International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 10 , October 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

PROVIDING A SECURE GROUP COMMUNICATION BY USING A NOVEL KEY TRANSFER PROTOCOL AND BY GENERATING MULTIPLE SESSION KEYS

Dr. A.S.N. Chakravarthy[1], Mr. T. Anjikumar[2]

[1]*Department of CSE, JNTUniversity, Kakinada, Andhra Pradesh, India*

[2]*Department of CSE, SITAM College, Vizianagaram, Andhra Pradesh, India*

ABSTRACT

Key transfer protocols rely on a mutually trusted key generation center (KGC) to select group keys and transport group keys to all communication entities secretly. Most often, KGC encrypts group keys under another secret key shared with each entity during registration and send to all the communication entities. But there is a chance of knowing the group key by the hacker through cryptanalysis during transmission. The transmitted group key is used to encrypt / decrypt different messages at the sender / receiver during a group communication. But, chosen-plaintext attacks have been proposed when a single group key is used to encrypt / decrypt different messages in a group. In this paper, we propose a novel key transfer protocol based on secret sharing scheme that KGC can broadcast a set of key values to all the group members at once and only authorized group members can recover the set of key values, thus providing confidentiality and authentication. We also propose a method where the set of key values is used to generate multiple session keys which are used to encrypt / decrypt different messages during group communication, which is secure under chosen-plaintext attacks.

Keywords : Authentication, Confidentiality, Key generation center, Key transfer protocol, Key value, Session key.

I. INTRODUCTION

Now a days, group communication plays a major role in the society. Many emerging network applications (e.g., teleconference, information services, and so on) are based upon a group communication model. As a result, securing group communication, i.e., providing confidentiality, authenticity, and integrity of messages delivered between the group members, becomes a critical networking issue.

In order to provide confidentiality and authentication, one-time group key is needed to be shared among communication entities to encrypt and authenticate messages. Thus, a key establishment protocol needs to distribute one-time group key to all participating entities before exchanging communication messages. Confidentiality and authentication should be provided for group key by the key establishment protocol. There are two types of key establishment protocols according to [3]: key transfer protocols and key agreement protocols.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Key transfer protocols depends on a trusted key generation center (KGC) to select group keys and these group keys are transmitted to all the communication entities secretly. Generally, the group key is encrypted by KGC under another secret key shared with each entity during registration. In key agreement protocols, the group key is determined by all the communication entities in a group. Diffie-Hellman (DH) key agreement protocol [4] is the most commonly used key agreement protocol.

In order to design group key distribution protocols, secret sharing has been used. There are two different approaches using secret sharing: one assumes a trusted offline server active only at initialization [2], [5], [8], [1] and the other assumes an online trusted server, called the key generation center, always active. The name of the first type of approach is called as the key predistribution scheme. A trusted authority generates and distributes secret pieces of information to all users offline in a key predistribution scheme. Users belonging to a privileged subset can compute individually a group key common to this subset at the beginning of a conference. The main disadvantage of this approach is that every user is required to store a large size of secrets. The second type of approach requires an online server to be active [7]. This approach is similar to the model used in the IEEE 802.11i standard [6] that employs an online server to select a group key and transmit it to each group member. However, the difference between this approach and the IEEE 802.11i is that, instead of encrypting the group temporal key (GTK) using the key encryption key (KEK) from the authentication server to each mobile client separately as specified in the IEEE 802.11i, the trusted KGC broadcasts group key information to all group members at once. In this paper, we propose a novel key transfer protocol that provides confidentiality and authentication for distributing the set of key values to all the communication entities. We also propose a method where the set of key values is used to generate multiple session keys which are used to encrypt / decrypt different messages, which is secure under chosen-plaintext attacks.

The rest of this paper is organized as follows: In Section 2, we provide the description of the existing system for group communication. In Section 3, we provide the description of the proposed system for group communication. The experimental results are shown in section 4. Finally, the paper is concluded in section 5.

