ISSN:0975-9646

An Efficient Group Key Transport Protocol

Manisha Y. Joshi[1], R.S. Bichkar[2]

[1] *M.G.M.'s College of Engineering, Nanded*

[2] *G.H. Raisoni College of Engineering, Wagholi, Pune*

***Abstract*: Conditional access system offers different services to the many groups simultaneously. The broadcast contents are scrambled with the secret key that protects it from unauthorized users. The secret key is distributed by server to the authorized users and shared it between user and server. The key transport protocol is used to transfer the secret key securely to these users. In this paper we present an efficient group key transport protocol using Chinese remainder theorem for access control. In this protocol, user has to carry only two secret numbers or keys. The decoding of broadcast message is done by only one modular division and one decryption. The main advantage of our scheme is that, a server can update the scrambling key or group key in one message, without changing user's key. The proposed protocol can be used for multiple group control, which is generally useful in Pay TV. Updating process of the group key does not increase communication and computation overhead on user as well as the server**.

***Keywords*: Conditional access system, key transport protocol, Chinese remainder theorem, Pay TV.**

I. INTRODUCTION

In the era of pay per view and conditional access systems, efficiency of access control system is a very important issue. Access control systems are responsible for scrambling of the video signal broadcasted by server. A video stream is scrambled with secret key and broadcasted. Only the authorized user or subscriber receives the video signal broadcasted by the server. This process is also called as broadcast encryption [1]. To maintain the confidentiality and access control, a receiver has to preserve the secret key, generally called as user's long time secret key which has been shared by the server and a receiver. As the number of users is dynamic, server has to change the scrambling key from time to time. Thus, there is a need of scalable key transport protocol for single and multiple access control.

Key management protocols are used to send the session key or private key to the intended receivers. In these protocols, the sender (generally key server) is responsible to generate the key and transfer it to receiver securely. Hence the receiver or its device has less responsibility and less resource requirement compared to the sender. Because of this feature these are preferred in the client server environment. Rest of the paper is organized as follows; section 2 gives a brief review of the related work. This includes Chiou and Chen's secure lock scheme [2] and key transport protocol based on secret sharing scheme by Eskicioglu and Delp [4]. Section 3 explains our proposed scheme for single access control. Section 4 presents an extension of scheme for multiple access control application. Section 5 presents analysis of the proposed scheme and its comparison with other scheme. Finally, section 6 concludes the paper.

II. RELATED WORK

There are several solutions for key distribution based on logical hierarchical key tree [5, 6]. In these solutions n users have to keep $\Theta(\log_2 n)$ keys and carry out the same number of encryptions as well as decryptions [7]. Hence it is not efficient when receiver's devices are less powerful. Use of Chinese remainder theorem for broadcast encryption was first proposed by Chiou and Chen [2]. They have used this theorem to construct a secure lock and have suggested both public key and symmetric key based solution. While using symmetric key based solution, each of n users has to maintain n modulie or integer $m_1, m_2, \ldots . m_n$, relatively prime with each other and n secret keys $k_1, k_2, \ldots . k_n$ and secure lock is a function of n modulies. The main disadvantage of this scheme is that if group size changes, the server has to redistribute new updated number of modulie n' to all user. Hence this scheme is not scalable for dynamic group. Our proposed scheme is derived from this scheme but in our scheme each user u_i has to keep only two keys (m_i, k_i) instead of n key pairs. If new user joins or existing user leaves, server has to update the scrambling key as well as key database and communicate to existing users. The existing users need not to change their keys. This makes our scheme more scalable.

The key transport protocol presented by Eskicioglu et al. uses secret sharing scheme [3]. In this scheme, one share of secret i.e. one point (x_i, y_i) of polynomial passing through origin, is with i^{th} user device and another secret i.e. another point (x_0, y_0) is with key the server. Server sends its share and scrambled video signal. Receiver computes scrambling key, which is intercept of polynomial using its own share and received share. As scrambling key is a function of server and user share, if any new user joins or existing user leaves, server has to regenerate the shares and redistribute among the users. Thus although this scheme reduces computation at receiver's side, it is not scalable for a set of dynamic users.

