International Journal of Multimedia and Ubiquitous Engineering
Vol.11, No.11 (2016), pp.169-178
http://dx.doi.org/10.14257/ijmue.2016.11.11.14

Intra-domain Mapping Update Authentication Method in Identifier/ Locator Separation Network

Lijuan Zheng, Dan Liu and Chunhui Piao

School of Information Science and Technology Shijiazhuang Tiedao University
Shijiazhuang 050043, China
E-mail: zheng_lj@sina.com

Abstract

The Identifier/Locator Separation network is a new network architecture, and the mapping update theory in the model is an indispensable part in the process of communication. Besides, falsification attack, replay attack and network eavesdropping attack may be encountered in the process of mapping update. In order to resist these attacks, to ensure the secure transmission of update messages to the target node, this paper puts forward a intra-domain mapping update authentication method, this method can not only provide authentication services, but also can resist replay attack, DoS attack, and can ensure data confidentiality.

***Keywords**: Identifier/Locator Separation, Mapping Update Authentication, Binding Update Authentication*

1. Introduction

Traditional network is faced with various problems, and the fundamental reason of these problems is the dual attributes of IP address. Identifier/ Locator Separation Network [1-3,7,9-10] separates double semantics of IP address .Each terminal has two identifiers, one is locator identifier used for global routing, and the other is identity identifier used to identify terminal identity information. The identifier/locator separation network can effectively solve the routing scalability, mobility and security problems in traditional networks [8].

In the Identifier/Locator Separation Network when MN (Mobile Node) moves in the same administrative domain, nASR (new Access Switch Router) first authenticates its identity. nASR redistributes routing identifier RID (Routing IDentifier)for mobile node that has passed authentication, then this new routing identifier and mobile node's identity identifier are paired as a new identifier mapping relationship, which is deposited in the local user's mapping table. Later nASR will notify IMS (Internet Mapping Server) this new identifier mapping relationship. At the same time the new identifier mapping relationship is noticed to oASR (old Access Switch Router) by IMS, oASR sets switching routing identifier as temporary forwarding identifier, and the data sent to the mobile node is sent to nASR. Then the data is forwarded to the mobile node.

In this process, nASR notices new identifier mapping relationship of the mobile node to IMS, then IMS sends a notification of the new identifier mapping relationship to oASR. This step is the key to the whole process. The notification of this mapping relationship is the mapping update. The mapping update authentication is directly related to the security of communication when the node moves. If security measures are not adopted, in the process of mapping update it may face replay attack, man-in-the-middle attack and other various threats.

Secure binding update mechanism in traditional network such as binding update authentication method based on trust chain is based on assumption that mobile node and its correspondence node have a secure link [4]. When there are more than one communication, it is difficult that each pair of communication is equipped with a secure link. Secure routing optimization based on identity signature [5], which solves the triangle routing in MIPv6, but this method can not resist the DoS attack.Bake/2 binding update process [6], return routability test mechanism can not effectively resist eavesdropping and man-in-the-middle attack. CAM-DH authentication mechanism cannot resist man-in-the-middle attack [6]. It is thus clear, the scheme has some security flaws.

According to the characteristics of intra-domain mapping update process in Identifier/ Locator Separation Network, this paper puts forward a new intra-domain mapping update authentication method. Compared with traditional mapping update authentication method, this method can effectively resist replay attack, man-in-the-middle attack, impersonation attack, can ensure the confidentiality of the mapping update message.

2. Intra-domain Mapping Update Authentication Model

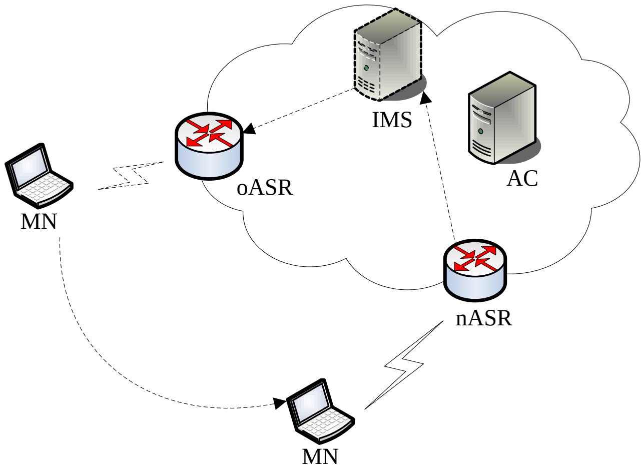

Figure 1.Intra-domain Mapping Update Authentication Model

Intra-domain mapping update authentication model is shown as Figure 1.

