SeoulTech UCS Lab

A security Authentication Scheme of 5G Ultra-Dense Network Beased on Block chain

Presented by: Abir EL.

SeoulTech, Departement of Computer Science and engineering.

ubiquitous computing and security UCS Lab

Organisation:

- Introduction
- Problematic
- logical solution
- Key Words diffinition
- Solution proposed in the paper
- security challanges
- Security authentication scheme based on blockchain
- APG-PBFT Algorithm
- Algorithm analysis
- Conclusion

Introduction:

From the smallest personal item to the largest continents, everything everywhere will be digitally connected, and responsive to our wants and desires.

In partially, wireless communication are dominating everything, mainly empowered by revolutionary 5G technology.

And towards realizing the ambitious goals set for 5G, the density of access/serving nodes is expected to increase up to the point where it is comparable to or even surpass the (also increasing) density of user equipment, thus introducing the ultra-dense network paradigm.

Problematic:

- UDN is generaly considered to be one of the most effective means to solve the rapid growth of high traffic in 5G network.
- The Aps have a smaller coverage compared to the traditional base stations.
- For High moving mobile users, the UE have to switch frequently between the Aps, which will reduce the access speed and stability.

Problematic:

- The existing Authentication and key agreement Algorithm (AKA) in 4G network is mainly designed for security identification between the user equipment UE and the fixed Mobility Management Entity MME, thus, it cannot adapt to this fast and frequent authentication.

Solution:

If the UE can move smoothly in a trusted Aps group APG without frequent authentication, the problem will be solved!

Block Chaining technology

- 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.
- The core of block chain technology is to solve the trust security problem in the decentralized enviroment based on the consensus problem mechanism.

The Byzantine Generals Problem

- The essence of Byzaintine Generals is a consensus problem, that is, how to reach consensus on an untrustworthy distributed network, according to Lesie Lamport paper(proposed in 1982) to tolerate f traitors or less, we need 3f + 1 generals and f + 1 rounds of information exchange.
- The BGP has been extended to Fault-tolerant theory in the field of network computing.

Block chain and Consensus Mechanim

- The consensus mechanism is an algorithm to reach agreement on the recognition of transaction order rules in a time period.
- According to the different application scenarios, a variety of consensus algorithms have been designed including Proof Of Work, Proof of Stake, Delegated Proof of Stake, Casper, Practical Byzantine Fault Tolerance, proof of Elapsed Time…

The solution proposed in the paper:

- The paper propose a security authentication scheme of 5G UDN based on block chaining technology.
- An APG-PBFT algorithm based on BC technology with PBFT consensus algorithm is proposed.
- In this 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 block chain message propagation mechanisme

The solution proposed in the paper:

- This scheme can reduce the authentication frequency when UE moves among the Aps and improve the access efficiency.

