

Efficient and Secure Authentication Protocols for Mobile VoIP Communications

Huang-Ju Chen
Department of Information
Engineering and Computer
Science
Feng Chia University
Taichung, Taiwan

Jyh-Ming Huang
Department of Information
Engineering and Computer
Science
Feng Chia University
Taichung, Taiwan

Lei Wang
Department of Electrical
Engineering
Feng Chia University
Taichung, Taiwan

Abstract

Mobile Voice over IP (Mobile VoIP) allows mobile users to continuously talk with each others while roaming across different networks. In such wireless application, it is vulnerable to information security. In this paper, we present two efficient and secure authentication protocols for mobile VoIP services. In our approaches, we first develop a secure authentication protocol for mobile IP registration procedure. And then, based on this authenticated process, we extend the similar concept to a SIP-based VoIP service, and thus propose the second simple and secure communication protocol. For verifying our contributions, we demonstrate our proposed protocols secure and efficient: (1) by conducting security analysis on the aspects of data integrity, confidentiality, and several common network attacks, such as replay, man-in-the-middle; and (2) by conducting simulations and showing comparison results with other existing protocols, in terms of the communication and computation overheads imposed on the mobile node. All results point out that our protocols are superior to others.

Keywords: Authentication, wireless security, Mobile IP, VoIP, SIP

1. Introduction

With the rapidly developing of wireless communication technologies, several portable devices like handsets and notebooks equipped with wireless LAN cards can easily access the Internet anytime and anywhere. In such a wireless communication environment, user mobility is an important feature. In order to avoid interrupting the ongoing data session, Mobile IP was proposed to enable the mobile user to maintain his connectivity while moving from one attachment point to another [22], [23].

Traditionally, voice information is always transmitted over Public Switched Telephone Network (PSTN). In recent years, Voice over IP (VoIP) service that unites the telephony (e.g. phone calls, fax calls, and voice traffic) and Internet data worlds has become a popular trend.

Internet telephony requires the communicating partners to find each other and to signal to the other parties they desire to communicate. There are two competing protocols emerged for Internet telephony signaling and controls. One is the International Telecommunications Union (ITU) Recommendation H.323 [9], and the other is the Internet Engineering Task Force (IETF) Session Initiation Protocol (SIP) [3]. Currently, the evolution of VoIP service is gradually towards a cordless (mobile) Internet. There have been much research efforts spreading over different protocol layers for the mobility supporting of VoIP applications [2], [16], [18], [19], [20], [29].

Since wireless data transmission is broadcast in nature, anyone within the transmission range of a wireless device can easily intercept the packets without interrupting the data flow. A key concern with wireless communications is information security and privacy. Message authentication is a mechanism provided for allowing communicating parties to verify their received messages, and thus can be used to prevent from many network attacks, such as replay attacks and falsification. Many different authentication schemes were proposed. In [14], [17], the authors developed mechanisms to authenticate the received messages via a smart card. Even these card-based schemes can work with a high speed, an additional hardware supporting is necessary. Public-key-based strategy is another approach used for message authentication [1], [11]. Although this method can provide a higher security protection than other schemes, it will significantly degrade the system performance, due to its complicated encryption/decryption computation overheads. Hybrid authentication schemes, based on the integration of secret and public keys, were also proposed by [5], [12], [21], [28]. In their schemes, the complicated encryption and decryption computations imposed on the mobile nodes have been eliminated. In addition, no additional hardware support is required.

For those reasons as stated before, in this paper, we focus on the interesting research topic of how to provide an acceptable secure mechanism for mobile VoIP service. In our approach, we first integrate Mobile IP with VoIP functions to form the mobile VoIP service, and propose an

efficient and secure hybrid authentication protocol for Mobile IP registration procedure. Our authentication protocol is based on the Sufatrio and Lam's ones [28], but with less computation loads imposed on the mobile node. Then, we extend the similar concept to a SIP-based VoIP service, and present the second simple authentication procedure to achieve the security requirements on the voice information. For evaluating the merits of our proposed protocols, we give a detail cryptanalysis on the aspects of data integrity, confidentiality, and several common network attacks, such as man-in-the-middle and replay. Moreover, we also compare our authentication protocols with existing others. As will be seen in Section 4, the comparison results show that, under the same security level, our authentication protocols are superior to some existing schemes, in terms of the communication and computation costs imposed on the mobile node.

