

A Framework for Security-Enhanced Peer-to-Peer Applications in Mobile Cellular Networks

Shuping Liu¹, Shushan Zhao², Weirong Jiang³

¹*Department of Electrical Engineering, University of Southern California, Los Angeles, USA*

²*Department of Computer Science, University of Windsor, Windsor, Canada*

³*Juniper Networks Inc, Sunnyvale, USA*

E-mail: lius@usc.edu, zhao114@uwindsor.ca, weirongj@acm.org

Received May 24, 2011; revised June 21, 2011; accepted July 1, 2011

Abstract

Due to the dual trends of increasing cellular network transmission capacity and coverage as well as improving computational capacity, storage and intelligence of mobile handsets, mobile peer-to-peer (MP2P) networking is emerging an attractive research field in recent years. However, these trends have not been clearly articulated in perspective of both technology and business. In this paper, we propose a novel MP2P framework that is based on existing cellular network architecture to provide secure and efficient P2P file sharing for 3G and future 4G systems. Our framework, which is built on P2P over Session Initiation Protocol (SIP) mechanism, provides to network operators and P2P service providers efficient data transmission in cellular networks. With a secure enhancement using identity-based cryptography, the framework also provides desirable support for security, group management, mobility, and chargeability to meet business requirements.

Keywords: Mobile Cellular, 3G, P2P, SIP, IMS, Identity-Based Cryptography

1. Introduction

Mobile cellular networks and handsets are developing rapidly in recent years. While GSM systems have proven successful, 3G systems (including W-CDMA, CDMA-2000, and TD-CDMA/TD-SCDMA) are burgeoning and 4G is on the way. These new technologies have brought many conveniences to our life and in some way changed the life style of modern people, although there are also some criticisms against this change.

The P2P network has emerged as an efficient system, being typically used for sharing content files containing audio, video, data or any digital-format files and distributing services over fixed networks. Currently, P2P applications are considered to be generating most of the internet traffic [1,2].

Meanwhile, the technology of P2P has recently begun to extend its scope to address relevant problems of mobile systems in the cellular networks. P2P data exchange is a very promising business in cellular networks, but it has attracted very little academic interest due to both business and technical reasons. On the one hand, the business model regarding how this business can operate and make profit is not yet very clear. On the other hand, although

there is no technique impediment for applying P2P in cellular networks theoretically, there is no complete solution taking practical issues into consideration, e.g. security, group management, mobility, and chargeability. There are many complications considering the complexity of cellular networks. A P2P application makes a cellular network more prone to security issues such as trust (privacy: how much information does the un-trusted peer need to know about me? and confidentiality: what if the peer who knows my information misuses it?) and DoS attacks. Techniques widely applied in Internet, such as PKI, are not suitable for cellular networks, due to specific characteristics of the latter, such as lack of infrastructure, constrained communication and computational resources *etc.* A reliable framework for authentication without centralized elements is a challenge [3].

To inspire more interest and promote research on this topic, we would like to propose a MP2P solution framework in this paper. The framework considers P2P applications in cellular networks in particular 3G networks, based on IMS and SIP signaling. The framework has a security add-on layer to meet business requirements, such as user authentication, non-repudiation, data and identity integrity, confidentiality.

The rest of the paper is organized as follows. In Section 2, we will present types of architectures for MP2P and propose a hybrid P2P architecture which can be applied to IMS-based P2P networks, and introduces the application of SIP in P2P network. In Section 3, we first state the security requirements for the MP2P system, and then propose a solution. To evaluate the performance of the proposed framework we build a mathematical model that takes as input search and download queries, and returns as output hit-rate probabilities and time delay. In Section 4, we analyze the system performance and security features mathematically. The last section concludes the paper.

2. A MP2P Framework in IMS

2.1. Types of Traditional P2P Architectures and Proposed Hybrid P2P Architecture

Traditionally, there are two types of P2P architectures: centralized P2P and Decentralized P2P.

