A New Authentication Model Based on CL-PKC in Resource limited P2P Systems

Jian Liu
Department of computer science
Xiamen University
Xiamen,China
ws226bz@yahoo.cn

Zhongwen Li
Department of computer science
Xiamen University
Xiamen,China
lizw@xmu.edu.cn

Abstract—**This paper proposes a new authentication model based on CL-PKC technology (Certificateless public key cryptography) in peer-to-peer systems. With the progress in peer-to-peer technology, lots of things related to the security problems of peer-to-peer systems have been exposing. To solve these security problems, authentication must be settled firstly. So this paper develops an authentication method based on CL-PKC technology, considering the dynamic properties of hybrid peer-to-peer systems. This method simplifies the procedure of getting public keys and authentication procedure, so the efficiency is increased, and the mount of bandwidth required is lower. This method is very fit to the systems with limited resources.** *(Abstract)*

Keywords- P2P；CL-PKC；Authentication

I. INTRODUCTION

With the advent of Naspster, the peer-to-peer era has come. Because of storing of resource indexes in a server, Naspster was shut down by law. But people, who had fallen love with this technology, still fellow this technology. Researchers start to design structured and unstructured peer-to-peer network topology and to increase the efficiency, and so on. [1] proposes the pure unstructured peer-to-peer network topology (Gnutella), which aparts from the limitation of center servers. But there are still some problems, such as "The small world "[5], the heterogeneity of nodes[3,4] Free Riding[2] and so on. And then many unstructured peer-to-peer network topologies, such as KaZaA、eDonkey、Freenet and so on, appear.

Accompanying the emergence of the unstructured peer-to-peer system topology, structured peer-to-peer systems also appeared. Such as Chord[6]，CAN[7]，Tapestr[8] and so on. Beside these topologies, hybrid peer-to-peer system topology also been promoted, such as Pastry[9,10]. But there are still many problems to be settled. For example, considering the number of files shared, the fact is that as high as 25% users are not sharing any file in Gnutella, about 75% users sharing less than 100, and only 7% users sharing more than 1000 files. By contrary, the number of the files shared by the only 7% users is more than the sum of the files shared by the other 93% users [16].

Researchers bring the conception—reputation into peer-to-peer systems. Peer-to-peer systems vary the quality of services by their different reputation value. But if we want to use the reputation value, peer-to-peer systems must design user authentication procedure firstly. To build a safe peer-to-peer environment, we must try to find an authentication solution.

These exiting peer-to-peer systems have adopted some authentication methods. In Napster[20], the system supports two authentication methods: one method is that every user has a nick name and associative secret key, so the system can verify the secure key to identity the user ; the other method, when the system sending messages to users, is that the system uses a one direction Hash (md5) function to sign messages. In Mangomind[21] , every person must present the invention before joining the peer-to-peer system. After passing through the verification of invention, the user generates his public/private key, and then sends the public key to the peer-to-peer system to simplify the procedure of the authentication of users. In WebRiposte[22] , the authentication is realized based on the Windows NT/2000 security model. In Groove[23], the authentication of users also need the support of public/private key.

In the academic, researchers also pay attention to the study of authentication in peer-to-peer environments. [24] proposes a duel authentication based on distributed Hash. [25] proposes a public key management infrastructure in a two-tier hybrid peer-to-peer system to fulfill the users' authentication. [26] proposes a distributed authentication service based on public/private key.

They all share the PKI infrastructure. So the verification of the binding between public key and ID is need. This paper puts forward the authentication model based on CL-PKC[27,28] in peer-to-peer environments, solves the problems with certification. It simplifies the authentication procedure, increases the efficiency and lowers the mount of bandwidth.

This paper is organized as follows: first section presents an introduction of the need of authentication in peer-to-peer systems and the progress in this field; second section presents a detailed introduction of authentication in peer-to-peer system at present; third section presents the system's components, its building procedure and the security analysis; fourth section presents some conclusions and future study.

II. RELATED WORK

Authentication methods can be divided into two main categories. One is authentication of node identifications, which

The authors would like to acknowledge the support of Fujian natural science foundation (2008J0034), Program of 2007 New Century Excellent Talents in Fujian Province.

