A Thesis for the Degree of Master

A Study on Adaptive Authentication Mechanism for Virtual Community

Hyunrok Lee

School of Engineering

Information and Communications University

2003

A Study on Adaptive Authentication Mechanism for Virtual Community

A Study on Adaptive Authentication Mechanism for Virtual Community

Advisor : Professor Kwangjo Kim

by

Hyunrok Lee
School of Engineering
Information and Communications University

A thesis submitted to the faculty of Information and Communications University in partial fulfillment of the requirements for the degree of Master of Science in the School of Engineering

Taejon, Korea
Jan. 6. 2003
Approved by

(signed)

Professor Kwangjo Kim
Major Advisor

A Study on Adaptive Authentication Mechanism for Virtual Community

Hyunrok Lee

We certify that this work has passed the scholastic standards required by the Information and Communications University as a thesis for the degree of Master

Jan. 6. 2003

Approved:

Chairman of the Committee
Kwangjo Kim, Professor
School of Engineering

Committee Member
Jung Hee Cheon, Assistant Professor
School of Engineering

Committee Member
Chulsoo Lee, Invited Professor
School of Engineering

M.S. Hyunrok Lee
2001099

A Study on Adaptive Authentication Mechanism for Virtual Community

School of Engineering, 2003, 48p.
Major Advisor : Prof. Kwangjo Kim.
Text in English

Abstract

According to the advance of the Internet and development of information technologies, people tend toward establishing virtual communities and asserting their opinions. To build virtual community, most important things are how they can make the community and carry their points in a cyberspace. We can consider many approaches to achieve these goals. The most useful approaches are that we can think peer-to-peer (simply P2P) system as a tool for establishing the community on the Internet, and the Internet voting can be regarded as the way to assert their opinions. However, P2P and the Internet voting system are hesitated people about many security problems. Particularly, authentication problems are considered an important issue. Through this thesis, we propose two mechanisms for efficient authentication: adaptive authentication for P2P system and extension of votopia[29] based on adaptive authentication.

The technology of communication among people on the Internet was previously focused on the server-oriented system, but recently changed into a kind of distributed computing, P2P systems which can not only be applied to instant messaging, collaborate computing, etc., but also

be considered the foundation for binding people. Like a real face-to-face trust relationship, each peer with complicated trust relationship faced complex security problems. Especially, an authentication problem among peers will be an important issue. Although P2P network must not only provide pseudonymity but also satisfy strong authentication in case that a peer does business transaction with another one, most of current P2P services just adopt a weak authentication method using pseudonym and password. Hence, we propose an Adaptive Authentication Protocol based on Reputation(AAPR) which can satisfy requirements ranging from pseudonymity to strong authentication based on certificate. Also we consider the context–dependent reputation concept and the minimization of certificate issuing cost by using different type of certificate under the concept of zero-dollar cost certificate if required.

The Internet voting for aggregating people's opinion becomes new challenging area in cryptographic application. A variety of schemes are designed and implemented based on cryptographic protocols. One of best practices was the votopia which was successfully served into the Internet voting based on modified Ohkubo et al.'s scheme[39] under Public Key Infrastructure (PKI) and Java technology. The votopia was used to select the Most Valuable Player and Best Goal Keepers of 2002 FIFA World Cup Korea/Japan^{TM} through the Internet where most voters can access and cast their ballots from any place and at any time. However, the votopia assumed that the resources of the Internet voters only connected via wired environment and specific certificate issued by votopia's Certificate Authority(CA). In this thesis, we suggest how to extend votopia to general Internet voting with adaptive authentication ranging from the Internet polling to plebiscite, and also we expand votopia into mobile device which has limited computing resources.

Contents

Abstract **i**

Contents **iii**

List of Tables **v**

List of Figures **vi**

List of Abbreviations **vii**

List of Notations **viii**

I Introduction **1**

1.1 Overview 1

1.2 Adaptive Authentication Protocol for P2P System 1

1.3 Extension of Votopia 3

1.4 Outline of thesis 5

II Preliminaries **6**

2.1 Related works 6

2.1.1 Classification of Authentication Mechanism . . . 6

2.1.2 P2P System and Trust 8

2.1.3 Secure Multicasting 10

2.1.4 Overview of Votopia 11

2.1.5 Java Mobile Technology 14

2.2 Previous works 14

2.2.1 Authentication Mechanisms on the current P2P System 14
2.2.2 Authentication in Votopia 16
2.2.3 Previous Mobile Voting Systems 17

III An Adaptive Authentication Protocol based on Reputation for P2P System 19
3.1 Requirements 19
3.2 Proposed Protocol 20
3.3 Comparison 29

IV Extension of Votopia to General Internet Voting 32
4.1 Type of the Internet Voting 32
4.2 Requirements 33
4.3 Proposed Voting System 33
4.4 Comparison 38

V Conclusions and Future work 40

국문요약 42

References 44

Acknowledgement 49

Curriculum Vitae 51

List of Tables

3.1 Cryptographic Notations 22
3.2 Notations for Message passing 22
3.3 Notations for Trust relationship 23
3.4 Example of recommendation table 23
3.5 Recommendation table of β 27
3.6 Recommendation table of γ_1 27
3.7 Recommendation table of β 28
3.8 Recommendation table of γ_1 28
3.9 Recommendation table of γ_2 28
3.10 Recommendation table of γ_3 29
3.11 Recommendation table of γ_4 29
3.12 The comparison of authentication for P2P 31

4.1 The comparison of the Internet voting system 39

List of Figures

2.1 Gnutella/Freenet–like system. 9
2.2 Napster–like system. 9

4.1 Architecture of Generalized Votopia 35
4.2 Certificate Manager for Generalized Votopia 36

List of Abbreviations

CDC Connected Device Configuration

CLDC Connected Limited Device Configuration

CPU Central Processing Unit

DB Data Base

DES Data Encryption Standard

GSM Global System for Mobile communication

JVM Java Virtual Machine

MAC Message Authentication Code

P2P Peer-to-Peer

PDA Personal Digital Assistant

PC Personal Computer

PIN Personal Identification Number

PKI Public Key Infrastructure

SMS Short Message Service

SSL Secure Socket Layer

WAP Wireless Application Protocol

WTLS Wireless Transport Layer Security

XML Extensible Markup Language

List of Notations

x : peer(identity) $x \in \{\alpha, \beta, \Gamma\}$, where $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$, $\gamma_i \neq \alpha$ and $\gamma_i \neq \beta$ for $i = 1, 2, \ldots, n$.

$x \rightarrow y$: x sends one message to y or Y.

$P_x(m)$: x's public key encryption to message m.

$S_x(m)$: x's private key signature to message m.

r_x : random numbers of x.

K_x : x's session key.

CK : set of community keys, where $CK = \{CK_1, CK_2, \ldots, CK_l\}$.

CK_x : x's subset of $CK \equiv CK_x \subset CK$.

$MAC(CK, m)$: keyed Message Authentication Code.

$cert_x$: x's certificate.

F_{cert} : formal certificate issued by legal CA.

I_{cert} : informal certificate issued by service provider or super peer node.

S_{cert} : self-signed certificate.

$V_{\{cert_x\}}$: selected x's certificate.

sel_G : selective message for *Guest protocol*.

sel_M : selective message for *Member protocol*.

$permit_x$: allow x to communicate with pseudonym–based authentication.

$refuse$: refuse communication.

$req_{\{m\}}$: request the message m.

C_{BT} : critical business transaction.

R_i : the range of trust, where $R_{min} \leq R_i \leq R_{max}$, for $i = 1, 2, \ldots, n$, $R_{min} = R_1$ =total distrust, $R_{max} = R_n$ =complete trust.

V_i : trust value, where $0 \leq V_i \leq 1$ for $i = 1, 2, \ldots, n$.

W_C : weight factor of category, where $0 \leq W_C \leq 1$.

$\overrightarrow{T_x}$: the vector of trust value of x, $(requestor\ ID, category, target\ ID, V_i)$.

$\overrightarrow{T_{x,\gamma_i}}$: $\overrightarrow{T_x}$ from $\gamma_i \in \Gamma$ for $i = 1, 2, \ldots, n$.

$com(x)$: calculated total trust value of x.

$\alpha \Rightarrow \beta$: recommendation(indirect) trust.

$\alpha \rightarrow \beta$: direct trust.

AS : Admin Server.

CT : Counting Server.

WS : Web Server.

$B()$: Blinding function.

$UB()$: Unblinding function.

BB : Bulletin board and ballot box.

VT_i : Voter i.

vt_i : vote value by VT_i.

C_i : VT_i's selected certificate.

I. Introduction

1.1 Overview

According to the advance of the Internet and development of information technologies, people tend toward establishing virtual communities and asserting their opinions. To build virtual community, most important things are how they can make the community and carry their points in a cyberspace. We can consider many approaches to achieve these goals. The most useful approaches are that we can think peer-to-peer (simply P2P) system as a tool for establishing the community on the Internet, and the Internet voting can be regarded as the way to assert their opinions. However, P2P and the Internet voting system are hesitated people about many security problems. Particularly, authentication problems are considered an important issue. Through this thesis, we propose two systems to solve authentication problem: adaptive authentication for P2P system and extension of votopia[29] based on adaptive authentication.

1.2 Adaptive Authentication Protocol for P2P System

These days, the Internet exhibits three valuable characteristics. Compared with the environment of the Internet for previous years, it is rapidly growing in terms of the amount of information exchanged, the capacity of bandwidth and the power of computing resource. First of all, massive information is flowing via network. Second, the network bandwidth is increasing. Lastly, the power of computing resources are

growing. So the Internet needs a new paradigm, that is different from existing one such as server oriented paradigm, which can handle three characteristics well.

A new peer-to-peer (simply P2P) system has been attracted a focus of public attention. The services on the Internet were previously focused on the server-oriented system, but recently changed into a kind of distributed computing, P2P systems which can be applied to instant messaging, collaborate computing, etc. SETI@home[46] have empowered millions of users to contribute their computing powers to work on a common computational analysis. An instant messaging services have enabled users to communicate and collaborate instantly with their peers on the Internet or the intranet. And a file sharing service embodied by applications like Napster[37], Gnutella[22], etc. has offered a compelling and intuitive way for the Internet users to find and share resources directly with others. A peer can have both client and server processes at the same time. The P2P computing[41] is direct sharing of computing resources and services between peers in arbitrary network. Such a P2P computing can be categorized largely into pure P2P and hybrid P2P[40]. The former is that all peers have the same capability and responsibility to build symmetric communications. The latter is that some servers can facilitate the interaction between the peers even if they perform the interaction directly.