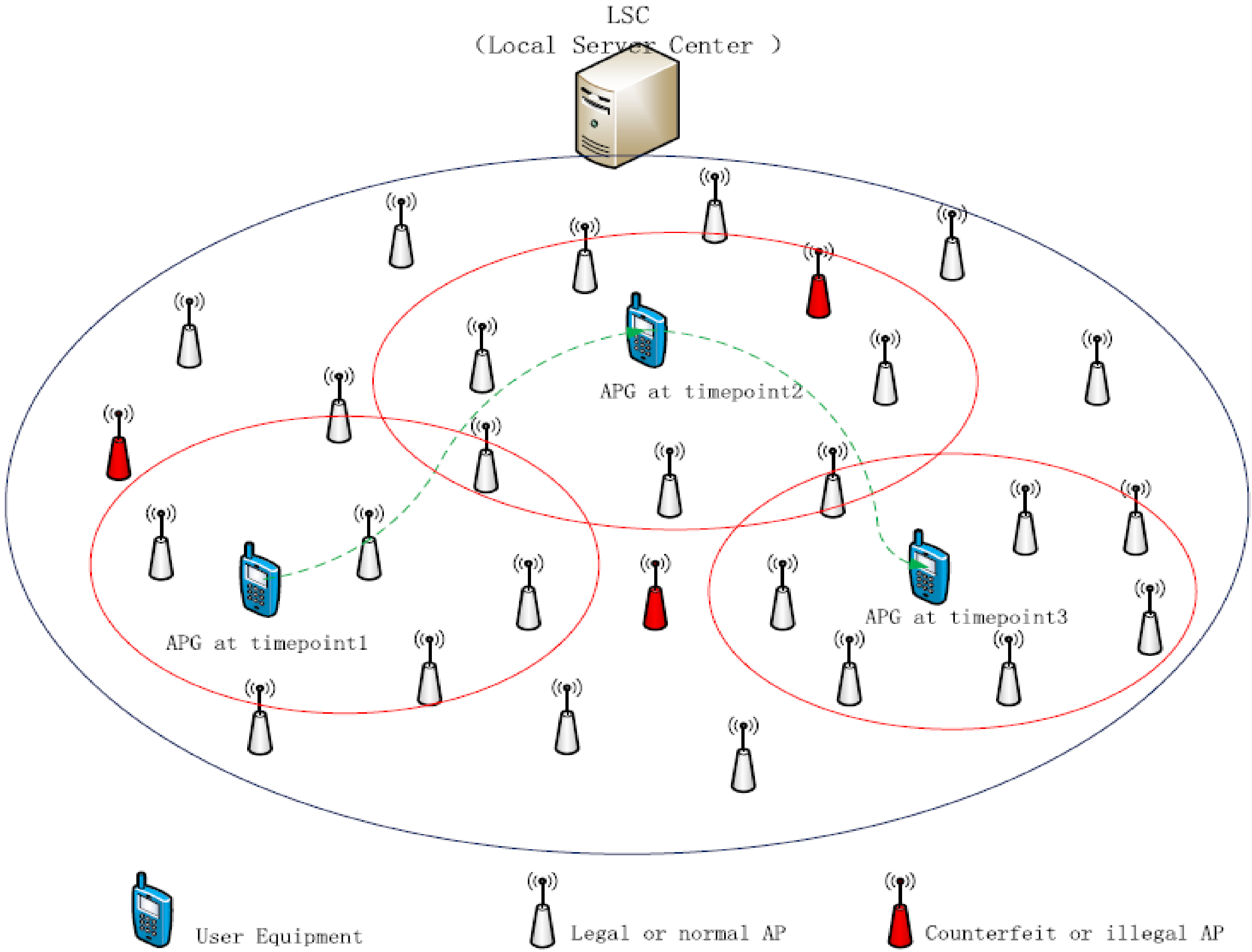


Figure 1: User centric UDN architecture

Security Challenges for users to access 5G UDN

In the 5G ultra dense network, each Aps is completely equivalence with another Aps in an APG, thus, Aps form an organization that has no center. Therefor, access security of the Aps and UE faces the following challenges.

Security Challenges for users to access 5G UDN:

- Ap fraud and APG untrusted security issues:

There is a possibility of an illegal Aps to join the APG during the member update process.

- The problem of authetication efficiency of UE access through dense Aps:

