IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON FOG RADIO ACCESS NETWORKS (F-RANS) FOR 5G: RECENT ADVANCES AND FUTURE TRENDS

Received August 15, 2018, accepted September 17, 2018, date of publication September 24, 2018, date of current version October 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2871642

A Security Authentication Scheme of 5G Ultra-Dense Network Based on Block Chain

ZHONGLIN CHEN[1], SHANZHI CHEN[1,2], (Senior Member, IEEE), HUI XU[2], AND BO HU[1]

[1]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100081, China
[2]State Key Laboratory of Wireless Mobile Communication, China Academy of Telecommunications Technology, Beijing 100081, China

Corresponding author: Zhonglin Chen (chenzl@263.net)

This work was supported in part by the National Science and Technology Major Projects for the New Generation of Broadband Wireless Communication Networks under Grant 2016ZX03001017 and in part by the National Natural Science Foundation of China for Distinguished Young Scholars under Grant 61425012.

ABSTRACT The ultra-dense network (UDN) is one of the most promising technologies in the fifth generation (5G) to address the network system capacity issue. However, it is a new challenge that the user equipment (UE) secure access UDN composed of the access points (APs) which characterized with autonomy, temporary, and dynamic. In 5G UDN, the APs are independent and equal. The UDN can be regarded as a decentralized access network. Compared with the traditional base station, the AP has a smaller coverage. There has an issue that the interaction between the UE and APs will be more frequent when UE moves. However, the existing 4G authentication and key agreement algorithm cannot adapt to this fast and frequent authentication requirement. If the UE moves smoothly in a trusted APs group (APG) without frequent authentication, this problem will be solved very well. In order to achieve this goal, we propose a security authentication scheme of 5G UDN based on the block chaining technologies. In this paper, an APG-PBFT algorithm based on the block chaining technology with Byzantine fault tolerance (PBFT) consensus algorithm is proposed. In the algorithm, the consensus mechanism will be optimized and a new reverse screening method will be embedded. In our solution, a trusted chain APG can be generated with APs by APG-PBFT algorithm, and the authentication results can be shared in the APG using the blockchain message propagation mechanism. The principle of fast authentication with APG-PBFT algorithm is present in this paper. The scheme can reduce the authentication frequency when UE moves among the APs and improve the access efficiency. Finally, we analyze the performance of APG-PBFT algorithm and compare it with the traditional PBFT algorithm. The simulation results show that the APG-PBFT algorithm can improve the APG generation efficiency and reduce the authentication frequency of UE, which will be valuably applied to the UDN environment.

INDEX TERMS Ultra-dense network, block chain, access point group, Byzantine fault tolerance.

I. INTRODUCTION

In 5G, in order to realize the "Internet of Everything," corresponding requirement for performance have reached a consensus, including higher speed data traffic and the user experience, massive terminal connection and lower delay [1]. Improving the density of Access Points (APs) in the unit area and forming Ultra Dense Network (UDN) is an important way to deal with the challenge of increasing network traffic by 1000 times and improving user experience speed by 10∼100 times.

UDN is generally considered to be one of the most effective means to solve the rapid growth of high traffic in 5G network, especially in hotspots area [2], [3].

It is predicted that the deployment density of the small access points based on various Radio Access Technology (RAT), will reach more than 10 times the current site density in the area covered by the macro station radio network of the future [4], [5]. In the case of UDN, the number of massive APs may even have a considerable density with the user equipment (UE), and all APs form a peer-to-peer uncentered network. In UDN, the AP has low power and small coverage. For the high moving mobile users, user UE will frequently switch between APs and reduce access speed and stability [6]. In 5G, the APs are no longer just the network link channel, but also take more business interaction with the UE. It will provide data services and control data services

based on the difference of functional requirements. The AP is the key point of UE accessing the mobile Internet. The registered data that users verify through the AP will face the security risk, which will affect the safety of user transaction information. Therefore, how to ensure the safe and efficient access to trusted UDN network is a new challenge to the future 5G network architecture and security mechanism.

Presently, the existing Authentication and Key Agreement algorithm (AKA) in 4G networks, such as EPS-AKA algorithm [7], mainly designed for security identification between the user UE and the fixed Mobility Management Entity (MME), as well as encrypted communication between UE and fixed evolved NodeB (eNB) or Home eNodeB (HeNB). However, in the future 5G UDN, the APs are independent and equal. and the UDN network is considered as a uncentered access network composed of APs. At the same time, because of the small coverage of AP in UDN, with the movement of UE, the AP that interacts with UE is more easily changed. The existing 4G access authentication algorithm cannot meet the access requirements of UE fast and secure access to a dynamic access points group (APG). Therefore, in this paper, we propose a mobile security authentication scheme for UE access to uncentered access point group, which mainly solves the issues of how to generate trusted access point chain as APG and how accessed UE switch smoothly and safely among trusted access point chain members.

The main contributions of our proposed scheme are summarized as follows.

1) Based on the block chaining technology, by optimizing the consensus mechanism and the reverse screening method, we proposed the efficient APG-PBFT generation algorithm. The APs is organized into a secure trusted chain as APG, which improves the security and reliability of APG.

2) Based on the block chain propagation mechanism, the UE authentication results are transmitted in the trusted chain (APG) by directional trust transfer, so that APG members can share the UE authentication results, reduce the authentication frequency when UE moves between APs, and improve access efficiency and user experience.

