INTERNET-DRAFT
Expires May 2003

Miyoung Kim
Youngsong Mun
Soongsil University
Jaehoon Nah
Seungwon Sohn
ETRI
Nov 2002

Dynamic Binding Update using AAA
<draft-mun-aaa-dbu-mobileipv6-00.txt>

Status of this Memo

Abstract

This document describes the procedure of how dose the Mobile Node(MN) exchange the messages with it's Corresponeant Node(CN) by using the secure communication platform, the AAA infrastructure that consists of the many AAA servers in different domains when the MN is about to enter the visited link.

The MIPv6 node (MN, CN or both) has the unique identifier, NAI (Network Access Identifier) to distinguish itself from others and by parsing the NAI[5], we can get the information on which domain the MN

belongs.

In this document, we consider the main idea is applied into two different cases. The first case is that the MN and CN are belonged to the same domain which means that the MN and CN has the same domain identifier in their NAI. In this case, the two nodes have the same AAA server. Another case is denoted as the MN and CN belong to the different domain in which the two nodes have the different AAA servers.

We assume that the AAA servers are connected each other using the secure communication protocols (e.g. DIAMETER) and they have the common and global roaming contracts for mobility service.
By this assumptions, the AAA server in the MN's visited domain is responsible for processing the request from the MN which comes from the different domain and passing it to the MN's home AAA server using its AAA infrastructure.

We use the 'Diameter' protocol as the AAA infrastructure which is extendible for our purpose and guarantees the secure communications. Comparing to another AAA protocol (e.g. RADIUS), the Diameter reduced and optimized the message round-trips for their use.
(However, we don't set limits to use Diameter. If another protocol is developed and proved as it is secure, the new one can be applied to these cases.)

In this document, we define the new Diameter messages and AVPs to provide the functionalities for making it possible that the MN is roaming across the different domains. Also, we describe the procedure to exchange the messages(and AVPs) between MN and CN.

Using this procedure, the mobile entities(MN and CN) are able to share the keying-materials which are used to derive the secure key to protect the 'Binding Registration(BU/BA)' and 'Route Optimization' messages.

1. Introduction

We introduce the new Diameter messages and the related AVPs to deliver the parameters needed from considering the two cases as described earlier.

In the case of a large amount of traffic occurs between the MN and

CN, the route optimization procedure can take place to optimize the packet routing[2] and the secret key is used to make the BU/BA messages secure.

To protect the binding information, the various methods are proposed. These methods provide the strong-level of security however it is the burden for the mobile node since each received packets encrypted with the strong-level of security algorithms are also decrypted by the mobile node with the same mechanism where the node is most likely the battery-powered device. IPSec/IKE is tested for many mobile consider-

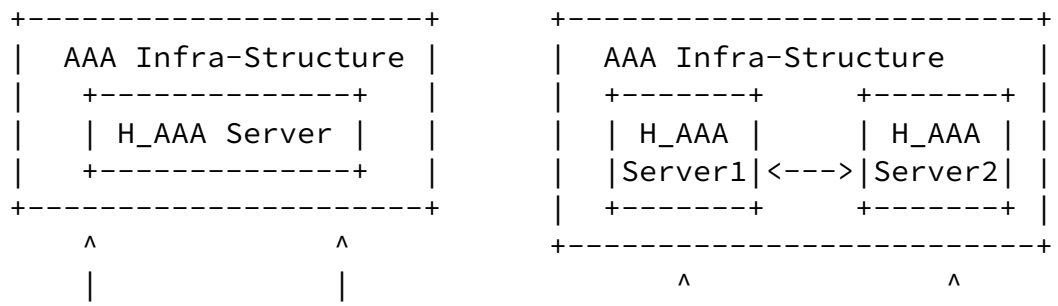
ations to bring it into MIPv6, however the test results are reported as it is contrary to expectations for their performance and extensibility for the large scale mobile networks.[6]

Another mechanism, the RR(Return Routablity) is proposed to protect the binding information to simplify the distribution of the keying-materials without depending on the underlying infrastructure where the MN starts the procedure and the CN is responsible for making the binding key and distributing the keying-materials to the MN. However, even if the MN implements the strong-level of security algorithms and it negotiates with the CN for the security key to make the RO more secure, the attacker in the middle of them is able to eavesdrop the negotiation packets and bring down the level of security algorithm by forging the packets of deceiving the two nodes (Bidding Down Attack). This can be a big problem since the level of security provided by the RR isn't strong now.