II. EXISTING SYSTEM

In the existing system, group key transfer protocol relies on one trusted entity, KGC, to choose the key, which is then transferred to each group member involved. Each user is required to register at KGC for subscribing the key distribution service. The KGC keeps track of all registered users and remove any unsubscribed users. During registration, KGC shares a secret with each user. In most key transfer protocols, KGC encrypts the randomly selected group key under the secret key shared with each user during registration and sends the ciphertext to each group member separately. An authenticated message checksum is attached with the ciphertext to provide group key authenticity. In this approach, the confidentiality of group key is ensured using any encryption algorithm which is computationally secure. The ciphertext received from the KGC is decrypted by each group member by the secret key shared with each user during registration by KGC and obtains the group key. This group key is used to encrypt / decrypt different messages at the sender / receiver during a group communication. Even though it is a secure process for group communication, there are some issues present in this existed system. The first issue is that there is a chance of knowing the group key by the hacker through

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

cryptanalysis during transmission of the group key from KGC to the communication entities. The second issue is that chosen-plaintext attacks have been proposed when a single group key is used to encrypt / decrypt different messages in a group communication.

III. PROPOSED SYSTEM

In order to overcome the problems present in the existing system, we propose a novel key transfer protocol based on secret sharing scheme that KGC can broadcast a set of key values to all the group members at once and only authorized group members can recover the set of key values, thus providing confidentiality and authentication. We also propose a method where the set of key values is used to generate multiple session keys which are used to encrypt / decrypt different messages during group communication, which is secure under chosen-plaintext attacks.

In the proposed system, the group communication process is divided into five phases. They are as follows.

3.1. INITIALIZATION OF KGC

The KGC randomly chooses two safe primes p and q (i.e., primes such that $p_t = p-1/2$ and $q_t = q-1/2$ are also primes) and compute n = pq. n is made publicly known.

3.2. USER REGISTRATION

Each user is required to register at KGC for subscribing the key distribution service. The KGC keeps track of all registered users and remove unsubscribed users. During registration, KGC shares a secret, (x_i, y_i), with each user U_i, where $x_i, y_i \varepsilon Z^*n$.

3.3. GENERATION AND DISTRIBUTION OF KEY VALUES

Upon receiving a group communication request from any user, KGC generates a set of key values K= {m, x, y, c} that are used to compute multiple session keys which are used to encrypt / decrypt different messages during group communication. KGC needs to distribute these key values to all group members in a secure and authenticated manner. All communications between KGC and group members are in a broadcast channel.

Let us assume that a group consists of t members, $\{M_1; M_2;\ldots; M_t\}$, and shared secrets are (x_i, y_i) for i = 1,…, t. The key value generation and distribution process contains six steps.

Step 1: The initiator sends group communication request to KGC with a list of group members as $\{M_1; M_2;...; M_t\}$.

Step 2: The KGC sends a group communication response by broadcasting the list of all participating members, $\{M_1; M_2; \ldots ; M_t\}$.

Step 3: A random challenge, $R_i \varepsilon Z^*n$, is generated by each participating group member and is sent to KGC.

Step 4: KGC generates a set of key values K= {m, x, y, c} that are used to compute multiple session keys.

Step 5: For each key value "a" in the set K (i.e. a ε K), KGC generates an interpolated polynomial f(x) with degree t to pass through (t +1) points, (0, a) and $(x_i, y_i \oplus R_i)$, for i = 1, . . . , t. KGC also computes t additional points, P_i, for i =1,. . . , t, on f(x) and Auth =h(a,M_1, . . . , M_t,R_1, ...,R_t, P_1, . . . , P_t), where h is a one-way hash function. All computations on f(x) are over Z*n. KGC broadcasts {Auth, P_i}, for i =1, . . . , t, to all group

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

members. All computations are performed in Z*n.

