Indian J.Sci.Res. 17(2): 335-338, 2018

ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

# HANDOVER KEYMANAGEMENT IN 4GLTE/SAE NETWORKS SECURITYANALYSIS

[1]HibaMohd Abdul Qadeer,[2]Shireen Nilopher,[3]Asma Afreen
[1,2,3] Electronics and Communication Engineering, Nawab Shah Alam Khan College of Engineering and Technology, Hyderabad

***Abstract*** **:** The goal is to move mobile cellular wireless technology into its fourth generation by using 3GP Long Term Evolution/System Architecture Evolution (LTE/SAE) .To close a security gap through which a single compromised or malicious device can endanger an entire mobile network because of the open nature of these networks is one of the unique challenges of fourth-generation technology. To revoke any compromised key(s) and as a consequence isolate corrupted network devices Hand over key management in the 3GPPLTE/SAE has been designed.This.paper, identifies .and .details .the .vulnerability .of. this hand over key management to what are called resynchronization attacks; such attacks jeopardize secure communication between users and mobile networks. Although period updates of the root key are an integral part of hand over key management, our work here emphasizes how essential these updates are to minimizing the effect of resynchronization attacks that ,as of now ,cannot be effectively prevented. Our main contribution, however, is to explore how network operators can determine for themselves an most favorable interval for updates that minimizes the signaling load they impose while protecting the security of user traffic. Our analytical and simulation studies demonstrate the impact of the key update interval on such performance criteria as network topology and user mobility.

***Keywords:***Authentication and keyagreement,evolvedpacketsystem,handoverkeymanagement,long-termevolution security.

## I. Introduction

The enormous popularity of the Internet has produced a significant stimulus to P2Pfile sharing systems. There are two types of P2P systems: unstructured and structured. Unstructured P2P networks such as Gnutella and Free net do not allocate responsibility for data to specific nodes. According to some loose rules no disjoin and leave the network. Currently, unstructured P2Pnetworks' file query method is based on either flooding where the query is propagated to all the node's neighbors, or random-walkers where the query is forwarded to randomly chosen neighbors until the file is found. Flooding and random walkers cannot guarantee data location.

Structured P2P networks ,i.e. Distributed Hash Tables(DHTs), with their features of higher efficiency, scalability, and deterministic data location can over come the drawbacks. They have strictly proscribed topologies, and their data residency and lookup algorithms are precisely defined based on a DHT data structure and consistent hashing function. Even if the system is in a continuous state of change then responsible for a key can always be found.

Most of the DHTs require *O(log n)* hops per lookup request with *O(logn)* neighbors per node, where n is the number of no desin the system. Akey condition to judge is its file location efficiency for P2P file sharing system.several methods have been propose to enhanced this efficiency. One method uses a super peer topology, which consists of supernodes with fast connections and regular nodes with slower connections. Some regular nodes,and a regular node connects with a super node and a supernode connects with other super nodes. Then odesat the center of the network are faster and therefore produce a more reliable and stable backbone in this super-peer topology.This allows more messages to be routed than a slower backbone and,therefore ,allows greater scalability.

Super-peer networks occupy the middle-ground between centralized and entirely symmetric P2P networks, and have the potential to combine the benefits of both centralized and distributed searches.Another class of methods to improve file location efficiency is through a proximity-aware structure.A logical proximity abstraction derived from a P2P system doesnot essentially match the physical proximity information in reality. The shortest path according to the routing protocol(i.e.,the least hop count routing)is not essentially the shortest physical path. This difference becomes a big obstacle for the deployment and performance optimization of P2Pfilesharingsystems.

AP2P system should utilize proximity information to reduce file query over head and improve its efficiency. In otherwords, allocating or replicating a file to anode that is physically closer to a request er can significantly help the requester to recover the file efficiently. Proximity-aware clustering can be used to group physically close peers to competently improve efficiency. To improve file location efficiency is to cluster nodes with similar interests, which reduce the file location latency is the third method. Although numerous proximity-based and interest-based super-peer topologies have been proposed with different features, few methods are able to cluster peers according to both proximity and concern. Most of these methods are on unstructured P2P systems that have no strict policy for

[1]**Corresponding Author**

topology construction. Inspite of their higher file location efficiency they cannot be directly applied to general DHTs

## II.RelatedWork

The related works most relev an to PAIS in three groups: super-peer topology is discussed, proximity-awareness, and interest-based filesharing. Super-peer topology. Fast Track[10] and Morpheus[20]use super-peer topology. The super-peer network in[8]is for resource fuland scalable file consistency maintenance in structured P2Psystems.

A super-peer network for load balancing[9] was built in previous work.Garbackietal.[21]proposed a self-organizing super-peer network architecture that solves four issues in a fully decentralized manner: how client peers are related to super-peers ,how super-peers locate files, how the load is balanced among the super-peers, and how the system deals with node failures. Proximity-awareness Techniques to make use of topology informationinP2Poverlay routing include geographic layout.