The rest of this paper is organized as follows: in Section 2, we first briefly review some background knowledge related to this research topic. We then describe in detail our proposed secure authentication protocols in subsequent section. Section 4, we conduct the security analysis for our authentication protocols, and make performance comparisons with other existing related protocols. Finally, concluding remark and future work are drawn in Section 5.

2. Background

Before describing our authentication protocols, it should be helpful to reviewing some background materials related to the topics of Mobile IP, VoIP, and authentication.

2.1 Mobile IP Review

Traditionally, IP routing is always performed on a static IP address basis for an end user. In response to the increasing popularity of mobile computers, the Internet Engineering Task Force (IETF) designed the Mobile IP to provide the routing service for a mobile host with dynamic address [22], [23]. In Mobile IP, a mobile node (MN) is initially assigned to a particular network (named as home network) and a predefined IP address (termed as home address). When a mobile node moves from its original home network to another network (called foreign network), it is responsible for listening agent advertisement messages, and making its presence known by registering with a node (known as foreign agent FA) on the visited network. The mobile node then uses a registration procedure to inform its home agent (HA) of its care-of address (CoA). The care-of address identifies the current foreign agent's location. The registration procedure will control the IP tunneling and IP forwarding configuration. Tunneling is used to forward IP datagrams from a home address to a care-of address. After a successful registration, the home agent can be able to intercept and forward IP datagrams that were sent to the mobile node's home address via tunneling. Fig. 1 shows a

standard Mobile IP registration and IP tunneling scenario. The correspondent node is abbreviated as CN.

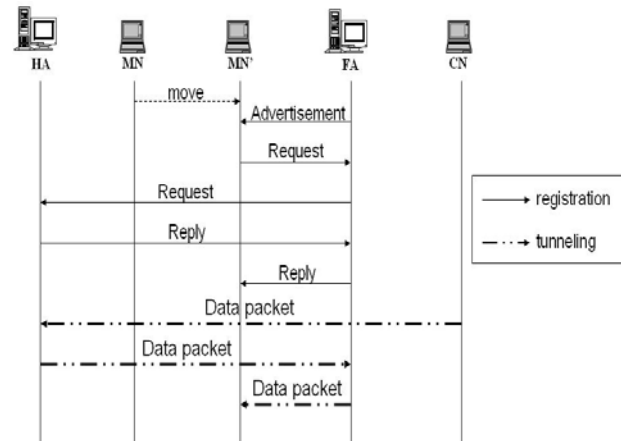


Fig. 1 Mobile IP registration and IP tunneling

2.2 VoIP Review

Voice over IP (VoIP) is an emerging technology that allows people to talk with each other via the Internet, instead of traditional PSTN network. In general, VoIP usually segments the voice information into a series of packets, and transmits them over an IP-based network. The segmented packets will be finally reassembled for listening at the receiving end.

Two major protocol stacks for VoIP service are ITU Recommendation H.323 [9] and the IETF Session Initiation Protocol (SIP) [3]. H.323 is an integrated suite of protocols for voice, video and data communications over packet-based network. It embraces the more traditional circuit-switched approaches which are based on the ISDN Q.931 protocol [10] and earlier H-series recommendations [6], [7], [8]. The weakness of H.323 protocol comes from its complexity and the lack of flexibility.

The SIP architecture contains several types of servers, such as proxy server, redirect server, registrar server, and location server [25]. Proxy server handles requests and forwards them to the other servers. Redirect server maps the destination address to zero or more new addresses. Registrar server deals with the SIP registration procedure. It is responsible for booking the users' location message to a location server. Location server serves as a database in that the location information of all users are stored. A caller can obtain the current location message of his correspondent callee, by querying the location server. A SIP session establishment procedure can be described as follows.