In our proposal, we introduce the methods with Diameter message exchange between the mobile entities(MN and CN) without using the RR.

2. Model and Entities

The model and entities for our proposal is denoted as:



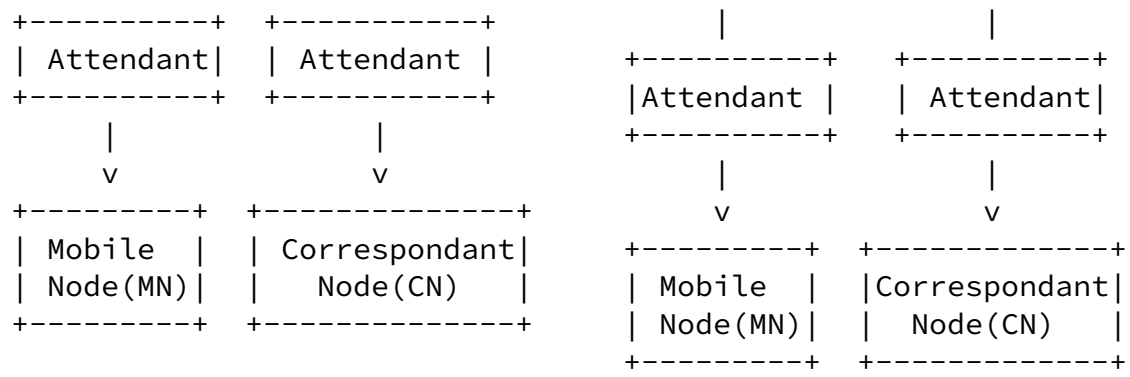


Figure 1. AAA Authentication Model

The Diameter network provides the Diameter servers with secure communication infrastructure[1]. Entering to the visited link, the MN has to be authenticated by the authentication entity in the link to gain the access for the link. The Attendant is the first

entity the MN tries to connect when it enters into the visited link. At this point, the MN searches the attendant using the layer-2 protocol(e.g. ethernet broadcast) and the EAP protocol(also layer 2) is used to send and receive the authentication request/ response messages between the MN and Attendant since the IP adress is not allocated to the MN and the access from the MN is not granted by the local authentication entity.

The left-side of the figure shows that the MN and CN belong to the same domain where they have the same AAA server. Another side of figure shows that the MN and CN which belong to the different domains are communicating.

The entities to provide the mobility and roaming service in the same or different domains are Home AAA server, Local AAA server(in visited link), Attendant, MN, CN, and HA.

- Home AAA server (H_AAA): AAA server in MIPv6 node's home domain.

- Local AAA server (V_AAA): AAA server in the domain the MN is visiting.

- Home Agent: A node in the MNPv6 node's home link which is able to maintain the binding information and process the 'Home

Registration' message from the MN to provide the MN with mobility service.

- Attendant: An entity which is capable of controlling the access from the MN to use the visited link. Attendant is the first entity the MN connects to and it plays a role as the bridge between the MN and the visited network. The link between the MN and Attendant(Air) MUST be secure with the session key.

- Mobile Node(MN): a node implementing MIPv4/v6 [2]

- Correspondant Node(CN): A node implementing MIPv4/v6 [2] and communicating with the MN. It is responsible for generating the secure key and distributing the keying-materials to the MN when performing the RO(Route Optimization)

3. Message Definition

The messages are listed as:

AReq(Attendant Request): The first authentication message from issued by the MN. It is used for MN to request the establishment of the session key(MN <-> Attendant), and Route Optimization(MN <-> CN). This message is encoded as the form of Layer-2 protocol, EAPoL(EAP over LAN) even though the MN has configured its CoA from the local DHCP server since the AReq is sent from the MN before establishing the session key and the CoA is not granted to access the link

at that point of time.

AMR(AA-MN-Request): A Diameter message converted and mapped by the Attendant from the AReq(EAPoL) message sent from the MN to request the authentication and keying-materials. Attendant relays this message to it's local AAA server which delivers it to the MN's home AAA server for further processing.

ACR(AAA-CN-Request): The message sent from the AAA server to the CN which contains the parameters of keying materials for generating the binding key. The AAA server converts the Diameter message into the other message form known to the CN. (This maybe the normal IP packets).

ACA(AA-CN-Answer): The response message for ACR sent from CN.