- **Centralized P2P:** In wired network, centralized P2P is the first generation architecture which uses several central index servers to control the whole network and provide metainformation service, such as index of files for sharing by each peer. To participate in these networks, the peer must connect as a client to the centralized server and then locate specific contents. When the peer is located, the requesting node starts the transfer directly from the located peer.
- **Decentralized P2P:** The decentralized P2P architecture lacks central entities which could control the network, and every node in the network acts as a peer which is unaware of other peers. All the information, including metainformation, is maintained by peers. The decentralized architecture can be divided into structured and unstructured. Though search and download queries are flushed in both structured and unstructured P2P network, queries in structured P2P network are easier to be hit than unstructured P2P network. That is because the topology of structured P2P network is tightly controlled and files for sharing are placed at specific locations. Such kinds of systems usually deploy Distributed Hash Table (DHT). The unstructured P2P networks have no precise control over the network topology or the file placement. Queries in such systems are usually forwarded to random neighbors [4]. In decentralized P2P network, flushing queries consumes a lot of time and bandwidth.
- **Semi-centralized P2P:** The semi-centralized P2P architecture combines the efficiency and resilience of both centralized and decentralized architectures. It

structures the network in hierarchies by establishing a backbone network of super peers which function as the central index servers in centralized P2P. As a result the whole P2P network is partitioned by these super peers into several sub-networks logically. Each logical sub-network is characterized by centralized P2P architecture. When a client peer logs on to the network, it makes a direct connection to a single super peer which collects and maintains information about client peers and content available for sharing.

Comparison among different P2P architecture is given in **Table 1**.

In the context of cellular networks, a cellular network covers a certain area that is divided into possibly overlapping cells. Each cell has a fixed base station (BS). The base stations are connected to each other by a wired network. In cellular network, radio link is costly and inadequate. For this reason, in normal structure of cellular communication, there is no direct correspondence between cellular phones. Several architectures have been proposed, such as mobile hash-based structured P2P architecture (HS-P2P) [5] and mobile agent P2P architecture [6].

In this paper we proposed a hybrid P2P architecture that combines the efficiency and resilience of both centralized and decentralized architectures [7]. By using semicentralized architecture, each mobile terminal connects to a single super peer directly, which is basically Base Station (BS) of cellular networks. The super peer collects and maintains information about peers and metainformation of contents available for sharing. Then all these super peers form a decentralized P2P backbone

Table 1. Comparison of different P2P architectures.

Architecture	Centralized	Decentralized	Semi-Centralized
Network Scalability	Medium	Low	Very High
Resiliency	Low	Very High	Medium
Search Efficiency	Very High	Medium	High
Search Coverage	Very High	Medium	High
Operator Control	Very High	Low	High
Signaling Overhead in SP	Very High	--	High
Signaling Overhead in OP	Low	High	Low

network. In this way, the traffic loads are moved to the network (super peers) side, which minimizes the usage of the radio link. Additionally, due to the two-layer hierarchies, semi-centralized architecture is more scalable.

By using SP, the performance of P2P applications is dramatically improved. At the same time, decentralized P2P applications are also supported for peers with special requirements, for example high privacy in their communication.

2.2. Database Tables in Super Peers

Each super peer maintains four tables: content table, client table, caching table, membership table.

The content table stores the information about content for sharing in its network and facilitates SP to locate the client peers (in following sections client is used to refer to client peer). To improve searching efficiency, SP builds three levels index for the lookup table. The first level index consists of different classes of content. For instance, the first level index can be categorized into: music, picture, literature and so on. The second level comprises different clusters in each class in the first level, which divides the first level classes into more detailed sub-classes. The third level is made up of leaf nodes which are the specific meta-information of content file for sharing. Each file has a unique id.

To illustrate the use of index table, let us look at an example. One client has a piece of song, called "Country Road" for sharing. According to the classification of index, this song belongs to class of music in the first level index and country music in the second level index. SP obtains this information and adds the new item along with the file profiles, such as ownership and file size into its content table. Because the content of shared file with the same name may be different, each content table also contains the basic information of shared file, such as file size, modified time and so on.

In client table, each entry is a client which is identified by the client's ID (such as the telephone number). Each entry records the specific bandwidth and membership information of one client. The client table provides the parameters which SP can choose so that QoS is guaranteed when downloading the files.

The caching table, by nature, is similar with the content table. The only difference is that caching table stores the sharing content owned by clients in other SP networks. For example, initially the caching table is empty. When a SP A can not find the requested information in its content table, it floods the requests to all the other SPs. If a SP B responses to SP A, which means B has the requested information, A locates the client (who has the requested resource) and at the same time stores the re-

sponse information and corresponding SP in its caching table. The caching table is updated in the way of Least Recently Used (LRU) cache, in which the items are saved in decreasing order by the times of most recent request. More popular the file, closer it is to the top of the lookup table. To fit the fixed length of caching table, once response information reaches the end of the list, it is removed from the caching table, when a new item is added. Once the caching table has been built, the SP may obtain its next hop without flushing the request message, which, to some extent, reduces traffic flooding.

