I.J. Information Technology and Computer Science, **2010, 2, 55-62**
Published Online December 2010 in MECS (http://www.mecs-press.org/)

AuMID: An Authentication Mechanism based on Identity Tag under Future Internet Architecture

Ming Wan
Beijing Jiaotong University/National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing, China
Email: ming305.bjtu@gmail.com

Ying Liu and Hongke Zhang
Beijing Jiaotong University/National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing, China
Email: yliu@bjtu.edu.cn, hkzhang@bjtu.edu.cn

***Abstract*—It has been commonly recognized that the current Internet faces serious security and scaling problems. To address these problems, the architecture of ID/locator separation is the focus of future Internet development. However, the relevant authentication mechanism has not been proposed under this architecture. In this paper, we advance a new authentication mechanism called AuMID under ID/locator separation architecture, and describe the detailed procedures of access authentication and handoff authentication, and simultaneously give the deployment of authentication centers. Besides, AuMID uniquely introduces the Identity Tag which represents the terminal's identity information to implement the sustainable authentication for the terminal. This mechanism adopts the challenge-response approach and achieves the double-way authentication between the terminal and access network. At the same time, by the use of Identify Tag AuMID successfully guarantees the authenticity of the source under ID/locator separation architecture. In conclusion, this paper gives a qualitative analysis for the scalability and security of this AuMID and an evaluation of handoff authentication delay.**

***Index Terms*—sustainable authentication, handoff authentication, Identity Tag, authenticity, ID/locator separation architecture**

I. Introduction

In recent years, Internet has become an important driving force of the social and economic advancements, and it has become a significant part of people's lives. However, it is widely recognized that today's Internet routing and address system is facing serious scaling and security issues. In order to address these serious issues, most of research communities have a consensus that all of these are briefly caused by the dual semantics of IP address [1]. That is, an IP address delegates not only the identity information but also the location information of a terminal. And the study has found that the dual role of IP addresses as host IDs and locators makes difficult to design efficient solutions to mobility, multihoming and security under the traditional Internet architecture. Therefore, many countries have regarded the future Internet architecture as the most exigent research content in resent years [2,3]. And several new proposals introduce ID/locator separation into network architecture, such as A Secure and Scalable Internet Routing Architecture (SIRA) [4], Host Identity Protocol (HIP) [5] and Locator/ID Separation Protocol (LISP) [6]. This approach uses a new identity namespace as the host identifiers (IDs) in the transport and upper layer, and uses a new locator namespace as the locators to forward packets and to locate the destination hosts. As the basic research of the new generation Internet architecture, references [7,8] put forward universal network based on the architecture of identifier separation and mapping, and its main object is to separate the host's identity and location information and resolve the dual semantics of IP address. The authentication mechanism AuMID proposed by this paper is based on the ID/locator separation architecture of the upper universal network, and it effectively guarantees the authenticity of the hosts under this architecture.

It has gradually become a consensus in the network security research field to take the network security issues into consideration at the beginning of establishing the new network architecture. And the authenticity of the source is an important topic of network security research. It not only brings considerable benefits to the network forensics, but also is conducive to the rapid and sound development of network. The authentication mechanism is an effective method to guarantee the authenticity of the source. Nowadays many kinds of authentication schemes appear under different network architectures. Reference [9] proposes an one-pass GPRS and IMS authentication procedure for Universal Mobile Telecommunications System (UMTS). And reference [10] presents a localized fast re-authentication protocol to substitute the standard fast re-authentication protocol for the 3G-WLAN interworking architecture. Besides, reference [11] suggests a strong peer authentication algorithm that authorizes the peer which requests a service usage of the other peer in super peer based P2P network environment. But all of these authentication schemes can not accommodate to the characteristics of the ID/locator architecture, and can not meet the security requirements of this architecture. Therefore this paper proposes a new authentication mechanism AuMID under ID/locator

separation architecture, and it introduces the Identity Tag to implement the sustainable authentication when the terminal is associating with access network.

At the same time, along with the development of the wireless technologies, the requirement of the mobility also becomes increasing. However, at the design stage today's Internet did not consider supporting the mobility, and the dual semantics of IP address makes itself changed and results in the interruption of the transport layer connections when the terminal is moving in different access networks. Therefore, future Internet architecture has regarded the mobility as its chief contents. Researches indicate that our ID/locator separation architecture provides better mobility for the terminals [8]. Although our ID/locator separation architecture has resolved the mobility problem, the following thing is how to guarantee the identity authenticity of the mobile terminals in the handoff process. In today's Internet, some protocol standards have been developed to protect the mobile terminals and access networks, such as AAA protocol [12] and 802.1X [13], but they increase the handoff delay and can not do well in our ID/locator separation architecture. For the above reasons, this paper proposes the authentication mechanism AuMID which can make the terminals achieve the secure handoff authentication by the use of Identity Tag.

