IEIE Transactions on Smart Processing and Computing

ISAS: AAA Protocol-Based Handover and Improved Security Methodology through the Integration Security Authentication System Constitute

Byungjoo Park[1], Jaehwan Kim[2], and Janise McNair[3]

[1] Department of Multimedia Engineering, Hannam University, 133 Ojeong-dong, Daeduk-gu, Daejeon, Korea, bjpark@hnu.kr
[2] Department of Multimedia Engineering, MMC Lab., Hannam University, 133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
[3]Department of Electrical and Computer Engineering, University of Florida, Gainesville, Florida, USA, mcnair@ece.ufl.edu

* Corresponding Author: Janise McNair, mcnair@ece.ufl.edu

Received March 21, 2012; Revised May 2, 2012; Accepted June 15, 2012; Published July 30, 2012

** Regular Paper: None*

** Review Paper: This paper reviews the recent progress, possibly including previous works in a particular research topic, and has been accepted by the editorial board through the regular reviewing process.*

***Abstract*:** Security risks were raised during the handover of Mobile Nodes (MNs) in the Mobile Internet Protocol version 6 (MIPv6), which were demonstrated in the instigation of route optimization between the MN and its Correspondent Node (CN). The return routability procedure provides a basic security measure for the communication between the MN and CN, but this security scheme still suffers from various weaknesses and loopholes. Thus, various methodologies in securing the handovers for MIPv6 were incorporated in line with the security agreement with authentication, authorization, and accounting (AAA) infrastructure. This paper proposes an establishment of the Integration Security Authentication System based on the AAA infrastructure to maintain the security level of the fast handover mobility management to provide an improved Quality of Service

***Keywords*:** Mobility Management, AAA, RR, Handover, Multicast

1. Introduction

The continuous evolution of the Information Technology (IT) industry has increased the user demand for high-level services and improved mobile devices and wireless communication technology. The wireless environments have achieved great success wherein network mobility management, such as the MIPv6 protocol, was standardized using the Internet Engineering Task Force (IETF). In this regard, various studies and research were conducted on the different methods of securing wireless communications. Within the MIPv6 environment, the MN should receive certification and authorization as it moves from its home network to other networks. On the other hand, security issues were raised during the request for these security measures. Discussions regarding solutions to these problems were in progress, constituting infrastructure-based security agreements in AAA protocol.

This paper proposes the Integration Security Authentication Scheme (ISAS) to improve the general QoS of the wireless communication system. The proposed security scheme is an independent security solution based on the AAA infrastructure capable of intensifying the security level of communications while maintaining efficient route optimization.

The remainder of this paper is outlined as follows: the analysis of the related works and problems are discussed in Section 2. Section 3 outlines the processes involved in the proposed security technique. Section 4 provides the analysis of the performance evaluation. Section 5 reports the conclusion.

2. Related Works and Problem

2.1 AAA and RR Protocol

The standard MIPv6 protocol utilizes the Internet Protocol Security (IPsec) function as its basic security measure. On the other hand, this scheme cannot detect the movement of mobile nodes. That is why numerous studies have been conducted regarding security agreements to address such problems. Security system methodologies could be based on the infrastructure. Thus, one typical scheme utilizes an Authentication, Authorization, and Accounting (AAA) infrastructure-based security certification generation. The AAA protocol can provide a high-level security certification for the MN, which is a separate process from the MIPv6 IPsec function. The AAA protocol has been proposed to be used for various Bootstrap methods and in authentication and authorization methods, which are linked with an AAA server within MIPv6 environments. Other related protocols with the AAA system-building were the RADIUS, TACACS+, and DIAMETER. The Diameter MIPv6 Application is an AAA system, which is based on the DIAMETER protocol that is on the way to standardization [1]. Based on the DIAMETER protocol, the AAA system links independent protocols by utilizing AAA certifications to secure MIPv6 operations.

Figure 1 presents an AAA protocol signaling procedure based on the DIAMETER protocol whenever a handover occurs.

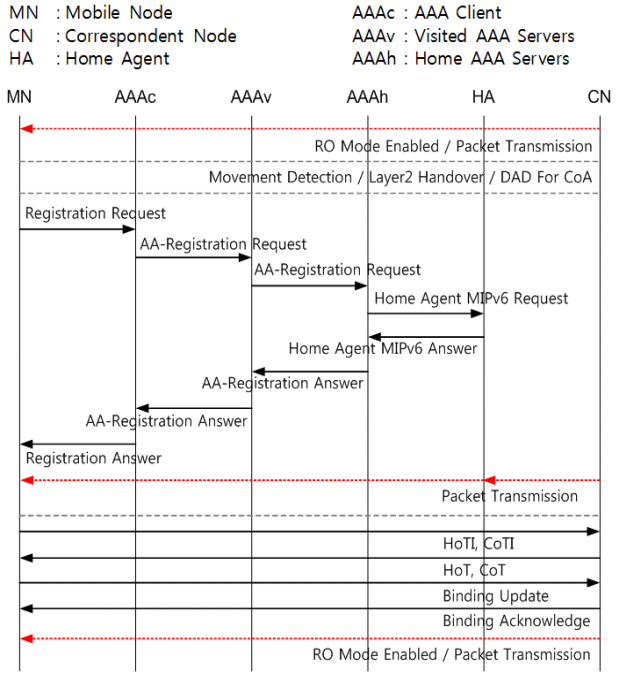

Figure 1. Handover Procedure of AAA

The AAA protocol utilizes an AAA server to conduct a security certification process with the HA registration, but it is similar to the RR protocol to secure the CN communications in RO mode in the MIPv6 environment. Table 1 summarizes the certification process of the 'Diameter Mobile Ipv6 Application' [3].

