A Study on Authentication/Authorization/Accounting and Roaming Mechanism in Pervasive Environment‡

Jong-Sik Moon[1], Jong-Hyuk Park[2] and Im-Yeong Lee[1*]
[1] *Division of Computer Science and Engineering, Soonchunhyang University.*
[2] *Department of Computer Science and Engineering, Kyungnam University.*
[1] *{comnik528, imylee}@sch.ac.kr,* [2] *jhpark@.kyungnam.ac.kr*

Abstract

As the Internet and networks advance, the combination of wired/wireless technologies is spreading rapidly, since it enables the creation of new services, and provides new features to both users and service providers. In such wired/wireless integrated services, network integration is very important, because such systems are integrated by links between heterogeneous networks, and they involve an integration of transmission technologies across networks. In this situation, existing security and communication technologies are unsuitable, since networks are integrated with heterogeneous networks. The network may have several security flaws. Also, services available will be services for roaming users. In these services, we must provide fast authentication and security for roaming. Therefore, in this paper we proposed roaming and AAA mechanisms in heterogeneous network environments. Our system provides secure communication and efficiency.

1. Introduction

Fast transmission speeds and various wired network services were combined with the convenience and mobility of wireless services. The combination of wired/wireless technologies is spreading rapidly, since it enables the creation of new services and provides new features to both users and service providers. In such wired/wireless integrated services, network integration is very important, because such systems are integrated by links between heterogeneous networks, and they involve an integration of transmission technologies across networks. Due to the development of mobile devices and networks, users want services to be available anywhere, anytime, securely and conveniently.

In combined wired/wireless network environments, the configuration of the service that is available is predominantly targeted towards mobile users. During roaming, the service needs to provide fast, secure authentication. However, weaknesses in current security and transfer technology are apparent when utilized in changing environments. Also, since the heterogeneous network is mobilized as service is received, accounting is more difficult and home authentication service overhead may occur. Because many weaknesses exist, this research studied roaming in heterogeneous network environments and an AAA(Authentication, Authorization, Accounting) mechanism. To authenticate users of the mobile device to receive a service, OPT(One-Time Password) and an ID-based public key method was used, while a ticket was used for fast roaming and reduction of home authentication server overhead. In the early stages of the accounting service, the user prepaid the amount that the mobile device will use, and the ticket was formed to include the payment information. Subsequently, when the mobile device service is used, the amount is deducted from the ticket and the ticket is renewed. Therefore, the mobile device information about payment did not have to be continuously transferred to the home server, and was processed via a trust relational server. When this type of method is used, billing service information update and fast roaming can be provided in a hierarchal trust relational server in a heterogeneous network environment. Also, even when the mobile device moves to a heterogeneous environment, the home network does not have to be accessed. Instead, continuous service is received by obtaining authentication via a heterogeneous network authentication server with hierarchal network

‡ "This research was supported by the MKE(Ministry of Konwledge Economy) Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)" (IITA-2008-(C1090-0801-0025))
* Corresponding Author : Im-Yeong Lee, imylee@sch.ac.kr

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.4161
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.4161

authentication. Therefore, authentication technology using a hierarchical trust relational server is proposed, which is secure and effective. The organization of this paper is as follows. Section 2 describes the security requirements and overview of AAA and bilinear pairing. Section 3 describes existing studies. Section 4 explains the proposed method. Section 5 analyzes the efficiency of the proposed method in terms of the security requirements given in Section 2. Finally, Section 6 presents the conclusion and provides directions for future work.

2. Preliminaries

This section explains the security requirements, and provides an overview of AAA and bilinear pairing.

2.1. Overview of AAA

The AAA(Authentication, Authorization, and Accounting) standard devised by the IETF working group is applicable to the Diameter protocol. The stage was reached where an AAA protocol appropriate for the next-generation roaming environment was established, without restricting the existing RADIUS(Remote Authentication Dial In User Service) protocol. For this protocol standard, a formal working group was formed in December 1998, and the applicable AAA protocol was named Diameter. The basic structure of the Diameter protocol is divided into transmission protocols that include SCTP(Stream Control Transmission Protocol), a base protocol that includes accounting functions, and various high level application protocols.