The membership table contains information about groups. Groups are categorized by interest. To participate or leave a group, the client has to apply to SP. SP examines whether the group ID in the request message matches the group ID in the response message.

2.3. Backup Super-Peer

In the introduced MP2P hybrid architecture, the super-peer becomes a single-point failure for its network, when super-peer fails or be offline the all shared information in the network is lost. To increase the reliability of the architecture, the backup super-peer is introduced. They copy all the data information from the super-peer periodically. When the super-peer fails or be offline network the backup peer replaces it and operates as a super-peer. The possibility of both a super-peer and its backup peer failing at the same time is much smaller than failure of super-peer alone. Therefore, the introduction of the backup super peer improves the architecture's robustness greatly.

2.4. P2P Based on SIP in the IMS

To apply the hybrid architecture in the IMS, it is natural to implement the SP as an SIP application server (SP-AS) which hosts and executes services. SP-AS interfaces with the S-CSCF (Serving Call/Session Control Function) using SIP in the ISC (IMS Service Control) interface, as shown in **Figure 1**. The ISC interface is between the Serving CSCF and the service platforms. The SP-AS uses the ISC interface to communicate with the S-CSCF. The S-CSCF is connected to a P-CSCF (Proxy Call/Session Control Function) through the Mw interface. The Mw reference point allows the communication and forwarding of signaling messaging between CSCFs, e.g. during registration and session control [8]. The S-CSCF and PCSCF are SIP proxies with IMS functionality. The SCSCF is the central node in the signaling plane and the P-CSCF is the inbound/outbound SIP proxy between the terminal and the IMS network [9].

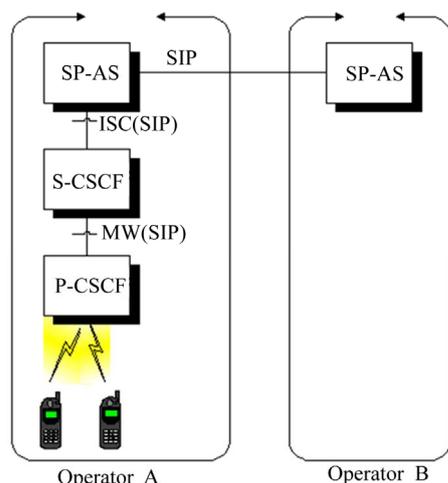


Figure 1. Interfaces and elements of P2P in IMS.

The SP-AS server has three main functions: content management, cache management and membership services. The SP-AS server maintains the directory of meta-information. When he/she registers to the network, the client sends the initial list of content for sharing as well as further updates as the content changes to the SPAS. When a client requests resources, the SP-AS consults its lookup tables and replies back with matching contents. It as well forwards the requests to other SP-AS.

SIP provides an established method for routing the P2P connection to the end peer utilizing a set of proxy servers. The INVITE message performing this function carries the P2P control message in SDP (Session Description Protocol) format. The SDP describes the streams used for communication and allows the end peers to agree on the session parameter.

3. Security Enhancement to the Framework

3.1. Security Requirements for MP2P Business

The MP2P framework proposed above provides a high-performance content sharing model, and is the carrier of P2P traffic, but it will not work without meeting security requirements for MP2P business. From business perspective, security requirements come from two aspects: the network operator and terminal users, although there is some overlap between them. These requirements include:

- Identity authentication and non-repudiation: verifies that the data or request came from and goes to a specific, valid user. From network operator perspective, this is to ensure that only subscribed users can get the service, and bills are charged to correct users. From end user perspective, this is to ensure communicating with the correct peer.
- Data confidentiality: keeps data secret to outsiders.

Only the destination user can get the data, and not anybody else; even an outsider gets it, he/she cannot get the meaning of the data. From the network operator perspective, this is to prevent free access to content, and encourage more traffic. From the end user perspective, this is to prevent eavesdropping and protect their privacy.