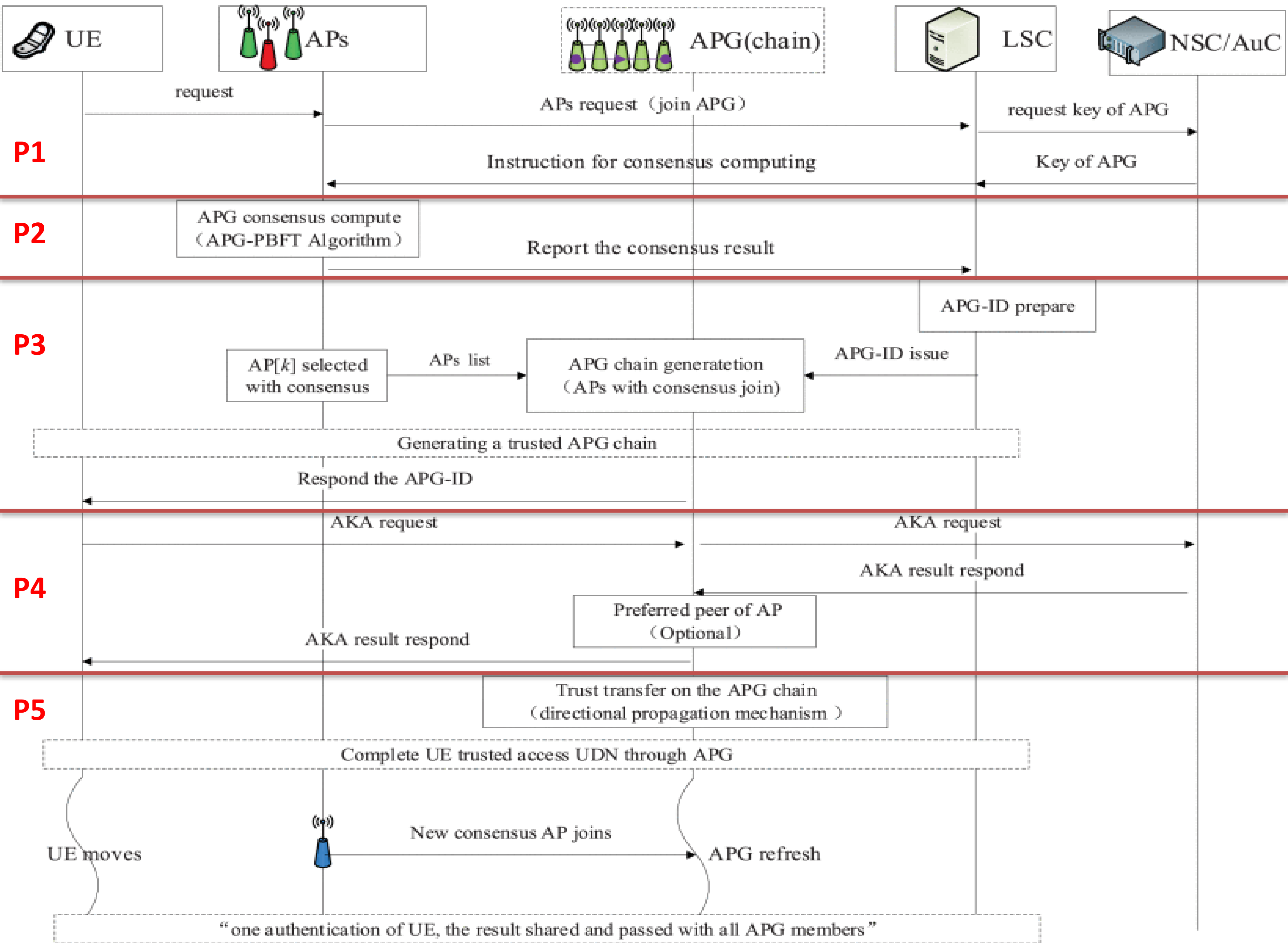
Frequent authentication poses a challenge that can not meet high quality user experience requirement.

A fast Security Authentication schene based on block chain

- Block chain provides an innovative idea for solving the APG trusted generation and security.
- The UE access the APG which is composed of Aps.
- The Aps may be legit nodes as well as fake ones.
- Therefore, forming a secure and trusted APG chain around the UE is an important prerequisite.

A fast Authentication scheme based on block chain:

- In order to realize the faulte tolerant and fast generation of APG chain, the paper propose an APG generation algorithm named APG-PBFT.
- This solution can be divided into five phases.


UE
APs
APG(chain)
LSC
NSC/AuC
request
APs request（join APG）
request key of APG
P1
Instruction for consensus computing
Key of APG
P2
APG consensus compute
（APG-PBFT Algorithm）
Report the consensus result
APG-ID prepare
P3
AP[k] selected
with consensus
APs list
APG chain generatetion
（APs with consensus join)
APG-ID issue
Generating a trusted APG chain
Respond the APG-ID
AKA request
AKA request
AKA result respond
P4
Preferred peer of AP
（Optional）
AKA result respond
P5
Trust transfer on the APG chain
（directional propagation mechanism ）
Complete UE trusted access UDN through APG
New consensus AP joins
UE moves
APG refresh
"one authentication of UE, the result shared and passed with all APG members"

APG-PBFT Consensus Algorithm

//The UE begin to send the request message Msg to LSC
//The LSC is considered as the root in this algorithm and assigned AP0

UE.Send(<cID, Msg, *t>, request, LSC);* *//with cID: identify,* t: timestamp
LSC.Verify(<cID, *h, Msg, t>, AP0);* *//h: the Msg high*
AP0.Prepare(<v, h, d>, Msg); *//d: the Msg digest, v: view* identity
AP0.Broadcast(<v, h, d, s>, APn); *//s: the digest signature* of *AP0*
//the following are similar.
//When APi receive the Msg, he begin to prepare & broadcast.

