IDENTITY-BASED AAA AUTHENTICATION PROTOCOL

Dong-myung Kim, Young-bok Cho, Dong-heui Lee, Sang-ho Lee

Dept. fo Network Security Laboratoy Chungbuk National Univ.
E-mail : { singall@hanmail.net, bogi0118@netsec.cbnu.ac.kr, easttwo62@kdc.ac.kr, shlee@netsec.cbnu.ac.kr}

ABSTRACT:

IETF suggested AAA for safe and reliable user authentication on various network and protocol caused by development in internet and increase in users. Diameter standard authentication system does not provide mutual authentication and non-repudiation. AAA authentication system using public key was suggested to supplement such Diameter authentication but application in mobile service control nodes is difficult due to overhead of communication and arithmetic. ID based AAA authentication system was suggested to overcome such weak point but it still has the weak point against collusion attack or forgery attack. In this thesis, new ID based AAA authentication system is suggested which is safe against collusion attack and forgery attack and reduces arithmetic quantity of mobile nodes with insufficient arithmetic and power performance. In this thesis, cryptological safety and arithmetical efficiency is tested to test the suggested system through comparison and assessment of current systems. Suggested system uses two random numbers to provide stability at authentication of mobile nodes. Also, in terms of power, it provides the advantage of seamless service by reducing authentication executing time by the performance of server through improving efficiency with reduced arithmetic at nodes.

KEY WORDS: Diameter, ID-based Cryptography, AAA, Mobile IP

1. INTRODUCTION

With development in internet, users moves between mobile network and local network and enjoy internet services. Particularly with increase in internet service users, a problem was produced in relation to security and charge in relation to the use of internet service with inter domain. For this, IETF suggested AAA standard for authentication, authorization verification, and charge of various wire/wireless services. Diameter standard, which is a new version of AAA, supports mobile IP and provides more flexible structure and security compared to previous versions of radius.

ID based cipher produces public keys through one-by-one mapping between public keys and the identities of users. E-mail addresses or NAI's of users may be used as the public keys of users. As a result, the load for obtaining and confirming CRL's in relation to public keys is removed and there is a advantage that the communication between system networks and mobile devices is reduced. Byeong-Gil Lee and Doo-Hoe Choe suggested ID based AAA authentication protocol using weil-pairing. However, although the authentication protocol suggested by Byeong-Gil Lee and Doo-Hoe Choe resolved the problem of mutual authentication and non-repudiation with use of ID based cipher, still has the weak point that cannot screen collision attack and forgery attack (1 and 2). In this thesis, an integrated authentication system of mobile IP and diameter is suggested with use of ID based cipher. In the suggested system, an cipher system with ID base using weil-pairing of D. Bon 또 and D. Franklin. The suggested authentication system may easily be applied in mobile nodes because it reduces the arithmetic load and communication load compared to public key based cipher and is safe against collision attack or forgery attack as well as mutual authentication and non-repudiation that were previously required (3 and 4).

In this thesis, it was intended to supplement the problems with previous studies which were suggested to supplement AAA authentication system of which the importance is more elevated with development in mobile internet and to suggest an authentication system that may reduce arithmetic load of mobile nodes during authentication. For this study, below related studies are conducted: firstly, a review is made in relation to diameter that is the most updated version of AAA and can be the environment for suggestion of authentication system; secondly, a review is made in relation to ID based cipher to supplement the weak points in mobile internet environment using public key base; and thirdly, current ID based AAA authentication system, which supplemented the known weak points with diameter, is analyzed. The mobile nodes using mobile IP have limited power and the arithmetic performance inferior to common PC's. Therefore, Authentication system is designed so as to execute authentication with minimized arithmetic of cipher needed in authentication process (5). For this, times of arithmetic at mobile nodes are reduced by producing two random integer numbers and signature value is made with use of each produced integer number. In the suggested system, possible attacks in mobile internet environment are assessed and is compared with current systems. Also, the performance is compared with current systems to ass the arithmetic efficiency. The thesis consists of 'Chapter 1. Scope' and 'Chapter 2' to explain ID based cipher and diameter in mobile IP environment as related study; in Chapter 3, a new ID based AAA authentication system is suggested; in Chapter 4, the requirement for the security of suggested system is compared with current systems to asses it; and in Chapter 5, conclusion is made.

