社団法人 情報処理学会　研究報告
IPSJ SIG Technical Report

2004－MBL－31　(16)
2004－ＩＴＳ－19　(16)
2004／11／12

The Proposal and Evaluation of AAA for Bootstrapping Mobile IPv6 and ISATAP

Ryoji KATO* Shinta SUGIMOTO* Johnson Oyama*
Hidetoshi YOKOTA** and Akira IDOUE**

* New Business and Technology Division, Nippon Ericsson K.K. 1-4-14 Koraku, Bunkyo-ku, Tokyo, 112-0004 Japan

** Mobile Network Laboratory, KDDI R&D Laboratories 2-1-15 Ohara, Kamifukuoka-shi, Saitama, 356-8502, Japan
E-mail: *{Ryoji.Kato, Shinta.Sugimoto, Johnson.Oyama}@ericsson.com, **{Yokota, Idoue}@kddilabs.jp

Keyword Mobile IPv6, ISATAP, AAA, bootstrap, EAP, IPsec, Mobile

1. Overview

This paper proposes a way for IP terminal to bootstrap (initialize and start up) IP network services (e.g. MIPv6, ISATAP) from scratch, shows the differences and benefits comparing with the current art of bootstrapping, and evaluates it in terms of the performance measured in our test-bed. When bootstrapping IP network services, the important aspects include how to discover the servers (or routers) serving a specific service (either statically or dynamically), what kind of parameters need to be known by the clients and servers (or routers) prior to bootstrapping these services, and how the servers (or routers) authenticate and authorize the IP terminals (or/and vice versa). Our proposal makes use of AAA (Authentication, Authorization and Accounting) framework to get around these important points. The reason why our proposal is based on AAA framework is that 1) in most cases IP terminals start the authentication and authorization process at the beginning before accessing the commercial IP network, 2) an authenticated or secured communication can be assumed between an IP terminal and an AAA server during AAA operation and 3) it can be used to provide IP network services that requires some authentication. The IP terminal that we have focused in is the mobile terminal because it will frequently bootstrap, e.g. when powered on, when brought to the new mobile networks (roaming).

1.1. Network Environments

In our proposal, we focus on the mobile terminals as IP terminals. The mobile terminals will be tuned on or roamed to the various network environment, for example, the various network access media (probably the wireless media for the mobile terminals, e.g. the cellular network, the wireless LAN, Bluetooth etc), the various network access operators, the various IP protocols (either IPv4 or IPv6), the various authentication protocols (e.g. PPP, 802.1x, PANA). Our intension here is to show our proposal can be used to or extended to go with such various network environments.

Deployment is also what we take care of in this proposal. Here, we will not propose a specific method that works very well but that must be deployed in every access points in which the mobile terminals probably visit. In our proposal, we tried to keep the impact to the existing networks as small as possible for easy deployment. We investigated the existing networks, e.g. W-CDMA, CDMA2000, W-LAN Hot Spot Service etc, and made a proposal that fits in such networks.

1.2. Network Services

And, we focus on Mobile IPv6 and ISATAP as the IP network services to be bootstrapped because both are fundamental and necessary for the seamless IP connectivity, which is primary requirement for the mobile terminals. The combination of Mobile IPv6 and ISATAP (called as GLOB6[2]) enables IP terminals to keep any IPv6 connections beyond the changes of IP address and IP protocols (IPv4 and IPv6).

1.3. Achievements

When bootstrapping Mobile IPv6 and ISATAP, our proposal has some advantages in comparison with

the current specifications or the current services.

At first, our proposal keeps the static configuration as small as possible, in other words, the dynamic configuration as much as possible. In our proposal, only configurations about the authentication are necessary to the mobile nodes. All other configurations, e.g. discover ISATAP router, assign Mobile IPv6 Home Address or establish the security association etc, will be done by the network side. So, the network operator can select the most suitable server (Home Agent for Mobile IPv6 and ISATAP router for ISATAP) for each mobile node. And it can increase the degree of freedom for the network
design.

