma and Goto (2017)]. Smart devices based on ARM processor bring us more convenience, they also become an attractive target of cyber-attacks. While improving the routing and speed performance in wireless mesh network, the security problem is becoming more and more important. With the increasing demand for data confidentiality and privacy protection in modern society, the WLAN mesh network security has also become a major obstacle to large-scale commercial Mesh

[1] State Key Laboratory of Geohazard Prevention and Geoenvironment Protection, Chengdu University of Technology, Sichuan, China.

[2] Institute of Natural and Mathematical Sciences, Massey University, Auckland, New Zealand.

[*] Corresponding Author: Mingzhe Liu. Email: liumz@cdut.edu.cn.

network.

To address such security issues, Abujoda et al. [Abujoda, Dietrich, Papadimitriou et al. (2015)] implement and deploy a software-defined WMN (SDWMN) control plane in one of the confined community networks, in order to coordinate WMN transmission redirection. Through a comparative study of WMN and paws, Valdes et al. [Valdes, Montesinos, Ariza et al. (2015)] further study the potential benefits of shared WMN for public internet access. Their experimental results have shown that the shared WMN can provide a higher share of bandwidth utilization and can accommodate a large number of inbound traffic. In Hussain et al. [Hussain, Ahmed, Saikia et al. (2016)], a multi-hop wild network based on gateways is proposed to improve end-to-end throughput and latency performance, and a significant improvement in the related MAC protocols is shown in saturation throughput and average end-to-end packet latency in multi-hop. Majumder and Roy [Majumder and Roy (2017)] introduce an improved version of FPBR program to deal with Internet and Intranet traffic. A mobile management scheme based on enhanced forward pointer is implemented to handle Internet and Internal network traffic in wireless mesh networks. Choumas et al. [Choumas, Syrigos, Korakis et al. (2014); Yu and Wong (2017)] proposed a network resource management framework by considering the characteristics of wireless mesh network and small interval interference. Deng et al. [Deng, He, Gui et al. (2017)] focus on analyzing the MAC layer performance of IEEE 802.11s wireless mesh Network in smart grid based on a Markov model.

To our best knowledge, security administrators determine which user(s) can access a particular piece of information in the literature. With that said, these current protocols are more vulnerable to hacking as well as anonymous intrusions. Nonetheless, as a new cryptographic technology, the block chain is seen as a strong fit to provide a suitable solution to addressing this problem through its attractive features such as immutability and decentralization. Block chain is a public ledger of all transactions which achieves decentralized self-management by using point-to-point networks and distributed time stamping servers [Xia, Sifah, Asamoah et al. (2017)]. Developers are already hard at work building applications and services for identity management. A hybrid cryptographic scheme based on block chain was proposed in Monroe by Yuan et al. [Yuan, Xu and Si (2017)], which is independent of central nodes. Sasson et al. [Shen, Mackenzie and Lab (2016); Sasson, Chiesa, Garman et al. (2014)] suggest a new scheme with zero-knowledge proof which allows users to hide transaction information only by interacting with the cryptographic algorithm itself, so that all transactions are created equally. When transactions are generated on block chain, cryptographic signatures are used to judge the legality of the transactions and the identities of the senders. Furthermore, the signature algorithms are aimed at privacy preserving of the transactions, including the addresses of both sides and transaction amount. However, in block chain, there has been mature attack algorithms, such as selfish mining attack [Eyal (2015); Sapirshtein, Sompolinsky and Zohar (2017)], eclipse attack [Heilman, Kendler, Zohar et al. (2015)], and stubborn mining attack [Nayak, Kumar, Miller et al. (2016)]. There is therefore the urgency to develop a block chain-based access control method that sufficiently controls the access to WLAN mesh networks.

Using the advantage of block chain in authentication and encryption, this paper proposed

a block chain-based identity signature by analyzing the safety performance of the proposed scheme. Furthermore, this paper implemented the proposed method on five nodes, and the experimental results confirmed that block chain-based authentication can decrease the authentication delay in multi-hop environment that makes the packet loss rate larger. Note that mining data from multiple data sources to extract useful information [Wang, Ji, Liu et al. (2018)] for better understanding of security risk evaluation should be considered in the future study, and it is also important to analyze the behaviors of target application [Jiang, Liu, Yang et al. (2018)] running on mesh nodes.

2 Overview of mesh network

A WLAN mesh network consists of some mesh nodes having mesh routing functions. These nodes are also served as APs for other mesh nodes and for non-mesh devices having no mesh routing functions. This type of mesh node is referred to as mesh AP hereinafter. Non-mesh devices also can get network access by communicating with the mesh APs by 802.11 infrastructure mode.

Although a WLAN mesh network itself is assumed to be operated by an organization owning the location where the WLAN mesh network is deployed, the WLAN mesh network allows a roaming user to connect the network, which enables mutual use of WLAN facilities among multiple organizations. To deploy campus or enterprise WLAN systems using mesh network technologies, the following security mechanisms should be considered: user authentication, AP authentication, mutual authentication and traffic encryption.