Before the SIP session is established, both caller and callee must register their current locations to the location server. While a caller initially sends a SIP invite message to a SIP server (e.g. proxy server or redirect server), the SIP server will forward this invite message to a location server for obtaining the correspondent callee's address.

After that, the caller destines his invite message to the callee. Upon receiving the invite message, the callee sends back an acknowledgement message for agreeing on this invitation. The communicating parties begin their voice communication services after the SIP signaling procedure is accomplished. Many benefits, such as extensibility, multi-party service flexibility, ease of interoperability, and development simplicity, make SIP more attractive. In this paper, we therefore integrate Mobile IP with a SIP-based VoIP service to explore our secure authentication protocols.

2.3 Authentication Schemes Review

In traditional authentication schemes, clients are always requested to handle encryption and decryption computation tasks, and thus are responsible for preventing from various security attacks. Such solutions are workable if powerful devices are used. However, in wireless communications, since mobile devices are usually limited on power and computation capabilities, authentication strategies used in the wired environment cannot be directly applied to such cordless applications. How to develop secure and power-saving protocols becomes a challenge.

In Mobile IP, as a form of remote redirection, the registration process is very critical and must be guarded against any malicious attack. Pure secret-key based authentication procedure in Mobile IP is not a scalable approach [21]. Thus, Jacobs proposed a certificate-based public-key cryptography authentication protocol for Mobile IP registration [11]. He defines a new certificate extension message format intended to carry certificate information. Jacobs's protocol mainly suffers from the complicated public-key cryptography operations on the mobile node. In order to get rid of the shortcoming discovered in Jacobs's protocol, Sufatrio and Lam presented a hybrid authentication scheme [28]. Their scheme, in one hand, makes use of the secret key cryptography to minimize the computing power consumptions and administration cost imposed on the mobile node, on the other hand, it offers the benefits of scalability and non-repudiation, via the usage of public key cryptography, and maintains the compatibility with the original Mobile IP and other authentication extension protocols. These merits make the mobile users more flexible to choosing such authentication scheme. Based on the similar concept and procedures presented in Sufatrio and Lam's protocol [28], in this paper, we propose a revised authentication protocol for mobile IP registration, but with less computation overheads induced on the mobile node. We qualitatively and quantitatively compare our protocols with other existing and Sufatrio and Lam's schemes. All comparison results show that our protocols can save much computation time spent on the mobile node.

3. Design of our Protocols

In this section, we describe the design philosophy of our proposed secure and efficient authentication protocols in detail.

3.1 System Model and Notations

The system model is shown in Fig. 2. With this system model, we make the following assumptions.

- A Certificate Authority (CA) is responsible for issuing certificates to location server, HA, FA, and SIP servers.
- A centralized public key infrastructure (PKI) is available.
- All servers (SIP) and agents (HA, FA) possess X.509 public key certificates [4], [30], and can authenticate each others via their certificates.
- A predefined secret key S_{HA-MN} and random number R are shared by HA and MN.

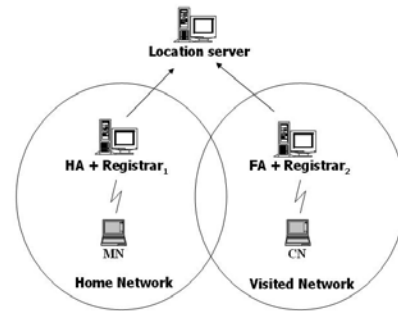


Fig. 2 The system model

In addition, Table 1 interprets the notations that will be used in our authentication scheme.