978-1-4244-3693-4/09/$25.00 ©2009 IEEE

is to confirm whether the node identification is valid. Another is an authentication of user permissions, which is to confirm whether the user can use the service. In this paper, we focus on the first, and authentication means validating a message by using e-signature generated by the private key based on CL-PKC.

An exiting authentication method called PKI[30] is the most famous method to authentication nodes. But PKI enables an authentication with servers called CA, and needs CA to certify the correctness of public key. In this procedure, we need to construct a certification chain, and then certify the public key along the chain. Considering the dynamic nodes joining and leaving in peer-to-peer systems, so traditional authentication methods (PKI) do not fit to provide authentication service in peer-to-peer systems.

[24] considers the dynamic feather associating with the nods in peer-to-peer systems, so excludes the use of CA and introduces the distributed management of public keys. The distributed management of public keys is based on hash called HADM, which constructs its route table relying on to Web of Trust and DHT. So HDAM can be used in any system to fulfill the efficient distributed authentication. Users must search public keys; as a result, the higher communication cost is needed. The route table is also constructed based on unsafe Web of Trust, so this system's safety can not be guaranteed.

[26] proposes a distributed authentication service called CorSSO. CorSSO grants authentication to a group of authentication servers. Each application server S selects a subset of the authentication servers by authentication policy to operate the authentication to application server S. Authentication servers are more likely to exhibit independence when they are managed by separate entities, which are physically separated. But this paper is based on PKI; it must solve the authority of the public key using certification chain.

[25] proposes public key management framework to distribute public key safely without PKI infrastructure for two-tier super peer architecture. In order to build the system, users must generate their own public/private keys and then send some messages to authentication servers. This mechanism must store users' messages and respond to users' request. So the center server may fail.

This paper authenticates super peers and common peers through PKG. Users can get public keys send by other nodes, not by making request to servers. And we can certify the authenticity of public keys locally not remotely, resulting lower load in authentication server and lower bandwidth requirement. So this mechanism is very fit to resources limited environment.

III. TARGET SYSTEM ARCHITECTURE

We propose a three-tier peer-to-peer system based on CL-PKC technology (PKG authentication center, super peer layer, common peer layer). PKG is responsible for the authentication of super peers and common peers. In super peer layer, we use the Chord topology to organize super peers, and to place and search resources or peers; a common peer is a client belonging to a super peer, and is the supplier and consumer of resources.

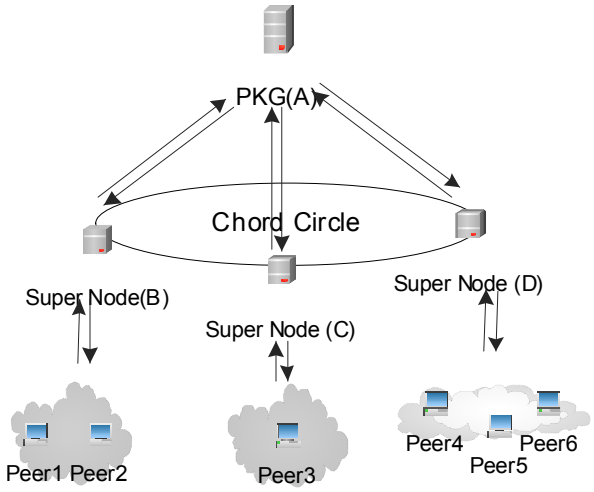

Figure 1 the overview of the P2P system

The building procedure of peer-to-peer system consists of PKG center building procedure, super peer building procedure and common peer building procedure.

A. *PKG CENTER BUILDING PROCEDURE AND SUPER PEER BUILDING PROCEDURE*

According to [27][28], PKG center (A) generates its own system parameters $<G_1,G_2,e,n,P,P_0,H_1,H_2>$ and master key $s \in Zq^*$.

Super peer (B) sends a message (msg1) encapsulated with his own ID to PKG (A) center through a secret channel (*Kerberso*) to get its partial private key and public key. When PKG gets the requisition (msg1) from super peer, PKG using formula (1) calculates the partial private key and public key, and then sends a message (msg2) back to super peer through a secure channel. The requestor (B) receives the feedback message (msg2) from PKG, and use equation (2) to certify the correctness of the message. If the verification is passed, super peer (B) uses equation (3) to compute his own private key and public key.

$$Q = H_1(ID) \in G_1^* \quad (1)$$

$$D = sQ \in G_1^* \quad (2)$$

$$e(D,P) = e(Q, P_0) \quad (3)$$

After super peer (B) gets his own private/public key, all messages sent by him can be certified by signatures. If super peer (B) plans to send a message to super (C), B must get A's public key at first. The procedure is as Figure 2.

