An Efficient ECDSA Authentication Scheme for Mobile IP Networks

Chou-Chen Yang¹, Ting-Yi Chang², Jian-Wei Li³, Min-Shiang Hwang⁴

ABSTRACT

The use of portable computing devices has been booming in recent years. Making sure of the security in mobile systems has become a very important issue. However, a Mobile IP has to deal with some crucial problematic situations such as two Mobile Hosts communicating with each other while moving to the same visited network, for the datagram must pass through Foreign Agent. In this article, we shall propose a link-layer routing between two Mobile Hosts to make it possible for Mobile Hosts to communicate with each other directly. And we shall also employ the elliptic curve digital signature algorithm (ECDSA) to achieve authentication and to ensure security.

Keywords: Mobile IP, ad hoc, authentication, elliptic curve, security.

1 Introduction

Wireless communication has become more and more popular in recent years. Everyone can conveniently connect his/her portable devices to the Internet and communicate with people all around the world. Unlike a traditional wired network, a wireless network can be easily accessed. It is easier to tell which host is communicating with others in a wired network than in a wireless network. However, verifying user identities is very important in wireless network environment. As a matter of fact, some problematic situations have not been properly considered in the Mobile IP [4, 8, 16] system. For example, there are times when some people carry their computer notebooks to a hotel room or office to hold a meeting. In this case to communicating directly among meeting attendees without network administration or additional infrastructure is necessary.

¹ Department and Graduate Institute of Computer Science and Information Engineering, Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.
Email: ccyang@cyut.edu.tw
² Department of Computer and Information Science, National Chiao Tung University
1001 Ta Hsueh Road, Hsinchu, Taiwan, R.O.C.
³ Department of Computer Science and Information Engineering, National Cheng Kung University
No1. Ta-Hsueh Road, Tainan City, Taiwan 701, R.O.C.
⁴ Department of Management Information Systems, National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Email: mshwang@nchu.edu.tw
and yet Mobile IP does not provide such services as direct traffic links between/among end systems. In the existing Mobile IP system, when the Mobile Hosts are located in the same range under a foreign agent, the datagram still must travel through the foreign agent, which acts as an intermediary for the Mobile Hosts.

In 2001, Binkley and Trost [3] proposed an ad hoc routing [5] at the link layer for mobile systems. It provides the direct communication between Mobile Hosts. Mobile Hosts broadcast the beacon messages which include the IP and MAC addresses to provide direct communication via MAC address. In their system, the property of ad hoc protocol is used to solve the above problem, so that all Mobile Hosts can capture the existing shared context by choosing a fresh password and sharing it by symmetric key among those present in the room. However, it is an impracticable application in practice. In this paper, we employ the elliptic curve discrete logarithm problem (ECDLP) [9] to strengthen the weak password as the symmetric key. There will be no other packets exchanged in our protocol.

The remainder of our paper is organized as follows. In Section 2, we shall take a brief look at Mobile IP registration and routing. In Section 3, we shall present a discussion of background issues and problems yet to be solved, and then we shall also show weaknesses of using password-based authentication. In Section 4, we shall introduce our new authentication based on the elliptic curve digital signature algorithm (ECDSA). In section 5, we shall analyze the security of our scheme. Finally, our brief conclusion will be given in Section 6.

2 Overview of Mobile IP

2.1 The Registration of Mobile IP

Mobile IP [4, 6, 8] is a modification to IP that allows hosts to continue to receive datagram no matter where they happen to be attached to the Internet. As Figure 1 illustrates, a home agent (HA) is a host or router on a mobile host's home network. When a mobile host (MH) moves away from its home network, the HA is responsible for tunneling datagram to the MH and maintaining current location information (care-of-address) for the MH. A foreign agent (FA) is a router on an MH's visited network that provides routing services to the mobile node while registered. When an MH moves away from its home network, it obtains a care-of-address on the visited network by soliciting or listening for FA advertisements or contacting DHCP (Dynamic Host Configuration Protocol) [1, 6]. Then, the MH registers the care-of-address with its HA through FA. When the HA receives a registration request from an FA, the HA maintains the current care-of-address for the MH.
2.2 The Routing of Mobile IP