Table 1. Notations list

| Notations | Descriptions |
|-----------------------|---|
| $M N$ | Concatenation of two messages M and N, in the order specified |
| MN_{HM} | MN's home address |
| CoA_{MN} | MN's care-of-address |
| ID_{HA} | HA's IP address as its ID |
| ID_{FA} | FA's IP address as its ID |
| N_{MN}, N_{FA} | Nonce issued by MN and FA, respectively |
| $[M]_K$ | Encryption of message M under key K |
| $\langle M \rangle_K$ | MAC value of message M under key K |
| S_{HA-MN} | Secret key pre-shared by HA and MN |
| ADV | Advertisement indicator |
| REQ | Request indicator |
| REP | Reply indicator |
| RES | The result of the request |
| K-REQ | Session key request indicator |
| K-REP | Session key reply indicator |
| SK_{MN-FA} | Secret key shared by MN and visited FA |
| R | Random number issued by HA |
| $Cert_A$ | Certificate of entity A |
| KU_A | Public key of entity A |
| KR_A | Private key of entity A |

A X.509 certificate contains the user's public key and other information and a CA signature for this information. The following instance indicates a certificate of entity A ($Cert_A$).

$$Cert_A = \{ID_A, KU_A, Date_A, LF_A, [ID_A, KU_A, Date_A, LF_A]KR_{CA}\}$$

Where ID_A denotes the identity of entity A, $Date_A$ means the issue date of the certificate to A, and LF_A is the lifetime of A's certificate. ID_A , KU_A , $Date_A$, and LF_A are signed by the CA, using its private key KR_{CA} .

3.2 Authentication Protocol for Mobile IP Registration

In this subsection, we first demonstrate our efficient and secure authentication protocol for Mobile IP registration procedure. And then, we apply the similar concept to a SIP-based VoIP service to develop another authentication protocol in subsequent section. Fig. 3 depicts our secure authentication procedure used in Mobile IP registration process.

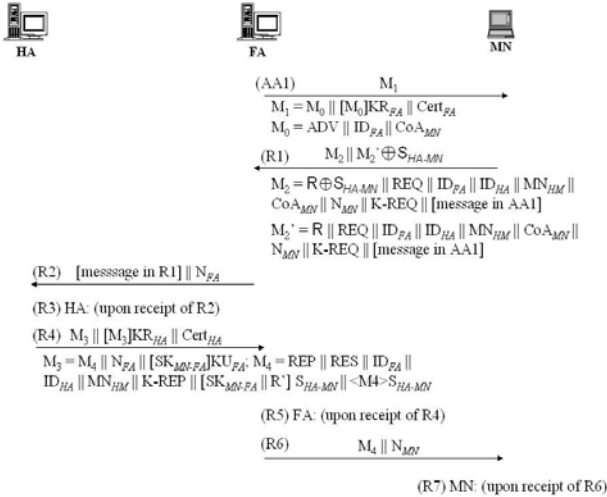


Fig. 3 The proposed authentication procedure for Mobile IP registration

This procedure involves two phases: agent advertisement (AA1) and registration (R1 – R7) phase. The detail steps for each phase are explained as follows.

- Agent Advertisement phase

(AA1) FA periodically sends and signs its advertisement message (M_1). The advertisement message contains FA's IP address, care-of address (CoA), and encrypted with its private key. The certificate of FA can provide HA to authenticate the identity of FA.

- Registration phase

(R1) When received an agent advertisement message from FA, the mobile node (MN) can retain the CoA in this message, and send a registration request message to register with its HA. The

(R2)

(R3)

(R4)

(R5)

(R6)

(R7)

3.3 Authentication Protocol for SIP-based VoIP

After successfully registered to the HA, MN may start the VoIP session initiated procedure. To ensure the mobile VoIP service to be secure as well, we extend the design concept of our secure authentication registration protocol to develop the secure session communication procedure for mobile VoIP service. Fig. 4 shows the mobile VoIP session establishment procedure.