The rest of the paper is organized as follows. The block chaining technology and relevant background knowledge are presented in Section II. In Section III, the security challenges for users to access 5G are analyzed. The principle of APG chain generation and group authentication based are described in Section IV. Furthermore, the APG-PBFT algorithm and its performance evaluation analysis are presented in Section IV. The final conclusions are drawn in Section V.

II. BLOCK CHAINING TECHNOLOGY AND RELATED WORK

Block chain is a chain data structure composed of data blocks sequentially connected in a chronological order, and cryptographically guaranteed non-falsified and unforgeable distributed ledger technologies [19]. Blockchain is a series of data blocks associated with cryptographic methods, which is essentially a decentralized database. Blockchain networks have a small-world model [20]. Because the small-world model can maintain the stability of the network in the case of node changes (join, exit, change), it ensures the robustness of the blockchain network and ensures the integrity and consistency of the transaction data on the blockchain [21]. The core of blockchain technology is to solve the trust security problem in the decentralized environment based on the consensus problem mechanism.

A. THE BYZANTINE GENERALS PROBLEM

The origin of the consensus problem was the question of Byzantine Generals, first proposed by Leslie Lamport in 1982, known as The Byzantine Generals Problem or Byzantine Failure [22]. The generals of the Byzantine Empire's army must all unanimously decide whether to attack a certain enemy army, but each army is far apart. The generals and generals can only communicate by messenger, and there may be traitors in the generals. The core description of the problem, therefore, is how the loyal generals can reach a consensus in the case of a traitor in the army and ensure the agreement of a certain order (such as an attack or a retreat together). The essence of Byzantine Generals is a consensus problem, that is, how to reach consensus on information based on an untrustworthy distributed network. Lamport has proved that the most likely betrayal is m (or less), and when the total number of generals is greater than 3m, a loyal general can achieve the same order. The Byzantine Generals Problem has been extended to a fault-tolerant theory in the field of network computing.

B. BLOCK CHAIN AND CONSENSUS MECHANIM

In distributed systems, multiple network nodes make up network clusters through asynchronous communication. Due to the network delay between nodes and nodes, the order of transactions received by each node cannot be completely consistent. The consensus mechanism is an algorithm to reach agreement on the recognition of transaction order rules in a time period. Consensus algorithm is the key technology of block chain. In the block chain, the arbitration rights for bookkeeping are randomly allocated according to certain rules, and the arbitration rights for keeping accounting are not bound to a certain node. At each accounting time, the arbitration rights are randomly assigned to the entire network, and then the other nodes follow the node to complete the accounting task. In this way, each node reached a consensus on the book of accounts, and the next bookkeeper was indeterminate, in line with the characteristics of decentralization. At each bookkeeping, there will be a node leading the other nodes to complete. Different node voting methods form a variety of consensus algorithms.

According to the different application scenarios such as the Public blockchain and the Consortium blockchain, a variety of consensus algorithms have been designed, including: Proof of Work (PoW) [8], Proof of Stake (PoS) [9], delegated Proof of Stake(dPoS) [10], Casper [11], Practical Byzantine Fault Tolerance (PBFT) [12], Proof of

Elapsed Time (PoET) [13] and so on. These consensus algorithms have their own application scenarios and have different advantages and disadvantages. For example, the PoW algorithm has a large energy consumption, easy to be attacked by force, a longer consensus cycle, and so on. It is not suitable for the communication system with time delay. The comparison of other common consensus algorithms is shown in table Tab_1.

TABLE 1. Comparison of consensus algorithm.

Algorithm	PoS	DPoS	Casper	PBFT	PoET
Performance	relatively high	high	relatively high	high	high
Decentralization	completely	completely	Completely	Semi-centralized	Semi-centralized
Maximum number of malicious nodes allowed	51%	51%	51%	33%	51%
Tokens	yes	yes	yes	no	no
Application type	Public block chain	Public block chain	Public block chain	Consortium block chain	Consortium block chain
Can prevent witch attacks	Yes	Yes	Yes	No	Yes
Technical maturity	mature	mature	Not applied	mature	Not applied
Need special hardware	no	no	no	no	yes

In the UDN system, the real-time requirement is high. The key to the technical adaptability of the block chain is the performance of the consensus algorithm without the token. The hypothesis of the traditional PBFT algorithm is relatively fixed in the consensus node, while the trusted node group APG in UDN is dynamically changing following UE mobility. Therefore, in order to improve the efficiency of the algorithm and the adaptability based on APG, our security authentication scheme is based on the PBFT algorithm, combined with the adaptability of APG to optimize the consensus algorithm and improve efficiency.

III. SECURITY CHALLENGES FOR USERS TO ACCESS 5G UDN

In 5G, the UDN is a direct access network for users, which is connected to the 5G network by means of APs. In UDN, users need to secure access to the network, and they must ensure that access is secure, and the UE is not connected to the fake or illegal AP. Since UE will move between different APs, UE will have access to multiple APs. Therefore, it requires the UDN to ensure that all APs that interact with UE must also be secure [14].