Egners et al. [Egners, Herrmann, Jarmuzek et al. (2014)] showed the real-world testbed equipped with the 802.1X-based authentication mechanism over WLAN mesh network. Fig. 1 illustrates an example of such a deployment. Each arrow indicates that the supplicant (source) is connected to the authenticator (destination). In this deployment method, there are mainly two issues. The first one is that the network administrators must configure secret keys on each AP and RADIUS server. Therefore, the deployment cost will increase as much as the number of mesh APs. Moreover, additional configurations are required if the IP addresses of some mesh APs change when renewing the IP addresses by DHCP or when the network connection to upper networks has recovered.

First, the mesh AP N1 is connected to the backhaul network and N1 obtains its IP address. In order for N1 to forward RADIUS authentication packets to the RADIUS server, the secret key needs to be configured manually at N1's authenticator and the RADIUS server. When N2's supplicant requests network access to N1's authenticator, the AP authentication is processed based on 802.1X between N2's supplicant and the RADIUS server. A shared secret key needs to be set at both N2's authenticator and the RADIUS server in order to allow N2's authenticator to join the RADIUS network. By repeating this operation, the WLAN mesh network is built. Although the mesh APs are authenticated by the local RADIUS server in Fig. 1, the RADIUS server may also be located in an outside network as the same way as mesh network systems.

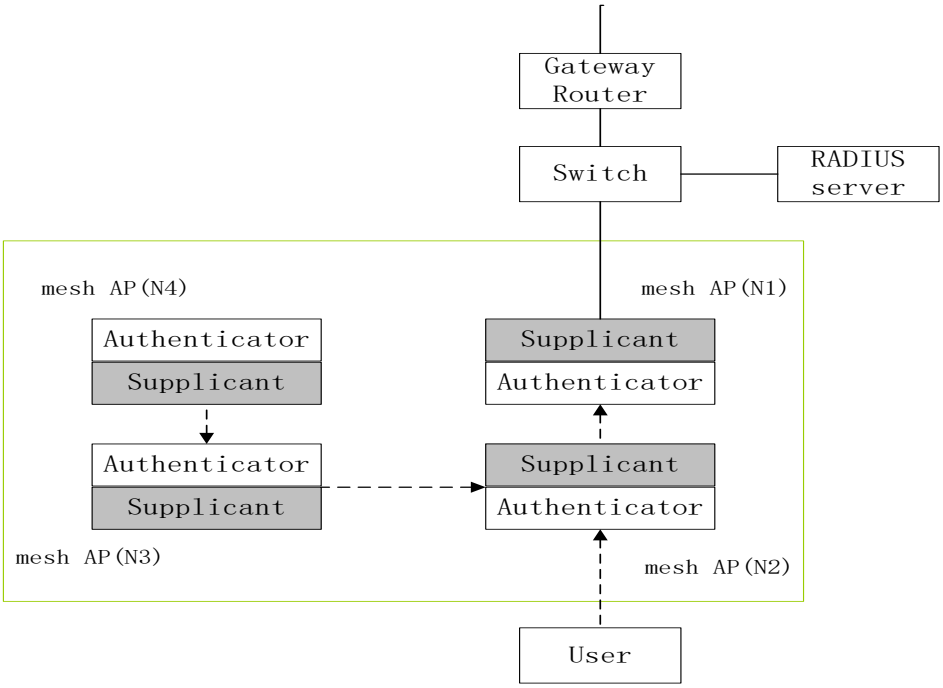

Figure 1: Mesh network overview

3 Block chain-based authentication protocol

Fig. 2 shows the authentication procedure. If the joining node associates with the authenticator AP, the joining node sends the authentication request to the authenticator AP. The authenticator AP checks the realm and examines if the client certificate can be verified locally or not. If the authenticator AP can verify the certificate, the authentication is executed at the authenticator AP.

If the certificate cannot be verified at the authenticator AP, the authentication request is the proxy to the RADIUS server in home institution of the joining node. After the authentication, the joining node gets PMK (Pairwise Master Key) by the 4-way handshake and gets its IP address by DHCP. If the joining node is a mesh AP, the mesh AP tries to establish TLS sessions with the authenticator AP and broadcast this request to block chain, lastly starts to work as an authenticator AP.