AMA(AA-MN-Answer): The Diameter message sent from the AAA server to the Attendant. The AAA server gathers the ACR the response message for ACA and constructs the Diameter message and AVPs by putting the parameters from the ACA into the AVPs.

ARsp(Attendant Response): The response message for AReq which is converted to EAPoL by the Attendant and sent to the MN.

4. Payloads (The contents of AVPs)

The parameters carried by the Diameter messages defined in Section 3 are as follow:

aaa_key: Keying materials generated by the MN(Algorithm, the secret value and lifetime for encryption)

attendant_key: Keying materials generated by the MN which is used to protect the messages between the MN and Attendant.

BU(Binding Update: The MIPv6 message to update or create the binding information. Home Registration MUST be processed.

BA(Binding Acknowledgement): The response message for received BU.

CR(MN Credential): The AAA credentials sent from the H_AAA to authenticate the MN. The MN may create the authentication information using the Diffie-Hellman public value and the H_AAA is able to authenticate the MN's validity by searching the DH public value.

SecureParam_I: The security parameters sent from the MN which contains the items(HASH_I, SA, Ni, KE, etc.) to establish the SA(Security Association).

SecureParam_R: The security parameters sent from the CN which

contains the items(HASH_R, SA, Nr, KE, etc.) to establish the SA.

NAI(MN's NAI): The identifier for the MN. It is used for the V_AAA server to find the home domain of the MN by referencing the domain part of the NAI and send the request messages from the MN to the AAA server in the MN's home domain.

Public_key: A public key of H_AAA.

RPI(Replay Protection Indicator): A random value(Timestamp, Nonce or Cookies) to provide the replay protection between the MN and H_AAA.

HoA(Home Address): MN's Home Address.

HaA(Home Agent Address): Home Agent's Address of the MN.

RC(Result Code): The result code for the AAA response messages.

5. Diameter Message and AVPs

In our proposal, we define the new Diameter messages and it's AVPs according to the Diameter message format described in [2].

There are two messages, AMR and AMA.
(The abbreviation name of the messages are identical to its name and message codes are not fixed here since it SHOULD be allocated by the IANA and Diameter WG later)

- AMR: AA-Authentication-Request-MN (Code: Not specified, Abbr: AMR)
- AMA: AA-Authentication-Answer-MN (Code: Not specified, Abbr: AMA)

New AVPs are:
Group1. Address AVP(Assigned code=1)
  : Defines the options related on the address processing.
  - Home-Address-Option: MN's home address (code=0x01)
  - CN-Address-Option: CN's address(code=0x03)
    The CN's address communicating with the MN. This option can be encoded multiply since the MN communicates with one or more CNs.

Group2. Security AVP(Assigned Code=2)
  : Defines the options related on the security processing.
  - Nonce-Option: Timestamp, Nonce or Cookies for replay protection. (code=0x01)
  - AAA-Key-Option: The keying-materials protected by the H_AAA's public key. It is used to protect the AAA messages (code=0x02)
  - Attendant-Key-Option: A key protected by the aaa_key(specified in AAA-Key-Option). This is used to protect the messages between MN and Attendant. (code=0x03)
  - Security-Parameter-Option: The keying materials protected by the aaa_key(specified in AAA-Key-Option). It contains the parameters (HASH, Nonce, SA, KE, etc.) to establish the SA for CN.(code=0x04)

- Authenticator-Option: The hash value to verify the integrity of the message payloads. This is a signature for the AVPs.(code=0x05)

