SIP Protocol with Group Management Model and Security

Ben-Bin Chen Dong-Hui Guo

Department of Electronic Engineering, Xiamen University
Xiamen, Fujian 361005, China
chenbenbin@163.com, dhguo@xmu.edu.cn

Received 29 November 2013; Revised 15 February 2014; Accepted 29 April 2014

Abstract. An innovative application for communication platform called PPTalk based on SIP protocol is presented in this paper. In this application, a group management model (GMM) is proposed for SIP with grouping functions, in which a new encryption mechanism that combines AES and RSA algorithm is included in this model to ensure the security of SIP-based instant message (IM) and the Internet protocol (IP)-based multimedia subsystem (IMS) communication. Different from the traditional applications based on SIP that do not focus on the security and don't very emphasize the deployment of application services, the proposed architecture of this new platform requires a data service node to store the configuration list of the group management and the public key of RSA that can provide the highly competitive solution to integrate various application services such as documents sharing with packet segmentation strategy (PSS) and security to make it more convenient and extensive for use. Finally, this communication platform of PPTalk is implemented with a user agent (UA), a SIP server (option), and a data service node, which constitute an effective deployment of PPTalk platform. The experiment with the platform shows that, PPTalk is able to work with low bandwidth and provides high quality and could be widely utilized in enterprises, groups and organizations with group management and security.

Keywords: SIP, GMM, security, UA, PPTalk

1 Introduction

The Session Initial Protocol (SIP) [1] defined by IETF (The Internet Engineering Task Force) [2] has got support from several companies and becomes the chief signaling protocol of VoIP (Voice over Internet Protocol) because of its simplicity, flexibility and scalability. The extended applications based on SIP, such as Instant Message (IM), VoIP [3], [4] and Net Meeting System, have been proposed one after another. To alleviate the deficiency of SIP in C/S architecture, the Pear-to-Pear (P2P) technology has been adopted [5], [6], [7], [22], [23]. There are also many studies and policies to traverse the NAT and firewall (FW) in SIP application [3], [8], [9].

Compared to traditional PSTN (Public Switched Telephone Network) phone, whose features, services, and innovation have spread very slowly [13], SIP is an example of an open standard over the Internet where new applications and services are immediately available worldwide to anyone with Internet connectivity. As the core technology and service of NGN (Next Generation Network) form [18], VoIP has gone beyond the traditional PSTN phone to become the main form of voice services. Fig. 1 shows the market analysis [10] of research consulting, which reveals the great business development potential of VoIP in USA. So, based on the SIP VoIP system is becoming a hot spot of current research in this area.

Nevertheless, SIP message is an open standard protocol which could be easy acquired by normal tool Ethereal [14], [19], The traditional encryption of SIP signaling uses HTTP digest authentication protocol, the security has been confirmed is not safe and reliable [15]. Till now there is a lack of the highly competitive solution to integrate the group management model with security to make it more convenient and extensive for use with SIP. In this paper, we integrated the voice, video and instant messaging services in one platform by using the research results in these respects. During these researches we find that, compared to other communication tools such as Skype, the group management is not emphasized in SIP application. The paper [20] extends the SIP protocol to reduce the load on registration but do not present the effective group based model for SIP. So in this paper a group management model is designed to fill this gap. In this group management model, quickly structuring and building their own communication platform with low expense is considered for the enterprises and organizations. Actually, considering the decrease of work, study efficiency and security by using the common IM tool, enterprises and organizations are eager to have their own communication platform, but with low-cost and security. This paper intends to build such a platform including user agent and simple services. Team or department (group) concept can be fast and easy to be applied to suit to the business operation and management. Information security is another important part of common network application. Based on the above group management model, this paper also presents a new mechanism that combines AES (Advanced Encryption Standard) and RSA encryption algorithm to provide the security of SIP messages and documents sharing with PSS. In addition, for widening the fields of its application, a methodology for NAT/FW traversal by using ICE (Interactive Connectivity Establishment) and HTTP tunnel [9] is applied, which enhances the adaptability of the platform in different application environment, but is not expressed in this paper.

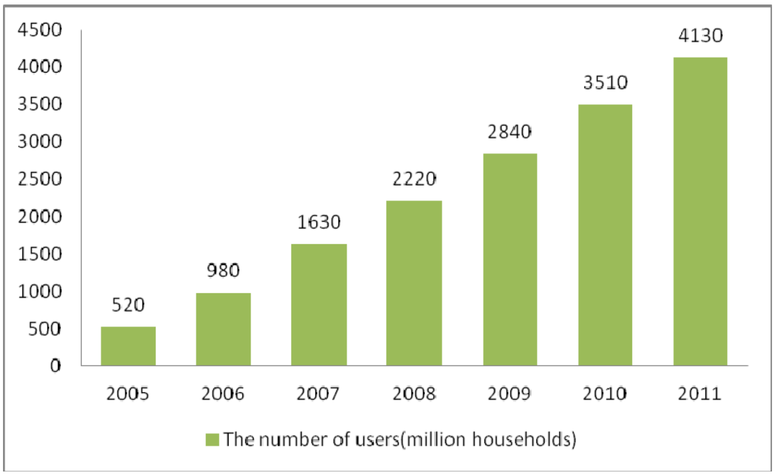


Fig. 1. Business development potential of VoIP

On this platform of PPTalk, firstly the deployment entities such as enterprises should either have their own network to access the wide area network (WAN) for getting the open SIP services of Internet, or set up an internal SIP server. And then a simple service node is needed to provide the storage of group management data, public-key of RSA and others user information. If they can't access the WAN, the data service node can be used to build a simple SIP server. All the mapping and processing of the information is carried out by the user agent of the platform.