Table 1. Signal Configuration of AAA Process

Process	Procedure
MN → AAAc	MN piggybacks the BU message of NAL and the HA on the RR(Registration Request) message and sends it to AAAc
AAAc→AAAh	changes to the ARR(AA-Registration Request) message of the received message and transmits the changed message to AAAn passing through AAAv
AAAh → HA	receives and examines ARR message transmits HOR(Home Request) message to the HA
HA → AAAh	verifies received message transmits BA(Binding Acknowledgement) message or HOA(Home Answer)message to AAAh
AAAh → MN	transmits ARA(AA-Registration Answer) with BA message to the MN
MN → CN	uses RR technique to activate CN and RO mode after getting BA message and transmits BU message after using it.

The AAA system is categorized into the AAA Client (AAAc), which assumes the changes of AAA message, and the Visited AAA Servers (AAAv), which interwork with each domain. The Home AAA Servers (AAAh) take charge of the definitive certification. The AAA server requires an ID and password, which refers to a Network Access Identifier (NAI) for certification requests of users in registering with the HA network operators.

2.2 Problems of former AAA Protocol and RR technique

The AAA protocol and RR technique provide strong security when both procedures can be completed simultaneously because of the exchange of binding update (BU) messages. The AAA protocol includes a certification process to reduce the quantity of swapping. On the other hand, there is no presence of a security agreement between the MN and AAAc. Thus, the location data of the MN and the HA information can be susceptible to security risks whenever the binding process is done.

The AAA certification process works well with MIPv6 whenever the DIAMETER protocol is used only if the binding process is supported according to the security agreement between the MN and the HA, which can be considered another protocol. Figure 2 presents the AAA system wherein the HA certifications are optimized through the AAA server.

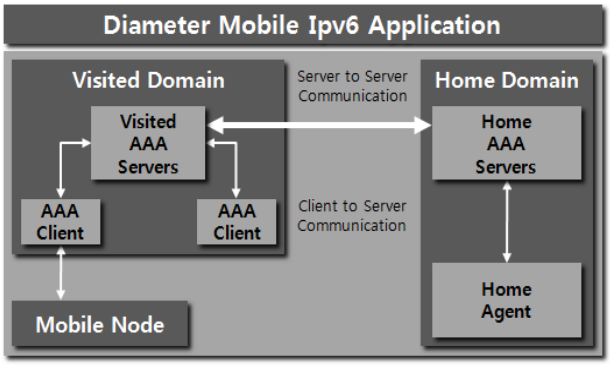

Figure 2. AAA System Configuration Map

The IETF has recommended the RR technique in securing MIPv6 handovers, which they believe can address the security loopholes. The RR technique determines if the MN receives the packet from the CN via the HA. It also distinguishes whether the HoA of the MN in the home network and its Care-of Address (CoA) were established as the source address properly. The RR technique can be considered very efficient in the resource allocation of processes aspect because it only uses encryption technology, such as random-number generation or hash functions. On the other hand, the security weakens because there will be an easy outflow of keys if the direct transmission and tunneling through the HA are exposed. In addition, there will be very high signal traffic through wireless communications, which causes a longer delay in the authentication process. The AAA protocol and RR technique were susceptible to security risks because the exchange of messages was not coded, resulting in the disclosure of information.

3. Proposed technique

The weaknesses of the different established technologies were analyzed in the previous section. Many studies on the organization of security agreements on wireless communication devices are being conducted and discussions before developing a standard in forming the MIPv6 infrastructure.

The following are the recommendations for the establishment of a security system for the standardized IETF protocols:

1) Build a fast and safe RO mode that depends on securing the exchange of BU messages.
2) Enhancement of security measures for wireless communications between the MN and the HA and wired communications between the HA and the CN.
3) Develop a moderate resource allocation process for the MN driving and communication infrastructure.
4) Build a higher level of security authority system on the existing RR technology.
5) Provide an authentication mechanism for multicast services and optimized unicast services that will be introduced in the future.

This paper proposes a new security process method to improve QoS at the observant level.

3.1 ISAS security module on AAA

The ISAS security system based on AAA infrastructure is a security module and an independent security authentication mechanism. Figure 3 presents the structure of the ISAS system model.

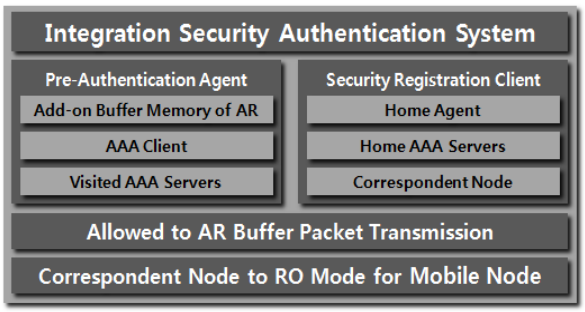

Figure 3. Shape of the ISAS System Model

The ISAS structure includes a Pre-Authentication Agent (PAA), which is responsible for the pre-authentication, and a Security Registration Client (SRC), which is provided with the security authentication system. The SRC is provided with an additional module at the end of the network, transfers binding to the CN instead of the MN, and activates RO mode. Figure 4 depicts the system organization of the ISAS system.