Suppose that a correspond node (CN) sends the datagram to the MH. That datagram will be sent to the MH’s home address (HA’s address) and then tunneled by its HA to the care-of-address. In the reverse direction, the datagram sent by the MH are generally delivered to their destination using standard IP routing mechanisms, not necessarily passing through the HA (see Figure 2). Datagram going to the MH must travel through the HA when the MH is away from home, and this asymmetric routing is called triangle routing. In order to route optimization [10], when the HA receives packets from the CN destined for the MH, the HA will send a binding message to the CN. Once the CN has received the binding message, it can encapsulate the packets and send them directly to the care-of-address for the MH.
3 Problems Discussion

3.1 Adjacent Mobile Hosts

In practical application, when two MHs move to the same visited network and they would like to communicate with each other, the datagram must pass through FA twice, even if the HA has sent out a binding message (see Figure 3). Such a mechanism is not efficient because it wastes network resources.

![Diagram of Adjacent Mobile Hosts](image)

**Figure 3: Adjacent Mobile Hosts**

For example, there are often times when some people bring their computer notebooks to a hotel room or office to have a meeting. The MHs should be able to communicate with each other without network administration or any additional infrastructure. See Figure 3. Since $MH_a$ and $MH_b$ share the same link, they should be able to communicate directly. However, for either normal IP or Mobile IP, the same problem pops up that there is a need for a router to communicate. In Mobile IP, MHs must use an FA.

In the normal IP environment, the traditional IP subnet and ARP [11] may be used to solve the problem. A subnet mask is used to determine whether the destination host is on a directly-connected link or not. If on a direct connection, the sender will use an ARP table to match the MAC address and then directly send the packet out by using the MAC address. In [2], it is said to be easy to spoof IP-to-MAC address bindings by using ARP. In the Mobile IP environment, the host can be quite mobile. $MH_a$ and $MH_b$ have no knowledge as to who the neighbor is (that is sharing the same link). According to Mobile IP routing, assume $MH_a$ sends the datagrams to $MH_b$. The datagrams sent to $MH_a$'s home
address are intercepted by its $MH_a$, tunneled by its $MH_a$ to the care-of-address, received at the $FA$, and finally delivered to $MH_b$. For the same reason, $MH_b$ also sends the datagrams through $FA$.

Moreover, in the wireless or mobile environment, access is quite easy. Any attacker may send an ARP packet containing its own MAC address and the victim’s IP address to usurp the IP-to-MAC address binding of the victim in another part’s ARP cache. This enables the attacker to receive packets intended for the victim.

3.2 Ad Hoc Routing at the Link Layer

Binkley and Trost used [3] an ad hoc protocol to solve the above problem. In an ad hoc network, there is no fixed mobile switching center or base station. $MH$s within each other’s radio range communicate directly, while those that are far apart rely on other hosts as routers relay messages. In practice, it is point-to-point communication that the ad hoc network provides. In Mobile IP, each agent broadcasts an ICMP Router Discovery [15] advertisement message to inform nearby $MH$s that are in the home network or some visited network. In the ad hoc protocol, $MH$s broadcast beacon messages [3] which augment the ICMP Router Discovery packet with the MAC and IP addresses.

Figure 4 shows the ad hoc protocol in use. $MH_c$ has moved into range of $MH_a$ and $MH_b$ and transmitted a beacon message which includes IP and MAC address. When $MH_a$ and $MH_b$ receive the beacon message, they verify the authenticity. If the beacon message is authentic, they add the IPC and MACc addresses to their tables of known bindings. So, $MH_a$ and $MH_b$ have knowledge of $MH_c$’s IP and MAC addresses so as to use IP-to-MAC mapping to send packets to $MH_c$ directly.