Most of current P2P services have security problems which play an obstacle to practical use. Like a real face-to-face trust relationship, each peer which has a complicated trust relationship is entangled in complex security problems. Especially, an authentication problem among peers will be an important issue. Although P2P network must not only provide pseudonymity but also satisfy with strong authentication in case that a peer does business transaction with another one, most of current P2P services just adopt a weak authentication method using pseudonym

and password[37, 27, 25, 36, 1] or does not support any cryptographic authentication[46, 22, 15, 28]. Furthermore, the Groove Network[23] provides public key based strong authentication mechanism. However, this mechanism both needs a central server that provides directory service for retrieving user's public key every time and does not have a legal force that can control and settle a dispute. Even if Fahrenholtz et al. [18] proposed a strong authentication mechanism and a reputation management for P2P system, they did not cope with server oriented paradigm and also did not support pseudonymity and minimizing the cost of issuing certificate. Therefore, those are not suitable to serious P2P commercial transaction which can occur in the near future such as exchanging valuable information of knowledge, applying e-commerce, etc. And also those do not satisfy requirements like pseudonymity which are required in trivial services.

In this thesis, we propose an adaptive authentication protocol based on reputation(AAPR) which can satisfy requirements ranging from pseudonymity to strong authentication based on certificate without particular server. Also we consider the context–dependent reputation concept and minimizing the cost of issuing certificate due to different type of certificate used under the concept of zero-dollar cost certificate if required. The zero-dollar cost certificate does not need a price which imposes the cost on issuing certificate by a legal Certificate Authority(CA) except for the cost of processing power which is necessary in the time for generating and signing certificate.

1.3 Extension of Votopia

Voting is one of efficient methods for decision making in any society. The research on electronic voting through the Internet will play an important role for the progress of democracy. If a secure and convenient electronic

voting system is provided, it will be used more frequently to collect the opinion of suitable voters for many political and social decisions ranging from the Internet polling to plebiscite through cyberspace.

The Internet voting has become in reality. There are many experiments and implementations done successfully over the Internet such as the election scheme proposed by the state of California[5], Caltech–MIT joint project[9], and most recently one so called the votopia for selecting the Most Valuable Player and Best Goal Keepers of 2002 FIFA World Cup Korea/Japan^{TM}. All voting schemes have successful served in the wired Internet environment where voters use desktop PC or notebook providing enough resource for quite heavy computation, and the authentication of the voting schemes follows restrict step which is dominated by each scheme. For example, the votopia selects certificate–based authentication, which is issued by specific CA of the votopia, with password–based authentication to prevent double voting.

But now, the Internet voting, including the votopia, faces a new requirement to enable voting to be satisfied the demands of people who belong to virtual community. They want to use the Internet voting ranging from the Internet polling to plebiscite. Also the Internet voting can be performed on mobile devices such as PDA (Personal Digital Assistant) or mobile phone which has limited computing resources and low power supply. The mobile voting has just begun. For example, CyberVote[10], VoteHere[48], eVoteSheffield[17] and Euro–Citi[16] try to serve mobile voting via mobile phone or PDA device. The Internet voting system as well as the mobile voting system must meet cryptographic requirements such as anonymity, privacy, completeness, fairness, verifiability, and receipt–freeness. Some mobile voting systems don't provide end–to–end security using only encrypted channels (i.e., SSL) and simple identification mechanism (i.e., PIN code). Others attempt to apply a cryptographic voting protocol satisfied with the requirements

to their system. However, the most important point in the design of the mobile voting system is reduction of computation in a mobile device.

In this thesis, we describe the requirements of extension of the votopia with mobile voting, and extend the functionality of the votopia to general version, named as generalized votopia.

1.4 Outline of thesis

The rest of this thesis is organized as follows: In Chapter II, we introduce some related works like the classification of authentication mechanisms, P2P system including trust and a secure multicast technique for requesting information from arbitrary peers. Also an overview of the votopia and Java mobile technology are followed. The previous works, such as authentication mechanisms on the current P2P system, authentication in the votopia and previous mobile voting system, are described here. Chapter III describes our adaptive authentication protocol for P2P system with comparison. We present the extension of votopia in Chapter IV. And finally conclusions and future works of this thesis will be made in Chapter V.

II. Preliminaries

2.1 Related works

2.1.1 Classification of Authentication Mechanism

Authentication is a primary technology between any cryptographic technologies. The authentication methods can be classified into password–based, secret key–based and public key–based authentication.

Password–based authentication

Password–based authentication verifies user's identity with the knowledge of user(password). This method spreads widely in practical system up to now because of it's convenience. But the password–based authentication has problems as follow:

1. Registered password saved at the key center must be secret.
2. If the password is revealed, the security of authentication will be broken.

To solve problems partially, UNIX password with a block cipher DES and one–time password using oneway hash function.

Secret key–based authentication

Although this authentication method has problems that are complex key distribution and management, this method is realistic method for the authentication limited users in specific system. A typical step of secret key–based authentication is following.

1. User A generates a random number r_A, then A sends r_A to user B.

2. User B generates a random number r_B. B sends the result of encryption with secret key K $X = E_K(B \parallel A \parallel r_A \parallel r_B)$ to A.

3. User A decrypts X, then A verifies r_A. After A calculates $Y = E_K(A \parallel r_B)$, sends Y to user B.

4. User B decrypts Y, then verifies r_B.

Public key–based authentication

To solve key distribution and management, public key cryptography is appeared. This authentication method using public key concept can be divided into

- Using public key/digital signature (including certificate–based authentication).
- Using zero knowledge proof.
- Using identification protocol; such as FS[21] identification protocol.

In this thesis, we concentrate on certificate–based authentication. So we introduce the strong authentication protocol based on certificate as follow:

Let $D_A = (r_A, B, data_1, P_B(k_1)), D_B = (r_B, A, r_A, data_2, P_A(k_2))$.

$$\begin{aligned} A \rightarrow B: &\quad cert_A, D_A, S_A(D_A) \\ B \rightarrow A: &\quad cert_B, D_B, S_B(D_B) \\ A \rightarrow B: &\quad (r_B, B), S_A(r_B, B) \end{aligned}$$

2.1.2 P2P System and Trust

A P2P system is different from the traditional client–server model because the peers work as both clients and servers as stated before. While they can request information to other servers, they also simultaneously have performed the operation of servers and responded to requests for information from other clients. The value of network increases gradually as the number of joining peer grows because it not only takes resources and services from a source, but it also has the ability to share that resources and services with other sources. These resources and services include the transaction of payment, the exchange of information, the sharing processing cycles, the sharing files, etc. The P2P computing has an additional feature that is allowing systems to have temporary associations with one another; having groups of things come to join and be active for a while, and then separate.

Such a P2P system can be categorized largely into pure and hybrid P2P system. The pure P2P shares the data and the resource in equal condition without central server. It dynamically discovers other peers on arbitrary network and interacts with each of them for sending and receiving content. Gnutella[22] and Freenet[19] are typical examples as shown in Fig. 2.1. On the other hand, the hybrid P2P has a central server which has a role about controlling and mediating the peers, but the peers communicate directly each other. Napster[37] is a well-known example of hybrid P2P as shown in Fig. 2.2.

In order to protect "the tragedy of the commons"[24] that also can be applied in digital resources, the authors [14] suggested how the accountability can be achieved by utilizing micropayments and reputations in P2P systems. Accountability measures based on micropayments require that each party offer something of value in exchanging information. Such micropayments can be categorized into nonfungible and fungible

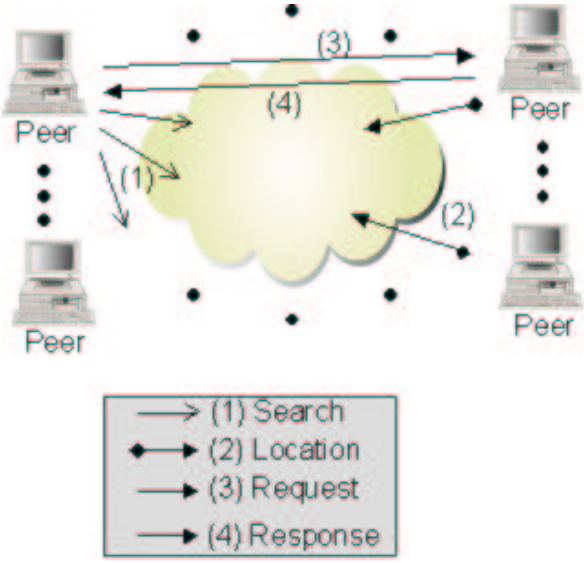

Figure 2.1: Gnutella/Freenet–like system.

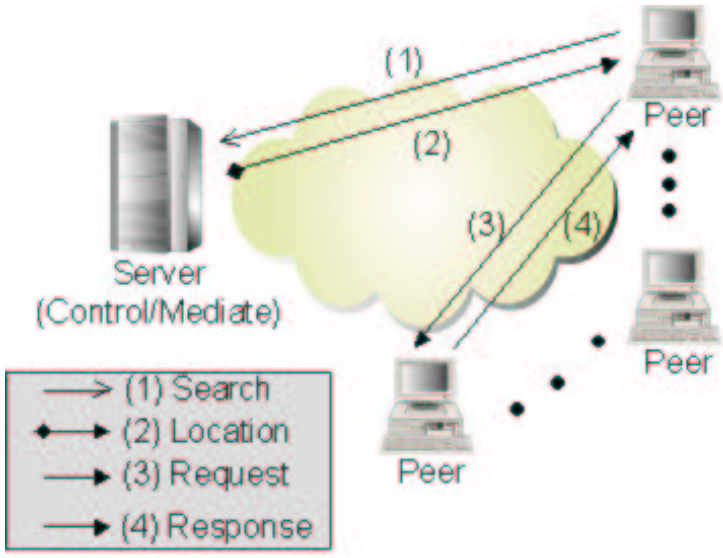

Figure 2.2: Napster–like system.

micropayments. The former does not purchase a real price, however it pays a proof of work(POW), showing that a peer performed some computationally difficult problem; a price via processing in other words. The latter uses commonly a digital cash which can offer a real cash in an exchange. Both of these schemes may be used to protect against resource allocation attacks. For selecting a trustworthy peer, the P2P systems can employ the concept of reputation to ensuring accountability. The advantage of applying the concept of reputation in authentication is to avoid dangerous peer and punish/reward via network. The previous proposal[3, 2] show how reputations and trusts can be adopted in virtual communities which is like P2P communities. Moreover, the JXTA[12] which is to establish such a decentralized trust model and to build a recommendation system from Sun Microsystems and a white paper[31] from OpenPrivacy.org provides a P2P framework for building intercommunicating systems using opinion accumulation based on the concept of reputation. But these works related in reputation concept take an initial step for designing system.

