Mobile IPv6 상에서 AAA 기반의 지역화된 키 관리 기법에 관한 연구☆

A Study on the Localized Key Management Using AAA in Mobile IPv6

김 미 영* 문 영 성**
Mi-Young Kim Young-Song Mun

요 약

Mobile IPv6 서비스는 특성상 다수의 서로 다른 관리 도메인에 속한 망간에 걸쳐 IP 계층의 로밍이 발생하므로 많은 취약점을 가지고 있다. 특히, 무선 인터넷 사용자의 로밍으로 인해 사업자간 망간에 걸쳐있는 망 노드들간 인증을 제공하는 안전한 로밍 서비스 기술 즉, AAA 기술이 기본적으로 요구된다. 이러한 로밍 서비스는 통신 사업자의 망간에 걸쳐 있으므로 제도적인 측면, 기술적인 측면에서 다양한 요구사항들이 반영 되어야 한다.
본 논문에서 제안하는 구조는 로밍 서비스를 위해 Mobile IPv6를 적용하고, AAA 관련 메시지의 전송 횟수를 줄이기 위해인증에 필요한 전체적인 트래픽 양 및 메시지 교환 횟수를 최적화하는 키 분배를 위한 서비스 구조를 제안한다.

Abstract

Mobile IPv6 services exposes its vulnerability when a mobile node is roaming across the subnets which belongs to the different domains. The AAA infrastructure is strongly recommended when the ISPs need to authenticate the mobile user come from the different domains. In addition to the basic requirements for AAA service, the authentication latency and AAA message overhead should be minimized for contiguity of the service. This paper considers the roaming service with AAA infra structure in Mobile IPv6 and proposes the key distribution method to authenticate the mobile node with secure manner by reducing and optimizing the exchanged messages for AAA entities.

키워드 : Mobile IPv6, AAA(Authentication, Authorization, Accounting)

1. Introduction and Related Works

This paper specifies the way of authentication procedure which should be performed when a mobile node is accessing a network in the visited link. When a mobile node moves from a domain to another in away from home, if the framework such as AAA to provide the robust authentication in a secure way does not exist then an access to the resources in visited link will not be allowed in which results a mobile node fail on keeping on-going sessions. The Mobile IP draft-18 dose not specify a way how to authenticate a mobile node roaming across the different domains. For example, in a 802.11 wireless network[5], when a node tries to get an access to AP(Access Point) it should get the right to use the resources of that network with prior to any mobility supporting operations. If

☆ 본 연구는 숭실대학교 교내연구비 지원으로 이루어졌음

* 정 회 원 : 숭실대학교 컴퓨터학과 박사수료
mizero31@sunny.soongsil.ac.kr (제 1저자)
** 종신회원 : 숭실대학교 컴퓨터학부 부교수
mun@computing.ssu.ac.kr (공동저자)

this process fails, the mobile node is not allowed to use that link so that on-going sessions will be dropped. To get a continuous mobility service, the contract and authentication method between the different domains should be established to enable inter-domain roaming.

In general, there are 12 steps to complete the authentication for inter-domain roaming[1]. The embedding option to send a Binding Update and Binding Acknowledgement within AAA messages exchanged between AAA servers is proposed but it is exposed to an attacker since the mobility information(BU/BA) is used before SAs between mobile node and attendant are established. The embedding option to send a Binding Update and Binding Acknowledgement within AAA messages exchanged between AAA servers is proposed[3] but it is exposed to an attacker since the mobility information(BU/BA) is used before SAs between mobile node and attendant are established.

