# Enhancement for Security of Peer-to-Peer by Expanding CGA Mechanism*

Seonggeun Ryu and Youngsong Mun

School of Computing, Soongsil University,
Sangdo 5 Dong Dongjak Gu, Seoul, Korea
sgryu@sunny.ssu.ac.kr, mun@computing.ssu.ac.kr

**Abstract.** In the conventional peer-to-peer(P2P) systems, security was not important, since P2P applications were used in the private networks. Recently, the use of P2P applications is growing dramatically, in particular, for sharing large video/audio files and software in the public networks. Hence, in this paper, we propose a scheme to enhance the security of P2P systems, particularly on a peer's authentication. We expand the Cryptographically Generated Addresses (CGA) mechanism to provide the peer's authentication. In the proposed scheme, we define a new identifier made by IP address and peer's public key to secure the peer and exchanging messages. The identifier is an expanded CGA used in application level. The P2P applications applying the proposed scheme will be secured, since the identifier and public key algorithm provide authentication of peers and messages. We analyze security threats of P2P systems and show how the proposed scheme protects the network from those threats.

## 1 Introduction

With applications such as Napster [1] and Gnutella [2], the peer-to-peer (P2P) model is quickly emerging as a significant computing paradigm of future Internet. Unlike traditional distributed computing, P2P networks aggregate a number of computers, possibly mobile or handheld devices, which join and leave the network frequently. Nodes in a P2P network, called peers, play a variety of roles in their interaction with other peers. When accessing information, they are clients. When serving information to other peers, they are servers. When forwarding information for other peers, they are routers. This new breed of systems creates application-level virtual networks with their own overlay topology and routing protocols. An overlay topology provides mechanisms to create and maintain the connectivity of an individual node to the network by establishing network connections with a subset of other nodes (neighbors) in the overlay network. The

* This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement) (IITA-2006-C1090-0603-0027).

O. Gervasi and M. Gavrilova (Eds.): ICCSA 2007, LNCS 4706, Part II, pp. 1062–1071, 2007.

P2P routing protocols allow individual computers and devices to share information and resources directly, without dedicated servers. Although P2P networking technologies may provide some desirable system properties for supporting pervasive and cooperative application sharing across the Internet, such as anonymity, fault-tolerance, low maintenance and administration costs, and transparent and dynamic operability, there are some well-known problems with most of the current P2P systems. For the P2P paradigm to be adopted widely, the technology must meet several challenges. In this paper, we focus on security of P2P system, such as authentication.

We describe general models of P2P systems, and analyze threats in the models. Then, we propose a scheme to protect peers and messages in P2P systems. The proposed scheme expands Cryptographically Generated Addresses (CGA) mechanism [3] to provide peers' authentication. In the proposed scheme, we define a new identifier made by IP address and peer's public key to secure the peer and exchanging messages. The identifier is an expanded CGA used in application level. The P2P applications applying the proposed scheme will be secured, since the identifier and public key algorithm provide authentication of peers and messages.

In this paper, we focus on the specific problems of peer authentication and message authenticity and integrity. In P2P system, authenticating peers and messages are very important, since P2P system is an environment that every peer does not have trust relationship each other. To solve these problems, we propose a scheme which provides authentication for peers and message authenticity and integrity, inspired by the CGA mechanism. The CGA mechanism is used in Secure Neighbor Discovery (SEND) [4] which secures Neighbor Discovery (ND) [5] in IPv6 [6].

We define a new identifier, Identifier Number (IDNUM), which expands the CGA. The IDNUM is used as an identifier of a peer in P2P system, and generated from the public key of the peer, IP address and auxiliary parameters. The messages are signed by the private key of the peer. Thus, the authentication of peer is guaranteed by the IDNUM. In the same manner, authenticity and integrity of messages are ensured by the signature.

We analyze security threats of P2P systems and show how the proposed scheme protects the network from those threats.

This paper is organized as follows: In section 2 we explains related works, such as P2P systems and CGA mechanism. Section 3 presents the security threats in P2P systems and Section 4 presents the proposed solution to protect the systems from those threats. Finally, in section 5 we draws the conclusions.