Many researches[47, 34, 33, 30, 43, 44] proposed authentication metric which can be used in formalizing and representing trust relationships between entities. The author of [4] proposed a equation to use formal representation of trust relationships through probabilistic view. We modify and apply this method to trust computing. The detail of trust computing and example are appeared in Chapter III.

2.1.3 Secure Multicasting

Canetti et al.[8] presented solutions to the authentication problem based on Message Authentication Code (MAC) with shared key mechanism which can be regarded as middle–solution between traditional MAC and digital signature. Their basic scheme proceeds as follows:

- S denotes a sender whose a set of l keys, where $R = \{K_1, \ldots, K_l\}$.
- Each of the receivers knows a subset of this set of keys : receiver u knows the subset $R_u \subset R$.
- When S sends a message M it authenticates with each of the keys, using a MAC. That is, a message M is accompanied with $\{\text{MAC}(K_1, M), \text{MAC}(K_2, M), \ldots, \text{MAC}(K_l, M)\}$.
- Each receiver u verifies all the MACs which were created using the keys in its subset R_u. u reject the message M if any of these MACs is incorrect.

This multicast authentication scheme for a single source can be adopted effectively into transmitting recommendation messages from a peer requester to other peer who has connected in the same community with the set of keys.

2.1.4 Overview of Votopia

In this Subsection, we introduce briefly the system design and implementation of the votopia. It is quite natural assumption that all the voters can trust the admin server completely, and anybody can post, but nobody can erase or overwrite the data once written in the bulletin board. We use some cryptographic primitives such as ElGamal cryptosystem, Schnorr digital signature, and Schnorr blind signature. This ensures that the overall security of the votopia is based on the difficulty of solving discrete logarithm only.

Cryptographic Requirements

Many extensive researches [7, 20, 32, 35, 38, 45] on electronic voting have been conducted and an extensive list of cryptographic requirements for

electronic voting is available. In general, we can classify the cryptographic requirements of electronic voting system into the two parts.

Basic Requirements

- Privacy: All votes should be secret.
- Completeness: All valid votes should be counted correctly.
- Soundness: Anyone cannot disturb the voting.
- Unreusability: All voters can vote only one.
- Eligibility: Anyone who is eligible can vote.
- Fairness: Noting can affect the voting.

In general most electronic voting system as well as paper voting system must meet these basic requirements at least.

Extended Requirements

- Walk–away: The voter need not to perform any action after voting.
- Robustness: The voting system should be successful regardless of partial failure of the system.
- Universal verifiability: Anyone can verify the validity of the whole voting process.
- Receipt–freeness: Voter should not be able to prove his or her vote to a buyer. Voter does not have any receipt for the vote to prevent vote-selling.

The universal verifiability and receipt-freeness are of great cryptographic interest, but are guessed to be very expensive for practical implementation. To the best of our knowledge, there is no relevant electronic

voting system which satisfies the basic and extended requirements together. Note that Safevote [6] presents a set of requirements in paper, electronic and Internet voting systems.

Since our goal is to design and implement the Internet voting system to be useful in practical system, universal verifiability and receipt–freeness are ignored to implement. Our design mainly focuses ourselves to provide high efficiency and low communication delay to the Internet voters satisfying with all the basic requirements including walk–away and robustness.

Architecture of the votopia

The votopia has three main stages: registration, voting and counting as most voting systems do. Before initiating these stages, the system parameter including key pairs of each servers except a voter should be generated and distributed by PKI and Java cryptographic library. In order to implement the votopia efficiently, software products made by Korean security industries have been chosen and their functions have been extended to meet the objectives of the votopia such as CA server, Java cryptolibrary, and firewall. And we implemented admin server and bulletin board under Unix system using Apache as a web server, Tomcat as a servlet container and JavaServer Page^{TM} (JSP) implementation. The main part of admin server and bulletin board have been developed by using JSP, JDK1.2, and Java cryptolibrary. Oracle DB is used by admin server to manage a large number of informations of all voters and candidates. Bulletin board also uses an independent DB to handle ballots. All clients must get the voting signed applet which is downloadable program code executed in a web browser of a voter supporting Java. This contains necessary information to support the actual candidate selections. The key size of ElGamal cryptosystem and Schnorr digital signature are fixed to 512-bit for fast computation to a

client side.

2.1.5 Java Mobile Technology

For expanding and implementing mobile voting, Java is an important technology due to the platform–independent characteristics. Sun Microsystems has introduced Java 2 Micro Edition[26](J2ME) is suitable to mobile and handheld devices. J2ME, a highly optimized Java Runtime Environment, is categorized into two different configurations by the size of the virtual machine. For supporting the devices that have limited memory (less than 512KB) and unstable network connection, CLDC(Connected Limited Device Configuration) was designed. This configuration provides the virtual function named KVM that has limited function. In order to support more powerful mobile devices that have over 2MB memory and stable network, CDC(Connected Device Configuration) was designed. In this configuration, fully functional JVM is provided. Running above each configuration are "Profiles"which provide functions to applications. At current status, MIDP(Mobile Information Device Profile) v1.0 on CLDC, Personal Profile on CDC and MIDlet that equally supports the role of applet are available.

2.2 Previous works

2.2.1 Authentication Mechanisms on the current P2P System

In this subsection, we describe various authentication mechanisms for using P2P system till now. But we ignore some typical P2P services such as [19, 13, 49] in here because those services concentrate on providing anonymous publishing called as censorship–resistant publishing system

not authentication mechanism.

There are a number of well-known products available that permit insecure file and resource sharing in P2P. Gnutella[22], which is famous in audio file sharing, identifies a peer with IP address and pseudonym. Kazza[28] and e–Donkey[15] are a software program for sharing any files by identifying each other with their pseudonyms. SETI@Home[46] is typical example of CPU sharing system that also uses pseudonym and IP address for processing the signal.

Napster[37]–like services allow peers to use a central discovery and lookup server to find the location of audio files that can directly be downloaded from other peers. In Napster, weak authentication is supported by user's pseudonym and password. Instant messengers[27, 25, 36, 1], that are widely spread for direct communication on the Internet, also use the password–based authentication.

To provide strong authentication, called challenge–response authentication scheme is utilized into P2P system. The authentication of Groove[23] has two different purposes. One is that their scheme binds users to their electronic identities, and the other is that link actions; such as modification to file, chat message and keystroke to electronic identities. In order to maintain multiple keys, the public/private key pairs are encapsulated in XML tag. The authors of FL02[18] proposed a solution of strong authentication based on reputation management system with PKI. They consider context–dependent feedback gathered in questionnaires.

As mentioned before, current P2P services apply three types for authentication. But all of those authentication mechanisms cannot satisfy various services from file sharing to electronic commerce(EC), also cannot provide the concept of reputation to ensure accountability among peers. Therefore, P2P system needs an adaptive authentication protocol which can accept various services and adopt the concept of reputation.

To the best of our knowledge, there is no relevant authentication mechanism which satisfies considering reputation, providing pseudonymity, guaranteeing strong authentication and minimizing the cost of issuing certificate.

2.2.2 Authentication in Votopia

The authentication of the votopia is performed through registration and voting stage.

In registration stage, a voter downloads a registration form and inputs his information required for certificate issuing. The information is encrypted with admin server's public key and is sent to admin server. Then admin server checks that the voter has the right to vote after decrypting the Information. If the voter doesn't have the right, admin server gives an error message. Otherwise, admin server gives the voter the right to download key generation applet. After donwloading a key generation applet and generating key pairs, the voter keeps his private key in safe storage and sends his public key to admin server to request his certificate. Admin server requests the certificate issuing to CA. CA issues a certificate and store the certificate in DB instead of the voter.

In voting stage, the voter downloads a login applet and provides authentication data (ID and password). Admin server checks whether the voter has already voted or not. If the voter had already voted, admin server rejects the authorization. Otherwise, admin server gives the voter the right to download the voting applet.

2.2.3 Previous Mobile Voting Systems

CyberVote

After European industry initiated to allow the Internet voting in highly secure and verifiable way by using PC, PDA or mobile phones. It will be tested during some trial elections in Germany, in France and in Sweden. The system is based on Cramer et al.'s scheme[11] that aims at guaranteeing universal verifiability without using vote receipts and accuracy of the final tally by multiple-talliers combines the use of PKI for eligible voters registration, system modules (talliers and scrutineers) certification, result time stamping and digital signature, with the use of homomorphic functions and zero knowledge proof to guarantee universal verifiability of the results and voters' privacy. But, the system, especially mobile voters, has communication overhead and computational complexity for proofs of knowledge and validity. So, the system provide no efficiency in voter's point of view.

VoteHere

The system was designed by US company based on Cramer et al.'s scheme. VoteHere guarantees accuracy through multi-authority tabulator, but do not provide an efficiency in mobile devices by the same reason of CyberVote.

Euro–Citi

A European research project started in September 2000. The system will be tested during some trial elections in Greece, England and Spain. The Euro–citi platform is organized to permit system user access either from their home PC or from public places, kiosks, or from GSM terminals. For providing mobile voting, the system just use WAP(Wireless

Application Protocol), WTLS(Wireless Transport Layer Security) and PIN(Personal Identification Number) code.

eVoteSheffield

The eVoteSheffield use mobile SMS (Short Message Service) voting with PIN code. The detailed concept of system did not define yet.

III. An Adaptive Authentication Protocol based on Reputation for P2P System

3.1 Requirements

The requirements of authentication protocol in P2P systems satisfied from pseudonymity to strong authentication to be listed as follows:

R1. Pseudonymity : The purpose of most P2P system is that a peer can easily subscribe, leave and access contents. In a trivial information transaction, a peer might want to hide their information with pseudonym. So authentication for P2P must satisfy this requirement.