2. TITLE AND ABSTRACT BLOCK

2.1 AAA

AAA protocol is the framework that controls the functions including authentication, authorization verification, and charge on multi network and platform and executes below-listed functions:

- *Authentication : verifies the identities of users prior to permit access to network*
- *Authorization : decides the authorization and service to be permitted for the uses permitted to use the network*
- *Verification : provides the users with the methods to collect the information related to the resources.*

In general, RADIUS protocol has been used as the AAA protocol for the services such as PPP or terminal server access (6). However, due to rapidly increasing network environment, REDIUS became inappropriate as the protocol for AAA service in terms of scalability, security, and technological limit of protocol and diameter protocol was suggested. The diameter protocol, for which standard definition work is being done, may provide with various

services through various applications in addition to basic protocol. Below-shown are the various applications of diameter protocol:

- *Mobile IP Application : Development of routing technology to support roaming of IP nodes using IPy4 or IPy6 between serve network and media.*
- *CMS Security Application : Messages among servers are transferred as the order consisted of AVP; development to assure integrity and confidentiality among the nodes messages are passing.*
- *NASREQ Application : Definition of NAS's to make supports from simple use of dial up and to VPN support, smart authentication method, and roaming.*
- *Diameter Base Protocol : Protocol development in relation to diameter to support charge, transfer, security, and proxy.*

Mobile IP is the application service that makes it possible to receive the services for users continuously when mobile nodes moves from home network to other network.

2.2 ID-base Cryptography

The concept of ID based system, which produce public keys with use of individual identity information of subscribers as one-way function, was suggested by Shanmir [7] in 1984 for the first time. ID based system has the strong point that authentication of a person may easily made with use of identity information, which is the only one for identification of the identity of users, such as internet domain address, e-mail address, registered residence number, telephone number, and card number of a person who wants transaction, and that public key based electronic signature and key distribution may independently made based on such authentication. D. Boneh and D. Frankin suggested new ID based cipher using weil-pairing (8). The stability of this is based on Gap DHP. The authentication system suggested in this thesis uses ID based cryptology suggested by D. Boneh and D Franklin.

The next is the ID based cipher suggested by K. Boneh and D. Franklin: E is an elliptic curve on which is defined as ; is prime finite field of p and , . Let's assume that and are cyclic groups where order is prime number q, is an additive group that consists of points on , and is a multiplicative consisted of subgroups on . If function satisfies following condition, is called weil pairing.

2.2.1 Stability base problem : To resolve key management problem in conventional encryption system, the safety used in public key encryption system is based on the difficulty in DH(Diffie-Hellman) system. DH problems are classified into arithmetic DH problem, deterministic DH problem, and GDH(Gap Diffie-Hellman) problem.

1) DLP : Problem seeking for n *that satisfies* $Q = nP$ *to given two elements,* P *and* Q

2) DDHP : Problem determining whether $c = ab \bmod q$ *to given* P, aP, bP, cP.

3) CDHP : Problem calculating $c = ab \bmod q$ *to given* P, aP, bP.

4) Problem calculating abP *from* P, aP *and* bP *with use of DDH Oracle.*

G, which is a group consisted of the points on elliptic curve Fl, is a cyclic group having generator P, and $a, b, c \in Z/l$. when the relationship among above-shown problems, DDHP may be resolved if CDHP is resolved.

2.2.2 Weil-pairing : The example that satisfies the characteristics of GDHP is weil-pairing. Although many scientists conducted studits to seek for GDH group, no GDH group has been known excluding supersingular elliptic curve with application of bilinear function such as weil-pairing. Weil-pariting is the bilinear function defined on the supersingular elliptic curve and is defined as follows:

1) ***Bilinearity****:To random* $P, Q, R \in G1$ *and* $a, h \in ZP$, $e(aP, bQ) = e(P, Q)^{ab}$ *or* $e(P + Q, R) = e(P, Q) \cdot e(Q, R)$, $e(P, Q + R) = e(P, Q) \cdot e(P, R)$ *, is satisfied.*

