ON THE DESIGN OF SECURE GROUP-ORIENTED COMMUNICATION CHANNELS IN INTERNET ENVIRONMENTS

Woei-Jiunn Tsaur and Shi-Jinn Horng

Department of Electrical Engineering
National Taiwan Institute of Technology
Taipei, Taiwan 107, R.O.C.
horng@ntit64.ntit.edu.tw

Abstract

This paper presents efficient protocols for establishing secure group-oriented communication channels in internet environments based on a geometric method. Since the data encryption/decryption requires a common secret session key between two communicating parties, finding an efficient way to distribute the group-oriented secret session key in internet environments has become a nontrivial task. We assume that the internet environments consist of many hosts, and each host has many users attached to it. The scheme proposed in this paper incorporates the public-key distribution and the trigonometry concepts as the basic theory. since this scheme does not need any trusted key distribution center to distribute the common secret session key between two groups, it is quite suitable to be used in internet environments so that the key distribution is convenient, time-saving and reparable. Furthermore, an authentication protocol is also proposed. Such a protocol can not only identify both the sender and the receiver of a group correctly but also make sure the transmitted message to be reached to its destination safely.

1 Introduction

Due to the rapid development and increasing popularity of multiuser internet environments, the data encryption has been widely used to prevent confidential data from being disclosed, destroyed, or altered by unauthorized users. However, conventional cryptosystems and the public key cryptosystems usually only address secure communications between two individuals. They still cannot be directly used to establish secure group-oriented communication channels in internet environments. Therefore, finding some approaches for establishing secure group-oriented communication channels in internet environments is very important.

With a fine design, we can derive a secure group-oriented data communication scheme based on a geometric method. Various schemes have been proposed to implement the group-oriented cryptosystems. Frankel [1] had proposed a protocol to solve some of these problems for the message transmission. However, this protocol requires the use of trusted centers to distribute the encrypted message, so it is not practical for use in large-scale internet systems that each interconnected network must has its own trusted center in this protocol. In [2], Desmedt and Frankel proposed a scheme based on the concept of the threshold scheme discussing the problem of deciphering the message by a group of people. In their scheme, a trusted center has to distribute the shadows of the deciphering key to the authorized receivers. It is inconvenient and time-consuming if the deciphering key is renewed or if the member of the authorized receivers who work together to decipher the message is changed. In [3], Chang and Lee presented a scheme based on the generalized secret-sharing scheme proposed by Lin and Harn [4] to tackle the generalized group-oriented cryptosystem. Although all the above schemes can solve some or all of these problems for the message transmission, they all do not emphasize the importance and meaning of establishing secure group-oriented communication channels in internet environments, not to mention the implementation for it.

In this paper, we propose efficient protocols based on a geometrical method to establish secure group-oriented communication channels in internet environments. These protocols do not need any trusted key distribution center to distribute the common secret session key between two groups, so the key distribution in this paper is convenient and time-saving as compared with [5, 6], and is reparable according to the concept proposed by Hwang and Ku [7]. Also, it can reduce the computation time needed for sending messages to a group of receivers due to non-exponential operations.

2 A group-oriented environment in internet systems

Desmedt [8] first introduced the concept of society and group-oriented cryptography. In practical applications, conventional and public key cryptosystems are not adapted when messages are intended for a group instead of for an individual. The main merit of the so-called group-oriented cryptosystem is that the security about crucial information accesses relies on all or some of the members in the group, not on a single individual. Frequently, a conference may consist of groups of individuals who may be in different and remote places and the group decision is made by all or some of the group members. Assume that all members in the group share the same decision respon-

0-7803-3692-5/96 © 1996 IEEE

sibility authorized by their supervisors in the same group. In such a case, three strategies can be adopted by supervisors for the group authorization:

(1) individuals of the group are highly authorized: any member in the group can make the group decision by himself;

(2) individuals of the group are lowly authorized: the group decision can be made only when all members in the group collaborate to work together;

(3) individuals of the group are restrictedly authorized: the group decision can be made by some members in the group if the number of collaborating members is over a predefined threshold value.

