MIS Protocol for Secure Connection and Fast Handover on Wireless LAN

Hitoshi Morioka
ROOT Inc.
hmorioka@root-hq.com

Hiroshi Mano
ROOT Inc.
hmano@root-hq.com

Motoyuki Ohmori
Chikushi Jogakuen University
Department of English Media
ohmori@chikushi-u.ac.jp

Masataka Ohta
Tokyo Institute of Technology
Graduate School of Information
Science and Engineering
mohta@necom830.hpcl.titech.ac.jp

Abstract

MIS (Mobile Internet Services) architecture is designed for secure connection and fast handover with wireless LAN. This architecture consists of three protocols, MISP (Mobile Internet Services Protocol), MISAUTHP (Mobile Internet Services Authentication Protocol) and MIS MobileIP, and two kinds of servers, authentication servers and home agent, base routers and mobile nodes. MISP is a protocol designed for authentication, IP address assignments, session key exchanges and various negotiations between mobile nodes and base routers with one-round-trip packet exchange after a mobile node receives beacons. MISP quickly establishes link between mobile nodes and base routers. MISAUTHP is a protocol for authentication between authentication servers and base routers. MISAUTHP can authenticate mobile nodes and base routers with single exchange of packets too. MIS MobileIP is a mobility support protocol for IPv4. This is a subset of RFC2002 MobileIP. We mainly describe about MISP, MISAUTHP and comparison between MISP with MISAUTHP and IEEE802.11 with IEEE802.1x.

1. Introduction

In case of using IEEE802.11[1] wireless LAN as mobile communication media, there are some problems.

One of these problems is security. We should consider potential risk of eavesdropping, session hijack, man-in-the-middle attack and fake access point attack more than wired LAN because wireless LAN uses radio wave as media. IEEE802.11 based wireless LAN supports WEP for security. But all users using the same access point use the same key for WEP. This means one user can decrypt other users' frames. Recently IEEE802.1x[2], WPA and WPA2 are supported by many wireless LAN equipments. But they also have some problems for mobile use as we describe later.

Another problem is handover latency. Handover is an essential technology to mobile communications. Handover means a mobile node changing an access point without breaking the communication between the mobile node and the correspondent node. But a communication blocking happens. It is caused by handover latency when a mobile node uses mobile IP on wireless LAN. This may cause packet losses. This communication blocking is especially a big problem for real time applications like IP telephone.

To solve this problem, we developed new protocols, which are called MISP[3][4] and MISAUTHP[5]. MISP is a protocol designed for authentication, IP address assignments, session key exchanges and various negotiations between mobile nodes and base routers with single exchange of packets after a mobile node receives beacons. MISP quickly establishes IP connection between mobile nodes and base routers. So it can reduce the time to make a connection between a mobile node and a base router. MISP also provides secure connection between mobile nodes and base routers without additional packet exchange. MISAUTHP is a protocol for authentication between authentication servers and base routers. An authentication server can authenticate both mobile nodes and base routers with single exchange of packets by MISAUTHP.

2 MIS Architecture

MIS architecture is an open architecture published by Mobile Broadband Association in Japan. MIS architecture consists of Authentication Server (AUTH), Home Agent

(HA), Base Router (BR) and Mobile Node (MN) shown in Fig. 1. MISP is used between MN and BR. MISAUTHP is used between BR and AUTH. MIS mobile IP[6] is used between MN and HA. This mobile IP is a subset of mobile IPv4 published in RFC2002[7]. Wireless LAN interface is used in pseudo-adhoc (adhoc-demo) mode. This mode is supported by some chipsets and not defined in IEEE802.11 standard. It uses only IEEE802.11 PHY and encapsulation. Most IEEE802.11 MAC functions such as channel scan and association procedure are not supported in this mode.

MISP which is used between MN and BR supports fast mutual authentication and encryption for each MN. By using pseudo-adhoc mode, it can control channel scan by MN and establish sessions with multiple access points simultaneously.

Fig. 2 is a diagram of MISP and MISAUTHP. MISP and MISAUTHP supports some kinds of security methods. In this paper, we describe about HMAC-MD5/HMAC-MD5/AES-CBC-128bit security type which uses MD5[8] and HMAC-MD5[9] for authentication, HMAC-MD5 for transferring session key and AES-CBC-128bit[10] and MD5 for data encryption. MISP supports multiple network layer protocol. But in this paper, we describe about IPv4.