As stated above, this paper proposes a new authentication mechanism called AuMID under our ID/locator separation architecture, and it uniquely introduces the Identity Tag to implement the sustainable authentication and handoff authentication when the terminal is associating with access networks. Besides, AuMID uses the challenge-response approach and achieves the double-way authentication between the terminals and access network, and successfully guarantees the authenticity of the source under our ID/locator separation architecture. At the same time, this paper also gives the deployment of authentication centers which are responsible for the access authentication and handoff authentication.

The remainder of this paper is organized as follows. In Section II we simply introduce our ID/locator separation architecture. In Section III we present each part of AuMID in detail, and give the basic access and handoff authentication processes. And in Section IV we provide a qualitative analysis for the scalability and security of this mechanism and an analysis of handoff delay. Finally, we conclude.

II. ID/LOCATOR SEPARATION ARCHITECTURE

In order to resolve the dual semantics of IP address, our ID/locator separation architecture mainly includes two parts [14]: Access Network and Core Network. As shown in Fig. 1. Access network takes charge of the access and authentication behaviors of various terminals (e.g. fixed terminals, mobile terminals, sensors, etc.), the terminals in access networks are the sources or destinations of the data packets. On the other hand, core network takes charge of the data packets' routing and forwarding, and it also can be composed of different autonomous systems (ASes). Corresponding to the network topology, our ID/locator separation architecture synchronously introduces two identifiers to implement the ID/locator separation: Access IDentifier (AID) and Routing IDentifier (RID). The main definitions are the following:

AID (Access IDentifier): it is only used in access network, and represents the terminal's public identity information. A terminal can own one or more AIDs, and AID is consistent regardless of terminal moving in different access networks.

RID (Routing IDentifier): it is only used in core network, and represents the terminal's location information. As the identifier of network layer, RIDs must be the same format for the packets' routing and forwarding.

ASR (Access Switch Router): it is located between access network and core network, and provides the access services of various terminals. ASR also completes the functions of mapping between AID and RID, and achieves the packets' forwarding from access network to core network.

GSR (General Switch Router): it is only located in core network. Moreover it uses RID to route and forward the data packets in core network.

AC (Authentication Center): it is located in core network, and it provides the access authentication and authorization for the terminals.

IDMS (IDentifier Mapping Server): it is located in core network, and provides the lookup and mapping service between AID and RID. At the same time, in our design one AS can own several IDMSes, or one IDMS can belong to several different ASes.

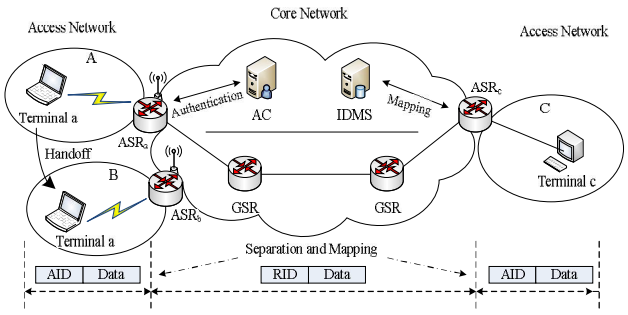

Figure 1. Structure of our ID/locator separation architecture.

The completed communication procedure is the following:

When one terminal wants to associate with an access network, it first achieves the access authentication from AC. And then the ASR registers the terminal's mapping relation AID-to-RID to IDMS. When the terminal initiates a communication, it sends the packets whose source and destination fields are its and the receiver's AIDs. Moreover when the ASR receives the packets, it first query the receiver's mapping relation AID-to-RID from IDMS, and then it uses the sender's and receiver's RID to substitute the source and destination fields of the packets. Through routing and forwarding with the guidance of the destination RID in core network, the packets could be transmitted to the destination access

network. After the source and destination fields are substituted with the origin sender's and the receiver's AID by the receiver's ASR, the packets would eventually arrive at the receiver. In any access network AID remains the same during the whole communication, and RID is kept secret from the terminals at all times.

When a terminal moves from one access network to another access network, it first registers the new mapping relation AID-to-RID to IDMS by the new ASR. After that, the terminal can continue the communication whose detail process has been described in previous section. It is to be noted that in the whole handoff process AID remains unchanged all the time.

III. Authentication Mechanism AuMID

The authentication mechanism AuMID is carried out by ACs under our ID/locator separation architecture. It mainly includes three parts: the process of access authentication, the process of sustainable authentication and the process of handoff authentication. In the process of access authentication, AC is responsible to issue the Identity Tag to the user who wants to associate with access network. In the process of sustainable authentication, AC uses the Identity Tag to implement the sustainable authentication for the user. And in the process of handoff authentication, terminals achieve the secure handoff authentication by the use of Identity Tag. Table I shows the main symbol's definitions.