With rapid growth of modern technology, more and more people rely on computer networks to exchange knowledge, access information, and process data in internet environments. One major drawback of transmitting data through such environments is that many security holes could be intruded by intruders and wiretappers. A internet system is to interconnect many network systems located in different countries around the world, using the long-distance data communication technology. The geographical distribution of a system makes it more difficult to prevent intruders from getting physical access to parts of the system, including the communication lines.

To meet the demand of people who seek secure communications, various kinds of data transformation, or encryption/decryption techniques have been developed such that the data through open media become secure, but the original text can be recovered when the data reach the destination. The encryption/decryption performed between the sender and the receiver requires to share a secret session key between these two parties. Traditionally, trusted key distribution centers are utilized to distribute the secret session key in internet environments, as proposed by Lu and Sundareshan [5, 6]. But with the explosion of secret communications over large-scale internet systems that each interconnected network system has its own trusted key distribution center, this approach is time-consuming and inconvenient.

The secure and efficient group-oriented communication protocols that we will present in this paper incorporate the public-key distribution [4] and the trigonometry concepts as the basic mathematical tools. They are very suitable for large-scale internet systems since they do not need any trusted key distribution center to distribute the common secret session key between two groups. We assume that the internet systems consist of many hosts (H), and all network users (U) must register under one of these hosts. These hosts handle requests from their users, and they have no ability to interpret secret conversations carried out among different users of the system, as long as the proposed secure group-oriented communication protocols are run.

3 A fast and perfect secret key sharing scheme

In the following, we will present a fast and perfect secret key sharing scheme based on a simple geometric method [9].

[t − out − of − n] :
The sender selects a hyperplane equation with the constant coefficient K (the secret key) in a t-dimensional space as follows.
$X_t = a_{t-1}X_{t-1} + a_{t-2}X_{t-2} + ... + a_1X_1 + K$,
where the coefficients a_i, for i=1, 2, 3, ..., $t-1$, are chosen at random from the set $Z_q = \{0, 1, 2, ..., q-1\}$ for some large prime number q. For i=1, 2, 3, ..., n, the sender takes n different points $(X_{11}, X_{21}, ..., X_{t1})$, $(X_{12}, X_{22}, ..., X_{t2})$, ..., $(X_{1i}, X_{2i}, ..., X_{ti})$, ..., $(X_{1n}, X_{2n}, ..., X_{tn})$ from this hyperplane, and distributes each set of coordinates to a corresponding participant (receiver) P_i as his share to the secret key K. It is the property that in a t-dimensional space, any t distinct points being located on an object described by the equation $(X_1 - c_1)^2 + (X_2 - c_2)^2 + ... + (X_{t-1} - c_{t-1})^2 = r_1^2$, where $(c_1, c_2, ..., c_{t-1})$ are the coordinates of the object center and r_1 is the object radius but these t points not being located on an object described by the equation $(X_1 - d_1)^2 + (X_2 - d_2)^2 + ... + (X_{t-2} - d_{t-2})^2 = r_2^2$, where $(d_1, d_2, ..., d_{t-2})$ are the coordinates of the object center and r_2 is the object radius, can absolutely construct this hyperplane in a t-dimensional space. Therefore, in general we take $X_{1i} = r_1\cos\theta_{1i}$, $X_{2i} = r_1\sin\theta_{1i}\cos\theta_{2i}$, $X_{3i} = r_1\sin\theta_{1i}\sin\theta_{2i}\cos\theta_{3i}$, ..., $X_{(t-1)i} = r_1\sin\theta_{1i}\sin\theta_{2i}...\sin\theta_{(t-3)i}\sin\theta_{(t-2)i}$ and $X_{ti} = a_{t-1}r_1\sin\theta_{1i}\sin\theta_{2i}...\sin\theta_{(t-2)i} + ... + a_1r_1\cos\theta_{1i} + K$ if t is odd, or $X_{1i} = r_1\cos\theta_{1i}$, $X_{2i} = r_1\sin\theta_{1i}\sin\theta_{2i}$, ..., $X_{(t-1)i} = r_1\sin\theta_{1i}\sin\theta_{2i}...\sin\theta_{(t-3)i}\cos\theta_{(t-2)i}$ and $X_{ti} = a_{t-1}r_1\sin\theta_{1i}\sin\theta_{2i}...\sin\theta_{(t-3)i}\cos\theta_{(t-2)i} + ... + a_1r_1\cos\theta_{1i} + K$ if t is even, for some real numbers r_1, θ_{1i}, θ_{2i}, ..., $\theta_{(t-2)i}$ in the t-dimensional polar coordinates such that any t distinct $(X_{1i}, X_{2i}, ..., X_{ti})$, $1 \le i \le n$, are not located on the object described by the equation $(X_1 - d_1)^2 + (X_2 - d_2)^2 + ... + (X_{t-2} - d_{t-2})^2 = r_2^2$. It is easy to see that when any t receivers come together they have t pieces of information. They can use these t pieces of information to recover this hyperplane in a t-dimensional space, so they can obtain the secret key K easily. We can find that this geometric approach is perfect, because any group of receivers fewer than t cannot singly recover this hyperplane in a t-dimensional space.

