異質性廣域網路下連結認證及密匙分配協定
A General Approach of Interconnecting Authentication and Key Distribution Protocols for Heterogeneous WAN

林子喬
Tzu-Chiao Lin
台灣大學資訊工程系
Dept. of Computer Science and Info. Engineering
National Taiwan University, Taipei, Taiwan
tclin@cmlab.csie.ntu.edu.tw

黃肇雄
Jau-Hsiung Huang
台灣大學資訊工程系
Dept. of Computer Science and Info. Engineering
National Taiwan University, Taipei, Taiwan
jau@csie.ntu.edu.tw

摘要

本文提供了一個異質性廣域網路下連結不同認證及密匙分配協定的通解，且不影響到原有的安全平台環境.

ABSTRACT

In this paper, we propose a general solution of interconnecting various authentication and key distribution protocols over a heterogeneous WAN without affecting the original security platforms.

I. INTRODUCTION

In a wide area environment, many local area environments (which is also called *realms* or *domains*) may be interconnected via a backbone network. Each realm may adopt a security platform for its requirements. Therefore, there may be many different authentication and key distribution protocols [3, 5, 6, 7, 8, 9] in various realms. Each realm can use its required encryption algorithm, such as DES, RSA [10], or MAC (Message Authentication Code) encryption technique [11]. For this reason, a *heterogeneous WAN* can be defined as (1) each realm can adopt a different security protocol, and (2) each realm may use a different encryption algorithm. Otherwise, the environment is called *homogeneous*.

Therefore, an end-to-end inter-realm authentication and key distribution protocol is important for practical heterogeneous environment usage. Many researchers constructed protocols for inter-realm authentication and key distribution, such as Lu and Sundareshan's protocol [1, 2], Kerberos [3], Piessens, Decker and Janson's protocol [4]. Lu and Sundareshan's method used a hierarchical architecture to construct their end-to-end inter-realm protocol, so the same protocol should be adopted in all realms. Kerberos has the similar situation. In this situation, the original security platform which the realm adopts should be abandoned if inter-realm secure communication is required. Piessens, Decker and Janson's method connects two different existing protocols successfully, but it can be used only in connecting two adjacent realms.

This paper proposes a general solution of interconnecting various authentication and key distribution protocols over a heterogeneous WAN without affecting the original security platform. The control center of the long-haul network (LHCC) in [1, 2] is not needed in our protocol. The network topology is also unrestricted. The inter-realm protocol is easy to port and totally transparent to users.

This article is organized as follows : Section II gives a brief description of various inter-realm protocols. Section III illustrates the interconnection mechanisms of our design. Section IV demonstrates a example for inter-realm authentication and key distribution to show the generality of our design. Section V compares our designed protocol with several existing inter-realm protocols. Also, performance issues are discussed. Section VI gives a conclusion of this article.

II. PREVIOUS WORKS

A. Lu and Sundareshan's protocol [1, 2]

Lu and Sundareshan's protocol adopts the hierarchical architecture to perform authentication and key distribution. The control

center of the long-haul network, LHCC, is set up to maintain the inter-AS exchange keys of authentication servers in various realms.

After the completion of the above protocol, the requesting client and the requested server in different realms share a session key for secure communication. Note that both realms should adopt the same protocol, which involves LHCC, ASs, and the restricted flow steps, for accomplishing end-to-end secure communication. This protocol is classfied as one which is operated in homogeneous environments since the same protocol should be performed in various realms.

B. Kerberos [3]

In Kerberos version 4, each TGS (Ticket-Granting Server) stores secret keys with other TGSs, so the local TGS can provide the ticket for remote TGSs. This approach causes the problem of scalability. In contrast, Kerberos version 5 adopts a hierarchical concept, in which each TGS shares secret keys with TGSs in its parent and child realms. The multi-hop inter-realm authentication is then performed in version 5. The scalability problem is resolved, whereas additional message transmissions for requesting remote services occur. Note that Kerberos is also executed in homogeneous environments.

C. Piessens, Decker and Janson's protocol [4]

The object of Piessens, Decker and Janson's protocol is to interconnect existing different protocols of adjacent realms. A proxy mechanism is used in gateways to accomplish the object.