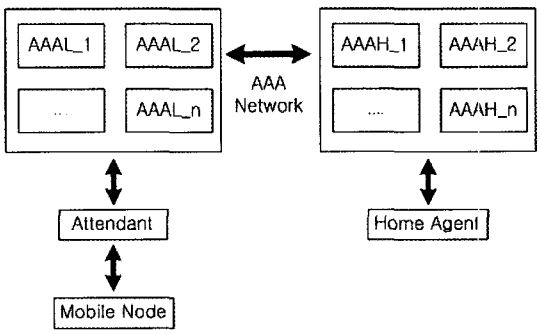
2. Proposed Scheme

2.1 Delegation Model

An option is defined to delegate the V_AAA to manage the keying materials and SAs context for MN. When MN enters the visited link in different domain, the 12 steps described in [1] are performed to get a session_key and registers the MN's current location. If MN sends the AReq message with delegation option, this message is relayed to the entity such as H_AAA or Home Agent which plays the role of generating and distributing session key and keying materials. If H_AAA has the right to manage the keying materials, the security context used to authenticate and generate session_key for MN is transferred when H_AAA responds to the m_AR with h_AA. Then V_AAA will receive the h_AA message with security context. V_AAA compares its capabilities with security context (SAs, algorithms, hash functions, etc.). If it has capabilities specified in the security context then V_AAA create an entry into the delegation entry list to accept and process delegation request. If it has insufficient capabilities, the delegation request is ignored and the message is processed as specified in [1]. If MN moves to another visited link in the same domain with MN's previous location and the delegation request option is set, V_AAA determines whether the MN is registered in delegation entry list. If the entry exists then V_AAA authenticates the MN and generates the session_key according to the security context. After the delegation procedure is completed, V_AAA responds to m_AR with h_AA which contains session_key, keying materials and some security parameters. When the home agent has the right to manage the keying materials, the security context is transferred when the home agent responds to AHR with AHA. The rest of processing is identical to the procedure described above.

2.2 Authentication Path

There may exist one or more AAA servers in a domain for the purpose of redundancy or administrative policy.



(Figure 1) AAA Authentication Mode with Multiple AAA Servers

By delegation, V_AAA has an entry with security context for MN. But this entry information is not

distribute to all AAA servers in the visited domain because it is difficult to manage the AAA servers with consistency for refreshment and deletion of the entry. To distinguish and select the exact V_AAA which is used in the first request for the delegation, the 'Authentication Path' is defined. The authentication path consists of the NAI of H_AAA and V_AAA which is returned by H_AAA and V_AAA. If the delegation option is set, when H_AAA returns the h_AA after processing the AHA, it returns h_AA with it's NAI. When V_AAA returns h_AA the NAI of V_AAA is also added into h_AA. MN receives the ARsp from attendant which contains the authentication path(NAI of V_AAA and H_AAA) and saves it into local storage or memory. In the next movement to another link in the same domain, MN uses this information to specify the AAA server which maintains the delegation entry for MN.

2.3 Messages

The messages related on authentication are as below[1].

- AS(Attendant Solicitation): First message between the attendant and the mobile node. It is sent by the mobile node and its purpose is to discover or to select an attendant. At the point of time the MN knows its mobility it send this message to the attendant.
- AA(Attendant Advertisement): Second message between the attendant and the mobile node. It is sent by the attendant and carries a local challenge issued or transmitted by the attendant. The local challenge is used for authenticating the messages between mobile node and attendant until the SA is established.
- AReq(Authentication Request): Third message between the attendant and the mobile node. It is sent by the mobile node in order to ask for the allocation or the registration of local/care-of address. This message is loosely authenticated by the local challenge repeated from the AA.
- ARsp(Authentication Response): Forth/Last message between the attendant and the mobile node. It is sent by the attendant. We assume that in general the mobile node must wait for this message before sending a home registration (because this message validates the care-of address).
- m_AR(Authentication Request from MN): AAA message from the attendant to the AAAH. This is the first AAA message(AAA message contains under score in the message name). The contents of this messages are mapped from the MN request, AReq.
- h_AA(Authentication Answer from HA): AAA message from the AAAH to the attendant. This is the final AAA message(AAA message contains under score in message name). It contains the session key and keying materials to distribute to attendant and mobile node. The attendant plays a role of mapping the contents of AReq/m_AR and ARsp/h_AA.
- AHR(Authentication Home Agent Request): Second AAA message from the AAAH to the HA. The contents of it is identical to m_AR.
- AHA(Authentication Home Agent Answer): Third AAA message from the HA to the AAAH. It is mapped into h_AA.
- ASK(Security Key from AAA): When the 'Delegation' is used, the session key generated by local AAA server(V_AAA) should be sent to MN's Home Agent to authenticate the binding registration messages. This messages is for carrying the created session key and additional information about the MN. BU(Binding Update): As defined in [4].
- RC(AAA Result Code): It consists of the operation status(success(1)/fail(0)) and the cause code.