In the UDN architecture, a user-centric, ultra-dense network architecture (as shown in Fig.1) [15]–[18] is used to compose a certain range of APs around the UE. The APG provides access services for the UE. The APG member can be dynamically updated as the UE moves, which allows the user to feel that there is a mobile network coverage that has been accompanied with it, thereby effectively addressing the mobile traffic demand and better improving the user experience. In the User-centric Ultra-Dense Network (UUDN)

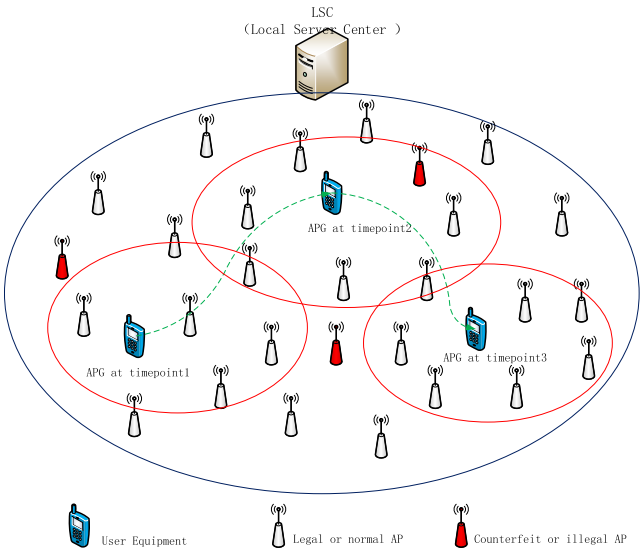

FIGURE 1. User-centric UDN architecture.

architecture, the APG is responsible for access interaction with the UE. Therefore, as long as the APG is guaranteed to be secure, for example, a fake or rogue AP is not included in the APG or does not work in the APG, it can be ensured that the UE access is secure without having to require that all APs are secure nodes, which can effectively reduce the difficulty of security protection. The follow-up of this article is mainly based on the UUDN architecture for analysis and design.

In the 5G ultra-dense network, either the regular access nodes of UDN APs, or a member of APG in UUDN APs, for UE, each APs is completely equivalence between each other, is an organization that has no center. Therefore, access security of the APs (or APG) and UE faces the following challenges:

(1) AP fraud and APG untrusted security issues.

Due to the diversity of demand, the AP has diverse functions and flexible deployment mode (even user-deployed). The physical security environment of AP is complex and different. There is a possibility of counterfeit or illegal APs. At the same time, because of the dynamic and non-centralization of APG, how to ensure the overall security of the APG is challenged during the APG member update process.

(2) The problem of authentication efficiency of UE access through dense APs.

In the UDN scenario, APs are densely deployed. The traditional UE and AP use a one-to-one authentication method. Frequent authentication poses a challenge to access efficiency and user access rate, which cannot meet high-quality user experience requirements.

Block chain, as a kind of information security technology with no centralization features, provides an innovative idea for solving the APG trusted generation and security and efficient access to UE under the UDN environment. It has a very good application prospect for the realization of user centered and enhanced user experience.

IV. A FAST SECURITY AUTHENTICATION SCHEME BASED ON BLOCK CHAIN

In the future 5G, different operators will have their UDN systems. Based on the blockchain technology, different UDN systems interoperate to form a consortium blockchain. In UDN environment, the UE accesses the APG which is composed of APs. LSC can manage a certain range of APs communication clusters (there may be fake nodes), APs is independent of each other. Therefore, for the UE to perform secure and reliable access, forming a secure and trusted APG (chain) around the UE is an important prerequisite.

A. THE PRINCIPLE OF FAST AUTHENTICATION SCHEME

In order to realize the fault-tolerant and fast generation of APG chain, we propose an APG generation algorithm named APG-PBFT based on the improved PBFT consensus mechanism. A UDN fast security authentication scheme using the APG-PBFT algorithm was implemented. The solution can be divided into five Phases.

Phase 1: The request for APG generation. After the UE submits an access request to the network, the APs within a certain range (quantity assumed n, AP[n]) around UE will receive the message and forward the request. When the request finally arrived at LSC, LSC was asked to organize an APs group (APG) to provide services for the UE. According to the context of the UE request, LSC asks NSC/AUC for APG key and other parameters to prepare related data, such as APG unique identifier (APG-ID). Then, LSC sends instructions for consensus computing to all the access points (AP[n]) which apply to service the UE. The APG-PBFT algorithm in this paper is based on PBFT optimization. According to different scenarios, some other consensus algorithms can be chosen.

Phase 2: The selection of trusted APs based consensus result identification. Because of some security reasons, there may be one or more untrustworthy or fake AP in all application access points. In the traditional PBFT algorithm, the consensus results only indicate the consistency of information decision making. The consensus consistency information will be recorded in the accounts of all APs. However, who owns the right to write accounts can't decide that the AP participating in the consensus computation if it's trusted.

Therefore, in our improved APG-PBFT algorithm, the identification of AP[i] is added to the consensus computing, and the decision messages received or sent will be classified and counted. All the APs should inform the LSC of the consensus results. When the AP marked as AP[i] is consistent with the last computed consensus information, it indicates that the AP[i] is consensus trust and will be used as the selected AP. Otherwise, it indicates that the AP is unbelievable, giving up the selection.

The selection of trusted AP[i] in the consensus computation process is temporary. If the computation fails to reach consensus, it needs to be recomputed. If a new AP request to join into the APG, a consensus result need to be recomputed.

Phase 3: APG trusted block chain generation. In the APG-PBFT algorithm, a relatively fixed consensus result chain APG is designed and maintained. After a consensus computation is completed, the selected AP[i] (the i may be no longer continuous) as a new block AP[k] (k = [1..m], $m <=$ n) will finally generate an APG trusted chain. The trusted chain APG will really provide services for UE. At the same time, LSC will issue an APG-ID to the APG, indicating that the trusted chain APG has been created successfully. Only the members AP[k] of the trusted chain can get the APG identity. Otherwise, the AP will be discarded as an untrusted node.