## 2 Related Works

### 2.1 P2P Network

A P2P system is a distributed system whose component nodes participate in similar roles, and the nodes are therefore peers to each other. P2P can be viewed as decentralized network architecture. In contrast, a client-server architecture implies a sharp distinction between the clients which request and consume services,

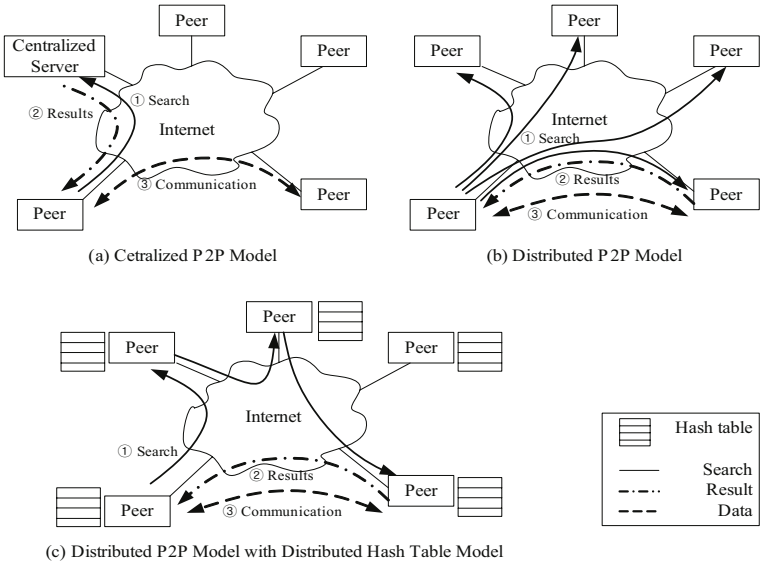


**Fig. 1.** Three P2P Models

and servers which provide services. Even though the nodes have similar roles, there may still be some structure to the P2P system, and it usually possesses some degree of self-organization that each node finds its peers and helps to maintain the system structure. This makes a P2P network node more complex than a client in client-server system. The main benefits of P2P system are scalability, fault-tolerance, and the lack of resource bottlenecks in servers. The P2P concept is related to distributed computing, but differs from them in that P2P nodes usually serve their own needs acting as intelligent agents, instead of performing a collective function as a group. Recently, the concept has achieved recognition in the general public in the context of P2P file sharing which is one application of P2P networks.

The P2P nodes are more powerful than a client on client-server network. This is because the Internet environment has been changed. The performance of the CPU of PC has been tremendously improved and the bandwidth of Internet connection cable has got bigger very quickly. And this change has made client inefficient for a host on Internet, if it plays only the role of the conventional client. Moreover, Internet users are demanding more and more, to be able to get served anonymously.

P2P models can be categorized into three groups, depending on the characteristics of each application. The three groups are centralized P2P model, distributed P2P model, and distributed P2P model with distributed hash table. Figure 1 shows three kinds of P2P models.

### 2.2 CGA Mechanism

Cryptographically Generated Addresses(CGA) are IPv6 addresses that the interface identifier of the address bits is generated by hashing the public key of the address owner and auxiliary parameters, and it is used in Secure Neighbor Discovery(SEND). The address owner uses the corresponding private key to declare the address ownership and to sign the message sent from the address without any security infrastructure. A node which received messages with CGA address may verify the message by re-computing the hash value and compare the hash value with the interface identifier. The integrity of the message is guaranteed by attached digital signature and the material generating CGA address. This authentication process is done without any certification authority or any security infrastructure. Note that every node can make CGA address with their own public key or even somebody else. However, a malicious node is not able to make a proper signature for another CGA address, because the malicious node does not have the other's private key.

**Generation of CGA and Signature.** A node which wants to generate a CGA address should follow the CGA mechanism, and the message with CGA address as source address must have a digital signature. Figure 2 shows generation of CGA address and digital signature in simple manner. The important point is that CGA address is generated from the public key of the owner of the address, and the message is digitally signed by the private key of the address owner. The