First of all, the MN (e.g. caller) sends an encrypted invite message to a SIP server that might locate on the HA, the invite message then will be forwarded to the location server for deriving the current location of the callee (e.g. correspondent node (CN)). The invite message is protected by providing the corresponding certificate, and encrypted with the public key. After receiving the response message from location server, the MN can be able to deliver the invite message to the FA which the CN is attaching to. The FA then encrypts this invite message, with the shared session key SK_{CN-FA} just obtained from HA in the Mobile IP registration procedure, and forwards it to the CN. The CN returns an acknowledgement to agree with the invitation. Based on the previous secure Mobile IP authentication registration protocol, the security targets at mobile VoIP service should also be achieved.

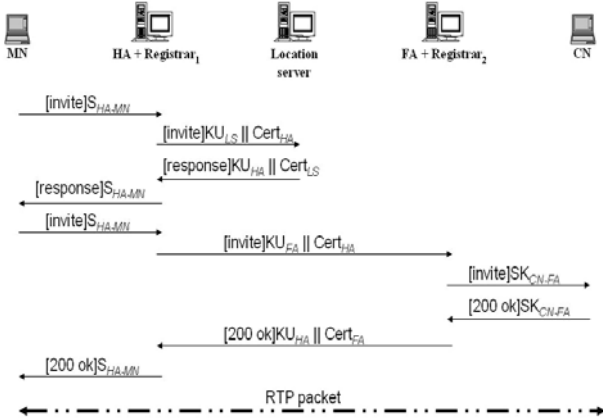


Fig. 4 Mobile VoIP session establishment procedure

4. Security Analysis and Performance Comparison

To claim our proposed secure and efficient authentication schemes practical, we conduct the security analysis, in this section, on the aspects of data integrity, confidentiality, non-repudiation, man-in-the-middle attack, and replay attack. In addition, we also make performance comparisons with other existing authentication protocols. All results show that our authentication protocols can not only achieve an acceptable security level, but also outperform the others, in terms of MN's communication and computation overheads.

4.1 Security Analysis

- **Integrity**

Data integrity checking can assure that the transmitted information was not modified by malicious attackers. In our mobile IP registration protocol, we first utilize the encrypted data $(M_2' \oplus S_{HA-MN})$ for achieving the message integrity in procedure (R1). Since only both the specific HA and MN have the exactly pre-shared keys (R and S_{HA-MN}), the attackers can not modify and reconstruct message M_2' . Moreover, we further use a secret-key based HMAC algorithm [13] to ensure the data integrity in procedure (R4). Therefore, if the packets were modified by attackers during transmission, they can be easily detected by the intended receiver.

- **Confidentiality**

Confidentiality implies that the transmitted data cannot be read out by illegal users except the intended communicators. In our protocols, we use the shared key S_{HA-MN} to encrypt the transmitted packets between HA and MN, and apply a secure session key SK_{CN-FA} to communicate with FA and MN. So, the data confidentiality can be assured.

- **Non-repudiation**

For each time, while the communicating party (HA or FA) sends out his message, the certificate of the sender will be appended. Since the certificate always contains the sender's private key, based on the concept of public key, the sender can not deny the message that was sent by him. As a result, the non-repudiation property is retained.

- **Resistance to Replay Attack**

Replay attack means that an attacker re-sends the message he captured on the network to spoof the authentication mechanism of a server. During the communication period, if the same ciphertexts are used more than once and without involving any protection scheme, adversaries could easily tackle these messages and illegally replay them. In our authentication protocols, we alternatively use the values R and R' associated with HA and MN, and the nonce values with MN and FA to resist replay attacks.

- **Resistance to Man-in-the-Middle Attack**

Man-in-the-middle attack means the communication procedure and exchanged data are monitored, captured, and controlled by the third party. This attack is somewhat similar to the identity spoofing attack. In our proposed authentication protocols, adversaries can not forge the message from MN or HA without the pre-shared values R and S_{HA-MN} . So thus our protocol can resist the man-in-the-middle attack.

4.2 Performance Comparison

In addition to the security analysis as described before, from the point view of resource usage, it is crucial to

minimize the computation overheads imposed on the mobile node, for wireless communications. For verifying the effectiveness of our proposed authentication protocols, we make comparisons with other existing protocols, in terms of the number of HMAC operations, the number of symmetric encryptions and decryptions, the number of asymmetric encryptions and decryptions, and the number of exchanged information issued by the mobile node. The following table shows the results.