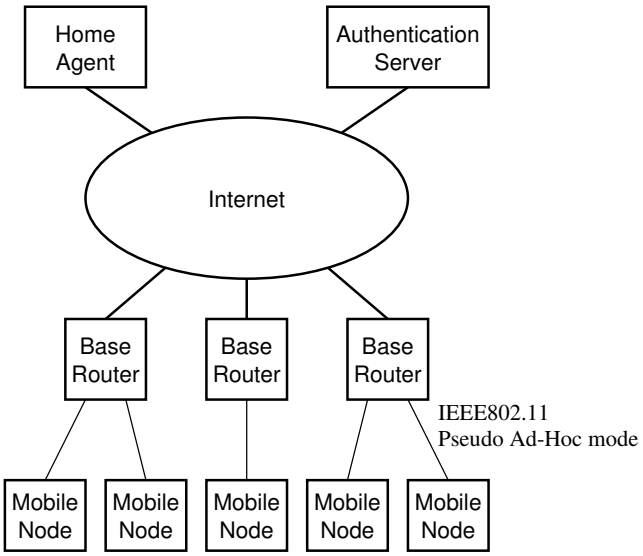

Figure 1. MIS System

2.1 MISP Messages

MISP uses 6 types of messages. One is the data message which transfers the upper layer packets. Others are the control messages which are used for session control between MNs and BRs.

There are five control messages, beacon message, authentication request message, authentication success message, authentication failure message and finish session message. All control messages consist of an MISP header and MISP objects. The MISP header that is 4 octet length consists of a message code, flags and a message length. The MISP object consists of an object type, an object length and an object value. Table 1 shows the MISP objects and their type, length, name and messages which includes.

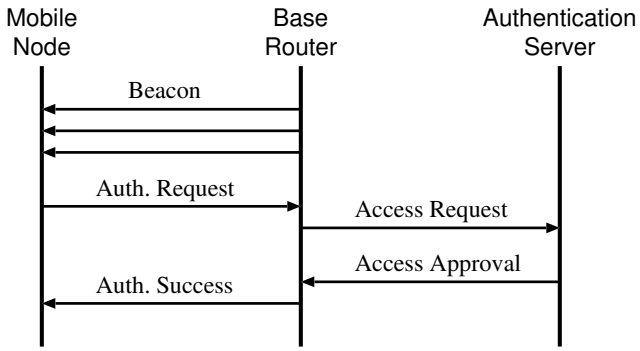

Figure 2. Diagram of MISP and MISAUTHP

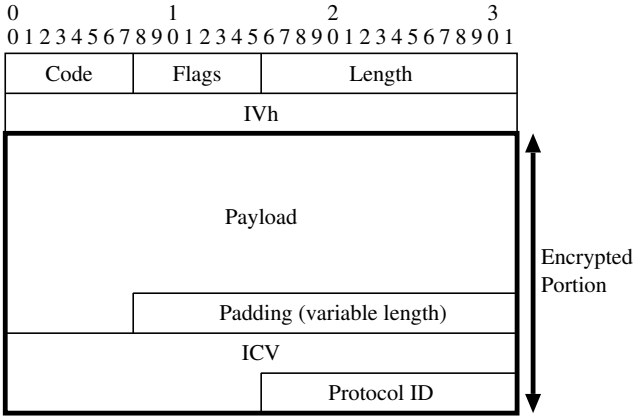

Figure 3. MISP Data Message Format

The data message format is shown in Fig. 3. The code field is always 0 in the data message. The IVh field is the upper 8 octet of the initialization vector of AES-CBC. The padding field is filled by 0 for AES-CBC encryption. The ICV field is the integrity check value for the message authentication. The protocol ID field indicates the upper layer protocol. The payload, the padding, the ICV and the protocol ID fields are encrypted.

2.2 MISAUTHP Messages

MISAUTHP uses three types of messages. They are access request message, access approval message and access denial message. They are transferred as packets of IP.

Table 1. MISP Objects

Type	Length	Name	Beacon	Auth. Req.	Auth. Suc.	Auth. Fail.
0x00	1	Padding	Optional	Optional	Optional	Optional
0x02	10	Beacon Timestamp	Required	Required	Required	Required
0x03	6	IPv4 Local Address		Optional	Optional	
0x04	6	IPv4 Remote Address			Optional	
0x05	Variable	ICV (Integrity Check Value)		Required	Required	
0x06	Variable	NAI (Network Access Identifier)		Required		
0x08	Variable	Session Key Delivery Data		Required		
0x09	14	Geographical Information	Optional			
0x0a	3	IPv4 Available Address Number	Optional			
0x0b	3	IPv4 Source Address Filter	Optional			
0x0d	4	Error Reason				Required
0x0e	2+4n	BR Group	Required			
0x0f	4	Session Key Valid Time			Required	
0x10	4	Serial Number	Required			
0x11	4	Beacon Interval	Required			
0x12	2+2n	Security Type	Required	Required		
0x13	8	Uplink Speed	Optional			
0x14	3	Channel	Optional			
0x15	2+2n	Network Layer Type	Required	Required	Required	