TABLE I. EQUATION OF VARABKLES

VARABLE NAME	FORMULA
msg	< ID, <X,Y> , i ,C >
M	H_1 (ID ‖ <X, Y> ‖ i)
C	Sig_s (M)

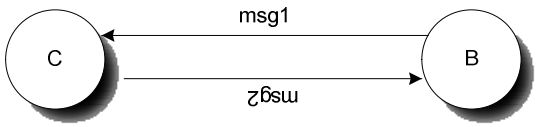

Figure 2 the communication procedure

TABLE II. COMPUTE AND CHECK SIGNAGTURES

Tasks super peer B does when sending message msg1	*Task super peer C does after sending message msg1(assuming C=<U,V>)*
1. random select $r \in Z_q^*$	1. check $X_B, Y_B \in G_q^*$ and $e(X_B, P0)=e(Y_B,P)$,then continue,else exit.
2. compute $M_B = H_1 (ID_B \| <X_B, Y_B> \| i_B)$	2. compute $Q_B=H_1(ID_B) \in G_q^*$
	3. random select $r \in Z_q^*$
3. compute signature $C_B = <rP, M_B \oplus H_2(e(S_B,rP))>$	4. computer signature $V \oplus H_2(Q_B,Y_B)^r) = M_B$

After C gets msg1, he can compute:

$$M_B' = M_B = H_1 (ID_B \| <X_B, Y_B> \| i_B)$$

If $M_B' = M_B$ holds, B's public key held by C is true. B also can get C's public key after receiving msg2. Super nodes can authenticate each other by signatures.

B. *Common peer building*

- Common peer joining. Every common peer has his own identity ID in the peer-to-peer system. Peer1 want to join the system, firstly he must choose his own identity ID_D, and then send this own message to Super Node (B) through Kerberos protocol; Super Node (B) receives the "joining" message and transfers the message to PKG (A). PKG using equation (2) computes partial private key, and sends back it to Peer1 through super node (B) by a secure channel. Peer1 certifies the message received. If successes, Peer1 generates his own private key and public key using his own secret message and message send by super node (B). And then Peer1 sends his own resource indexes to Super Node (B). Super Node (B) stores these resource indexes and other messages. The procedure is like figure (2): 1, 2,3,4,5.
- Common peer searching. Peer1 sends a message (msg) containing required resource name and other feathers to Super Node (B). After receiving the message (msg), Super Node (B) must certify the sender's identity and the integrity of the received message, and then process it (here we assume message will be sent to Super Node (C)). After receiving the message transferred by Super Node (B), Super Node (C) also checks the sender's identity and the integrity of the received message. If verification is passed, he searches required resource locally or otherwise sends the required message to other super peers. If the desired resource is found in Super Node (C), Super Node(C) will send information back to Super Node (B). After passing through checking sender's identity and integrity of message, Super Node (B) sends a message to Peer1. Peer1 gets the replied message, and then checks sender's identity and integrity of the message. If verification is passed, the procedure is finished. The procedure is like figure (2): 6,7,8,9.
- Common peer downloading. If Peer1 wants to download some resources locating in Peer2, Peer1 can send message to Peer2. After receiving the request from Peer1, Peer2 must certify user's authenticity and the integrity of the message. If they are all right, Peer2 sends message to Pee1. If they can make sure of each other's true identity, they can continue the downloading according with some predefined policies. The procedure is like figure (2): 10, 11.

C. *ANALYSIS OF TARGET SYSTEM*

If Pee1 want to communicate with Peer2, Peer1 holds dirty public key associated with Peer2. The table shows the real message.