The Diameter protocol provides basic services, such as the management of accounting or a session needed in an application, and it performs the transmission of AVP(Attribute-Value Pair), negotiation and error reporting on node capabilities, transmission protocol control and watch dog functions. Considering the Diameter protocol class and the application protocol standard, there are NASREQ(Network Access Service Requirements) applications for wire-based networks, to access authentication, and general access control of the existing traditional PAP/CHAP(Password Authentication Protocol/Challenge Authentication Protocol), EAP application, to enhance security functions in a wireless LAN environment, which authenticate with various authentication methods provided by the EAP(Extensible Authentication Protocol) working group, and the Mobile IPv4 application, to support the mobile roaming environment. In addition, there are credit control applications for pre-payment and post-payment card service, SIP(Session Initiation Protocol) applications for the SIP protocol-based VoIP(Voice over IP) service user authentication, and AAA applications associated with the bootstrapping of the Mobile IPv6, in accordance with the completion of the Mobile IPv6 standard. With the extension of IP-based Internet, there is an increase in demand for accessing the network in wireless mobile environments. Even in wireless environments, there were multiple service environments for users, including QoS provision or pre-payment card and others. In order to satisfy requirements of users, wired and wireless businesses must provide secure and high level services for legitimate users. The AAA protocol is an essential element for such secure network access, mobile service, user authentication, authorization and accounting processing. In 1991, the AAA protocol was proposed with the Radius protocol by Livingston Company, and provides an AAA service for the SLIP(Serial Line Internet Protocol) or PPP(Point-to-Point Protocol) linkage service within the management domain in its first version. However, at present, service networks are gradually evolving into open-types, and networks are evolving into a series of multiple domain environments. Therefore, the IETF AAA working group is focused on the standardization of the Diameter protocol for providing AAA services appropriate for the roaming environments. In the case of domestic environments, within the recent mobile Internet business domain, the relevant businesses are quickly working on providing Mobile IPv4 and Mobile IPv6 services. For such mobile environments, AAA services between domains must be applied. For practical services in environments, there is a need for technological development in accordance with the existing standard, however, technological development of the mutual operation test is required, to determine if interworking is possible between the standard adaptability test and products. From domestic standardization organizations and foreign standardization organizations, once the Diameter protocol standard is completed and the mobile Internet environment is standardized, the use of the Diameter protocol will expand rapidly, and the market is expected to grow more rapidly[2][3][5][8][10].

2.2. Bilinear Pairing

Bilinear pairing is a problem in discrete mathematics about ellipses that was simplified by reducing it to a discrete logarithm of a finite field. It was originally proposed as a map that attacks a conventional crypto-system. Recently, an encryption map for information protection was used, instead of an attack map, so, Bilinear Pairing is equivalent to a Bilinear Map. The following terms are used as stated in this paragraph and this theory is defined below[1].

[Definition 1.] Characteristics that satisfy an Admissible Bilinear map are as follows;

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.4161
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.4161

- Bilinear: Define a map $\hat{e} = G_1 \times G_1 \to G_2$ as bilinear if $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ where all $P, Q \in G_1$, and all $a, b \in Z$.
- Non-degenerate: The map does not relate all pairs in $G_1 \times G_1$ to the identity in G_2. Observe that since G_1, G_2 are groups of prime order, this implies that if P is a generator of G_1, then $\hat{e}(P, P)$ is a generator of G_2.
- Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in G_1$.

Based on the bilinear premise, the following definition was constructed.

$$\hat{e}(aP, bQ) = \hat{e}(P, bQ)^a = \hat{e}(aP, Q)^b = \hat{e}(P, Q)^{ab} = \hat{e}(abP, b) = \hat{e}(P, abQ)$$

From this premise, for ellipses, the D-H decision problem can be easily solved via the following equation.

$$\hat{e}(aP, bQ) = \hat{e}(cP, P) \Rightarrow ab = c$$

Therefore, the following is the basis for resolving the difficulties of the bilinear premise that is used as an encryption tool by many encryption protocols.

[Definition 2.] When elements G_1, P, aP, bP, cP (BDHP, Bilinear Diffie-Hellman Problem) are given, this refers to $\hat{e}(P, P)^{abc}$ calculation problem.

In this research, the Admissible Bilinear Map was used as the basis of the secret numbers production in the key construction process between heterogeneous devices. This problem can be solved if the ellipse curve discrete mathematics problem can be solved. For example, a can be calculated from aP, then $\hat{e}(P, P)^{abc}$ can be calculated through $\hat{e}(bP, cP)^a$

2.3. Security Requirements

Unlike existing wired networks, communication in wireless networks has many weaknesses, providing easy access for a third party. Therefore, when the user accesses the network and requests a service, the transmitted message and communication must satisfy the following security requirements.