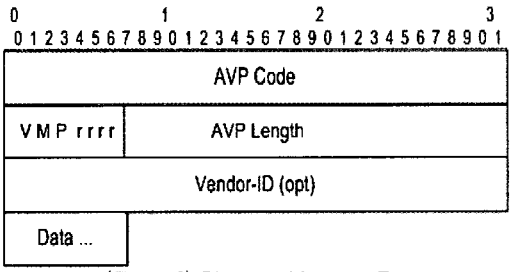
2.4 New Commands and AVPs

The Diameter[2] protocol is flexible to extend with the new commands and parameters(AVP: Attribute Value Pair). In this section, we describe the commands and AVPs newly defined to form the Diameter messages from the request/response messages exchanged between MN and attendant. This paper introduces four new Command Codes:

AA-Authentication-Request-from-MN(MAR)
AA-Authentication-Answer-from-H_AAA(HAA)
AA-Authentication-Request-to-HA(AHR)
AA-Authentication-Answer-from-HA(ARA)
Security-Key-from-AAA(ASK)

2.4.1 New AVPs

The general format for Diameter AVP is defined like as [2]:

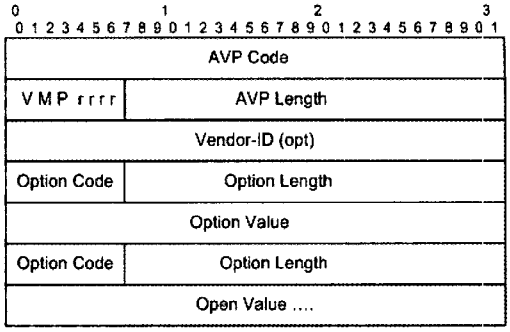


(Figure 2) Diameter Message Format

Various AVPs are defined by Diameter WG as the standard parameters exchanged between Diameter peers[2]. In the message format, the length of the 'Data' field is variable and any type of data can be encoded into that field.

We also define the 'Option' to carry the multiple parameters within an AVP. The options with the similar meaning are grouped into the same AVP. One or more options can exist in 'Data' field with distinct Option code and value.

-Option Code: Code value assigned to each 'Options'(0-127)
-Option Length: The length of 'Option Value' (Byte or Octet)
-Option Value: The contents of the 'Option'



(Figure 3) Diameter AVP Format

To form and represent the Diameter message parameters by referencing the non-Diameter message sent by the MN, the new AVPs are defined as below. Group 1 Address AVP(Assigned Code1). It specifies the options related on address processing such as CoA, HoA and HA's address. Group 2 Security AVP(Assigned Code2). It specifies the options related on security processing such as Authentication, Session-Key, Keying-Materials, Security-Parameter, Security-Context and Random Number. Group 3 Authentication-Path AVP(Assigned Code3). It specifies the options related on authentication path to distinguish first path where the MN is authenticated in the visited link. NAI is used for this purpose. Group 4 Action AVP(Assigned Code4). It specifies the options for actions requested from the MN and HA. Delegation, Delegation-Lifetime, Dynamic-Home-Agent-Discovery and Result-Code options are defined for this AVP.