The paper is organized as follows. Section 2 describes the basic theories of SIP protocol, the architecture of the SIP-based PPTalk solution and the network framework of communication platform for enterprise. Section 3 introduces the development of user agent and application platform with group management model, the encryption algorithm and the documents sharing mechanism. In Section 4, the user agent of communication platform is introduced concisely. Eventually, after evaluating the proposed scheme and verifying that the communication platform is effectively used in the LAN in Section 5, the paper concludes in Section 6.

2 Architecture of SIP-Based Solution

SIP is an application layer protocol, provides the transmission of connection-oriented and connectionless-oriented. However, SIP protocol don't define the specific structure of any way of multimedia, so SIP needs to cooperate with other protocols to constitute the system of PPTalk. In this section, we introduce the protocols stack and deployment framework of PPTalk with oSIP which is a general protocols stack of SIP.

2.1 SIP-Baed VoIP

The Session Initiation Protocol is a signaling protocol. It is described as a control protocol for creating, modifying and terminating sessions with one or more participants. These sessions include Internet multimedia conferences, Internet (or any IP Network) telephone calls and multimedia distribution. SIP supports session descriptions that allow participants to agree on a set of compatible media types. It also supports user mobility by redirecting requests to the user's current location.

As a request/response-based protocol standardized by IETF for voice, video or other interactive sessions over the Internet, SIP is based on a client-server model where each SIP entity depending on the context behaves either like a user agent client (UAC) or a user agent server (UAS) [1], [2].

SIP-based VoIP [3], [4] solution mainly consists of three parts: SDP (Session Description Protocol), RTP (Real-Time Transport Protocol), and SIP protocol. SDP [11], [12] is a protocol that defines a text-based format for describing streaming media sessions and multicast transmissions. SDP is not a transport protocol but a method of describing the details of the transmission. RTP [3] is used to encapsulate VoIP data packets inside UDP packets. RTP is defined in RFC 3550 - RTP: A Transport Protocol for Real-Time Applications [12]. SIP gets streaming media session information using current SDP and is compatible with RTP for VoIP communication. The architecture of a typical SIP-based VoIP stack is displayed in Fig. 2. SIP needs to cooperate with other protocols to constitute the system. PPTalk system is based on the oSIP which is the next generation SIP and has good performance as general protocols stack to build the communication platform with group management model and security.

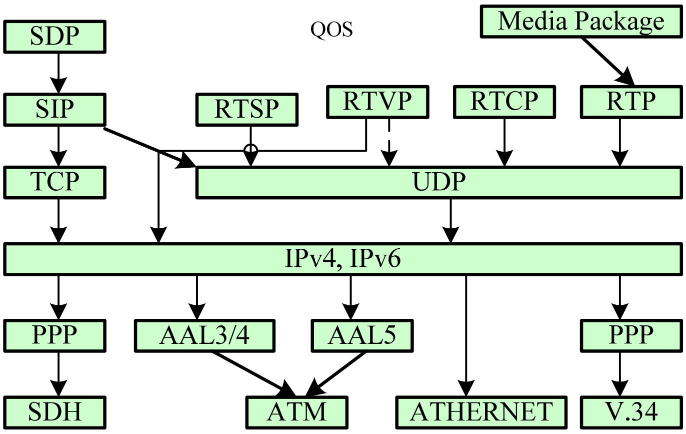


Fig. 2. Protocol stack of SIP-based VoIP system

The main job of media processing layer is SIP signaling scheduling, SDP session and media negotiation, RTP/RTPC AV (audio/video) business processing, RTSP/MMS streaming multicast business and so on [16]. oSIP as the control role for the processing of other protocols operation is composed of three parts: parser module, finite state machines and tool module showed in the Fig. 3.The mainly work of the parser module is to complete the analysis of SIP signals, the SDP negotiations and URL location. With the receiving text, parser module parses the SIP message into a SIP message structure or parses the SIP message structure back into SIP text message. The finite state machines module completes records on a transaction status, and triggers the corresponding events in a particular state. oSIP finite state machines is divided into four categories, respectively ICT (Invite Client Transaction, outgoing), NICT (Non-Invite Client Transaction, outgoing), IST (Invite Server Transaction, incoming), NIST(Non-Invite Server Transaction, incoming). Tool module consists of a dialogue tool and SDP consultation tools. Dialogue tool can help record request and response message that can help the terminal make responses quickly and accurately. Negotiate tools are used to provide the codec negotiation.

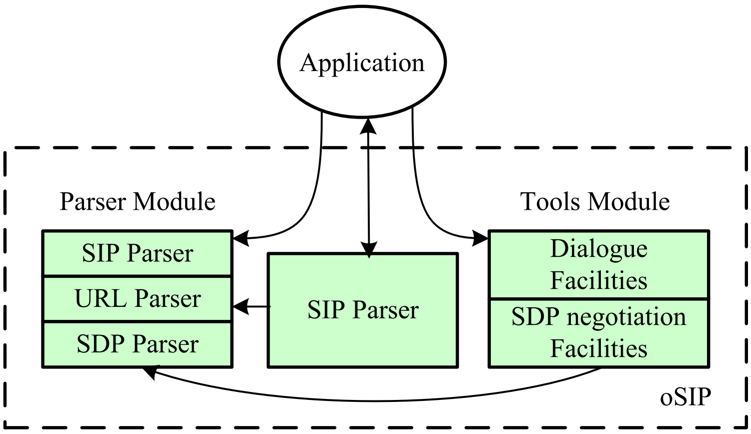


Fig. 3. The structure of oSIP

2.2 Architecture of the PPTalk

As shown in Fig. 4, the framework of SIP-based network of PPTalk could be structured with SIP network services and company existing network. The SIP services, which can be connected to PSTN by gateway, are consisted of location service, redirect service, registrar service, proxy services and option data server with common data and private data named by user ID which is very convenient to extend the application of PPTalk with security such as group management and the using of AES&RSA based on special user ID. The option data server and location server could be combined as one server. In particular, all of the services can be integrated on a server, as long as its performance can meet the requirements. The option data service node in the location server of SIP network services is the same as the data service node of the enterprise local network which can be used when the entities don't have their own SIP services but only use the common SIP server resources. This could help the entities to not only save resources, but also enjoy the PPTalk service with their own existing network. The enterprise entities network includes the user agents and a simple data service node which can be also used as a user agent. In this framework of communication platform, the hardware of the SIP network services and the enterprise network exist. The differences are the data service node with configuration list, the logic mapping for GMM and the change of user agent. If the access to Internet is forbidden, then it is needed to use the data service node to build an internal SIP server with data service to complete the functions of SIP Network Services.