The APG trusted chain is logical. In physical location, the members AP[k] of APG may be scattered around UE, they have no order and no direction. That means the APs of APG are in centerless status.

Phase 4: The mutual authentication between UE and an APG member. The APG processed by APG-PBFT algorithm is trusted, and the authentication result between the UE and any APG member can be reliably propagated within APG. Therefore, all APs of the APG can be considered trustable. The member AP[k] (k $\in$ m) will be selected according to the signal strength, delay, bandwidth and other status parameters of the network. The member AP make a mutual authentication with UE.

The authentication is similar to the process of AKA (Authentication and Key Agreement) in 4G LTE. If the authentication is passed, the AP[k] will obtain the authentication result (vector).

Because of the mobility of UE, APG members are updating and do consensus computation constantly. Some AP may be selected many times. In order to enhance user experience, the choice of AP can be optimized. The algorithm records the quantity of the member selected on the APG chain. If the selected AP is already on the APG chain, it only marks the times number and without any other processing. The AP with most selected times can be used for the preferred peer with UE authentication. For the first consensus computation, the first selected AP_0 can be used as the preferred peer.

Phase 5: The trust transfer of the authentication results on the APG chain. The authentication results (vectors) are propagated through the block chain propagation mechanism among the members of the APG chain, named APG directional propagation process. Authentication results can be shared and saved by members on the APG chain. When UE moves to the coverage of AP[j] ($j = 1, 2, \ldots, m$), the UE submits authentication vector to AP[j]. If vector verification is passed, AP[j] provides services directly, instead of repeating the new complete mutual authentication process. The UE will smoothly connect to the AP and its next without awareness. Then, the user will always be in a seamless coverage of APG services until APG is revoked.

As the UE moves, the APG refreshes. The step 4 and step 5 are repeated, so that the user can obtain the best experience and intensive traffic support.

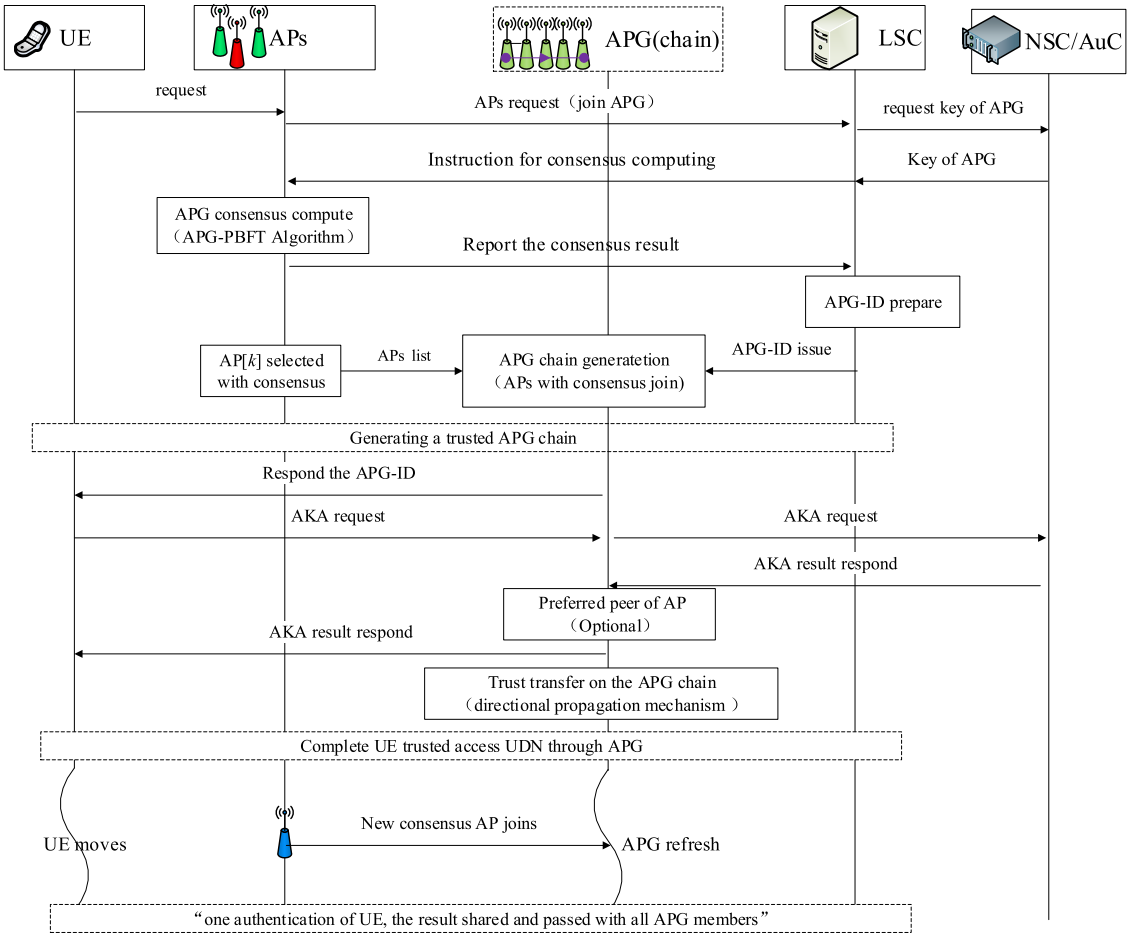

FIGURE 2. The principle of APG generation and group authentication based on block chaining technology.