TABLE I.
MAIN SYMBOL'S DEFINITIONS

RAND	Pseudo-random number
CV	Challenge vector
$Cert_a$	Digital certificate of terminal
$Cert_c$	Digital certificate of AC
CertReq	Request payload of digital certificate
$sig_a()$	Digital signature of terminal
$sig_c()$	Digital signature of AC
Pu_a	Public key of terminal
Pu_c	Public key of AC
E(Pu,X)	Encrypt data X with Pu
Id-Tag	Identity Tag
IdReq	Request payload of Identity Tag

A. Process of Access Authentication

Fig. 2 describes the process of access authentication. The main idea includes the double-way authentication between the terminal and AC and the issue of the Identity Tag. The specific interaction procedures are the following.

Step 1: When the terminal starts to associate with access network, and sends a request authentication message *A* to ASR for the access authentication.

Step 2: After ASR receives message *A*, it will issue a puzzle challenge to the terminal. It first generates a pseudo-random number *RAND* automatically, and computes the challenge vector *CV* by using equation (1). The message *B* mainly includes the pseudo-random number *RAND* and the challenge vector *CV*.

$$CV = prf(AID \mid RAND). \quad (1)$$

Here, $prf()$ is a one-way hash function, and AID is the terminal's access identifier. We propose to use prime factorization of *CV* as a puzzle, which is hard to compute but extremely easy to verify [15]. This is important to reduce ASR's load and implicitly prevent Denial of Service (DoS) attacks against ASR using this method. If the terminal wants to access the network, it must solve the challenge puzzle. Otherwise ASR will not forward the terminal's authentication request. At the same time, the pseudo-random number *RAND* can prevent pre-calculation.

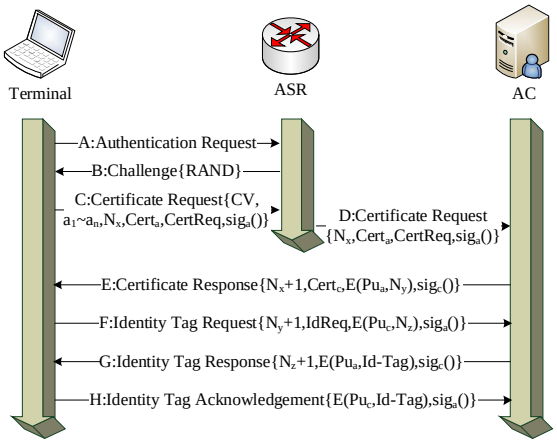

Figure 2. Access authentication process.

Step 3: When the terminal receives the challenge, if it is willing to respond, it will calculate the prime factorization of *CV* as depicted in equation (2). Here, a_i is each prime of *CV*. After that, the terminal constitutes and sends the certificate request message *C*, including *CV*, $a_1 \sim a_n$, the pseudo-random number N_x generated automatically by itself, its own digital certificate $Cert_a$, and the request payload *CertReq* for the digital certificate of AC. $sig_a\{N_x|Cert_a\}$ is the digital signature for the fields of N_x and $Cert_a$.

$$CV = \prod_{i=1}^{n} a_i \quad (2)$$

Step 4: After ASR receives message *C*, it first check the validity of the prime factorization, if incorrect, then refuse the terminal to access the network; and if consistent, then gets rid *CV* and $a_1 \sim a_n$ from message *C* and forwards message *D* to AC. When AC receives message *D*, it first checks the validity of $sig_a\{N_x|Cert_a\}$ with the public key Pu_a in $Cert_a$, if inconsistent, then refuse the terminal to access the network; and if consistent, then constitutes the certificate response message *E* to provide AC's digital certificate. Message *E* mainly includes N_x+1, AC's digital certificate $Cert_c$, the encrypted information $E(Pu_a,N_y)$ which represents that AC uses the public key Pu_a to encrypt the pseudo-random number N_y generated by itself, and the digital signature $sig_c(N_x+1|Cert_c|E(Pu_a,N_y))$. $E(Pu_a,N_y)$ can confirm that $Cert_a$ indeed comes from the terminal, because only the terminal can decrypt $E(Pu_a,N_y)$ and get N_y.

Because ASR only forwards the messages which are exchanged between the terminal and AC, we ignore ASR in Fig. 2 and in the following steps.

Step 5: After message *E* arrives at the terminal, the terminal first checks the validity of $sig_c(N_x+1|Cert_c|E(Pu_a,N_y))$ with the public key Pu_c in $Cert_c$, if consistent, then store the digital certificate $Cert_c$ and decrypt $E(Pu_a,N_y)$ to get N_y. Whereafter the terminal constructs the request message *F* for the Identity Tag, mainly including N_y+1, the request payload *IdReq* for the Identity Tag, $E(Pu_c,N_z)$ in which N_z is the pseudo-random number generated by the terminal, and $sig_a(N_y+1|IdReq|E(Pu_c,N_z))$. $E(Pu_c,N_z)$ can confirm that $Cert_c$ indeed comes from AC.