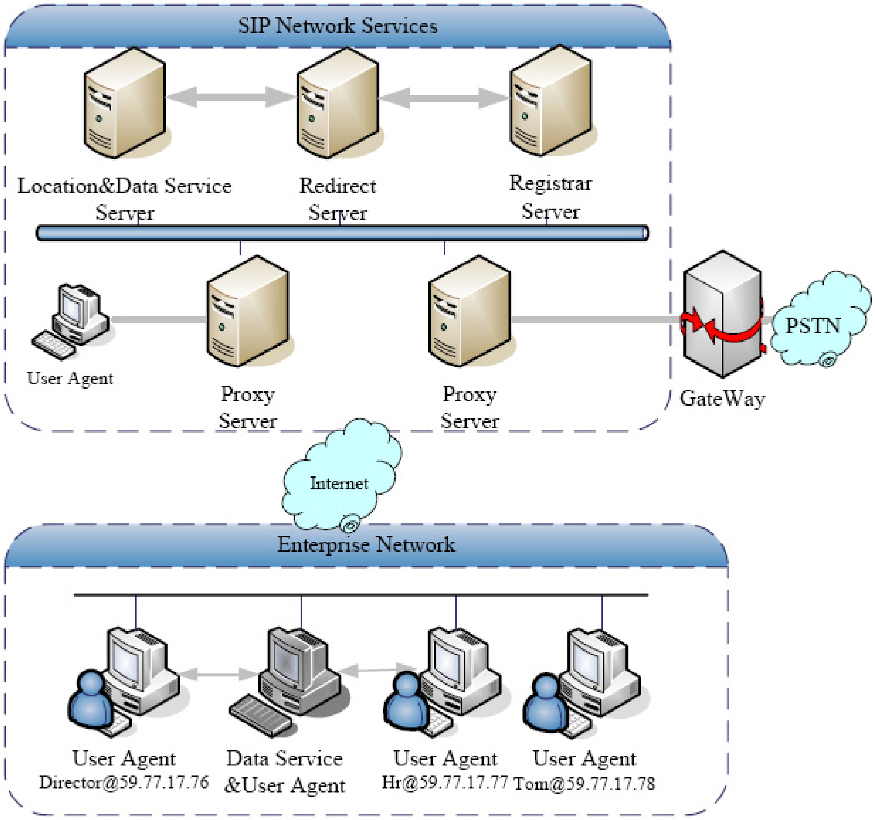


Fig. 4. Network framework of SIP-based PPTalk

After finishing the user agent with GMM model and the encryption algorithm, which are the important parts of the PPTalk communication platform (introduced in Section 3), a SIP internal server with the SIP software services is also built. It is very important for entities to select the appropriate solution to deploy their communication platform, whether with internal SIP server or not.

3 Innovative design of PPTalk

Due to the low coupling loose structure and the simplicity, flexibility and scalability of the SIP, the solution of the PPTalk communication platform mentioned in Section 2 can be enhanced with value added services like GMM with secure IM and document sharing with PSS presented in this paper. To indicate the details of innovative application, this paper below will introduce the detailed information.

Firstly, the framework of the application with UAC and user data services will be presented in Fig. 5, which is the important part of the framework of PPTalk communication application platform based on SIP protocol. And then, we extend the protocol stack of SIP-based VoIP system up and down SIP protocol layer with group management and encryption system application. The innovation parts of application are marked in yellow, which mainly contain the GMM model with the combination encryption algorithm of AES and RSA, the extended SIP signals such as user states signal including online, offline, busy, free, away and so on, and the documents sharing with PSS and the user data service node, which stores the common data including public key of RSA. The ICE and HTTP tunnel is also including in UAC but is not presented in detail.

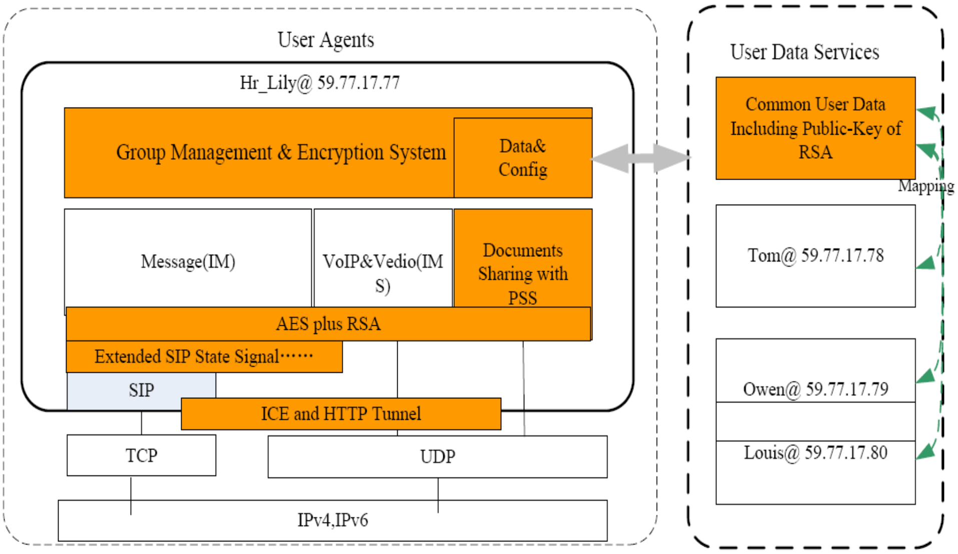


Fig. 5. Innovative parts of PPTalk UAC and user data services

The UA such as Hr_Lily@59.77.17.77 creates the private and common data and syncs the common data including user ID and public key of RSA to the data services node. The data services node maintains the common unified user data and keeps mapping with the private data of user including the group information that is created by users.