The major disadvantage of Piessens, Decker and Janson's protocol is that only interconnections of adjacent realms are considered. The protocol can not be applied across several realms or over a large WAN. The protocol suffers another problem of interconnecting various security platforms. It is difficult for both cryptosystems to share a session key, for example, a conventional-encryption cryptosystem such as DES can not agree a session key with a public-key cryptosystem such as RSA. Except this condition, problems can also happen when interconnecting both conventional-encryption cryptosystems or interconnecting both public-key cryptosystems. This problem is mentioned in [4].

III. Interconnecting Mechanisms

A. Proxy Mechanism

The proxy mechanism used in our protocol adopts the concept of Piessens, Decker and Janson's protocol, with some modifications. There are proxy processes, which play the roles of clients and servers, in gateways. But in contrast to their protocol, proxies for the requested servers are generated in the gateway which connects to the realm of the requesting client, whereas proxies for the requesting clients are generated in the gateway which connects to the realm of the requested servers. Besides proxies of clients and servers, gateway proxies are generated for each session period. These gateway proxies handle all inter-gateway transactions, including protocol translations, cryptography transformations, etc.

B. DH+MSR

The DH+MSR mechanism [12] in Fig. 1 is composed of the Diffie-Hellman key exchange technique [13] and the MSR (Mean Square Root) technique [14].

C. Stateful and Stateless Gateways

Gateways can be categorized into two types. One called *stateful gateways* can keep long-term and short-term information for communicating endpoints. The other called *stateless gateways* can keep short-term rather than long-term information. The definitions of short-term and long-term states in gateways in [4] are re-illustrated as follows :

- short-term state: state that has to be kept during the translation of one dialogue.
- long-term state : state that has to be kept between successive dialogues.

D. Virtual Link

If there are no inter-gateway keys between gateways, the system is insecure. If there are inter-gateway keys for every adjacent gateways, the system is insecure and inefficient since transformations should be performed in the intermediate gateways. If there are inter-gateway keys for every two gateways, the scalability problem occurs.

The most efficient way to solve the problem is to distribute inter-gateway keys dynamically when inter-realm communication

occurs. The key exchange occurs along with the request and the response messages. Then the encryption /decrytion operations are handled only at the source and destination gateways, whereas the intermediate gateways simply forward messages. We call this method the *virtual link* technique (Fig. 2) since it seems that there is a direct link between the source and the destination gateways.

The method used in this paper to implement the virtual link technique is the DH+MSR mechanism. The major advantage of the technique is that no inter-realm third party, such as LHCC in [1, 2], is required.

IV. EXAMPLE

The meaning of the notation in the examples came from [4], and are described as follows :

- The common notation of entities is represented as Q_{iX}^{n} or $Q_{iX}^{'n}$, which Q_{iX}^{n} is the real entity and $Q_{iX}^{'n}$ is the proxy process in a gateway.
- Q is an object of C (client), S (server), AS (authentication server), or GW (gateway).
- Q_{iX}^{n} means that it is the *i*-th entity in domain X, which uses authentication system *n*.

Fig. 3 illustrates the flows that a client C_{iX}^{1} requests services from a server S_{jY}^{2}. Assume realm X adopts the KSL protocol, whereas realm Y uses the NS protocol. The parenthesis {}, <> and () in the following description represent different cryptography such as DES.