2.3.1 General Security Requirements

- Confidentiality: The data used in communication must be confirmed only by the qualified object. The adversary is prevented from learning the traffic characteristics of the data source, destination, frequency, lengths, or communication network.
- Integrity: The transmitted message must not be forged, deleted or modified. The user must confirm modifications.
- Authentication: The message transmitted or the source of the electronic document sent by the user wishing to use the service must be accurately confirmed, and must be verified to remove the possibility of false identification.
- Access Control: Invalid users must not be able to use the service.
- Non-repudiation: Within a legal contract even an implicit one, sending and receiving information must be confirmed by a third party. This is to provide protection from compromised information within a group of dealers. Non-repudiation is the same as integrity security, and can be realized using digital signatures.

2.3.2 Security Requirements for Protection from Third Party Attack

In addition to the security requirements mention above, the system must be robust to the following attacks by a third party.

- Eavesdropping: Although some transferred data may be compromised, data can be secured from eavesdropping provided passwords are not compromised.
- Replay attack: This is an impersonation process where an adversary resends copied messages, while adhering to the protocol. Such attacks can be detected and blocked, based on the time and order of messages by challenge/response or timestamps. During communication, attempts by others to obtain the data and resend it with authentication, must be blocked.
- Impersonation attack: In an insecure channel, adversaries can disguise themselves as valid users and utilize services. Therefore, such users must be blocked.
- Password guessing attack: In an insecure channel, adversaries can analyze passwords by intercepting transferred messages. Therefore, such activities must be blocked.

2.3.3 Security Requirements in Heterogeneous Networks

- Mutual authentication: Mutual authentication is used to authenticate communication at both ends. A heterogeneous network involves communications

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.4161
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.4161

between different objects, thus, authentication is essential.

- End-to-end security: In order to ensure end-to-end security, encryption is used, and data is encrypted at the source terminal. The encrypted data is transferred without changing the destination terminal and the host. Communications between hosts in heterogeneous networks requires end-to-end security
- Fast roaming authorization: In a heterogeneous network, roaming between domains occurs frequently. Presently, if the authorization time period is long, roaming service cannot be given without service disruption. Therefore, during roaming, fast authorization needs to be considered, in order to provide continuous service.
- Home authorization server overhead: When there are frequent authorization requests to the home authorization server from a remote location, then, home authorization server overhead may occur. Therefore, steps towards reducing or simplifying requests for authorization and access to the home authorization server need to be considered.
- Billing information update: In the current method, the information about a user service was accumulated, then, processed by the middle management server. However, in this type of method, middle management server overhead can increase and effectiveness can be reduced.
- Hierarchal Trust Relationship: In the current device's mobile environment, when the device moves and requests authorization or updates a ticket, it accesses the home authorization server to make the request. This type of method directly affects server overhead and burdens the network. Therefore use of the hierarchal trust relationship method must be considered.

3. Related Work

This section describes existing roaming, accounting, ID-based schemes as well as their characteristics and advantages/disadvantages.

3.1. Scalable Authentication Scheme for Roaming

In an environment where domestic roaming and heterogeneous network handover is progressing, a fast and superior scalable authentication method is needed, instead of merely providing a secure communication service. This method is associated with a highly scalable authentication framework providing fast roaming, therefore, a trust relationship structure based on direct/indirect domains and hierarchal caching is needed. When hierarchal authentication caching is used, scalability is guaranteed, authentication delay is reduced and the network burden associated with authentication is reduced. In domains with the basic trust relationship, smooth roaming can be provided, and scaling of the authentication system is possible[6]. However, there is the disadvantage of possible delays, due to the authentication process and caching agent substitute registration in the initial stages of roaming.

3.2. Mobile Commerce AAA Scheme

Wireless LAN is rapidly becoming a crucial component in next-generation mobile communication. Despite this success, there are user privacy and access control issues such as authentication problems and accounting and billing problems. Especially in the accounting field, research about packet accounting based on IP is insufficient, thus, several ISP's adopted a fixed-sum accounting system. This paper presents a packet accounting model compatible with international standards of mobile commerce and the verification results[4]. However, the disadvantage is that the payment confirmation and recharge must proceed via a separate process and the home authentication server and billing server overhead may increase.

3.3. ID-based Authentication Key Exchange Scheme

An identity-based Authentication and Key Exchange (AKE) protocol is proposed, which is extensively based on the provable security model of Canetti and Krawczyk (CK-model), using pairings for securing heterogeneous wireless access[7][9]. Based on the CK-model approach, an ideal and secure key exchange protocol was initially proposed. Then, a fully-fledged authenticator is built, to provide authentication of the ideal protocol. This provides a practical AKE protocol for heterogeneous environments, while handling the security burden. Analysis shows that this protocol is secure, with partial forward-secrecy, and efficient in the asymmetric wireless environment. However, this protocol does not provide perfect forward-secrecy.