In this model, MN is the mobile node, IMS is used to store the mapping relationship in this domain. AC (Authentication Center) is responsible for verifying the identity of the ASR (Access Switch Router) and IMS, and issues public key certificate to ASR and IMS. In the local domain, the MN accesses the network through ASR.

If mobile node MN moves from oASR to nASR, and a new mapping relationship will be distributed to MN by nASR. In order to ensure the later communication of mobile node it needs mapping update. The nASR notifies IMS this new identifier mapping relationship, then IMS notifies it to oASR, as shown in dotted line in Figure 1.

3. Intra-domain Mapping Update Authentication Process in Identifier/ Locator Separation Network

3.1. Symbol Definition

Table 1. Symbolic Representation

Symbol	Meaning
ID_{MN}	identifier of MN
RID_{MN}	routing identifier of MN
A->B: X	X is the message that A sends to B
PK_A/SK_A	the public/private key pair, where $PK_A = g^{SK_A}$
$K_{A,B}$	key shared between A and B
$[X]_K$	represents the cipher text gotten from message X which is encrypted by secret key K using the symmetric encryption algorithm
$\{X\}_{SK_A}$	represents the signing message gotten from message X which is signed by A's private key SK_A using digital signature algorithm
g^n	the nth power of g, g is generator of G which is a finite multiplicative group
$Cert_A$	public key certificate of A
T_A	timestamp generated by A
h	hash function
h(X)	hash value of X using the hash function h

3.2. The Registration Process

First of all the IMS, oASR and nASR registers, then AC verifies the credibility of their identity. After verification, AC generates public key certificates CertIMS, CertoASR, CertnASR corresponding to IMS, oASR and nASR.

3.3. Intra-domain Mapping Update Authentication Process

Intra-domain mapping update authentication process is shown as Figure 2.

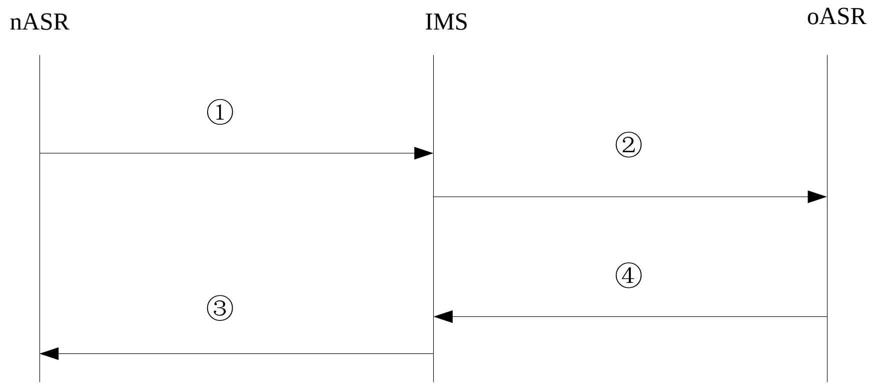

Figure 2. Intra-domain Mapping Update Authentication Process

Among them:

①$nASR \rightarrow IMS$:$[(ID_{MN},RID_{MN}),[ID_{MN} \oplus RID_{MN} \oplus g^{R_{N1}}]^{K_{nASR,oASR}},h(g^{R_{N1}}),g^{R_N}]^{K_{nASR,IMS}}$, $h(g^{R_N})$,$Cert_{nASR}$,T_{nASR},$\{h(g^{R_N})\}^{SK_{nASR}}$;

②$IMS \rightarrow oASR$:$[(ID_{MN},RID_{MN}),[ID_{MN} \oplus RID_{MN} \oplus g^{R_{N1}}]^{K_{nASR,oASR}},h(g^{R_{N1}}),g^{R_I}$, $Cert_{nASR}]^{K_{IMS,oASR}},h(g^{R_I})$,$Cert_{IMS}$,$T_{IMS}$,$\{h(g^{R_I})\}^{SK_{IMS}}$;