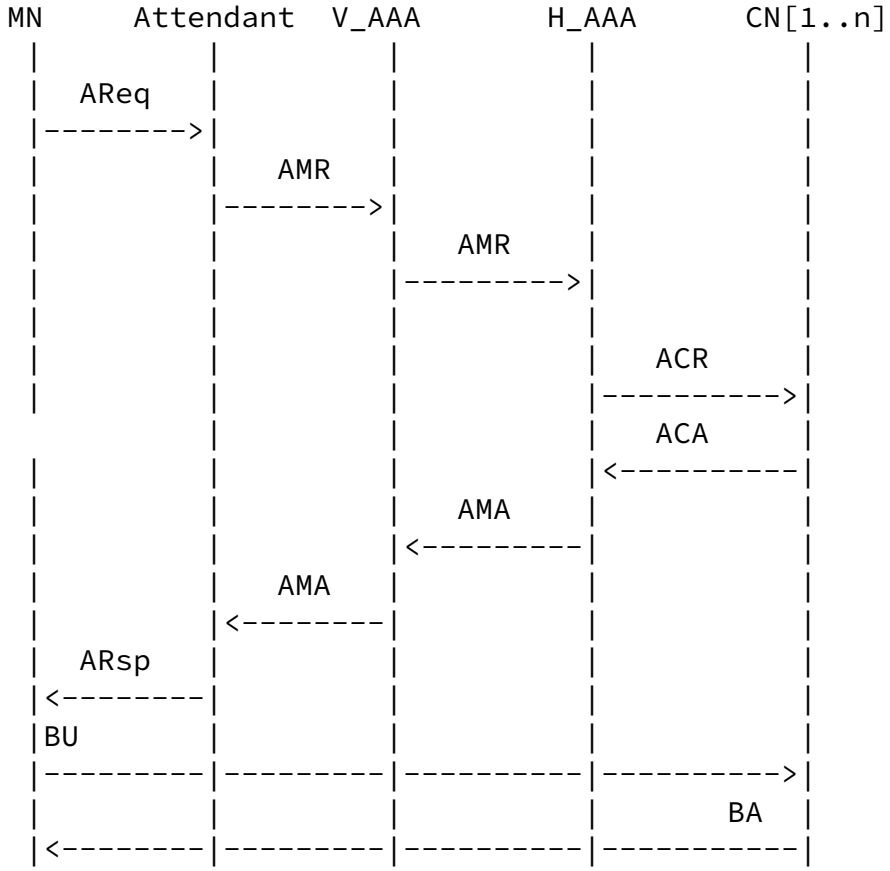
Group3. Authentication-Path AVP(Assigned Code = 3)
: Defines the NAI of the MN.
- NAI-Option: The MN's identifier to find the home AAA server of the MN(code=0x01)

Group4. Action AVP(Assigned Code = 4)
: Defines the option for the results of the AAA message processing. (code=0x01). It defines the following abnormal codes.
NAI_ROAMING_INVALID(1): Error on the wrong NAI(Invalid NAI) occurs or no roaming contract exists between the visited and home domains.
MSG_AUTHENTICATOR_ERR(2): The validation of message integiry has failed.(Message has changed from the illegal node.)
ACA_TIME_OUT(3): The H_AAA didn't get the response message for ACR during the specified waiting-time. (Response Timeout)

6. Protocol Overview

6.1 Binding Key Exchage between two nodes belong to the same domain

The following message exchanges occur for the nodes which belong to the same domain.



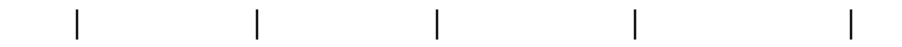


Figure 2.Binding Key Exchange between two nodes
belong to the same domain

When the MN is about to enter the visited link, it receives the Attendant Advertisement message from the Attendant or scans the attendant by sending the Attendant Search message and receiving the Attendant Response message. At this point of time, although the MN has configured it's CoA with stateful or stateless methods[2] from the local DHCP server or MN's interface ID and it's prefix value advertised from the local router, the IP packets outgoing and incoming from/to the MN are deffered or discarded by the attendant since the MN is not authenticated from the local AAA server and not allow to access the visited link. Therefore, the Layer-3 protocol, IP is unable to be used until the allocation of the session key by authentication between the MN and attendant is completed. So, the EAPoL(layer-2 protocol) is used between the MN and Attendant at this time and the Local Challenge(LC) advertised from the Attendant Advertisement message is used for providing the minimal security between them.

The following keys are needed to provide the secure roaming:

- MN-Attendant Session Key: The session key to protected the packets between the MN and attendant. After successful authentication of MN they share the session key.[6][7]

- MN-CN Binding Key: The binding key to protect the route optimization messages(BU and BA) exchanged between the MN and CN.

The following procedures represent the messages and its parameters for each step.

Step1. AReq(Attendant Request: MN -> Attendant)
To authenticate itself to the visited domain and to get the keying materials, the MN first sends the request message to the attendant using the EAPoL.
Parameters:
- Local Challenge: The random value copying from the previous 'Attendant Advertisement' message. This is used to protect the messages between the MN and Attendant.