Step 6: After AC receives message *F*, it first checks the validity of $sig_a(N_y+1|IdReq|E(Pu_c,N_z))$, and then checks N_y. AC can confirm that $Cert_a$ indeed comes from the terminal with N_y. If all of these are coincident, AC would construct message *G* to provide the Identity Tag for the terminal. Identity Tag is a 160-bit value, and it basically consists of three parts: AS number domain, AC identity domain and terminal identity domain. As shown in Fig. 3.

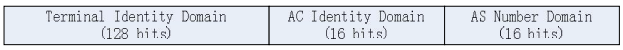

Figure 3. Structure of Identity Tag.

Here, AS number domain is a 16-bit value which is the same as the current AS number. And AC identity domain is a 16-bit hash value of each AC's digital certificate, and it represents each AC's identity information. In our design, AC can fast lookup the terminal's identity information by using AS number domain and AC identity domain when the terminal moves from one access network to another access network. Same as above, terminal identity domain *Id-Domain* is a 128-bit hash value of some parameters, consisting of $Cert_a$, AID_a, the current timestamp T_s and the pseudo-random number N_t. The formula of *Id-Domain* is the following:

$$Id\text{-}Domain = hash(Cert_a \mid AID_a \mid T_s \mid N_t) \quad (3)$$

Identity Tag represents the temporary identity information of the terminal, and its lifecycle is the period from accessing the network to leaving the network. The timestamp T_s and the pseudo-random number N_t can make identity Tag non-repeated. $E(Pu_a,Id\text{-}Tag)$ can ensure the privacy of *Id-Tag*. $sig_c(N_z+1|E(Pu_a,Id\text{-}Tag))$ in message *G* is the digital signature of AC.

Step 6: After message *G* arrives at the terminal, the terminal first checks the validity of $sig_c(N_z+1|E(Pu_a,Id\text{-}Tag))$, and then checks N_z. The terminal can confirm that $Cert_a$ indeed comes from AC with the pseudo-random number N_y. Finally, the terminal can decrypt $E(Pu_a,Id\text{-}Tag)$ with its private key and get *Id-Tag*. And then it constructs message *H* to respond that it has received the Identity Tag *Id-Tag*. $E(Pu_c,Id\text{-}Tag)$ can ensure the privacy of *Id-Tag*. And $sig_a(E(Pu_c,Id\text{-}Tag))$ in message *E* is the digital signature of the terminal.

When AC receives message *H*, it first checks the validity of message *H*, and then informs ASR that the terminal can access the network. Besides, AC also stores the identity Tag *Id-Tag* into its database.

B. Process of Sustainable Authentication

AC maintains an Identity Tag mapping table, as shown in Table II. The table mainly includes five parts: the terminal's Access IDentifier *AID*, the terminal's digital certificate $Cert_a$, the terminal's Identity Tag *ID-Tag*, the authentication timing cycle T_x and the revocation timing cycle T_y. The authentication timing cycle indicates the time interval after which AC sends a request message for the terminal's Identity Tag. In other words, whenever the authentication timing cycle drops to zero, AC sends a request message for the terminal's Identity Tag, and waits for the terminal's response. The revocation timing cycle indicates the time interval during which AC waits for the terminal's response. In other words, when the revocation timing cycle drops to zero, AC still has not received the terminal's response for the Identity Tag. Then AC must inform that ASR should disconnect the terminal from access network. This way guarantees the real-time authenticity of the sources, and avoids the Sybil attack to some extent.

TABLE II.
IDENTITY TAG MAPPING TABLE

Access IDentifier	*AID*
Digital certificate	$Cert_a$
Identity Tag	*ID-Tag*
Authentication timing cycle	T_x
Revocation timing cycle	T_y

Fig. 4 describes the process of sustainable authentication. AC uses the Identity Tag to implement the sustainable authentication after the access authentication. The specific interaction procedure is the following. Here we also ignore the forwarding of ASR.

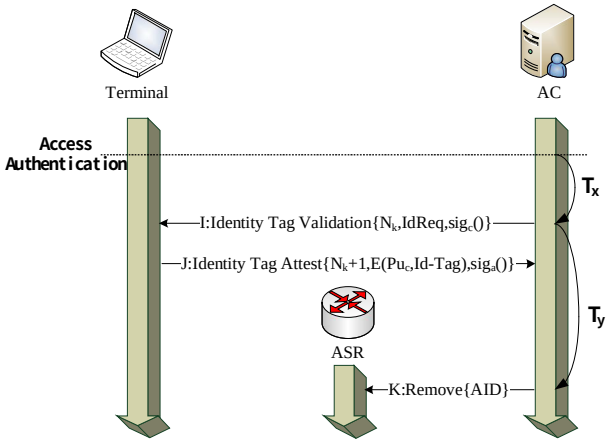

Figure 4. Sustainable authentication process.

