International Journal of Computer Science and Applications
Vol. 6, No. 3, pp 10 – 19, 2009


# MOBILE NODE AUTHENTICATION PROTOCOL FOR PROXY MOBILE*

JUNGWOOK SONG

*Computer & Information Communication, Konkuk University*
*1 Hwayang, Gwangjin, Seoul 143-701, KOREA*
*swoogi@konkuk.ac.kr*

SUNYOUNG HAN†

*Computer & Information Communication, Konkuk University*
*1 Hwayang, Gwangjin, Seoul 143-701, KOREA*
*syhan@konkuk.ac.kr*

We are now going to the 4G network and in the 4G network environment, there are so many devices connected to the Internet while they move. We have protocol that can support movement of communicating node without any disruption of their connection status named Mobile IP(MIP). But, the major problem of this MIP is too heaviness of the protocol for small mobile nodes. So, IETF now propose PMIP to solve this problem. But, there is no way to authenticate the mobile node in PMIP.

In this paper, we propose updated version of one-time key based authentication protocol for PMIPv6[Song (2008)] and show the extended results of analysis. With our proposed protocol, we can give a lot of securing features to current PMIPv6.

*Keywords*: AAA; Proxy MIP; Security.

## 1. Introduction

We are now living in the 3G(3rd generation) network environment and are going to the 4G(4th generation) network. The backbone of the 4G network will be a optical network that has very huge bandwidth and it can over some Tbps(tera bit per second) speed and edge of the 4G network will obviously be a wireless link. And we expect that all information devices will be unified into IP. This means that the 4G network will give ubiquity network environment to us. We already have many mobile devices which can connect to the Internet during our moving and numerous mobile devices will appear in a few years.

We have the protocol supporting mobility of mobile devices named Mobile IP(MIP)[Perkins (2002); Perkins (2008); Johnson *et al.* (2004)]. But these protocols have some serious problems. First of them, to deploy these protocols, we must change the

* This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute for Information Technology Advancement)(IITA-2008-C1090-0804-0015).
† Corresponding Author.

protocol stacks of all current mobile nodes. And second, these protocols are too heavy to install to mobile devices that have small size and low computing power.

So, to solve problems of MIP, we have made new protocol called Proxy MIP(PMIP)[Gundavelli *et al.* (2008)]. The PMIP is network based mobility supporting protocol. If PMIP were deployed, it does not need any changes on the mobile node. Thus, PMIP can be more easily deployed than MIP, and so we can say that PMIP is more TELCO(telecommunication company) friendly protocol.

It must be required that any type of authentication method for authenticating mobile node to offer the Internet connection service with PMIP. But, there is no proper authentication method in current PMIP.

In this paper, we propose the updated one-time key based authentication protocol for authenticating the mobile node in PMIP environment. To do this, we add some modification to current PMIPv6 and introduce two new terminologies. We can achieve some security features in PMIPv6 with our authentication protocol.

The rest of this paper is organized as follows. Section 2 describes some related works and section 3 describes current problems to solve with this paper. Section 4 describes our proposing newly updated authentication protocol for PMIPv6 and section 5 shows results of analysis. Conclusion is in section 6.

## 2. Related Works

### 2.1. *Proxy MIPv6*

Proxy Mobile IPv6 (PMIPv6) is the protocol which provides mobility of mobile node in the network without utilizing or requiring of participation of mobile node in IP related signaling. All the mobility signaling and setting up the required routing state is done by mobility entities in the network.

The core functional entities in this technology are Local Mobility Anchor(LMA) and Mobility Access Gateway(MAG). The LMA's responsibility is the maintaining mobile node's reachability state and being the topological anchor point for the mobile node's home network prefix. The MAG is the entity which situates in the access link where the mobile node is connected; it performs the mobility management on behalf of a mobile node. The responsibility of MAG is detecting of mobile nodes movement into access network and out from access link, it initiates the binding registrations to the mobile node's LMA.