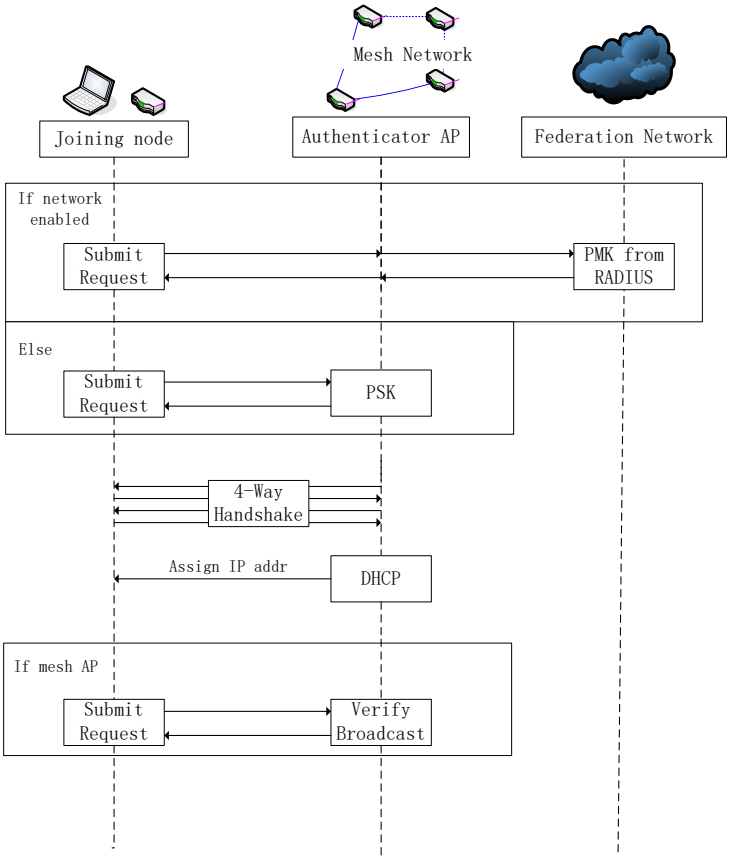

Figure 2: Authentication procedure

3.1 Identity cryptosystem

The user's identity in the scenario can be used as the public key, so there is no need to store and sign the user's public key. In addition, the scheme protects the requester's identity from being stolen by the attacker. Authentication protocol based on Identity cipher system does not need certificate, which makes network configuration simple, system construction cost reduced, system maintenance simple, system running efficiency is improved (see Fig. 3). The specific description of the message in the agreement is as follows:

1) The user A sends public key Pub_A, ID_A and $Sign_A$ to system S.

2) The system S receives the user A's request, generates the random number N_S, and the temp public key Pub_S which is used to do DH key exchange.

3) The temporary public key generated by the system S stored in the node is then computed and extended by the key export function to the shared key MSK between S and A,

$$MSK=H_{KD}(acPub,N_S) \quad (1)$$

And MSK is used to encrypt the identity information dish of the applicant with

symmetric encryption algorithm $\{ID_S\}_{MSK}$, temporary public key Pub_A generated by the received authenticator generates a unicast session key(UMK) between S and A,

$$UMK=H_{KD}(ASPub, N_S|N_A) \quad (2)$$

S computes the signature of the message M_1, $Sign_S = Sign_S(H_2(M_1))$, M_1:

$$M_1=\{ID_S\}_{MSK}|ID_A|ID_S|N_A|N_S|Pub_A|Pub_S \quad (3)$$

4) The system S receives the message from the user A, and uses the extended message to authenticate the key MAK to generate the message authentication code $MAC_{A,S}$, verify the $MAC_{A,S}$, If validation pass:

$$Sign_S = Sign_S(H_2(Pub_A|Pub_S)) \quad (4)$$

5) Using generated message authentication key MAK to generate hash authentication code:

$$Hash_A=SHA\text{-}1(MAK, M_2|Sign_A|Sign_S) \quad (5)$$

Then send the hash code and another information to User A, and also send those to block chain by using P2P technology. Lastly set the authentication status to success.

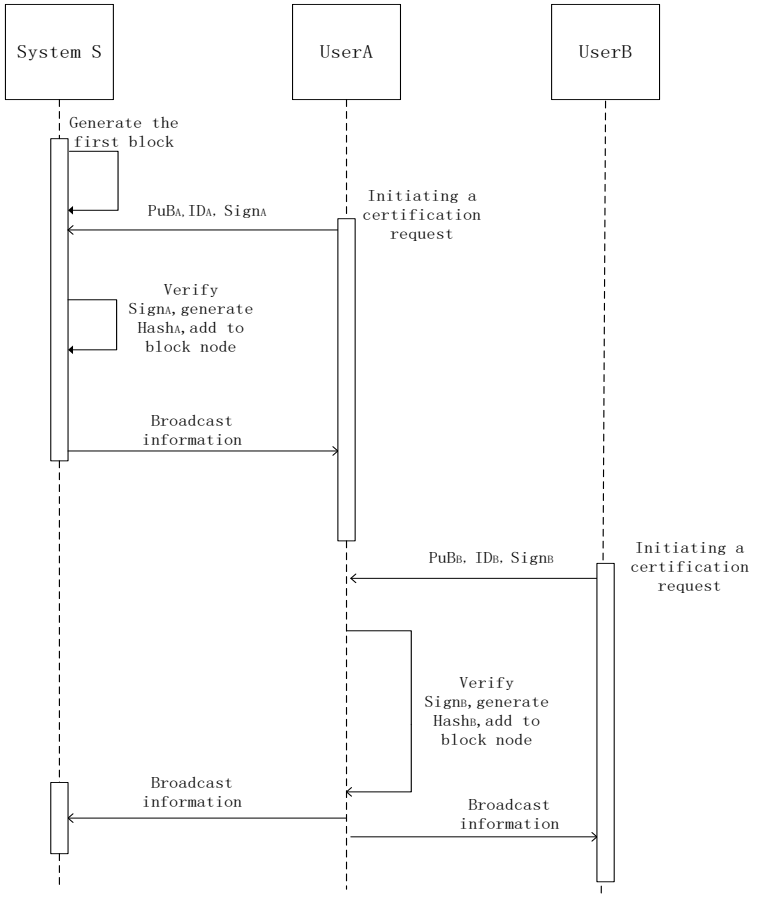

Figure 3: Protocol authentication process

3.2 Certification process

When the system s authenticates the user A's personally identifiable information, it can authenticate the user A's personally identifiable information through the third party verification platform, including the way of verifying by email or phone, or other mutually ap-proved way. When the validation fails, the application status is returned, and the public key and digital signature provided by user A is validated when the validation succeeds. When validation fails, returns the status of the application, and when the validation succeeds, the user A's related personally identifiable information (mailbox or cell phone number, etc.) and the public key are hashed, and the system s generates a digital signature with its own private key, plus a timestamp, broadcast to the public ledger (see Fig. 4).