TABLE III. INFORMATION HELD BY PEERS

INFORMATION TYPE	**PEER NAME**		
	Peer1	***Peer2***	***Peer3***
ID	ID_E	ID_F	ID_G
PUBLIC KEY	$<X_E,Y_E>$	$<X_F,Y_F>$	$<X_G,Y_G>$
PRIVATE KEY	S_E	S_F	S_G

- Public key exchange. If Peer3 catches the message destined to Peer1, which is send by Peer2, and changes the public key to his. Assume Peer1 receive the message $< ID_F , <X_G,Y_G> , i , C = Sig_{SG} (M) >$, $M = H_1(ID_F \|<X_G,Y_G>\| i)$ and do certification as follow:

$$\begin{aligned} & V \oplus H_2 (e(Q_F , Y_G)^r) \\ &= V \oplus H_2 (e (Q_F, X_G sP)^r) \\ &= V \oplus H_2 (e (X_G sQ_F , P)^r) \\ &= V \oplus H_2 (e (S_F', P)^r) \\ &= M_F' \end{aligned} \quad (1)$$

  Because M_F != M_F' holds true, so Peer1 can determine the received public key not belonging to Peer2.
- Super Node not safety. Although super node holds some partial private key, it can not get common peer's private key. This is equal that a person knowing system's parameters $<G_1,G_2,e,n,P,P_0,H_1,H_2>$ 、$Q = H_1(ID) \in G_1^*$ 、$D = sQ \in G_1^*$ and $P=<X=xP,Y=xsP>$ computes the value x[28]. Because this problem can not be solved at present, super node can not get users ' private key.
- Defend DDOS attack. Because of the dynamic properties of peer-to-peer systems, we hope users can get their own public/private keys automatically. If users get their key directly, the PKG is easy to be

attacked by DDOS. This paper lets super peer position between users and PKG to avoid those accidents. This mechanism puts PKG behind, so the probability to be attached is lower. This solution is based the safety of super nodes.

- Replay attack. This system can defend the replay attack, because message generated by the system hold a field i which makes system safe.

IV. CONCLUSION

This paper proposes an authentication model based on CL-PKC in peer-to-peer systems, and also analysis some ordinary attacks. This model has advantages over traditional models, such as: 1) compared with traditional PKI authentication mechanisms, this system can get public key not by requiring, and certify the public key locally, so it needs lower bandwidth to achieve higher security; 2) compared with distributed management of public key based on Web of Trust, this system gets higher level security; 3) this system do not need to store registered users' information resulting in relieving the requirement of hardware; 4) for adopting CL-PKC, this system can use a few resources to get the same level security as the traditional methods. We can continue our work with the integrity of information, reputation computation, access control, the global optimization and so on.

REFERENCES

[1] Ripeanu, M.;Peer-to-Peer Computing, 2001. Proceedings. First International Conference on 27-29 Aug. 2001 Page(s):99 - 100

[2] Hughes, D.; Coulson, G.; Walkerdine, J.; Free riding on Gnutella revisited: the bell tolls. Distributed Systems Online, IEEE Volume 6, Issue 6, June 2005

[3] Chen Wang; Li Xiao; An Effective P2P Search Scheme to Exploit File Sharing Heterogeneity. Parallel and Distributed Systems, IEEE Transactions on Volume 18, Issue 2, Feb. 2007 Page(s):145 - 157

[4] Kin-Wah Kwong; Tsang, D.H.K.; Building Heterogeneous Peer-to-Peer Networks: Protocol and Analysis. Networking, IEEE/ACM Transactions on Volume 16, Issue 2, April 2008 Page(s):281 - 292

[5] Wang, Yong; Yun, Xiaochun; Li, Yifei;Analyzing the Characteristics of Gnutella Overlays. Information Technology, 2007. ITNG '07. Fourth International Conference on 2-4 April 2007 Page(s):1095 - 1100

[6] Stoica, I.; Morris, R.; Liben-Nowell, D.; Karger, D.R.; Kaashoek, M.F.; Dabek, F.; Balakrishnan, H.;Chord: a scalable peer-to-peer lookup protocol for Internet applications. Networking, IEEE/ACM Transactions on Volume 11, Issue 1, Feb. 2003 Page(s):17 - 32

[7] Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard Karp, Scott Shenker. A Scalable Content-Addressable Network. In Proceedings of ACM SIGCOMM 2001

[8] Zhao, B.Y.; Ling Huang; Stribling, J.; Rhea, S.C.; Joseph, A.D.; Kubiatowicz, J.D.; Tapestry: a resilient global-scale overlay for service deployment. Communications, IEEE Journal on Volume 22, Issue 1, Jan. 2004 Page(s):41 - 53

[9] P. Druschel and A. Rowstron. PAST: A large-scale, persistent peer-to-peer storage utility, HotOS VIII, Schoss Elmau, Germany, May 2001.