The mobile node delivers and obtains messages with the help of MAG which is connected by bidirectional tunnel with the LMA. All the reconfiguration and IP related signaling is made between the MAG and LMA. It is possible that in the network there may be multiple LMAs where each can support different groups of mobile nodes. You can see the PMIPv6 architecture in Fig. 1. While mobile node enters to the PMIPv6 access link, it sends Router Solicitation(RS) message. MAG in the access link receives the request from mode and sends Proxy Binding Update(PBU) message to LMA, LMA

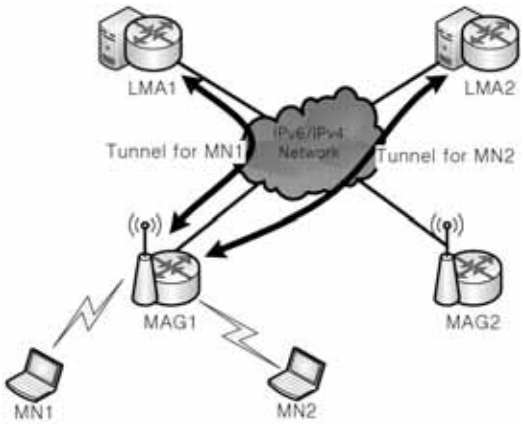


Fig. 1. Proxy Mobile IPv6

replies with the Proxy Binding Acknowledgement(PBA) message where mobile node's home prefix is included. Moreover bidirectional tunnel will be created between LMA and MAG. You can see two tunnels in Fig. 1 which are created for MN1 and MN2. MAG after setting up forwarding functions for mobile node, sends Router Advertisement(RA) messages to the mobile node on the access link advertising the mobile node's home network prefix. After then, mobile node can configure its own IP address[Gundavelli *et al*. (2008)].

### 2.2. *Extensible Authentication Protocol*

Extensible Authentication Protocol (EAP) is an authentication framework which supports multiple authentication methods which is defined by document [Adoba *et al.* (2004)] and [IEEE 802.1X-2004 (2004)]. It is suitable for both wireless and wired networks. It works directly on the top of data link layer protocol, so independent from IP level.

EAP is high flexible and there are several authentication methods with EAP such as Generic Token Card (GTC), One Time Password (OTP), Message Digest 5 (MD5)-Challenge, Transport Layer Security (TLS), EAP for GSM Subscriber Identity (EAP-SIM), EAP for UMTS Authentication and Key Agreement (EAP-AKA), Lightweight Extensible Authentication Protocol (LEAP) and Protected Extensible Authentication Protocol (PEAP). Here we give brief introduction of the most commonly used methods.

LEAP is developed by Cisco as a first implementation of the EAP. It is based on pre-shared keys and does not provide high security. Later EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) was designed as an alternative for LEAP. EAP-FAST provides an encrypted tunnel to distribute pre-shared keys.

The most widely supported EAP standard in the world is EAP-TLS. It uses the handshake protocol in TLS which is based on public key infrastructure (PKI). EAP-TLS is known as one of the highest security methods.

PEAP is developed by Cisco, Microsoft and RSA Security as an open standard. It is based on server-side public key certificates. PEAP creates an encrypted SSL/TLS tunnel between client and authentication server. The ensuing exchange of authentication information to authenticate the client is then encrypted and user credentials are safe from eavesdropping.

### 2.3. *One-time Password*

Traditional passwords can be easily accessed and stolen as intruders have enough time and attempts to crack them. To overcome these shortcomings it was developed One-time password (OTP) mechanism. As its name says, it generates temporary password based on some specific values and can be used only one time.

There are three types of OTP. First type generates next password using a mathematical algorithm. Input value is a previous password. In the second type OTP password is generated based on current time. Usually, special devise -- token is associated with this type OTP. Beside current time stamp, device ID also can be used for OTP generation. In this algorithm time synchronization between client's token and authentication server is very important. The third type is based on a challenge chosen by authentication server or by client[Haller *et al.* (1998)].