III. PROPOSED SCHEME FOR SINGLE ACCESS CONTROL.

As our scheme is based on Chinese remainder theorem, the statement of the Chinese remainder theorem (CRT) is discussed prior to the proposed protocol.

a. CHINESE REMAINDER THEOREM

Let there be n integers $m_1, m_2, \ldots . m_n$, such that, $gcd\ (m_i, m_{i+1}) = 1$ i.e m_i and m_{i+1} are co prime and n residue $a_1, a_2, \ldots . a_n$, There is an integer $x \equiv x(mod\ M)$ such that,

$$x \equiv a_1 (mod\ m_1)$$
$$x \equiv a_2 (mod\ m_2)$$
$$x \equiv a_3 (mod\ m_3)$$
$$.$$
$$.$$
$$x \equiv a_n (mod\ m_n)$$
$$M = \prod_{i=1}^{n} m_i$$
$$x \equiv x (mod\ M)$$
$$x = \left(\sum_{i=1}^{n} a_i\, c_i\, y_i \right) mod\ M$$

Where, $y_i = {}^{M}/_{m_i}$, $c_i = y_i^{-1}\ mod\ m_i$

B. REGISTRATION AND PRE DISTRIBUTION OF KEYS

Server generates, $n+1$ pair of integers, each called as a key pair (m_i, k_i) , where, $0 \le i \le n$. There are $m_0, m_2, \ldots, m_n$ such that $gcd\ (m_i, m_{i+1}) = 1$. There are $\{k_0, k_2, \ldots, k_n\}$ keys for n users and one for server, as shown in figure 1. Key pair (m_0, k_0) is not allotted to any user. All the key pairs are securely communicated to n users by either smart cards or using any secure authenticated protocol like SSL [8]. Let vs be the video signal which server want communicate securely. Server generates secret key S which is used to scramble the video signal for a group G.

C. KEY TRANSPORT PROTOCOL USING CRT

Server encrypts key S using each users key k_i and generates sub key S_i for each user i.e.

$$S_i = E_{k_i}\{S\}, \text{where } 0 \le i \le n$$

i. Server computes a lock X using Chinese remainder theorem as follows

$$X = \left(\sum_{i=0}^{n} S_i\, C_i Y_i\right) mod\ M, \text{ where,}$$
$$M = \prod_{i=0}^{n} m_i\ , S_i = E_{k_i}\{S\},\quad Y_i = {}^{M}/_{m_i},\quad C_i = Y_i^{-1}\ mod\ m_i,$$

ii. Server broadcast or multicast the message $\{X\} \parallel E_S\{vs\}$

iii. Each user computes $S_i = X\ mod\ m_i$ and decrypts S_i using its key k_i i.e. $S = D_{k_i}\{S_i\}$. Here the encryption/decryption can be performed by any standard symmetric cipher such as DES, AES [9, 10].

iv. User or user's device will decrypt the video signal $vs = D_S\{E_S\{vs\}\}$

There is need to change the scrambling key S if any new member subscribes to the CAS, called as ***Join*** and if any member's subscription ends and he doesn't want to continue, called as ***leave.***