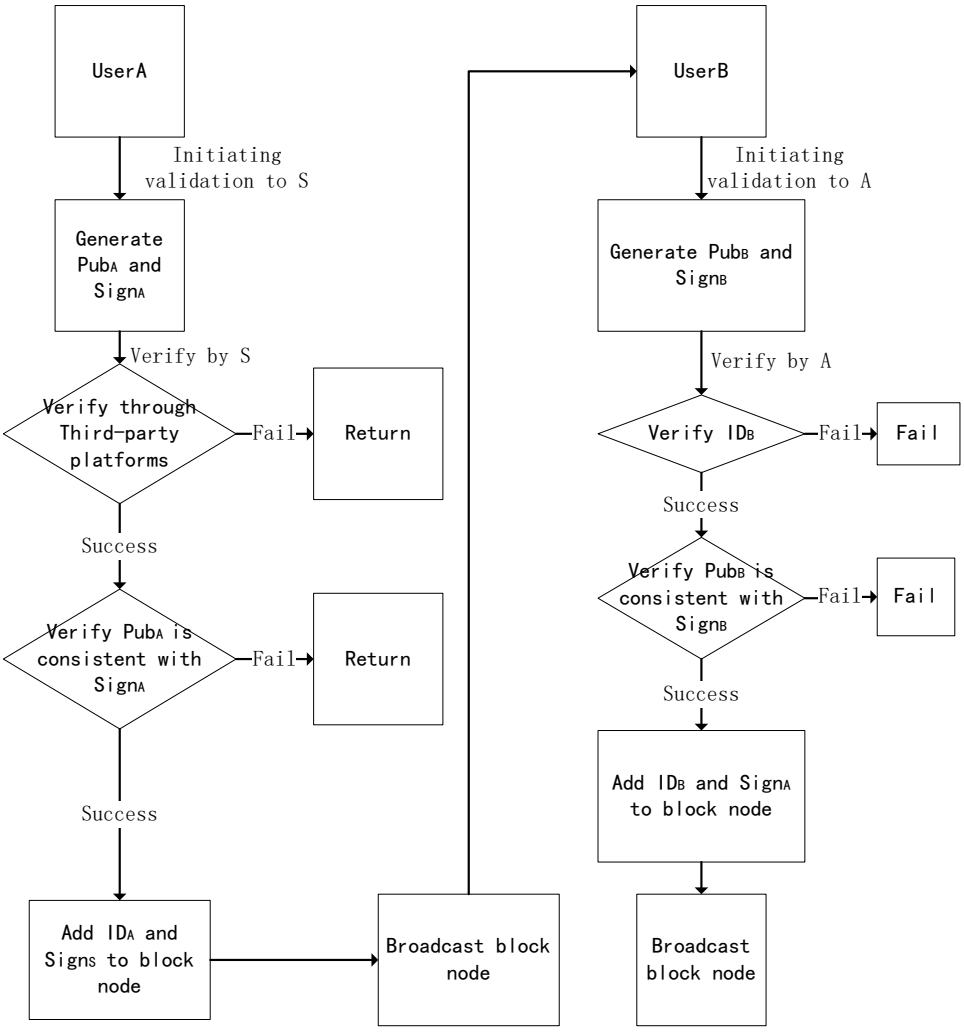

Figure 4: The Process for add to block chain in authentication

When User B joins this block chain, User B can apply to user A to launch this block chain application, User B will own security equipment to generate public key and personal identity information (such as mailbox or mobile phone number, etc.), with the private key for digital signature, all submitted to User A, User A verifies User B's personal information and verifies User B's digital signature, and when validation passes, the User B's personally identifiable information and the public key generate a hash value, user A creates a digital signature with its own private key and adds a timestamp, and finally broadcasts to the block chain to open the ledger.

3.3 System implementation

WLAN mesh management software provides a variety of block chain interfaces including trading interface for WiFi channel data transmission, real-time submission, mesh core for authentication request. IPC notifies the core block chain module (core chain) for verification work. After the verification is completed, the system will issue two asynchronous messages, one is to call the kernel's WiFi drive module through the ioctrl socket, and route algorithm, but to broadcast the block information of the block chain to the block chain network through Peer-to-peer way. The results are phased notifications to each node. The write, read in the figure is the use of MySQL technology to store the block chain of public ledger information to the local. If the local does not establish a database, this operation is not local (see Fig. 5).