For i = 1 to n
{
APi.Receive(<v, h, d, s>);
APi.Verify(<v, h, d, s>, f, n);
APi.Prepare(<v, h, d, s>);
APi.Broadcast(<v, h, d, s>, AP|n-i|);
APi.count(<f: fault d>, count m);
}

Each peer recieve the msg from AP0, verified it and Prepare to brodcaste it between the other peer.

The peers continue to forward and recieve the msg From each other and at the same time begin to a Accumulate the quantity of msg in thier memory. When the prepare messages is over f+1 different Peers are recieved, the peers reach the prepared Status and broadcast the Commit.

//if m > f+1, broadcast commit, mark and reply to LSC(*AP0).*

While count: m > (f + 1) then

{

// add a marking function to determine whether it is consistent with the final result.

//r: the result of the request operation

APi.Mark(<v, in : d, out : d, t, Mark: k>); // this sub function is important for the lookup stage

APi.Commit(<v, h, d, s, t>, Result : k, AP0);

}

AP0.Receive(<v, h, d, s, t>, Msg: r, count m);

While count:m>(2f+1) ***then***

{

AP0 .Comput(<*v, h, d, s*>, *Msg*: r , APk=0 .Mark = *r*);

generateBlock Chain(APG, APG_ID, AP0 , *null*); =

//AP0 performs reverse lookup and marks the queue.

All peers return thier results to
The primary peer AP0.
When each peer recieves more
Than 2f+1 different peers commit
Messages, according to the PBFT
Algorithm, the peers has reached
Consensus. Then the peers reach
The committed status and BC
Can be generated now.

For k=1 to n

{

AP0 . *reLoopup*(APk.*Mark* = *r*);

if APk.*Mark* == $\boldsymbol{AP_0}$.*Mark* ***then***

{

//According to the consensus result and the marks of the peers, if Apk result is consistent with the final result marked in AP0, that means the APK is a trusted node and it will be added to the BC

addBlock Chain(APG, APG_ID, AP0 , APk);

}

else

skip ;