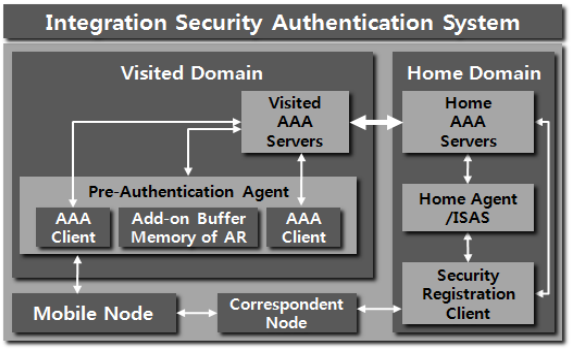

Figure 4. ISAS System Configuration Map

The configuration comprises the existing AAA infrastructure components and additional security authentication modules on the Home and Visited domains. At the Visitor's domain, the PAA module performs limited authentication linked with AAAc and AAAv to work actively in connection with buffer memory. The ISAS, an adjunctive module of SRC or the HA in the Home domain, is included. The ISAS assists the SRC module in receiving information from AAAh and transmitting BU messages to the CN via the HA, which serves as the main server of the

security authentication system. Through this scenario, the PAA produced an authentication mechanism, and SRC activated the RO mode between the MN and the CN without the aid of the wireless infrastructure of RR technology. The advantages that can be brought by the system when developed into the security authentication process can be the following:

1) Guarantee the high-level quality of security by working independently from the wireless communication system and as it is based on the AAA infrastructure.
2) Provide a high-level quality of security for communications between the MN and the HA through the use of AAA infrastructure, enforce the PAA security, and increase the utilization of Multi Cast service and Router buffer memory.
3) Completes the authentication and registration on time and activates the RO mode faster because BU and establishment of security agreement are made up simultaneously.

3.2 Handover Procedure

The overall organization of the proposed system was detailed in the previous section, and this section will outline its detailed operations. Figure 5 shows the handover procedure of the proposed system. As shown in Figure 5, the handover on a wireless network was omitted in a signaling-planar figure as the proposed ISAS system is based on the AAA protocol infrastructure.

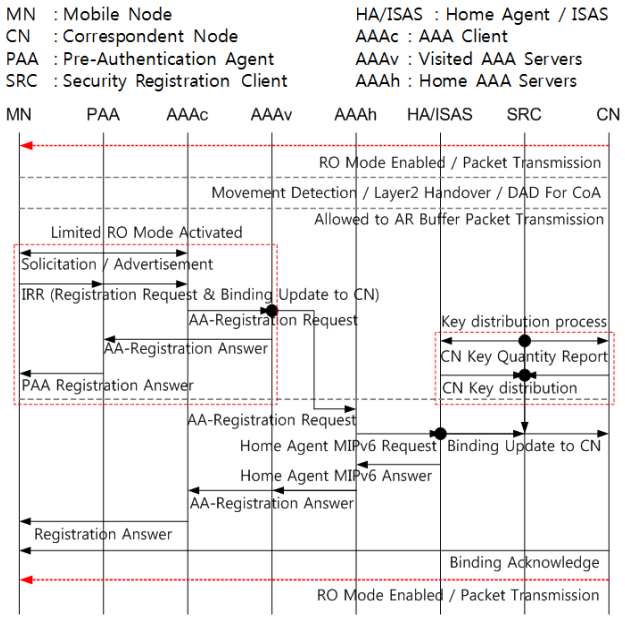

Figure 5. Handover Procedure of ISAS

As discussed earlier, the RO mode activates as PAA, AAAc, and AAAv work by being connected and performing a preliminary authentication process. The ISAS operation on the HA and SRC are made simultaneously, which builds up the security authentication system through encryption techniques. Based on the wireless communication system produced through the AAA infrastructure, the process of CoA allocation and Duplicate Address Detection (DAD) would be different. On the other hand, according to the standardized process, when approaching a new domain, the Advertisement messages containing basic network information (e.g., local challenge or visiting network identifier) come from the Router attached to the network or AAAc. The MN can produce its CoA based on its received Router advertisement. The Integrated Registration Request (IRR) message is created to activate the security authentication for the HA through the AAA server, and the RO mode with its CN will be activated. The information in the IRR message includes the request messages of PAA and AAA registration and BU messages to the CN, which performs the security authentication and the activation of the RO mode. The parameters in the IRR message include NAI to register CoA and AAA, which will be used as the source address for all messages, addresses of each stopover, and BU message for the CN. The message was sent by allocating the CoA as the source address, including the authentication and authorization process. The following section discusses each of the working processes.

3.3 ISAS Operating Algorithms

Figure 6 shows the overall working environment of the proposed ISAS system.

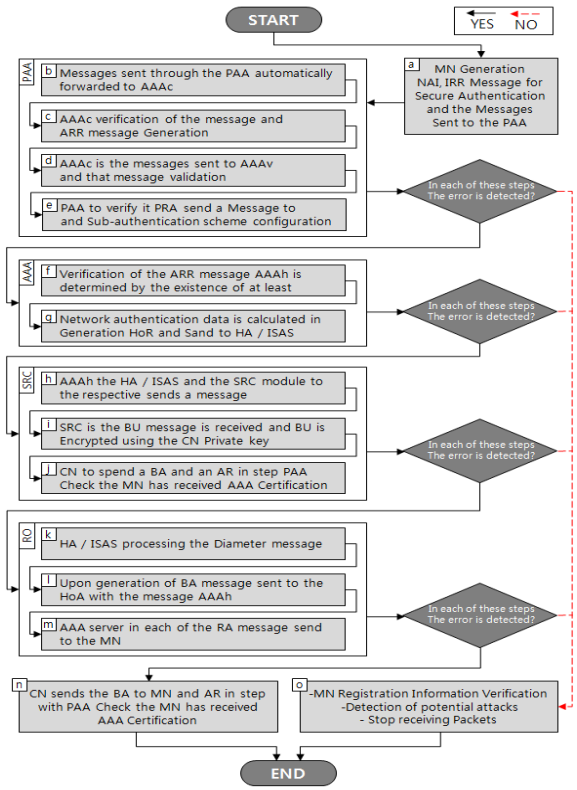

Figure 6. ISAS Process Diagrams

(a) The MN produces NAI and IRR messages to activate RO mode with the CN and security authentication for the HA through the AAA server. The messages allocate CoA as the source address and PAA as a destination address. The IRR messages include a request message for PAA and AAA