3.1 Group Management Model.

PPTalk GMM presents the data service concept with user's common and private data. User ID in UA and data service node are used to distinguish users and services between different users and different services. User ID in this GMM is very important to expand the applications with different division of user such as IM group communication module, IMS group communication module, the encryption system and document sharing mechanism module. The concept of enterprise is emphasized in the GMM. Only human resources (HR) of company can add new employee (user) to the configuration list and divide the list to different departments. All users can create their own communication groups by data interaction with data service node (shown in Fig. 5 and Fig. 6). In order to be compatible with enterprise's existing programs, the mapping from external data of SIP services to internal information of enterprise has been considered.

Data service node contains the common data and private data with the folders named by user ID. Data interaction between UA and data service node can be FTP, socket or database techniques. FTP technique is adopted by this platform. To reduce the management complexity of data service node of the communication platform, we define the principles of GMM as below.

- The unified configuration file with user information of enterprise is both in data service node and UA. Thus, the server maintains a unified friends list in common data.
- Each user maintains its own group list and keeps it sync with the data service node as the private data.
- UA keeps the logic to synchronize with data service node. The unified common data (friends list) strictly maps with the private data to ensure the conformity of users.

3.2 Security Policy of SIP

Since the GMM and carried out the UAC and the data service node have been presented, the PPTalk communication's security is another important issue for application in enterprise. This paper proposes a combination encryption algorithm of AES&RSA which provides the security of SIP messages and others communication, based on the above GMM model. The encryption algorithm is described as follows.

- Use AES symmetric encryption for SIP body.
- AES key needs to be randomly generated and kept it in SIP message.
- Take advantage of RSA to encrypt the AES key with message receiver's public key of RSA (user's RSA public key).
- Each user maintains its own RSA public key and the RSA private key.
- Use the user private key of RSA stored in local user agent to decrypt the AES key in the message.
- Decrypt the SIP body with AES symmetric secret key.

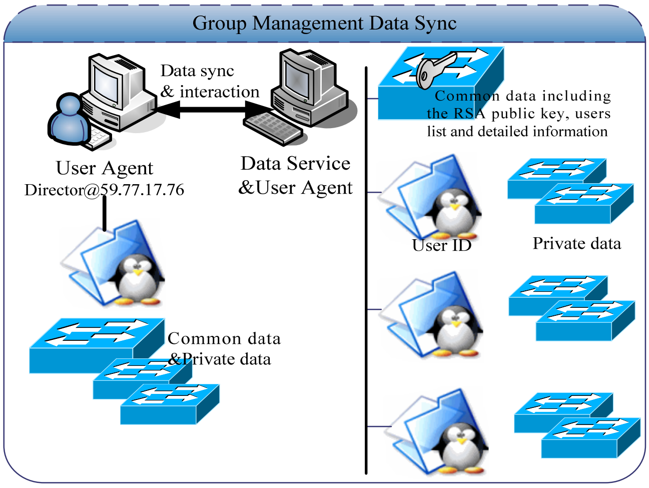

Group Management Data Sync
Data sync & interaction
User Agent
Director@59.77.17.76
Data Service &User Agent
Common data including the RSA public key, users list and detailed information
User ID
Private data
Common data &Private data

Fig. 6. Group management data sync

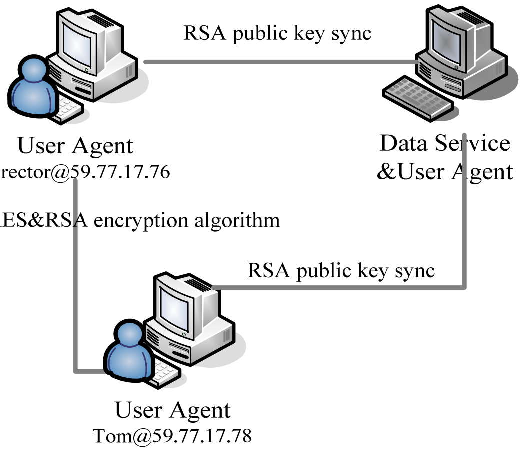


Fig. 7. AES&RSA encryption algorithm

From the encryption algorithm, the messages between two user agents are encrypted by AES&RSA algorithm and the RSA public key can be stored in the common data of data service node and be kept sync with the user agent's update (shown in Fig. 7). Because the configuration list of GMM is stored in data service node as common data and kept sync with UA, this process will be carried out easily after the completion of GMM. The encryption and decryption process are listed below.

1) Encryption process of RSA.

For plain text m ($m < n$), take

$c \equiv m^e \pmod{n}$. c is the cipher text of m.

2) Decryption process of RSA.

Take $m \equiv c^d$ (mod n). m is the plain text of original message.

The public key (n, e) consists of the modulus n and the public (or encryption) exponent e. The private key (n, d) consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of times using the private key. The numbers n, d and e need satisfy the following process.

1) Choose two distinct prime numbers p and q.

2) Compute $n = pq$. $\varphi(n) = (p - 1)(q - 1)$.

3) Choose an integer e such that $1 < e < \varphi(n)$ and $gcd(e, \varphi(n)) = 1$; i.e. e and $\varphi(n)$ are coprime.

4) Determine $de \equiv 1$ (mod $\varphi(n)$), i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).

It has been more than 20 years of time since the RSA algorithm was put forward and it is widely used in the security and the security has been proved to be reliable [17]. In this paper, we combine the RSA and AES to ensure the PPTalk system security for communication.