[10] A. Rowstron and P. Druschel. Storage management and caching in PAST, a large-scale, persistent peer-to-peer storage utility, ACM Symposium on Operating Systems Principles (SOSP'01), Banff, Canada, October 2001.

[11] Hari Balakrishnan, M. Frans Kaashoek, David Karger, Robert Morris, Ion Stoica. Looking up data in P2P systems. February 2003 Communications of the ACM , Volume 46 Issue 2

[12] Yunhao Liu; Zhenyun Zhuang; Li Xiao; Ni, L.M.; AOTO: adaptive overlay topology ptimization in unstructured P2P systems.Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE Volume 7, 1-5 Dec. 2003 Page(s):4186 - 4190 vol.7

[13] Yunhao Liu; Xiaomei Liu; Li Xiao; Ni, L.M.; Xiaodong Zhang; Location-aware topology matching in P2P systems. INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies Volume 4, 7-11 March 2004 Page(s):2220 - 2230 vol.4

[14] Hailong Cai; Jun Wang; Exploiting Geographical and Temporal Locality to Boost Search Efficiency in Peer-to-Peer Systems. Parallel and Distributed Systems, IEEE Transactions on Volume 17, Issue 10, Oct. 2006 Page(s):1189 - 1203

[15] Hassan, O.A.-H.; Ramaswamy, L.; Message replication in unstructured peer-to-peer network. Collaborative Computing: Networking, Applications and Worksharing, 2007. CollaborateCom 2007. International Conference on 12-15 Nov. 2007 Page(s):337 - 344

[16] Ripeanu, M.; Peer-to-peer architecture case study: Gnutella network. Peer-to-Peer Computing, 2001. Proceedings. First International Conference on 27-29 Aug. 2001 Page(s):99 – 100

[17] Yanchao Zhang, Y.; Yuguang Fang, Y.; A Fine-Grained Reputation System for Reliable Service Selection in Peer-to-Peer Networks. Parallel and Distributed Systems, IEEE Transactions on Volume 18, Issue 8, Aug. 2007 Page(s):1134 - 1145

[18] Yu-mei Liu; Shou-bao Yang; Lei-tao Guo; Wan-ming Chen; Liang-min Guo; A Distributed Trust-based Reputation Model in P2P System. Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International

[19] Bin Yu; Singh, M.P.; Sycara, K.; Developing trust in large-scale peer-to-peer systems. Multi-Agent Security and Survivability, 2004 IEEE First Symposium on 30-31 Aug. 2004 Page(s):1 - 10

[20] http://www.napster.com/

[21] http://www.mangosoft.com/products/mangomind/securitywhitepaper.asp

[22] http://www.eschergroup.com/WR%20Release%20Notes.pdf

[23] http://www.ece.rutgers.edu/~parashar/Classes/01-02/ece579/slides/groove.pdf,

[24] Takeda, A.; Hashimoto, K.; Kitagata, G.; Zabir, S.M.S.; Kinoshita, T.; Shiratori, N.; A New Authentication Method with Distributed Hash Table for P2P Network. Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on 25-28 March 2008 Page(s):483 - 488

[25] Hyeokchan Kwon, Sangchoon Kim, Jaehoon Nah, Jongsoo Jang. Public Key Management Framework for Two-tier Super Peer Architecture. 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07)

[26] William K. Josephson, Emin Gün Sirer and Fred B. Schneider. Peer-to-Peer Authentication with a Distributed Single Sign-On Service. Lecture Notes in Computer Science, Peer-to-Peer Systems III

[27] Guo, Lifeng; Hu, Lei; Li, Yong; A Practical Certificateless Signature Scheme. Data, Privacy, and E-Commerce, 2007. ISDPE 2007. The First International Symposium on 1-3 Nov. 2007 Page(s):248 - 253

[28] Sattam S. Al-Riyami and Kenneth G. Paterson, Certificateless Public Key Cryptography , Lecture Notes in Computer Science, pp. 452 - 473, 2003