registration and BU message to the CN. This is to perform security authentication and RO activation simultaneously. The IRR message parameter values include NAI for CoA and AAA registration, which will be used as the source address for all messages, addressing for all stopovers, and the BU message for the CN.

(b) The sent messages arrive automatically at AAAc through the PAA. The AAAc checks the LC value and DAD from the authentication request message from the MN to produce an ARR message.

(c) The ARR message also includes messages, such as authentication requests to upper system layers and BU messages from the MN, which are sent to AAAc and AAAh.

(d) The AAAv server on the transmission process checks if the messages are transmitted automatically from registered AAAc. After the additional message verification processes based on the PAA system algorithm, the ARA (AA-Registration Answer) is produced and sent to PAA.

(e) PAA investigates it and sends back a PRA (PAA-Registration Answer) message to the MN to complete processing the lower authentication system. The detailed algorithm for this process is explained in the next section.

(f) The ARR message sent through the former course passes through AAAh to check if the message is from a registered AAAv.

(g) If there is no error, the HOR message is produced based on other information needed for the authentication algorithm, calculates network authentication data, and sends the message to the HA/ISAS.

(h) The message is transmitted and distributed from AAAh to the HA/ISAS and SRC module to activate RO mode by organizing the upper authentication system. The SRC module, which always works on the Key Allocation Process, performs under the relevant algorithm, and maintains a certain value by reporting its Secret Key volume with KQR (Key Quantity Report) message. If values are lacking in the KCN of the CN, it requests messages to keep the amount of KCN of the CN. This process is explained in detail with the algorithm in the next section.

(i) The SRC receives the BU message and encodes it with the KCN of the CN to renew as the CN.

(j) On the process, if the CN confirms that the message has no errors, it sends a BA message and packets to the MN, wherein the RO mode is activated.

(k) The HA/ISAS processes the Diameter message, which goes through the authentication process with the AAAh message.

(l) When the received message is clear, it produces a BA message and transmits a HOA message that includes the encapsulated BA message for the MN. the HA saves the Binding Information in Binding Cache, and the key value is calculated to activate the security agreement with the MN under the ISAS security module.

(m) The AAAh produces and transmits an ARA message, which passes through AAAv. The AAAc changes the received AAA message into RA (Registration Answer), which meets the applied communication infrastructure and interface standard of the MN before transmission to the MN to complete the AAA authentication process.

(n) The BU message from SRC to the CN is confirmed, and the BA (Binding Acknowledge) message to activate the MN and RO mode is sent to the MN. RO mode is then activated, and the system can transmit packets directly to the MN. In some cases, problems, such as the BA message between the MN and the CN, can arrive earlier than RA messages of the HA/ISAS between the MN and AAA may occur. In this regard, The PAA module checks the messages toward the MN and gives a standby order to the connected AR (Access Router) to prevent distorted message scenarios. The registration information of the MN needs to be confirmed first and test the possibility of attack if errors are found during the verification process or if the information is not identified.

(o) When there is a request to stop receiving packets, the verification process containing the error is repeated. Based on the result, it moves to the next process and notifies the attack confirmation or warning message. Through these courses, the general system is completed, and the way of working the module is reported in the next chapter.

3.3.1 Pre-Authentication Operating Algorithms

The PAA organizes a low certification system to connect the space between AAAc and AAAv. The PAA method includes a certification by coding its secret key system, which uses a created NVC (Node Verification Code) as an authentication code. The key components of NVC are based on ARA information received from AAAv. It includes a mobile cookie received from the MN, the registration information of the MN, and data associated with the service request. Figure 7 presents the primary components of NVC.

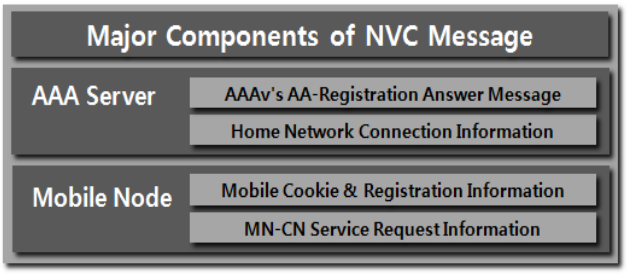

Figure 7. Major Components of the NVC Message

The AAA certification message received from AAAv guarantees that there were no problems in the process of AAA certification, which the MN goes through, and it ensures integrity by adding information received from the MN. The MN cannot decode the created NVC; only the PAA can read the data through a secret key. The reason for having a composition like this is not to expose a secret key of PAA to an attacker. Figure 8 shows the process diagram of PAA.