Proximity routing and proximity-neighbour selection. Geographic layout way maps the overlay's logical ID space to the physical networks or that neighboring nodes in the ID space are also close in the physical network. It is employed in topologically-aware CAN [11].In the proximity routing method, the reasonable overlay is constructed with out considering the essential physical topology.

Interest-base file sharing. One class of interest-base file sharing networks is called schema based networks. They use explicit schemas to depict peers' contents based on semantic description and allow the aggregation and in corporation of data from distributed data sources. Hang and Sia proposed a method for clustering peers that share similar property together and a new intelligent query routing strategy.

Liuetal. proposed on line storage systems with peer assistance. The works in employ the Bloom filter method for file searching. Despite the efforts devoted to proficient file locationinP2P systems, there are few works that merge the super-peer topology with both interest and proximity based clustering methods.

In addition,it is difficult to realize in DHTs due to their harshly defined topology and data allocation policy. howPAIS tackles the challenge by taking advantage of the hierarchical structure of a DHT is describes in this paper.

## III. Problem Statement

### Exiting Model

Existing analyzes the authentication and key agreement protocol adopted by Universal Mobile Telecommunication System (UMTS), an emerging standard for third-generation(3G)wireless communications. The protocol, knownas3GPPAKA,is based on the security framework in GSM and provides significant improvement to address and correct real and professed weaknesses in GSM and other wireless communication systems.

3GPPAKA protocol is susceptible to a alternate of the so-called false base station attack. The defense lessness allows an adversary to re direct user traffic from one network to another. Moreover, we demonstrate that the use of synchronization between a mobile station and its home network in considerable complexity for the normal operationof3GPPAKA.

Securityproblemsinthe3GPPAKA,we then present a new authentication and key agreement protocol which defeat sre direction attack and drastically lowers the impact of network corruption. The protocol, called AP-AKA ,also eliminates the need of synchronization between a mobile station and its home network. AP-AKA specifies a sequence of multiple flows.

## IV.Proposed System

Our proposed method an unaffected session key would permit target e Node B to know which session key the source e Node B used .To prevent this, the source e Node B computes a new session key by applying a one-way function to a current session key. This ensures backward key separation in the handover. However, backward key separation blocks an e Node B only from deriving past session keys from the current session key.Otherwise, this e Node B would know all session keys used in further sessions in a whole chain of hand overs. As a consequence, forward key separation was introduced to ensure that network elements add fresh materials to the process of creating a new session key for then ext serving e Node B. The current e Node B,unaware of this additive, would be unable to derive the next key.

**The main contributions of this paper are threefold***:*

1) Hand over key management of the EPS security mechanism flaws has been identified.

2)Promising mathematical model for the EPS hand over key management to measure the effect of a compromised key has been designed

3)Investigated the performance criteria(e.g., user mobility, network topology, and so on)involved in selecting an optimal operational point for key updating.

## V. Overview

### PAIS: A Proximity Aware Interest-Clustered P2P File Sharing System.

we studied a Bit Torrent user activity trace to analyze the user file sharing behaviors. We found that long distance file recovery does exist.Thus, we can cluster physically close no des into a cluster to enhance file sharing efficiency

.Also, peers tend to visit files in a few interests. Thus, we can further cluster nodes that share an interest into a sub-cluster. Finally, popular files in each interest are shared among peers that are globally distributed.

Thus ,we can use file replication between locations for popular files, and use system-wide file searching for unpopular files .We introduce the detailed design of PAIS below.It is suitable for a file sharing system where files can be classified to a number of interests and each interest can be classified to a number of sub-interests.

## VI. PAIS Structure

PAIS is developed based on the Cycloid structured P2P network. Cycloidis a lookup efficient, constant-degree over lay with $n=d.2d$ nodes,where d is its dimension. It achieves a time complexity of $O(d)$ per look up request by using$O(1)$ neighbors per node. Each Cycloid node is represented by a pair of in dices$(k,a_{d-1}a_{d-2}....a_0)$where k is a cyclic index and$(a_{d-1}a_{d-2}....a_0)$ is a cubical index. The cyclic index is an integer ranging from 0to d-1,and the cubical index is a binary number between 0 and 2d-1. The nodes with the same cubical index are ordered by their cyclic index mod do n a small cycle,which we calla cluster.

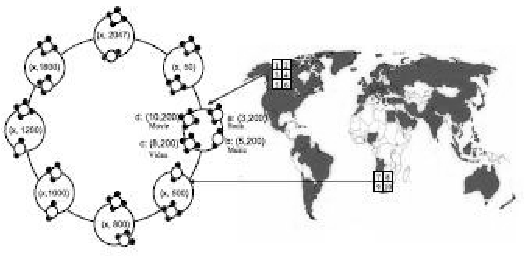

Figure 1

## VII.PAIS Construction And Maintenance

Node proximity representation. A land marking method can be used to represent node closeness on the network by in dices used in .Landmark clustering has been widely adopted to generate proximity information.It is based on the intuition that nodes close to each other are likely to have similar distances to a few selected land mark nodes. We assume there are m land mark nodes that are randomly scattered in the Internet.