Step 1: After AC receives message *H*, the authentication timing cycle begins to count down. And when the authentication timing cycle T_x drops to zero, AC sends the Identity Tag validation message *I* for the terminal's Identity Tag. Message *I* mainly includes the pseudo-random number N_k, the request payload *IdReq* for the Identity Tag and the digital certificate $sig_c(N_k|IdReq)$. At the same time, the revocation timing cycle T_y begins to

count down. When the revocation timing cycle drops to zero, AC still has not received the terminal's response for the Identity Tag. Then AC must constitute remove message *K* to inform that ASR should disconnect the terminal from access network, meanwhile, AC withdraws the Identity Tag mapping table of the terminal. Before the revocation timing cycle drops to zero, AC has received the terminal's response for the Identity Tag. The authentication timing cycle ought to be reset to T_x and begin to count down. Meanwhile, the revocation timing cycle ought to be reset to T_y as well.

Step 2: After the terminal receives message *I*, it first checks the validity of $sig_c(N_k|IdReq)$, if consistent, then constitutes attest message *J* to inform its Identity Tag, mainly including the pseudo-random number N_k+1, the encrypted information $E(Pu_c,Id\text{-}Tag)$ and the digital certificate $sig_a(N_k+1|\ E(Pu_c,Id\text{-}Sig))$. $E(Pu_c,Id\text{-}Tag)$ can ensure the privacy of *Id-Tag*.

After AC receives message *J*, it first checks the validity of $sig_a(N_k+1|\ E(Pu_c,Id\text{-}Sig))$ and decrypts $E(Pu_c,Id\text{-}Tag)$ with its private key and gets *Id-Tag*. And then AC compares the *Id-Tag* with the one in the Identity Tag mapping table, if consistent, AC can validate that the terminal remains active in the access network and the terminal's identity is authentic. After that, AC resets the authentication timing cycle to T_x and begins to count down; if inconsistent, AC must constitute remove message *K* to inform that ASR should disconnect the terminal from access network, meanwhile, AC withdraws the Identity Tag mapping table of the terminal.

C. Process of Handoff Authentication

When the terminal moves from one access network called home access network to another access network called local access network, it also will accomplish the handoff authentication by the use of Identity Tag. As depicted in Fig. 5. The local AC inquires the terminal's Identity Tag mapping table from the home AC, and then uses these identity information to authenticate the terminal. After that, the local AC stores the Identity Tag mapping table into its database. In our design, in the whole core network each AC has the same digital certificate and the same public and private keys.

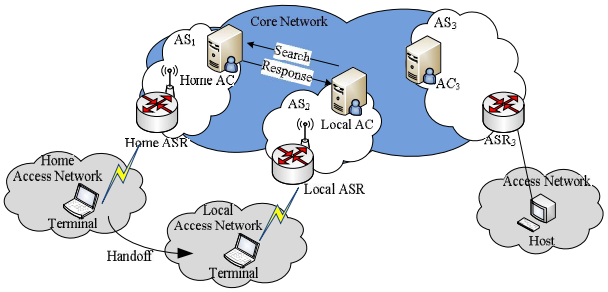

Figure 5. Mobile handoff of the terminal.

Fig. 6 describes the process of handoff authentication. This process only needs to exchange the information once by the use of the Identity Tag, and ensures the fast handoff authentication. The specific interaction procedure is the following. Here we also ignore the forwarding of the local ASR.

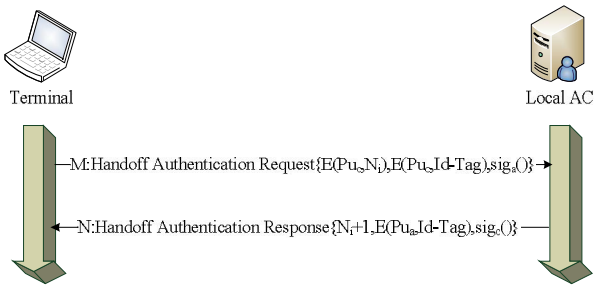

Figure 6. Handoff authentication process.

Step 1: When the terminal moves into another access network, it first sends message *M* to request the handoff authentication of the local AC who is responsible for the authentication of local access network. Message *M* includes $E(Pu_c,N_i)$, $E(Pu_c,Id\text{-}Tag)$ and $sig_a(E(Pu_a,N_i),E(Pu_c,Id\text{-}Tag))$. N_i is a pseudo-random number generated automatically by the terminal, and it can ensure message *M* to be fresh and unique. $E(Pu_c,Id\text{-}Tag)$ can ensure the privacy of *Id-Tag*, and $sig_a(E(Pu_a,N_i),E(Pu_c,Id\text{-}Tag))$ can ensure the authenticity of message *X*.