③$oASR \rightarrow IMS$: $[[g^{R_{N1}},ID_{MN},g^{R_{O2}}]^{K_{oASR,nASR}},h(g^{R_{O2}}),g^{R_{O1}}]^{K_{oASR,IMS}},h(g^{R_{O1}})$,$Cert_{oASR}$, T_{oASR},$\{h(g^{R_{O1}})\}^{SK_{oASR}}$;

④$IMS \rightarrow nASR$: $[[g^{R_{N1}},ID_{MN},g^{R_{O2}}]^{K_{oASR,nASR}},h(g^{R_{O2}}),g^{R_{I1}},Cert_{oASR}]^{K_{IMS,nASR}},h(g^{R_{I1}})$, $Cert_{IMS}$,T'_{IMS},$\{h(g^{R_{I1}})\}^{SK_{IMS}}$.

Details of the steps are as follows:

(1) nASR distributes RID_{MN} to MN after receipt of an access request from MN, but this time the mapping relationship (ID_{MN},RID_{MN}) has not been marked as valid, mapping relationship will be marked as valid only after MN is confirmed as a legitimate node, then the mapping relationship is notified to IMS and oASR.

nASR generates random numbers R_{N1} and R_N, calculates $g^{R_{N1}}$,g^{R_N} as well as the hash value $h(g^{R_{N1}})$,$h(g^{R_N})$.Besides, $K_{nASR,oASR}$ is the shared key between nASR and oASR, $K_{nASR,oASR} = g^{(SK_{nASR}*SK_{oASR})}$.$K_{nASR,IMS}$ is the shared key between IMS and nASR, $K_{nASR,IMS} = g^{(SK_{nASR}*SK_{IMS})}$.At the same time, attaching certificate of nASR $Cert_{nASR}$ and to let the IMS can obtain the public key of nASR, T_{nASR} is the timestamp generated by nASR. Meanwhile, $\{h(g^{R_N})\}_{SK_{nASR}}$ is the signature of nASR. Then nASR sends the message including $[(ID_{MN},RID_{MN}),[ID_{MN} \oplus RID_{MN} \oplus g^{R_{N1}}]^{K_{nASR,oASR}},h(g^{R_{N1}}),g^{R_N}]^{K_{nASR,IMS}},h(g^{R_N})$,$Cert_{nASR}$, T_{nASR},$\{h(g^{R_N})\}^{SK_{nASR}}$ to IMS.

(2)After receiving messages from nASR, IMS firstly verifies the legitimacy of the certificate belonging to nASR, secondly checks out whether error between the timestamp T_{nASR} and current system time is within a reasonable range. Then acquires the public key of nASR $PK_{nASR} = g^{SK_{nASR}}$ from $Cert_{nASR}$, meanwhile calculates the shared key $K_{nASR,IMS} = g^{(SK_{nASR}*SK_{IMS})}$ between nASR and IMS to decrypt: $[(ID_{MN},RID_{MN})$,

$[ID_{MN} \oplus RID_{MN} \oplus$ $g^{R_{N1}}]_{K_{nASR,oASR}}$, h($g^{R_{N1}}$), g^{R_N}] $^{K_{nASR,IMS}}$,and then gets hash value of g^{R_N} got from decryption, checks out whether the value equals with the value h(g^{R_N}) from message ①.Only validation and comparison above has passed, it is convinced that message ① is issued by nASR and not be tampered. Otherwise, it shows that the message is tampered and the authentication process ends.

IMS stores mapping update relationship (ID_{MN}, RID_{MN}) into mapping relationship table, but this time the mapping relationship cannot be marked as valid. Then IMS generates a random number R_I, calculates g^{R_I} and its hash value h(g^{R_I}),encrypts (ID_{MN},RID_{MN}) , $[ID_{MN} \oplus RID_{MN} \oplus g^{R_{N1}}]_{K_{nASR,oASR}}$,h($g^{R_{N1}}$), g^{R_I} with the key $K_{IMS,oASR} = g^{(SK_{IMS} * SK_{oASR})}$ which is shared between IMS and oASR, attaches the certificate $Cert_{IMS}$ of IMS and timestamp T_{IMS} so that the oASR can get public key $PK_{IMS} = g^{SK_{IMS}}$ of IMS. The random R_I and timestamp T_{IMS} can be used to prevent replay attacks, and {h(g^{R_I})} $^{SK_{IMS}}$ can be used as the signature of IMS. Finally, IMS sends the above message to oASR.