## VIII. Experimental Result

We implemented a prototype of PAIS on Planet La,a real-world distributed test bed,to measure the performance of PAIS in comparison with other P2P file sharing systems. We set the experiment environment according to the study results of a B it Torrent trace.We randomly selected 350 Planet Lab nodes all over the world.Among these nodes, we randomly selected 30 nodes as landmark nodes to calculate the Hilbert numbers of nodes.We clustered all nodes into 169 different locations according to the close ness of their Hilbert numbers.

We used the 56,076files in the Bit Torrent trace.The number of interests in the system was set to 20,so we also set the dimension of the Cycloid DHTto20.We simulated

100,000 peers by default in the experiments. Each peer was randomly assigned to a location cluster among all 169 clusters, and further randomly assigned to a Planet-Lab node with in this location. According to ,a peer's requests mainly focus on around 20 percent of all of its interests. Thus,we randomly selected four interests(20percentof total20interests)for each peer as its interests.

The files are randomly assigned to a sub-cluster with the files'interestoverthetotal160 locations, and then randomly assigned to no desin the sub-cluster.Eighty percent of all queries of a requester target on files with owners with in the same location,among which 70 percent of its queries are in the interests of the requester.

According to [48],80 percent of all requests from a peer focus on its interests,and each of other requests is in a randomly selected interest outside of its interests. A request in a n interest means a request for a randomly selected file in this interest.We also let each file have a copy in another peer in a different location in order to test the proximity-aware file searching performance.

In recent years,to enhance file location efficiency in P2P systems, interest-clustered super-peer networks and proximity-clustered super-peer networks have been proposed. Although both strategies improve the performance of P2P systems, few works cluster peers based on both peer interest and physical proximity simultaneously. Moreover ,it is harder to realize it in structured P2P systems due to their strictly defined topologies, although they have high efficiency of file location than unstructured P2Ps.

## IX.Conclusion

In this paper ,we introduce aproximity-aware and interest-clustered P2P file sharing system based on a structured P2P.It groups peers based on both interest and proximity by taking advantage of a hierarchical structure of a structured P2P.PAIS uses an intelligent file replication algorithm that replicates a file frequently requested by physically close nodes near their physical location to enhance the file look up efficiency.

Finally, PAIS enhances the file searching efficiency among the proximity-close and common interest nodes through a number of approaches. The trace-driven experimental results on Planet Lab demonstrate the efficiency of PAIS in comparison with other P2Pfile sharing systems. It dramatically reduces the over head and yields significant improvements in file location efficiency even in node dynamism. Also, the experimental results show the effectiveness of the approaches for improving file searching efficiency among the proximity close and common-interest nodes.

## References

[1] BitTorrent.(2013)[Online].Available:http://www. bittorrent.com/

[2] Gnutella homepage. (2003)[Online]. vailable:http://www.gnutella.com

[3] I.Clarke,O.Sandberg, B.Wiley,andT. W. Hong,"Freenet:Adistributedanonymousinformationstorageandretrievalsystem," inProc. Int. Workshop Des. IssuesAnonymityUnobservability,2001,pp.46–66.

[4] I. Stoica, R. Morris, D. Liben-Nowell, D. R. Karger, M. F.Kaashoek,F.Dabek,and H.Balakrishnan,"Chord: Ascalablepeer-topeerlookupprotocolforinternetapplications,"IEEE/ACMTrans. Netw.,vol.11,no.1, pp.17–32,Feb.2003.

[5] A. RowstronandP. Druschel, "Pastry: Scalable, decentralized objectlocationandroutingforlarge-scalepeer-to-peer systems," in Proc.IFIP/ACMInt. Conf.Distrib.Syst.PlatformsHeidelberg,2001,pp.329–350.

[6] B. Y. Zhao,L.Huang,J. Stribling,S.C.Rhea,A.D.Joseph,andJ.Kubiatowicz," Tapestry:Aresilient global-scaleoverlayforservicedeployment,"IEEEJ.Sel.AreasCommun., vol.22,no.1,pp.41–53,2004.

[7] H.Shen,C.Xu,andG.Chen,"Cycloid:Ascalableconstant-degreeP2Poverlaynetwork,"Perform.Eval.,vol.63,pp.195–216,2006.

[8] Z. Li, G. Xie, andZ. Li, "Efficient and scalable consistencymaintenanceforheterogeneouspeer-to-peer systems," IEEETrans.ParallelDistrib.Syst.,vol.19, no.12, pp.1695–1708,Dec.2008.

[9] H. ShenandC.-Z. Xu, "Hash-based proximity clustering forefficientload balancing in heterogeneous DHT networks," J.ParallelDistrib.Comput.,vol.68, pp.686–702,2008.