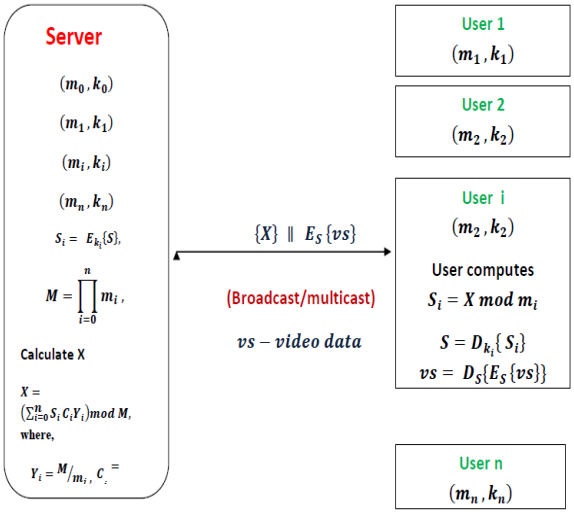

Figure 1: proposed scheme for single group

D. JOIN

New member registration is similar to that mentioned in the registration phase. New pair of keys (m_{new}, k_{new}) is generated for new user and new scrambling key S' is generated by server as shown in figure 2. Where m_{new} is relatively prime with M calculated in step 2 in the previous section and k_{new} is fresh.

Lock X is recomputed as follows

i. $M = M \times m_{new}$

ii. $S_i = E_{k_i}\{S'\}$, $Y_i = {}^{M}/_{m_i}$ $C_i = Y_i^{-1}\ mod\ m_i$ where ,$0 \le i \le n+1$

iii. $X = \left(\sum_{i=0}^{n+1} S_i\, C_i Y_i\right) mod\ M$

iv. Server broadcast or multicast the message $\{X\} \parallel E_S\{vs\}$

v. Each user computes $S_i = X\ mod\ m_i$ and $S' = D_{k_i}\{S_i\}$.

vi. User or user's device will decrypt the video signal $vs = D_{S'}\{E_{S'}\{vs\}\}$

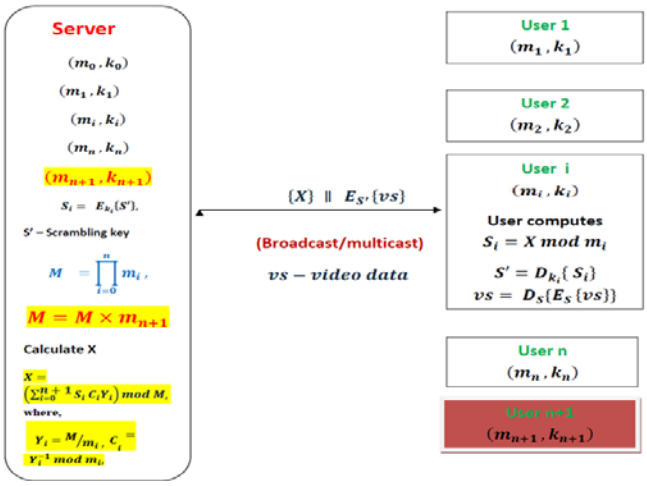

Figure 2: New user joins a group

E. LEAVE

Figure 3, shows that, when a user u_l leaves the group, its key pair (m_l, k_l) is deleted from key database and new scrambling key S' is generated by server. Secure lock X is recomputed using following steps

i. $M = {}^{M}/_{m_l}$

ii. $S_i = E_{k_i}\{S'\}$, $Y_i = {}^{M}/_{m_i}$ $C_i = Y_i^{-1} \bmod m_i$ where ,$0 \le i \le n-1$

iii. $X = \left(\sum_{i=0}^{n-1} S_i C_i Y_i\right) \bmod M$

iv. Server broadcast or multicast the message $\{X\} \parallel ES' vs$

v. Each user computes $S_i = X \bmod m_i$ and $S = Dki\,Si$ User or user's device will decrypt the video signal $vs = D_{S'}\{E_{S'}\{vs\}\}$

vi.