4. Proposed Scheme

In the proposed scheme, the mobile device transmits information about billing amounts to the home authentication serve in a heterogeneous network environment; then, it requests authentication and receives the ticket. Subsequently, even if the mobile device moves to a heterogeneous network, if the ticket that was authenticated by the home server is presented, the heterogeneous authentication server additionally transmits an authentication request message as a trust relational authorization message. In home authentication, in order for the mobile device to be authenticated, the ID-based private key generation number is transmitted. The mobile device receives a service after obtaining authentication. In

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.4161
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.4161

a heterogeneous network, depending on the mobile device's service usage, the appropriate amount is deducted from the prepaid amount information in the ticket, which is renewed to settle accounting. Roaming and authentication henceforth is performed in accordance with the same process. By this means, the information and authentication request for accounting associated with the mobile device does not have to be transferred to the home authentication server, but may be handled at the trust relational server. Also, the server and trust relation may be formed in the previous step, and the mobile device can be effectively authenticated if it moves to another heterogeneous network. When this is type of method is used, the hierarchal trust relationship service may be used for renewal of authentication and accounting information, and fast roaming is provided in the heterogeneous network

4.1. System Parameters

The system parameters used in this scheme are as follows.

- $*$: (MD : Mobile Device, $AAAH$: Home Network Authentication Server, HN : Heterogeneous Network Authentication Server)
- ID_* : Identification of *
- PW : Password of Mobile Device
- $h(\ )$: Secure One-way Hash Function
- PIN : Serial Number of Mobile Device
- AT_* : Authentication Time Value of *
- OTP_* : One-Time Password of *
- $e: G_1 \times G_1 \rightarrow G_2$ Bilinear Map
- α_*, β_* :Authentication Value for Authentication of *
- MAC : Message Authentication Code
- KGV : Value for ID based Key Generation
- $E_*[\ ]$: Encryption with key of *
- $Sign_*$: Signature of *
- KU_* / KR_* : ID-based Private/Public Key of *
- $KUCert_* / KRCert_*$: Certification based Private/Public Key of *
- KS : Pre-shared Key between Mobile and Home Network Authentication Server
- HTS_Req : Hierarchal Trust Relationship Server Authorized Request message for Roaming
- $Account\_in\ fo$: Information for accounting
- $Balance\_in\ fo$: Useable Pre-paid accounting information
- $Balance\_in\ fo_{renewal}$: Renewal Pre-paid accounting information
- $Lifetime$: Lifetime of Ticket

4.2. Proposed Protocol

In the proposed protocol, the process of issuing a ticket that includes authentication and accounting information, and the process of accounting information renewal in a heterogeneous network, constitutes a accounting information renewal process with a hierarchal trust relation. The distributed mobile device's serial number, password and symmetric key are separated in the registration process. The accounting method was that the user prepaid the amount, and the amount is updated in the issued ticket. Subsequently, the user is billed for the amount used, and the prepaid amount information is renewed accordingly. The ticket is renewed until there is no remaining difference between the prepaid amount and the value of service received between heterogeneous networks.

4.2.1. **Authentication and Accounting Information Ticket Issue.**

In these steps, the mobile device receives authentication from the home server, transfers the information to settle the amount it will use and receives the ticket (Fig. 1.).

4.2.2. **Accounting Information Renewal.**

In the accounting information renewal process, the mobile device moves to a heterogeneous network, then, presents the ticket to the heterogeneous authentication server, then, authentication is received. Depending on service usage, after payment, the appropriate deduction is made to the ticket value, then, renewed (Fig. 2.)

4.2.3. **Accounting Information Renewal using Hierarchal Trust Relation.**

When mobile devices move from the current heterogeneous network to another heterogeneous network, the ticket that was issued by the previous heterogeneous network authorization server must be presented to the new heterogeneous network authorization server to ensure that there is the same information renewal process. Unlike the current method, the authorization request and ticket renewal does not occur at the home server, but is handled in the previous step at the heterogeneous authentication server. By this means, the authorization server with the trust relational approval is accessed to handle authorization and approval and payment which, reduces overhead of the home authorization server(Fig. 3.).