Step 2: After the local AC receives message *M*, it first decrypts $E(Pu_c,Id\text{-}Tag)$ with its private key and gets *Id-Tag*. And then the local AC utilizes *Id-Tag* to search the terminal's Identity Tag mapping table from home AC. When the local AC gets the *AID* and $Cert_a$, it first checks whether *AID* matches the one of the terminal, and then checks the validity of $sig_a(E(Pu_a,N_i),E(Pu_c,Id\text{-}Tag))$, if false, then refuses the terminal to access the network; and if right, then informs the local ASR that terminal *a* can access the network. Besides, it constitutes handoff authentication response message *M* to the terminal, including N_i+1, $E(Pu_a,Id\text{-}Tag)$ and $sig_c(N_i+1,E(Pu_a,Id\text{-}Tag))$.

When the terminal receives message *N*, it checks the validity of $sig_c(N_i+1,E(Pu_a,Id\text{-}Tag))$, and decrypts $E(Pu_a,Id\text{-}Tag)$ to get *Id-Tag*. Through the Identity Tag *Id-Tag* the terminal understands that it has been allowed to access the local access network and continues the communication.

D. Structure of ACs

All ACs in the core network compose a tree structure like DNS (Domain Name System) infrastructure. As described in Fig. 7. The root node of this tree is a Root Server who administrates all the AS Servers on the branches, and the Root Server mainly takes charge of the search of Identity Tag mapping table in different ASes. Because the AS number domain is 16 bits, the largest number of AS Servers is 2^{16} which equals the AS's largest number of current Internet. In the same way, AS Server administrates all the ACs who belong to this AS, and it is responsible for the search of Identity Tag mapping table in the same AS. Furthermore, the leaf nodes of this tree are all ACs. In the form of Identity Tag, the AC identity domain is 16 bits, therefore one AS owns at most 2^{16} ACs. When the terminal moves from home

access network to local access network, the search algorithm of Identity Tag mapping table basically includes the following two principles:

(1) The situation that the two access networks are attributed to the same AS:

When the local AC finds that the AC identity domain of terminal's Identity Tag belongs to the same AS, it sends a request message to the local AS Server for the Identity Tag mapping table. After that, AS Server forwards this request message to the home AC. When the home AC receives this request message, it directly sends the terminal's Identity Tag mapping table to the local AC.

(2) The situation that the two access networks are attributed to different ASes:

When the local AC finds that the AS identity domain of terminal's Identity Tag is different from the local AS, it sends a request message to the local AS Server for the Identity Tag mapping table, and then the local AS Server forwards this request message to the Root Server. According to the AS identity domain of the terminal's Identity Tag, the Root Server forwards this request message to the corresponding home AS Server. When the home AC receives this request message from the home AS Server, it directly sends the terminal's Identity Tag mapping table to the local AC.

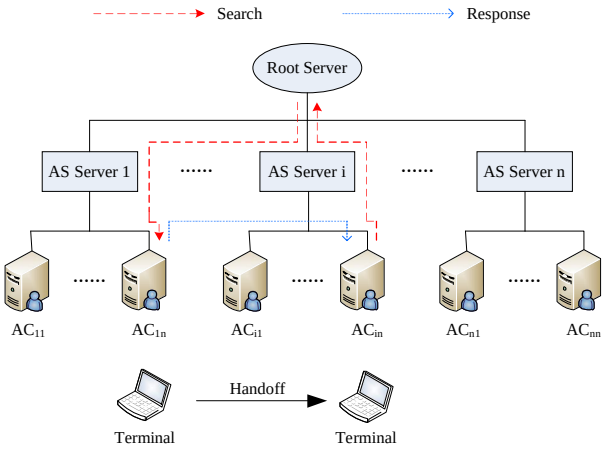

Figure 7. Structure of ACs.

IV. Evaluation of AuMID

A. Scalability

The main purpose of AuMID is to provide the authentication service for the whole ID/locator separation architecture. Therefore, any authentication service should have good scalability. Because the number of Identity Tag is 2^{160}, it is very large when compared with the number of persons on the earth, which is about $6.6*10^9$. Similarly, owing to the AC identity domain and the terminal identity domain, each AS can hold 2^{16} ACs and each AC can serve 2^{128} terminals. Indeed, these numbers are large enough for the users of future Internet. At the same time, an AC in one AS only needs to store the Identity Tag mapping tables of all the terminals in AC's access network. Take Beijing Jiaotong University (BJTU) campus network (with about 40,000 terminals) for instance. Suppose that each Identity Tag mapping table is about 744 bytes (16-byte AID, about 700-byte X.509 digital certificate [16], 20-byte Identity Tag, 4-byte Authentication timing cycle and 4-byte Revocation timing cycle), for all the terminals AC only employs about 29MB memory space to store these Identity Tag mapping tables. With current technology, it is feasible for ACs to do it. Therefore, AuMID can adapt for the large-scale network construction, and provides fine scalability.