3.3 A mechanism of sharing the documents

Online documentation can effectively realize the sharing of resources among the participants, improve the interoperability of PPTalk communication system. There are many kinds of document sharing mechanism, the commonly used ones are FTP in C/S model, HTTP download model and TELNET remote access model. The core of documents sharing mechanism is to establish reasonable, fast and convenient download channel among the sharing sides. So we adopt the FTP strategy, which is also mentioned in Section 3.1 as data interaction between UA and data service node, with GMM and MD5 (Message Digest Algorithm 5) [24] verification mechanism to provide the support of breakpoint transmission. The support of breakpoint transmission mechanism is very important for document sharing on the Internet because of the jitter of the network.

MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128 bits (16 bytes) hash value, typically expressed as a 32 digit hexadecimal number. Input information is divided groups by 512 bits. The main loop of algorithm for each group is 4 cycles. The functions (1)-(4) of four cycles loop are briefly listed as below.

$$F(B, C, D) = (B \wedge C) \vee (\neg B \wedge D) \tag{1}$$

$$G(B, C, D) = (B \wedge D) \vee (C \wedge \neg D) \tag{2}$$

$$H(B, C, D) = B \oplus C \oplus D \tag{3}$$

$$I(B, C, D) = C \oplus (B \oplus \neg D) \tag{4}$$

where $\oplus$, $\wedge$, $\vee$, $\neg$ denote the *XOR*, *AND*, *OR* and *NOT* operations, respectively. After a series of processing, the algorithm output composed by 4 groups with 32 bits [24], and cascade this 4 groups will generate a hash value with 128 bits. For example, the output hash of the zero-length input string is:

MD5("") = d41d8cd98f00b204e9800998ecf8427e.

MD5 could ensure the accuracy and integrity of sharing documents receiving from Internet, but can’t improve the file transfer rate (FTR) of the files. A packet segmentation strategy is proposed to improve the performance of large files transmitting on the Internet. The large documents breakpoint splitting mechanism and small document segmentation mechanisms may be different. In order to ensure the transmission speed of large documents is faster than small documents, large documents must be split to reasonable number of packets and to open more threads to transmit. From the Fig. 8, a large file must be disassembled into multiple packets. Each packet size is best integer times of the network data buffer of UA. And then, these packages are transferred by multithreaded to im prove the FTR. The packet size is the integer times of net buffer that can reduce delays of the packet processing. Once the data is sent out, they must be transferred forward via a router, so the packet size also need to satisfy the integer times requirement of the router MTU (Maximum Transmission Unit).

4 Implementation of PPTalk

The PPTalk communication platform has been deployed in our laboratory with three modes of UA. Each choice represents one service choice. They are UA accesses open SIP services of Internet because the UA of PPTalk is based on the standard SIP protocol, it can be compatible with the existing server on the Internet, or user agent accesses the internal SIP services of laboratory, and user agent accesses the P2P services which is completed in this application but not expressed in this paper. Fig. 9 is the diagram of the system function design of UA of PPTalk.

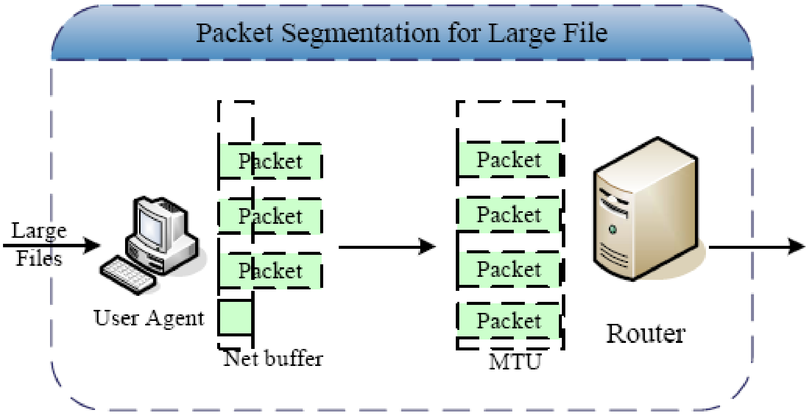


Fig. 8. Packet segmentation strategy for large file

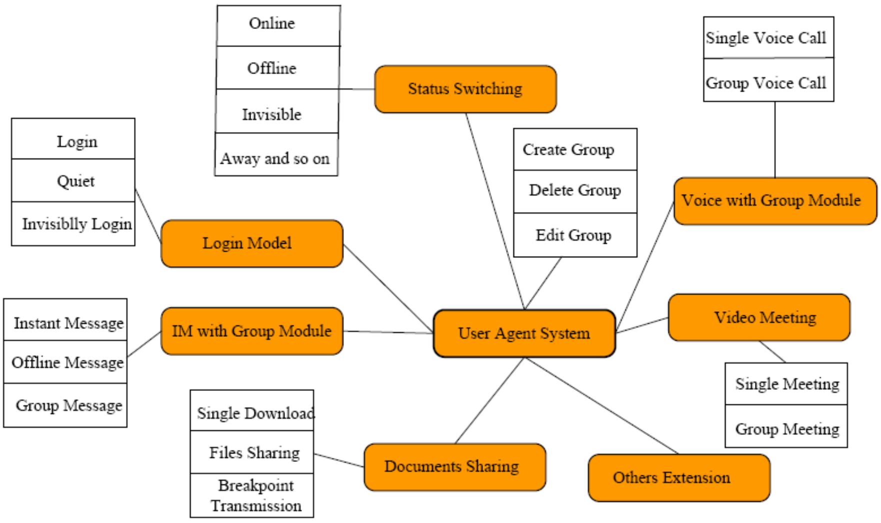
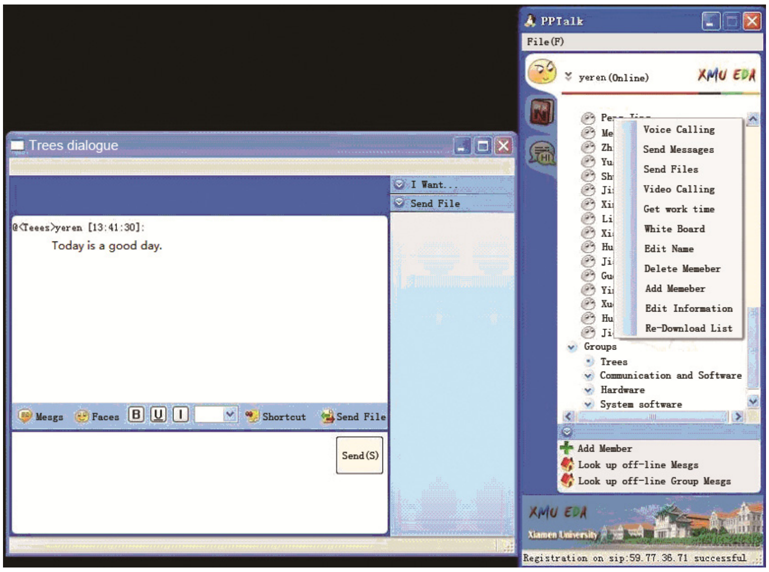