Step 6: For each group member, M_i, knowing the shared secret, (x_i, $y_i \oplus R_i$), and t additional public points, P_i, for i = 1, . . . ,t, on f(x), is able to compute the polynomial f(x) and recover the key value a = f(0). Then, M_i computes h(a, M_1, . . . M_t,R_1, . . ., R_t, P_1, . . . , P_t) and checks whether this hash value is identical to Auth. If these two values are identical, M_i authenticates that the key value is sent by KGC. In this way, each group member, M_i, receives the set of key values K= {m, x, y, c} from KGC using the secret sharing scheme.

The following Fig. 3.1, illustrates the novel key transfer protocol for a group having 4 members, A, B, C, and D.

STEP	KGC		USER
1		Group Communication Request { A,B,C,D} ←	Initiator
2		Group Communication Response { A,B,C,D} →	A,B,C,D
3		R_A ← R_B ← R_C ← R_D ←	A B C D
4	KGC generates a set of key values K= {m, x, y, c} that are used to compute multiple session keys.		
5	For each a ε K, KGC computes f(x) passing through (0,a),(X_A,$Y_A \oplus R_A$), (X_B,$Y_B \oplus R_B$), (X_C,$Y_C \oplus R_C$), (X_D,$Y_D \oplus R_D$). KGC also computes P_1,P_2,P_3, P_4 on f(x) and Auth = h(a, A, B, C, D, R_A, R_B, R_C, R_D, P_1, P_2, P_3, P_4).	Auth, P_1, P_2, P_3, P_4 →	A,B,C,D
6			Each participating user M_i computes an interpolating polynomial f(x) passing through P_1, P_2, P_3, P_4 and (X_i,$Y_i \oplus R_i$). M_i checks whether Auth = h(a, A, B, C, D, R_A, R_B, R_C, R_D, P_1, P_2, P_3, P_4).

Fig. 3.1: Novel key transfer protocol.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

3.4. GENERATION OF MULTIPLE SESSION KEYS

Each group member, M_i, receives the set of key values K= {m, x, y, c} from KGC using the secret sharing scheme. The key values are passed to the key generation function which generates multiple session keys. The equations that computes the session keys are $x = mx + c \rightarrow (1)$; $z = y + x \rightarrow (2)$; where z is the session key computed from the four values m, x, y, c. The two equations are executed repeatedly for each message transfer and the value of x during the last message transfer will be used for the computation of the new session key for the next message transfer. The value of x varies for each message transfer whereas the values of m, c, y remains constant.

3.5. GROUP COMMUNICATION USING MULTIPLE SESSION KEYS

Initially, all the group members compute the initial common session key. When any user wants to send the data, he encrypts the message using the common session key and sends it to the receivers in the group. The receivers in the group then decrypts the encrypted message using the common session key. After one message transfer, a new common session key is computed by all group members and this key is used to transfer the next message. In this way, new session key will be computed by the group members every time when a new message is to be transferred. The main security goals achieved by our system are key freshness, key confidentiality and key authentication.

IV. EXPERIMENTAL RESULTS

This experimental work is implemented in java and carried out on windows operating system.

The following Fig. 4.1 shows the initialization of Key Generation Center (KGC) server.