1. $C_{iX}^{1} \rightarrow S_{jY}^{'1}$: N_c, C_{iX}^{1}
2. $S_{jY}^{'1} \rightarrow AS_X^{1}$: $N_c, C_{iX}^{1}, N_s, S_{jY}^{'1}$
3. $AS_X^{1} \rightarrow S_{jY}^{'1}$: $\{N_s, C_{iX}^{1}, K_{cs}\}_{Kgwx}, \{N_c, S_{jY}^{'1}, K_{cs}\}_{Kc}$
4. $S_{jY}^{'1} \rightarrow GW_X^{'1}$: $S_{jY}^{'1}$ passes the request to $GW_X^{'1}$
5. $GW_X^{1} \rightarrow GW_Y^{2}$: $N_{gwx}, GW_x, C_{iX}^{1}, S_{jY}^{2}, P_x, Cert_x$ where $P_x=\alpha^{Sx} \bmod N$, $Cert_x=\sqrt{h(GW_x, P_x)} \bmod N_u$
6. $GW_Y^{'2}$ checks if $Cert_x^{2}=h(GW_x,P_x) \bmod N_u$, if so, computes the inter-gateway key $EK_{xy}=(P_x)^{Sy} \bmod N$, $GW_Y^{'2} \rightarrow C_{iX}^{'2}$: $GW_Y^{'2}$ passes the request to $C_{iX}^{'2}$
7. $C_{iX}^{'2} \rightarrow S_{jY}^{2}$: $C_{iX}^{'2}, N_c$
8. $S_{jY}^{2} \rightarrow AS_Y^{2}$: $S_{jY}^{2}, (C_{iX}^{'2}, N_c, T_s)_{Ks}, N_s$
9. $AS_Y^{2} \rightarrow C_{iX}^{'2}$: $(S_{jY}^{2}, N_c, K_{c's}, T_s)_{Kgwy}, (C_{iX}^{'2}, K_{c's}, T_s)_{Ks}, N_s$
10. $C_{iX}^{'2} \rightarrow S_{jY}^{2}$: $(C_{iX}^{'2}, K_{c's}, T_s)_{Ks}, (N_s)_{Kc's}$
11. $C_{iX}^{'2} \rightarrow GW_Y^{'2}$: $C_{iX}^{'2}$ passes $K_{c's}$ and the ticket $(C_{iX}^{'2}, K_{c's}, T_s)_{Ks}$ to $GW_Y^{'2}$
12. $GW_Y^{'2} \rightarrow GW_X^{'1}$: $GW_x, <N_{gwx}>_{EKxy}, GW_y, N_{gwy}, P_y, Cert_y, (C_{iX}^{1}, S_{jY}^{2}, EK_{xy}, K_{c's}, (C_{iX}^{'2}, K_{c's}, T_s)_{Ks})_{Kyy}$

where $P_y=\alpha^{Sy} \bmod N$, $Cert_y=\sqrt{h(GW_y, P_y)} \bmod N_u$

13. $GW_X^{'1}$ Checks if $Cert_y^{2}=h(GW_y,P_y) \bmod N_u$, if so, computes the inter-gateway key $EK_{xy}=(P_y)^{Sx} \bmod N$ $GW_X^{'1} \rightarrow GW_Y^{'2}$: $GW_y, <N_{gwx}>_{EKxy}$
14. $GW_X^{'1} \rightarrow S_{jY}^{'1}$: $GW_X^{'1}$ passes the ticket $(C_{iX}^{1}, S_{jY}^{2}, EK_{xy}, K_{c's}, (C_{iX}^{'2}, K_{c's}, T_s)_{Ks})_{Kyy}$ to $S_{jY}^{'1}$
15. $S_{jY}^{'1} \rightarrow C_{iX}^{1}$: $\{N_c, S_{jY}^{'1}, K_{cs}\}_{Kc}$, $\{T_{gwx}, C_{iX}^{1}, K_{cs}, EK_{xy}, S_{jY}^{2}, (C_{iX}^{1}, S_{jY}^{2}, EK_{xy}, K_{c's}, (C_{iX}^{'2}, K_{c's}, T_s)_{Ks})_{Kyy}\}_{Kcs}, N_s, \{N_c\}_{Kcs}$
16. $C_{iX}^{1} \rightarrow S_{jY}^{'1}$: $\{N_s\}_{Kcs}$

Fig. 4 illustrates the flows of repeated authentications of the above protocol. The detailed steps are shown as follows.