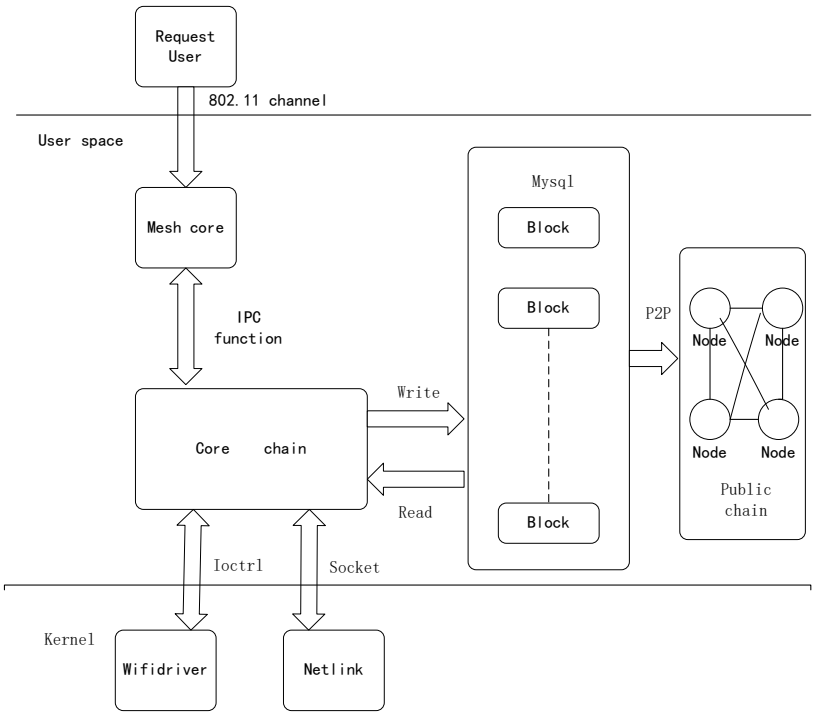

Figure 5: The block chain Architecture for WLAN mesh

3.4 Block structure

A block is made up of a format which uniquely identifies the block. This is followed by the block size which contains the entire size of the block. The next structure is the block headers. The block header is hashed with sha256 (sha256()) as the bitcoin header. The block header plays a significant role in the block chain network by ensuring immutability. By changing a block header, an attacker is able to change all block headers starting from the genesis block in order to falsify a blocks record. This significantly ensures security on the network since there is a maximum assurance of an impossibility to achieve this task. This mechanism extensively guarantees data provenance. For malicious activities, block mismatch will alert the system of a suspicious ongoing event which triggers data forensics.

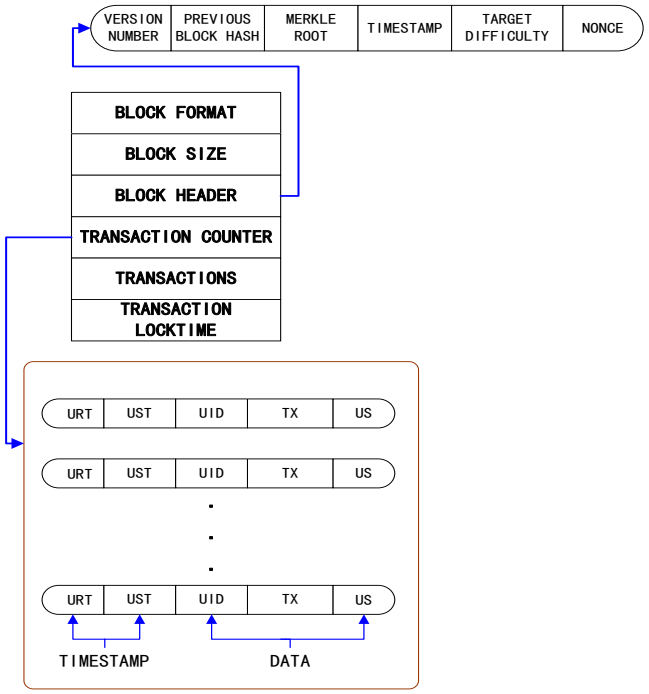

Figure 6: Block structure

The block header contains the data version which indicates the validation rules to follow a particular data type. The header is also made up of the previous blocks hash which is a sha256 (sha256()) hash whose function is to ensure that no previous block header can be changed without changing this blocks header. The merkle root hash forms part of the header by ensuring that none of the blocks in the block chain network can be modified without modifying the header. This is achieved by taking the hashes of all the events in the block chain network and appending the output to the current block. The final output is a sha256 (sha256()). The header includes a timestamp for creating a block.

The block has a transaction counter whose function is to record the total number of transactions in the entire block. The transaction is made up of the user transaction in

relation to the purposes and processing of records as explained in the transaction section. The transaction is categorized into two parts that are the timestamps and the data. The timestamps are URT and UST whilst the data part is made up of UID, TX, and US. This forms the transaction for the user. User transactions are designed to accommodate multiple but limited events for user transaction instances that are not accounted for.

3.5 Transaction process

The following figure describes the process of the transaction (see Fig. 7).