R2. Strong authentication: The authentication between each peer must provide cryptographically strong mechanism to support commercial transaction. It must protect transaction between peers from possible attack, such as man-in-the-middle attack.

R3. Reputation : To ensure accountability on P2P network, the concept of reputation must be installed.

R4. Community authenticity : Each community member can recognize whether a message was sent by a community member.

R5. Guarantee : After executing serious commercial transaction between peers, this transaction can be pending in the court if it was wrong. So the requirement of a legal force that can control and settle a dispute is required. It can be achieved by a formal certificate that is guaranteed by legal CA.

R6. Flexibility : It is possible to easily adopt into any P2P systems either pure or hybrid system.

R7. Cost effectiveness : The formal certificate issued by CA needs the issuing cost. If a peer is enough to trust like family, we can request only self-signed certificate. This self-signed certificate need not extra cost.

3.2 Proposed Protocol

The first step of our scheme is to start negotiation to decide selective property such that pseudonymity or strong authentication. For supporting the decision of selective condition, the extra message field is required. This field can contain two types of operation that satisfy conditions. And then it proceeds to the next step of protocol according to the above selective condition. This step consists of two protocols; *Guest* and *Member protocol*. In *Guest protocol*, strong authentication scheme is ignored in order to support pseudonymity that is possible through Gnutella–like authentication using pseudonym. In *Member protocol*, the strong mutual authentication will be executed based on the result of trust value calculation. By using trust value, we can select the relevant certificate. Detailed operation of our scheme will be described in *protocol actions*.

The protocol of the proposed scheme works as follows:

Protocol. ***Adaptive Authentication Protocol based on Reputation*** **(AAPR)**

SUMMARY : A peer α sends a peer β one message that include extra selective field and β responds along the property of the selective field. After β requests recommendation to the remaining peers in the same

community, the remaining peers respond recommendation results. Then β calculates the trust value of α from received recommendations. Using variant certificate appropriate for the trust value, authentication and key establishment are performed. After α and β finish the communication, α and β adjust their trust value respectively.

RESULT : (According to user's choice)

1. The pseudonym–based weak authentication between peers.
2. Mutually strong peer authentication and time-variant session key transport with key authentication using different source of certificate based on trustworthy.

Notation.

The notations of our scheme are summarized in Tables 3.1,3.2 and 3.3.

System setup.

1. A peer chooses given two operations which is a value of selective fields; sel_G or sel_M.
2. Each peer has its public/private key pair for encryption and signature.
3. Existing peers on same community share their key previously.
4. Each peer has the trust value of others within specific category(context).
5. Each peer has own initial weight factor of inclination toward optimistic, intermediate or pessimistic. This factor is used for initiating relationship with new peer.
6. Each peer has the table of recommendation for others. It consists of category(context), the weight factor of category(W_C) and recommendation vector as shown in Table 3.4.

Table 3.1: Cryptographic Notations

x	peer(identity) $x \in \{\alpha, \beta, \Gamma\}$,
	where $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$,
	$\gamma_i \neq \alpha$ and $\gamma_i \neq \beta$ for $i = 1, 2, \ldots, n$.
$x \rightarrow y$	x sends one message to y or Y.
$P_x(m)$	x's public key encryption to message m.
$S_x(m)$	x's private key signature to message m.
r_x	random numbers of x.
K_x	x's session key.
CK	set of community keys, where
	$CK = \{CK_1, CK_2, \ldots, CK_l\}$.
CK_x	x's subset of $CK \equiv CK_x \subset CK$.
$MAC(CK, m)$	keyed Message Authentication Code.
$cert_x$	x's certificate.
F_{cert}	formal certificate issued by legal CA.
I_{cert}	informal certificate issued by service
	provider or super peer node.
S_{cert}	self-signed certificate.
$V_{\{cert_x\}}$	selected x's certificate.

Table 3.2: Notations for Message passing

sel_G	selective message for *Guest protocol*.
sel_M	selective message for *Member protocol*.
$permit_x$	allow x to communicate with
	pseudonym–based authentication.
$refuse$	refuse communication.
$req_{\{m\}}$	request the message m.
C_{BT}	critical business transaction.

Table 3.3: Notations for Trust relationship

R_i	the range of trust, where
	$R_{min} \leq R_i \leq R_{max}$, for $i = 1, 2, \ldots, n$
	$R_{min} = R_1$ =total distrust,
	$R_{max} = R_n$ =complete trust.
V_i	trust value, where $0 \leq V_i \leq 1$
	for $i = 1, 2, \ldots, n$.
W_C	weight factor of category,
	where $0 \leq W_C \leq 1$.
$\overrightarrow{T_x}$	the vector of trust value of x
	$(requestor\ ID, category, target\ ID, V_i)$.
$\overrightarrow{T_{x,\gamma_i}}$	$\overrightarrow{T_x}$ from $\gamma_i \in \Gamma$ for $i = 1, 2, \ldots, n$.
$com(x)$	calculated total trust value of x.

Table 3.4: Example of recommendation table

Category (Context)	Weight (W_C)	Recommendation vector {(trust value, target ID), ...}
MP3FileRead	1.0	{(0.9, Lee), (1.0, Kim), ...}
MP3FileWrite	0.8	{(0.8, Bob), (0.95, Alice), ...}
...	...	.....

Protocol messages.

- ***Guest protocol:***

$$\alpha \rightarrow \beta : sel_G, \alpha \tag{III.1}$$

$$\beta \rightarrow \alpha : permit_\alpha \tag{III.2}$$

- ***Member protocol:***

$$\alpha \rightarrow \beta : sel_M, \alpha \tag{III.3}$$

$$\beta \rightarrow \Gamma : req_{\{\overrightarrow{T_\alpha}\}} | \left[MAC(CK_\beta, req_{\{\overrightarrow{T_\alpha}\}}) \right] \tag{III.4}$$

$$\Gamma \rightarrow \beta : \quad \overrightarrow{T_{\alpha,\gamma_i}} | \left[MAC(CK_{\gamma_i}, \overrightarrow{T_{\alpha,\gamma_i}}) \right] \tag{III.5}$$

$$\beta : \quad \textit{Computing trust} \quad \text{at (III.13).} \tag{III.6}$$

$$\begin{aligned} \beta \rightarrow \alpha : refuse \quad & \text{if} \quad && com(\alpha) \leq R_1 && && \text{(III.7)} \\ req_{\{F_{cert}\}} \quad & \text{if} \quad R_1 < && com(\alpha) \leq R_2 \quad \text{or} && C_{BT} \\ req_{\{I_{cert}\}} \quad & \text{if} \quad R_2 < && com(\alpha) \leq R_3 \\ req_{\{S_{cert}\}} \quad & \text{if} \quad R_3 < && com(\alpha) \leq R_4 \end{aligned}$$

Let $D_\alpha = (r_\alpha, \beta, P_\beta(K_\alpha)), D_\beta = (r_\beta, \alpha, r_\alpha, P_\alpha(K_\beta))$.

$$\alpha \rightarrow \beta : \quad V_{\{cert_\alpha\}}, D_\alpha, S_\alpha(D_\alpha) \tag{III.8}$$

$$\beta \rightarrow \alpha : \quad V_{\{cert_\beta\}}, D_\beta, S_\beta(D_\beta) \tag{III.9}$$

$$\alpha \rightarrow \beta : \quad (r_\beta, \beta), S_\alpha(r_\beta, \beta) \tag{III.10}$$

$$\alpha, \beta : \quad \textit{Adjusting trust value} \tag{III.11}$$

Computing trust.

In order to calculate total trust value of a target peer, we have adopted and modified the probabilistic computing method used in [4]. But any computing method can be applied into our scheme to support flexibility. R_{max}, which can be expanded to any range, the maximum trust value means that β trusts α completely. If a peer can define the range, such as selecting from bad, middle and good, then the value of R_{max} is 3.

- Simple model

  Let the recommendation(indirect) trust value is V_1 where $\alpha \Rightarrow \ldots \Rightarrow \gamma_1$ ($\Rightarrow$: indirect trust), and the direct trust value is V_2 where $\gamma_1 \rightarrow \beta$ ($\rightarrow$: direct trust). Then, the trust value of $\alpha \Rightarrow \ldots \Rightarrow \gamma_1 \rightarrow \beta$ with considering the weight factor of category W_C is

$$com(\alpha) = R_{max} \cdot \left\{1 - (1 - W_C \cdot V_2)^{W_C \cdot V_1}\right\} \qquad \text{(III.12)}$$

- Generalized model

  When a peer requests recommendation to others, multiple recommendation for single target peer can be arrived. All direct and indirect recommendations in same category have to combine in one value. If for each $1 \leq i \leq m$, there are n_i distinct paths from α to β with edge $\gamma_i \rightarrow \beta$, with direct trust values $V_{i,1}, \ldots, V_{i,n_i}$, then combined total trust value with W_C is

$$com(\alpha) = R_{max} \cdot \left\{1 - \prod_{i=1}^{m} \sqrt[n_i]{\prod_{j=1}^{n_i}(1 - W_C \cdot V_{i,j})}\right\} \qquad \text{(III.13)}$$

Protocol actions.

A peer who wants to connect with other peer select initial field from given two operation sel_G and sel_M for negotiate to decide *Guest* or *Member protocol* such that satisfies the following conditions: "strong authentication is not required or required". If an initiator peer α chooses sel_G and sends identifier α in step (III.1), then β sends $permit_\alpha$ in step (III.2). And then α and β can communicate with each other. However, it does not influence their reputations.

If an initiator peer α chooses sel_M and sends identifier in step (III.3), then β requests context–dependent trust vector of α to Γ in same community on step (III.4). After β receives the trust vector from Γ at step

(III.5), β performs the calculation of trust value in step (III.6). β determines which certificate is required. And it can request appropriate certificate or refuse all communication in step (III.7). If $com(\alpha) \leq R_1$ which means total trust value of α less than the degree of total distrust, then β refuses all communication. If $R_1 < com(\alpha) \leq R_2$ or C_{BT} message enabled by β, β cannot trust α and so requests a formal certificate issued by legal CA. $R_2 < com(\alpha) \leq R_3$ means that β has a middle trustworthy to α. β requests informal certificate which is issued from super peer node or control server. The super peer means the leader peer of the community, and the control server represents a kind of server which is managed by a specific P2P service provider. When the trust value meets a condition like $R_3 < com(\alpha) \leq R_4$, β trusts sufficiently α like trust relationship between family. So β requests self-signed certificate to α. Of course, the range of trust value from R_1 to R_4 can be decided by β.