Fig. 9. Diagram of the system function design of UA

From this diagram, the main application modules proposed above have been integrated in the user agent system of PPTalk communication platform to constitute a complete system. There are login management which could connect to the existing user database of laboratory that keep compatible with the original application of our laboratory, IM communication which includes the group management with GMM model mentioned in Section 3.1, VoIP communication, FTP documents sharing modules, service status hints and so on. Security is embedded in the IM, the control information of voice communication with the information security supported by GMM model. UA of PPTalk maintains the logic of configuration of group and security and keeps sync with data service node. Using PPTalk, we are convenient to start a pear-to-pear communication and create or delete a discussion group for group's IM and voice communication, even for video communication. With the GMM model, the data sync of group members is done in UA. The data service node keeps the unified configuration file of user information and public key of RSA, and the private data of group information are created by user oneself. The UI of UA is shown in the Fig. 10.

As an optional choice, a SIP server with SIP services has been built in this application with the data service node. Because the SIP protocol is a normative and the scalable protocol and the compatibility is taken into account in our design, we can use the SIP software of open sources, such as open-sips, to build and set up the SIP server. This is very useful for enterprise to structure a complete communication platform without the Internet services.



@<Teees>yeren [13:41:30]:
Today is a good day.

Registration on sip:59.77.36.71 successful

Fig. 10. The UI of PPTalk UA

5 Performance Evaluation

As shown in Fig. 11, the experimental environment contained more than six windows XP PCs, one linux server and one SUN workstation server in the same LAN, and also contained one PC in the another city of WLAN (wide area network) of Internet. The wireless links between each node are connected via router in the LAN. The linux sever is used as SIP server which provides the SIP service. The SUN workstation is used as the data server node of GMM and other service such as FTP service. Individual PCs install the PPTalk application as UA and the test tools such as Wireshark, VQManager, Ethereal and LanJin NBM and so on. Wireshark is network packets catching and analysis tool, which supports all the network devices and network protocols. Here we can use it for the protocol packet analysis. VQManager is a powerful online real-time monitoring tool of the QOS with VoIP network. Ethereal is another network protocol testing tool, which is used for catching packets and protocol analysis. These tools can be used on the analysis of the SIP packets and RTP packets which are very important in the VoIP system.

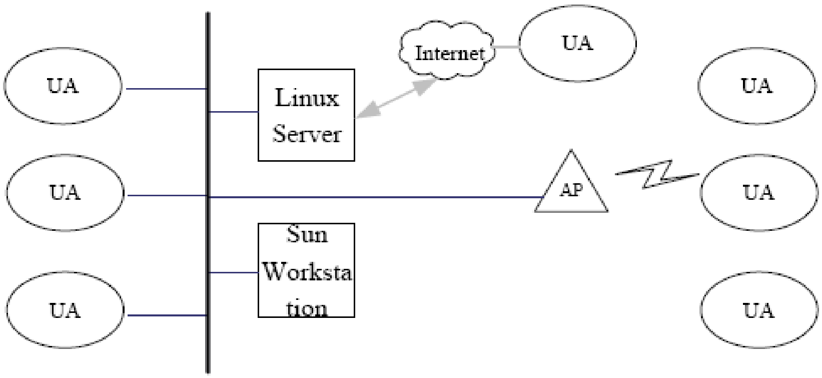
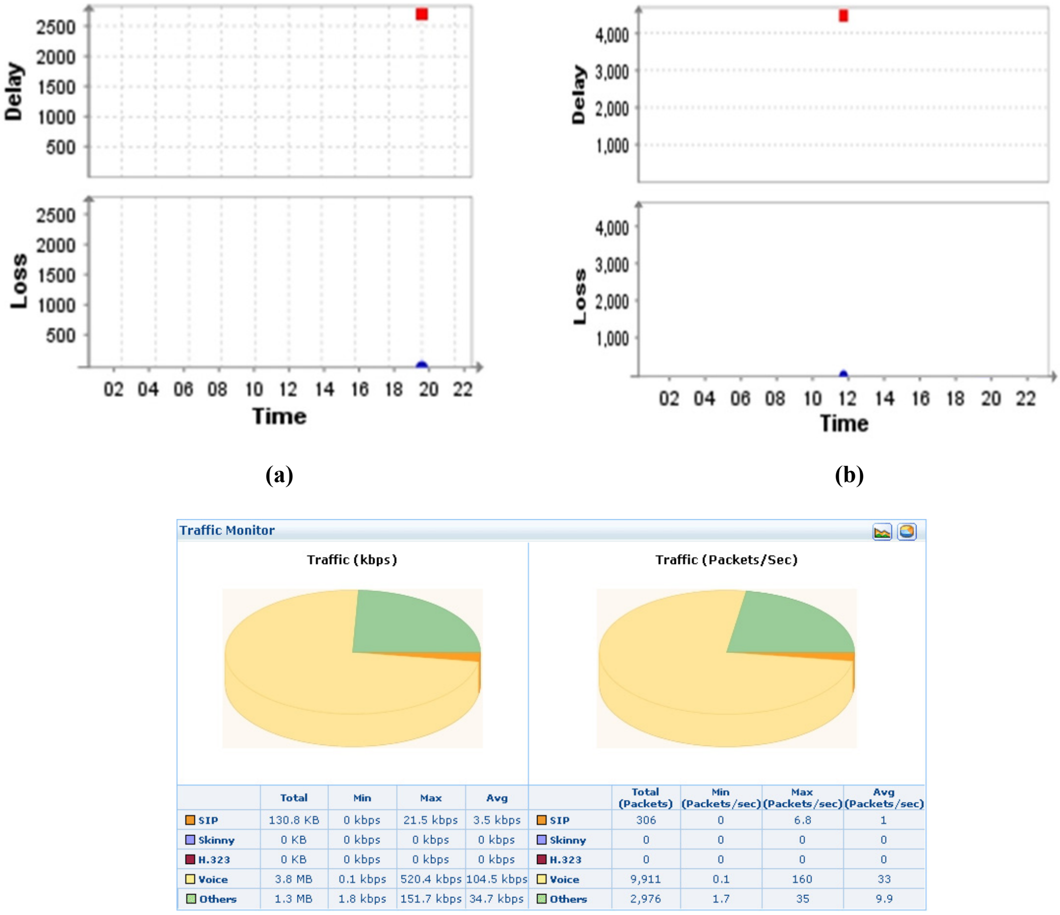