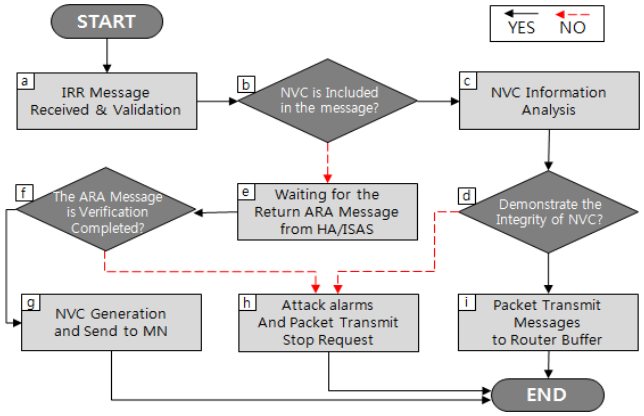

Figure 8. PAA Process Diagrams

(a) The PAA authentication process starts whenever an IRR message is received from the MN.

(b) The IRR message is then checked to see if it includes an NVC.

(c) The presence of an NVC in the IRR message will trigger the verification step.

(d) The integrity of the NVC is demonstrated through the verification process that checks whether the NVC is appropriately created. It also checks issues regarding packet transmission order from the buffer memory of the Router and completes organizing the lower authentication mechanism. As with all other security authentication systems, weak points of security can be found during the first authentication process, and the PAA has a process to supplement it. The MN does not have NVC information while it accesses the wireless system and when it registers to the HA or the CN. Consequently, the NVC would be included in transmitting an IRR message.

(e) The PAA has a waiting time for returning a reply after its registration to the HA.

(f) It receives an ARA message replied after the AAA authentication AAA process and determines if the verification process is completed by checking the ARA message.

(g) The PAA creates the NVC based on the ARA message and transmits it to the MN, which uses the authentication value in the handover process.

(h) If the integrity of NVC is not verified or ARA message information is not correct, the PAA sends a request message to stop packet transmission and reports an attack alarm to the upper authentication layer. The secret key of PAA is not disclosed on the network to provide a highly secured authentication. The renewal process of the packet distribution tree may be delayed from a few to a dozen seconds on some existing Multicast Routing protocols because the authentication process for a multicast service is accomplished at the top level. A multicast service is unreliable, and decreasing packet losses through fast handovers will be a key consideration.

With this technique, fast handovers with an authentication process on the lower network level guarantee mobility and secure handovers.

3.3.2 Security Registration Operating Algorithms

The SRC is a lower module in the HA/ISAS that includes security on BU messages and activation of RO mode. The preconditions for this algorithm are identified as follows:

(1) The MN must have a symmetry key($K_{S\text{-}MN}$) and notifies the HA with its registration information.

(2) The HoA message from AAAh must contain a BU message to register to the CN.

(3) The SRC module shares symmetry keys with each CN as the service provider.

The SRC has $K_{S\text{-}CN}$ with the CN, a service provider, and must retain the security through IPsec in the wired communication section. The SRC processes the binding with the CN includes the following steps: receives a coded KCN or nonce from the symmetry key between SRC and the CN, keeps it in the SRC module, chooses one of the KCN randomly among the keys it had when it receives BU message of MN from AAAh, encode it, and sends the BU through the CN. This process is recommended, even if there is a security agreement from IPsec, because double transmission of a secret key may cause the disclosure of its key value, which is considered a security risk. In addition, the transmission of BU messages to the CN with the symmetric key can be susceptible to adversary attacks, which makes the symmetric key information available for decoding received messages. Therefore, even if the adversary penetrates the security channel secured by IPsec, analyzes the symmetric key of SRC and the CN, and obtains the secret key of the CN, the MN has allocated secret key information randomly, so the adversary needs to analyze all the transmitted packets to insert its aggression information. When the adversary analysis may have been completed, the lifetime of the nonce values may already have expired. Hence, the secret key becomes useless. Figure 9 depicts the Process Diagram, which contains all the number of cases of SRC.

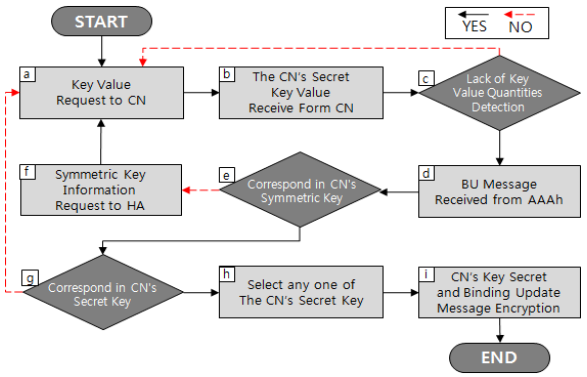

Figure 9. SRC Process Diagrams

(a) First, the SRC requests a secret key value from the CN. The request message for secret key value is sent coded with a mutual symmetric key, such as other messages, to preclude the adversary from analyzing the request message and finding the key value of the CN because it includes secret key request information for the CN address.

(b) The SRC receives and keeps the coded secret key with a symmetric key from the CN.

(c) The number of secret keys of the CN that SRC keeps is checked, and it is determined if the key values for later authentication are enough. If it is insufficient, return to the first step requesting a key value from the CN. When the authentication for the BU message increases or the secret key of the CN is in shortage due to the expiration of the lifetime of the nonce of the CN, the process also needs to return to the first step. The reason why SRC keeps the secret key of the CN is to be ready to encode and transmit promptly when the BU message arrives. The amount of secret keys of the CN that SRC needs to keep is decided on the average value, which depends on the BU receiving the message on the network.

(d) Next, the AAAh sends only BU messages to SRC among the messages from the MN.