Before step (III.8), the peer α generates random number r_α and obtains a session key K_α, and then sends $V_{\{cert_\alpha\}}$,D_α and $S_\alpha(D_\alpha)$ to β. The peer β verifies the authenticity of $V_{\{cert_\alpha\}}$, extracts α's signature public key, and verifies α's signature on the data D_α. β then checks the identifier and r_α in message of step (III.8). Then β also generates r_β and sends message of step (III.9) to α. The peer α carries out actions analogous to those carried out by β. If all checks succeed, α declares the authentication of β successful, sends message of step (III.10) for verification, and saves key K_β. After receiving the message, β verifies it. If all checks are passed, β declares the authentication of α to be successful, decrypts K_α using its private key, and saves this shared key. Now α and β communicate with each other using session–key.

After completing all communication between α and β, they adjust their trust value respectively. Finally, they insert the trust value of other party into their recommendation table.

Examples of Trust Computing.

We present two examples of trust computing for understanding.

EXAMPLE 1.

We assume that a peer α want to be authenticated by β in category "MP3FileWrite". Let $\alpha \Rightarrow \gamma_1 = V_1$, $\gamma_1 \rightarrow \beta = V_2$, R_{max} of β is 3 and β's $R_1 = 0, R_2 = 1, R_3 = 2, R_4 = 3$. The recommendation table of β is shown in Table 3.5, and the recommendation table of γ_1 is shown in Table 3.6

Table 3.5: Recommendation table of β

MP3FileRead	1.0	{(0.9, γ_1), ...}
MP3FileWrite	0.8	{(0.8, γ_1), ...}
...	...	.....

Table 3.6: Recommendation table of γ_1

MP3FileRead	0.95	{(0.8, β), (1.0, α), ...}
MP3FileWrite	0.7	{(0.9, β), (1.0, α), ...}
...	...	.....

We recall the equation III.12, then we can get

$$\begin{aligned} com(\alpha) &= 3 \cdot \left\{1 - (1 - 0.8 \cdot 0.8)^{0.8 \cdot 1.0}\right\} \\ &= 3 \cdot \left\{1 - (0.36)^{0.8}\right\} \\ &= 3 \cdot 0.442 \\ &= 1.326 \end{aligned}$$

The requested certificate is informal certificate of α due to the condition of the protocol step III.7.

EXAMPLE 2.

We assume that a peer α want to be authenticated by β in category "MP3FileRead". Let $\alpha \Rightarrow \gamma_1 \rightarrow \beta$, $\alpha \Rightarrow \gamma_3 \Rightarrow \gamma_2 \rightarrow \beta$, $\alpha \Rightarrow \gamma_4 \Rightarrow \gamma_2 \rightarrow \beta$, R_{max} of β is 3 and β's $R_1 = 0, R_2 = 1, R_3 = 2, R_4 = 3$. The recommendation table of β, γ_1, γ_2, γ_3 and γ_4 are shown in Tables 3.7, 3.8, 3.9, 3.10, 3.11 respectively.

Table 3.7: Recommendation table of β

MP3FileRead	1.0	{(0.9, γ_1), (0.95, γ_2), ...}
MP3FileWrite	0.8	{(0.8, γ_1), (0.4, γ_2), ...}
...	...	.....

Table 3.8: Recommendation table of γ_1

MP3FileRead	1.0	{(0.95, β), (1.0, α), ...}
MP3FileWrite	0.7	{(0.7, β), (1.0, α), ...}
...	...	.....

Table 3.9: Recommendation table of γ_2

MP3FileRead	0.9	{(0.8, β), (0.9, γ_3), (0.8, γ_4), ...}
MP3FileWrite	0.8	{(0.7, β), (0.9, γ_3), (0.7, γ_4), ...}
...	...	.....

We recall the equation III.13, then we can get

$$com(\alpha) \quad = \quad 3 \cdot \sqrt{(1 - 0.272)(1 - 0.147)}(1 - 0.1)$$

Table 3.10: Recommendation table of γ_3

MP3FileRead	0.9	{(0.9, α), (1.0, γ_2), ...}
MP3FileWrite	0.9	{(0.7, α), (1.0, γ_2), ...}
...	...	.....

Table 3.11: Recommendation table of γ_4

MP3FileRead	0.85	{(0.8, α), (0.6, γ_2), ...}
MP3FileWrite	0.8	{(0.7, α), (0.5, γ_2), ...}
...	...	.....

$$
\begin{aligned}
&= 3 \cdot \sqrt{0.728 \cdot 0.853} \cdot 0.9 \\
&= 3 \cdot \sqrt{0.621} \cdot 0.9 \\
&= 3 \cdot 0.709 \\
&= 2.1276
\end{aligned}
$$

The requested certificate is self–signed certificate of α due to the condition of the protocol step III.7.

3.3 Comparison

In this Section, we compare AAPR with others. The comparison is performed whether satisfy the requirements from *R1* to *R7* for P2P authentication or not.

A challenge–response strong authentication based on certificate, which is self–signed or trusted introducer–signed who has no legal force, is provided by using directly PGP[50] in P2P authentication. And it can be easily adopted in any P2P system because of its flexible trust model

called "web of trust". So, this scheme supports *R2*, *R6* and *R7*, but does not support *R4* and *R5*. And it partially support *R1* and *R3* because of following two reasons. First, if peer can register different e–mail address, then he can manipulate the key pairs that is generated from an identifier(like pseudonym) and e-mail address of peer. Second, to build a key–ring for trust, the trusted PGP users introduce others but it provides only restrict reputation mechanism.

We can apply directly into existing P2P system that the authentication can utilize PKI[42] which the certificate is issued by a legal trustworthy CA. This scheme satisfies *R2* and *R5*. However, the restrict properties like satisfying legal force, existing TTP(Trusted Third Party), paying cost for issuing formal certificate, etc. is the reason that PKI cannot support *R1*, *R3*, *R4*, *R6* and *R7*.

Four requirements(*R2*, *R4*, *R6*, *R7*) are provided with the attributes of Groove network. Because this system support rigorous authentication in specific network for the environment of collaborating work, it does not achieve *R1*. Also this system neither has legal force nor the concept of reputation. So, two requirements(*R3*, *R5*) is not accomplished.

Although the FL02 is designed originally for P2P system with the concept of reputation, it just satisfy two requirements(*R2*, *R3*).

Our proposed scheme supports all requirements: *R1* is achieved by using selective field which can permit restrict power in *Guest protocol*. If a critical business occurs or not enough to trust a peer, we request formal certificate to the peer(*R5*). Our scheme provides certificate–based strong authentication(*R2*), so we meet security from possible attacks like replay, man–in–the middle attack, etc. *R4* is accomplished by using secure multicasting mechanism. Nevertheless our scheme does not need particular server, it can perform well with any server. Because a hybrid P2P is subset of a pure P2P(*R6*). We adopt the concept of reputation to choose safe peer(*R3*) and use variant certificate to minimize

the cost of certificate($R7$). The result of comparison is summarized in Table 3.12. In this table, symbols : ◯, △ and × that mean the degree of supporting the component of requirements by each corresponding scheme : support, partially support and no support, respectively.

Table 3.12: The comparison of authentication for P2P

	PGP	PKI	Groove[23]	FL02[18]	AAPR
R1	△	×	×	×	◯
R2	◯	◯	◯	◯	◯
R3	△	×	×	◯	◯
R4	×	×	◯	×	◯
R5	×	◯	×	×	◯
R6	◯	×	◯	×	◯
R7	◯	×	◯	×	◯

IV. Extension of Votopia to General Internet Voting

4.1 Type of the Internet Voting

There are many voting systems, those are included from paper–based to the Internet voting, for decision making in any society. Here, we describe the type of the Internet voting which can be adapted into decision making in virtual community as follow:

- Voting supervised by government : The voting to elect representatives of nation such as presidential election, plebiscite, etc. This voting needs not only cryptographically strong protocol, but also has legal basis and validity. If a voter want to proof his identity rigorously, he must exhibit formal certificate issued by legal CA.
- Restrict voting : The voting for elect a member of directory in such company, institute, academy, etc. The community which is limited specific area can issue informal certificate for guaranteeing member's identity.
- Internet polling : The voting for a public–opinion poll. The Internet polling with cookie information to prevent double voting is a popular practical system. However, this polling system is very weak in the point of cryptographic view. As a substitute cookie information, we can use self–signed certificate with the seed value which is sent from polling server via network or e–mail.

4.2 Requirements

While preserving the overall architecture of the votopia, we have to consider the following requirements for generalized votopia with serving mobile devices as a voting client:

1. *Cryptographic Requirement* : At least mobile voting must satisfy the cryptographic requirements which was offered by the votopia previously.

2. *Portability* : Generalized votopia have to support any voting system ranging from the Internet polling to plebiscite. This requirement can be supported by using multiple certificate, from formal certificate issued by official CA to self-signed certificate issued by voter himself.

3. *Computational and Communicational Requirement* : To overcome limitation of computational power of mobile devices, most computational work such as key generation for clients should be performed at server side. Only useful information is sent to users. The binary code sent to user must be optimized too. In addition, server side should have a recognizing mechanism which kind of clients is connecting to server.

4. *Device Requirement* : Mobile devices used in the votopia must support TCP/IP protocol stack (regardless of communication media) and Java virtual machine for achieving platform independence.

4.3 Proposed Voting System

In this session, we proposed our design and main protocol step for generalized votopia supporting with mobile voting. For convenience, our

notations are follow:

Notations

- AS : Admin Server.
- CT : Counting Server.
- WS : Web Server.
- $B()$: Blinding function.
- $UB()$: Unblinding function.
- BB : Bulletin board and ballot box.
- VT_i : Voter i.
- vt_i : vote value by VT_i.
- C_i : VT_i's selected certificate.