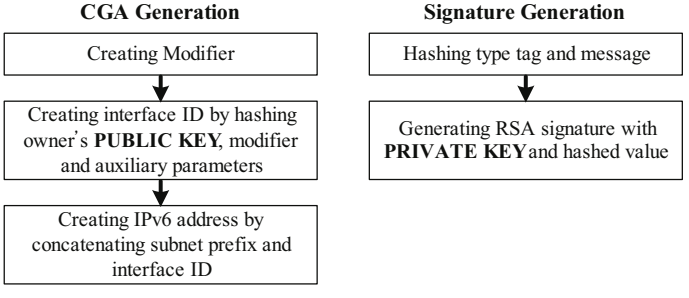


**Fig. 2.** A Simple Flow of Generations of CGA and Signature

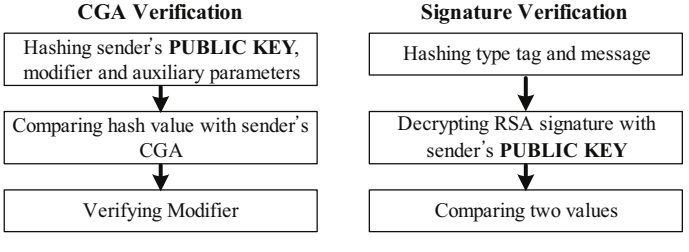


**Fig. 3.** A Simple Flow of Verifications of CGA and Signature

material to generate CGA address and signature is delivered in option field, such as CGA Option Field and CGA Signature Option Field.

**Verification of CGA and Signature.** A node which received a message with CGA address as source address must verify authenticity of the message. In order to do that, the receiver regenerates the source CGA address using delievered information in the message. The message itself can be verified by decrypting the digital signature with sender's public key. Figure 3 shows verification of CGA address and digital signature in simple manner.

## 3 Analysis of Security Threats

In this section, we analyze security threats of the centralized P2P network which include threats of three kinds of P2P network models. The security threats of P2P network can be categorized in three ways, such as disclosure threats, deception threats and disruption threats. The disclosure threats are circumstances or events whereby an entity gains access to data for which the entity is not authorized. The deception threats are circumstances or events that may result in an authorized entity receiving false data and believing it to be true. The disruption threats is circumstances or events that interrupt or prevent the correct operation of system services and functions [7].

### 3.1 Disclosure Threat

In P2P network, any entity can look the traffic between peers even if it has no authorization. It means the unauthorized entity can directly see some sensitive data, such as data for access to the network, transferred between authorized peers. Also the unauthorized entity can get sensitive data indirectly by reasoning from the external features or byproducts of the communication between authorized peers. With the sensitive data, the unauthorized entity can circumvent the security protections of the P2P network system, and acquires another sensitive data. As a result, authorized peers can not obtain the access permission and the private information of those peers can be exposed. Figure 4 shows disclosure threats in P2P systems.

Piggyback Attack is a form of active wiretapping in which the attacker gains access to a system via intervals of inactivity in another user's legitimate communication connection. It is sometimes called as between-the-lines attack. Hijack Attack is a form of active wiretapping in which the attacker seizes control of a previously established communication association. Spoofing Attack is a type of attack in which one system entity illegitimately pretends as (assumes the identity of) another entity. This attack is performed by using information got from passive attacks.

### 3.2 Deception Threat

A malicious node sends a modified messages to a victim node, and hence it can connect to the victim and perform unintended action. The malicious node

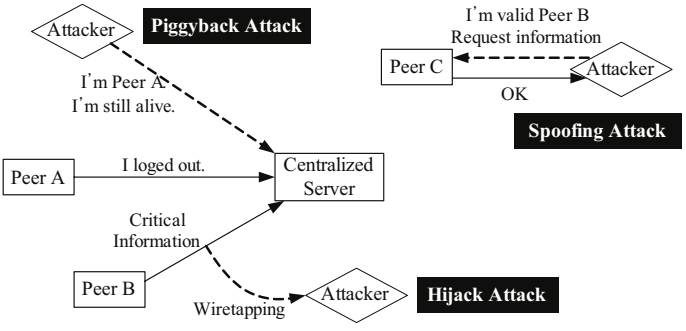


**Fig. 4.** Disclosure Threats in P2P System

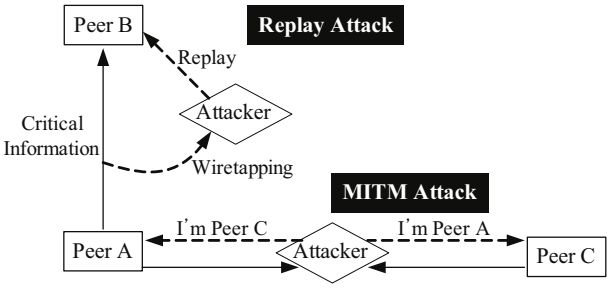


**Fig. 5.** Deception Threats in P2P System

modifies important information and send the invalid information to deceive the victim. Thus the malicious unauthorized node acquires the access right to the P2P system. The malicious node pretends itself as an authorized node and performs a spiteful action, such as transmitting false data to deceive an authorized node or release false information to the nodes in the system. In the P2P network, peers can not get serviced because the malicious node modifies sensitive information, and these threats may cause DoS, DDoS or Flooding attacks. Deception threats are shown in Fig. 5.