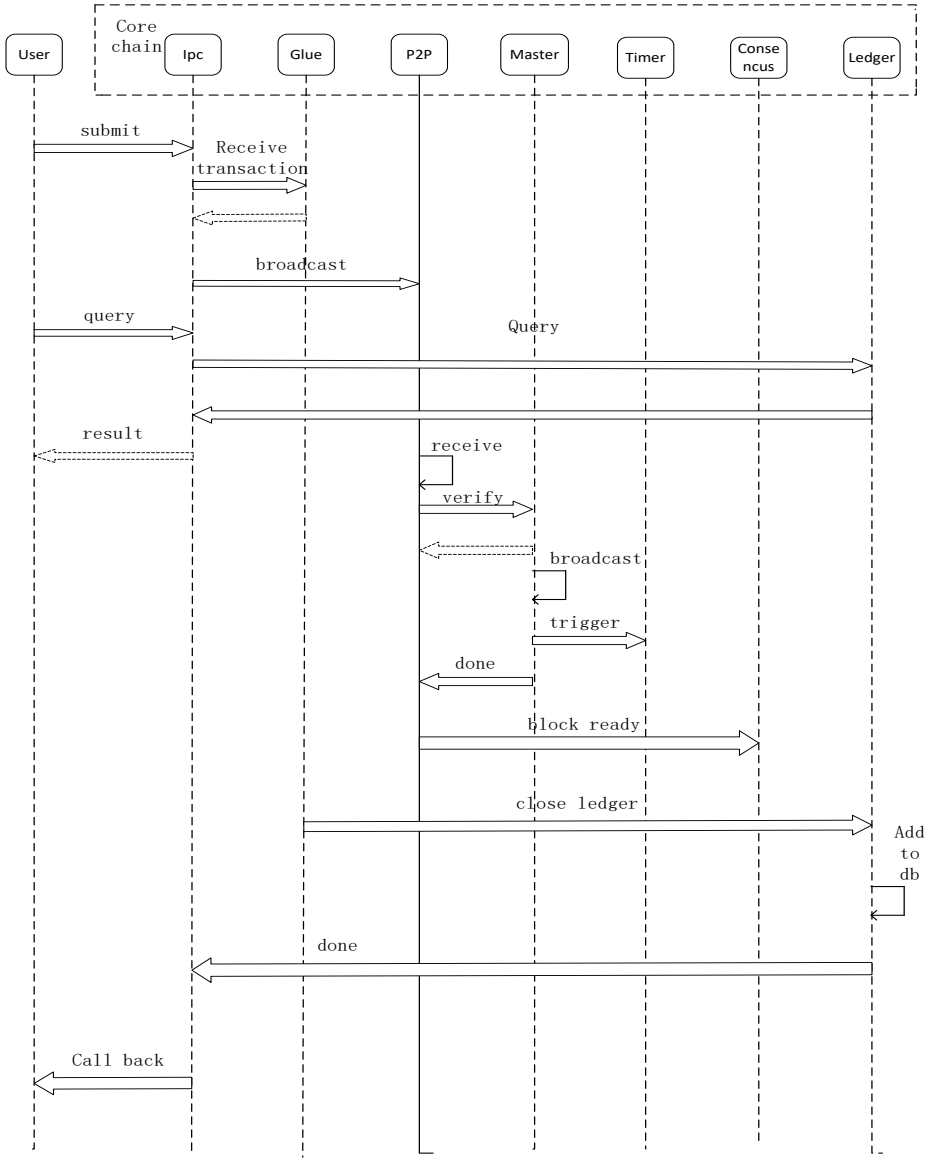

Figure 7: The Transaction Process for block chain

4 Implementation and evaluation

4.1 Implementation

We implemented the proposed method on the mesh AP using hardware as shown in Fig. 8. The mesh network is formed by multiple non-homogeneous nodes, where each node is built by different manufacturers, but both of them have access to the same network. The tested hardware includes, a surface pro3 (rtl8192ce)->Node 1, a Samsung Galaxy S7 (mvl8787) ->Node 2, a Raspberry pi (wcn36xx) ->Node 3, a Samsung4412 dev board (ath9k) ->Node 4 and a laptop computer equipped with Intel Core i5-460M processor, 2 GB memory and Intel Centrino Advanced-N wireless chip -> Node 5. Fig. 8 shows the test network and server environment. Nodes 1, 2, 3 and 4 are mesh APs implemented on the laptop computer whereas Node 5 is implemented on router. Another phone is considered as a user terminal that measures the authentication delay.