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.4161
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.4161

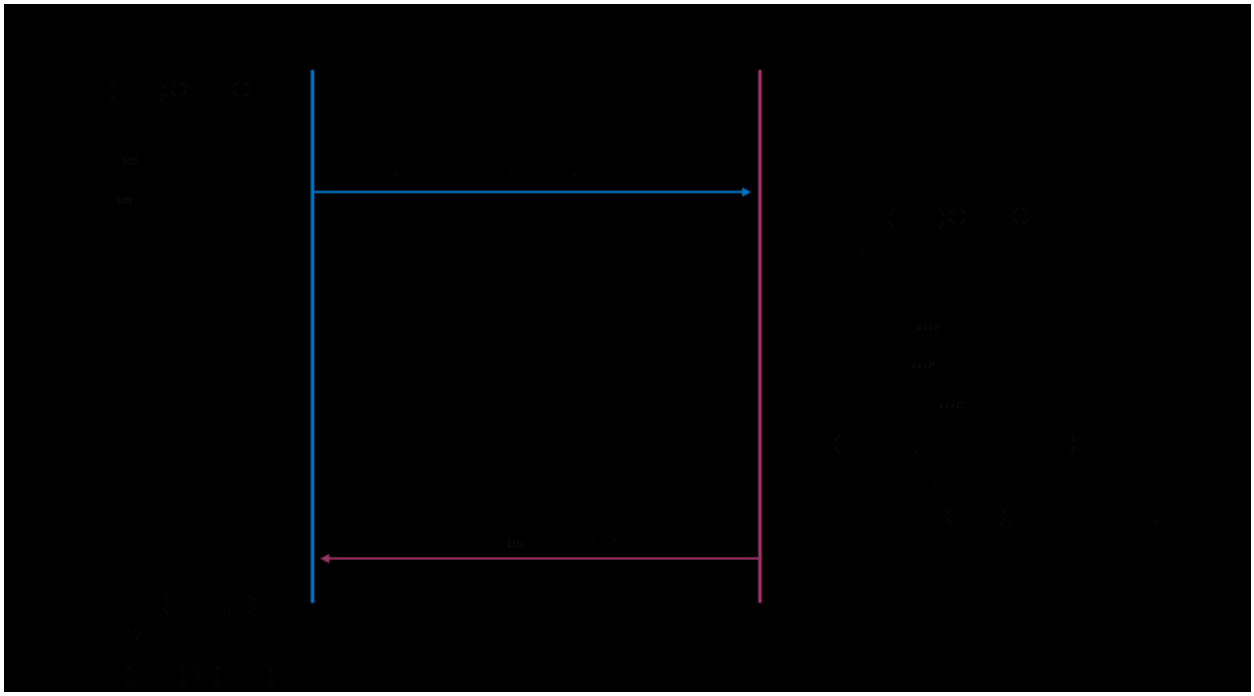

Fig. 1. Authentication and Accounting Information Ticket Issue

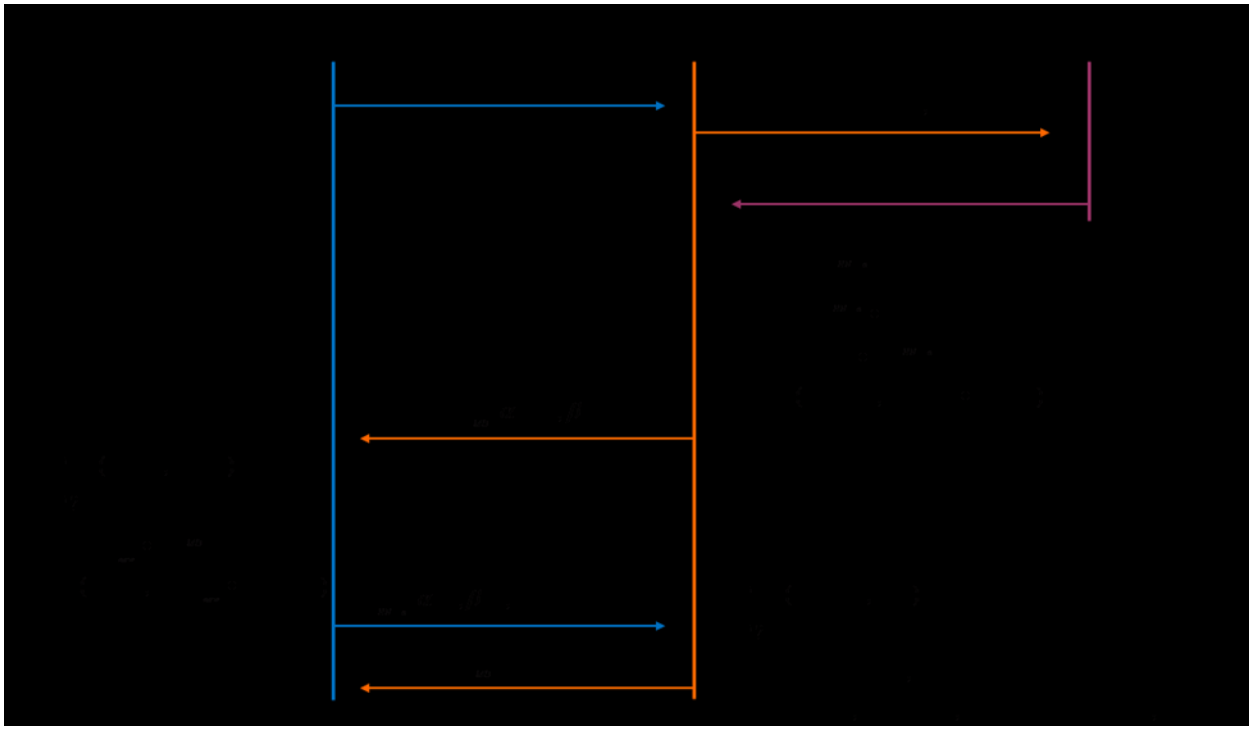

Fig. 2. Accounting Information Renewal

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.4161