2.3 Pre-Shared Information

There are two pairs of pre-shared information. One is shared by the MN and the AUTH The other is shared by the BR and the AUTH. The MN and the AUTH share the user identifier and the secret key. Each MN has a different identifier and a secret key. This secret key is called "MN-key". The BR and the AUTH share the secret key. Each BR has a different secret key and is identified by its IP address. This secret key is called "BR-key".

2.4 Session Initiation

Before an MN communicate with other hosts by IP, it must be authorized. If the authentication is successfully finished, a security association between the MN and the BR is established. This security association is called "session". After that, the MN can communicate with other host by IP.

BR transmits beacons in a fixed interval, which are not encrypted. The beacons include a timestamp, a beacon interval, a radio channel and so on. The MN receives beacons during channel scanning. If the MN finds multiple BRs, the MN selects the BR with the highest signal strength of the received beacon.

Then the MN sends an authentication request message to the BR. The authentication request message includes the integrity check value(ICV), the timestamp of the latest beacon, the seed of the session key and so on. The seed of the session key is generated randomly. The ICV is generated by the following method.

1. Making the authentication request message with the ICV field filled by 0.
2. Attaching the sender MAC address, the receiver MAC address to the authentication request message.
3. Generating a 16 octet byte stream by applying MD5 to the byte stream made in 2. This byte stream is called the authentication data.
4. Generating a 16 octet byte stream by applying HMAC-MD5 to the authentication data made in 3 with the MN-key.
5. Overwrite the ICV field in the authentication request message by the byte stream made in 4.

When the BR receives the authentication request message, it checks the timestamp. If the timestamp is too old, the BR sends an authentication failure message to the MN. The BR calculates the authentication data by the same method as described above and extracts the seed of the session key and ICV from the authentication request message. Then the BR makes the access request message which includes the seed of the session key, the authentication data, the ICV and the authenticator. The authenticator is generated by the following method.

1. Making the access request message with the authenticator field filled by 0.

2. Applying HMAC-MD5 to the byte stream made above with BR-key.

3. Overwrite the authenticator field in the access request message by the byte stream made in 2.

The access request message is sent to the AUTH.

The AUTH that received the access request message, extracts the authenticator, the authentication data and the ICV from the access request message. It calculates the authenticator from the access request message by the same method as described above. It compares two authenticators, one is extracted from the access request message and the other is calculated by the AUTH, to check the integrity of the access request message. It also calculates the ICV by applying HMAC-MD5 to the authentication data with MN-key and compares two ICVs, one is extracted from the access request message and the other is calculated by the AUTH. If these two ICVs are same, the authentication succeeds.

If the authentication succeeds, the AUTH sends the access approval message to the BR. The access approval message contains the ICV, the authenticator and the session key delivery data. The ICV is the same one extracted from the access request message. The authenticator is calculated by the same method as described before. The session key delivery data is generated by the following method.

1. Extracting the seed of the session key from the access request message.

2. Applying HMAC-MD5 to the seed with MN-key. This is the session key.

3. Applying HMAC-MD5 to the ICV extracted from the access request with BR-key. This is called the hashed ICV.

4. Calculating exclusive-OR of the session key and the hashed ICV. This is the session key delivery data.

When the BR receives the access approval message, it checks the integrity of the message by the authenticator. Then it extracts the ICV and the session key delivery data from the message and decodes the session key by using them. After that, the BR sends the authentication success message to the MN. This message includes the ICV and the network layer information such as IP address of the MN. The session key is not included in the message. The ICV in the authentication success message is calculated by the same method as described before but it uses the session key as the key of HMAC-MD5 instead of the MN-key.

The MN calculates the session key from the seed of the session key that is sent to the BR in the authentication request message. Receiving the authentication success message, the MN checks the integrity of the message by the ICV. Then it sets up the IP layer such as IP address according to the information in the message.

As described in this section, the MN and the BR authenticate each other, share the session key for encryption and set up IP layer by one round trip packet exchange.

2.5 Data Message

After the session is established, the MN and the BR communicate by the data message that encrypted by AES-CBC using the session key. As described in section 2.1, every data message has the ICV field for authentication of each data message.