- NAI: MN's identifier.
- RPI: A random value for replay protection(Timestamp, Nonce, or Cookies)
- HoA: MN's home address.
- HaA: MN's home-agent address.
- CnA: CN's address. This can be specified in multiple.
- aaa_key: A keying material protected by the H_AAA's public value. It is used to protect the AAA messages.
- attendant_key: A key protected by the aaa_key.
- SecureParam_I: The keying materials protected by th aaa_key which contains the various items to establish the Security Association.
- CR: An authenticator to verify the sender of the message and

check the integrity of that message.

Step2. AMR(AA-MN-Request: Attendant -> V_AAA)
Upon receiving the AReq message, the Attendant passes it to its AAA server with converted message.(Diameter message form)
Parameters:
- Address AVP
  Home-Address-Option(Code=0x01, HoA)
  Home-Agent-Address-Option(Code=0x02, HaA)
  CN-Address-Option(Code=0x03, CnA)
- Security AVP
  Nonce-Option(Code=0x01, RPI)
  AAA-Key-Option(Code=0x02, aaa_key)
  Attendant-Key-Option(Code=0x03, attendant_key)
  Security-Parameter-Option(Code=0x05, SecureParam_I)
  Authenticator-Option(CR)
- Authentication-Path AVP
  NAI-Option(Code=0x01, NAI)

Step3. AMR(AA-MN-Request: V_AAA -> H_AAA)
The V_AAA server looks up the MN's home AAA server by referencing the NAI option and forwards this message to that server.
Parameters:
- Same paramaters are used since it does modified on this message (just through passing)

Step4. ACR(AAA-CN-Request: H_AAA -> CN)
The purpose of this message is to deliver the keying materials sent from the MN to its CNs. The H_AAA server determines the address of

the CN by referencing the CnA parameter. If more than one CNs exist, which means the multiple CN's address CnA parameters are included in the message parameter, then the H_AAA SHOULD send the same message to the multiple targets after converting the previous message(AHR) to another form known to the CNs.
Parameters:
- HoA: MN's home address
- SecureParam_I: The keying materials protected by the aaa_key. It contains the various items (HASH_I, Ni, SA, KE, etc.) to establish the Security Association.

Step5. ACA(AA-CN-Answer: CN -> H_AAA)
As the response for the ACR request message, the CN stores the SecureParam_I received in Step4 into the secure local storage and returns the SecureParam_R the keying materials used to generate CN's Security Association.
Parameters:
- SecureParam_R: The parameters for establishing the Security Association for the CN.

Step6. AMA(AA-MN-Answer: H_AAA -> V_AAA)
After receiving the ACA the response messages for

ACR, the H_AAA server constructs the Diameter message to send. If the ACR message was sent to the multiple CNs then, it waits the response messages(ACA) from them until the specified timer (lifetime) expires. If it can't receive the response message from some CNs, the H_AAA sets the 'ACA_TIME_OUT(4)' in the Result Code for the CNs when returning this messages.
Parameters:
- Address AVP
  Home-Address-Option(Code=0x01, HoA): Optional
  Home-Agent-Address-Option(Code=0x02, HaA): Optional
- Security AVP
  Security-Parameter-Option(Code=0x04, SecureParam_R of HA, SecureParam_R of CNs)
- Action AVP
  Result-Code-Option(Code=0x01, status value)

Step7. AMA(AA-MN-Answer: V_AAA -> Attendant)
After adding some parameters for local security to the AMA message, the V_AAA sends this message to the Attendant.
Parameters:

- Security AVP
  Attendant-Key-Option(Code=0x03, attendant_key)
  Nonce-Option(Code=0x01, RPI)

Step8. ARsp(Attendant Response: Attendant -> MN)
Upon receiving the AMA from V_AAA server, the Attendant extracts the secret values from the Nonce-Option and Attendant-key-Option for local security and sends this message to the MN after converting the Diameter to EAPoL.
Parameters:
- Local Challenge: As a random value to protect messages between the MN and Attendant, this value is same one with the challenge sent in the Attendant Response(AR) the response message from MN to find the attendant(Attendant Request,AR) when the MN is about to enter the visited link and try to access the resource of it.
- RPI: A random value for replay protection(e.g. Timestamp, Nonce, or Cookies)
- HoA: MN's home address.
- HaA: MN's home agent address.
- attendant_key: A key protected by the aaa_key.
- SecureParam_R: The keying materials protected by the aaa_key. it contains the items to establish the Security Association for CN. If the ACR message is destined to the multiple CNs, this parameter contains the set of security parameters. {SecureParam_R(CN) x N}, where N is the number of CNs which has received the ACR from the H_AAA.
- Result: A code value indicating the result of the message processing(The definition of the code value is identical to as defined in 'Result-Code-Option'.