### 2.4. *ID-based Cryptography*

ID-Based Cryptography (or Identity-Based Encryption (IBE) or Identity-based Cryptography) is a type or public-key cryptography in which the public key of a user is some unique information about the identity of the user(e.g. a user's email or IP address[Shamir (1084); Baek *et al.* (2004); Boyen *et al.* (2007)].

Unlike a conventional public key infrastructure, IBE does not require complex pre-enrollment of revocation checking. There is essentially no need for certificates. Instead, a recipient's public key is derived from his or her identity. An IBE system also does not require a complex PKI to generate, certify, decertify, and store individual public keys. IBE is so simple because the public key is based on the email or IP address(or some other identity).

## 3. Current Problems

### 3.1. *Security Threats to PMIPv6*

As described in document [Vogt (2007)], there are many security threats to PMIPv6. The PMIPv6 executed on the interface between an LMA and a MAG to establish, update, and tear down routes for data plane traffic of mobile nodes. So, there are man-in-the-middle attacks such as intercept, inspect, modify, or drop such traffic, or redirect it to destination in collusion with the attacker with compromise or impersonation of a

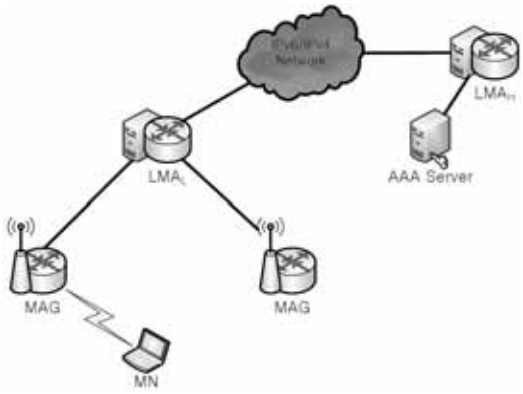


Fig. 2. Configuration of Proposed System

legitimate MAG or a legitimate LMA. A compromised mobile node can also attack the PMIPv6 system. Through inspection, attacker can catch authentication data for mobile node, and spoofing attack can be done to mobile node's home network.

### 3.2. *Problem on Authenticating Mobile Node*

An attacker that is able to forge the mobile node identity of a mobile node can trick a MAG into redirecting data plane packets for the mobile node to the attacker[Vogt (2007)]. Current problems on PMIPv6 can be summarized as follows:

- There is no way to authenticate legal mobile node.
- There is no way to find mobile node's AAA server easily.
- There can be compromise or impersonation of a legitimate MAG.
- There can be compromise or impersonation of a legitimate LMA.
- There can be compromise or impersonation of a legitimate mobile node.

## 4. Mobile Node Authentication Protocol

To solve problems described in previous section, we add some modification to current PMIPv6. We introduce two new terminologies local-LMA and home-LMA. A configuration of our modified PMIPv6 is depicted in Fig. 2. The local-LMA is in same operator's network with MAG and the home-LMA is in MN's home network.

The sequences of our authentication protocol are depicted in Fig. 3. In our protocol, authenticating MN and binding update procedure can be done at the same time.

The summarized sequences of our proposing authentication protocol are summarized as follows:

(1) The MN attaches to the MAG in foreign network.
(2) The MAG builds up $PBU_L$ message and sends it to the local-LMA.
(3) The local-LMA reconstitutes that message as $PBU_H$ and sends it to the home-LMA.
(4) The home-LMA examines data from the MN through AAA server and replies the result to the local-LMA with $PBA_H$ message.