4 Protocols for secure group-oriented communications in internet environments

Suppose the sender U_s attached to H_i in Fig. 1 wants to create a secure communication channel (to share a secret session key) with a member U_{g_j} of a group of receivers attached to H_j, $j \neq i$ in internet environments. We outline an authentication protocol between U_s and U_{g_j} to transmit an information I from U_s to U_{g_j} safely through their common secret session key K_{sg_j}.

(1) U_s sends the ciphertext $E_{K_{sg_j}}(ID_s, I)$ to U_{g_j}, where ID_s is the identifier of U_s and I is the information to be transmitted.

(2) U_{g_j} first deciphers $E_{K_{sg_j}}(ID_s, I)$ with the secret key K_{sg_j} to obtain ID_s and I. After these steps, U_{g_j} sends the ciphertext $E_{K_{sg_j}}(ID_s, ID_j)$ to U_s,

where ID_j is the identifier of U_{g_j}.

(3) U_s deciphers $E_{K_{sg_j}}(ID_s, ID_j)$ with the secret key K_{sg_j} to obtain ID'_s and ID'_j, and then compares its identifier ID_s to ID'_s. If they match, i.e. $ID_s = ID'_s$, then U_s recognizes U_{g_j} as the legitimate receiver and assures that the information I is exactly transmitted to U_{g_j}. U_s subsequently sends $E_{K_{sg_j}}(ID'_j)$ to U_{g_j}.

(4) U_{g_j} deciphers $E_{K_{sg_j}}(ID'_j)$ with the secret key K_{sg_j} to get ID'_j. If its identifier ID_j is equal to ID'_j, then U_{g_j} confirms the receipt to U_s and assures that the information I was actually from U_s.

Thus, the sender U_s and the receiver U_{g_j} have identified themselves to each other.

A practical scheme presented as follows can simultaneously establish secure group-oriented communication channels for these three open problems as described in Section 1 in internet environments.

4.1 Messages for a group of receivers

The sender S may send a message M to a group G of n members in such a way that M is readable only when any t members ($t \leq n$) from G come together to decipher the message. Assume that each member, g_i, holds two sets of secret polar coordinates $r_{g_i} = (r_{g_i,1}, r_{g_i,2}, ..., r_{g_i,(t-1)})$ and $\theta_{g_i} = (\theta_{g_i,1}, \theta_{g_i,2}, ..., \theta_{g_i,(t-2)})$, for some real numbers $r_{g_i,1}$, $r_{g_i,2}$, ..., $r_{g_i,(t-1)}$, $\theta_{g_i,1}$, $\theta_{g_i,2}$, ..., $\theta_{g_i,(t-2)}$, and publishes function f_j (or f'_j) and the value of $Y_{g_i,j}$, $1 \leq j \leq (t-1)$, as computed by f_j (or f'_j) as follows.

$Y_{g_i,1} = r_{g_i,1} f_1(\theta_{g_i,1}) = r_{g_i,1} \cos\theta_{g_i,1}$

.....