Table 2. Computation overheads imposed on the mobile node for some existing protocols

| | Jacob's protocol | Sufatrio and Lam's protocol | Proposed protocol |
|--|------------------|-----------------------------|-------------------|
| The number of HMAC operation | 0 | 2 | 1 |
| The number of symmetric encryption/decryption | 0 | 1 | 1 |
| The number of asymmetric encryption/decryption | 4 | 0 | 0 |
| The number of exchange information at user | 1 | 1 | 1 |

Table 2 shows that our protocol is more practical and efficient than the others, in terms of communication and computation costs. The main difference between our protocol and Sufatrio and Lam's ones comes from HMAC computation times. Instead of using HMAC operation as Sufatrio and Lam's protocol, we use twice exclusive-or operations on (R1) message processing, and thus save the HMAC operation one times. Since an HMAC operation contains at least twice exclusive-or and other operations [26], our protocols can be thought with less computation cost. This improvement is expected to be significant for mobile nodes with limited computational resources.

In order to quantify the real time spent on our registration protocol and Sufatrio and Lam's protocol, we also conduct simple simulations to evaluate the execution times for HMAC and twice exclusive-or operations used in (R1) message processing. We ignore to count the message concatenation times because of those operations are trivial, compared to the other operations. Our experimental environment is based on Mobile Intel Pentium4 1.80 GHz 32-bit processor, and with Microsoft Windows XP operating system. The simulation programs are executed in Microsoft Visual C++ 6.0. We also utilize the QuickHash library functions [27] to calculate the execution time for HMAC operation (take HMAC-MD5 as an example). The simulation result shows that our protocol spends about 0.57223 microseconds on (R1) message processing, in contrast to about 775 microseconds spent on HMAC-MD5 operation used in Sufatrio and Lam's protocol.

5. Conclusion and Future Work

In this paper, we integrate Mobile IP and Voice over IP (VoIP) functions to make mobile VoIP service feasible.

For supporting a secure wireless communication environment, based on the Sufatrio and Lam's scheme [28], we propose two efficient and secure authentication protocols. One is for Mobile IP registration procedure, and the other is applied to SIP-based VoIP applications. Both protocols are built on the integration of certificates and simple key operations. Through the security analysis, we argue that our proposed protocols can not only satisfy many basic security requirements, but also prevent from some well-known network attacks. For verifying the effectiveness of our protocols, we qualitatively and quantitatively compare our protocols with some existing others, especially with Sufatrio and Lam's ones. The comparison results indicate that our authentication protocols are superior to other similar existing schemes, in terms of the computation and communication overheads imposed on the mobile node.

Currently, we are striving to transfer our protocols to a real mobile VoIP platform, and conduct further practical testings. In the near future, we would like to extend our proposed protocols to a movable subnet [15]. In such a movable subnet, mobile agents will be additionally included to support mobility property.

6. References

- [1] A. Aziz and W. Diffie, "Privacy and Authentication for Wireless Local Area Networks," IEEE Personal Communications, 1994, pp. 25-31.
- [2] H. Fathi, R. Prasad, and S. Chakraborty, "Mobility Management for VoIP in 3G Systems: evaluation of low-latency handoff schemes," IEEE Wireless Communications, 2005, pp. 96-104.
- [3] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: Session Initiation Protocol," IETF RFC 2543, 1999.
- [4] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X. 509 Public Key Infrastructure Certificate and CRL Profile," IETF RFC 2459, 1999.
- [5] Z. X. Huang, "An Anonymous Authentication Protocol and Security Scheme of Mobile IP," Master thesis, Department of Electrical Engineering, Chung Yuan Christian University, 2004.
- [6] ITU-T Recommendation H.225.0, "Call Signaling Protocols and Media Stream Packetization for Packet-based Multimedia Communication Systems," 1996.
- [7] ITU-T Recommendation H.245, "Control Protocol for Multimedia Communication," 1996.
- [8] ITU-T Recommendation H.261, "Video Codec for Audiovisual Services at p x 64 kbit/s," 1993.
- [9] ITU-T Recommendation H.323, "Packet-Based Multimedia Communications Systems," 1998.
- [10] ITU-T Recommendation Q.931, "ISDN User-network Interface Layer 3 Specification for Basic Call Control," 1998.