2) ***Identity*** *: To random* $P \in G1$, $e(P, P) = 1$ *is satisfied.*

3) ***Alternation*** *:To random* $P, Q \in G1$, $e(P, Q) = e(P, Q) - 1$ *is satisfied.*

4) ***Non-degeneracy*** *:To* $Q \in G1$, *if* $e(P, Q) = 1$, P *is infinite point (0).*

5) ***Efficiency*** *: An algorithm that the calculation of* $e(P, Q)$ *is efficient exists. Let's assume that points on elliptic curve,* P, aP, bP, cP *are given. In this case, when CDHP, i.e. are given, the problem to seek for* abP *is not easily resolved. However, the problem whether* $abP = cP$ *is formed when DDHP, i.e.* P, aP, bP, cP *are given may easily be resolved by confirming whether* $e(aP, bP) = e(P, cP)$ *is formed with use of weil-pairing. If equation* $e(aP, bP) = e(P, cP)$ *is formed,* P, aP, bP, cP *become DDH pairs. Therefore, they may be used in cipher system as the example that satisfies the characteristic of GDHP.*

2.3 Current ID based AAA authentication system

The ID based AAA authentication system of Byeong-Gil Lee and Doo-Ho Choe was suggested to resolve mutual authentication and non-repudiation known as current problem and to resolve the problems with public key base with use of ID based cipher. This authentication system used the ID based cipher system using weil-pairing suggested by D. Boneh and D. Franklin and the ID based signature system of Jae-Choon Cha and Jeong-Hee Cheon [6,9]. However, the suggested authentication system used the ID based cipher using weil-pairing suggested by D. Boneh and D. Franklin and the ID based signature system suggested by Jae-Choon Cha and Jeong-Hee Cheon, thus, does not satisfy the security requirements of AAA and has arithmetic weak point. Below-shown is the ID based cipher system using weil-pairing suggested by D. Boneh and D. Franklin and the ID based signature system suggested by Jae-Choon Cha and Jeong-Hee Cheon, which are currently being used [6, 8].

- **Setup :**
  - G : GDH group having prime number as order
  - P : G Generator of
  - e : bilinear function
  - $H_1 : \{0,1\}^n \times G \rightarrow Z/p$, $H_2 : \{0,1\}^n \rightarrow G$: Collision-resistant function
  - ID_B : ID of B
  - $b (\in Z/p)$: Master key of signer B
  - $Q_B = H_2(ID_B) = bQ_B$: Public key related to ID of B
  - $D_B = b \cdot H_2(ID_B) = bQ_B$: Secret key related to ID of B
  - $P_B = bP$: public
  - m : meassge
- **Encrypt:**
  - ID is converted into Q_{ID} , the point on G.
  - Random value, $\sigma \in \{0,1\}^n$ is produced and below-shown is calculated $\gamma = H_1\{\sigma, M\}$
  - Below-shown is calculated and converted into cipher.
- **Decrypt:**
  - In assumption that $C =< U, V, W >$, below-shown is calculated.
  - $M = W \oplus G_1(\sigma)$ is calculated.
  - After calculation the equation $r = H_1(\sigma, M)$, if $U \neq rP$, message is refused and, if they are equal, the cipher is interpreted. Below-shown is the signature system suggested by Jae-Choon Cna and Jeong-Hee Cheon.[9]
- **Sign:**
  - Signer B select random number $r = Z/p$, calculate , $U = rQ_B$, $h = H_1(M, U)$ and $V = (r + h)D_B$, and $sig = (U, V)$ is defined as the signature to message M.
  - The signature of message M, sig , is verified by confirming using $e(P_B, U + hQ_B) = e(P, V)$ bilinear function e.

3. ID BASED AAA AUTHENTICATION SYSTEM DESIGNG

This thesis suggests a new ID based authentication system in AAA environment with application of the ID based cipher using weil-pairing suggested by D. Franklin and the ID based signature suggested by Jae-Choon Cha and Jeong-Hee Cheon. In the suggested system, two random values are produced, arithmetic load is reduced with reduced times of

arithmetic at mobile node, and security safety is provided with produced signature value using produced two random values. As authentication is executed with use of EAP supplied by diameter, application is possible in AAA environment with no additional conversion. EAP supplied by diameter, application is possible in AAA environment with no additional conversion.