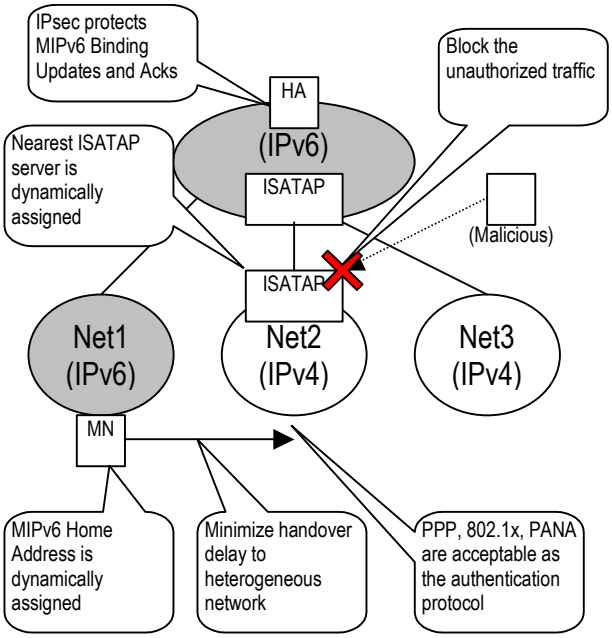


Figure 1: Examples of Achievements

At second, our proposal enables Mobile IPv6 and ISATAP to be used as the reliable commercial services. Different from the experimental or closed networks, the authentication is necessary for accounting in the commercial networks and the security is necessary for the reliable networks. For example, IPsec SA is mandatory for Mobile IPv6 (as specified in [1]), ISATAP router needs to have authenticate the mobile node's IP address to enable the accounting and to drop the unauthorized traffic.

Figure 1 includes some examples of how our proposal improves Mobile IPv6 and ISATAP.

1.4. Evaluations

In this paper, the methods of bootstrapping including our proposal will be evaluated in terms of 2 technical perspectives.

One is the amount of information that must be distributed to the clients and servers (or routers) preliminarily. This is related to the operational scalability or complexity. For example, in the case of establishing IPsec Security Association (SA) for Mobile IPv6 Binding Update and Binding Acknowledgement, if both ends (Mobile Node and Home Agent) has agreed on all IPsec parameters preliminarily (static configuration in other words), the time of establishing IPsec SA is very low (or none), but the operational complexity is very high. It could be awful operational costs to configure the IPsec parameters (e.g. shared keys, security parameter index (SPI), IP address etc) for millions of mobile subscribers and maintain millions of synchronization between Mobile Nodes and Home Agents.

The other aspect of evaluation is the time to bootstrap. There are some cases that the time to bootstrap is critical. One example is the handover to a heterogeneous wireless network. Different from doing handover within same wireless network, the mobile nodes will have to setup the network configurations nearly from scratch when doing handover to the heterogeneous wireless networks.

2. Assumptions and Definitions

In this section, some assumptions that are necessary for our proposal are described and some words are defined to stands for the necessary concepts to explain our proposal.

2.1. AAA Architecture Model

Our proposal for bootstrapping is based on AAA framework and utilizes and extends it. But we think AAA framework assumed here is straightforward and very common in the current mobile networks. Figure 2 shows the assumed AAA framework model in this proposal.

A mobile node (MN) is assumed to be a subscriber of Home Domain in Figure 2, which would be either the real mobile network operator or the mobile virtual network operator (MVNO).

When MN visits Visited Domain, it will start the authentication procedure to get authorized to access to the network by using some AAA protocol (e.g. PPP, 802.1x etc depending on the administrative policy of the visited domain). From the NAI or something else

that is used as the identifier of AAA protocol, the access router (AR) or the AAA server in Visited Domain (AAAv) can know Home Domain that MN subscribed. Then, the connection of AAA protocol (which will be probably different from AAA protocol between AR and MN) will be established toward Home Domain to inquire, e.g. whether MN is a valid subscriber, what kind of services should be served, or what kind of accounting should be used etc. If the AAA server in the home network (AAAh) authenticates the mobile node, the successful result will be transferred to AR in Visited Domain through AAA protocol. Then, AR will open the port of MN's access link and MN gets the permission to access Visited Domain and beyond.