(3) After receiving messages from IMS, oASR firstly verifies the legitimacy of certificate $Cert_{IMS}$, secondly checks out whether the error between the timestamp T_{IMS} and current system time is within a reasonable range. Thirdly oASR acquires the public key $PK_{IMS} = g^{SK_{IMS}}$ and identity information of IMS from certificate $Cert_{IMS}$ which belongs to IMS, meanwhile calculates the shared key $K_{IMS,oASR} = g^{(SK_{IMS} * SK_{oASR})}$ between oASR and IMS, then use $K_{IMS,oASR}$ to decrypt message ② to get (ID_{MN},RID_{MN}), $[ID_{MN} \oplus RID_{MN}$ $\oplus g^{R_{N1}}]_{K_{nASR,oASR}}$,h($g^{R_{N1}}$), g^{R_I} ,$Cert_{nASR}$. And then calculates hash value of g^{R_I}, checks out whether the value equals with h(g^{R_I}) from message ②.If the comparison results are inconsistent, then the message is tampered, the authentication process ends. Only validation and comparison above has passed, it is convinced that message ②is issued by IMS and not be tampered.

After that oASR verifies the nASR's certificate $Cert_{nASR}$. If passed, public key of nASR $PK_{nASR} = g^{SK_{nASR}}$ is available from the certificate, then oASR calculates the shared key $K_{nASR,oASR} = g^{(SK_{nASR} * SK_{oASR})}$ and decrypts to get $ID_{MN} \oplus RID_{MN} \oplus g^{R_{N1}}$. Finally, the $g^{R_{N1}}$ is got from $ID_{MN} \oplus RID_{MN} \oplus g^{R_{N1}}$ according to the mapping relationship (ID_{MN},RID_{MN}) of message ②, and then calculates its hash value, checks out whether the value equals with the value h($g^{R_{N1}}$) . If comparison result is consistent, it can be assured the message has not been tampered. After decryption, oASR acquires MN's identity identifier ID_{MN}, and inquires mapping relationship about ID_{MN} in its own mapping table, If exists, then it is confirmed that the ID_{MN} is legitimate.

The mapping relationship of MN is updated to (ID_{MN}, RID_{MN}) by oASR, at the same time the mapping relationship is set as temporary forwarding identifier. oASR generates two random numbers R_{O1} and R_{O2} ,calculates $g^{R_{O1}}$,$g^{R_{O2}}$,h($g^{R_{O1}}$)as well as h($g^{R_{O2}}$),then calculates the shared key $K_{oASR,nASR} = g^{(R_{N1} * SK_{oASR})}$ and $K_{oASR,IMS} = g^{(R_I * SK_{oASR})}$. Using key $K_{oASR,nASR}$ to encrypt messages $g^{R_{N1}}$,ID_{MN}, $g^{R_{O2}}$,and then using key $K_{oASR,IMS}$ to encrypt [$g^{R_{N1}}$,ID_{MN}, $g^{R_{O2}}$] $^{K_{oASR,nASR}}$,h($g^{R_{O2}}$) and $g^{R_{O1}}$ .Finally, oASR sends the above messages attaching h($g^{R_{O1}}$),Cert$_{oASR}$,T$_{oASR}$ and {h($g^{R_{O1}}$)}$^{SK_{oASR}}$ together to IMS, in which Cert$_{oASR}$ is certificate of oASR, so that IMS can verify the identity of oASR and acquire public key $PK_{oASR} = g^{SK_{oASR}}$. T$_{oASR}$ is timestamp generated by oASR. {h($g^{R_{O1}}$)}$^{SK_{oASR}}$ can be used as signature of oASR.

(4)After receiving messages from oASR, IMS firstly verifies the legitimacy of certificate Cert$_{oASR}$ of oASR, secondly checks out whether the error between the timestamp and current system time is within a reasonable range.

Then IMS acquires the public key $PK_{oASR} = g^{SK_{oASR}}$ and identity information of oASR from certificate of oASR, combines with the random numbers RI produced by IMS to generate the shared key $K_{oASR,IMS} = g^{(R_I*SK_{oASR})}$,then uses $K_{oASR,IMS}$ to decrypt the received message and get [$g^{R_{N1}}$, ID$_{MN}$, $g^{R_{O2}}$]$^{K_{oASR,nASR}}$, h($g^{R_{O2}}$), $g^{R_{O1}}$. Next, IMS computes hash value $g^{R_{O1}}$ to get h($g^{R_{O1}}$) and checks out whether the value equals with the value of h($g^{R_{O1}}$) from the message.