- Data integrity: prevents data from being altered.
- Data freshness: keeps data in correct order and up-to-date.
- Data availability: data should be available on request.

With P2P-over-SIP architecture, the operator can identify and control the transferred contents. As a SIP signaling message passes through the SP, the content type, content name and potentially some other information can be extracted. This allows the operator to deny access to illegitimate contents and have group management.

Cellular networks have already provided security from Mobile Switching Centre (MSC) to base stations, and base station to handsets. GSM network access security uses A3/A8 (COMP128 actually used in GPRS) authentication algorithm and A5 encryption algorithm, which have already been broken [10,11]. 3GPP has developed proprietary cryptographic algorithms—the MILENAGE algorithm set and KASUMI cryptographic core to replace the broken ones in GSM. However, much of the work with the UMTS access architecture has been focused on backward compatibility with GSM/GPRS [12]. From a security point of view, backward compatibility with a system with weaker security is undesirable but dictated by commercial reality.

On the other hand, as for end-to-end security between two cellular terminals, current 3G networks do not provide any mechanism. In Internet world, the traffic can be protected by using Public Key Infrastructure (PKI). It is not feasible in cellular networks, especially for handsets. First, there is no such infrastructure in cellular networks. Second, PKI is too heavy weight for cellular handsets.

In light of the above reasons, we propose to employ identity-base cryptography (IBC) in this framework. Such a scheme has the property that a user's public key is an easily calculated function of his identity, while a user's private key can be calculated for him by a trusted authority, called Private Key Generator (PKG). The identity-based public key cryptosystem can be an alternative for certificate-based PKI, especially when efficient key management and moderate security are required.

Compared to PKI, it has the following advantages in cellular networks:

- Lightweight: PKI is implemented in RSA, and IBC is implemented in Elliptic Curve Cryptography (ECC).

For a security level of 2048-bit RSA, ECC outperforms in every aspect; for a security level of 1024-bit RSA, ECC outperforms in scenarios such as in mobile cellular networks [13]. This saves storage and computational resources of the handsets.

- Easy to deploy: In PKI, the Public Key Certificate (PKC) of a user need be signed by the Certificate Authority (CA) before being distributed to other users, and a user need to store all PKC's of all other users he/she wants to communicate. In IBC, the public key is implicit in the communication traffic, and there is no need to have it signed, distributed and stored. This saves communication and storage resources of the network and handsets.

3.2. Basic System Setup

Our security scheme is based on Boneh's implementation of IBC [14]. The scheme needs a setup phase in which system parameters are distributed to its users. These parameters include system public key, master key, private key of each user, and algorithms to be used for hashing/encryption/decryption.

The operator chooses a Bilinear Map denoted as $\hat{e}: G_1 \times G_1 \rightarrow G_2$ between two cyclic groups G_1, G_2 of order q for some large prime q , where G_1 is the group of points of an elliptic curve over F_p and G_2 is a subgroup of $F_{p^2}^*$. At system setup phase, the operator sets the system public key P_{pub} as sP where s is a random number in Z_q^* , and P is an arbitrary point in E/F_p of order q . It also chooses a cryptographic hash function $G: \{0,1\}^* \rightarrow F_p$ to map variable identity strings to points in E/F_p , and chooses hash functions $H1: F_{p^2}^* \rightarrow \{0,1\}^n$, $H2: F_{p^2}^* \rightarrow Z_q$, $H3: \{0,1\}^n \times \{0,1\}^n \rightarrow F_p$, and $H4: \{0,1\}^n \rightarrow \{0,1\}^m$ for keys of specified length.

The initial master key $s \in Z_q$ and the system parameters $\langle p, n, P, P_{pub}, G, H1, H2, H3, H4 \rangle$ are determined and calculated by the operator. The network operator assigns a short code to each super peer in the network and publishes the numbers. For a MP2P subscriber, the operator uses the MSISDN as the unique identity and hence public key. For each $ID \in \{0,1\}^*$, the cryptographic scheme builds an initial private key dID as $dID = sQID$ where QID is a point in E/F_p mapped from ID . Every user gets the system parameters and its private key from the operator when he/she subscribes the MP2P service.