(e) The SRC then checks whether the secret key of the CN that the MN wants for a BU message exists. The possible problem is that another MN is set as a CN.

(f) In that case, symmetric key information of the MN from the HA/ISAS is needed. The SRC makes and sends a transmit request message for a secret key with the symmetric key from the HA/ISAS.

(g) If there is a secret key value of the CN and if all the secret key of the CN is exhausted, return to the first step.

(h) On the other hand, if there are enough secret keys of the CN, distribute them randomly, encode the BU message, and send it to the CN.

The BU message and SRC module authentication in the proposed methodology will not take a long time unless the identified issues on the steps will not arise. Although some issues may arise at every step, a long delay would not happen. Theoretically, in the proposed methodology, the MN can activate RO mode as soon as it receives the AAA authentication message of the HA/ISAS because the process is expected to be performed before the AAA authentication response message from the HA/ISAS to MN is transmitted or at the same time.

4. Performance Evaluation / Comparing and Analyzing performance

The procedure and problems of existing methodologies and techniques will be analyzed in comparison with the performance of the proposed methodology. This section will outline the evaluation of the performance of the proposed methodology using the established AAA and RR techniques, the delay time, and the handover of ISAS.

The handover delay time refers to the time it would take to activate the RO mode between the MN and the CN when the handover occurs both on the existing and proposed wireless network system. In the proposed methodology, the delay time of packet transmission will be analyzed separately between the delay time for the packet transmission approval of PAA and RO mode activation through SRC because they undergo separate processes. When handover occurs, a simplified timing diagram for each model will be evaluated to compare its delay time when the MN moves into a different administrative domain. Each value by section is designated by the base of the signal time of an existing wireless network. To compare the functions of the existing and proposed methodology, it will be assumed that they are under the network environment with identical wireless protocols and a delay time designated randomly in wireless networks in order to obtain the most similar result of real-time handover.

Table 2 lists the necessary parameters for the evaluation. The Packet Re-Transmissions Rate and the packet loss ratio happening in MIPv6 are defined as α, and the DAD procedure on AAAc is defined as t_{dad}.

Table 2. Definition of the Handover Latency section

Symbol	Description
t_1	MN ↔ AAAc
t_2	AAAc ↔ AAAv
t_3	AAAv ↔ AAAh
t_4	AAAh ↔ HA/ISAS, SRC
t_5	MN ↔ CN
t_a	MN ↔ PAA
t_b	PAA ↔ AAAc
t_c	SRC ↔ CN
t_d	AAAv ↔ PAA
t_w	Wireless Network Delay
t_{dad}	Duplicate Address Detection
α	Packet Re-Transmissions Rate

In addition, the delay time of wireless processing on a virtual network is defined as a t_w of any value. The comparison will be expressed graphically to have objectivity for the analysis as calculations on the increasing amount of each transport delay according to the number of handovers.

4.1 Time Diagram and Formula of former/proposed techniques

Figure 10 presents the Timing Diagram of the existing AAA technique. Each section was assigned through the AAA procedure and showed the signaling processes for the RR technique to activate the RO mode between MN and the

CN and the certification/registration of the HA through AAA infrastructure. The HoTI or HoT message reaches the CN via the HA in the RR technique, but it arrives at the CN immediately for flexibility in the calculation. Equation 1 was formulated based on the environment of the virtual wireless communication system by including an activation step of RO mode for comparative analysis between techniques.

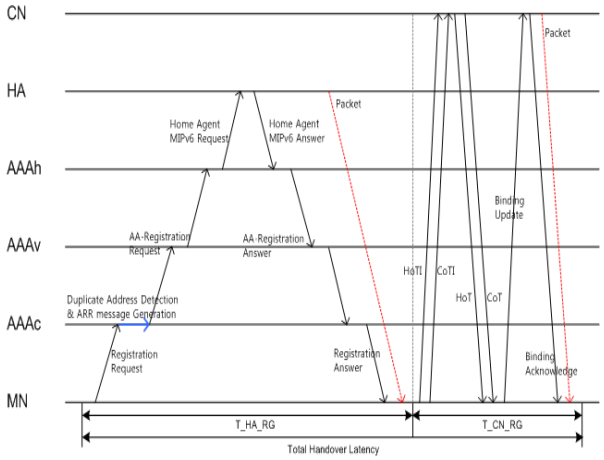

Figure 10. AAA Timing Diagram

The creation and encoding times of the messages in the activation of the RR method were omitted because of the difference in each technique.

$$T_{AAA} = T_{\_HA\_RG} + T_{\_CN\_RG} = \alpha(t_W) + 2t_1 + 2t_2 + 2t_3 + 2t_4 + 6t_5 + t_{dad} \quad (1)$$

Thus, in the case of the α-value, it was calculated through the connection with any wireless delay time of t_w and has applied an increasing time according to the signal procedure accomplished in each layer. Figure 11 presents the Timing Diagram of the signal sequence of the proposed methodology. The differing sections are designated based on the standard AAA protocol on the existing method and ISAS procedure of the proposed methodology. Figure 11 shows it as an accessory system with a process between PAA and AAAc, and between the HA/ISAS and SRC sections so that it sets the formation of a relatively lower delay time. In addition, the PAA process is completed. A transfer command of the packet is issued to the AR buffer memory, and the procedure before the RO mode is activated.