The sender generates the data message by the following method. After here, IV means the initialization vector, IVh means the upper 8 octet of the IV and IVl means the lower 8 octet of the IV.

1. Generating the IVh randomly. Upper 6 octet of the IVh is used as the ICV.

2. Rotating each octet of the IVh to 1bit left. This is the IVl.

3. Coupling the IVh and the IVl. This is the IV.

4. Encrypting the payload, the padding, the ICV and the protocol ID field by AES-CBC using the session key and the IV.

5. Making the data message by adding the MISP header and the IVh.

The receiver decrypts and authenticates the data message as following.

1. Extracting the IVh from the data message. Upper 6 octet of the IVh is the ICV.

2. Rotating each octet of the IVh to 1bit left. This is the IVl.

3. Coupling the IVh and the IVl. This is the IV.

4. Decrypting the encrypted portion by AES-CBC.

5. Extracting the ICV from the decrypted message and comparing it to the ICV got in 1. If these ICVs are same, the data message is correct.

2.6 Session Key Updating

The session key is expiring in 70 seconds. So the MN should update the key by re-authentication in less than 70 seconds. The MISP specification defines the interval of the re-authentication as 60 seconds. So the MN and the BR can use two session keys between re-authentication and expiration of the old key. These two keys are identified by the flag in the MISP header.

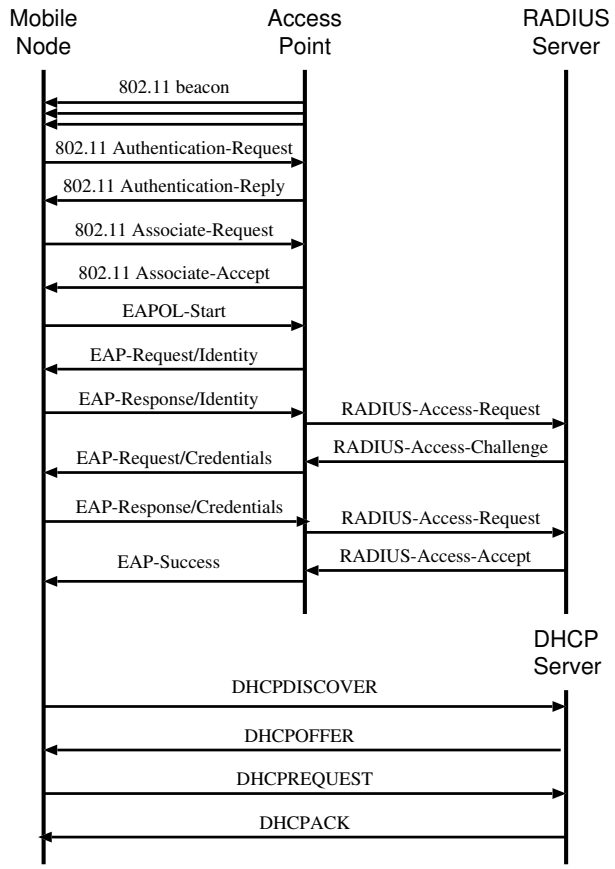

Figure 4. Diagram of IEEE802.11, IEEE802.1x and DHCP

3 Comparison between MISP with MISAUTHP and IEEE802.11 with IEEE802.1x and DHCP

We compare MIS architecture with IEEE802.11, IEEE802.1x and DHCP[11] from two points of view, handover and security.

3.1 Consideration about Handover

An ordinary handover manner is following.

1. Mobile node starts channel scan for searching access point at certain timing (e.g. signal strength becoming less than threshold)
2. After finding an appropriate access point, a mobile node set up link layer. (e.g. association in IEEE802.11 infrastructure mode)
3. Mobile node set up IP layer. (e.g. DHCP)
4. Mobile node sends binding update request to home agent.
5. After home agent receives binding update request, home agent changes the forwarding destination.
6. Handover completes and mobile node can communicate with correspondent nodes.

Mobile node cannot communicate with its correspondent nodes during these actions. While home agent continues to forward packets to mobile node via old access point until 5, mobile node already break connection with old access point. This causes packet losses.

Though FMIPv6[12] is proposed in IETF to reduce packet losses caused by handover, it cannot solve communication blocking. Because FMIPv6 does not accelerate link layer set-ups and IP connection establishments. Buffering of FMIPv6 can reduce packet losses, but increases transmission delay.

Communication blocking is caused by the following actions.

- Channel scan
- Setting up link layer
- Setting up IP layer
- Latency of binding update

To solve communication blocking by handover, we must consider all of them.