The principle of UDN fast security authentication scheme based on consensus mechanism of the block chaining technology is shown in Fig.2.

B. APG-PBFT CONSENSUS ALGORITHM

In UDN, LSC is the management node of the APs. LSC is controlled by operators in the telecommunication network, which is considered to be trustworthy. According to the PBFT algorithm, it is assumed that there are n peers in the system, including the primary peer AP0 and the common peers (AP_1 ~AP_n). Each peer participating in the consensus computation will assign a number label. In the current consensus, LSC is designated as the primary peer with the label of 0. The other peers' label is arranged in sequence from 1, and the last peer has the label of n. Among them, $\boldsymbol{j}$ is the quantity of Byzantine peers which can be tolerated or untrusted peers in the system.

The peers are the APs in our algorithm. the APG-PBFT algorithm is based on the improvement of PBFT adapting to UDN scenario. Firstly, UE sends the APG request to the LSC. LSC is assigned as AP_0, when it receives the request message and verifies it. As the primary peer, LSC broadcasts ***prepare*** $<v, h, d, s>$ messages to all the other peers. In the algorithm, the $\boldsymbol{v}$ means the current view identity. The $\boldsymbol{h}$ indicates the high of the message. The $\boldsymbol{d}$ is the digest of the message and the $\boldsymbol{s}$ is the digest signature for the message. Other peers ($AP_1 \sim AP_n$) receive the prepared messages from the AP_0 broadcasted, verified and prepares ***prepare*** $<v, h, d, s>$ message. The peers can continue to forward or receive the message from other peers. At the same time, the peers that received messages (such as AP_i) begin to accumulate the quantity of messages in their memory. When the prepare message over $\boldsymbol{f}+1$ different peers are received, the peers reaches the prepared status and broadcasts the ***commit*** $< v, h, d, s >$ message, marks and counts the status the received and broadcast messages. All peers ($AP_1 \sim AP_n$) return their results to the primary peer AP0. When each peer receives more than $\boldsymbol{2f}+1$ different peers commit messages, according to the PBFT algorithm, the peers ($AP_1 \sim AP_n$) has reached a consensus. Then the peers reach the committed status.

According to the consensus results and the marks of the peers ($AP_1 \sim AP_n$), the primary AP_0 find out the peer AP_k which marked result is consistent with the final consensus result in AP0. The peer AP_k is regarded as trusted peer which can correctly convey the instructions of LSC (AP_0). Therefore, all these peers, such as the AP_k, can be added to

the block chain APG. The APG block chain (identified as APG_ID) takes the trusted AP_0 as its root.

When all the peers have completed its consensus, the APG chain can generated with the consensus selected peers. When the new AP is joined, the label number is increased sequentially. Then a new round of consensus computation and the APG refresh starts.

The graphical representation of APG-PBFT algorithm are shown in Fig.3.

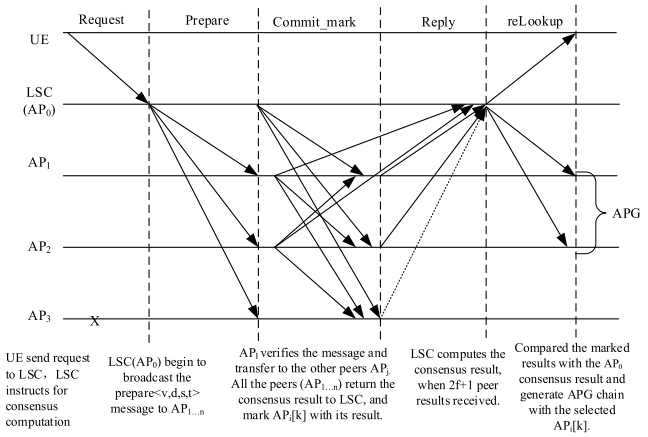

FIGURE 3. The graphical representation of APG-PBFT algorithm.

In UDN, the joining or leaving AP will lead to changes in quantity of peers and naturally begin a new round of consensus computation. This is essentially the same as the change of views in PBFT. The time point for each new AP adding is equivalent to a view update point.

This is essentially the same as the change of views in PBFT. The time slice triggered by each new node is equivalent to a view. Therefore, there is no need to express the view change process separately in the APG-PBFT algorithm. Therefore, the view change process of PBFT is no longer specifically expressed in the APG-PBFT algorithm.

The APG-PBFT algorithm is shown in Algorithm 1.

C. APG-PBFT ALGORITHM ANALYSIS

The essence of the block chain is to generate the distributed ledger. To avoid bifurcation or other malicious attacks, a certain time interval is set up to ensure the randomness of writable privileges on the ledger in block chaining technology. However, the important feature of the block chain based on traditional PBFT algorithm is not well suitable for the high efficiency requirement under security guarantee in UDN. On the one hand, the consensus of a group peers can be generated quickly when some untrusted peers participate. On the other hand, there is no need to store the ledger data in the real-time communication UDN scenario.

Therefore, the APG-PFBT algorithm for UDN has made specific improvements to the traditional PBFT algorithm, which is mainly reflected in the following four aspects.