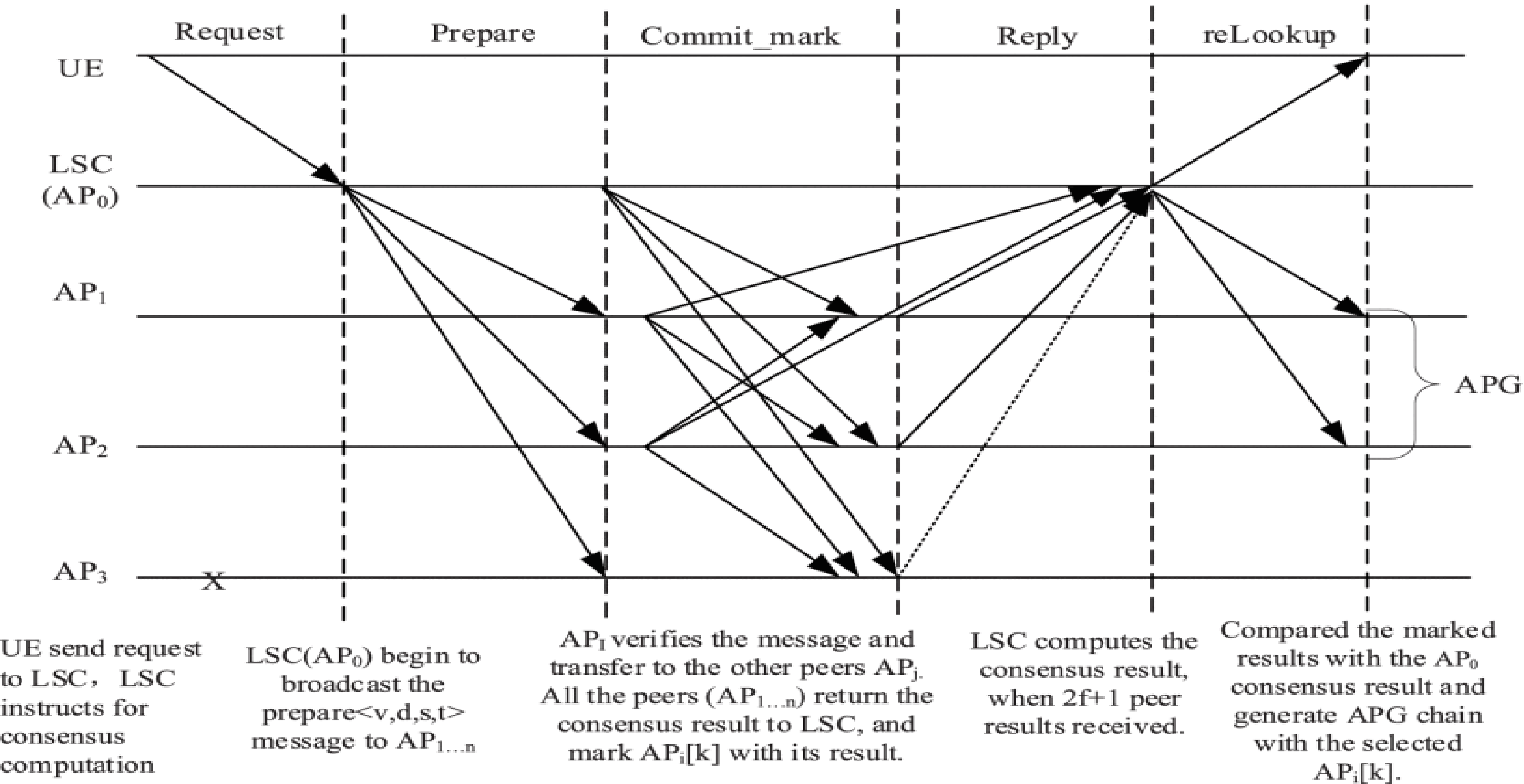
}

AP0 .Send(<*v, h, d, s, t*>, *Reply*:r , UE: cID);

}

// When all the peers have completed its consensus, the APG chain can be generated with the trusted Api peers. And when a new AP join or leave the APG, the nimber of Aps changes, therefore a new round of consensus algorithm is generated.

The graphical representation of the algorithm



APG-PBFT Agorithm Analysis

The APG-PFBT algorithm for UDN has made noticable imrovement on the traditioanal PBFT algorithm which is mainly reflected in the following four asspects

APG-PBFT Agorithm Analysis

- This algorithm put in consideration that the primary node (AP0) can be a fault node, this reduces the selection judgment process and computational complexity in the PBFT adapted in the udn actual scene

APG-PBFT Agorithm Analysis

- The sub procedure *mark* is added before the *commit* procedure. This is improves the efficiency of the lookup.
- More over, the lookup function based on the return mgs and mark is added to this algorithm, this improvement can quickly generate a trusted APG group

APG-PBFT Agorithm Analysis

- The first two stages in the traditioanl PBFT *pre-prepare AND prepare* are merged in one step *prepare* in this algorithm which shorten the transmission time.

APG-PBFT Agorithm Analysis

In order to evaluate the performance of the algorithm using simulation system for UDN, the score formula is as following:

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

With: Apn represent the quantity of peers, TPS is the transaction per second, the time Represent the average time to complete a consensus, refresh is the dynamic change of The quantity of the peers and the parametres a, b and c represent the corresponding Weight, thier deffault value are 1 and can be configurated by demande in the System initiation