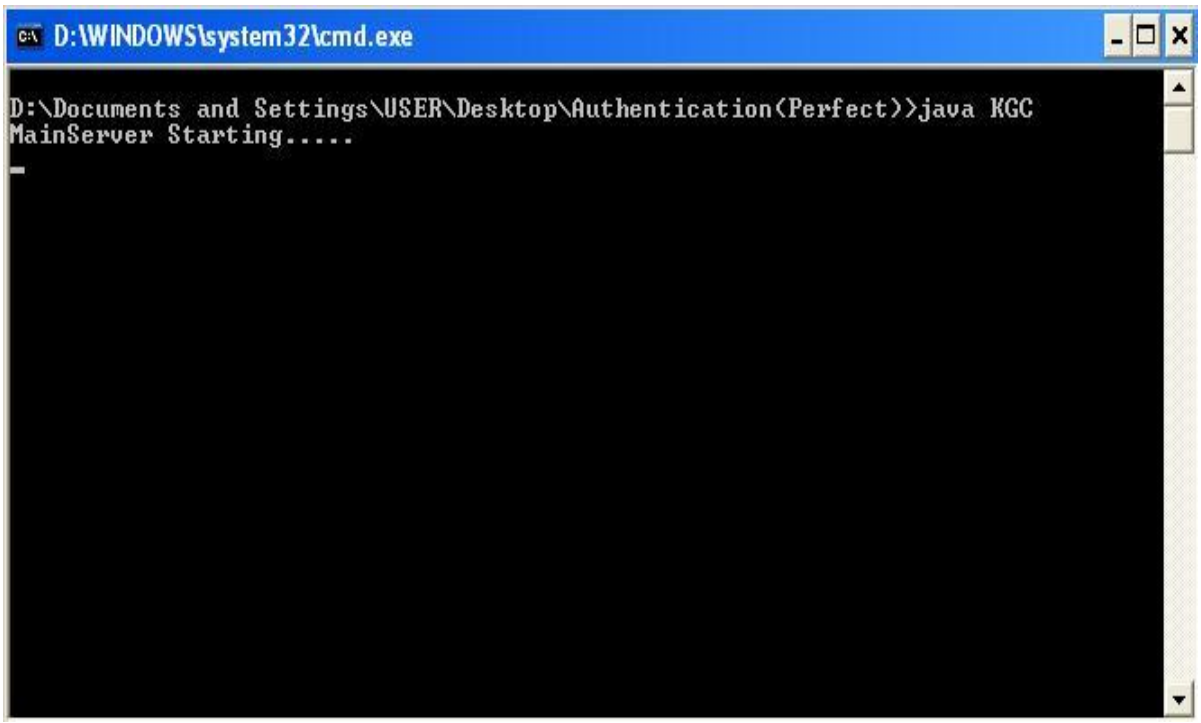

Fig. 4.1: Initialization of KGC server.

International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 10 , October 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The following Fig. 4.2 shows the registration of user A at KGC server.