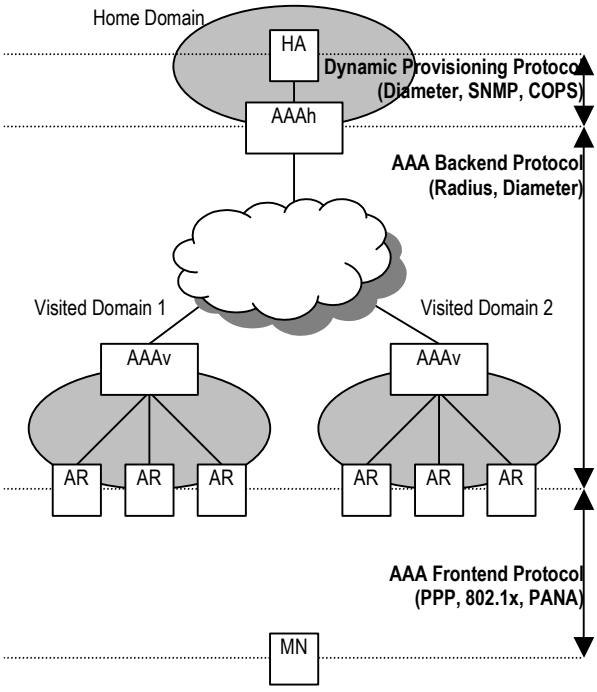


Figure 2: AAA Architecture Model

Normally, there are roaming agreements between Home Domain and Visited Domain (from the pure technical point of view, such agreements may not be necessary. But it is very natural to assume them if thinking the accounting issues.). AAA servers (AAAv and AAAh in Figure 2) will have mutual trust preliminarily.

2.2. AAA Frontend Protocols

Between MN and AR, an authentication protocol is assumed. In the current cellular networks, PPP is widely adopted as the authentication protocol (PPP is used not only to authenticate but also to establish the access link and assign IP address etc). And 802.1x is widely deployed in W-LAN hot spot services. We call such AAA protocols between MN and AR as "AAA Frontend Protocol" in this paper.

New authentication protocol, PANA[7], which is now being standardized in IETF, is also used as AAA Frontend Protocol.

2.3. AAA Backend Protocols

Between AR and AAAv and between AAAv and AAAh, there are the inter-domain AAA protocols, e.g. Radius or Diameter[4]. AR will work as AAA client of inter-domain AAA protocol when a mobile node starts to access the AR through AAA Frontend Protocol. AR establishes an AAA connection to AAAh to which the mobile node subscribes. It would be either direct or indirect (relayed by AAAv). The word "AAA Backend Protocol" is used to represent such inter-domain AAA protocols.

2.4. Extensible Authentication Protocol (EAP)

EAP[8] is the most important assumption in our proposal. EAP is used as the authentication method, which can replace the other authentication method, like PAP or CHAP. EAP itself doesn't have any authentication mechanism but can convey the various authentication methods, e.g. MD5 challenge and response, X.500 certification based method. Actually, almost AAA protocols (PPP, 802.1x, PANA, Radius, Diameter[5] etc) use EAP as the authentication method. So the assumption of EAP is very reasonable even for the existing mobile networks. Then, the authentication methods other than EAP (e.g. PAP, CHAP, web-based authentication) are out of scope in this proposal.

2.5. Dynamic Provisioning Protocols

We also assume another protocol used to manage the network nodes within the single administrative domain. This protocol may be the used for the management or provisioning. This protocol is assumed to enable to configure the remote network node. In this model, AAAh will use this protocol to configure the service node in the same domain

(MIPv6 Home Agent is pictured as the example of the service node in Figure 2.