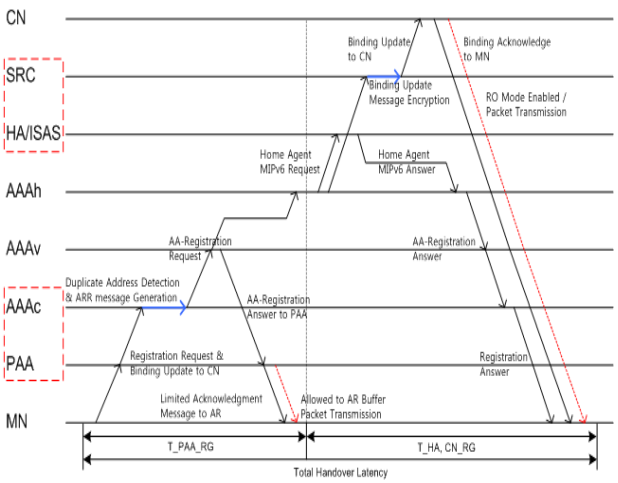

Figure 11. ISAS Time Diagram

Equation 2 expresses the time needed to form only the activation of RO mode in the ISAS procedure, including the response message of PAA. The encryption process of SRC was calculated as the additional delay time for sections, even though it was not expressed in the equation. Equation 3 shows only the time taken for the PAA process.

$$T_{ISAS} = T_{\_PAA\_RG} + T_{\_HA,CN\_RG} = t_W + t_{dad} + 2t_a + t_b + t_c + 2t_2 + 2t_3 + 3t_4 + t_5 \quad (2)$$

$$T_{\_PAA\_RG} = t_W + t_{dad} + 2t_a + t_b + t_d + t_2 \quad (3)$$

4.2 Performance evaluation of suggested ISAS

The ISAS function will be evaluated first before comparing the functions of both the existing technique and the proposed methodology. Figure 12 presents a graph of the handover delay time in activating the RO mode, which is caused by the delay of SRC encryption under ISAS. Based on the evaluation, more delay time than reality was set to see a difference in each time. Figure 12, produced from equation 2, presents the case in the proposed methodology. The activation of RO mode increases the delay time caused by the encoding process, as explained in the previous section.

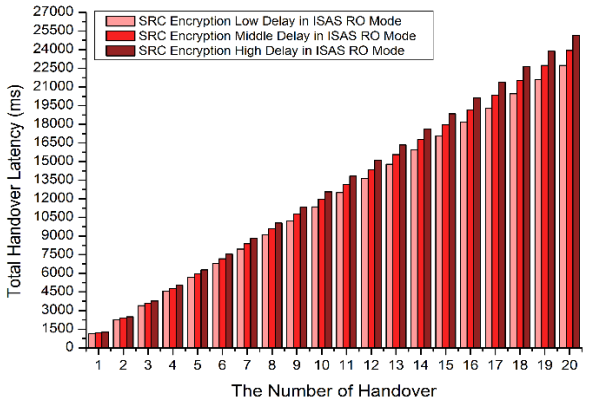

Figure 12. Handover latency According to The SRC Process

The traffic between the HA/ISAS and SRC or the rapid increase in the request for encryption triggers this case. Based on the graph, the changes cannot be noticed and the increase rate decreases when the handover occurs only for one time. Thus, the encoding authentication process of SRC does not have a significant effect in activating RO mode, and the time consumed from the first handover to the activation of RO mode was less than 1500ms.

4.2.1 Comparison of Performance of AAA and ISAS

The delay based on the increase of Packet Re-Transmissions Rate and the calculation according to the increase of delay of the wireless network will be analyzed to objectively compare the performance of the proposed methodology with the existing technique. The encoding time of ISAS and SRC for the evaluation was calculated with mid-delay, not with the minimum delay. The graph depicted in Figure 13 used equations 1, 2, and 3. It was produced considering that the 'Out-of-Sequence' did not arise during the packet transmission of BU for the HA, and the CN was performed simultaneously in ISAS.

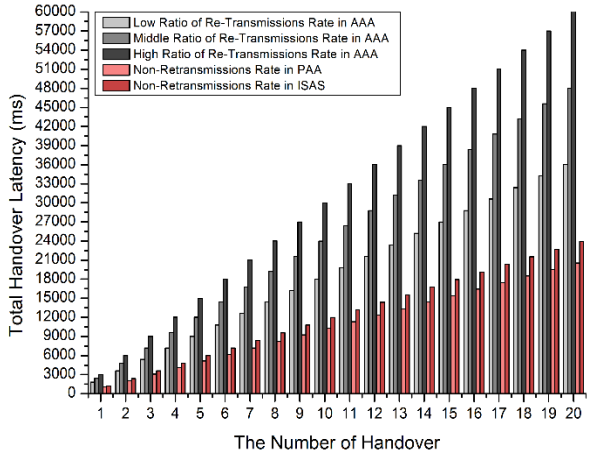

Figure 13. Handover latency According to the Increase in α

The primary purpose of PAA was to provide a packet transmission order into a multicast packet or AR buffer. It reduces the system load by not overlapping orders with other systems, and it also enables a fast transmission system before activating the RO mode. The gap in the delay time between PAA and ISAS does not appear clearly on the graph using the traditional DAD technique. In contrast, with the Look-Up method or PMIPv6, which is a wireless communication technique for upper layers, it is expected to have a maximum of 1000ms of time to be reduced. In the case of the existing technique, the handover delay surges as α increases. This is a significant advantage in ISAS because packet mixing does not occur. Thus, the handover delay only increases gradually based on the number of handovers. The graph in Figure 14 uses equations 1, 2, and 3 that outline the handover delay according to the variations of t_w, meaning a random wireless delay time.