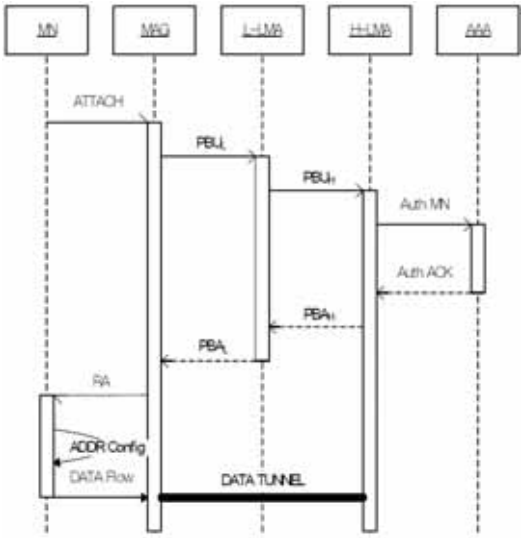


Fig. 3. Sequences of Authentication and Binding Update for MN

(5) The local-LMA passes the result from home-LMA to the MAG with $PBA_L$ message.
(6) If the MAG receives positive reply, the MAG sends RA message to MN and sets up the tunnel to home-LMA for data traffic form or toward the MN.
(7) When the MN receives RA, the MN configures its own IPv6 address following normal IPv6 address configuration procedures[Thomson (19980)].
(8) Now, the MN can send or can receive through the tunnel between MAG and home-LMA.

### 4.1. *Mobile Node Identifier*

According to document [Gundavelli *et al*. (2008)], there is no specific definition of format for a MNID(Mobile Node Identifier). So, we propose a MNID as following format in Fig. 4. The MNID consists of following fields:

- MN-HNP (48bit)
  This represents the home network prefix of mobile node. The local-LMA can find home-LMA with this field. The local-LMA consists anycast address for home-LMA and send $PBU_L$ to home-LMA.
  According to document [IANA (2002)], the ISP will be given minimum 48 bits length prefix for their network, so it is enough length for this field as 48 bits. If it needs more bits, we must update our protocol.
- Device ID (48bit)
  This is typically a MAC address of interface or given special ID by service provider. This is used to distinguish each mobile node and for generating properly next field named One-time Key field.
- One-time Key (32bit)

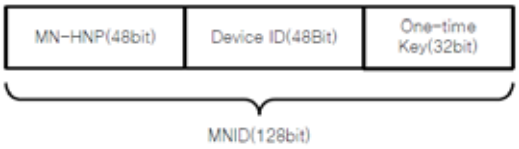


Fig. 4. Mobile Node ID

This is the verification field for mobile node and generated code by the specific random function which installed both side of mobile node and home-LMA. We can use a time-synchronized type OTP function. There are two seeds for generating this key. One of them is Device ID and the other is current timestamp. The OTP function must have to regenerate One-time Key every few seconds, because sequence of setting up will be done in a few hundred milliseconds. This is one of main features of our protocol. With this One-time Key, we can authenticate mobile node in simple one-way message from mobile node to home-LMA.

With this MNID, we can authenticate the mobile node properly and we can also prevent man-in-the-middle attack with intercepting MNID, because of short time validity of the One-time Key.

### 4.2. *One-time Key Generation*

We can generate One-time Key with Timestamp, Device ID, Device Key and special function as illustrated in Fig. 5. First, we use pseudo-Timestamp because it will take a little time that delivering authentication message from mobile node to home-LMA and we could not transmit Timestamp value with authentication request message for security reason. And also we don't have more space for Timestamp in MNID. So, mobile node and home-LMA could not generate One-time Key at the same time. To solving this problem, mobile node and home-LMA use pseudo-Timestamp that is not exact current timestamp. We can get pseudo-Timestamp from simple modulo operation. If we want to change One-time Key every five seconds, we can calculate pseudo-Timestamp with following Eq. (1).

$$pT = T - (x \bmod 5) \tag{1}$$

$pT$ means pseudo-Timestamp, $T$ means Timestamp and $x$ means the last digit of Timestamp. And we can get the general equation for pseudo-Timestamp as Eq. (2) when time-resolution is $r$.

$$pT = T - (x \bmod r) \tag{1}$$

But, this equation has a little problem. If $r$ is not divisor of 10, there is one little pseudo-Timestamp. We can solve this problem with more complicated partitioning equation or using one of divisor of 10 as resolution value $r$.