B. Security

(1) Double-way authentication

AuMID achieves the double-way authentication by the use of terminal's digital certificate $Cert_a$ and AC's digital certificate $Cert_c$. And through the encrypted pseudo-random number N_y and N_z the receiver could determine the authenticity of the digital certificate. So this scheme guarantees the double-way authentication between the terminal and AC.

(2) Avoid DoS attack

AuMID proposes to use prime factorization as a puzzle, which is hard to compute but extremely easy to verify. This is important to reduce ASR's load and implicitly prevent Denial of Service (DoS) attacks against ASR using this method. If the terminal wants to access the network, it must solve the challenge puzzle. Therefore, when a terminal launches a DoS attack to AC, the terminal's resource will be exhausted.

(3) Avoid Sybil attack

Sybil attack is composed of two situations: one is that an attacker can forge the legitimate user's AID to achieve the authentication and authorization; and the other is that an attacker can impersonate the legitimate user to access the network in the mobile handoff process. For the first case the terminal's digital certificate $Cert_a$ determines the authenticity of user identity in the access process. And for the second case the non-repetitive 160-bit Identity Tag *Id-Tag* determines the authenticity of user identity in the mobile handoff process. Therefore, AuMID can avoid the Sybil attack.

(4) Avoid replay attack

AuMID avoids this attack by the use of the pseudo-random N_x, N_y, N_z, N_k.and N_i. The pseudo-random number is temporary interaction number, and it owns some randomness and unpredictability. Therefore it can make the interaction messages between the terminals and ACs fresh.

C. Handoff Authentication Delay

From what is said above, we can draw that under our ID/locator separation architecture the handoff authentication delay mainly includes two parts: mobile handoff delay t_{MH} and the authentication delay t_{AU}. The equation of the handoff authentication delay t_{HA} is the following:

$$t_{HA} = t_{MH} + t_{AU} \quad (3)$$

Reference [8] has described that t_{MH} is about 25ms, so the handoff authentication delay can be expressed as:

$$t_{HA} \approx 25ms + t_{AU} \quad (4)$$

Let us analyze t_{AU} more detailed. When a terminal moves from one access network to another access network, AuMID basically includes two parts: the one is the information interaction process between the terminal and AC, and the other is the lookup process of Identity Tag mapping table. Therefore, the equation of t_{AU} is the following:

$$t_{AU} = t_{trans} + t_{lookup} \quad (5)$$

t_{trans} is the information interaction delay between the terminal and AC, and it can correspond to a RTT delay. t_{lookup} is the lookup delay of Identity Tag mapping table. For the information interaction delay t_{trans}, we conduct an experiment to measure the RTT delay between a mobile terminal and an access point (AP) whose maximal transmission rate is 108Mbps, and we find that the average RTT delay is about 5ms. Similarly, because the structure of ACs feels like the DNS infrastructure, we believe that the lookup delay approximately equals to Query Response Time (QRT) of DNS. From Reference [17] we can see that the worst mean QRT is less than 350ms. Thus we can come to the conclusion that t_{lookup} is less than 350ms. As stated above the handoff authentication delay is the following:

$$t_{HA} \le 25ms + 5ms + 350ms = 375ms \quad (6)$$

According to the handoff delay ranged from 150 to 400ms of the common real-time applications [18], the handoff authentication delay t_{HA} in our ID/locator separation architecture meets the needs of these real-time applications.

V. Conclusions and Futrure Work

This paper proposes a new authentication mechanism called AuMID under ID/locator separation architecture, and describe the detailed procedures of access authentication and handoff authentication, and simultaneously give the deployment of authentication centers. Furthermore, it uniquely introduces the Identity Tag to implement the sustainable authentication and handoff authentication when the terminal is associating with access network. AuMID uses the challenge-response approach and achieves the double-way authentication between the terminal and access network, and successfully guarantees the authenticity of the sources under our ID/locator separation architecture. At last, we give some ordinary analyses of AuMID, including the scalability, the security and the handoff authentication delay. In the future work we will further analyze this mechanism, and gives the relation between the authentication timing cycle T_x and the revocation timing cycle T_y. At the same time, we also will further simulate and analyze the handoff authentication delay.

Acknowledgment

This work is supported in part by the National Basic Research Program of China (973 Program) (No. 2007CB307101 and 2007CB307106), in part by the Program of Introducing Talents of Discipline to Universities ("111 Project") (No. B08002), in part by the Fundamental Research Funds for the Central Universities (Grant NO. 2011JBM016) and in part by Beijing Natural Science Foundation (Grant NO. 4091003). The authors should thank the other cooperators in this project for their contributions in this paper. And the authors are very grateful to the anonymous referees for their insightful comments and suggestions.