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.4161

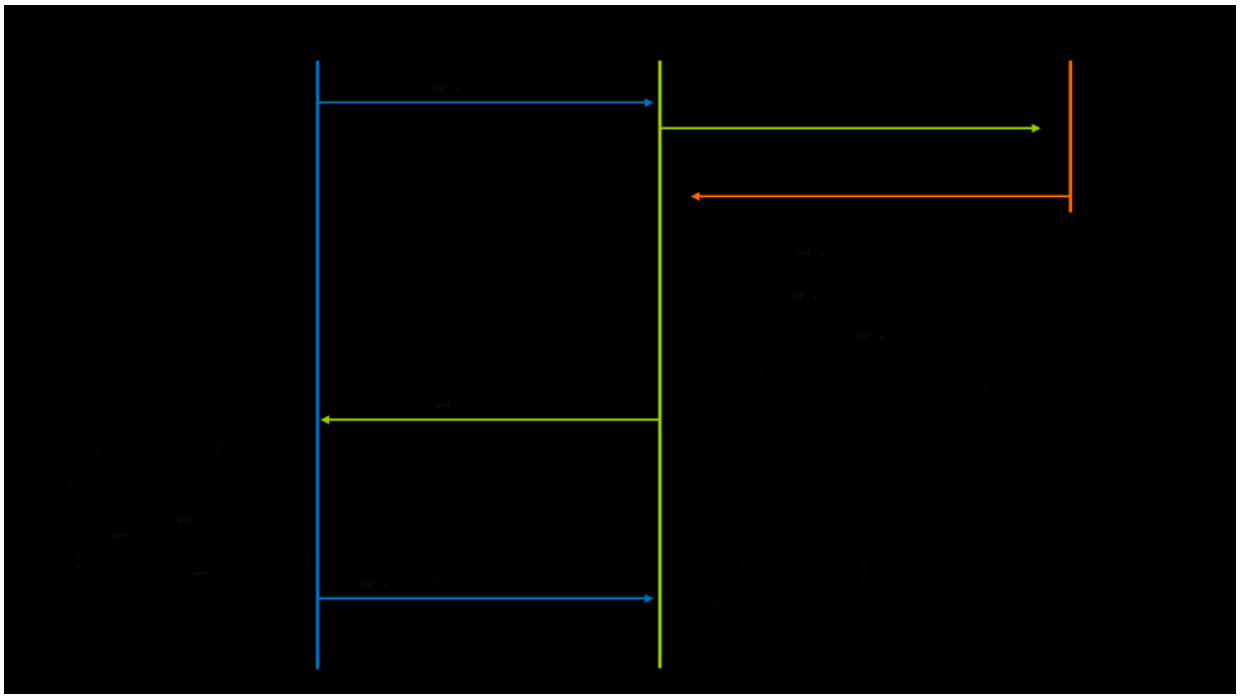

Fig. 3. Accounting Information Renewal using Hierarchal Trust Relation

5. Analysis of Proposed Scheme

The proposed protocol is analyzed in terms of security, third-party attacks, and security requirements of the ticket mentioned in Section 2, as follows.