$Y_{g_i,(t-1)} = r_{g_i,(t-1)} f_{t-1}(\theta_{g_i,1}, ..., \theta_{g_i,(t-2)})$
$= r_{g_i,(t-1)} \sin\theta_{g_i,1} ... \sin\theta_{g_i,(t-3)} \sin\theta_{g_i,(t-2)}$

if t is odd; or

$Y_{g_i,1} = r_{g_i,1} f'_1(\theta_{g_i,1}) = r_{g_i,1} \cos\theta_{g_i,1}$

.....

$Y_{g_i,(t-1)} = r_{g_i,(t-1)} f'_{t-1}(\theta_{g_i,1}, ..., \theta_{g_i,(t-2)})$
$= r_{g_i,(t-1)} \sin\theta_{g_i,1} ... \sin\theta_{g_i,(t-3)} \cos\theta_{g_i,(t-2)}$

if t is even.

[The Sender]:

(1) Obtain the public values $Y_{g_i,1}$, $Y_{g_i,2}$, ..., $Y_{g_i,(t-1)}$ and the public functions $f_1, f_2, ..., f_{t-1}$ or $f'_1, f'_2, ..., f'_{t-1}$ ($1 \leq i \leq n, g_i \in G$) from the public directory.

(2) Select two sets of secret polar coordinates $r_s = (r_{s,1}, r_{s,2}, ..., r_{s,(t-1)})$ and $\theta_s = (\theta_{s,1}, \theta_{s,2}, ..., \theta_{s,(t-2)})$, for some real numbers $r_{s,1}$, $r_{s,2}$, ..., $r_{s,(t-1)}$, $\theta_{s,1}$, $\theta_{s,2}$, ..., $\theta_{s,(t-2)}$, and compute the public values $Y_{s,j}$ and the common secret session key $K_{sg_i,j}$, $1 \leq j \leq (t-1)$, as follows.

(a) $Y_{s,1} = r_{s,1} f_1(\theta_{s,1}) = r_{s,1} \cos\theta_{s,1}$

.....

$Y_{s,(t-1)} = r_{s,(t-1)} f_{t-1}(\theta_{s,1}, ..., \theta_{s,(t-2)})$
$= r_{s,(t-1)} \sin\theta_{s,1} ... \sin\theta_{s,(t-3)} \sin\theta_{s,(t-2)}$

if t is odd; or

$Y_{s,1} = r_{s,1} f'_1(\theta_{s,1}) = r_{s,1} \cos\theta_{s,1}$

.....

$Y_{s,(t-1)} = r_{s,(t-1)} f'_{t-1}(\theta_{s,1}, ..., \theta_{s,(t-2)})$
$= r_{s,(t-1)} \sin\theta_{s,1} ... \sin\theta_{s,(t-3)} \cos\theta_{s,(t-2)}$

if t is even.

(b) the common secret session key $K_{sg_i} = (K_{sg_i,1}, K_{sg_i,2}, ..., K_{sg_i,(t-1)})$ between the sender S and the receiver g_i:
$K_{sg_i,1} = r_{s,1} Y_{g_i,1} f_1(\theta_{s,1}) = r_{s,1} Y_{g_i,1} \cos\theta_{s,1}$
$= r_{s,1} r_{g_i,1} \cos\theta_{g_i,1} \cos\theta_{s,1}$

.....

$K_{sg_i,(t-1)}$
$= r_{s,(t-1)} Y_{g_i,(t-1)} f_{t-1}(\theta_{s,1}, ..., \theta_{s,(t-2)}) =$
$r_{s,(t-1)} Y_{g_i,(t-1)} \sin\theta_{s,1} ... \sin\theta_{s,(t-3)} \sin\theta_{s,(t-2)}$
$= r_{s,(t-1)} r_{g_i,(t-1)} \sin\theta_{g_i,1} ... \sin\theta_{g_i,(t-3)}$
$\sin\theta_{g_i,(t-2)} \sin\theta_{s,1} ... \sin\theta_{s,(t-3)} \sin\theta_{s,(t-2)}$

if t is odd; or

$K_{sg_i,1} = r_{s,1} Y_{g_i,1} f'_1(\theta_{s,1}) = r_{s,1} Y_{g_i,1} \cos\theta_{s,1}$
$= r_{s,1} r_{g_i,1} \cos\theta_{g_i,1} \cos\theta_{s,1}$

.....