References

[1] D. Meyer, L. Zhang, and K. Fall, "Report from the IAB workshop on routing and addressing," *IETF Internet Standard, RFC4984*, September 2007.
[2] GENI: Global Environment for Network Innovations, http://www.geni.net.
[3] FIND: Future Interact Network Design, http://find.isi.edu.
[4] B. Zhang, V. Kambhampati, D. Massey, et al. "A secure and scalable Internet routing architecture (SIRA)," ACM SIGCOMM 2006, Pisa, Italy, September, 2006.
[5] R. Moskowitz, P. Nikander, P. Jokela, T. Henderson, "Host identity protocol (HIP)," *IETF Internet Standard, RFC 5201*, April, 2008.
[6] D. Farinacci, V. Fuller, D. Oran, et al. "Locator/ID separation protocol," *IETF Internet Draft, draft-farinacci-lisp-09.txt*, October 2010.
[7] P. Dong, Y. Qin, and H. Zhang, "Research on universal network supporting pervasive services," *Acta Electronica Sinica*, vol 35, China, 2007, pp. 599-606.
[8] P. Dong, D. Yang, Y. Qin and Hongke Zhang, "Research on the Mobility Management Scheme in Future Internet," *Acta Electronica Sinica*, vol 36, China, 2008, pp. 1916-1922.
[9] Y. Lin, M. Chang, M. Hsua and L. Wul, "One-pass GPRS and IMS authentication procedure for UMTS," *IEEE Journal on Selection Areas in Communications*, vol 23, 2005, pp. 1233-1239.
[10] A. AL Shidhani and V.C.M. Leung, "Local fast re-authentication protocol for 3G-WLAN interworking architecture," *Wireless Telecommunications Symposium, WTS 2007*, California, 2007, pp. 1-8.
[11] Byeong-Thaek Oh, Sang-Bong Lee and Ho-Jin Park, "A Peer Mutual Authentication Method using PKI on Super Peer based Peer-to-Peer Systems," *10th International Conference on Advanced Communication Technology, ICACT 2008*, Gangwon-Do, 2008, pp. 2221-2225.
[12] C. Metz, "AAA protocols: authentication, authorization and accounting for the internet," *IEEE Internet Computing*, vol 3, 1999.
[13] IEEE 802.1 Working Group, "Standard for port-based network access control," *IEEE Draft P802.1x*, New York, 2001.
[14] H. Zhang and W. Su. Fundamental Research on the Architecture of New Network—Universal Network and

[15] Pervasive Services. *Acta Electronica Sinica*, vol 35, China, 2007, pp. 593-598.
[16] F. Tegeler and X. Fu, "SybilConf: computational puzzles for confining sybil attacks," *IEEE Conference on Computer Communications Workshops, 2010 INFOCOM*, San Diego, USA, 2010, pp.1-2.
[17] R. Housley, W. Ford, W. Polk and D. Solo, "Internet X.509 public key infrastructure certificate and CRL profile," *IETF Internet Standard, RFC2459*, January 1999.
[18] B. Lee, Y. Tan, Y. Sekiya, Y Sekiya, A. Narishige and S. Date, "Availability and effectiveness of root DNS servers: a long term study," *2010 IEEE Network Operations and Management Symposium (NOMS)*, Osaka, Japan, 2010, pp.862-865.
[19] P. Lam, S. Liew and J. Lee, "Cellular universal IP: a low delay mobility scheme based on universal IP addressing," *MSWiM'05*, Montreal, October 2005, pp.323-332.

Ming Wan received the BS degree in information and communication engineering from Beijing Jiaotong University (formerly known as Northern Jiaotong University) in July 2007. From September 2007 to now, he is a PhD candidate in National Engineering Laboratory for Next Generation Internet Interconnection Devices of Beijing Jiaotong University. He has published 4 research papers in the areas of identity authentication and network monitoring. His research interests include the areas of architecture of future Internet, network and information security.

Email: ming305.bjtu@gmail.com

Ying Liu received the B.S. and M.S. degrees from Beijing Jiaotong University in 2000 and 2003, respectively. She is currently working toward the PhD degree in communication and information systems at Beijing Jiaotong University, where she is a lecturer with the School of Electronic and Information Engineering. Her research interests include Internet routing, network monitoring and network security.

Email: yliu@bjtu.edu.cn

Hongke Zhang received the MS and PhD degrees in electrical and communication systems from the University of Electronic Science and Technology of China (formerly known as Chengdu Institute of Radio Engineering) in 1988 and 1992, respectively. From September 1992 to June 1994, he was a postdoc research associate at Beijing Jiaotong University (formerly known as Northern Jiaotong University). In July 1994, he joined Beijing Jiaotong University, where he is a professor. He has published more than 100 research papers in the areas of communications, computer networks, and information theory. He is the author of eight books written in Chinese and the holder of more than 30 patents. He received the Zan Tianyou Science and Technology Improvement Award in 2001, the Mao Yisheng Science and Technology Improvement Award in 2003, the first class Science and Technology Improvement Award of the Beijing government in 2005, and other various awards. He is now the chief scientist of a National Basic Research Program ("973" program).

Email: hkzhang@bjtu.edu.cn