3.3. Secured P2P Communication

The P2P applications installed on cellular terminals take care of secure communication between two terminals and

between a terminals and a SP. When node A wants to send a message to node B , either a SP or a regular peer node, the application encrypts and authenticates the message as follows:

1) A first generates an implicit shared key with B , without any interaction with B : $k = H1(g^r)$, where $g = \hat{e}(dA, QB)$, $r = H2[\hat{e}(QA, QB)]$, $QA = G(IDA)$, $QB = G(IDB)$, $dA = sQA$. IDB is the MSISDN or short code of the receiver to whom the sender intends to send the message.

2) A encrypts the message M , and outputs the cipher text $C = EH4(k)(M)$, where Ek is a secure symmetric cryptosystem encryption function.

3) A signs the message with its own private key and the receiver's public key using a message authentication code (MAC) function, named $H3$ here, the authentication code $\sigma = H3(C, k)$ is determined by the message to be sent and the private key of the originator, and serves as a signature to the message signed by the node. The encrypted message C and signature σ are put into the payload field of the packet, $M' = \langle C, \sigma \rangle$.

At the receiver B side, the message is verified and decrypted as follows:

1) B first generates the implicit shared key with A , without any interaction with A : $k = H1(g^r)$, where $g = \hat{e}(QA, dB)$. Note that IDA is the MSISDN of sender derived from the packet header and $\hat{e}(QA, dB) = \hat{e}(dA, QB)$.

2) For a received message $M' = \langle C, \sigma \rangle$ in the defined format with signature σ and cipher text C , the signature is re-calculated: $\sigma' = H3(C, k)$ and verified against the one in the received message. If they match, the message is processed further. Otherwise, the message is discarded.

3) For the received message, B decrypts it with the shared key: $M'' = DH4(k)(C)$, where Dk is a secure symmetric cryptosystem decryption function. M'' should be the same as the original message M .

One weakness of this scheme is key escrow [15], i.e. the network operator knows the encryption key between A and B . To transfer content that A and B want to keep secret from the operator, the following extra steps can be executed for calculating a shared session key between A and B after they get a pairwise secret key:

$KAB = \hat{e}(dA, QB) = \hat{e}(QA, dB) = KBA$. KAB is then divided into two parts Ke and Ka . Encryption under Ke prevents all other networks nodes from reading the messages, whereas Ka is used in a message authentication code to enable mutual authentication. Then, $A \rightarrow B: A, EKe(K1)$, $B \rightarrow A: B, EKe(K2)$, $MACKa(A, EKe(K1), EKe(K2))$, $A \rightarrow B: MACKa(B, EKe(K2), EKe(K1))$. A shared session key can be set up as $Kses = f(K1, K2)$ [16]. This key provides forward security and prevents the

operator from being a key escrow.

3.4. Group Generation and Communication

The MP2P architecture supports fixed group and ad-hoc group for peers to share data by broadcasting to group members. The security scheme generates group key for each fixed group and ad-hoc group.

Each fixed group is formed by the network operator, and includes one super peer and any number of regular peers. The group broadcasting key is chosen by the super peer, and can be generated from a random number. One regular peer can join a super peer's group by sending a request message and get a reply message, including the group key, from the super peer. These messages are encrypted and signed using the scheme introduced in Section 3.3. After that, the super peer can announce information by broadcasting to its subscribers. The information can include the updates in its content table, client table, caching table, and membership table.

Regular peers can generate ad-hoc groups by themselves, and exchange data that are protected to outsiders using a group-wide secret key. The secret key is generated in this way:

1) Node 1 computes its broadcast parameter that is unique for node 1: $K1N = \hat{e}(sQid1, Qid2 + Qid3 + \dots + Qidn) = \hat{e}(sQid1, Qid2) \cdot \hat{e}(sQid1, Qid3) \dots \hat{e}(sQid1, Qidn)$ and distribute $P1-brdcst = K1N \cdot P$ to all candidate nodes using respective pairwise encryption.

2) Node 1 use $P1-brdcst$ to encrypt a message sent to the group, and sign a message as

$M : \langle U, V \rangle = \langle rQ_{id1}, K_{1N}^{-1}(r+h)Q_{id1} \rangle$ where r is a random number and h is a hash of the original message.

Other group members decrypt the message with $P1-brdcst$, and verify if $\hat{e}(P1-brdcst, V) = \hat{e}(P, U + hQid1)$ holds.