- Confidentiality: The data used in communication can be confirmed only by the qualified object. The adversary must be prevented from learning the traffic characteristics of data source, destination, frequency, lengths or communication network. The confidentiality is provided by the symmetric key shared between the user and the home authentication server, and the ID-based private/public key.
- Integrity: The transmitted message must not be forged, deleted or modified, unless its modification is confirmed. In the proposed scheme, this is provided by verifying the hash and MAC values.
- Authentication: In the proposed method, the one-time password between mobile device, home authorization server and mobile device, heterogeneous network server, OTP, α , β is provided via ticket verification.
- Access control: Authorized attempts to write and change information resources must be distinguished from unauthorized attempts, which must then be blocked. The access management function is used within the system. Within the network, invasion interception is used to supplement access management. Further, unauthorized users must not gain access to services. Unauthorized users cannot receive a key from the heterogeneous network, thus, key establishment is impossible.
- Non-repudiation: Non-repudiation can be solved via an electronic signature; the proposed method provides both ID-based public key/personal key for non-repudiation. Also, between the home authorization server and heterogeneous server, a signature is provided.
- Eavesdropping: Although some transferred data may be compromised, data security is ensured provided passwords are not compromised. Using encrypted communications, data is secure from eavesdropping attacks.
- Replay attack: The authentication and accounting information process and accounting information renewal process, authentication time value and ticket lifetime is secure from replay attack in the proposed method.
- Impersonation attack: In an insecure channel, adversaries can disguise themselves as valid users and receive services. Therefore, unauthorized users must be blocked. The proposed scheme provides mutual authentication at every step, thus, impersonation attacks are impossible.
- Password guessing attack: In an insecure channel, adversaries can analyze a password by intercepting transferred messages. Therefore, these problems must be eliminated. The essential information required for

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.4161
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.4161

authentication is not the password, it is OTP, thus, it is impossible to guess the password. This method performs an XOR operation with ATV and encrypts it as a public key of the key management server, thus, even analysis of the message will not yield the password.

- Mutual Authentication: In the initial stages of authentication and ticket issue in the proposed process, the home network authentication n server uses the OTP of the mobile device and checks the authentication. The mobile device then verifies the ticket of the home network authentication server and performs mutual authentication. In the heterogeneous network, all processes undergo mutual authentication by a ticket and α, β.
- End-to-end security: In order to ensure end-to-end security, encryption is used and the data is encrypted at the source terminal. The encrypted data is transferred without changing the destination terminal or the host. Communications between hosts in heterogeneous networks require end-to-end security. The proposed scheme supports security between servers as well as end-to-end security, to improve security.
- Fast Roaming Authentication: In a heterogeneous environment, because roaming occurs frequently, the proposed method uses the hierarchal trust relational server for fast roaming authentication. This can reduce authentication delays; using a ticket, accounting can be handled, therefore the number of message exchanges can be reduced.
- Home authentication server overhead: In a heterogeneous network roaming environment, mobile devices that have moved through an external network frequently ask for home network authentication, which may result in home authentication server overhead. Therefore, the proposed method does not request home authentication server authentication during roaming. Instead it receives authentication from servers with hierarchal trust relations, so, the home network authentication server overhead and delay is reduced.
- Accounting information renewal: The accounting information is accumulated from services used by the mobile device; ultimately the middle management server handles the accounting. This leads to an increase in the middle management server overhead and reduces effectiveness. In the proposed method, the amount to be used by the mobile device is prepaid by the user, and the new accounting information is included in the formation of the ticket. When the mobile device service is used, the amount used is deduced from the ticket value and it is renewed, thus, it does not need access to the middle management server. This reduces the home server overhead and costs associated with effectiveness and package.
- Hierarchal trust relation: hierarchal trust relation is the formation of a tree structure of trust via authorization between servers. It can authenticate the mobile device itself. Therefore, when the mobile device migrates and requests authentication or ticket renewal; If this is processed by accessing the home authorization server, it may directly affect the server's overhead; If this uses the proposed process, it does not always have to access the home authorization. Instead it uses servers that are based on hierarchal trust relations and are effective.
- Overhead analysis: The authentication method of the proposed method and the current heterogeneous network is compared via annual production of the home authentication server overhead. In order to compare the overhead, the following terms are defined: the device's number is n ($n = 1,100,200,...,1000$), the authentication request message to the home authentication server is m, the overhead of the home authentication server is OH, the movement count from the start to the end of the mobile device session is r ($r = 10$, it is assumed that the frequency of mobile device roaming between networks is 10). Therefore, the equation for overhead analysis is $OH = m*n*r$ and $OH = 100*100*10 = 100000$. For example, in the current heterogeneous network, in the equation for the authentication method; if 100 mobile devices are registered in the home authentication server, then, the total movement count is 10, and every time a mobile device moves, it requests authentication from the home authentication server. However, in the proposed method, the same process is considered, but the mobile device requests authentication from the home authentication server only when it initially moves to heterogeneous network. Therefore the mobile device's roaming count decreases. Compared to the current heterogeneous network's authentication method, the proposed method decreases the overhead.