### 4.3. *Interfacing between MN and MAG*

Interfacing between MN and MAG is described in document [Gundavelli *et al.* (2008)] and [Laganier *et al.* (2008)]. We do not give any changes on this specification.

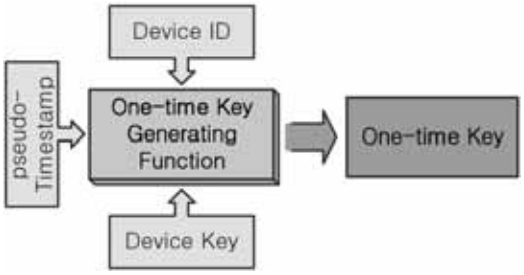


Fig. 5. One-time Key Generation

When mobile node attaches to MAG, MAG invokes the **`MN_ATTACH`** function on MAG and this function has some sub-functions. One of sub-functions is the **`MAG_GET_MN_ID`** and with this sub-function MAG can get MNID described in previous subsection.

### 4.4. *Interfacing MAG and LMA$_L$*

According to document [Gundavelli *et al.* (2008)], MAG and LMA must have pre-defined SA(Security Association) for communicating securely each other, because there are some security threats between them and corresponding LMA of MAG can be placed in other network. Theoretically there are much more MAGs than LMAs and number of MAG is growing up fast when deployment of PMIPv6 is on going. And, there is one or several LMAs per one PMIPv6-domain and one or several MAGs per one LMA. We can setup local MAP and local LMA with pre-defined SA easily, but it is very difficult to setting up local MAP and LMA in the other operator's network with pre-defined SA.

So, we introduce new terminologies local-LMA and home-LMA. The local-LMA is LMA that is under same operator's network with MAG which mobile node is attached and the home-LMA is LMA that is under home network of mobile node. The MAG and local-MAG can have pre-defined SA, so MAG and local-LMA communicate each other through the secure channel.

When mobile node attaches to MAG, MAG builds up $PBU_L$(Proxy Binding Update to local-LMA) message with MNID mobility option for mobile node and sends it to local-LMA instead of home-LMA. If MAG receives positive reply $PBA_L$ from local-LMA then MAG gives RA message to mobile node with data from $PBA_L$.

### 4.5. *Interfacing LMA$_L$ and LMA$_H$*

When local-LMA receives $PBU_L$ message, the local-LMA extracts home network prefix from the message and makes $PBU_H$ message and sends it to home-LMA. The local-LMA and home-LMA can dynamically authenticate each other with PKI(Public Key Infrastructure) such as X.509[Cooper *et al.* (2005)]. There will be too many MAGs for dynamic authenticating with PKI, so we propose architecture with local-LMA and home-LMA.

When home-LMA receives $PBU_H$, home-LMA looks up databases, if there is Device ID in the subscribers list or not. And then, home-LMA generates One-time Key with Device ID and timestamp and verifies it. If all information are valid, home-LMA sends positive $PBA_H$(Proxy Binding Acknowledgement message from home-LMA) to local-LMA and local-LMA passes home-LMAs reply to MAG with $PBA_L$ message. If at least one of information isn't valid, home-LMA replies with negative $PBA_H$.

## 5. Analysis

The EAP can be suitable for authenticating Mobile Node in PMIPv6 environment. But, EAP has some problems directly applying to PMIPv6. First, according to document [Kempf (2007)], mobile node can not take part in binding update procedure or authentication procedure except giving its own MNID. But, if we use EAP to PMIP, mobile node must send its information for authentication and this will change some procedures between MN and MAG.

Second, if mobile node tries to attach to foreign network, EAP can not authenticate properly because there is no information for mobile node in MAG's local AAA server and although mobile node has its AAA server, MAG can not forward any information form mobile node before it is authenticated.