Fig. 11. Experimental set-up

In the business of VoIP communication, quality of service QoS [21] is a core characterization. Fig. 12(a) shows the packet loss rate of voice is zero and the average delay of service is 27ms in the LAN. And the Fig. 12(b) shows the packet loss rate of voice is zero and the average network delay of service is 44ms in the WAN. From the two figures, communication quality is close between remote voice communication and local voice communication because the data is packets forwarding by server deployed in the laboratory, the network delay could be improved because of the interaction of the UA and server in the intranet. Data suggests that PPTalk has good performance within LAN and the packet loss rate on the performance is excellent (zero) no matter in the LAN or WAN.



(a) **(b)**

	Total	Min	Max	Avg		Total (Packets)	Min (Packets/sec)	Max (Packets/sec)	Avg (Packets/sec)
🟧 SIP	130.8 KB	0 kbps	21.5 kbps	3.5 kbps	🟧 SIP	306	0	6.8	1
🟪 Skinny	0 KB	0 kbps	0 kbps	0 kbps	🟪 Skinny	0	0	0	0
🟥 H.323	0 KB	0 kbps	0 kbps	0 kbps	🟥 H.323	0	0	0	0
🟨 Voice	3.8 MB	0.1 kbps	520.4 kbps	104.5 kbps	🟨 Voice	9,911	0.1	160	33
🟩 Others	1.3 MB	1.8 kbps	151.7 kbps	34.7 kbps	🟩 Others	2,976	1.7	35	9.9

(c)

Fig. 12. Test of QoS. (a) The loss&delay indicator of LAN QoS. (b) The loss&delay indicator of WAN QoS. (c) The bandwidth distribution

The bandwidth is another indicator of QoS. After the test, the results have shown that, in voice multicast, each additional members of a multicast only causes an increase of 15k to 20k in bandwidth consumption and the streaming media signal is very stable, which means that the voice multicast business have little influence on the LAN network load even when launching more than 50 people that is about 750K-1M bandwidth. The bandwidth is only 1/10 of the ordinary 10M household router bandwidth or 1/100 of 100M household router. Fig. 12(c) displays the bandwidth consumption distribution of the IM and VoIP communication in the LAN.

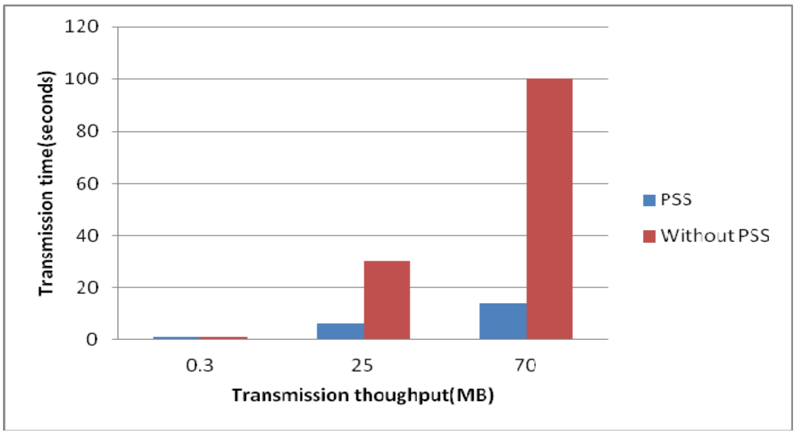


Fig. 13. File transfer rate (FTR) of documents sharing

Fig. 13 shows the FTR of document sharing with or without packet segmentation strategy (PSS), The FTR in the process of dealing with the file of 70 MB, keeps a speed about 5 MB/s, and maximum 7 MB/s with PSS which is much faster compared to the FTR without PSS. In the process of small data transmission, real-time speed is only 340 k/s on average, which is very close to the FTR without PSS. The reason is that if the file is small that do not need to cut the package, only one single thread is created for transmission, the FTR with PSS is slow and is similar to the speed without PSS.

Due to using the same PSS technology to update the common data of GMM model with security in data service node proposed in Section 3, the login time could be speeded up with a mass of group information. Although the SIP message with AES arithmetic can cause some delay of message communication, which real-time performance is not too high and the security has been proved to be reliable [17]. RSA can effectively ensure the safety of key SIP fields such as AES password and the QoS of voice has not been affected obviously because only key SIP fields of VoIP is encrypted.