3.1 Structure of the base of suggestion

3.1.1 Safety base problem : When implementation is made with use of ECC in this thesis, cryptologic safety is provided with use of Gap Diffie-Hellman Problem (GDHP) that has higher speed compared to other cipher base.

3.1.2 Weil-Pairing : Weil-pairing defined in 2.2.2. is used as the mathematic base of suggested system.

3.2 Design of suggested technique

Suggested system is divided into AAA servers and mobile nodes participating in authentication process, pre-stage for production of private keys of AAA clients, and authentication execution stage.

3.2.1 Pre-Stage : At pre-stage, all the AAA servers, mobile nodes, and AAA clients participating in pruduction of master key of KGG are registered in KGG and produces private key. E is an elliptic curve on Fp which is defined as $y3 = x3 + 1$; Fp is prime finite field of p and $p = 2 \bmod 3$, $p = 6q - 1$ $(q > 3)$. Let's assume that $G1$ and $G2$ are cyclic groups where order is prime number q, $G1$ is an additive group that consists of points on Fp , $G2$ and is a multiplicative consisted of subgroups on $Fp2$. If function $e = G1 \times G1 \rightarrow G2$ satisfies following condition, is called weil pairing.

[Table 1] Notation

Notation	*Description*
ID_{MN}	*ID in MN*
$a_{MN}(Z_P)$	*Master key in MN*
$P_{MN} = a_{MN} \cdot H_2(ID_{MN}) = a_{MN} P$	*Private keys related to Id of MN*

- Setup Step

$P_{pub}=sP$ is produced by selecting P, the generator of $G1$ and by selecting random master key $s \in Z^* q$. After completion of above-shown process, open $\{p, n, P, P_{pub}, , H_1, H_2, G_1, G_2\}$.

- Registration step

- MN calculates $a_{MN}G = (x_{MN}, y_{MN})$ and transfer to KGC.
- KGC select random number $k_{MN} \in [0,1] \rightarrow G$ and calculate the next.
- KGC transfer $(r_{MN}, s_{MN})s_{MN}$ that satisfy $s_{MN} \equiv k_{MN} + r_{MN} + s \bmod q$ and transfer it through calculation confidential channel.
- User A obtains $x(R_{MN}) = r_{MN} H_2(ID_{MN}) \bmod p$ from r_{MN} that received from KGC, recover R_{MN} , check , $(a_{MN} + a_{MN})G = r_{MN}P + R_{MN}$ and treat S_{MN} as confidential information.

3.2.2 Authentication step : Authentication stage is started with request for authentication by mobile node. Mobile node run authentication request stage and transfer produced information to authentication server. Authentication server receives the information of mobile node and authenticate mobile node.

- Authentication Request step

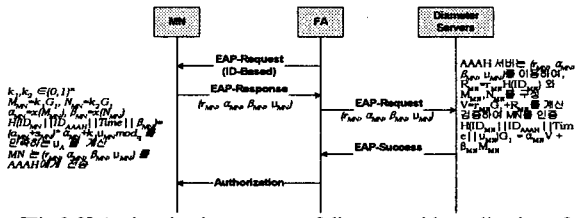
- MN select random numbers $k_1, k_2 \in \{0.1\}_n$ and calculate $M_{MN} = k_1 G$ and $N_{MN} = k_2 G$.
- A definition is made as $\alpha_{MN} = x(M_{MN})$ and $\beta_{MN} = x(M_{MN})$, calculate μ_{MN} that satisfy $H(ID_{IN} \| ID_{Server} \| Time \| \beta_{IN}) = (a_{MN} + s_{MN}) \cdot \alpha_{IN} + k_1 \mu_{MN} \bmod q$.
- MN transfer to authentication server for authentication.

- Authentication Respond step

- Check $0 < (r_{MN}, \alpha_{MN}, \beta_{MN}) < p$ and $0 < \mu_{MN} < q$.
- Construct below-shown one with use of the information of $(r_{MN}, \mu_{MN}, \alpha_{MN}, \beta_{MN})$. $r_{MN}H(ID_{MN}), M_{MN} = k_1 G$, and $N_{MN} = k_2 G$
- After calculation of $V = r_{MN}P + R_{MN}$, verify $H(ID_{MN} \| ID_{Server} \| Time \| \beta_{IN}) = (a_{MN} + s_{MN}) \cdot \alpha_{IN} + k1\mu_{MN} \bmod q$. and authenticate MN.