Third, there is no way to complete authentication at a same time with binding update procedure. And finally, using EAP in un-trusted network can not prevent some attacks such as man-in-the-middle attack from compromise or impersonation of a legitimate MAG or a legitimate LMA.

Following Table 1 shows comparison results between EAP and our proposed protocol OK-AP with some security factors. Major purpose of our protocol is authenticating mobile node, but in the procedure, local-LMA and home-LMA can authenticate each other, so mobile node also can authenticate local-LMA and home-LMA. If compromise or impersonation of a legitimate MAG or a legitimate LMA steals MNID, MNID will become useless in a few seconds, because mobile node changes its own One-time Key every few seconds.

Table 1. Comparison with EAP

| | **EAP** | **EAP over IBE or PKI** | **OKAP** |
|---|---|---|---|
| Auth MN (at home) | YES | YES | YES |
| Auth MN (at foreign) | possible | Possible | YES |
| Auth LMA (home) | NO | YES | YES |
| Auth LMA (local) | NO | YES | YES |
| Auth MAG | NO | YES | possible |
| One-way Auth | NO | NO | YES |
| Anti-MITM | NO | NO | YES |
| Sniffing-proof | possible | possible | YES |

| | | | |
|---|---|---|---|
| Spoofing-proof | NO | NO | YES |
| Combinable with BU | NO | NO | YES |

## 6. Conclusion

We propose the authentication protocol for PMIPv6 based on One-time Key. We suggest new MNID format, pseudo-Timestamp, local-LMA and home-LMA. With our authentication protocol, we can achieve authentication of mobile node when it is in home or not and we can also get other security. And we can also fully embed our protocol into existing Proxy MIP.

In our further research we will try to implementing our authentication protocol on PMIPv6 trial network or on simulation environment and we will improve our protocol for fast and lightweight authentication.

## References

Adoba B. *et al.* (2004). *Extensible Authentication Protocol (EAP)*, IETF RFC3748.

Baek, J. *et al.* (2004). *A Survey of Identity-Based* Cryptography, Proc. of the 10th Annual Conference for Australian Unix User's Gruop, 95–102.

Boyen, X., Martin, L. (2007). *Identity-Based Cryptography Standard (IBCS) #1: Super-singular Curve Implementations of the BF and BB1* Cryptosystems, ITEF RFC5091.

Cooper, M. *et al.* (2005). *Internet X.509 Public Key Infrastructure: Certification Path Building*, IETF RFC4158.

Haller, N. *et al.* (1998). *A One-Time Password System*, IETF RFC2289.

IANA. *IPv6 Address Allocation and Assignment Policy, http://www.iana.org/reports/2002/ipv6-allocation-policy-26jun02.*

IEEE 802.1X-2004. *IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control, http://www.ieee802.org/1/pages/802.1x-2004.html.*

Johnson, D. *et al.* (2004). *Mobility Support in IPv6*, IETF RFC3775.

Kempf, J. (2008). *Goals for Network-Based Localized Mobility Management (NETLMM)*, IETF RFC4831.

Laganier, J. *et al.* (2008). *Interface between a Proxy MIPv6 Mobility Access Gateway and a Mobile Node*, Internet Draft.

Perkins, C. (2002). *IP Mobility Support for IPv4*, IETF RFC3344.

Perkins, C. (2008). *IP Mobility Support for IPv4, revised*, IETF mip4 WG Draft.

Shamir, A. (1984). *Identity-based Cryptosystems and Signature Schemes*, Proc. of CRYPTO'84, LNCS 196: 47–53.

Song, J. Han, S. (2008). *One-time Key Authentication Protocol for PMIPv6*, Proc. of ICCIT 2008, Vol 2: 1150–1153.

Thomson, S., Narten, T. (1998). *IPv6 Stateless Address Autoconfiguration*, IETF RFC2462.

Vogt, C., Kempf, J. (2007). Security Threats to Network-Based Localized Mobility Management (NETLMM), IETF RFC4832.