6 Conclusions

In this paper, a GMM model to extend the application of SIP is proposed. And based on the GMM, the security of SIP is extended with IM communication with AES&RSA combination algorithm to ensure the security of PPTalk. A document sharing mechanism is also proposed with MD5 algorithm and packet segmentation strategy to extend the SIP based application and to speed up the login time for synchronizing the user data in data service. The deployment of the PPTalk system is also discussed to utilize the existing network and resources for building the low cost communication system. The experimental results have shown that the proposed GMM model is suitable to establish the group communication of IM and IMS group communication, and is also convenient to be added with the AES&RSA encryption algorithm for the security of PPTalk. The QoS is excellent and stable and the FTR of file transmission is faster with PSS in the LAN, which express that PPTalk is highly effective and convenient to build local area network communication system with low cost and security.

References

[1] T.P. Wang and H.Y. Lee, "User Location Management for Personal Mobility in SIP-based VoIP Services," in *Proc. of 3th Int. Conf. on Communications and Networking in China (ChinaCom 2008),* pp. 910-914, IEEE Press, 2008.

[2] J. Wilson, "The IETF: Laying the Net's Asphalt," *IEEE Computer*, Vol. 31, pp. 116-117, 1998.

[3] T. Zourzouvillys and E. Rescorla, "An Introduction to Standards-Based VoIP: SIP, RTP, and Friends," *IEEE Internet Computing*, Vol. 14, pp. 69-73, 2010.

[4] B. Rong and Y. Qian, "An Enhanced SIP Proxy Server for Wireless VoIP in Wireless Mesh Networks," *IEEE Communications Magazine*, Vol. 16, pp. 108-113, 2008.

[5] M. Steiner, T. En-Najjary, E.W. Biersack, "Long Term Study of Peer Behavior in the KAD DHT," *IEEE/ACM Transactions on Networking*, Vol. 17, pp. 1371-1384, 2009.

[6] J. Seedorf, "Security Challenges for Peer-to-Peer SIP," *IEEE Network*, Vol. 20, pp. 38-45, 2006.

[7] C.H. Lee, K. Han, Y.H. Lee, "Efficient Resource Registration and Location Scheme in P2P-SIP, using ID-based Signature," in *Proc. of 10th Int. Conf. on Advanced Communication Technology (ICACT 2008)*, Vol. 3, pp. 1823-1827, IEEE Press, 2008.

[8] Z. Li, P. Wu, W. Gao, W.J. Wu, "Study on Methodology for SIP Traversing Symmetric NAT Based on Interactive Connectivity Establishment," *Computer Engineering and Design*, pp. 159-162, 2005.

[9] S.F. Chen, Y. Chen, X.F. Xu, D.H. Guo, "Methodology for NAT/FW Traversal using ICE and HTTP Tunnel," *Telecommunications Science*, Vol. 24, pp. 39-43, 2008.

[10] User scale of VoIP, http://www.iresearch.com.cn/Report/View.aspx?Newsid=67851

[11] SDP- Session Description Protocol, http://www.3cx.com/PBX/SDP.html

[12] B. Chen, W. Zhou, Y. Li, D. Guo, "Innovative Application of SIP Protocol for Communication Platform," in *Proc. of 4th Int. Conf. on Anti-Counterfeiting, Security and Identification (ASID 2010)*, pp. 323-326, IEEE Press, 2010.

[13] B. Johnston, *SIP: Understanding the Session Initiation Protocol, Third Edition,* USA: Artech House, 2010.

[14] J. Franks, P. H. Baker, J. Hostetler, *HTTP Authentication: Basic and Digest Access Authentication*, RFC 2617, 1999.

[15] Y.P. Liao and S. Wang, "A New Secure Password Authenticated Key Agreement Scheme for SIP Using Self-certified Public Keys on Elliptic Curves," *Computer communications*, pp. 372-380, 2010.

[16] J. Rosenberg and H. Schulzrinne, "Models for Multi Party Conferencing in SIP," *International networking of communications*, New York, pp. 275-281, 2004.

[17] X.Y. Bu, "Research and Application for the Software Encrypt system Based on the Combination Algorithm with AES and RSA," *Yanan unive*rsity, pp. 84-90, 2007.

[18] A. Sanchez-Esguevillas, B. Carro, G. Camarillo, Y.B. Lin, M.A. Garcia-Martin, L. Hanzo, "IMS: The New Generation of Internet-Protocol-Based Multimedia Services," *Proceedings of the IEEE*, Vol. 101, No. 8, pp. 1860-1881, 2013.

[19] A.D. Keromytis, "A Comprehensive Survey of Voice over IP Security Research," *IEEE Communications Surveys & Tutorials*, Vol. 14, No. 5, pp. 514-537, 2012.

[20] K.H. Choi, S.K. Lee, K.S. Kong, H. Kim, "Extension of SIP for Group-based Registration," *Electronics Letters*, Vol. 48, No. 2, pp. 91-93, 2012.

[21] O. Micolini and A. Herrera, "Traffic Analysis over a VoIP Server," *IEEE Latin America Transactions*, Vol. 11, No. 1, pp. 370-375, 2013.

[22] D.S. Touceda, J.M.S. Camara, L.J.G. Villalba, J.T. Marquez, "Advantages of Identity Certificate Segregation in P2PSIP Systems," *IET Communications*, Vol. 5, No. 6, pp. 879-889, 2011.

[23] C.H. Huang and S.L. Chang, "Study on the Feasibility of NFC P2P Communication for Nursing Care Daily Work," *Journal of Computers*, Vol. 24, No. 2, pp. 33-45, 2013.

[24] M. Hu and Y. Wang, "MD5-Based Error Detection," in *Proc. of Int. Conf. on Pacific-Asia Circuits, Communications and Systems (PACCS 2009)*, pp. 187-190, IEEE Press, 2009.