Replay Attack is an attack in which a valid data transmission is maliciously or fraudulently repeated, by either the originator or an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack. Man In The Middle (MITM) Attack is a form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data in order to masquerade as one or more of the entities involved in a communication association.

### 3.3 Disruption Threat

For a malicious attacker, the disruption attack is the final attack to carry out. After the malicious node performs the disclosure threat and the deception threat, the malicious node can access to the sensitive data and be ready to aim a target

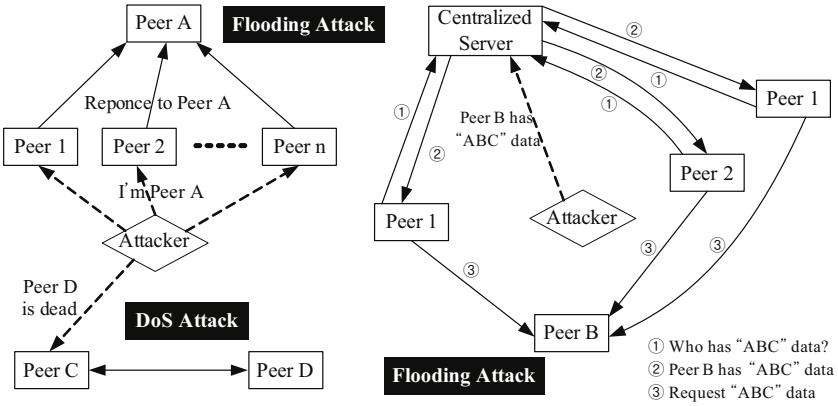


**Fig. 6.** Disruption Threats in P2P System

node. The malicious peer can interrupt delivery of the network service by hindering communication between another peers. Those victims can not communicate or response to any other peers. As a result, the entire P2P network can be in DoS, DDoS or Flooding attack. Figure 6 illustrates disruption threats in P2P systems.

Denial of Service (DoS) Attack is the prevention of authorized access to a system resource or the delaying of system operations and functions. Flooding Attack is an attack that attempts to cause a failure in (especially, in the security of) a computer system or other data processing entity by providing more input than the entity can process properly.

## 4 Solution for Security of P2P Networks

So far we figure many security threats in P2P network. For disclosure threats, peer authentication is needed to prevent piggyback, hijack, and spoofing attacks. Also, messages need to be encrypted to protect sniffing attackers. In distributed P2P with distributed hash table model, updating hash table must be secured. For deception threats, detection of duplicate message is needed to prevent replay attack. Also, messages between peers must be authenticated to prevent the sensitive messages modified by a attackers. Disruption threats are based on disclosure and deception threats. To invoke the disruption threats, both the disclosure attack and the deception attack need to be preceded. So we conclude that to secure the P2P network, peer authentication and data authenticity and integrity are needed.

### 4.1 The Proposed Scheme

We propose a scheme to secure peer authentication and authenticity and integrity for the message. We also use the sequence number for our scheme to prevent the

replay attack. We expand the CGA mechanism and define an identifier playing the same role as a CGA, and call it by IDNUM. IDNUM is made from the public key of the peer, IP address, and auxiliary parameters.

$$IDNUM = SHA1\{public\,key \,|\, IP\,address \,|\, auxiliary\,parameters\} \quad (1)$$

In (1), the public key of the peer, IP address, and auxiliary parameters are concatenated and hashed by SHA1 algorithm [8]. The output is 160bit long IDNUM.

Also, all messages are signed with the private key of the peer, like the way in CGA mechanism. Input parameters of RSA signature are IDNUM, public key, IP address, sequence number, and the message. All of these parameters are delivered in the message to verify the IDNUM and the signature like the way in CGA mechanism.

The proposed scheme can guarantee peer authentication through generating and verifying the IDNUM of the message, and the signature of the message provides data authenticity and integrity. The receiving peer can believe that the received message is sent from the owner of the IDNUM by our scheme. Also the message is protected from the replay attack by the sequence number. The important point is that the proposed scheme does not need any security infrastructure.