2.6. User Data

As the minimum data used in AAA operations, MN and AAAh must synchronize two kinds of data (that will probably be distributed in offline manner, embedded in ROM or SIM card for MN, recorded in the subscriber database for AAAh). They are:

- User Identifier (e.g. NAI, IMSI etc)
- Shared Secret Key (any random octet string)

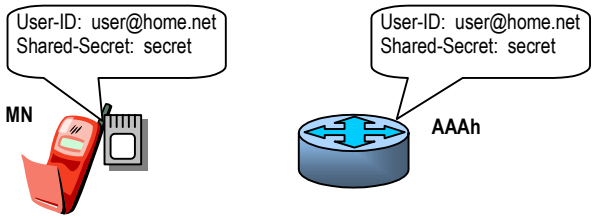


Figure 3: User ID and Shared Secret

The certificate like X.509 can be used instead of the shared secret key if there is appropriate authentication method that can generate the shared secret key between MN and AAAh. If so, we can assume it as the equivalent of the shared secret key.

2.7. AAA Protocol Stack

Figure 4 illustrates the AAA Protocol Stack including all protocols described in this section (AAA Frontend Protocol, AAA Backend Protocol, EAP and Dynamic Provisioning Protocol).

As described in Figure 4, the "EAP method" protocol layer is built only on MN and AAAh. It is very important for our proposal because our central idea is to introduce new EAP method, which means that any unknown EAP methods have no impact on AR and AAAv (both reside in the visited domain).

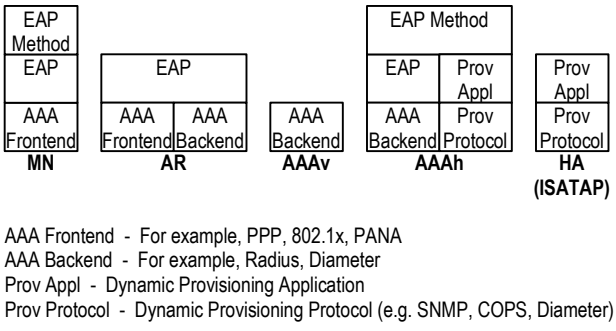


Figure 4: AAA Protocol Stack

So our proposal can be used with any visited domain that conforms to our assumption described in section 2.

3. Problems

3.1. Problems for Bootstrapping MIPv6

In order to bootstrapping MIPv6 from scratch, there are some issues should be solved.

- Assign Home Address for Mobile Node
- Discover MIPv6 Home Agent
- Establish IPsec SA for Binding Update and Binding Acknowledgement

Currently, there is no way to assign Home-Address within Mobile IPv6 specification. It is assumed that Mobile Node must be assigned Home-Address by some methods (statically or dynamically) other than MIPv6 signals before starting MIPv6.

About discovering Home-Agent, Dynamic Home Agent Address Discovery is defined in MIPv6 specification. But, it is not completely dynamic because MN must know the prefix of HA IPv6 address, which will be presumed from Home Address.

Establishing IPsec SA for MIPv6 Binding Update and Binding Acknowledgement is another problem because Home Address and Home Agent Address must be necessary to establish IPsec SA between them. Even if IKE is used to establish IPsec SA between MN and HA, MN and HA have a method to authenticate each other (in IKE specification, there are two ways for authentication, shared secret and X.509 certificate). But it introduces another restriction onto MN and HA. MN and its possible HA (could be multiple) keep other authentication method for IKE than what is used for AAA protocols.

3.2. Problems for Bootstrapping ISATAP

In order to bootstrap ISATAP, these issues must be solved.

- Discover suitable ISATAP router for Mobile Node (e.g. nearest ISATAP router to MN)
- Establish Security Association between MN and ISATAP router for accounting

In ISATAP specification, some ways are suggested to discover ISATAP routers. One is to use DNS to find the ISATAP router. But there are some problems to use DNS. From the suggestion of ISATAP specification, MN should keep PRL (Potential Router List) that is the list of FQDN for ISATAP routers. MN will select one FQDN and get IP address

of ISATAP router by using DNS. But selecting ISATAP router should be taken much care because the user traffic could be forced the triangle routing when selecting ISATAP router that is far from MN.

And, if Visited Domain assigns private IP address to MN, MN must select ISATAP router within Visited Network. It is not defined what FQDN can be used to get IP address of ISATAP router.

Security and Authentication should be considered seriously. Most of current network sites that are using private IPv4 addresses have natural security mechanism because it naturally prevents the direct attack from the outside networks. But ISATAP router assigns global IPv6 addresses automatically to all nodes in the private network.