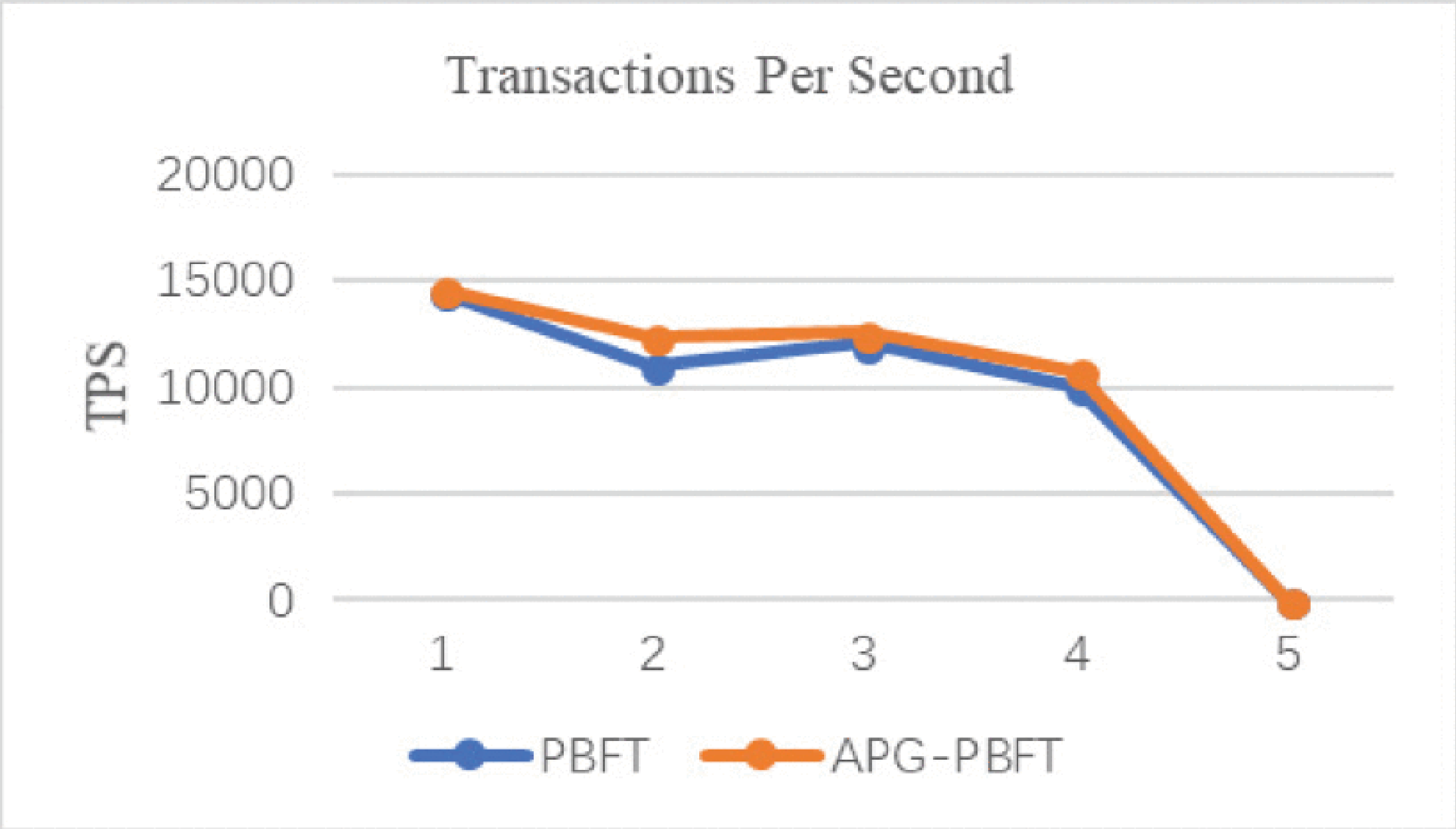
APG-PBFT Agorithm Analysis

This formula shows the relation betwen the density and the distribution radus

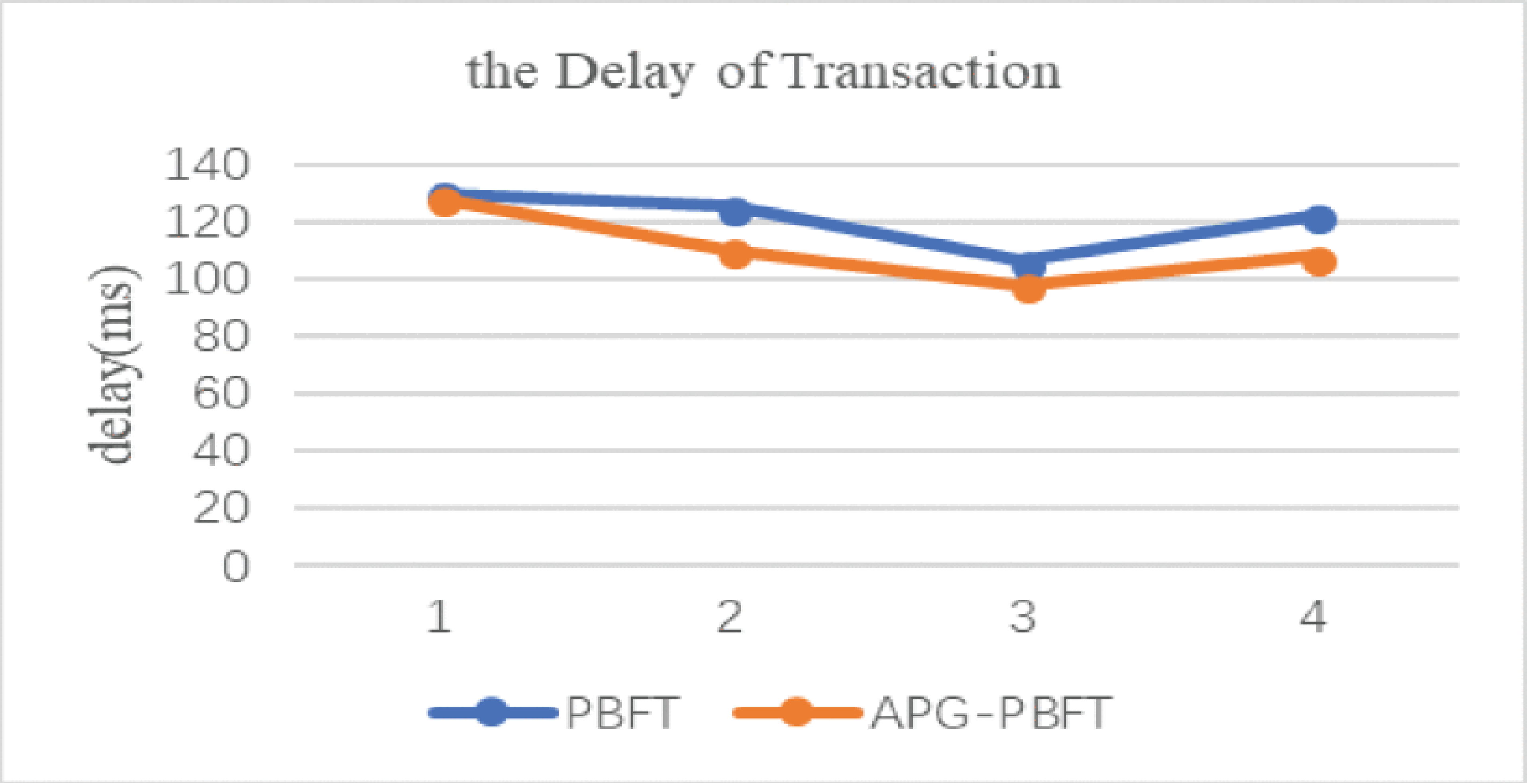
$$Max\left\lfloor d^2 \right\rfloor \le \frac{\pi r^2}{n} \le Min\left\lceil d^2 \right\rceil$$

Provided that n peers are randomly distributed around an UE. The distribution radus is *r* and the inter site distance ISD is *d* in UDN. Therefore, it is assumed that the ***Density*** around the UE should be between the *maximun spacind AND the minimum Spacing*