4. Discussion

4.1. Performance Analysis

From previous sections, we know that the search efficiency depends on the search in different SP. The efficiency of caching policy will be analyzed in the following section. Suppose all of the SPs form a graph in which all nodes have the same degree D . And there is up to N_f different files for sharing being cached in n number of N SPs, with N_i files in each SP. Each SP reserves the cache memory space for at most number of K files. Maximum searching steps, which limits the searching steps, are $n = \log D \{(D-1)Ni+1\} - 1$. Let s be the possible number of steps used to search the target.

And we assume searching steps and file location are evenly distributed in the content table and caching table.

The analysis falls into the following three categories,

- $N \times K = N_f$ and without search loops:

Assume that there are no duplicate contents in both the content table and the caching table. When no repeat content and search loop exists, the probability for hitting the target is,

$$\begin{aligned} P_{hit} &= P(hit|s=0)P(s=0) + \dots \\ &\quad + P(hit|s=n)P(s=n) \\ &= \frac{1}{n+1} \left\{ \frac{K}{N_f} + \left(1 - \frac{K}{N_f}\right) \left(\frac{K}{N_f - K}\right) \frac{K}{N_f - 2K} + \dots \right. \\ &\quad \left. + \prod_{i=0}^{n-1} \left(1 - \frac{K}{N_f - iK}\right) \frac{K}{N_f - nK} \right\} \\ &= \frac{1}{n+1} \sum_{i=0}^n \left(1 - \frac{K}{N_f - jK}\right) \frac{K}{N_f - iK} \end{aligned}$$

- $N \times K > N_f$ and without search loops:

At a certain time point, there are totally $N \times K$ files in SPs and N_f is fixed. If $N_f < N \times K$, the overlap of contents occur between the content table and caching table. The repeat probability is defined as follows $Pr(n)$ the probability for a certain cached file in the SP checked in n th steps to be the same as some file in the SP checked before, that is, in the SP checked in $0th, 1th, \dots, (n-1)th$ steps.

$$P_r(0) = 0;$$

$$P_r(1) = 1 - \frac{\binom{N_f - K}{K}}{\binom{N_f}{K}}$$

$$P_r(2) = 1 - \frac{\binom{N_f - K - K(1 - P_r(1))}{K}}{\binom{N_f}{K}};$$

...

$$P_r(n) = 1 - \frac{\binom{N_f - \sum_{i=0}^{n-1} K(1 - P_r(i))}{K}}{\binom{N_f}{K}};$$

Therefore the hitting probability is,

$$\begin{aligned}
 P_{hit} &= \frac{1}{n+1} \left\{ \frac{K}{N_f} + \left(1 - \frac{K}{N_f} \right) \frac{K(1-P_r(1))}{N_f - K} \right. \\
 &+ \left(1 - \frac{K}{N_f} \right) \left(1 - \frac{K(1-P_r(1))}{N_f - K} \right) \frac{K(1-P_r(2))}{N_f - K - K(1-P_r(1))} + \dots \\
 &\left. + \prod_{j=0}^{n-1} \left(1 - \frac{K(1-P_r(j))}{N_f - \sum_{k=0}^{j-1} K(1-P_r(k))} \right) \frac{K(1-P_r(n))}{N_f - \sum_{m=0}^{n-1} K(1-P_r(m))} \right\} \\
 &= \frac{1}{n+1} \\
 &\cdot \sum_{i=0}^n \prod_{j=0}^{n-1} \left(1 - \frac{K(1-P_r(j))}{N_f - \sum_{k=0}^{j-1} K(1-P_r(k))} \right) \frac{K(1-P_r(i))}{N_f - \sum_{m=0}^{i-1} K(1-P_r(m))}
 \end{aligned}$$

• **With search loops:**

Now we consider the condition that loops are possible. If the search process hits the target in n steps, then the maximum number of the checked SPs is n , and the maximum number of steps that can be wasted due to loops is $n - 2$. The wasted step means that one SP that has already been checked is checked for a second time. Suppose the number of possible loop is evenly distributed.