Only validation and comparison above have been passed, it is convinced that the message was issued by oASR and not be tampered, and IMS marks the mapping relationship (ID$_{MN}$， RID$_{MN}$) as valid.

Then IMS combines the private key SK$_{IMS}$ and the shared key $K_{IMS,nASR} = g^{(R_N*SK_{IMS})}$, in which g^{R_N} is acquired from message ①, to generate random number R$_{I1.}$ Then IMS uses $K_{IMS,nASR}$ to encrypt these message, which includes random number R$_{I1,}$ [$g^{R_{N1}}$, ID$_{MN}$, $g^{R_{O2}}$]$^{K_{oASR,nASR}}$, h($g^{R_{O2}}$) from message ③, Cert$_{oASR}$ of oASR and $g^{R_{I1}}$. Together with certificate Cert$_{IMS}$ of IMS and new timestamp T'_{IMS}, the data is sent to nASR. What's more, {h($g^{R_{I1}}$)}$^{SK_{IMS}}$ is used as signature of IMS.

After receiving messages from IMS, nASR firstly verifies the legitimacy of certificate Cert$_{IMS}$, secondly checks out whether the error between the timestamp T'_{IMS} and current system time is within a reasonable range. Then nASR acquires the public key and identities information of IMS from certificate Cert$_{IMS}$, combines the random number R$_N$ to generate the shared key $K_{IMS,nASR} = g^{(R_N*SK_{IMS})}$, using $K_{IMS,nASR}$ to decrypt to get [$g^{R_{N1}}$,ID$_{MN}$, $g^{R_{O2}}$]$^{K_{oASR,nASR}}$, h($g^{R_{O2}}$), $g^{R_{I1}}$,Cert$_{oASR}$. After that, gets hash value from $g^{R_{I1}}$ decrypted, checks out whether the value equal that of h($g^{R_{I1}}$) in the ciphertext.

Next, nASR verifies the legitimacy of certificate Cert$_{oASR}$ of oASR. If passed, public key of oASR $PK_{oASR} = g^{SK_{oASR}}$ and identity of oASR is available from the certificate. Then, nASR calculates the shared key $K_{oASR,nASR} = g^{(R_{N1}*SK_{oASR})}$ between oASR and nASR to decrypt [$g^{R_{N1}}$,ID$_{MN}$, $g^{R_{O2}}$]$^{K_{oASR,nASR}}$ and then gets hash value from $g^{R_{O2}}$, checks out whether the value equals with h($g^{R_{O2}}$) of message ④. What's more, nASR checks out the value of $g^{R_{N1}}$ to see whether it equal with the value of $g^{R_{N1}}$ calculated by random number R$_{N1\,.}$ R$_{N1}$ is generated by nASR. If both validations are passed, it can be assured that the message has not been tampered and is sent by oASR through IMS. Finally, mapping relationship (ID$_{MN}$, RID$_{MN}$) is marked as valid according to ID$_{MN}$. At this point, the entire intra-domain mapping update authentication process completes.

4. Security Analysis

4.1. The Registration Process

(1) Data Confidentiality

In this method, all the contents are transferred in ciphertext or hash value except timestamp and public key certificate are transferred in plaintext. The attacker can not analyze message content transferred. In this way, the confidentiality of the data is ensured.

(2) Access Control

In the message ①and ②, all the shared keys are power of each side's public key. That is to say, only the message sender or recipient can decrypt the message, know the message content and get access permissions. In the message ③and ④, the shared key is gotten by calculating the public key from the sending end and random number from the receiving end. Therefore only the sending end and the receiving end can decrypt the message according to the key and get the content of the message. So, it can achieve the effect of access control.

(3) Non-repudiation

In every step of the method, the sender signs the hash value of the random number using its own private key. And only the sender can decrypt the signature, so the sender can not deny that the message is sent by itself. Besides, the contents of the message are encrypted using the shared key, only sender and receiver can get the contents of the message. Shared key in message ③and ④is got by calculating the random numbers from messages ①and ②. So if the receiver sends message ③and ④, it can be concluded that the receiver has got the message.