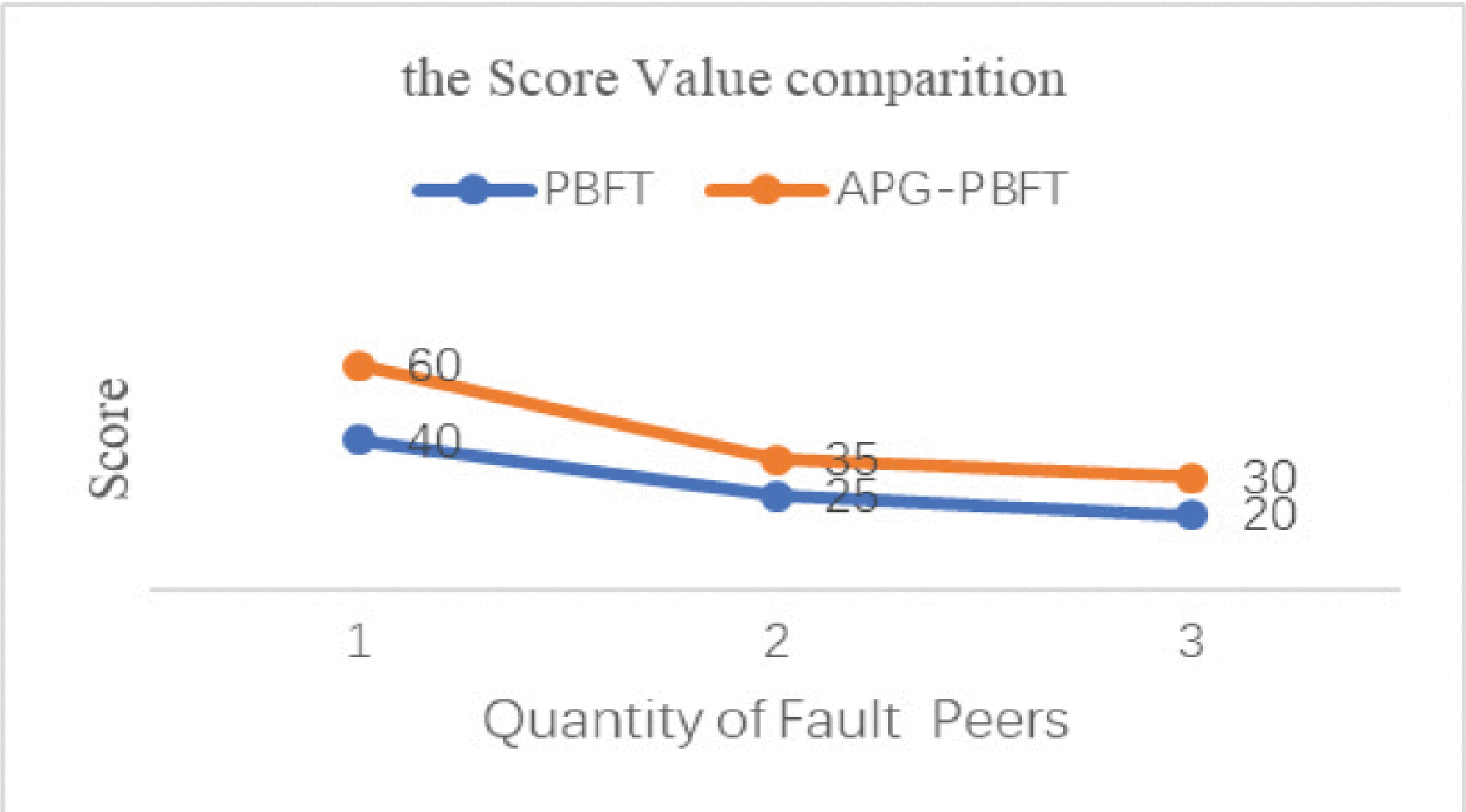
The TPS of APG-PBFT



The delay of Apg-PBFT



The score of Apg-PBFT compared with PBFT



APG-PBFT Agorithm Analysis

From the simulation results, we can see that APG-PBFT algorithm inherits the fault tolerant mechanisme and ability of PBFT as long as the fault or dishonest Aps f accod with f<= (n-1)/3

The trusted APG chain can still guarantee the security of APG for UE.

Conclusion and opinion

In the solution proposed in this paper, the APG-PBFT algorithm is improved and can generate a smooth access to the Aps for the UE with the concept of sharing the authetication result among a trusted APG in block chain so the UE can move smoothly without frequent authetication, moreover the simulation results shows that this algorithm can improve APG generatio, thus it will be valuably applied to the UDN enviroment.

I would like to hear your opinions about this Algorithm!

Thank you for your attention.

Abir EL.

SeoulTech, Departement of computer science and engineering.

ubiquitous computing and security UCS Lab