As shown in Fig. 4.1, our system consists of three stages : registration, voting, and counting stages. The details of each stage as follow:

Registration Stage

(R1) VT_i access AS via WS to download a registration form and certificate manager *Applet* or *MIDlet* as shown in Fig. 4.2. In order to extend the votopia to general purpose, and solve low computational limitation of mobile devices to eliminating key generation, the certificate manager can download and manage various certificate such as simplified certificate for the votopia, official X.509v3 certificate which is issued from CA companies like certificate for Internet banking. VT_i can retrieve official certificate and

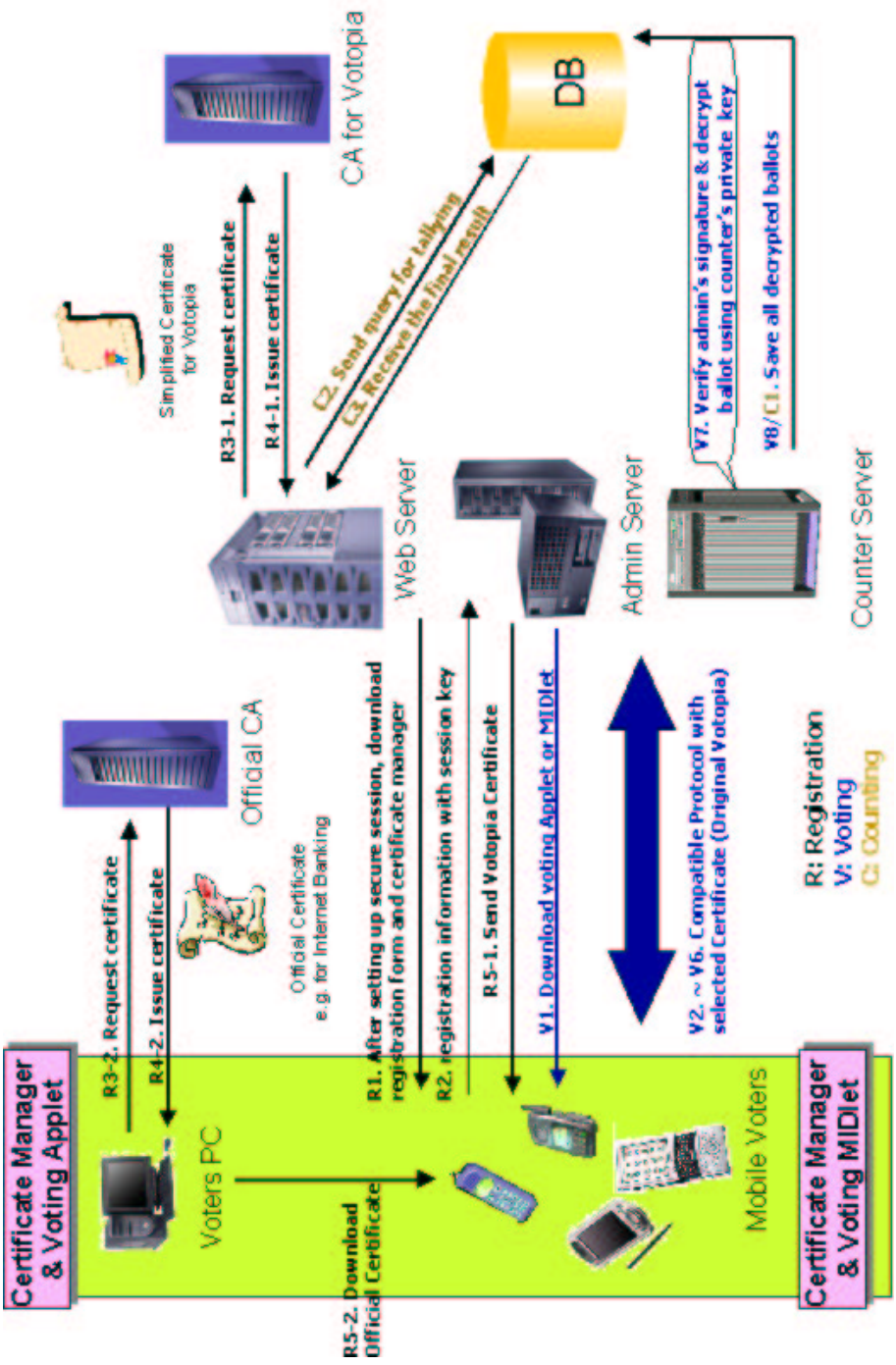

Figure 4.1: Architecture of Generalized Votopia

encrypted private key from stored-data in his computer. And also AS can issue C_i by using VT_i's registration information through CA. All certificate is managed by certificate manager.

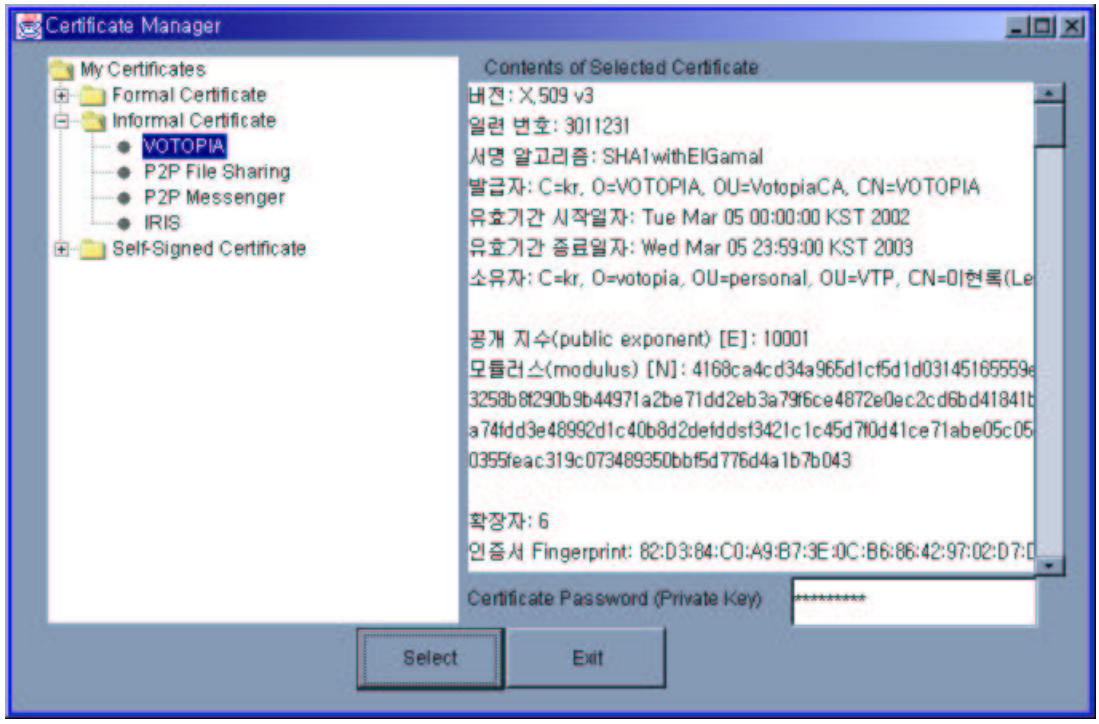

Figure 4.2: Certificate Manager for Generalized Votopia

(R2) After downloading or issuing certificate C_i, VT_i keeps his encrypted private key and certificate in safe storage such as smart card, flash ROM installed in his device, hard disk with encryption using pass–phrase.

(R3) All information that related in voting are passed through secure channel like using SSL. Especially, the registration information of

VT_i is encrypted with AS's public key and is sent to AS. The AS checks VT_i has the right to vote after decrypting the information. If VT_i doesn't have the right, AS gives an error message. Otherwise AS gives VT_i the right to download voting client(*Applet* or *MIDlet*).

Voting Stage

(V1) After downloading voting client to enter voting stage, VT_i provides authentication data (ID, password and selected certificate). AS checks whether the voter has already voted or not. If VT_i had already voted, AS rejects the authorization. Otherwise, AS gives VT_i the right to download suitable voting client.

(V2) Using the voting client, VT_i selects vote vt_i of his choice and encrypts vt_i with CT's public key of the ElGamal encryption as $x_i = E_{CT}(vt_i)$. VT_i blinds x_i as $e_i = B(x_i, r_i)$, where r_i is a randomly chosen blinding factor. VT_i signs e_i as $s_i = S_i(e_i)$ and sends $(ID_i, e_i., s_i)$ to AS.

(V3) AS verifies the signature s_i of message e_i. If s_i is valid, then AS signs e_i as $di = S_A(e_i)$ and sends d_i to VT_i. At the end of the voting stage, AS announces the number of voters receiving AS's signature, and publishes the final list as (ID_i, e_i, s_i).

(V4) VT_i retrieves the desired signature y_i of ballot x_i by $y_i = UB(d_i, r_i)$. VT_i checks whether y_i is AS's signature for x_i. If this check fails, VT_i claims it by showing that (x_i, y_i) is invalid.

(V5) VT_i sends (x_i, y_i) to BB via anonymous channel.

Counting Stage

(C1) CT verifies the signature y_i of x_i. If the verification fails, CT claims that y_i is not a valid signature of x_i and exclude the vote from further steps of the counting stage.

(C2) CT decrypts ballot x_i and retrieves vote vt_i as $vt_i = D_{CT}(x_i)$. CT store the voting results to DB.

(C3) After the period of voting is over, CT publishes the voting results by using BB.

4.4 Comparison

In this Section, we briefly compare generalized votopia(**GV**) with others. The comparison is divided into two parts. The first comparison is performed in points of providing cryptographic requirements(CR)and portability(PO). The second comparison is executed in points of communication overhead(CO) and computational complexity(CC) for consideration of the limitations of mobile devices. Especially, we consider that compare CO and CC in viewpoints of capability of mobile device, not in server side. Also CR is most important factor among all other factors.

Through all voting steps, CyberVote(**CV**), VoteHere(**VH**), Votopia (**VT**) and **GV** was based on cryptographically strong voting scheme such as Cramer et al.'s scheme[11], Ohkubo et al.'s scheme[39], etc., that were satisfied the cryptographic requirements, but eVoteSheffield(**ES**) and Euro–Citi(**EC**) do not meet these requirements. **ES** and **EC** just provide the security in network level with WTLS or PIN code identification. In the point of PO, only **GV** supports it because of applying adaptive authentication based on multiple certificate. Since **ES** and **EC** do not have complex voting step, they are achieved low computational and communication overhead. But, most voting system needs complex

step for generating proof of validity, generating public/private key, etc. So, **CV**, **VH** and **VT** necessarily meet heavy computational and communicational overhead. Because our proposed voting system reduces most operation which is the generation work as stated before in client side, we can attain tradeoff. It can be achieved by committing the operation to server side which has more computational and communicational power rather than client has.