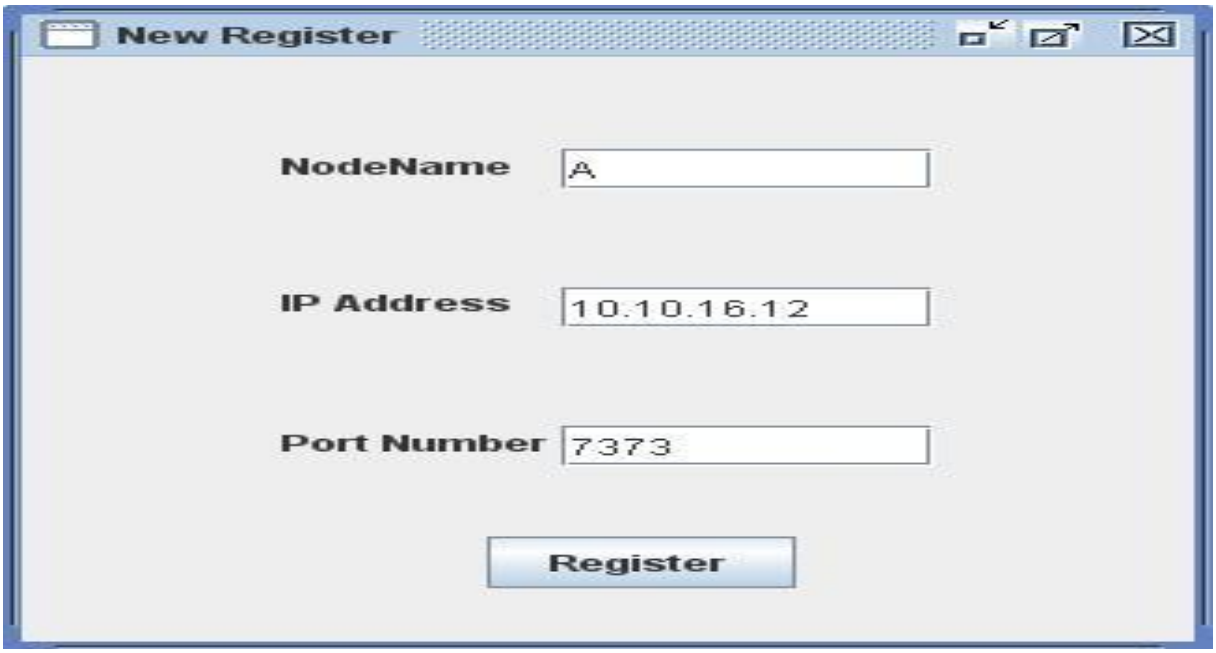

Fig. 4.2: Registration of user A at KGC server.

The following Fig. 4.3 shows user A sending group communication request to KGC server with a list of group members as {A,B,C}.

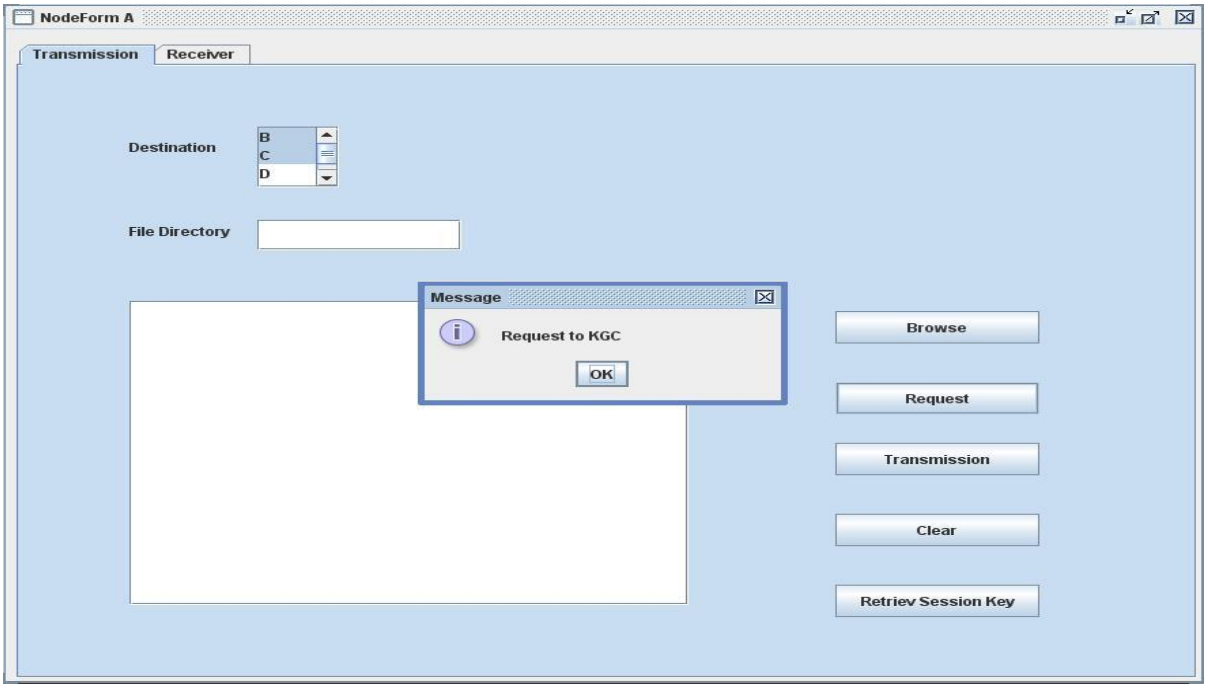

Fig. 4.3: Group communication request to KGC.