### 4.2 Operation of the Proposed Scheme

Whenever a peer sends a message, our proposed scheme protects the peer and the message. Also, whenever a peer receives a message, the proposed scheme verifies the sender and the message. The proposed scheme may be implemented as a security module in protocol stack in the same manner of implementing of IPsec [9]. Figure 7 shows the operation of the proposed scheme.

In the point of view of the sender, the security module finds a key pair(i.e public and private key of the peer). If the peer did not have the key pair, the security module generates a key pair. Then, the security module try to find IDNUM of the peer. If the peer did not have any IDNUM, the security module generates IDNUM. The security module increases sequence number and computes RSA signature of the message. All parameters used to generate IDNUM and signature are embedded in the message.

In the point of view of the receiver, the security module verifies the sequence number. It then re-generates sender's IDNUM by using the delivered parameters, and compares the re-generated IDNUM to the received IDNUM. Then, the security module verifies RSA signature with the public key of the sender. If the sequence number, IDNUM or signature in the message is not verified, the message is discarded. When all of the verification procedures have been succeeded, the receiver gets to believe that the sender is the owner of received IDNUM and the message is not modified.

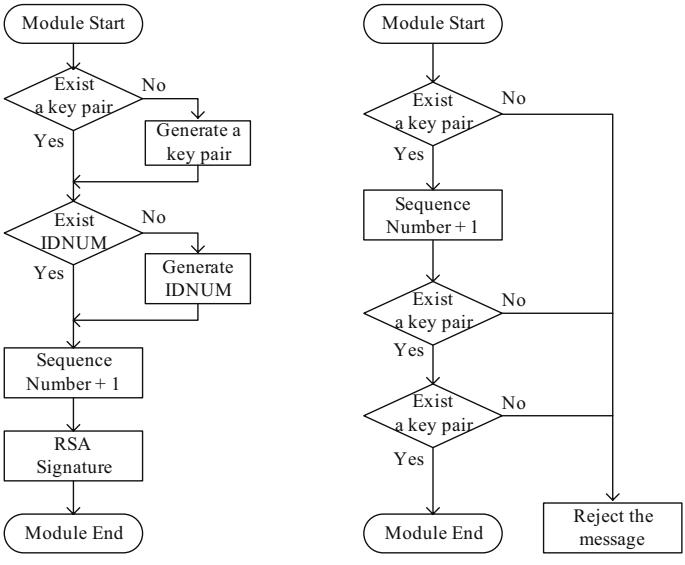


**Fig. 7.** Operation of the proposed scheme

## 5 Conclusions and Future Study

The peer-to-peer network is very useful and it already has became general. However the conventional P2P systems are vulnerable to numerous attacks, and do not have enough security mechanisms to ensure the authenticity and integrity of shared information. To solve this problem, we propose a scheme inspired by CGA mechanism. The proposed scheme guarantees peer authentication and authenticity and integrity of the data without any security infrastructure.

In section 2 we explained P2P systems, and in section 3 we analyzed security threats in P2P systems. We notice that P2P network is similar to Neighbor Discovery network in IPv6. SEND protocol is used to secure ND protocol, and CGA mechanism is used in SEND protocol. Thus we expand and apply CGA mechanism to P2P network to secure P2P network.

The proposed scheme will be able to support authentication for peers and provide data authenticity and integrity by expanding CGA mechanism. Moreover, we can use sequence number algorithm to prevent replay attack.

We hope that the proposed scheme will help current P2P applications to enhance security. Therefore, we will implement the proposed scheme as a security module and test the module in current P2P applications.

## References

1. Napster: peer-to-peer file sharing software application, `http://www.napster.com`
2. Gnutella: peer-to-peer file sharing software application, `http://www.gnutella.com`
3. Aura, T.: Cryptographically Generated Addresses (CGA), RFC 3972 (2005)

4. Arkko, J., Kempf, J., Zill, B., Nikander, P.: Secure Neighbor Discovery (SEND), RFC 3971 (2005)
5. Narten, T., Nordmark, E., Simpson, W.: Neighbor Discovery for IP Version 6 (IPv6), RFC 2461 (1998)
6. Deering, S., Hinden, R.: Internet Protocol, Version 6 (IPv6) Specification, RFC 2460 (1998)
7. Shirey, R.: Internet Security Glossary, RFC 2828 (2000)
8. Eastlake, D., Jones, P.: US Secure Hash Algorithm 1 (SHA1), RFC 3174 (2001)
9. Kent, S., Seo, K.: Security Architecture for the Internet Protocol, RFC 4301 (2005)