1'. $C_{iX}^{1} \rightarrow S_{jY}^{'1}$: $N_c, \{T_{gwx}, C_{iX}^{1}, K_{cs}, EK_{xy}, S_{jY}^{2}, (C_{iX}^{1}, S_{jY}^{2}, EK_{xy}, K_{c's}, (C_{iX}^{'2}, K_{c's}, T_s)_{Ks})_{Kyy}\}_{Kcs}$
2'. $S_{jY}^{'1} \rightarrow GW_X^{'1}$: $S_{jY}^{'1}$ passes EK_{xy}, S_{jY}^{2} and $(C_{iX}^{1}, S_{jY}^{2}, EK_{xy}, K_{c's}, (C_{iX}^{'2}, K_{c's}, T_s)_{Ks})_{Kyy}$ to $GW_X^{'1}$
3'. $GW_X^{'1} \rightarrow GW_Y^{'2}$: $N_{gwx}, S_{jY}^{2}, (C_{iX}^{1}, S_{jY}^{2}, EK_{xy}, K_{c's}, (C_{iX}^{'2}, K_{c's}, T_s)_{Ks})_{Kyy}$
4'. $GW_Y^{'2} \rightarrow C_{iX}^{'2}$: $GW_Y^{'2}$ gets EK_{xy} and passes $S_{jY}^{2}, K_{c's}, (C_{iX}^{'2}, K_{c's}, T_s)_{Ks}$ to $C_{iX}^{'2}$
5'. $C_{iX}^{'2} \rightarrow S_{jY}^{2}$: $N_c, (C_{iX}^{'2}, K_{c's}, T_s)_{Ks}$
6'. $S_{jY}^{2} \rightarrow C_{iX}^{'2}$: $N_s, (N_c)_{Kc's}$
7'. $C_{iX}^{'2} \rightarrow S_{jY}^{2}$: $(N_s)_{Kc's}$
8'. $C_{iX}^{'2} \rightarrow GW_Y^{'2}$: C_{iX} acknowledges $GW_Y^{'2}$
9'. $GW_Y^{'2} \rightarrow GW_X^{'1}$: $GW_x, <N_{gwx}>_{EKxy}, GW_y, N_{gwy}$
10'. $GW_Y^{'2} \rightarrow GW_X^{'1}$: $GW_y, <N_{gwy}>_{EKxy}$
11'. $GW_X^{'1} \rightarrow S_{jY}^{'1}$: $GW_X^{'1}$ acknowledges $S_{jY}^{'1}$
12'. $S_{jY}^{'1} \rightarrow C_{iX}^{'1}$: $N_s, \{N_c\}_{Kcs}$
13'. $C_{iX}^{1} \rightarrow S_{jY}^{'1}$: $\{N_s\}_{Kcs}$

In the above inter-realm protocol, the inter-gateway key EK_{xy} is included in the inter-realm ticket. This is because we assume stateless gateways are used. When a session is closed, the inter-gateway key between GW_X and GW_Y is removed. To include the inter-gateway key in the ticket avoids the additional overhead of computing that key. When the ticket passes through GW_X and GW_Y, the inter-gateway key EK_{xy} is directly distributed to both gateways.

If stateful gateways are used, long-term information can be stored. For example, cross-realm information, such as inter-gateway keys in Table. 1, can be cached in gateways. If an inter-realm request is issued, the source gateway, such as GW_X, looks up the inter-gateway key table. If a destination gateway, such as GW_Y, is found, an inter-gateway key EK_{xy} can be extracted from the inter-gateway key table. If no such information exists, the inter-gateway key exchange described above should be executed. In the stateful gateway case, the inter-gateway key EK_{xy} is not necessary to be included in the ticket in the above protocol,

since such information has been cached.

Every gateway has a secret key, for example K_{xx} and K_{yy} in the above protocol. If the secret key is compromised, replacement of a new secret key for the old key can be performed, and then the gateway remains in the secure state. For providing a secure environment, the gateway can change the secret key periodically.

V. DISCUSSION

A. Comparisons

The comparisons of our protocol with Piessens, Decker and Janson's protocol, Lu and Sundareshan's protocol, and Kerberos version 5 are listed in Table. 2.

All mechanisms of our protocol are performed in gateways. There are two major advantages for such design. First, the inter-realm protocol is totally transparent to users. Secondly, the design makes the protocol more efficient for porting. Porting can be done by simply changing gateways without affecting the original systems.

B. Performance Analysis

Since the security platforms in local realms remain unchanged, they are not the factors to affect performance. The main factors exist in gateways and inter-gateway transmissions. We evaluate the performance from the aspects :

(1) Does the protocol incur any additional message transmission?
(2) How much overhead will the protocol suffer from computing inter-gateway keys?
(3) How much overhead will the protocol suffer from transformations of different encryption algorithms in gateways?

For the part of (1), our protocol does not incur any additional message to perform the inter-gateway key exchange. The components of the DH+MSR mechanism, the public key and the certificate, accompany with the request and the response messages which are the necessary parts of inter-realm secure communication.

For the part of (2), gateways compute inter-gateway keys upon receiving the opponent's public key and certificate. Note the public key is pre-computed, and the certificate is given by an off-line central authority, these parts do not raise any overhead. The computations in gateways are : to check the certificate ($Cert_x^2 = h(GW_x, P_x) \bmod N_u$), and to compute the inter-gateway key ($EK_{xy} = (P_x)^{Sy} \bmod N$). In the case of stateful gateways, the procedure of the inter-gateway key exchange of two realms is executed only once since both gateways can cache long-term information. Stateful gateways can reduce such computations.