In this scheme, the agents and $MH$s broadcast beacon messages at a fixed rate. Agents broadcast advertisement messages once per second and $MH$s broadcast beacon messages once every ten seconds separately. $MH$s also transmit a beacon message to $FA$ immediately before sending a registration request. It is assured when $FA$ relays registration reply by using the IP-to-MAC mapping directly.
3.3 Symmetric Key

In Binkley and Trost's method of ad hoc protocol, all the MHs share a symmetric key for beacon message authentication. The user can generate an ad hoc key by entering a password. When they meet face-to-face, one person can write a password on a blackboard for every one to install on their MHs during the meeting. By the end of the meeting, they can break the acceptance of beacon messages authentication. Here, we show some problems of the password-based authentication as follows:

- If this password is a sufficiently long and random string, it can be used directly to set up a security meeting. In practice, to find a complicated password is difficult. It is much more user-friendly to set natural language phrases as passwords so that people can recognize them easily. However, natural language phrases are weak keys of symmetric cryptosystems because they are drawn from a rather limited set of possibilities. The adversary can mount dictionary attacks, recording the encrypted traffic and then attempting trial decryption with candidate passwords until he/she finds the correct one.
- If one person sets up a sufficiently long and random string to be the symmetric key, he/she must inform others to install it in their computers. In other words, in Binkley and Trost's method, it is necessary to knowing in advance who will attend this meeting, which also means it is not allowed to dynamically increase or decrease the number of persons to join the meeting. It is an impracticable application.
- If any one compromises the password or symmetric key, the security of mobile system will be broken. Moreover, if one of the legal users is malicious, he/she can use the symmetric key to make spoofing by sending to the victim a beacon message containing its own MAC address and the victim's IP address. Because everyone uses the same symmetric key, we have no ability to identify the malicious user.
4 Solution

Because UDP [12] is designed to be extensible, we augment the UDP registration with some extra information including MHT's MAC address and FA's public key for authenticating. FA and MHT have a secure authentication each other (see [18, 19] for more detailed description). For the authentication of IP-MAC list, using ECDSA to reach security requirements.

4.1 ECDSA

The authors of [9, 14, 17] have pointed out that ECDSA offers a level of security comparable to classical cryptosystem that use much larger key sizes and the time complexity of the ECDSA's signature generation and verification is much more efficient than that of RSA's signature [13] and ElGamal's signature [7].

For example, suppose FA wants to send the signature for message m. Any other MHSs can use FA's public key to verify the signature. FA first chooses an elliptic curve E over the finite field Fp and a point P of prime order n in E(Fp). Then, FA randomly chooses an integer d ∈ [1, n-1] as private key and the corresponding public key is Q=dP. To sign the message m, FA performs the following steps.

Step 1. Randomly choose an integer k ∈ [1, n-1].

Step 2. Compute kP=(x, y) and r=x, mod n.

Step 3. Compute s=k' prow P(h(m)+dr) mod n, where h(*) is a secure one-way hash function with fixed-length output.

The signature for the message m is (r, s). After receiving the information {(r, s), m}, the MHT can use FA's public key to verify the signature by performing the following steps.

Step 1. Compute u1=h(m)rs' mod n and u2=rs' mod n.
Step 2. Compute u1P+ u2P=(x, y) and v=x, mod n.

If v is equal to r, the signature (r, s) on message m is valid.

4.2 Mobile Host register to Foreign Agent

Figure 5 shows the procedure when MHT moves to a visited network and registers its location with its HA. The following procedure is performed.
Figure 5. Mobile Host A registering with Foreign Agent

(1) By receiving the FA advertisement message, MHₐ recognizes that it is in a visited network or the home network.

(2) MHₐ sends the Registration Request message.

(3) FA relays the Registration Request message to HA. So HA can create or modify a mobility binding for MHₐ.

(4) HA returns a Registration Reply message to FA. If MHₐ is a legal user, HA encrypts FA’s public key by \( K_{HA, MHₐ} \). The Registration Reply message will include MHₐ’s MAC address and \( C = E_{K_{HA, MHₐ}} \) (FA’s public key). To protect the messages, HA encrypts MHₐ’s MAC address and C by using \( K_{HA, MHₐ} \) (secret key shared between HA and FA).

(5) By receiving HA’s notification, FA obtains MHₐ’s MAC address (denoted as MACₐ) by using \( K_{HA, MHₐ} \). Then, FA records MHₐ’s IP address (denoted as IPₐ) and MACₐ in IP-MAC list.