At this point of time, the MN has the security parameters received from CNs(SecureParam_R(CN) x N) and it use the parameters as the keying materials to derive the binding key until the lifetime specified in the parameter expires. Similarly, the CNs also has the security parameter(keying materials) sent from the MN to derive the binding key to decrypt the binding registration message encrypted with the same key by MN.

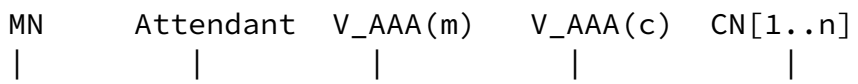
Step9. BU(Binding Update: MN -> CN)
After deriving the binding key from the security parameters, the MN sends the binding registration message(BU) to perform

the Route Optimization procedure. This message is protected by the key. The MN may send this message to multiple CNs if it has the keying materials and is able to derive the key for the CNs.
Parameters:
- All parameters defined in MIPv6 are included.[2]

Step10. BA(Binding Acknowledgement: CN -> MN)
The CN performs the Route Optimization request message(BU) using its key and sends the response message(BA) protected by the key derived from the keying materials sent by the MN(SecureParam_I). Upon receiving this message, the MN processes the message with its key.
Parameters:
- All parameters defined in MIPv6 are included.[2]

6.2 Binding Key Exchange between two nodes belonging to the different domain

The following message sequence occurs when the communication peers (the MN and CN) are belonging to the same domain:



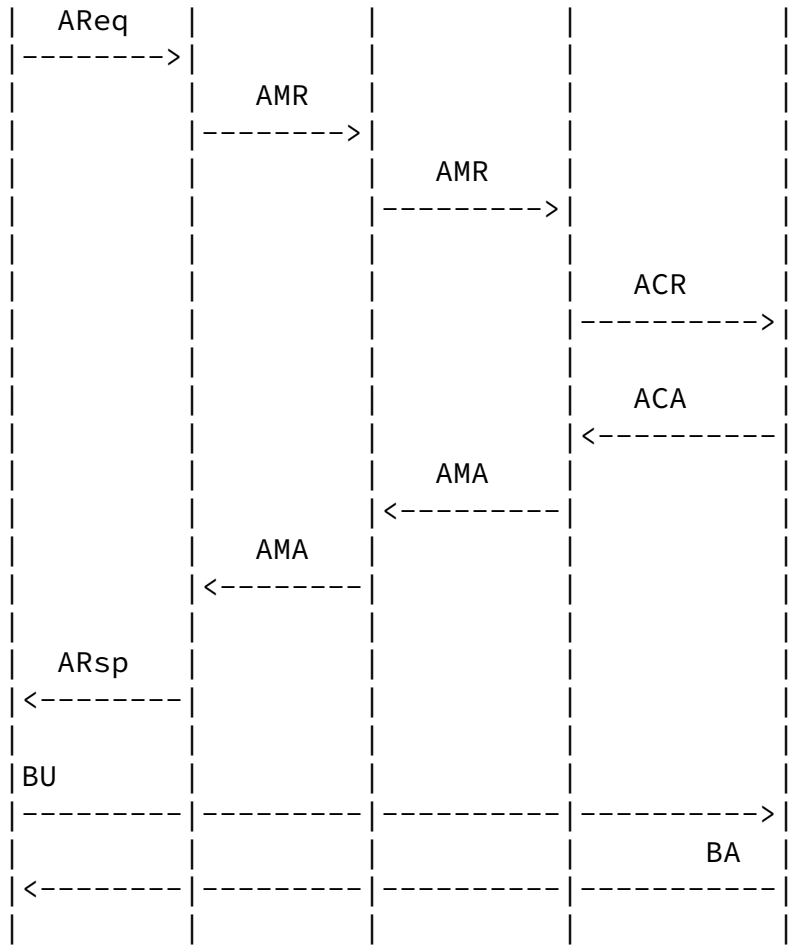


Figure 3. Binding Key Exchange between two nodes belonging to the different domain

In this case, we SHOULD consider the factors below when performing the Route Optimization procedure.