$K_{sg_i,(t-1)}$
$= r_{s,(t-1)} Y_{g_i,(t-1)} f'_{t-1}(\theta_{s,1}, ..., \theta_{s,(t-2)}) =$
$r_{s,(t-1)} Y_{g_i,(t-1)} \sin\theta_{s,1} ... \sin\theta_{s,(t-3)} \cos\theta_{s,(t-2)}$
$= r_{s,(t-1)} r_{g_i,(t-1)} \sin\theta_{g_i,1} ... \sin\theta_{g_i,(t-3)}$
$\cos\theta_{g_i,(t-2)} \sin\theta_{s,1} ... \sin\theta_{s,(t-3)} \cos\theta_{s,(t-2)}$

if t is even.
Repeat this step if there exits some i and j ($i \neq j$) such that $K_{sg_i} = K_{sg_j}$.

(3) Construct a polynomial $w(x_{t-1}, x_{t-2}, ..., x_1)$ of degree one
$w(x_{t-1}, x_{t-2}, ..., x_1) = x_t = a_{t-1}x_{t-1} + a_{t-2}x_{t-2} + ... + a_1x_1 + K$,
where the coefficients a_i, for i=1, 2, 3, ..., $t-1$, are chosen at random from the set $Z_q = \{0, 1, 2, ..., q-1\}$ for some large prime number q, and K will serve as the encryption key later.

(4) Encipher a message M into C using the key K,
$C = E_K(M)$,
where E denotes the predetermined encryption algorithm.

(5) Broadcast $Y_{s,1}$, $Y_{s,2}$, ..., $Y_{s,(t-1)}$ and the ciphertext C to all members of the receiving group.

(6) Compute
n shares $s_i = w(K_{sg_i,(t-1)}, K_{sg_i,(t-2)}, ..., K_{sg_i,1})$, $1 \leq i \leq n$. Transmit the share s_i to the member g_i by running the authentication protocol as presented in Section 4. After running the authentication protocol, not only the sender S can recognize whether g_i is the legitimate receiver or not, but also it can make sure whether the share s_i has been exactly transmitted to the member g_i or not.

[The Receiver]:

(1) g_i computes the common secret session key $K_{g_is} = (K_{g_is,1}, K_{g_is,2}, ..., K_{g_is,(t-1)})$ between the receiver g_i and the sender S:
$K_{g_is,1} = r_{g_i,1}Y_{s,1}f_1(\theta_{g_i,1}) = r_{g_i,1}Y_{s,1}\cos\theta_{g_i,1}$
$= K_{sg_i,1}$

.....

$K_{g_is,(t-1)}$
$= r_{g_i,(t-1)}Y_{s,(t-1)}f_{t-1}(\theta_{g_i,1}, ..., \theta_{g_i,(t-2)})$
$= r_{g_i,(t-1)}Y_{s,(t-1)}\sin\theta_{g_i,1}...\sin\theta_{g_i,(t-2)}$
$= K_{sg_i,(t-1)}$

if t is odd; or

$K_{g_is,1} = r_{g_i,1}Y_{s,1}f'_1(\theta_{g_i,1}) = r_{g_i,1}Y_{s,1}\cos\theta_{g_i,1}$
$= K_{sg_i,1}$

.....

$K_{g_is,(t-1)}$
$= r_{g_i,(t-1)}Y_{s,(t-1)}f'_{t-1}(\theta_{g_i,1}, ..., \theta_{g_i,(t-2)})$
$= r_{g_i,(t-1)}Y_{s,(t-1)}\sin\theta_{g_i,1}...\cos\theta_{g_i,(t-2)}$
$= K_{sg_i,(t-1)}$

if t is even.

(2) After running the authentication protocol as presented in Section 4, if the receiver g_i confirms the receipt to the sender S, he will obtain the share s_i being from the sender S exactly.

(3) When any t authorized receivers come together, the secret key K can be computed by using the perfect $t-out-of-n$ threshold scheme as presented in Section 3.

(4) The message $M = D_K(C)$,
where D denotes the corresponding decryption algorithm.