(1) In the initial stage, LSC is designated AP0 as a trusted primary peer. Considering that the primary peer is also possibly fault, this improvement reduces the selection judgment

Algorithm 1 APG-PBFT Algorithm

//The UE begin to send the request message Msg to LSC
UE.Send(<cID, Msg, *t*>, request, LSC); //cID: identify, t: timestamp
LSC.Verify(<cID, *h*, Msg, *t*>, $\boldsymbol{AP}_0$); //*h*: the Msg high
$\boldsymbol{AP}_0$.Prepare(<*v, h, d*>, Msg); //*d*: the Msg digest, *v*: view identity
$\boldsymbol{AP}_0$.Broadcast(<*v, h, d, s*>, $\boldsymbol{AP}_{\mathrm{n}}$); //*s*: the digest signature of $\boldsymbol{AP}_0$
//*s*: the digest signature of local AP, the following are similar.
//When $\mathrm{AP_i}$ receive the Msg, he begin to prepare& broadcast.
For $i = 1$ ***to*** n
{
$\boldsymbol{AP}_i$.Receive(<*v, h, d, s*>);
$\boldsymbol{AP}_i$.Verify(<*v, h, d, s*>, *f, n*);
$\boldsymbol{AP}_i$.Prepare(<*v, h, d, s*>);
$\boldsymbol{AP}_i$.Broadcast(<*v, h, d, s*>, $\boldsymbol{AP}_{|n-i|}$);
$\boldsymbol{AP}_i$.count(<*f*: fault *d*>, *count m*);
}
//When the Msg number received by $\boldsymbol{AP}_{\mathrm{i}}$. is greater than $2f$,
//the he begins to commit, mark and reply to LSC($\boldsymbol{AP}_0$).
While $count : m \succ (f+1)$ ***then***
{
// add a marking function to determine
//whether it is consistent with the final result.
//*r*: the result of the request operation
$\boldsymbol{AP}_{\mathrm{i}}$.Mark(<$v, in : d, out : d, t, Mark : k$>);
$\boldsymbol{AP}_{\mathrm{i}}$.Commit(<$v, h, d, s, t$>, $Result : k, \boldsymbol{AP}_0$);
}
//$\boldsymbol{AP}_0$ receives APs reply Msgs (>$2f+1$) and determines them.
$\boldsymbol{AP}_0$.Receive(<*v, h, d, s, t*>, Msg: *r*, count *m*);
While count : $m > (2f+1)$ ***then***
{
$\boldsymbol{AP}_0$.Comput(<*v, h, d, s*>, *Msg*: $r, \boldsymbol{AP}_{k=0}.\mathrm{Mark} = r$);
generateBlockChain(APG, APG_ID, $\boldsymbol{AP}_0$, *null*); =
//AP_0 performs reverse lookup and marks the queue.
For $k = 1$ ***to*** n
{
$AP_0.reLoopup(\boldsymbol{AP}_k.Mark = r)$;
if $\boldsymbol{AP}_k.Mark == \boldsymbol{AP}_0.Mark$ ***then***
{
//add the $\boldsymbol{AP}_k$ to the block chain APG.
addBlockChain(APG, APG_ID, $\boldsymbol{AP}_0$, $\boldsymbol{AP}_k$);
}
else
skip;
}
$\boldsymbol{AP}_0$.Send(<*v, h, d, s, t*>, *Reply*:*r*, UE: cID);
}

process and computational complexity in the PBFT adapted the UDN actual scene.

(2) In APG-PBFT algorithm, in order to mark and count the consensus results of AP_i, the sub-procedure $\boldsymbol{AP}_i.Mark(< v, in : d, out : d, t, Mark : k >)$ is added before the procedure $\boldsymbol{AP}_i$.Commit$(< v, h, d, s, t >, Result : k, \boldsymbol{AP}_0)$. This improves the efficiency of the lookup.

(3) In APG-PBFT algorithm, the comparison based on the marker result is added. The trusted AP_k can be selected by judging whether the results of common peer consensus are consistent with the consensus result of the primary peer. This improvement can quickly generate a trusted APG chain.

(4) The first two stages of ***pre − prepare*** <v, h, d, s>e and ***prepare*** <v, h, d, s> in the PBFT algorithm are merged into a ***prepare*** <v, h, d, s> stage, which shortens the transmission time and improves the efficiency of the algorithm.

When the traditional PBFT algorithm completes a consensus computation, someone peer wins and a transaction record will be added into the ledger in the block chain. ''one consensus won an opportunity to write the ledger''. It is assumed that all peers have equal computing power and equal opportunity. If there are the $\boldsymbol{n}$ honest peers selected, then $\boldsymbol{n-1}$ consensus should be computed at least. This method can be applied to the expansion of the ledger chain, but not suitable for the fast communication of UDN. It will seriously affect the generation efficiency of the APG chain. If UE moves, the APG will continue to refresh (new AP join or old member leave), and the computational load of consensus will be very heavy.

The APG-PBFT algorithm innovatively applies the voting principle to the judgement of consensus results. Before the final consensus is announced, each voting peer (AP in UDN) will bet on (such as marking function in the APG-PBFT algorithm) the result first. If a marked peer consensus is equal with the final consensus result, which means the bet win, then this peer will be selected to generate the trusted APG chain. The APG-PBFT algorithm reduces the repeated consensus computation and achieves UDN decentralization security.

In order to evaluate the performance of the consensus algorithms using simulation system for UDN, a score formula (1) is designed and shows as following.

$$Value(AP_n) = \sum_{c*refresh} \frac{a * TPS}{b * time}, \tag{1}$$

AP_n represents the quantity of peers. TPS represents the transactions per second, and $TPS = \sum Transactions/t$. The *time* represents the average time for a consensus completion. The *refresh* represents the dynamic change quantity of consensus peers. The parameters a, b and c represent the corresponding weight, and their default value are 1 and can be configurated on demand in system initiation.