2.5 Message Flow In Delegation for Session Key

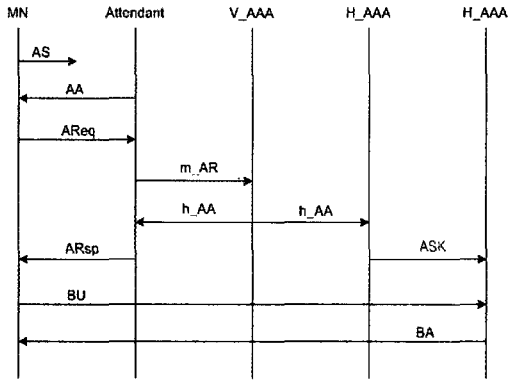
The V_AAA has a delegation entry for the MN after finished the request from MN which had a Delegation-Option if it was successful. The V_AAA can take two steps for processing the request with the delegation option. First, it checks whether the NAI or CoA of the MN is

belong to the delegation list in V_AAA.(It means that the delegation is already processed through this V_AAA server and the lifetime of it is not expired yet.) Second, if the delegation entry for MN has found in V_AAA, it generates the session key between the MN and Attendant that allows the MN to use the network resources(e.g. wireless link) in the visited domain or area(Attendant) and delivers it to the MN when returning the h_AA message by adding the options for the session key(Session-Key-Option, Key-Materials-Option). We depicts the delegation processing after the delegation list entry for MN has created in V_AAA.(It means that the MN has entered the visited domain and moves across one or more subnets which belongs the same domain) The procedure for the authentication request from MN is performed as the following sequence:

Step 1. Message: Attendant Solicitation
Send to: IPv6 multicast address. Parameters (AVPs): None Pre-condition: None Behavior: MN tries to find the attendant(entry point of visited link) by sending this message at the time when MN knows it has moved. If there is no reply from attendant, this message is issued periodically until it finds out the attendant.

Step 2. Message: Attendant Advertisement
Send to: MN's address(Care-of). Pre-condition: None. Behavior: If AS message received from MN, replies to MN with local challenge used to authenticate the AReq message in Step 3. The local challenge is likely to be a random number or cookie.

Step 3. Message: Authentication Request
Send to: discovered attendant address Precondition : None. Behavior: MN sends AReq to request the attendant to perform the AAA protocol operations to get a session key. The parameters included in this message are LC(local challenge), NAI for MN and AAA servers(for Authentication Path), Nonce, Home address of



(Figure 4) Message Sequence for Authentication

MN, Home agent address on MN, Authenticator(signature of the parameter set), Delegation Option(True or False).

Step 4. Message: Authentication Request for MN
Send to: Local AAA server in visited domain(V_AAA). Pre-condition: The communication channel between attendant and V_AAA is secure with some key materials for protection of AAA message.
Behavior: Same content as the previous IPv6 packet (translated to AAA message). The attendant extracts the payload data from AReq and constructs a new m_AR message with parameter set from the payload. When the V_AAA receives this message, it validates the NAI of the MN to decide if the requests will be allowed or not. If it is not valid then the V_AAA should send the h_AA to attendant with Result-Code-Option of the Action-AVP. In successful, if it contains the Action AVP with Delegation-Option then the V_AAA looks up the delegation entry if an entry for MN exists or not. The parameters for m_AR are Authentication-Path AVP(NAI-Option). Address AVP(Care-of-Address-Option, Home-Address-Option, Home-Agent-Address-Option). Security AVP Authenticator-Option(Nonce-Option, Security-Parameter-Option). Action AVP (Delegation-Option). If the entry exists and the lifetime is still alive then the V_AAA can compute the

session_key and its keying materials as follow. session_key = prf(N_m | N_a, m_HoA, m_CoA, a_R), key_material = {Nonces(N_a, N_m), SPI, HASH,..} where, N_a is a nonce value generated by the V_AAA in behalf of the MN's Home Agent or H_AAA server. m_HoA and m_CoA are the Home Address and Care-of Address of the MN as described before. The a_R is a random number generated by V_AAA for each required session key. All parameters except for the random number and nonce are referenced from the Security Context in the delegation list entry for MN.

Step 5. Message: Authentication Answer

Send to: Attendant. Pre-condition: None Behavior: V_AAA generates and delivers the session key and keying materials to Attendant. Result-Code-Option indicates the result of authentication request.