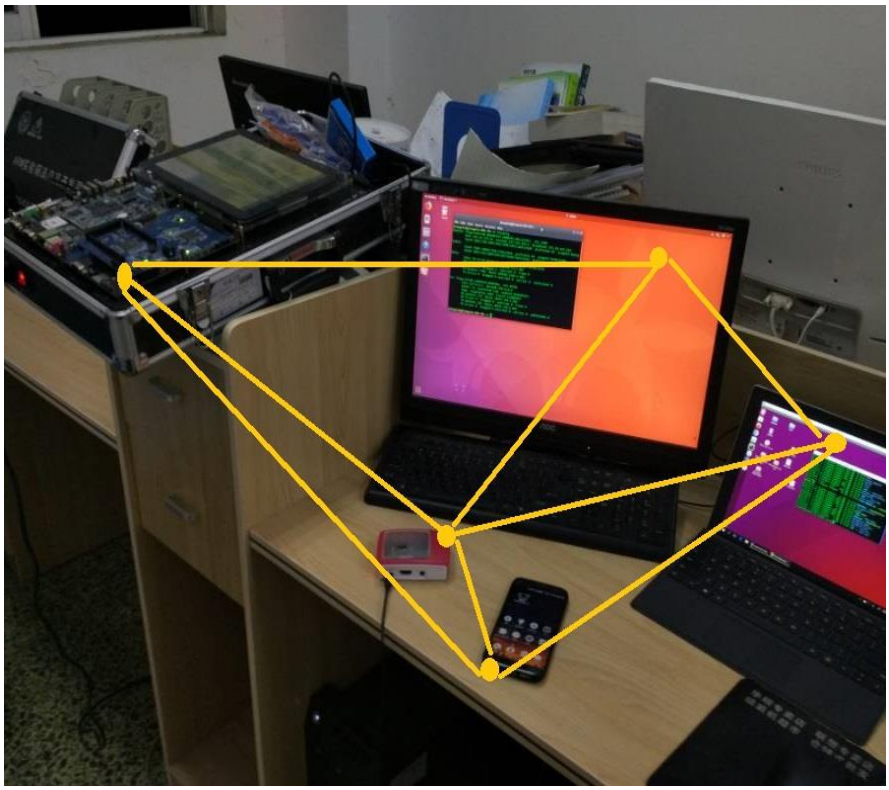

Figure 8: Topology of the experimental network

4.2 Evaluation

Fig. 9 shows the average authentication delay for different numbers of wireless hops. Each measurement was repeated 100 times. This experimental results show that the fallback authentication delays increase with the number of hops between the authenticator AP and the request phone. In fallback authentication, however, the

authentication delay with RadSec is less than the one with RADIUS especially where the number of hops is more than three. RadSec transports the authentication packets over TCP, whereas RADIUS transports them over UDP. Thanks to the TCP fast retransmit algorithm, RadSec authentication packets can be sent faster than the standard RADIUS if a packet loss happens. The experimental results have confirmed that block chain authentication can decrease the authentication delay in multi-hop environment that makes the packet loss rate larger.

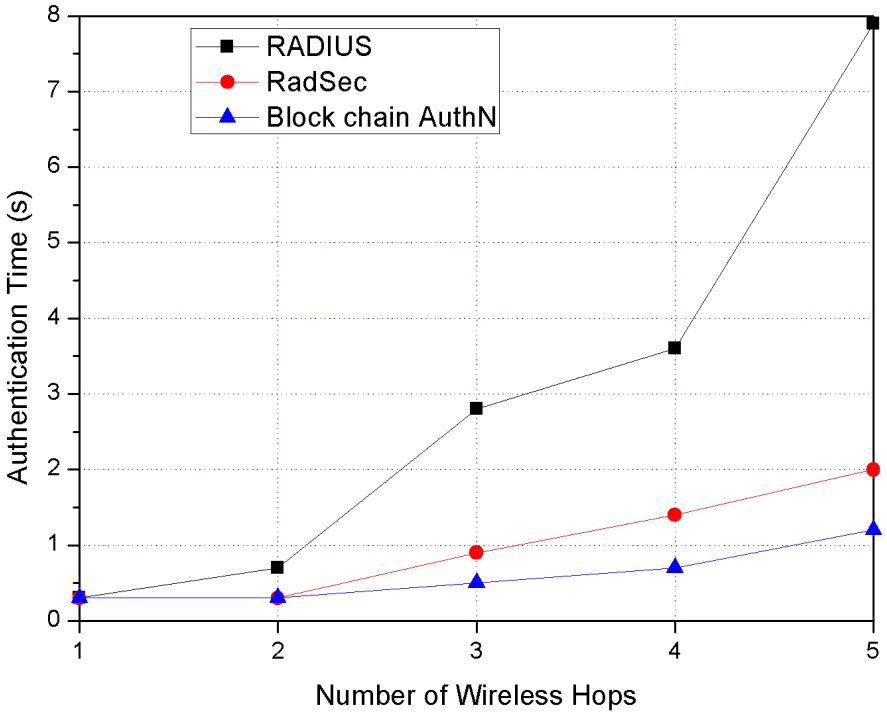

Figure 9: Authentication delay

5 Conclusions

This paper introduced the structure and characteristics of WLAN mesh network, and analyzed the common security threats and security requirements. The security authentication protocol between router nodes in WLAN mesh network is studied, and a new authentication protocol for WLAN mesh network is presented. The authentication process of the protocol was introduced in detail. Compared to the normal block chain network, we constructed a scalable (redesigned to allow speedy transactions) and lightweight blockchain to demonstrate the efficiency of our design which permits accessing to WLAN mesh network in a secure manner and protects the privacy of data. The main security and performance of the protocol are summarized as: (a) it makes the protocol deployable in time of disaster, in particular when the upper network is unavailable or some authentication servers or proxies are down, if an attack has been made against the authenticator, the requester can access and update the public ledger

from any node in the block chain; (b) the block chain-based authentication can also solve the extra overhead incurred by the mesh node because of obtaining the public key certificate and maintaining the public key certificate.

Acknowledgement: The authors declare that there is no conflict of interest regarding the publication of this paper. This work was supported by the National Natural Foundation of Science, China (41274109), the Innovative Team Project of Sichuan Province (2015TD0020), and the New Zealand Marsden Fund.

References

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.

Blum, M.; Santis, A. D. (1990): Noninteractive zero-knowledge. *Siam Journal on Computing*, vol. 20, no. 6, pp. 1084-1118.

Choumas, K.; Syrigos, I.; Korakis, T.; Assiulas, L. (2014): Video-aware multicast opportunistic routing over 802.11 two-hop mesh networks. *Eleventh IEEE International Conference on Sensing, Communication, and networking*, vol. 2014, pp. 486-494.