For the part of (3), our protocol should transform different encryption algorithms at source and destination gateways. The intermediate gateways simply forward messages. Note that the universally agreed intermediate-ciphered form is necessary since the destination gateway has to recognize arrived messages, and so does the source gateway. Without such form, every encryption algorithm should be recognized by each gateway, and it is impratical for design.

VI. CONCLUSION

We proposed a general solution to accomplish the inter-realm authentication and key distribution for heterogeneous environments without affecting original security platforms. Several mechanisms are used to construct the protocol. The proxy mechanism allows security platforms in each realm to operate independently. The DH+MSR mechanism is used to dynamically exchange inter-gateway keys. The virtual link technique allows the intermediate gateways to simply forward messages.

Comparisons with other inter-realm protocols are discussed. Performance issues are also proposed. We have demonstrated the outstanding features of the proposed protocol.

REFERENCES

[1] W. P. Lu and M. K. Sundareshan, "Secure Communication in Internet Environments : A Hierarchical Key Management Scheme for End-To-End Encryption," *IEEE Transactions on Communications*, vol.37, no.10, pp.1014-1023, Oct. 1989.

[2] W. P. Lu and M. K. Sundareshan, "Enhanced Protocols for Hierarchical Encryption Key Management for Secure Communication in Internet Environments," *IEEE Transactions on Communications*, vol.40, no.4, pp. 658-660, April 1992.

[3] B. C. Neuman, and T. Ts'o, "Kerberos : An Authentication Service for Computer Networks," *IEEE Communications Magazine*, pp.33-38, Sep. 1994.

[4] F. Piessens, B. D. Decker, and P. Janson, "Interconnecting Domains with Heterogeneous Key Distribution and Authentication Protocols," *Proceedings of the IEEE Symposium on Security and Privacy*, pp.66-79, 1993.

[5] R. M. Needham, and M. D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," *Communications of the ACM*, vol.21, no.12, pp.993-999, Dec. 1978.

[6] A. Kehne, J. Schönwälder, H. Langendörfer, "A Nonce-Based Protocol for Multiple Authentications." *ACM Operating System Review*, vol.26, no.4, pp.84-89, Oct. 1992.

[7] B. C. Neuman, and S. G. Stubblebine, "A Note on the Use of Timestamps as Nonces," *ACM Operating System Review*, vol.27, no.2, pp.10-14, Apr. 1993.

[8] T. M. A. Lomas, L. Gong, J. H. Saltzer, and R. M. Needham, "Reducing Risks from Poorly Chosen Keys," *ACM Operating System Review*, vol.23, no.5, pp.14-18, Dec. 1989.

[9] L. Gong, M. A. Lomas, R. M. Needham, and J. H. Saltzer, "Protecting Poorly Chosen Secrets from Guessing Attacks," *IEEE Journal on Selected Areas in Communications*, vol.11, no.5, pp.648-656, Jun. 1993.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cyptosystems," *CACM*, vol.21, no.2, pp.120-126, Feb. 1978.

[11] R. Bird, I. Gopal, A. Herzberg, P. Janson, S. Kutten, R. Molva, and M. Yung, "The KryptoKnight Family of Light-Weight Protocols for Authentication and Key Distribution," *IEEE/ACM Trans. on Networking*, pp.31-41, vol.3, no.1, Feb. 1995.

[12] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and Authentication on a Portable Communications System," *IEEE Journal on Selected Areas in Communications*, vol.11, no.6, pp.821-829, Aug. 1993.

[13] W. Diffie, and M. E. Hellman, "New Direction in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp.644-654, Nov. 1976.

[14] H. C. Williams, "A Modification of RSA Public-Key Encryption," *IEEE Transactions on Information Theory*, vol.IT-26, no.6, pp.726-729, Nov, 1980.

Destination	Destination GW	Inter-Gateway Key
S_1	GW_Y	EK_{xy}
S_2	GW_Z	EK_{xz}
.	.	.
.	.	.

