IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Security Analysis of Handover Key Management in 4G LTE/SAE Networks

Dr.P.Sumitra[1], P.Ponkavitha[2]

Assistant Professor, Dept. of Computer Science, Vivekanandha College of Arts & Sciences for Women (Autonomous), Elayampalayam, Tiruchengode, India[1]

Research Scholar, Dept. of Computer Science, Vivekanandha College of Arts & Sciences for Women (Autonomous), Elayampalayam, Tiruchengode, India[2]

Abstract: The goal of 3GPP Long Term Evolution/System Architecture Evolution (LTE/SAE) is to move mobile cellular wireless technology into its fourth generation. One of the unique challenges of fourth-generation technology is how to close a security gap through which a single compromised or malicious device can jeopardize an entire mobile network because of the open nature of these networks. Handover key management in the 3GPP LTE/SAE has been designed to revoke any compromised key(s) and as a consequence isolate corrupted network devices. This paper, however, identifies and details the vulnerability of this handover key management to what are called desynchronization attacks; such attacks jeopardize secure communication between users and mobile networks. Although periodic updates of the root key are an integral part of handover key management, our work here emphasizes how essential these updates are to minimizing the effect of desynchronization attacksthat, as of now, cannot be effectively prevented. Our main contribution, however, is to explore how network operators can determine for themselves an optimal 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 key agreement, evolved packet system, handover key management, long-term evolution security.

I. INTRODUCTION

Over the past fewyears, the immense popularity of the Internet has produced a significant stimulus to P2P file sharing systems. For example, BitTorrent constitutes roughly 35 percent of all traffic on the Internet. There are two classes of P2P systems: unstructured and structured. Unstructured P2P networks such as Gnutella and Freenet do not assign responsibility for data to specific nodes. Nodes join and leave the network according to some loose rules. Currently, unstructured P2P networks' 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.However, flooding and random walkers cannot guarantee data location. Structured P2P networks , i.e., Distributed Hash Tables (DHTs), can overcome the drawbacks with their features of higher efficiency, scalability, and deterministic data location. They have strictly controlled topologies, and their data placement and lookup algorithms are precisely defined based on a DHT data structure and consistent hashing function. The node responsible for a key can always be found even if the system is in a continuous state of change. Most of the DHTs require *O(log n)* hops per lookup request with *O(log n)* neighbors per node, where n is the number of nodes in the system. A key criterion to judge a P2P file sharing system is its file location efficiency. To improve this efficiency, numerous methods have been proposed. One method uses a super peer topology, which consists of super nodes with fast connections and regular nodes with slower connections. A super node connects with other super nodes and some regular nodes, and a regular node connects with a super node. In this super-peer topology, the nodes at the center of the network are faster and therefore produce a more reliable and stable backbone. 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 does not necessarily match the physical proximity information in reality. The shortest path according to the routing protocol (i.e., the least hop count routing) is not necessarily the shortest physical path. This mismatch becomes a big obstacle for the deployment and performance optimization of P2P file sharing systems.

A P2P system should utilize proximity information to reduce file query overhead and improve its efficiency. In other words, allocating or replicating a file to a node that is physically closer to a requester can significantly help the requester to retrieve the file efficiently. Proximity-aware clustering can be used to group physically close peers to effectively improve efficiency.

DOI 10.17148/IJARCCE.2016.5282

The third class of methods to improve file location efficiency is to cluster nodes with similar interests, which reduce the file location latency. 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 interest. In addition, most of these methods are on unstructured P2P systems that have no strict policy for topology construction. They cannot be directly applied to general DHTs in spite of their higher file location efficiency.

II. RELATED WORK

We discuss the related works most relevant to PAIS in three groups: super-peer topology, proximity-awareness, and interest-based file sharing. Super-peer topology. FastTrack [10] and Morpheus [20] use super-peer topology. The super-peer network in [8] is for efficient and scalable file consistency maintenance in structured P2P systems.

Our previous work built a super-peer network for load balancing [9].

Garbacki et al. [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 exploit topology information in P2P overlay routing include geographic layout.

Proximity routing, and proximity-neighbour selection. Geographic layout method maps the overlay's logical ID space to the physical network so 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 logical overlay is constructed without considering the underlying physical topology.

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

Liu et al. proposed online storage systems with peer assistance. The works in employ the Bloom filter technique for file searching. Despite the efforts devoted to efficient file location in P2P systems, there are few works that combine the super-peer topology with both interest and proximity based clustering methods. In addition, it is difficult to realize in DHTs due to their strictly defined topology and data allocation policy. This paper describes how PAIS tackles the challenge by taking advantage of the hierarchical structure of a DHT.

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, known as 3GPP AKA, is based on the security framework in GSM and provides significant enhancement to address and correct real and perceived weaknesses in GSM and other wireless communication systems.

3GPP AKA protocol is vulnerable to a variant of the so-called false base station attack. The vulnerability allows an adversary to redirect user traffic from one network to another. It also allows an adversary to use authentication vectors corrupted from one network to impersonate all other networks. Moreover, we demonstrate that the use of synchronization between a mobile station and its home network incurs considerable difficulty for the normal operation of 3GPP AKA.