(4) Resist Replay Attack

If the attacker intercepts the message sent by sender, after a period of time the attacker sends the message to the sender again. This is replay attack aiming at receiver. In our method, in addition to random number contained in the encrypted message, it also transmits timestamp in plaintext. If the receiver has received the same timestamp or value related to the random number, throws away the later received message. So it can resist replay attack.

(5) Against Man-in-the-middle Attack

The shared keys in message ③and ④are calculated according to the random numbers and public key of nASR and IMS. If the middleman intercepts message ①or ②, sends its random number to the receiver and compounds secret key by its public key and the sender's random number at the same time. The receiver compounds the secret key using the random number of the middleman and then encrypts the reply message using this secret key. The middleman generates public keys using its random number, personates the public keys of sender and receiver and sends to them respectively. The middleman compounds the shared key by using the public key of the sender and receiver and uses this shared key to decrypt the messages transferred between the sender and receiver. Next, it encrypts the message sent by receiver by using the compound secret key and sends it to the sender. Therefore, the middleman can willfully get and modify the message's content of the two sides by using the two secret keys shared between the sender and the receiver respectively.

In order to prevent the above situation, when the sender sends random number, it is encrypted by the key compounded using public key of sender and receiver. In this way, the middleman can't get the private key of any side, and it can't get the random number of the sender then can't compound the secret key. Thus, this method can against the man-in-the-middle attack.

(6) Against Counterfeit Attack

In this method, the sender's certificate was sent in plaintext. If the attacker want to personate the sender, it can only get the sender's public key from the certificate, but the secret key of the encrypted message must be calculated by the sender’s private key or the receiver’s private key. If the receiver uses the secret key compounded by the public key from the certificate and its private key but can’t get correct encrypted message using this secret key, it shows that this message is counterfeit and would be abandoned.

(7) Against DoS(Denial of Service) Attack

An attacker may personate nASR and send the mapping update message of Mobile Node (MN) to IMS, it sets the new RID of this mapping update message as hit target C’s RID. If the mapping update process is successful, all the messages sent to MN will be directed to target C. If all the mapping update messages sent from attackers are successful, a lot of messages would be sent to target C. As a result, C can’t communicate normally. This kind of attack is called DoS attack.

In this method, the sender’s certificate is attached in every step, so when the receiver receives message, the first thing to do is to verify the certificate of it. If the result of this verification shows that the message is not sent by its sender who asserts it, this message is counterfeit and is discarded. Even if the attacker can get the certificate of nASR, it can’t get the private key SK_{nASR} of the nASR and can’t compound the shared private key of nASR and IMS or of the nASR and oASR which can be used to decrypt the message. Hence, attackers can’t conduct DoS attack in this method.

In the research of security domain of Mobile IPv6, there are many kinds of research related to security binding update mechanism. Table 2 would compare the security among binding update authentication method based on trust chain (BUATC), secure routing optimization based on identity signature (SROIS), CAM-DH authentication mechanism and mapping update authentication protocol put forwarded in this paper.

Table 2. Security Compared among Various Binding Update Authentication and Our Mapping Update Authentication

Protocol	Attack			
	Network Wiretapping	DoS Attack	Replay Attack	Man-in-the-middle Attack
BUATC[4]	+	*	–	–
SROIS[5]	+	–	+	+
CAM-DH[6]	+	+	+	–
Ours	+	+	+	+

Note: “+” represents that this protocol can resist this kind of attack; “-” represents that this kind of authentication mechanism can’t resist this kind of attack; “*” represents that it can’t completely resist this kind of attack, but it can prevent this attack to some extent.

4.2. Efficiency Analysis

Computations during the execution of the protocol are used to measure efficiency of the protocol. During the protocol analysis, computing the computational of all entities together, which mainly includes exponent operation, hash operation, elliptic curve operation, symmetric encryption/decryption operation, public key encryption/decryption operation, round number of message exchange. Performance analysis of this protocol is compared to binding update authentication based on chain of trust, the secure routing optimization based on identity signature and CAM-DH authentication mechanism.

Protocol efficiency analysis results are shown as Table 3.