Deng, X.; He, T.; He, L.; Gui, J.; Peng, Q. (2017): Performance analysis for IEEE 802.11s wireless mesh network in smart grid. *Wireless Personal Communications*, vol. 96, no. 1, pp. 1537-1555.

Dobbertin, H. (1997): Ripemd with two-round compress function is not collision-free. *Journal of Cryptology*, vol. 10, no. 1, pp. 51-69.

Dobbertin, H.; Bosselaers, A.; Preneel, B. (1996): Ripemd-160: A strengthened version of ripemd. *Fast Software Encryption*, vol. 1039, pp. 71-82.

Egners, A.; Herrmann, P.; Jarmuzek, T.; Meyer, U. (2014): Experiences from security research using a Wireless Mesh Network testbed. *38th Annual IEEE Conference on Local Computer Networks*, vol. 2014, pp. 340-343.

Eyal, I. (2015): The miner's dilemma. *Security and Privacy*, vol. 2015, pp. 89-103.

Heilman, E.; Kendler, A.; Zohar, A.; Goldberg, S. (2015): Eclipse attacks on bitcoin's peer-to-peer network. *Usenix Conference on Security Symposium*, vol. 45, pp. 129-144.

Hu, J. (2011): The improved elliptic curve digital signature algorithm. *International Conference on Electronic and Mechanical Engineering and Information Technology*, vol. 1, pp. 257-259.

Hung, K. L.; Bensaou, B. (2014): *Throughput Optimization in Wireless Local Networks with Inter-AP Interference Via A Joint-association Control, Rate Control, and Contention Resolution*. Elsevier Science Publishers B. V, Netherlands.

Hussain, M. I.; Ahmed, Z. I.; Saikia, D. K.; Saikia, D. K. (2016): An efficient tdma mac protocol for multi-hop wifi-based long distance networks. *Wireless Personal Communications*, vol. 86, no. 4, pp. 1971-1994.

Jiang, X.; Liu, M.; Yang, K.; Liu, Y.; Wang, R. (2018): A security sandbox approach of android based on hook mechanism. *Security and Communication Networks*, vol. 2018, no. 7, pp. 1-8.

Johnson, D.; Menezes, A.; Vanstone, S. (2001): The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, vol. 1, no. 1, pp. 36-63.

Juliato, M.; Gebotys, C. (2009): Tailoring a reconfigurable platform to sha-256 and hmac through custom instructions and peripherals. *International Conference on Reconfigurable Computing and Fpgas*, vol. 2009, pp.195-200.

Majumder, A.; Roy, S. (2017): Implementation of enhanced forward pointer-based mobility management scheme for handling internet and intranet traffic in wireless mesh network. *Telecommunication Systems*, vol. 2017, pp.1-24.

Nayak, K.; Kumar, S.; Miller, Andrew, S. E. (2016): Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. *IEEE European Symposium on Security and Privacy*, vol. 2016, pp. 305-320.

Niizuma, T.; Goto, H. (2017): Easy-to-deploy wireless mesh network system with user authentication and wlan roaming features. *IEICE Transactions on Information and Systems*, vol. 100, no. 3, pp. 511-519.

Rackoff, C.; Simon, D. R. (1992): *Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack*. Springer Berlin, Heidelberg.

Rivest, R. L. (1978): A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, vol. 26, no. 2, pp. 96-99.

Sapirshtein, A.; Sompolinsky, Y.; Zohar, A. (2017): Optimal selfish mining strategies in Bitcoin. *International Conference on Financial Cryptography and Data Security*, vol. 2017, pp.515-532.

Sasson, E. B.; Chiesa, A.; Garman, C.; Green, M.; Miers, I. et al. (2014): Zerocash: decentralized anonymous payments from bitcoin. *Security and Privacy*, vol. 1, no. 5, pp. 459-474.

Shariffar, H. (2012): Sha1 and sha256 custom instruction design and characterization on nios ii processor. *Journal of the American Oil Chemists Society*, vol. 81, no. 10, pp. 979-987.

Shen, N.; Mackenzie, A.; Lab, T. M. (2016): Ring confidential transactions. *Ledger*, vol. 1, no. 2, pp. 1-18.

Valdes, L.; Montesinos, S.; Ariza, A.; Allende, S. M.; Joya, G. (2015): Peer selection in p2p wireless mesh networks: comparison of different strategies. *Soft Computing*, vol. 19, no. 9, pp. 2447-2455.

Wang, R.; Ji, W.; Liu, M.; Wang, X.; Weng, J. et al. (2018): Review on mining data from multiple data sources. *Pattern Recognition Letters*, vol. 109, no. 7, pp. 120-128.

Xia, Q.; Sifah, E. B.; Asamoah, K. O.; Gao, J.; Du, X. et al. (2017): Med- share: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, vol. 5, no. 99, pp. 14757-14767.

Yu, J.; Wong, W. C. (2015): Optimal association in wireless mesh networks. *Vehicular Technology IEEE Transactions on*, vol. 64, no. 5, pp. 2084-2096.

Yu, J.; Wong, W. C. (2017): A network resource management framework for wireless mesh networks. *Wireless Personal Communications*, vol. 95, no. 3, pp. 1-25.

Yuan, C.; Xu, M. X.; Si, X. M. (2017): Research on a new signature scheme on blockchain. *Security and Communication Networks*, vol. 2017, no. 2, pp. 1-10.