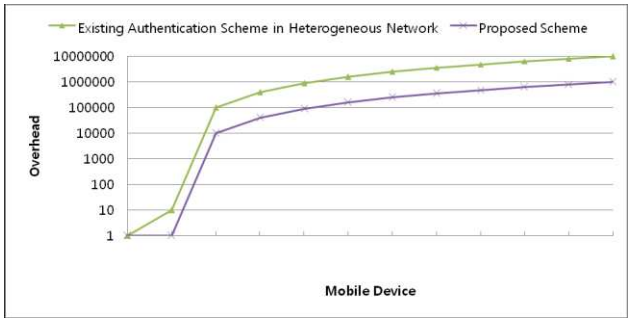

Fig. 4. Analysis of overhead by increase device

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.4161
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.4161

6. Conclusion

Due to the evolution of network environments, the next-generation network is combining the advantages of the current wired networks and mobility of wireless networks. This type of wired/wireless networks' combined service results in changes not only in terms of the environment but also in terms of security technology; in the rapid evolution of network environments, the absence of appropriate security technology means that service is threatened in combined wired/wireless network environments. Therefore, research and development into an appropriate security technology has reached a critical stage, as combined wired/wireless environments emerge.

This work performed research associated with roaming and an AAA mechanism in the wired/wireless heterogeneous network environment, and used the OTP and ID-based public key method for authentication of services received via the user's mobile device. Also, using a ticket, fast roaming and home authentication server overhead was reduced. In the initial stage, the accounting that will be used is prepaid and this amount is included in the renewed ticket. Subsequently, the amount used is deducted and the ticket is updated and renewed; a request for the mobile device's accounting information does not always have to be transmitted to the home authentication server; it can be handled at the trust relational server. If this type of method is used, the hierarchal trust relational server in the heterogeneous network environment may provide accounting information renewal and fast roaming. Also, it was proposed that even if the mobile device moves to a heterogeneous network, the home network does not have to be accessed; authentication can be obtained in the heterogeneous network authentication server with hierarchal trust relations. This enables continuous service. Using this hierarchal trust relational server, authentication technology will be secure and effective. Henceforth, when the system is built via analysis and performance evaluation of communication in terms of volume, detailed understanding of the situation will be needed..

References

[1] Adi Shamir, "dentity-based cryptosystems and signature schemes," CRYPTO'84, pp.47-53, 1984.

[2] B.J. Kim, "The Technological Trend of Next Generation Authentication Protocol DIAMETER AAA, " Telecommunication Technology Association Technology Standards Issue, 2001.

[3] Brian Lloyd, William Allen Simpson, "PPP Authentication Protocols," RFC 1334, 1992

[4] Gwanyeon Kim, Chinu Lee, Sehyun Park, Ohyoung Song, and Byungho Jung, "A Study on Mobile Commerce AAA Mechanism for Wireless LAN," HSI 2003, pp.719-724, 2002.

[5] H.G. Kim, B.G. Lee, D.H. Choi, S.K. Yoo, M.H. Kim, H.D. Lee, H. J. Yoo "On the International Standardization of AAA Technology," Etri Trend Vol. 20, No. 1, 2005.

[6] Heejin Lee, Yu-Kyong Song, Myung Soo Rhee, Chong-Kwon Kimj, "A Scalable Authentication Framework for Fast Remote Roaming with Hierarchical Cachingk," Korean Institute of Information Scientists and Engineers, Vol. 32, No. 5, pp.561-573, 2005.

[7] Jun Jiang, Chen He, Ling-ge Jiang, "On the Design of Provably Secure Identity-Based Authentication and Key Exchange Protocol for Heterogeneous Wireless Access," ICCNMC, pp.972-981, 2005.

[8] John Vollbrecht, Pat calhoun, Stephen Farrell, Leon Gommans, George Gross, Betty de Bruihjn, Cess Laat, Matt Holdrege and David Spence, "AAA Authorization Framework," RFC 2904, 2000.

[9] Jun Jiang, Chen He, Ling-ge Jiang, "On the Design of Provably Secure Identity-Based Authentication and Key Exchange Protocol for Heterogeneous Wireless Access," ICCNMC, pp.972-981, 2005.

[10] Pat Calhoun, John Loughney, Erik Guttman, Glen Zorn, and Jari Arkko, "Diameter Base Protocol," RFC 3588, 2003.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.4161
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.4161