3.3 Application of suggested system

As the authentication of suggested system may be executed with use of diameter EAP application connected to the registration process of mobile IP, application is possible with no additional change of diameter. Authentication in AAA environment is executed through MN and AAAH and the communication of MN-FA-AAAH-HA is done in relation to mobile IP. As all the communication message in AAA environment is done through diameter CMS application, there is a characteristic with AAA authentication protocol that session key is not produced for safety communication after authentication. [3.2] shows the authentication process of suggested system in AAA environment.



[Fig.3.2] Authentication process of diameter with application of suggested system

① Authentication in the suggested system is initiated with receipt of EAP-Request message from FA by mobile nodes.

② When mobile node access internet through visiting network, authentication information $(r_{MN}, \mu_{MN}, \alpha_{MN}, \beta_{MN})$ is produced with use of two random numbers, own ID, ID of AAAH, and timestamp and transferred to FA including message.

③ FA transfer EAP-Request message to AAAH of MN after receipt of EAP-Respose message. At this stage, FA cannot confirm the authentication information $(r_{MN}, \mu_{MN}, \alpha_{MN}, \beta_{MN})$ and transfer message to corresponding AAAH after reading EAP-Response message.

④ AAAH authenticate mobile node after confirmation of authentication information $(r_{MN}, \mu_{MN}, \alpha_{MN}, \beta_{MN})$ of mobile node. At this stage, if AAAH is not the proper owner of included in the arithmetic of mobile node authentication information, judgment of 'Impossible' is made at test. If MN is proper user, AAAH processes mobile IP registration in relation to MN. Upon completion of mobile IP registration process, MN transfers EAP-Success message to FA.

⑤ FA receipt EAP-Success message permit MN the authorization to access network.

4. ANALYSIS

The authentication system suggested in this thesis uses weil-pairing on elliptic curve and its safety is depended upon DLP (Diffie-Hellman Problem). The authentication scheme suggested in 4.1 will prove the safety against possible attacks between MN and FA sections. In 4.2, the cipher arithmetic of suggested authentication scheme will be assessed and the relative efficiency will be proved.

4.1 Stability analysis

In this part, the stability of suggested system in wireless environment against reuse attack, collision attack, forgery attack, known key-sharing attack, and exposure of confidential key of KGC is tested and is analyzed in comparison to current ID based authentication system suggested by Byeong-Gil Lee and Doo-Ho Choe.

- ***Replay Attack*** *: Attacker attempts to be authenticated as if it is MN with obtaining the information used by MN. However, it is impossible because cannot be expected at the stage of AAAH test. If the attacker forges , judgment of 'Impossible' is made at test.* $H(ID_{MN} \| ID_{Server} \| Time \| \beta_{MN}) = \alpha_{MN}V + \mu_{MN}P_{MN}$

- ***Impersonation Attack*** *: Let's assume that the attacker attempts to deceive AAAH with disguising itself as MN, the proper user. The attacker should obtain the values* $(a_{MN} + S_{MN})$ *. However, such obtaining is impossible and the attacker should produce random values of* $H(ID_{MN} \| ID_{AAAH} \| Time \| \beta_{MN'})$ *and the produced values should satisfy ; however, it is impossible.*

- ***Conspiracy Attack*** *: To know , which is the master key of KGC, with collision by n number of users, they should resolve the simultaneous equations,* $s_{Ai} = k_{ai} + r_{ai}a_{KGc} \bmod q(q \le i \le n)$ *, with use of n number of* (r_A, s_A)*. However, kA is confidential information to all the users and is differently given, thus, it is impossible to resolve this problem.*

- ***Unknownkey Share Attack*** *: Although attacker obtains the information being transferred and produces* $H(ID_{MN} \| ID_{AAAH} \| Time \| \beta_{MN'})$ *, the value of* $\beta_{MN'}$ *is judged 'Impossible' at confirm process.*