Let $Pl(a|b)$ denotes the probability for hitting target in a steps along with b steps wasted because of loops, then, $Pl(a|b) = Pl(A = a|B = b) = Pl(A1 = a|B1 = b) + Pl(A2 = a|B2 = b) + \dots$. Denote the probability for hitting the target in n th steps by S_n , then,

$$\begin{aligned}
 S_0 &= P_t(0|0); \\
 S_1 &= P_t(1|0); \\
 S_2 &= P_t(2|0); \\
 S_3 &= P_t(3|0) \cdot \frac{1}{2} + P_t(3|1) \cdot \frac{1}{2} = \frac{1}{2} (P_t(3|0) + P_t(2|0)) \\
 S_n &= \frac{1}{n-1} \sum_{i=2}^n P_t(i|0).
 \end{aligned}$$

Then the hitting probability is as follows,

$$P_{hit} = \frac{1}{n+1} \left\{ P_t(1|0) + P_t(2|0) + \sum_{i=3}^n \frac{1}{i-1} \sum_{j=2}^i P_t(j|0) \right\}$$

where $P_t(j|0)$

$$= \prod_{i=0}^{j-1} \left(1 - \frac{K(1-P_t(i))}{N_f - \sum_{m=0}^{i-1} K(1-P_t(m))} \right) \frac{K(1-P_t(j))}{N_f - \sum_{i=0}^{n-1} K(1-P_t(i))}.$$

From **Figures 2 and 3**, the advantages of the proposed

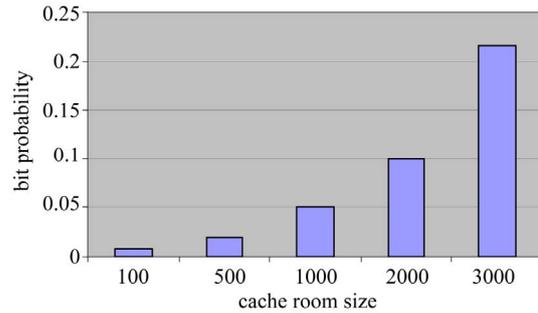


Figure 2. File number is 10000, $n = 3$, file caching room is in the range of 100 to 2000, connectivity degree = 10. File repeat probability is 0.

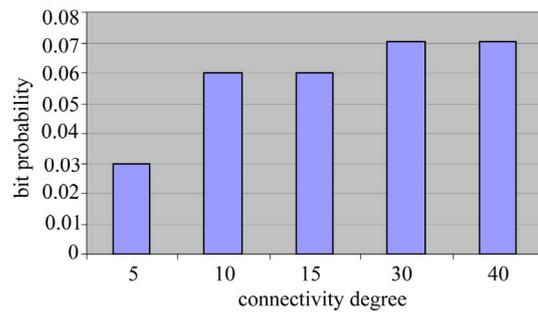


Figure 3. File number is 10000, $n = 2$ to 3, file caching room is 1000, connectivity degree = 5 to 40. File repeat probability is 0.

architecture when evaluating hit probability are clear. The hit probability is improved significantly as the cache room and connectivity degree rises. Our results reasonably show some trends for parameters changes.

4.2. Business Security Analysis

The security enhancement provides integrity, authentication, and confidentiality to MP2P messages by binding a message with a private key possessed only by the cellular terminal. It effectively prevents the following attacks previously available in cellular networks:

- **Identity Impersonation:** In cellular networks, the possibility exists that an attacker manages to impersonate the service provider or a terminal user. With the proposed security enhancement, the originating address of the sender is bound to the private key of the sender. The attacker, not knowing the private key, cannot forge an arbitrary address. This ensures correctness of delivered service and billing.
- **Message Forgery and Tampering:** Similarly to address forgery, an attacker can also forge or tamper the payload field of a data packet, namely the content of a message, in current cellular networks. With the proposed security enhancement, every message is signed by the sender. The attacker, not knowing the private

key of the sender, cannot tamper the message and generate a correct signature. It's easy to verify the integrity of the message.

- Eavesdropping: As was stated earlier, there are many possibilities an attacker can get access to messages transmitted through current cellular networks. The attacker can intercept the messages from the Internet or over the air, and easily get interesting information, since there is no strong protection to them. With the proposed security enhancement, every message is encrypted, and only the sender and receiver know the decryption key. Any attacker will need a great deal of effort if he wants to crack the encryption.

With these features, a MP2P service can be securely deployed; security requirements from both the network operator side and terminal user side can be well satisfied. A business model based on this framework is thus feasible, profitable, and also promising.