(6) Because FA knows the MHₐ’s MAC address, FA relays the registration reply message and \( C = E_{K_{HA, MHₐ}} \) (FA’s public key) via MHₐ’s MAC address, which informs MHₐ of the status of its request and indicates the lifetime granted by HA. Then, MHₐ uses \( K_{HA, MHₐ} \) to decrypt FA’s public key from \( E_{K_{HA, MHₐ}} \) (FA’s public key).

4.3 IP-MAC list message authentication

If MHₐ wants to know other MHs under the same range of FA, it sends the Request message of IP-MAC list to FA, then FA’s will use its private key to sign the IP-MAC list.
and broadcast it. See Figure 6, if $MH_a$ also under the same FA, both $MH_a$ and $MH_b$ have the knowledge of each other's IP and MAC addresses. In other words, any MH under the cover of a same FA can obtain any others' IP and MAC addresses from FA's signature on the $IP$-$MAC$ list. The following procedure is performed.

Figure 6: Request for $IP$-$MAC$ list

(1) $MH_A / MH_B$ sends the Request message of $IP$-$MAC$ list to FA.

(2) FA computes the signature $(r, s)$ for the $IP$-$MAC$ list and add the timestamp $T$ to avoid the replay attack.

(3) FA broadcasts the signature $(r, s)$ and $IP$-$MAC$ list.

(4) After receiving the signature $(r, s), MH_A / MH_B$ uses FA's public key to verify the signature.

After the above procedure, MHs in the same range of FA will receive the authenticated $IP$-$MAC$ list. They can directly communicate with each other by using this list mapping. However, if $MH_A$ and $MH_B$ do not within each other's radio communicate directly and they can not communicate directly, but still can through FA.

5 Security Analysis

We employ the public-key cryptosystem to achieve $IP$-$MAC$ list message authentication. ECDSA offers the security by providing the difficulty of elliptic curve
discrete logarithm problem (ECDLP). In the following, several possible attacks will be investigated to demonstrate the security of our scheme.

**Attack 1:** An adversary tries to obtain $FA$'s private key $d$.

*Analysis of Attack 1:* To obtain the private key $d$ from the public key $Q$ is as difficult as to break ECDSA itself. To ensure the security, the length of $d$ should be about 160 bits.

**Attack 2:** If an adversary tries to forge a valid signature $(r, s)$.

*Analysis of Attack 2:* Similar to Attack 1, the adversary should face the difficulty of breaking ECDSA scheme to obtain the $FA$'s private key. Note that the random number $k \in [1, n-1]$ should be different for each signature. Otherwise, the adversary will reveal the secret key $d$. For example, there are two valid signatures $(r_1, s_1)$ and $(r_2, s_2)$ on messages $h(IP-MAC\ list || T_1)$ and $h(IP-MAC\ list || T_2)$, respectively. The adversary can reveal the secret key $d$ in the following equation.

$$
\begin{align*}
    s_1 &= k^{-1}(h(IP-MAC\ list || T_1) + dr_1), \\
    s_2 &= k^{-1}(h(IP-MAC\ list || T_2) + dr_2).
\end{align*}
$$

(1)

Hence, the random number $k$ generated by $FA$ should be different for generating each signature.

**Attack 3:** An adversary produces his/her public key $Q_a$ and private key $d_a$ to generate a signature $(r_a, s_a)$ for the $IP-MAC\ list$.

*Analysis of Attack 3:* It is still impossible for the adversary to forge the signature. From Section 4.2, we know that the $FA$'s public key should be provided by $HA$. The adversary should face to obtain the secret key $E_{MAC}$. However, the secret key $E_{MAC}$ is unknown. For the same reason, the adversary tries to spoof a MAC address, he/she should break the authentication of between $HA$ and $FA$.

**Attack 4:** An Adversary exercises replay attack.

*Analysis of Attack 4:* The signature $(r, s)$ contains a timestamp $T$. When other $MHs$ receive the signature, they should add a timestamp to verify the signature.

6 Conclusion

In our new scheme, there is no need for $FA$ to be a router to transmit datagram between the $MHs$. On the other hand, we employ the ECDSA to strengthen the weak password-based authentication mechanism of Binkley and Trost's method and ensure the security of mobile systems.
References


[16] Fumio Teraoka, Yasuhiro Yokore, and Mario Tokoro, "A network architecture