Table 3. Efficiency Analysis of the Protocol

Performance Metric	ours	BUATC[4]	SROIS[5]	CAM-DH[6]
Hash Operations Times	8	1	0	8
Elliptic Curve Operations Times	0	1	0	0
Exponent Operation Times	4	0	0	3
Symmetric Encryption Times	3	4	0	4
Symmetric Decryption Times	5	4	0	0
Public Key Encryption Times	1	2	2	1
Public Key Decryption Times	1	1	2	1
Round Number of Message Exchange	2	3	4	2

Compared in terms of the round number of sending messages, message exchange rounds of our protocol is two. Message exchange rounds of authentication mechanism CAM-DH is two. Binding update authentication mechanism based on chain of trust needs to send three rounds to complete authentication, the secure routing optimization based on identity signatures needs four rounds to complete the certification.

This protocol applies to the identifier and locator separation network, providing high security, although calculation of the protocol have not much advantages compared with other methods. However, calculation is carried out mainly by access switch router and mapping servers, the computing requirements of the mobile node does not exist, so it is not a burden to the mobile node when the protocol processing. And the exponent operation of the protocol can be saved in advance by pre-computation, to improve the efficiency of the protocol.

5. Summary

This paper analyzes security threats during the process of intra-domain mapping process in identifier/locator separation network, and proposes a new intra-domain mapping update authentication. This method can ensure the confidentiality of the data, and can effectively resist replay attack, stealing attack, DoS attack and man-in-the-middle attack. The performance of this method is also good.

Acknowledgements

The work is supported by the Natural Science Foundation of Hebei Province (No. F2015210106), Hebei Educational Committee Foundation of Z995054, Doctoral Scientific Research Foundation of Shijiazhuang Tiedao University (No.Z991015137)

References

[1] D. Saucez, L. Iannone, O. Bonaventure and D. Farinacci, “Designing a Deployable Internet: The Locator/Identifier Separation Protocol”, IEEE Internet Computing, vol. 16, no. 6, **(2012)**, pp. 14-21.

[2] D. C. Phung, S. Secci, D. Saucez and L. Iannone, “The Openlisp Control Plane Architecture”, IEEE Network, vol. 28, no. 2, **(2014)**, pp. 34-40.

[3] P. M. Julia and A. F. Skarmeta, “Beyond the Separation of Identifier and Locator: Building an Identity-Based Overlay Network Architecture for the Future Internet”, Computer Networks, vol. 57, no. 10, **(2013)**, pp. 2280-2300.

[4] Y. Wei, R. Shi and H. Yong, “Trust chain based binding update authentication protocol in mobile IPv6”, Computer Applications and Software, vol. 25, no. 10, **(2008)**, pp. 265-267.

[5] Y. Hou, H. Qian and X. Wang, “ID-based Security Routing Optimization in Mobile IPv6”, Computer Engineering, vol. 35, no. 9, **(2009)**, pp. 127-129.

[6] A. Zhou, H. Gu, S. Li and S. Zhang, “Research on mechanisms of mobile IPv6 security binding update”, Computer Applications and Software, vol. 24, **(2007)**, pp. 9-11.

[7] H. Jie, “Research on key techniques of locator/identifier separation network”, [Ph.D. dissertation].

National University of Defense Technology, **(2011)**.

[8] L. Zheng, “Research and Design on Authentication Protocol in Identifier/Locator Separation Network”, [Ph.D. dissertation]. Beijing Jiaotong University, **(2014)**.

[9] R. J. Atkinson, “Identifier-Locator Network Protocol (ILNP) Architectural Description”, **(2012)**.

[10] D. Farinacci, V. Fuller, D. Meyer and D. Lewis, “The Locator/ID Separation Protocol (LISP)”, **(2013)**.

Authors

Lijuan Zheng, She received her master’s degree in computer application technology from North China Electronic Power University, Baoding, China, in 2003 and Ph.D. in information security from Beijing Jiao Tong University, Beijing, China, in 2014. Her research interests include security protocol analysis and design, trusted computing.

Dan Liu, She received her master’s degree in education technology from Shijiazhuang Tiedao University, in 2011. Currently, she is an lecturer at Shijiazhuang Tiedao University. Her interests is in software engineering.

Chunhui Piao, She received her master’s degree in computer science and technology from South West Jiaotong University, in 1988 and Ph.D. in computer application technology from RenMin University of China, Beijing, China, in 2011. Her interests include e-commerce privacy and e-commerce recommendation.