International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 10 , October 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The following Fig. 4.4 shows user A encrypting the first message using the initial common session key and sending the data to the users B and C.

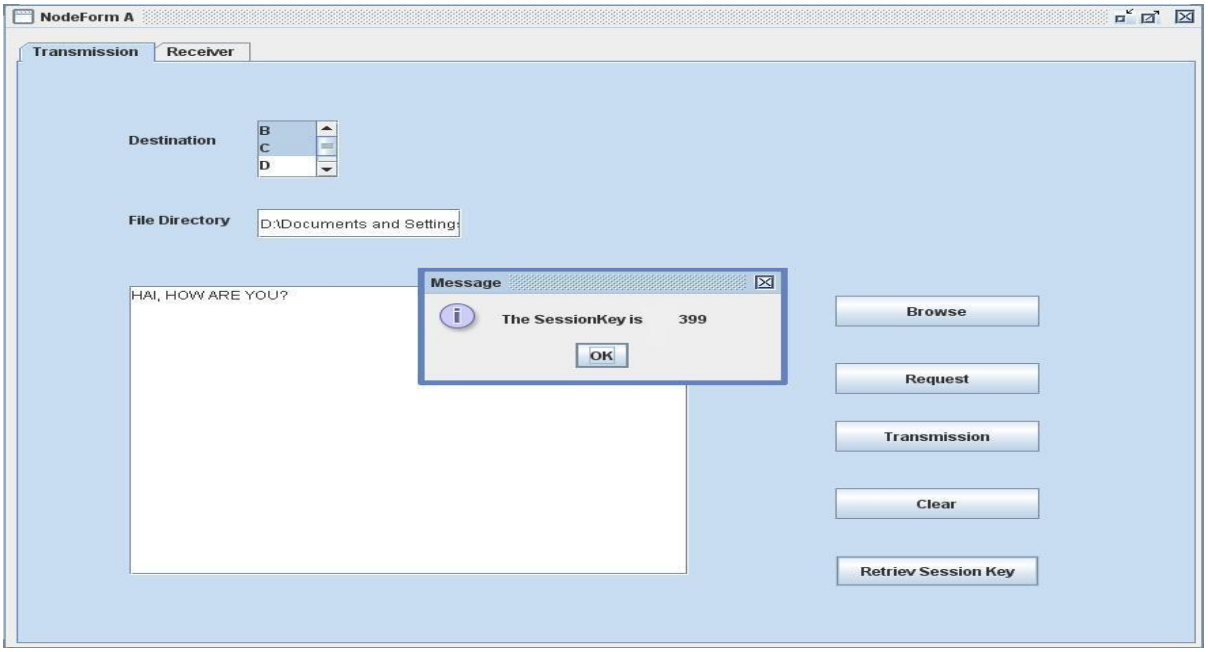

Fig. 4.4: Encryption of message using initial common session key.

The following Fig. 4.5 shows user B decrypting the message sent by user A using the initial common session key.