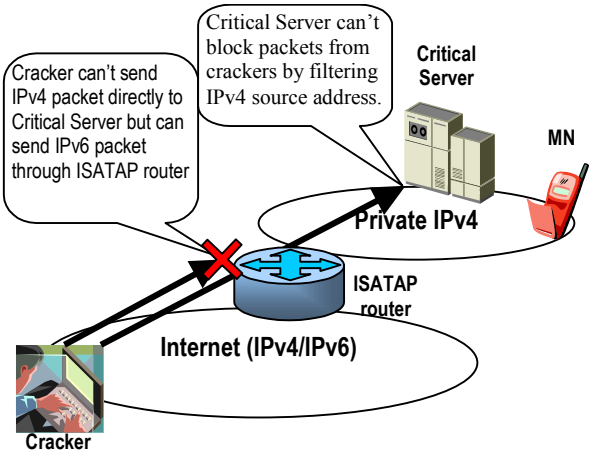


Figure 5: Attack from outside through ISATAP router

Figure 5 shows the example of attack from outside. Normally, private IPv4 address naturally avoids the direct attacks from the outside network, and currently many network sites use this fact as a security measure. But ISATAP router enables direct IPv6 access from outside networks. So when introducing ISATAP router, ISATAP router should authenticate and authorize MN's IP address for both security and accounting purposes. Any traffic to/from unauthorized IP address should be dropped in ISATAP router.

4. Proposal

4.1. EAP method for bootstrapping

4.1.1. Motivations

At first, we defined the new EAP method, which is one of the authentication methods of EAP. EAP, which can be conveyed on any various access or authentication protocols. EAP, by itself, doesn't have any authentication and authorization mechanism. It only defines 4 functions, Request, Response, Success and Fail. Many variety methods of authentication are defined as EAP methods, e.g., MD5-Challenge, TLS, AKA and PEAP etc. The important feature of EAP methods is that it is an End-to-End protocol. As shown in Figure 4, MN and AAAh (AAA server in Home Domain) implements EAP method, but the intermediate AAA nodes (AR and AAAv) are not required to implement EAP methods.

What we claim by this fact is that any EAP methods work independently from the implementation of Visited Domains. So, new EAP method we will propose here will work with any current Visited Domain (Network Access Provider).

On the other hand, new EAP method will be implemented on MN and AAA server in our proposal. MN and AAAh can be assumed to belong to the same network operator (because MN subscribes to Home Domain). So, single network operator can introduce any proprietary EAP method that works with any Visited Domain (Network Access Provider).

4.2. AAA for bootstrapping

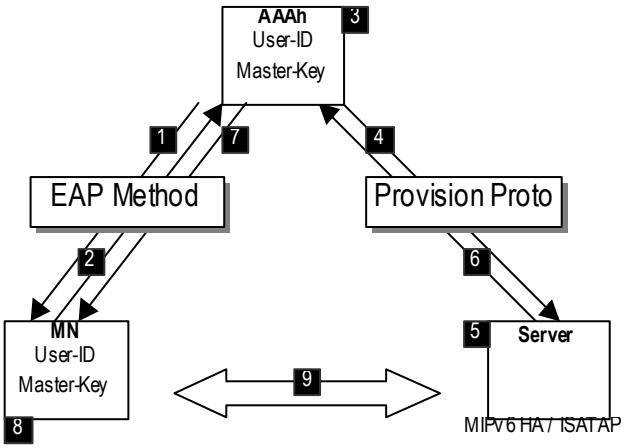
Figure 6 shows signal flow of AAA for Bootstrapping. Some statically assigned data is pictured in the square representing the network node (MN, Server (MIPv6 HA or ISATAP router) and AAAh). As mentioned before, User-ID and Master-Key is statically assigned in MN. They are also registered in kind of database of AAAh. Server has no prior static data about each MN. Probably, AAAh and Server have some general Service Parameters about each Service (MIPv6 or ISATAP) but no parameters about each MN. IP Address of ISATAP router is one example of Service Parameters kept by AAAh. AAAh knows Visited Network of MN, and then it can assign ISATAP router in Visited Network of MN.