- V_AAA[1..m]: The local AAA server that the CN is now visiting.
- CN[1..n]: One or more CNs the MN wishes to go on communicating.

where, the MN sends the request message to more than one CNs to make the Route Optimization and each CN is in the different domains(m=n) or some CNs may be in the same domain(m<n), it is desirable for the MN to get an information where the CN is currently belonging to.

When receiving the Route Optimization request message, the local AAA server in MN's visiting looks up the CNs addresses and tries to get the CN's domain from its address(this may be done with various methods with internal exchange of messages, however the detailed processing is outside the scope of this document) and send it to the resolved AAA servers. When the local AAA server the CN is visiting receives this message,it converts the Diameter message to another form known to the CN and forward the converted message(SecureParam_I is in it) to the CN which returns the SecureParam_R used to described its key.

The details of operation on message and parameter processing for V_AAA and Attendant are same with the descrived steps in the Section 6.1.

7. Security Considerations

There MUST be a security key shared between the MN and CN to protect the 'Binding Registration(BU/BA)' message for successful and secure Route Optimization.[2] In this document, to make our idea concrete, we assume the related factors on our model(See 2.2). If the SA exists between the MN and AAA server then the security key for Route Optimization can be exchanged securely with its underlying infra-structure. To make this model operate well as we defined here, the security considerations made in this document SHOULD be verified with carefully. The messages between the MN and AAA server SHOULD be exchanged in secure manner. If not so, an attacker is able to mount the DoS/MITM on the link between them.

The proposed method provides the message exchange sequence to exchange the keying materials in two cases. The first case is that the MN and CN are belonging to the same domain where they share the home AAA server and exchange the keying materials each other via this AAA server.

Another case is that the MN and CN are belonging to the different domanins where the mechanism to find the CN's current(visiting) domain server MAY be considerable if the CN is also mobile node.

This model employs the AAA protocol(DIAMETER) as the underlying transport protocol to exchange the binding keys since the AAA protocol guarantees the secure communication between the peers. However we don't let the restrictions on it, if the more simple and secure mechanism or protocol is developed then we may use it to apply our model.

8. Acknowledgments

All the RFC's, ID's, freely available 802.11 standards, and web-sites.

9. References

[1] Pat R. Calhoun, Erik Guttman, Jari Arkko, "Diamet Base Protocol", draft-ietf-aaa-diameter-12.txt, Internet Draft, IETF, July,2002.

[2] Davied B. Johnson, Charles E. Perkins, Jari Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-18.txt, Internet Draft, IETF, June, 2002.

[3] IEEE, "Part 11: Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications", 1999.

[4] IEEE, "802.1x - Port Based Network Access Control", 2001.

[5] F. Johansson, T. Johansson, "AAA NAI for Mobile IPv4 Extension", draft-ietf-mobileip-aaa-nai-03.txt, Internet Draft, IETF, June , 2003

[6] F. Dupont, J. Bournelle " AAA for Mobile IPv6", draft-dupont-mipv6-aaa-01.txt, Internet Draft, IETF, Nov, 2001.

[7] Pat R. Calhoun, Charles E. Perkins, "Diameter Mobile IPv4 Application" Internet draft, Internet Engineer Task Force, November 2001.

7. Author's Address

Miyoung Kim, Ph.D Student
Department of Computing, Soongsil University,
#1-1 SangDo-5 Dong, DongJak-Gu,
Seoul, 156-743
Korea

Phone: +82-2-812-0689
Fax: +82-2-822-2236
E-mail: mizero31@sunny.soongsil.ac.kr

Youngsong Mun, Professor
Department of Computing, Soongsil University,
#1-1 SangDo-5 Dong, DongJak-Gu,
Seoul, 156-743
Korea

Phone: +82-2-820-0676
Fax: +82-2-822-2236

E-mail: mun@computing.ssu.ac.kr

Jaehoon Nah
Network Security Department, ETRI
#161 Gajeong-Dong Yuseong-Gu Daejeon,
seoul, 305-350
KOREA

Phone: +82-42-860-6749
Fax: +82-42-860-5611
E-mail: jhnah@etri.re.kr

Seungwon Sohn
Network Security Department, ETRI
#161 Gajeong-Dong Yuseong-Gu Daejeon,

seoul, 305-350
KOREA

Phone: +82-42-860-5072
Fax: +82-42-860-5611
E-mail: swsohn@etri.re.kr