- [11] S. Jacobs, "Mobile IP Public Key Based Authentication," Internet Draft, <draft-jacobs-mobileip-pki-auth-00.txt>, 1998.
- [12] J. K. Jan and Y. H. Chen, "A New Efficient MAKEP for Wireless Communications," Proceedings of the 18th International Conference on Advanced Information Networking and Application, 2004, pp. 347-350.
- [13] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," IETF RFC 2104, 1997.
- [14] C. C. Li, M. S. Hwang, and W. P. Yang, "A Flexible Remote User Authentication Scheme Using Smart Cards," ACM SIGOPS Operating Systems Review, 2002, pp. 46-52.
- [15] C. W. Liao, "Movable Subnet Enhancement in Mobile IPv4 Environment," Master thesis, Department of Electrical Engineering, Feng Chia University, 2002.
- [16] W. Liao, "Mobile Internet Telephony Protocol: An Application Layer Protocol for Mobile Internet Telephony Service," Proceedings of IEEE International Conference on Communications (ICC), Vancouver, Canada, 1999, pp. 339-343.
- [17] M. H. Lin and C. C. Chang, "A Secure One-time Password Authentication Scheme with Low-Computation for Mobile Communications," ACM SIGOPS Operating Systems Review, 2004, pp. 76-84.
- [18] K. E. Malki, "Low Latency Handoffs in Mobile IPv4," IETF draft, <draft-ietf-mobileip-lowlatency-handoffs-v4-09.txt>, 2004.
- [19] G. A. Mills-Tettey and D. Kotz, "Mobile Voice over IP (MVOIP): An Application-level Protocol for Call Hand-off in Real Time Applications," 21st IEEE International Performance, Computing, and Communications Conference, 2002, pp. 271-279.
- [20] M. Moh, G. Berquin, and Y. J. Chen, "Mobile IP Telephony: Mobility Support of SIP," 8th International Conference on Computer Communications and Networks, 1999, pp. 554-559.
- [21] M. Mufti, and A. Khanum, "Design and Implementation of a Secure Mobile IP Protocol," International Conference on Networking and Communication (INCC), 2004, pp. 53-57.
- [22] C. Perkins, "IP Mobility Support," IETF RFC 2002, 1996.
- [23] C. Perkins, "IP Mobility Support version 2," Internet Draft, <draft-ietf-mobileip-v2-00.txt>, 1997.
- [24] R. Rivest, "The MD5 Message-Digest Algorithm," IETF RFC 1321, 1992.
- [25] H. Schulzrinne and J. Rosenberg, "The Session Initiation Protocol: Internet-Centric Signaling," IEEE Communications Magazine, 2000, pp. 134-141.
- [26] W. Stallings, "Cryptography and Network Security: Principles and Practices Third Edition," Pearson Education Inc., 2003.
- [27] SlavaSoft QuickHash Library: <http://www.slavasoft.com/quickhash/>.
- [28] Sufatrio and K. Y. Lam, "Mobile IP Registration Protocol: A Security Attack and New Secure Minimal Public-Key Based Authentication," International Symposium on Parallel Architectures, Algorithms, and Networks, 1999, pp. 364-369.
- [29] E. Wedlund and H. Schulzrinne, "Mobility Support Using SIP," 2nd ACM/IEEE International Conference on Wireless and Mobile Multimedia (WoWMoM'99), Seattle, Washington, 1999, pp. 76-82.
- [30] J. Zao et al., "A Public-key Based Secure Mobile IP," Wireless Networks, 1999, pp. 373-390.