Provided that the n APs (peers) are randomly distributed around a UE. The distribution radius is r, and the inter-site distance (ISD) is d in UDN. It is assumed that the APs density around the UE distribution should be between the maximum spacing and the minimum spacing among the APs.

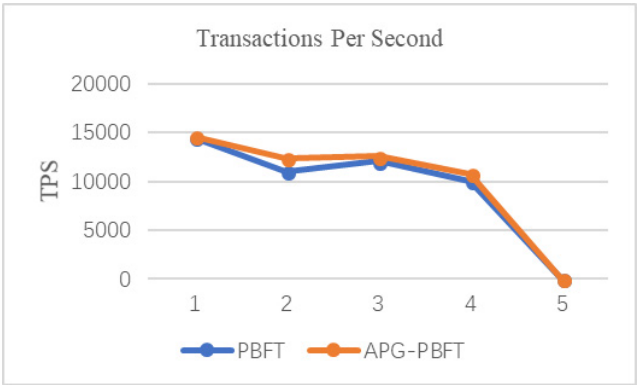

FIGURE 4. TPS of APG-PBFT algorithm.

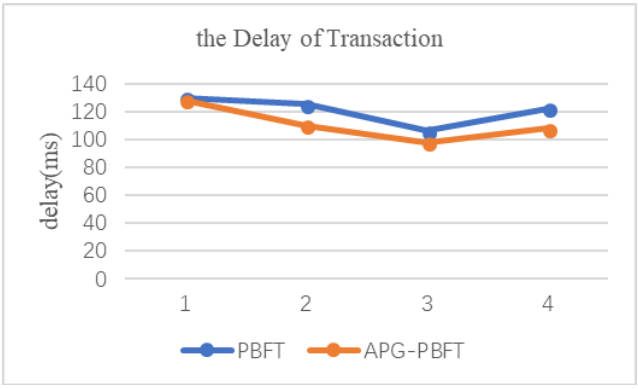

FIGURE 5. The delay of APG-PBFT algorithm.

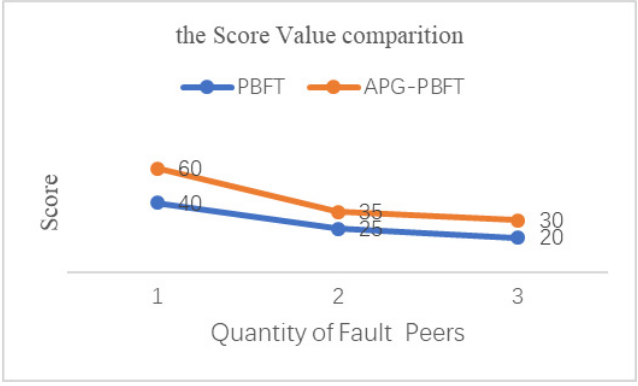

FIGURE 6. The Score of APG-PBFT comparison with PBFT.

The formula 2 shows the relation between the density and the distribution radius.

$$Max\left\lfloor d^2 \right\rfloor \le \frac{\pi r^2}{n} \le Min\left\lceil d^2 \right\rceil, \tag{2}$$

According to the ability of different fault tolerance formula (3), the maximum fault peers f are respectively assumed 1, 2, 3 and 4 to test and observe the result.

$$f < \lfloor (n-1)/3 \rfloor, \tag{3}$$

The observed correlation results after system simulation are shown in Fig. 4, 5, and 6.

From the simulation results, we can see that the APG-PBFT algorithm inherits the fault-tolerant mechanism and the fault tolerance ability of PBFT algorithm. As long as the fault or dishonest APs $\boldsymbol{f}$ accord with $\boldsymbol{f} \le \lfloor (n-1)/3 \rfloor$,

the trusted APG chain generated by the APG-PBFT algorithm can still guarantee the security of APG for UE. Furthermore, the APG-PBFT algorithm can improved the efficiency compared with the traditional PBFT algorithm, and it can be effectively applied to the UDN environment.

V. CONCLUSION

The ultra-dense network (UDN) of 5G is composed of the access points (APs) which characterized with autonomy, temporary and dynamic. Every AP is independent and equal and UDN can be regarded as a decentralized access network. How to ensure that UE can efficiently access a trusted UDN network is a new challenge in 5G. However, the security research of 5G UDN is still in an initial stage.

The APs of 5G has a smaller coverage compared with the traditional base station. The existing 4G Authentication and Key Agreement algorithm (AKA) cannot adapt to a fast and frequent authentication requirement for UDN. In this paper, based on the UDN features, we propose a security authentication scheme of 5G UDN based on block chaining technologies. In the solution, UE can move smoothly in a trusted APs group (APG) without frequent authentication. The trusted APG can be generated by APG-PBFT consensus algorithm based on Byzantine Fault Tolerance (PBFT) and the authentication results can be ''shared'' in the APG with propagation mechanism.

Finally, we analyzed the performance of APG-PBFT algorithm and compare it with the traditional PBFT algorithm. The simulation results show that the APG-PBFT algorithm can improve the APG generation efficiency and reduce the authentication frequency of UE, which will be valuably applied to the UDN environment.