4.2 Messages for anyone in the group

The sender S may send a message M to a group G of n members such that anyone in G can recover M. However, anyone outside the group G cannot be able to recover M. Here, we extend the concept of the conference key distribution scheme [10] to solve this problem.

[The Sender]:

(1) The sender S first executes Steps (1), (2), (3), (4), (5) and (6) as the sender S did in Section 4.1.

(2) Compute $t-1$ extra shares which are different from each other from polynomial w as defined in Step 3 in Sec. 4.1 such that $s'_m = w(j_1, j_2, ..., j_{t-1})$, $1 \leq m, j_1, j_2, j_3, ..., j_{t-1} \leq t-1$. Assume that $K_{sg_i,1}$, $K_{sg_i,2}$, ..., $K_{sg_i,(t-1)} \geq t$ for all i.

(3) Broadcast the $t-1$ extra shares $s'_1, s'_2, ..., s'_{(t-1)}$ to all members of the receiving group.

[The authorized Receiver g_i]:

(1) g_i computes the common secret session key $K_{g_is} = (K_{g_is,1}, K_{g_is,2}, ..., K_{g_is,(t-1)})$ between the receiver g_i and the sender S as the receiver did in Section 4.1.

(2) After running the authentication protocol as presented in Section 4, if the receiver g_i confirms the receipt to the sender S, it will obtain the share s_i being from the sender S exactly.

(3) Each authorized receiver g_i has t shares, so he can obtain the secret key K by using the perfect $t-out-of-n$ threshold scheme as presented in Section 3.

(4) The message $M = D_K(C)$.

4.3 Messages for a particular member in the group

The sender S may transmit the message M to a particular member g_i in private.

[The Sender]:

(1) The sender S first executes Steps (1) and (2) as the sender S did in Section 4.1.

(2) Send the public values $Y_{s,1}$, $Y_{s,2}$, ..., $Y_{s,(t-1)}$ to the particular member g_i of the receiving group.

(3) Transmit the message M to a particular member g_i by running the authentication protocol as presented in Section 4. As stated before, not only the sender S and the particular member g_i are identified but also the transmitted message M can reach the particular member g_i safely.

[The particular authorized Receiver g_i]:

(1) g_i computes the common secret session key $K_{g_is} = (K_{g_is,1}, K_{g_is,2}, ..., K_{g_is,(t-1)})$ between the receiver g_i and the sender S as the receiver did in Section 4.1.

(2) After running the authentication protocol as presented in Section 4, if the particular member g_i confirms the receipt to the sender S, he will obtain the message M being from the sender S exactly.

5 Security analysis

There are five possible attacks that will be discussed in this section. We list them as follows.

(Attack 1) If an impostor wants to pretend to be the sender S and establish a "secret channel" with a member g_i of a group G, then he can take the following approach. Because the ciphertext $R = E_{K_{sg_i}}(ID_s, s_i)$ or $R = E_{K_{sg_i}}(ID_s, M)$ is transmitted by the sender S

and it can be intercepted by wiretappers, the impostor can intercept it, replace R by R', and then sends R' to g_i. But, upon receiving R', g_i first deciphers R' with the common secret key K_{g_is}. Then, g_i sends the ciphertext $E_{K_{g_is}}(ID'_s, ID_i)$ to S, where ID_i is the identifier of g_i. S deciphers $E_{K_{g_is}}(ID'_s, ID_i)$ with the common secret session key K_{sg_i} to obtain ID'_s and ID_i, and then compares ID_s with ID'_s. Since ID_s is different from ID'_s, the comparison will fail and the request to establish a "secret channel" between the impostor and g_i will be rejected. Thus, this attack fails.

(Attack 2) An impostor may modify ID_s to ID_t (the imposter ID) and also modify R (as in Attack 1) to R' such that ID'_t is the result of deciphering R' with the common secret session key K_{sg_i}. If so, according to the authentication protocol as presented in Section 4, the comparison between ID_t and ID'_t will match and the impostor will successfully impersonate the sender S. However, since R is calculated from the equation $R = E_{K_{sg_i}}(ID_s, s_i)$ or $R = E_{K_{sg_i}}(ID_s, M)$ and K_{sg_i} is known to S and g_i only, computing R' from ID_t would be very difficult without the knowledge of K_{sg_i}.