The result of comparison is summarized in Table 4.1. In this Table, we use symbols : ◯, △ and × that mean the degree of supporting CR and PO by each corresponding scheme : support, partially support and no support, respectively. And the symbols : L, M and H that mean low, middle and high complexity, respectively.

Table 4.1: The comparison of the Internet voting system

	CV[10]	**VH**[48]	**ES**[17]	**EC**[16]	**VT**[29]	**GV**
CR	◯	◯	×	△	◯	◯
PO	×	×	×	×	×	◯
CO	H	H	L	L	H	M
CC	H	H	L	L	H	M

V. Conclusions and Future work

For establishing and maintaining virtual community, the most useful approaches are that we can think P2P system as a tool for establishing the community on the Internet, and the Internet voting can be regarded as the way to assert their opinions. However, P2P and the Internet voting system are hesitated people about many security problems. So, we propose an adaptive authentication based on multiple certificate to solve the problems in point of authentication. We can summarized our two contributions as following:

First, the P2P computing can be applied to large scale network for sharing information and resource over a network, which has never seen before. Although this enables rapid progress because of its pseudonymity, the lack of security of P2P system makes them less attractive. As well there is no mutual authentication protocol considering pseudonymity, the concept of reputation and the effectiveness of certificate issuing cost. Hence, we proposed an adaptive authentication protocol based on reputation for P2P system that satisfies the requirements. Moreover, we also consider the context–dependent reputation concept for ensuring accountability and propose briefly the method of computing trust among peers that present the way to select variant certificate from a standard certificate issued by legal CA to a flexible self-signed certificate issued by peer itself. We can conclude that our scheme may solve most of the authentication problems in any type of P2P systems which can be either pure or hybrid one.

Second, the Internet voting system makes people to participate easily in voting. But current voting system, including the votopia, was not suitable for many different types of voting. So we extend original votopia to general version through utilizing multiple certificate. Also we

consider mobile devices, that have limitations in computing resources, therefore voters are able to cast conveniently their vote in any where at any time.

As the future work, AAPR protocol needs that the part of trust measurement and calculation must be extended to be in a more formal way. And also bootstrapping which called as the first initial step of trust relationship is one of open problems. In order to implement completely generalized votopia, further works like binary code optimization that can be downloaded into mobile devices, adapting certificate manager in current voting client, defining the formal location of certificate in user's device must be executed. One of DB tables for saving user's certificate ("voters"table) will be eliminated, and also the part of retrieving public key in admin server for verifying user's signature should be modified.

가상 커뮤니티를 위한 선택적 인증기법에 관한 연구

이현록

인터넷 및 정보기술의 발전으로 인해 많은 사람들이 가상 커뮤니티(Virtual Community)를 만들어 자신의 의견을 표출하고 싶어하는 현상이 두드러지게 나타나고 있다. 이런 가상 커뮤니티를 생성하는 문제에 있어 무엇보다 중요하게 고려할 것은 어떻게 그 커뮤니티를 만들 것인가와 어떻게 커뮤니티에 속해 있는 사람들의 의견을 도출해 낼 수 있는가 하는 점이다. 많은 접근 방법들을 고려해 볼 수 있지만, 가장 유용한 접근방법 중 하나는 피어 투 피어(Peer-to-Peer, P2P) 시스템을 인터넷 커뮤니티 구성을 위한 도구로 보는 것이며, 인터넷투표 시스템(Internet Voting System)을 이용하여 커뮤니티 구성원의 의견을 이끌어 낼 수 있도록 하는 것이다. 하지만 P2P 시스템과 인터넷 투표 시스템을 가상 커뮤니티에 활용하기에는 아직 많은 보안 문제들이 도사리고 있다. 특히 사용자에 대한 인증 문제가 중요한 관심사라 할 수 있겠다.

우리는 본 논문을 통해 효율적인 인증을 제공하는 두 가지의 시스템을 제안하고자 하며, 적응성을 가지는 P2P 인증 프로토콜과 기존에 개발되어 성공적으로 실험을 마친 인터넷 투표 시스템 보토피아(Votopia)를 적응성을 가지는 인증을 기반으로 확장 및 일반화 시켜 나가고자 하는 것이 그 두 가지 시스템의 목표이다.

얼마 전까지만 해도 인터넷상의 통신 기술은 서버 중심의 시스템이 주류를 이루고 있었으나 최근에는 분산 컴퓨팅(Distributed Computing)의 한 종류로 볼 수 있는 P2P 시스템이 각광을 받기 시작하였다. 이런 P2P 시스템은 인스턴트 메세징(Instant Messaging), 협업

컴퓨팅(Collaborate Computing) 등과 같이 활용되고 있을 뿐 아니라 사람들 사이를 이어주는 다리와 같은 기반으로 생각되어 지고 있다. 실제 사람과 사람간의 신뢰 관계와 마찬가지로 각 피어(Peer)들 간에는 무척 복잡한 신뢰 관계를 형성하고 있으며, 이런 관계는 복잡한 보안 문제를 야기한다. 이런 복잡한 문제들 가운데 특히 피어들 간의 인증 문제가 중요하게 부각되고 있는 실정이다. 하지만 P2P 통신망은 그 빠른 확장을 가능하게 했던 가명성(Pseudonymity)을 지원해야 할 뿐만 아니라 향후 상업적으로 활용되기 위하여 강력한 인증(Strong Authentication)까지 포함하는 문제를 안고 있다. 따라서 위와 같은 상반된 조건을 만족시키는 적응성을 가지는 평판 시스템(Reputation System)에 기반한 P2P 인증 프로토콜(Adaptive Authentication Protocol based on Reputation)을 제안하고자 한다. 본 프로토콜은 또한 문맥(Context) 혹은 범주(Category)에 따른 평판을 고려하였으며, 적절한 인증서(Certificate)를 선택적으로 사용하여 인증서 발급시의 비용을 최소화하는 관점에서 작성되었다.

인터넷 투표를 이용하여 많은 사람들의 의견을 모으는 것은 암호 프로토콜 분야 중에 매우 새로운 도전 가능성을 가진 분야이다. 암호 프로토콜을 기반으로 하여 다양한 투표 시스템이 설계되고 구현되었으며, 공개키기반(PKI)기술과 자바(Java)기술을 적용하여 월드컵 최우수선수와 최우수 골키퍼를 선정하는 투표를 통해 실험된 보토피아는 매우 성공적인 인터넷 투표 설계 및 구현 사례이다. 하지만 보토피아는 사용자의 네트워크 환경이 유선으로 연결되어 있으며 성능이 우수한 컴퓨터를 사용한다는 가정과 자체적으로 운영한 인증기관(CA)를 통해 발급 받은 인증서만을 사용하여야만 하는 단점을 가지고 있다. 따라서 본 논문에서는 적응성을 가지는 인증을 통해 인터넷 여론조사에서 부터 실질적인 국민투표에 이르기 까지 활용할 수 있도록 보토피아를 확장하였으며, 이동장치(Mobile device)와 같은 제약적인 조건까지 수용할 수 있도록 하였다.

References

1. American Online Instant Messenger Homepage, *http://www.aim.com/*.

2. A.Abdul–Rahman and S.Hailes, "A Distributed Trust Model", *Proc. of ACM New Security Paradigms Workshop '97*, Cumbria, UK, September 1997.

3. A.Abdul–Rahman and S.Hailes, "Supporting Trust in Virtual Communities", *Proc. of IEEE the Hawaii International Conference on System Sciences*, January, 2000.

4. T.Beth, M.Borcherding and B.Klein, "Valuation of Trust in Open Networks", *Proc. of ESORICS '94*, LNCS 875, pp.3–18, Springer–Verlag, 1994.

5. The BELL Newsletter on Internet Voting, *The Bell*, Vol.1, No.4, Safevote Inc., August, 2000.

6. "Internet Voting Requirements", *The Bell*, Vol.1 No.7,p3, Safevote Inc., November, 2000, *http://www.thebell.net/papers/vite-reg.pdf*.

7. J. C. Benaloh and D. Tuinstra, "Receipt-free secret ballot elections", *Proc. of 26th ACM STOC*, pp.544–553, 1994.

8. R.Canetti, J.Garay, G.Itkis, D.Micciancio, M.Na–or and B.Pinkas, "Multicast Security: A Taxonomy and Some Efficient Constructions", *Proc. of IEEE INFOCOM'99*, vol. 2, pp. 708–716, New York, NY, March 1999.

9. CALTECH–MIT/Voting Technology Project, December, 2002, *http://www.vote.caltech.edu/*.

10. CyberVote Homepage, *http://www.eucybervote.org*.

11. R. Cramer, R. Gennaro, and B. Schoenmakers, "A Secure and Optimally Efficient Multi-Authority Election Schemes", *Advances in Cryptology-Eurocrypt'97*, LNCS 1233, pp.103–118, Springer-Verlag, 1997.

12. R.Chen and W.Yeager, "Poblano: A Distributed Trust Model for Peer-to-Peer Networks", *http://www.jxta.org/project/www/docs/trust.pdf*, Sun Microsystems, 2002.

13. R.Dingledine, M.J.Freedman and D.Molnar, "The Free Haven Project: Distributed Anonymous Storage Service", *Proc. of the Workshop on Design Issues in Anonymity and Unobservability*, LNCS 2009, July 2000.

14. R.Dingledine, M.Freedman and D.Molnar, "Accountability", *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*, Chap.16, pp.271–340, O'REILLY Press, 2001.

15. e-Donkey Homepage, *http://www.edonkey2000.com/*.

16. Euro–Citi Homepage, *http://www.euro-citi.org/*.

17. eVoteSheffield Homepage, *http://evotesheffield.com/*.

18. D. Fahrenholtz and W. Lamersdorf, "Transactional Security for a Distributed Reputation Management System", *EC-Web '02*, LNCS 2455, pp.214–223, Springer-Verlag, 2002.

19. Free Network Project Homepage, *http://freenet.sourceforge.net/*.

20. A. Fujioka, T. Okamoto and K. Ohta,"A Practical Secret Voting Scheme for Large Scale Election", *Advances in Cryptology-Auscrypt'92*, LNCS 718, pp.248–259, Springer-Verlag, 1993.