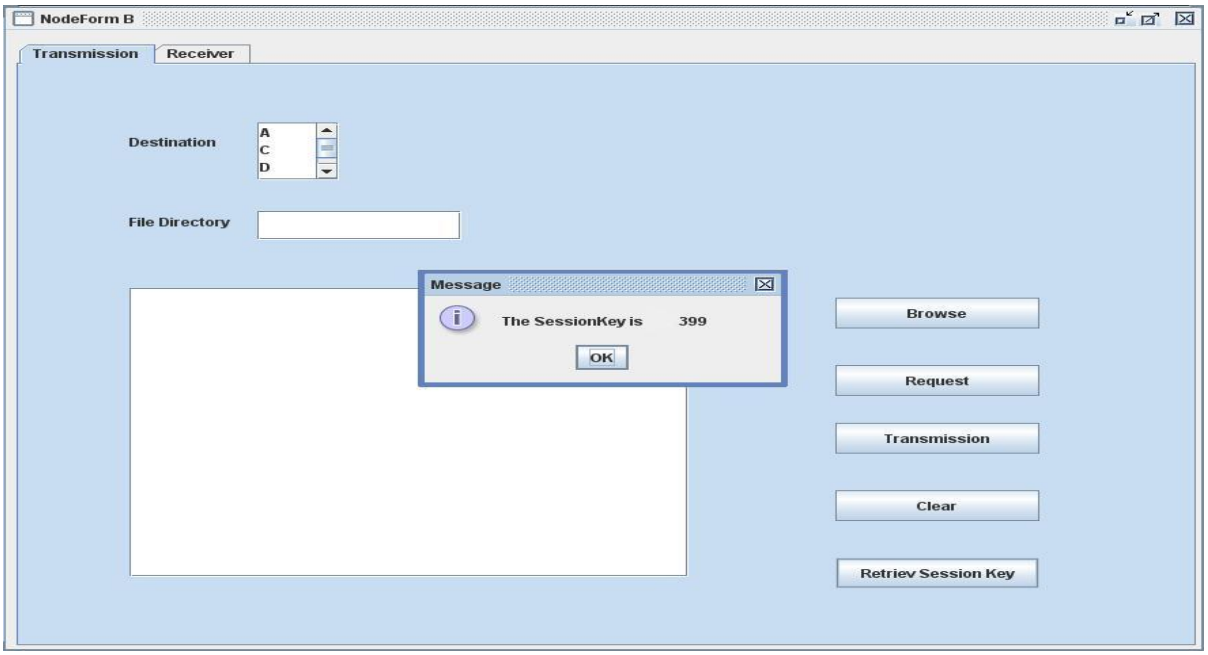

Fig. 4.5: Decryption of message using the initial common session key.

International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 10 , October 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The following Fig. 4.6 shows the message obtained at user B after decryption.