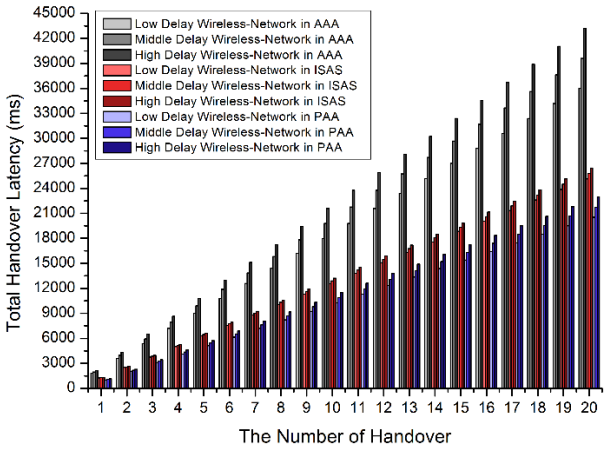

Figure 14. Handover latency According to the Increase in t_w

As with the previous result, the existing technique takes a longer time because the first handover and delay time surges according to the increase in the number of handovers. That is because the existing technique has much network traffic, as shown in the Timing Diagram. The PAA, which operates at the lower level of a network, has a large gap as the number of handovers increases, which can be understood as considerable signaling at the lower part of the network. On the other hand, the gap can be shortened whenever it operates in connection with the developed wireless communication infrastructure. Furthermore, the handover delay time gap between the existing and proposed methodology under the real wireless communication environment considering that the RR process for the existing technology will be simplified to an easy formation, is expected to be more significant.

5. Conclusion

This study analyzed existing techniques to identify the weaknesses and proposed a methodology that can speed up

the handover process while maintaining security by developing an ISAS system, which is an integrated security and authentication method dependent on the base of the existing AAA infrastructure. In the near future, a high-capacity media or Cloud service under a wireless environment, such as IPTV2.0, is expected to rise, and there is strong demand for studies on multicast services and standardization processes both from users and infrastructure aspects. The protocols for multicast services, wireless communications protocols, and AAA protocol have been working independently with their processes, which causes long delays during handovers and has low efficiency when using the infrastructure. Many studies have addressed these issues and converged the protocols but failed to reach standardization.

This paper proposed an ISAS system, a dependent and integrated security/ authentication methodology, which is expected to guarantee the expansion to multicast services and improve QoS delivery through fast security confirmation and registration process. In addition, the proposed methodology lightens the infrastructure load by process division and assists in better resource utilization for mobile nodes.

Acknowledgment

References

[1] P. Calhoun, G. Zorn, D. Spence, D. Mitton, “Diameter Network Access Server Application”, IETF, RFC 4005, Aug., 2005. https://www.rfc-editor.org/rfc/pdfrfc/rfc4005.txt.pdf

[2] D. Johnson, C. Perkins, J. Arkko, “Mobility Support in IPv6”, IETF, RFC 6275, July, 2011. https://www.rfc-editor.org/rfc/pdfrfc/rfc6275.txt.pdf

[3] Franck Le, Basavaraj Patil, Charles E. Perkins, and Stefano Faccin, “Diameter Mobile IPv6 Application,” Internet-Draft, November 2004.

Byungjoo Park received his B.S. degree in electronics engineering from Yonsei University, Seoul, Rep. of Korea in 2002, and M.S. and Ph.D. degrees (first-class honors) in electrical and computer engineering from the University of Florida, Gainesville, USA, in 2004 and 2007, respectively. From June 1, 2007, to February 28, 2009, he was a senior researcher with the IP Network Research Department, KT Network Technology Laboratory, Rep. of Korea. Since March 2, 2009, he has been a Professor in the Department of Multimedia Engineering at Hannam University, Daejeon, Korea. He is a member of the IEEE, IEICE, IEEK, KICS, and KIISE. His primary research interests include the theory and application of mobile computing, including protocol design and performance analysis in the next-generation wireless/mobile networks. He has published approximately 35 research papers on the theory and application of mobile computing, IPTV, and Internet Application. Since 2004, he has focused on IPv6, IPv6 mobility, media-independent handover, and cross-layer. His email address is bjpark@hnu.kr.

Jaehwan Kim received his B.S. degree in multimedia engineering from Hannam University, Daejeon, Rep. of Korea in 2011, and M.S. degree in 2013, respectively. His research interests are Wireless Networks, Mobile IPv6, Web3.0, IPTV2.0, Augmented Reality, Cloud Computing Real-Time Multimedia Transmission Service.

Janise McNair is an Associate Professor of electrical & computer engineering at the University of Florida (ECE Florida). She is a researcher in wireless networks and Internet of Things applications. Currently, her research creates frameworks for integrating IoT with 5G and 6G cellular systems. She was a pioneer in early next generation mobility management for cellular systems. She later focused on developing multi-discipline, cross-layer systems for smart grid security analysis, IoT systems for construction site safety and security, and IoT systems for agriculture and food safety. She is a member of the Intelligence, Science and Technology Experts Group of the National Academies of Sciences Engineering and Medicine, the Integrity Committee of the IEEE Computer Society, and participated in the 2008 DARPA Computer Science Study Group. She serves on the organizing committees of IEEE ICC 2024 and ACM CoNEXT 2022 and the editorial boards of Nature Communications Engineering and Springer Wireless Networks Journal. Dr. McNair earned her B.S. and M.S. degrees from the University of Texas at Austin and her Ph.D. degree in ECE from the Georgia Institute of Technology, with a research focus on medium access control and mobility management in next-generation wireless networks.