(Attack 3) Since R (as in Attack 1) can be intercepted by an intruder during transmission, users who have obtained R other than the sender S can also send R to someone else, and each claims itself to be the sender S. However, Since they lack the knowledge of the sender's secret information $r_s = (r_{s,1}, r_{s,2}, ..., r_{s,(t-1)})$ and $\theta_s = (\theta_{s,1}, \theta_{s,2}, ..., \theta_{s,(t-2)})$, they still cannot obtain the correct secret session key. Hence, this attack will fail also.

(Attack 4) According to the concept proposed by Hwang and Ku [7] that a reparable key distribution protocol is that the protocol is secure once all compromised keys have been replaced by secure keys, Hwang and Ku [7] had proved the key distribution protocols of Lu and Sundareshan [5, 6] are not reparable. But, the proposed protocols in this paper are reparable since no trusted key distribution center is used for distributing the common secret session key.

6 Conclusions

In this paper, we propose a new authenticated session key distribution scheme for establishing secure group-oriented communication channels in internet environments. There are some advantages of this scheme and we list them as follows.

(1) The common secret session key can be authenticated by two users, one is the sender and the other is any member of the receiving group, and it can be distributed successfully without the existence of a globally trusted key distribution center and many locally trusted key distribution centers in internet environments. Practically, such a trusted key distribution center may not exist in large-scale distributed systems. Therefore, the proposed protocols are very efficient and applicable in the real world.

(2) With our scheme, the common secret session key can be obtained only by the sender and any member of the receiving group. Hence, it is not exposed to other users or even to the hosts. So, the secure group-oriented communication channels can be well established in internet environments.

(3) In our scheme, each user holds two sets of secret polar coordinates and these secret values are never transmitted directly through computer networks. Therefore, it is extremely difficult for an intruder to obtain these secret values.

References

[1] Y. Frankel, "A practical protocol for large group oriented networks," Advances in Cryptology: Proceedings of Eurocrypt'89, Lecture Notes in Computer Science, Springer-Verlag, pp. 56-61, 1990.

[2] Y. Desmedt and Y. Frankel, "Threshold cryptosystems," Advances in Cryptology: Proceedings of Crypto'89, Lecture Notes in Computer Science, Springer-Verlag, pp. 307-315, 1990.

[3] C. C. Chang and H. C. Lee, "A new generalized group-oriented cryptoscheme without trusted centers," IEEE Journal on Selected Areas in Communications, Vol. 11, No. 5, pp. 725-729, June 1993.

[4] H. Y. Lin and L. Harn, "A cheater resistant generalized secret sharing scheme," Technical Report, Department of Computer Science/Telecommunication Program, Missouri-Kansas City University, private communication, 1991.

[5] W. P. Lu and M. K. Sundareshan, "Secure communications in internet environments: a hierarchical key management scheme for end-to-end encryption," IEEE Trans. Commun., vol. 37, pp. 1014-1023, Oct. 1989.

[6] W. P. Lu and M. K. Sundareshan, "Enhanced protocols for hierarchical encryption key management for secure communications in internet environments," IEEE Trans. Commun., vol. 40, pp. 658-670, Apr. 1992.

[7] T. Hwang and W. C. Ku, "Reparable key distribution protocols for internet environments," IEEE Trans. Commun., vol. 43, pp. 1947-1949, May 1995.

[8] Y. Desmedt, "Society and group oriented cryptography: a new concept," Advances in Cryptology: Proceedings of Crypto'87, Lecture Notes in Computer Science, Springer-Verlag, pp. 120-127, 1988.

[9] W. J. Tsaur and S. J. Horng, "A efficient and perfect group-oriented secret key sharing in distributed systems," Technical Report, TR-1995-EE-006, Department of Electrical Engineering, National Taiwan Institute of Technology, Taiwan, R.O.C., 1995.

[10] C. S. Laih, L. Harn and J. Y. Lee, "A new threshold scheme and its application in designing the conference key distribution cryptosystem," Information Processing Letters, 32, pp. 95-99, 1989.