REFERENCES

[1] D. Li, Z. Sun, and Y. Li, ''5G vision and demand,'' (Chinese), *Telecommun. Technol.*, vol. 1, no. 12, pp. 8–11, 2013

[2] S. Chen, ''Analysis and suggestion on developing 5G,'' (Chinese), *Telecommun. Sci.*, vol. 32, no. 7, pp. 1–10, 2016.

[3] X. Ge, S. Tu, G. Mao, and C. X. Wang, ''5G ultra-dense cellular networks,'' *IEEE Trans. Wireless Commun.*, vol. 23, no. 1, pp. 72–79, Feb. 2016.

[4] X. You, Z. Pan, X. Gao, S. Cao, and H. Wu, ''The 5G mobile communication: The development trends and its emerging key techniques,'' *Scientia Sinica Informationis*, vol. 44, no. 5, pp. 551–563, 2014.

[5] B. Yang, G. Mao, M. Ding, X. Ge, and X. Tao, ''Dense small cell networks: From noise-limited to dense interference-limited,'' *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4262–4277, May 2018.

[6] J. M. Zhang, W. L. Xie, and F. Y. Yang, ''Architecture and solutions of 5G ultra dense network,'' *Telecommun. Sci.*, vol. 32, no. 6, pp. 36–43, 2016.

[7] H. Mun, K. Han, and K. Kim, ''3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAP-AKA,'' in *Proc. Wireless Telecommun. Symp.*, Apr. 2009, pp. 1–8.

[8] S. Nakamoto, ''Bitcoin: A peer-to-peer electronic cash system,'' *Consulted*, 2008.

[9] K. Y. K. Hui, J. C. S. Lui, and D. K. Y. Yau, ''Small-world overlay P2P networks: Construction, management and handling of dynamic flash crowds,'' *Comput. Netw.*, vol. 50, no. 15, pp. 2727–2746, 2006.

[10] Y. Zhu, ''Security architecture and key technologies of blockchain,'' *J. Inf. Secur. Res.*, vol. 2, no. 12, pp. 1090–1097, 2016.

[11] L. Lamport, R. Shostak, and M. Pease, ''The Byzantine generals problem,'' *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.

[12] D. Liu and J. Camp, ''Proof of work can work,'' in *Proc. Weis*, Mar. 2006, pp. 13–15.

[13] P. Vasin, ''BlackCoin's proof-of-stake protocol v2,'' White paper. [Online]. Available: https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf

[14] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, ''Overview of 5G security challenges and solutions,'' *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.

[15] BitShares. (2014). *Delegated Proof-of-Stake Consensus*. [Online]. Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus/

[16] V. Buterin and V. Grifith. (Nov. 2017). *Casper the Friendly Finality Gadget*. [Online]. Available: https://arxiv.org/pdf/1710.09437.pdf

[17] M. Castro and B. Liskov, ''Practical Byzantine fault tolerance,'' in *Proc. ACM Symp. Operating Syst. Design Implement.*, Feb. 1999, pp. 173–186.

[18] Intel, Sawtooth Lake, ID, USA. (2017). *Architecture Description*. [Online]. Available: https://intelledger.github.io/

[19] S. Chen, F. Qin, B. Hu, X. Li, Z. Chen, and J. Liu, *User-Centric Ultra-Dense Networks for 5G*. Cham, Switzerland: Springer, 2017.

[20] S. Chen, F. Qin, B. Hu, X. Li, and Z. Chen, ''User-centric ultra-dense networks for 5G: Challenges, methodologies, and directions,'' *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 78–85, Apr. 2016.

[21] Z. Chen, S. Chen, H. Xu, and B. Hu, ''Security architecture and scheme of user-centric ultra-dense network (UUDN),'' *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 9, p. e3149, 2017.

[22] Z. Chen, S. Chen, H. Xu, and B. Hu, ''A security scheme of 5G ultra-dense network based on implicit certificate,'' *Wireless Commun. Mobile Comput.*, vol. 2018, no. 2, pp. 1–11, May 2018.

ZHONGLIN CHEN received the M.E. degree from Tsinghua University, China, in 2006. He is currently pursuing the Ph.D. degree in information and communication engineering with the Beijing University of Posts and Telecommunications, China. His current research interests include information security and security for future wireless mobile communication.

SHANZHI CHEN (SM'04) received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), China, in 1997. In 1994, he joined the Datang Telecom Technology & Industry Group, where he has been a CTO since 2008. He is the Director of the State Key Laboratory of Wireless Mobile Communications, China Academy of Telecommunications Technology. He is also a Board Member of the Semiconductor Manufacturing International Corporation. He has devoted his works to the research and development of TD-SCDMA 3G and TD-LTE-advanced 4G since 2004. He is currently a Professor with the State Key Laboratory of Networking and Switching Technology, BUPT. His current research interests include network architectures, wireless mobile communications, Internet of Things, and vehicular network. He was a recipient of the State Science and Technology Progress Award in 2001 and 2012. He received the Outstanding Young Researcher Award from the Nature Science Foundation of China in 2014.

HUI XU received the Ph.D. degree from Xi'an Jiaotong University, Xi'an, China, in 1999. She is currently the Manager of the State Key Laboratory of Wireless Mobile Communications, Ubiquitous Network Department, China Academy of Telecommunications Technology, Beijing, China. Her research interests include key technologies in Internet of Things and machine-to-machine communications.

BO HU received the Ph.D. degree in communications and information systems from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2006. He is currently an Associate Professor with the State Key Laboratory of Networking and Switching Technology, BUPT. His current research interests include future wireless mobile communication systems, mobile Internet, and software-defined networks.