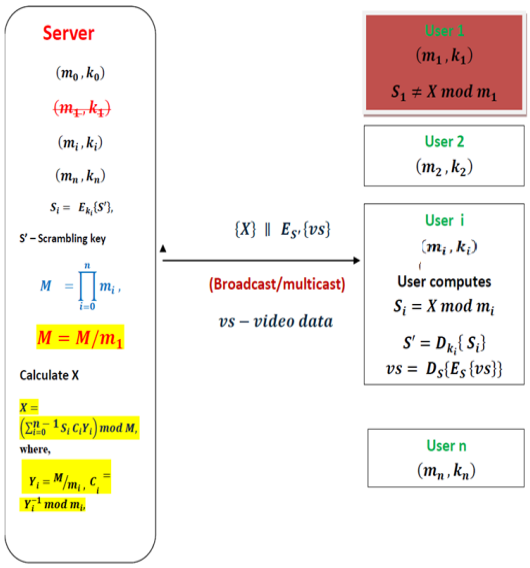

Figure 3: User leaves a group

IV. KEY TRANSPORT PROTOCOL USING CRT FOR MULTIPLE GROUP

In the multiple group , we have assumed that, there are l channels called as main set of channels $A = \{C_1, C_2, C_3, .. C_l\}$ and there are j subsets which are called as groups G_1, $G2, \ldots\ldots, Gj$ for example $G_1 = \{C_1, C_l\}, G_2 = \{C_1, C_4, \ldots, C_l\}$. Each user subscribes for one group at a time. User has facility to change the group. After changing a group user will not able to access previous group.

i. Server generates secret key $S_1, S_2, S_3 \ldots\ldots S_j$ which is used to scramble the video signal for a group G_j and sub key S_{ij} for each i^{th} user of j^{th} group i.e. $S_{ij} = E_{k_i}\{S_j\}$, where $0 \le i \le n_j$

ii. Server computes various locks $X_1, X_2, \ldots\ldots X_j$ using Chinese remainder theorem as follows,

$Xj = \left(\sum_{i=1}^{n_j} S_i C_i Y_i\right) \bmod M$, $M_j = \prod_{i=1}^{n} m_{ij}$,

$S_{ij} = E_{k_i}\{S_j\}$, $Y_i = {}^{Mj}/_{m_i}$ $C_i = Y_i^{-1} \bmod m_i$

iii. Server broadcast or multicast the message $\{X_1, X_2, \ldots, X_j\}$ for j groups

iv. Each user of respective group computes $S_{ij} = X_j \bmod m_i$ and decrypts the scrambling key using its own key k_i i.e. $S_j = D_{k_i}\{S_{ij}\}$.

When any user u_{ij} want to change group from G_1 to G_2, group keys of group G_1 and G_2 are changed. Scrambling key for group G_2 is constructed and distributed using our join algorithm discussed in previous section, except that there is no need to generate new key pair, as user still has a registered member. Scrambling key for group G_l is constructed and distributed using our leave algorithm in previous section except that the user's key pair is not deleted from key database. It is retained as user is still authorized user and only changing the group.