21. A.Fiat and A.Shamir, "How to prove yourself: practical solutions to identification and signature problems", *Advances in Cryptology – Crypto 1986*, LNCS 263, Springer–Verlag, pp.186–194, 1987.

22. Gnutella Homepage, *http://gnutella.wego.com/*.

23. Groove Networks, "A White paper: Groove Security Architecture", October 2002, *http://www.groove.net/products/workspace/security.html*.

24. Garrett Hardin, "The Tragedy of the Commons", *Science* 162, pp.1243–1248, 1968.

25. ICQ.Com Homepage, *http://web.icq.com/*.

26. Java2ME Homepage, Sun Microsystems, *http://java.sun.com/j2me/*.

27. Jabber Software Foundation Homepage, *http://www.jabber.org/*.

28. KaZaA Homepage, *http://www.kazaa.com/*.

29. Kwangjo Kim, "Result of the 1st Worldwide Internet Voting System", *Proc. of CISC2002*, pp 219–224, Seoul, Korea.

30. R.Levien and A.Aiken, "Attack-Resistant Trust Metrics for Public Key Certification", *Proc. of the 7th USENIX Security Symposium*, San Antonio, Texas, pp.229–241, January, 1998.

31. F.Labalme and K.Burton, "Enhancing the Internet with Reputations : OpenPrivacy white paper", 2002, *http://www.openprivacy.org/papers/200103-white.html*.

32. B. Lee, and K. Kim, "Receipt-free electronic voting through collaboration of voter and honest verifier", *Proceeding of JW-ISC2000*, pp.101–108, Jan. 25-26, 2000, Okinawa, Japan.

33. U.Maurer, "Modeling a Public-Key Infrastructure", *Proc. of ESORICS'96*, Rome, Italy, 1996.

34. S.Mendes and C.Huitema, "A New Approach to the X.509 framework : Allowing a global authentication infrastructure without a global trust model", *Proc. of the 1995 Internet Society Symposium on Network and Distributed System Security*, February, 1995.

35. M. Maichels and P. Horster,"Some remarks on a recirpt-free and universally verifiable mix-type votins scheme",*Advances in Cryptology-Asiacrypt'96* LNCS 1163, pp.125–132, Springer-Verlag, 1996.

36. Microsoft Network Messenger Homepage, *http://messenger.msn.com/*.

37. Napster Homepage, *http://www.napster.com*.

38. V. Niemi and A. Renvall,"How to prevent buying of voters in computer elections", *Advances in Cryptology-Asiacrypt'94*, LNCS 917, pp.164–170, Springer-Verlag, 1994.

39. M.Ohkubo, F.Miura, M.Abe, A.Fujioka and T.Okamoto, "An Improvement on a Practical Secret Voting Scheme", *Information Security'99*, LNCS 1729, pp.225–234, Springer–Verlag, 1999.

40. L. Olson, ".NET P2P:Writing Peer-to-Peer Networked Apps with the Microsoft .NET Framework", *MSDN Magazine*, Feb, 2001.

41. Peer-to-peer working group, "What is peer-to-peer?", *http://www.p2pwg.org/whatis/index.html*.

42. R.Perlman, "An Overview of PKI Trust Models", *IEEE Network Magazine*, pp.38–43, Nov/Dec, 1999.

43. M.K.Reiter and S.G.Stubblebine, "Resilient authentication using path independence", *IEEE Transactions on Computers*, Vol.47, pp.1351–1362, 1998.

44. M.K.Reiter and S.G.Stubblebine, "Authentication Metric Analysis and Design ", *ACM Transactions on Information and System Security*, Vol.2, No.2, pp.138–158, 1999.

45. B. Schoenmakers,"A Simple Publicly Verifiable Secret Sharing scheme and its Application to Electronic Voting", *Advances in Cryptology-Crypto'99*, LNCS 1666, pp.148–164, Springer-Verlag, 1999.

46. SETI@Home:The Search for Extraterrestrial Intelligence at Home, *http://setiathome.berkeley.edu/*.

47. A.Tarah and C.Huitema, "Associating Metrics to Certification Paths", *ESORICS'92*, LNCS 648, pp 175–189, Springer-Verlag, 1992.

48. VoteHere Homepage, *http://votehere.com/*.

49. M.Waldman, A.D.Rubin and L.F.Cranor, "Publius: A Robust, Tamper-evident, Censorship-resistant, Web Publishing System", *Proc. of 9th USENIX Security Symposium*, pp.59–72, August, 2000.

50. P.Zimmermann, "PGP 7.0 User's Guide", *http://www.pgpi.org/doc/guide/7.0/*.

Acknowledgement

I would like to take this opportunity to acknowledge and thank all of the people who have helped me through the research involved in producing this thesis. First, I would like to thank my advisor, Prof. Kwangjo Kim, for his encouragement and guidance during my graduate studies. He always has shown his consistent affection and encouragement for me to carry out my research and life in ICU. I would like to express my gratitude to the members of my thesis committee, Prof. Junghee Cheon and Prof. Chulsoo Lee, for their counsel and assistance.

I sincerely thank all of the current and former members of the cryptology and information security Lab. : Jongseong Kim, Wooseok Ham, Hyungki Choi, Kyusuk Han, Byunggon Kim, Songwon Lee, Hwasun Chang, Jaehyrk Park, Soogil Choi, Juhyung Lee, Vo Duc Liem from Vietnam, Yan Xie and Zhang Fangguo from China, Diviyan Munirathram from India, and former members : Byoungcheon Lee, Manho Lee, Myungsun Kim, Kookwhan Ahn, Jinho Kim and Jaegwan Park, for their help and friendship over the last two years. I spent a great deal of time at lab and my labmates are like my family. In addition, I want to thank all members of advanced cryptology Lab. : Sangbae Park, Jungyun Lee, Sangwon Lee, Jin Kim, Junbaek Ki, Chuljoon Choi, Sungjoon Min, Joongman Kim, and Yunkyoung Jeong, for their friendship and for putting up with me.

I also appreciate my great friends and all members of the special gathering, Manbam : Taeup No, Joonhyung Ahn, Jiwan Jeon and Sangkyu Lee; and Hangil Kim, Chulun Lee, Jongok Kim, Myungjin Lee and Jeonghan Kang. I cannot forget their endless concerns and encouragement.

I am grateful to my seniors, fellow students and juniors of Pusan National University : Nakwoon Sung, Kyusung Cho, Daeseok Choi, Seungmo Je, Bongjoon Huh, Shinhaeng Kim, Kiwan Park, Hyojoon Kim, Hyunyoung Chung. And my special thanks also goes to Prof. Jungtae Lee in network Lab. of PNU.

Last but not least, my love and thanks to my parents for endless affection and devotion. And I also give my love to my grandmother, younger sister and brother. I cannot forget their endless trust and constant encouragement on me. My uncle, aunt and cousins also give me warm–hearted concerns. I hope God bless my family and to be happy.

Finally, I will always remember the life of ICU. It filled up my poor knowledge and made me a grown–up person.

Curriculum Vitae

Name : Hyunrok Lee

Date of Birth : Nov. 14. 1975

Sex : Male

Nationality : Korean

Education

1994.3–1999.2	Computer Engineering Pusan National University (B.E.)
2001.3–2003.2	Cryptology and Information Security, Engineering Information and Communications University (M.S.)

Career

2002.1–	Graduate Research Assistant Supporting special education for the gifted person Education Center for IT Gifted Person, ICU
2002.1–	Graduate Research Assistant Middleware(8)

2002.2–	Graduate Research Assistant Cultivation of Top Level IT Security Manpower The Ministry of Information and Communications(MIC)
2002.4–2002.12	Graduate Research Assistant Research on Easy Security Technology Electronics and Telecommunications Research Institute(ETRI)
2001.2–2002.7	Graduate Research Assistant Development of Electronic Voting System for World-Cup 2002 Information Research center for Information Security, ICU Electronics and Telecommunications Research Institute(ETRI)
2001.2–2001.8	Graduate Research Assistant Study on Enabling Technologies for Next Generation Public Key Infrastructure SECUi.COM
2001.7–2001.8	Apprentice Researcher Electronic Commerce Research Team, Computer Software Institute, Electronics and Telecommunications Research Institute(ETRI)

Academic Experience

2002.4–	KIISC student member

2002.6–2002.8 Participate ISRI–ICU Program in Electronic Commerce
Carnegie Mellon University, Pittsburgh, PA, USA

Publications

Papers

(1) 2002.1 Manho Lee, Hyunrok Lee and Kwangjo Kim, "A Micro-payment System for Multiple-Shopping", *2002 Symposium on Cryptography and Information Security*, vol 1/2, pp.229–234, Shirahama, Japan, Jan.29 – Feb.1, 2002.

(2) 2002.11 Hyunrok Lee, Duc Liem Vo and Kwangjo Kim, "Extension of Votopia to Mobile Voting", *KIISC 종합학술발표회(CISC2001)*, 종합학술발표논문집, pp.225–229, 항공대학교, 한국, 2002, 11.

(3) 2003.1 Hyunrok Lee and Kwangjo Kim, "An Adaptive Authentication Protocol based on Reputation for Peer-to-Peer System", To appear in the *2003 Symposium on Cryptography and Information Security*, Hamamatsu, Japan, Jan.26 – 29, 2003.

(4) 2003.1 Hyunrok Lee and Kwangjo Kim, "An Adaptive Authentication Protocol for Peer-to-Peer System", Submitted to *Journal of KIISC*.

Domestic Software Registration

(4) 2002.11 이현록, 김광조, 김진호, 김종승, 김명선, 함우석, "안전한 인터넷투표 시스템을 위한 투표 관리 서버 프로그램".

(5) 2002.11 이현록, 김광조, 김진호, 김종승, 김명선, 함우석, "안전한 인터넷투표 시스템을 위한 유권자 관리 서버 프로그램".

(6) 2002.11 이현록, 김광조, 김진호, 김종승, 김명선, 함우석, "안전한 인터넷투표 시스템을 위한 집계 서버 프로그램".

(7) 2002.11 이현록, 김광조, 김진호, 김종승, 김명선, 함우석, "안전한 인터넷투표 시스템을 위한 유권자 프로그램".