- ***Exposure of the confidential key of KGC****: In the suggested scheme, confidential information used in authentication of MN is not directly exposed although the confidential information of KGC is exposed. To produce signature value in authentication in the scheme* r_{MN} *, that is the confidential information known by MN only is used, however, as this is produced by MN, the unique value of* r_{MN} *, which is used in authentication, cannot be produced although attacker knows SA .*

[Table 4.1] Safety analysis

	Byeong-Gel , Doo-ho Lee	Proposal
Mutual authentication	○	○
Conspiracy Attack	×	○
Impersonation attack	×	○
Unknownkey share attack	○	○
Exposure of the confidential key of KGC	×	○

○ : Safe against attack , ×: Unsafe against attack

As shown in [4.1], the suggested system has the strong point that it is more safe against collision attack or forgery attack compared to current ID based AAA authentication systems and that the confidential keys of users which are registered in KGC cannot be produced although the confidential information of KGC is disclosed. As current ID based AAA authentication systems use ID based encipherment and ID based signature system with no modification for authentication, they have weak points in mobile communication environment compared to suggested system.

4.2 Analysis of arithmetic quantity

The times of arithmetic, which produces the largest load on cipheric arithmetic, is reduced on mobile node. Two random integer numbers are produced in authentication and each signature value is used in authentication. In addition, arithmetic is to be executed in the process of authentication confirmation in AAAH server so as to reducethe load on mobile node.

[Table 4.2] Analysis of arithmetic quantity

		Proposal	Byeong-Gel and Doo-ho Lee
Times of communication (C)		2	2
Times of random integer number production (R)	MN	2	1
	AAAH	0	0
Arithmetic (E)	MN	0	1
	AAAH	1	0
Multiply arithmetic (M)	MN	2	3
	AAAH	2	2
Hash arithmetic (H)	MN	1	3
	AAAH	2	3
Duration of execution time by node	MN	2R+1E+2M+1H	1R+1E+3M+3H
	AAAH	2M+2H	2M+3H

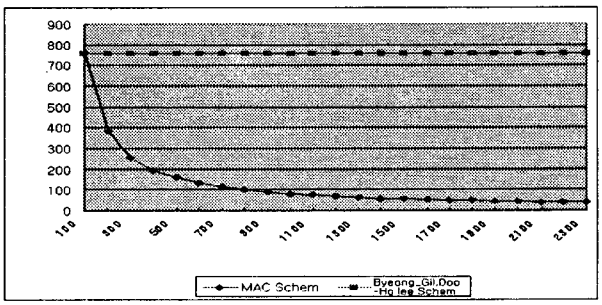
In the suggested system, to overcome the weak points in arithmetic and power at mobile node, the arithmetic executed in authentication process is arranged in authentication request confirm process by AAAH with relative superior arithmetic performance. Secondly, the performance of suggested authentication scheme is assessed in consideration of whole execution time during execution of communication to assess the performance of the suggested system. Secondly, to assess the efficiency of suggested system, a comparison is made with use of mean arithmetic time in execution of ID based cipher as the basic numerical value. Authentication execution performance of suggested system is shown in terms of time through this assessment.

The result value [13] of P. Barreto's test is used as the basic numerical number for assessment. P. Barreto's test uses Window XP operation system. After 50,000 times of execution in the environment of 2.1GHz CPU and 512 MByte of RAM, basic value was obtained with calculation of mean value. Multiply arithmetic (0.569ms), exponent arithmetic (755.88ms), and random integer number production (2.100ms) are used as the basic numerical numbers for assessment. Among afore-said authentication performance indexes by time, hash arithmetic is influenced by the change in inputted values and is excluded from assessment items. These basic numerical values are applied in execution arithmetic by node and total execution arithmetic of [Table 4.2] and the result is shown in [Table 4.3].

[Table 4.3] Comparison of arithmetic time

	Proposal	Byeong-Gel and Doo-ho Lee
MN	5.338ms	759.687ms
AAAH	757.018ms	1.138ms
Total execution time	762.356ms	760.825ms

As shown in [4.3], the result of total time of execution showed no significant difference between suggested system and current system. However, in general, AAAH is a server and has superior arithmetic performance compared to mobile node, thus, an assumption was made that the ID based cipher arithmetic time is also reduced at same ratio with increasing performance of AAAH server for comparison purpose.