Next, each step of bootstrapping MIPv6 in Figure 6 will be explained.

1 EAP interaction starts between AAAh and MN. AAA front-end protocol invokes it and AAA back-end protocol connects Visited Network and Home Network.

2 MN generates EAP-Nonce (random octet string)

and calculates EAP-Key (= Hashing Master-Key and EAP-Nonce). To prevent EAP-Key over the air, MN will send EAP-Nonce and authentication information (e.g. User-ID and MD5-Response) (and Service Parameters owned by MN if exists) to AAAh. EAP-Key will be used later.



(1) Send Request for EAP/Service (MIPv6 or ISATAP)
(2) Generate EAP-Nonce, Calc EAP-Key (= HASH(Master-Key, EAP-Nonce) (Send (User-ID, EAP-Nonce, Service Parameters of MN, e.g. MN's IP
(3) Calc EAP-Key (= HASH(Master-Key, EAP-Nonce), Generate Service-Nonce and Calc Shared-Key(= HASH(Master-Key, Service-Nonce) and Assign (Service Parameters of AAAh, e.g. Server's IP Address, Lifetime etc)
(4) Send (Shared-Key, MN Parameters, Service Parameters of MN + AAAh)
(5) Register (Shared-Key, MN Parameters, Service Parameters of MN + AAAh) and Assign (Service Parameters of Server, e.g. ISATAP IPv6 Prefix)
(6) Send (Service Parameters of Server)
(7) Send (Service-Nonce, Service Parameters of AAAh + Server) (encrypted by EAP-Key)
(8) Decrypt the packet from AAAh by EAP-Key and Calc Shared-Key for Service Authentication (= Hash (Master-Key, Service-Nonce))
(9) Shared-Key and Service Parameters of MN + AAAh + Server are shared between MN and Server (then, Service will be established)

Figure 6: AAA for Bootstrapping

3 On receiving EAP packet from MN, AAAh will assign Service Parameters configured in AAAh (e.g. MIPv6 Home Agent, ISATAP router). How to select Service Parameters is out of scope in this paper but it could be based on the location of MN, load balance of Servers. AAAh will calculate EAP-Key (= Hashing Master-Key and EAP-Nonce, generates Service-Nonce and calculates Shared-Key (= Hashing Master-Key and Service Nonce). Shared-Key will be used for authentication or security of Service between MN and Server.

4 AAAh sends Shared-Key and Service Parameters configured in AAAh over Provision Protocol.

5 On receiving Shared-Key and Service Parameters configured in AAAh, Server registers and assigns Service Parameters. It may also assign other Service Parameters configured (or newly assigned) in Server (e.g. IPv6 Prefix of ISATAP interface, SPI for IPsec SA).

6 HA sends Service Parameters configured in (or assigned in Step 5 by) Server to AAAh over Provision Protocol.

7 AAAh will forward Service-Nonce and Service Parameters from Server and Service Parameters configured in AAAh to MN. This message is encrypted by EAP-Key (calculated in Step 3).

8 On receiving EAP packet from AAAh, MN decrypts this message by EAP-Key (calculated in Step 2). The decrypted message includes Service-Nonce, Service Parameters configured in both AAAh and Server. Then, MN calculates Shared-Key (= Hashing Master-Key and Service-Nonce) for the authentication or security of Service between MN and Server.

9 In the case of MIPv6, MN will send BU and HA will send BA. Service-Key protects both messages. In the case of ISATAP, more interaction would be necessary when using IPsec because MN might not been assigned IP address (e.g. by DHCP, PPP) before the authentication finishes. In that case, another protocol is necessary to establish IPsec SA between ISATAP router (Server) and MN. IKE can do it but lighter and simpler (maybe proprietary) protocol will be suitable if exists because the shared key has been generated and shared already.

5. Evaluation

In order to evaluate our proposal, we will compare 3 methods to bootstrap MIPv6 and ISATAP.

5.1. Static Method for bootstrapping

In static methods, all necessary parameters to bootstrap (except IPv4 and IPv6 addresses) are assumed to be statically defined and manually configured. So, no dynamic service discovery is possible.