5. Conclusions

In this paper, we propose a framework for implementing P2P as a SIP-based service in cellular networks, in particular in IMS. The framework is based on MP2P hybrid architecture. We show several benefits of this framework by mathematical analysis and simulation. The framework also includes a security enhancement, with which the operators can have control on security and group management, and chargeability is possible. The enhancement is lightweight and convenient to deploy in cellular networks environment by using identity-based cryptography. Business model using this MP2P framework with security enhancement can be easily and successfully setup, which is one of our future works.

6. References

- [1] N. B. Azzouna and F. Guillemin, "Experimental Analysis of the Impact of Peer-to-Peer Applications on Traffic in Commercial IP Networks," *European Transactions on Telecommunications*, Special Issue on P2P Networking and P2P Services, Vol. 15, No. 6, November-December 2004, pp. 511-522.
- [2] T. Karagiannis, A. Broido, N. Brownlee, K. C. Claffy and M. Faloutsos, "Is P2P Dying or Just Hiding?" *Proceedings of IEEE Global Telecommunications Conference*, Dallas, Vol. 3, 29 November-3 December 2004, pp. 1532-1538.
- [3] K. Singh and H. Schulzrinne, "Peer-to-Peer Internet Telephony using SIP," Columbia University Technical Report, CUCS-044-04, New York, October 2004.
- [4] J. Yang, Y. P. Zhong and S. Y. Zhang, "An Efficient Interest-Group Based Search Mechanism in Unstructured Peer-to-Peer Networks," *Proceedings of the International Conference on Computer Networks and Mobile Computing*, Shanghai, 20-23 October 2003, pp. 247-252.
- [5] H. C. Hsiao and C. T. King, "Bristle: A Mobile Structured Peer-to-Peer Architecture," *Proceeding of International Parallel and Distributed Processing Symposium*, Nice, 22-26 April 2003, pp. 33-40.
- [6] H.-T. Hu, B. Thai and A. Seneviratne, "Supporting Mobile Devices in Gnutella File Sharing Network with Mobile Agents," *Proceedings of the 8th IEEE International Symposium on Computers and Communications*, Kemer-Antalya, 28 June-1 July 2004, pp. 25-30.
- [7] S. Liu, W. Jiang and J. Li, "Architecture and Performance Evaluation for P2P Application in 3G Mobile Cellular Systems," *Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing*, Shanghai, 21-25 September 2007, pp. 914-917. [doi:10.1109/WICOM.2007.235](https://doi.org/10.1109/WICOM.2007.235)
- [8] 3GPP TS 23.002 v5.12.0 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects Network architecture (Release 5). September 2003.
- [9] G. Camarillo and M. A. Garcia Martin, "The 3G IP Multimedia Subsystem," John Wiley & Sons, Hoboken, ISBN 0470 871563, 2004.
- [10] D. Wagner, "GSM Cloning," June 2010 <http://www.isaac.cs.berkeley.edu/isaac/gsm.html>
- [11] A. Biryukov, A. Shamir and D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC," *Proceedings of the 7th International Workshop on Fast Software Encryption*, 2000, pp. 1-18.
- [12] G. Koenig, "An Introduction to Access Security in UMTS," *IEEE Wireless Communications*, Vol. 11, No. 1, 2004, pp. 8-18. [doi:10.1109/MWC.2004.1269712](https://doi.org/10.1109/MWC.2004.1269712)
- [13] V. Gupta, S. Gupta, S. Chang and D. Stebila, "Performance Analysis of Elliptic Curve Cryptography for SSL," *Proceedings of the ACM Workshop on Wireless Security*, Atlanta, September 2002, pp. 87-94.
- [14] D. Boneh and M. Franklin, "Identity-Based Encryption From The Weil Pairing," *Proceedings of Cryptology, Lecture Notes in Computer Science*, Vol. 2139, Springer, 2001, pp. 213-219.
- [15] S. Zhao, A. Aggarwal and S. Liu, "Building Secure User-to-User Messaging in Mobile Telecommunication Networks," *Proceedings of Wireless Telecommunications Symposium*, Pomona, 24-26 April 2008, pp. 151-157. [doi:10.1109/WTS.2008.4547559](https://doi.org/10.1109/WTS.2008.4547559)
- [16] K. Hoepfer and G. Gong "Preventing or Utilising Key Escrow in Identity-Based Schemes Employed in Mobile Ad Hoc Networks," *International Journal of Security and Networks*, Vol. 2, No. 3/4, 2007, pp. 239-250.