[Fig. 4.1] Arithmetic time by performance of AAAH server

In [4.1], it is shown that the arithmetic capabilities of mobile node and AAAH server are same when the increase rate of the performance of AAAH sever is at 100. As the suggested system execute the arithmetic, which takes most of time for execution of authentication, in authentication confirm process, authentication execution time is reduced depended upon the performance of AAAH server. As a result, in case of current system, the arithmetic is executed at mobile node that receives the largest arithmetic and power load in ID based cipher, although the performance of AAAH server is improved, performance of authentication cannot significantly be changed. However, in case of suggested

system, the time needed in authentication at mobile node may be reduced and there is the advantage with mobile nodes that seamless service may be provided to the users of mobile IP.

5. CONCLUSION

IETF suggested AAA standard for security and charge related to authentication and service between mobile nodes and inter domain. However, diameter standard, the most updated version of AAA, has the problem that mutual authentication and non-repudiation are not possible and that application in moving environment is difficult in case that PKI is used, thus, to resolve such weak points, ID based AAA authentication system is suggested. Current systems use the ID based cipher system of D. Boneh and the signature system suggested by Jae-Joon Cha and Jeong-Hee Cheon and are not safe against collision attack or forgery attack.

In suggested system, two random values are produced, arithmetic load is reduced by reducing arithmetic times at mobile nodes, and safety in security is provided with signature value produced with use of produced two random values. Also, the efficiency of authentication performance at mobile nodes was tested through comparative evaluation with current systems. However, as the performance of AAAH cannot be calculated, authentication time in same condition of mobile node performance and AAAH server performance. In such assumption, the authentication performance of suggested system was compared to those of current systems with increasing performance of AAAH server. As a result, suggested system showed superior authentication performance at mobile nodes with increasing performance of AAAH compared to current systems.

REFERENCES

[1] Byung-Gil Lee, 2003., ICT 2003 ; *Concatenated Wireless Roaming Security Association and Authentication Protocol using ID-Based Cryptography Telecommunications*, 10th International Conference on , Volume: 1 , Pages:597 - 603

[2] Byung-Gil Lee, 2003:*Mobile IP and WLAN with AAA Authentication Protocol using Identity-Based Cryptography*" Vehicular Technology Conference,. VTC 2003-Spring. The 57th IEEE Semiannual , Volume: 3 Pages:1507 - 1511 vol.3

[3] Kyungah Shim.,2003. Electronics Letters; "*Efficient ID-based authenticated key agreement protocol based on Weil pairing* " ,Volume: 39 ,Issue: 8 ,17 April Pages:653 - 654

[4] J. C. 2002:*An Identity-Based Signature from Gap Diffie-Hellman Groups*, in Cryptology ePrint Archive, http://eprint.iacr.or~2002/018/2002.

[5] Sufatrio, K. 1999, I-SPAN:*Mobile IP Registration Protocol :A Security Attack and New Secure Minimal Public-Key Based Authentication*,".

[6] P.Calhoun, 2002 IETF work in pregress:*Diameter CMS Security Application*, draft-ietf-aaa-diameter-cms-sec-05.txt.

[7] A. Fiat.,1986. Crypto '86 :*How to prove yourself: Practical solutions to identification and siganture problems*, pp. 186-194.

[8] D. Boneh.,2001 LNCS vol. 2139. Crypto :*Identity Based Encryption from the Weil Pairings*, pp. 213-229,

[9] P.Calhoun, 2002.:*Diameter Mobile IPv4 Application*, IETF work inprogress.

[10] Y. Zheng, 1997. LNCS 1294 :*Digital signcryption or how to achieve cost(signature and encryption)<<cost(signature)+ cost(encryption)*, Advances Cryptology-CRYPTO'97,Springer-Verlag, pp. 165-179,

[11] D. Mitton., 2001. RFC 3127:*Authentication, Authorization, and Accounting: Protocol Evaluation.*

[12] P. Barreto, H. Kim, and M. Scott, Ecient Algorithms for Pairing-based Cryptosystems, Available from http://eprint.iacr.org, 2002.