5.2. Dynamic Method for bootstrapping

In dynamic methods, all necessary parameters to bootstrap are dynamically allocated and configured as much as possible by using methods described in the specifications, e.g. Home Agent Address will be allocated by Dynamic Home Agent Discovery, ISATAP router address will be allocated by DNS,

IPsec parameters are configured by IKE etc.

5.3. AAA Method for bootstrapping

Defined in Section 4.2.

5.4. Management Costs Evaluation

It is difficult to quantify the management cost. So, as a simple indication for this, we will use the number of items to be configured in each node. Especially, the number of configured items in Mobile Node is important because they are hard to be remotely changed by the network operator.

Especially, any static IP address configuration in MN (e.g. MIPv6 Home Address, ISATAP router address) will restrict the network design. It makes it difficult for the network operator to change their network topologies.

	Configuration Parameters
Static	AAA User-ID AAA Shared-Key Mobile IPv6 Home Address Mobile IPv6 Home Agent Address IPsec Shared-Key (BU) IPsec Encryption Algorithm (BU) IPsec SPI (BU) IPsec Shared-Key (BA) IPsec Encryption Algorithm (BA) IPsec SPI (BA)
Dynamic	AAA User-ID AAA Shared-Key Mobile IPv6 Home Address IKE User-ID IKE Shared-Key (or Certificate)
AAA	AAA User-ID AAA Shared-Key

Table 1: MN Parameters for MIPv6

	Configuration Parameters
Static	AAA User-ID AAA Shared-Key ISATAP router Address IPsec Shared-Key IPsec Encryption Algorithm IPsec SPI
Dynamic	AAA User-ID AAA Shared-Key IKE User-ID IKE Shared-Key (or Certificate)
AAA	AAA User-ID AAA Shared-Key

Table 2: MN Parameters for ISATAP

As shown in Table 1 and Table 2, static method demands lots of configuration parameters. It is unrealistic to define details of IPsec SA preliminarily. Even dynamic methods demands more parameters to be configured than our proposal.

5.5. Performance Evaluation

In most of wireless networks, especially cellular networks, the delay of wireless link is dominant for the delay of packet transfer. Then, we count the number of frames over the wireless link (in other words, between mobile node and any network node) when bootstrapping.

	Protocol	Frames
Static	802.1x	3
	EAP (MD5)	2
	IPv6 RS/RA	2
	MIPv6 BU/BA	2
	Total	**9**
Dynamic	802.1x	3
	EAP (MD5)	2
	IPv6 RS/RA	2
	DHADP	2
	IKE[3]	6
	MIPv6 BU/BA	2
	Total	**17**
AAA	802.1x	3
	EAP (MIPv6)	4
	IPv6 RS/RA	2
	MIPv6 BU/BA	2
	Total	**11**

Table 3: Wireless Link Frames to bootstrap MIPv6

	Protocol	Frames
Static	802.1x	3
	EAP (MD5)	2
	DHCP	3
	IPv6 RS/RA	2
	Total	**10**
Dynamic	802.1x	3
	EAP (MD5)	2
	DHCP	3
	DNS	2
	IKE	6
	IPv6 RS/RA	2
	Total	**18**
AAA	802.1x	3
	EAP (ISATAP)	4
	DHCP	3
	Total	**10**

Table 4: Wireless Link Frames to bootstrap ISATAP

We assume that MD5-Challenge is used as EAP method, 802.1x is used as frontend AAA protocol and shortest packet transfers for IKE (6 transfers) in case of static and dynamic method. As shown in Table 3 and Table 4, dynamic method demands lots of packet transfers over the wireless link mainly because of IKE. It could be more if certificate-based authentication is used for IKE. On the other hand,

AAA-based method is not so different from static method in respect to this performance evaluation.

5.6. Performance Measurement

We also measured the performance of bootstrapping in our test-bed. All functionalities are implemented as software of NetBSD and are running on PC architecture. All nodes are connected via 100Base-T Ethernet. For Mobile IPv6, the delay from starting AAA (authentication) and to finishing MIPv6 BU/BA was measured. And for ISATAP, the delay from starting AAA and to finishing to assign ISATAP IPv6 address to MN was measured. It is same as described in the previous section.