Security problems in the 3GPP AKA, we then present a new authentication and key agreement protocol which defeats redirection 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 unchanged session key would permit target eNode B to know which session key the source eNode B used. To prevent this, the source eNodeB 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 eNodeB only from deriving past session keys from the current session key. Otherwise, this eNodeB would know all session keys used in further sessions in a whole chain of handovers. 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 the next serving eNodeB. The current eNodeB, unaware of this additive, would be unable to derive the next key.

The main contributions of this paper are threefold:

1) We identified flaws in the handover key management of the EPS security mechanism.

2) We designed a promising mathematical model for the EPS handover key management to measure the effect of a compromised key;

3) We 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.

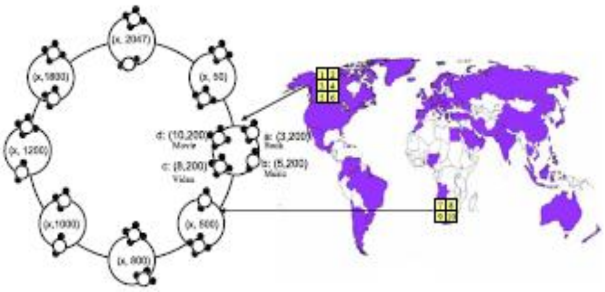
DOI 10.17148/IJARCCE.2016.5282

In our previous work], we studied a BitTorrent user activity trace to analyze the user file sharing behaviors. We found that long distance file retrieval does exist. Thus, we can cluster physically close nodes 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. Cycloid is a lookup efficient, constant-degree overlay with $n=d.\ 2d$ nodes, where d is its dimension. It achieves a time complexity of $O(d)$ per lookup request by using $O(1)$ neighbors per node. Each Cycloid node is represented by a pair of indices $(k,a_{d-1}a_{d-2}....a_0)$ 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 0 to 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 d on a small cycle, which we call a cluster.



VII. PAIS CONSTRUCTION AND MAINTENANCE

Node proximity representation. A landmarking method can be used to represent node closeness on the network by indices 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 landmark nodes. We assume there are m landmark nodes that are randomly scattered in the Internet.

VIII. EXPERIMENTAL RESULT

We implemented a prototype of PAIS on PlanetLa , a real-world distributed testbed, 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 BitTorrent trace. We randomly selected 350 PlanetLab 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 closeness of their Hilbert numbers.

We used the 56,076 files in the BitTorrent trace. The number of interests in the system was set to 20, so we also set the dimension of the Cycloid DHT to 20. 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 within 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 (20 percent of total 20 interests) for each peer as its interests.

The files are randomly assigned to a sub-cluster with the files’ interest over the total 160 locations, and then randomly assigned to nodes in the sub-cluster. Eighty percent of all queries of a requester target on files with owners within 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 an 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 a proximity-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 lookup efficiency.

Finally, PAIS enhances the file searching efficiency among the proximity-close and commoninterest nodes through a number of approaches. The trace-driven experimental results on PlanetLab demonstrate the efficiency of PAIS in comparison with other P2P file sharing systems. It dramatically reduces the overhead 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.

DOI 10.17148/IJARCCE.2016.5282

REFERENCES

[1] BitTorrent. (2013) [Online]. Available: http://www.bittorrent.com/
[2] Gnutella home page. (2003) [Online]. Available: http://www.gnutella.com[3] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong, "Freenet: A distributedanonymous information storage and retrieval system," inProc. Int. Workshop Des. Issues Anonymity Unobservability, 2001,pp. 46–66.
[4] I. Stoica, R. Morris, D. Liben-Nowell, D. R. Karger, M. F. Kaashoek,F. Dabek, and H. Balakrishnan, "Chord: A scalable peer-topeerlookup protocol for internet applications," IEEE/ACM Trans. Netw., vol. 11, no. 1, pp. 17–32, Feb. 2003.
[5] A. Rowstron and P. Druschel, "Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems," in Proc. IFIP/ACM Int. Conf. Distrib. Syst. Platforms Heidelberg, 2001, pp. 329–350.
[6] B. Y. Zhao, L. Huang, J. Stribling, S. C. Rhea, A. D. Joseph, and J. Kubiatowicz, "Tapestry: A resilient global-scale overlay for service deployment," IEEE J. Sel. Areas Commun., vol. 22, no. 1, pp. 41–53, 2004.
[7] H. Shen, C. Xu, and G. Chen, "Cycloid: A scalable constant-degree P2P overlay network," Perform. Eval., vol. 63, pp. 195–216, 2006.
[8] Z. Li, G. Xie, and Z. Li, "Efficient and scalable consistency maintenance for heterogeneous peer-to-peer systems," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 12, pp. 1695–1708, Dec. 2008.
[9] H. Shen and C.-Z. Xu, "Hash-based proximity clustering for efficient load balancing in heterogeneous DHT networks," J. Parallel Distrib. Comput., vol. 68, pp. 686–702, 2008.

BIOGRAPHIES

Dr.P.SUMITRA Prof & Head of the Department, Computer Science and Computer Application,Vivekanandha College of Arts and Sciences for Women (Autonomous) Elayampalayam, Tiruchengode.

P.PONKAVITHA Research Scholar, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous) Elayampalayam, Tiruchengode.

DOI 10.17148/IJARCCE.2016.5282