Table. 1 Inter-Gateway Key Table

	Our Protocol	Piessens, Decker & Janson	Kerberos V5	Lu & Sundareshan
Connect Existing Protocols	yes	partial	no	no
Permit Different Cryptography	yes	yes	yes	not mentioned
Across Several Realms	yes	no	yes	yes
Repeated Authentications Across Realms	yes	yes (only 2 realms)	yes	no
Inter-Realm Key Across Realms	DH+MSR	not mentioned	hierarchy	hierarchy
No More Message for Inter-Realm Keys	yes	not mentioned	no	no

Table. 2 Comparisons of Various Inter-Realm Protocols

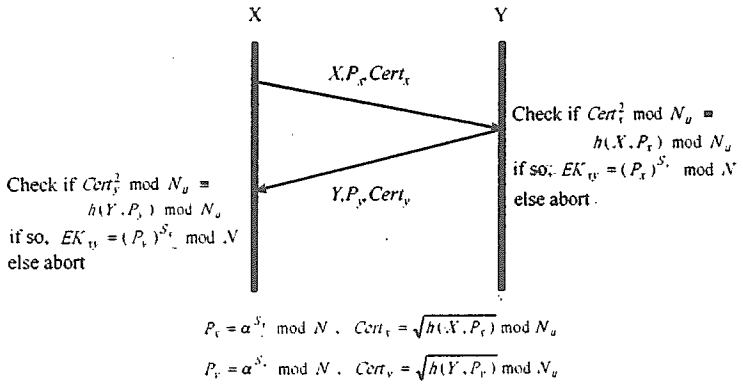

Fig. 1 DH+MSR mechanism

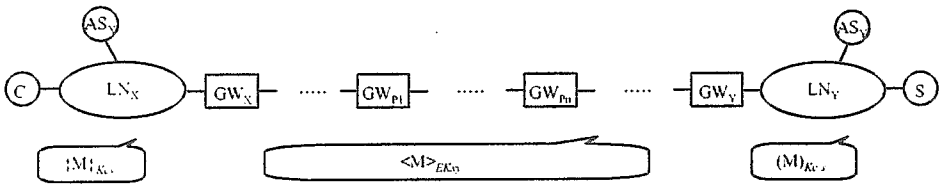

Fig. 2 Virtual Link Technique

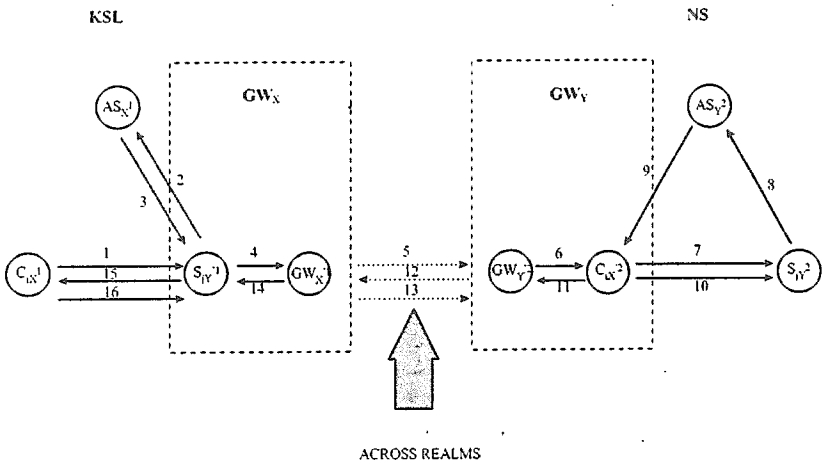

Fig. 3 Inter-Realm Protocol of KSL and NS

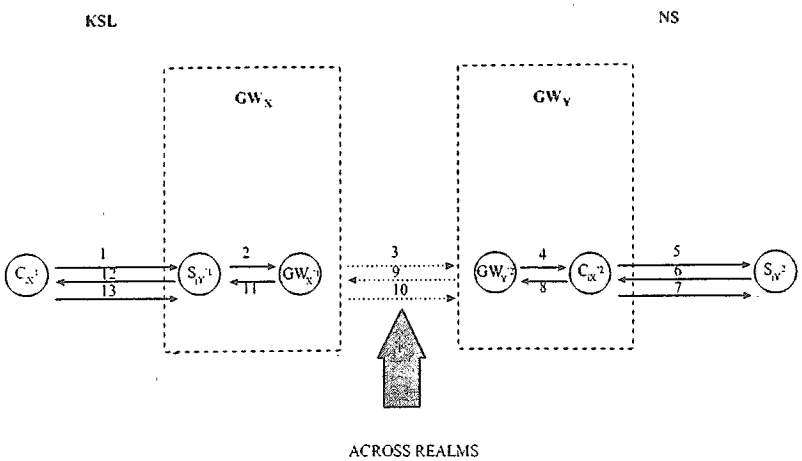

Fig. 4 Inter-Realm Repeated Authentication Protocol of KSL and NS