In these actions, channel scanning time depends on the number of channels to scan and beacon interval. It cannot be reduced by active scanning because mobile nodes must wait for response until timeout if there are no access points. While typical IEEE802.11 access points transmits beacons every 100ms, BR of MISP transmits beacons every 30ms. Though it depends on implementation, it takes 1300ms at least in IEEE802.11 and 416ms in MISP for 13 channels to scan passively.

Fig. 4 shows the diagram of IEEE802.11 infrastructure mode, IEEE802.1x (EAP-MD5) and DHCP. It takes one round trip of frame between a mobile node and an access point for association. After that, one round trip between the mobile node and the access point, and two round trip among the mobile node, the access point and the RADIUS server are needed for authentication. In addition, two round trips are needed for DHCP.

MISP and MISAUTH protocol can establish a connection between a mobile node and a base router faster than the combination of IEEE802.11 infrastructure mode, IEEE802.1x and DHCP. Fast connection establishment is effective for fast moving mobile nodes. Because if connection establishment is slow, mobile node will pass through

the cell before connection is established. In Mobile IPv6[13], IP connection should be established by normal IPv6 mechanism, stateless or stateful address autoconfiguration. This is also slower than MISP. And FMIPv6 can't reduce this connection establishment time.

3.2 Consideration about Security

On wireless LAN, following attacks are supposed.

- **Man in the middle attack**
  In IEEE802.11+IEEE802.1x, man in the middle attack is available by fake EAP Success messages. Because they do not have mutual authentication method. In MISP+MISAUTHP, because MN and BR are authenticated each other, man in the middle attack is unavailable.

- **Fake Access Points**
  In IEEE802.11+IEEE802.1x, access points can authenticate mobile nodes but mobile nodes cannot authenticate access points. So it is possible that an attacker installs fake access points and makes mobile nodes to connect them. In MISP+MISAUTHP, MN and BR authenticate each other. So fake BR attack in unavailable.

- **DoS attack by fake management frames**
  In IEEE802.11+IEEE802.1x, as management frames do not have the information for validity check, attackers can interfere established connections by transmitting fake management frames. In MISP+MISAUTHP, as authentication failure message do not have the information for validity check, attackers can interfere connection establishing by transmitting fake authentication failure message. But it can be avoided by the mobile node waiting for authentication success message until timeout.

- **Session hijack**
  In IEEE802.11+IEEE802.1x, all frames from the MAC address of the authenticated mobile node are transferred. So attackers can hijack the session by using the authenticated MAC address. In MISP+MISAUTHP, all frames are authenticated by ICV. So session hijack is unavailable unless the session key is stolen. As the session key is changed every 70sec, analysing the session key is virtually unavailable.

4 Conclusion

We described about MIS architecture which is suitable for mobile communications. MISP and MISAUTHP have advantages of security and handover latency over IEEE802.11 and IEEE802.1x.

Comparison of handover time between MISP+MISAUTHP and IEEE802.11+IEEE802.1x by experiment is a future issue.

References

[1] ANSI/IEEE std 802.11 Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications, IEEE 1999 Edition

[2] IEEE Std 802.1X-2001 Port-Based Network Access Control, IEEE, 2001

[3] Mobile Broadband Association, MBA Standards 0201 "MIS Protocol Specifications ver. 1.02," http://www.mbassoc.org/j-services/mbas0201.pdf, 2004.

[4] Y. Hori, H. Morioka, H. Mano, K. Sakurai, "Security Evaluation of MIS Protocol on Wireless LAN," , pp.247–252, The 2005 Symposium on Cryptography and Information Security, Japan, Jan. 25-28, 2005.

[5] Mobile Broadband Association, MBA Standards draft 0301 "MISAUTH Protocol Specifications," http://www.mbassoc.org/j-services/mbas0301.pdf, 2004.

[6] Mobile Broadband Association, MBA Standards 0202 "MIS Mobile IP Specifications," http://www.mbassoc.org/j-services/mbas0202.txt, 2004.

[7] C. Perkins, "IP Mobility Support," http://www.ietf.org/rfc/rfc2002.txt, 1996.

[8] R. Rivest, "The MD5 Message-Digest Algorithm," RFC1321, 1992.

[9] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC2104, 1997.

[10] S. Frankel, R. Glenn, S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec," RFC3602, 2003.

[11] R. Droms, "Dynamic Host Configuration Protocol," RFC2131, 1997.

[12] R. Koodli, "Fast Handovers for Mobile IPv6," http://www.ietf.org/internet-drafts/draft-ietf-mipshop-fast-mipv6-03.txt, 2004.

[13] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6," RFC3775, 2004.