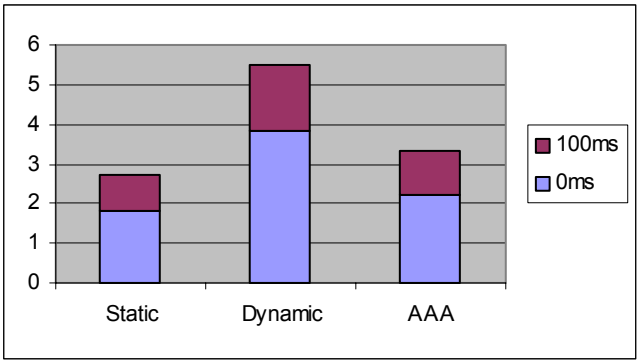


Figure 7: Delay to Bootstrap Mobile IPv6

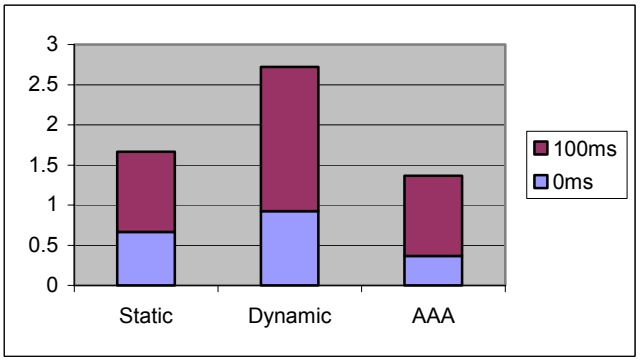


Figure 8: Delay to Bootstrap ISATAP

In each graph, 2 delay values are illustrated for each method. One is under the assumption that the wireless link delay is 0ms, and one is 100ms. Though those values include software delay that should be eliminated, significant software delays have been removed from these values already.

6. Conclusion

We considered and evaluated 3 methods for bootstrapping, static method, dynamic method and AAA method in terms of 2 points, management costs and bootstrapping delay. For the evaluation of the management costs, we listed up the necessary parameters (in MN, AAAh, MIPv6 HA and ISATAP router). The method that demands more parameters causes more management costs and more restrictions for the network design. As described in section 5.5, AAA method demands lesser configuration parameters for MN than dynamic method.

In terms of the performance, the delays of static method and AAA method are not so different. But the delay of dynamic method is clearly larger than others. If we assume the wireless link is more, the difference between dynamic case and others are larger.

When considering the packet loss of the wireless link, the dynamic method has weakness. It is because it has much more signals over the air then it is easy to loss the signals and retransmit them. The packet loss causes much more bootstrapping delay.

Considering all the various factors together, static method and dynamic method still has shortness for bootstrapping. Another supportive protocol or architecture is necessary for bootstrapping, especially in the commercial cellular networks. We think our proposal, AAA method, can provide the solution for this.

Reference

[1] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[2] Yamamoto, S., Yokota, H., Williams, C., Parthasarathy, M., “Mobile IPv6 Node traversal of IPv4 subnets using automatic tunnels”, draft-yamamoto-mipv6node-v4trav-00.txt, February 2004.

[3] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[4] P. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A. Rubens, "Diameter Base Protocol", RFC 3588, September 2003.

[5] P. Eronen, T. Hiller and G. Zorn, “Diameter Extensible Authentication Protocol (EAP) Application”, draft-ietf-aaa-eap-09.txt, August 2004.

[6] Calhoun, P., Johansson, T., Perkins, C., Hiller, T. and McCann, P., “Diameter Mobile IPv4 Application”, draft-ietf-aaa-diameter-mobileip-20.txt, August 2004.

[7] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin, “Protocol for Carrying Authentication for Network Access (PANA)”, draft-ietf-pana-pana-05.txt, July 2004.

[8] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, “Extensible Authentication Protocol (EAP)”, RFC 3748, June 2004.