Security AVP(Authenticator-Option, Session-Key -Option, Key-Materials-Option, Nonce-Option, Random-Number-Option). Action AVP(Result-Code-Option)

In this step, it must send the clone of the session_key to the MN's H_AAA or HA. In case of this flow, the ASK message is used to carry the session key and additional information about the MN.

Security AVP(Session-Key Option). Address AVP (Home-Address-Option, Home-Agent-Address -Option)

The session key forwarded to MN's home agent is used to authenticate the consequence binding registration messages from the MN.

Step 6. Message: Authentication Response

Sent to: MN's CoA. Pre-condition: None

Behavior: When the attendant receives this message, it should extracts the session_key with MN and stores it into it's local storage area to authenticate the session between the MN and the attendant. Notice that it should not send the session_key itself to the MN before the session is protected by it. The attendant converts the AAA(Diameter) message into the message known to the MN and Attendant(e.g. EAP). The parameters for ARsp are Nonce(which generated by V_AAA for replay protection), Keying Materials, Random Number, Authenticator.

Step 7. Message: Binding Update

Send to: MN's home agent. Pre-condition: SAs exist between mobile node and it's home agent. Behavior: It takes the same actions as Step 11 described in [1](General Flow).

Step 8. Message: Binding Acknowledgement

Pre-condition: None. Behavior: HA performs the binding registration procedure as described in mobile IP[4].

By using the delegation, the round trips are reduced to 8 steps. When MN is roaming rapidly across the subnets within a domain, the MN tries to get a session key to access the communication resource of the visited link.

3. Conclusion

The AAA infrastructure(Diameter) is used to distribute the security key with secure manner. To optimize the message exchange steps and to provides the continuity of the mobility service, we introduces the 'Delegation Model' which enables the MN to establish the session key with its Home Agent and the attendant in the visited link. The delegation model defined in this paper does not create new security breaches for the IPv6 MN and AAA entities in home and visited domain. On the contrary, it allows for an effective and efficient authentication and authorization to the MN when roaming across the subnet links in the same domain as well as between different domains.

Reference

[1] F. Dupont, J. Bournelle " AAA for Mobile IPv6", draft-dupont-mipv6-aaa-01.txt,

Internet Draft, IETF, Nov, 2001.
[2] Pat R. Calhoun, Erik Guttman, Jari Arkko, "Diameter Base Protocol", draft-ietf-aaa-diameter-12.txt, Internet Draft, IETF, July,2002.
[3] Pat R. Calhoun, Tony Johansson, Charles E. Perkins, "Diameter Mobile IPv4 Application", draft-ietf-aaa-diameter-mobileip-11.txt, Internet Draft, IETF, June, 2002.
[4] Davied B. Johnson, Charles E. Perkins, Jari Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-18.txt, Internet Draft, IETF, June, 2002.
[5] IEEE, "Part 11: Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications", 1999.
[6] P.Calhoun, C.Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, IETF, March, 2000.
[7] Franck Le, Basavaraj Patil, Charles E. Perkins "Diameter Mobile IPv6 Application", draft-le-aaa-diameter-mobileipv6-01.txt, Internet Draft, IETF, November, 2001.
[8] Pat R. Calhoun, Charles E. Perkins, "Diameter Mobile IPv4 Application" Internet draft, Internet Engineer Task Force, November 2001.

◐ 저 자 소 개 ◑

김 미 영

1992년 전주우석대학교 전산학과 (학사)
1995년 광운대학교 대학원 전산학과 (석사)
1995년~1997년 (주)필컴 시스템 개발부 근무
2000년~현재 : 숭실대학교 대학원 컴퓨터학과 박사과정
관심분야 : Mobile IP, AAA, Network Security
E-mail : mizero31@sunny.soongsil.ac.kr

문 영 성

1993년 연세대학교 전자공학과 (학사)
1986년 Univ. of Alberta 전자공학과 (석사)
1993년 Univ. of Texas, Arlington 전산학과 (박사)
1994년~현재 : 숭실대학교 컴퓨터학부 부교수
관심분야 : Mobile IP, IPv6, Security
E-mail : mun@computing.ssu.ac.kr