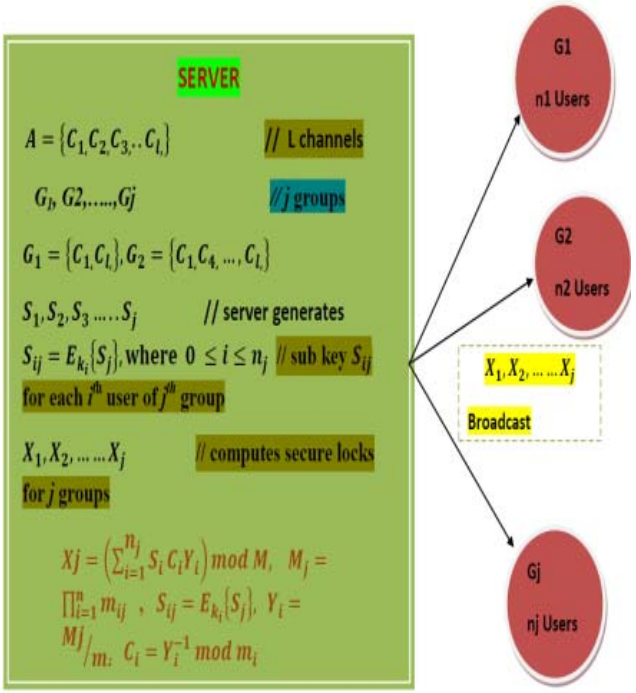

Figure 4: Multi-group key transport protocol

V. ANALYSIS OF PROPOSED SCHEME

In our scheme key pair (m_l, k_l) is kept secret by user hence only authorized user will be able to reveal encrypted scrambling key and that is decrypted by user itself. As encryption/decryption is performed by standard symmetric block cipher, the proposed protocol is secure from known plain text attack as well as brute force attack.

Secure lock X is function of key pair (m_0, k_0) which is with server, thus if any key like m_i is compromised, no one can forge the lock X. Hence our protocol is secure against impersonate attack and man in middle attack.

To compute the secure lock heavy computations are required but that will be computed by server. Server can use computationally efficient processor as well use divide and conquer algorithm [2] to implement the Chinese remainder theorem. Table 1 shows the comparison of our protocol with other schemes.

TABLE 1: COMPARISON OF THE PROPOSED PROTOCOL WITH OTHER SCHEMES.

Schemes	**Parameters for comparison**				
	Number of keys stored by user	Number of messages needed to transfer the key	Computation by users	Scalable to dynamic group	Can be used for multiple group
Chiou and Chen's	n-1	1	E+S+ M_D	No	No
Key transport protocolby Eskicioglu et.al	1	1	E+$\theta(t^2)$	No	No
Proposed protocol	**2**	**1**	**E+M_D**	**Yes**	**Yes**

n-number of users ,S-search, t-degree of polynomial , E-Encryption/decryption, M_D- modular division

V. CONCLUSIONS

In this paper we have presented an efficient key transport protocol which is useful for single and multiple group key management. As user has to store only two secret keys it is storage efficient. User has to perform only one modular division and one decryption to get access to the signal, it has advantage where receivers are having less resources. Proposed scheme is more applicable to conditional access system than group key management.

Protocol is efficient as only one message is sufficient to get access. An authorized user is not affected with new member joining or leaving.

REFERENCES

[1]. A.Fiat and M. Naor, "Broadcast encryption," in Advances in Cryptology, CRYPTO'93, 1994, vol. 773, pp. 480–491.

[2]. Chiou G. H. and. Chen W. T, "Secure broadcast using secure lock," IEEE Transanction on Software Engineering, vol. 15, no. 8, pp. 929–934, Aug. 1989.

[3]. A. Shamir, "How to share a secret," Communications of the ACM, MI. 22, no. 11, pp. 612-613, November 1979.

[4]. Ahmet M. Eskicioglu and Edward J. Delp "A Key transport protocol based on secret sharing, Application to information security" , IEEE Transactions on Consumer Electronics, Vol. 48, No. 4, pp 816-824,.Nov. 2002

[5]. Shyh-Yih Wang and Chi-Sung Laih *"*Efficient Key Distribution for Access Control in Pay-TV Systems "IEEE Transactions on Multimedia, vol. 10 ,pp. 480-491, April 2008

[6]. B. Liu, W. Zhang, and T. Jiang, "A scalable key distribution scheme for conditional access system in digital pay-TV system," IEEE Transaction on Consumer Electronics, vol. 50, no. 2, pp. 632–637, May 2004.

[7]. D. Wallner, E. Harder, and R. Agee, "Key management for multicast: issues and architecture," National Security Agency, RFC 2627, June 1999.

[8]. Rescorla, E. "SSL and TLS: Designing and Building Secure Systems." Reading,"MA:Addison- Wesley, 2001.

[9]. Schneier, B. "Applied Cryptography*."* New York, Wiley, 1996.

[10]. J.Daemen and V. R. Rijndael, "The Advanced Encryption Standard", Dr. Dobb's Journal, 2001.