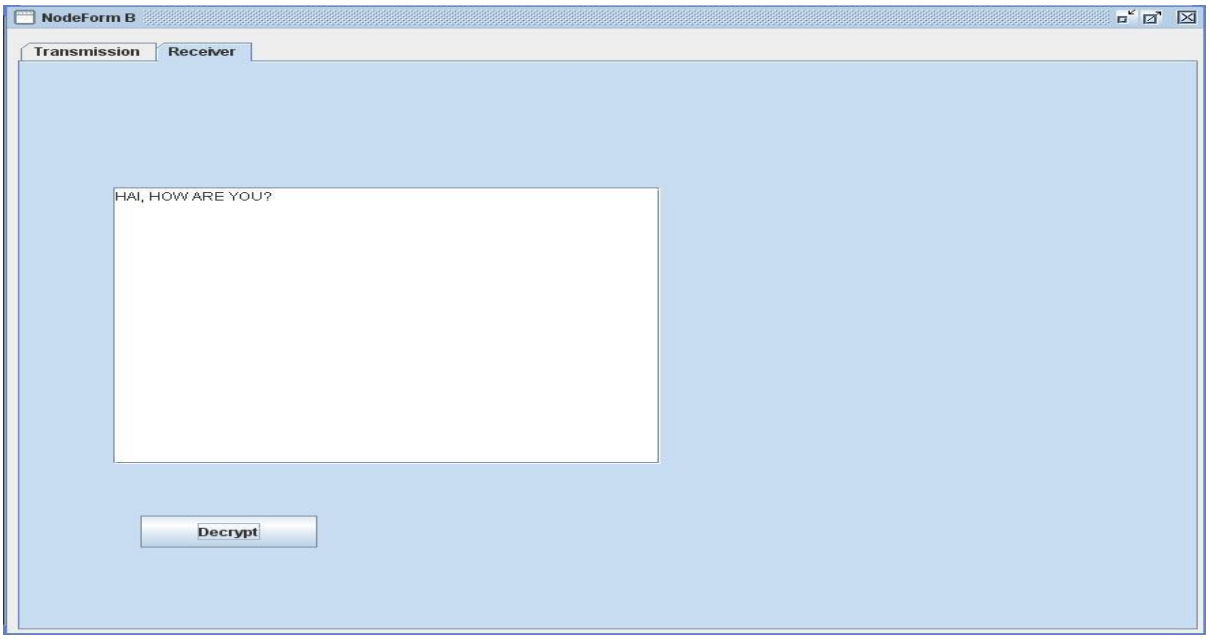

Fig. 4.6: The message obtained at user B after decryption.

The following Fig. 4.7 shows user A encrypting the second message using the new common session key and sending the data to the users B and C.

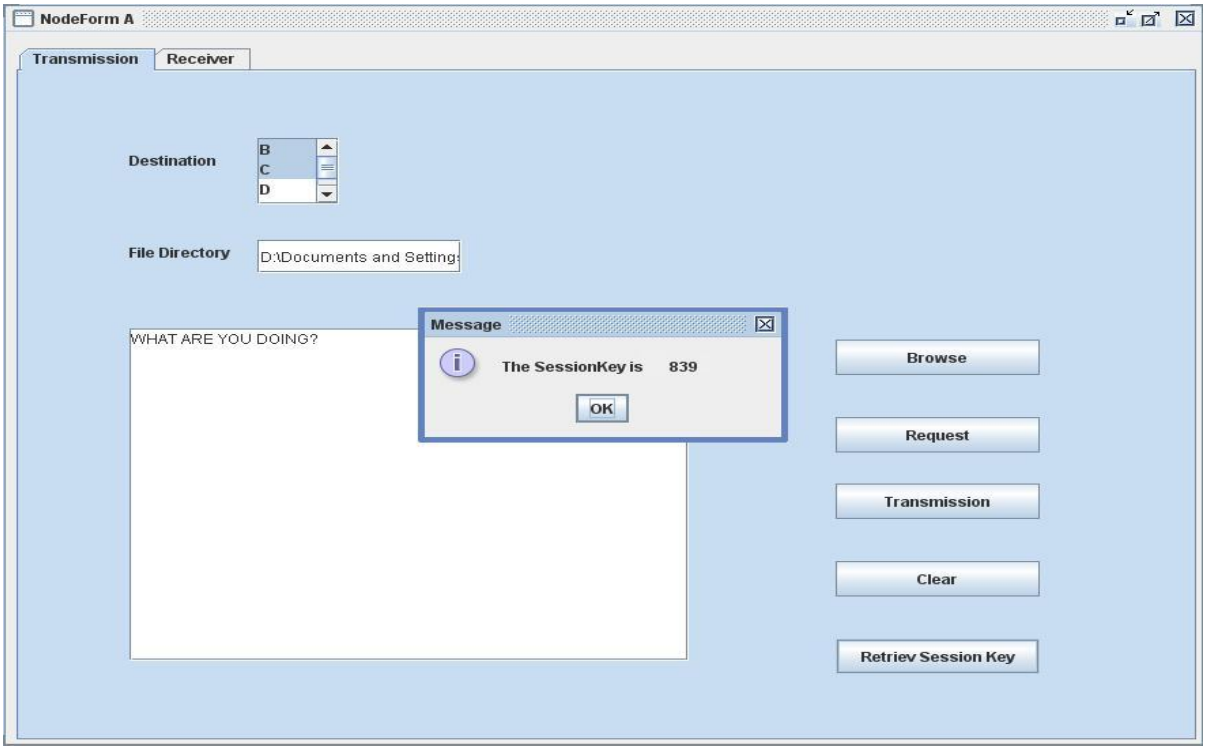

Fig. 4.7: Encryption of message using the new common session key.

International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 10 , October 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The following Fig. 4.8 shows user B decrypting the message sent by user A using the new common session key.

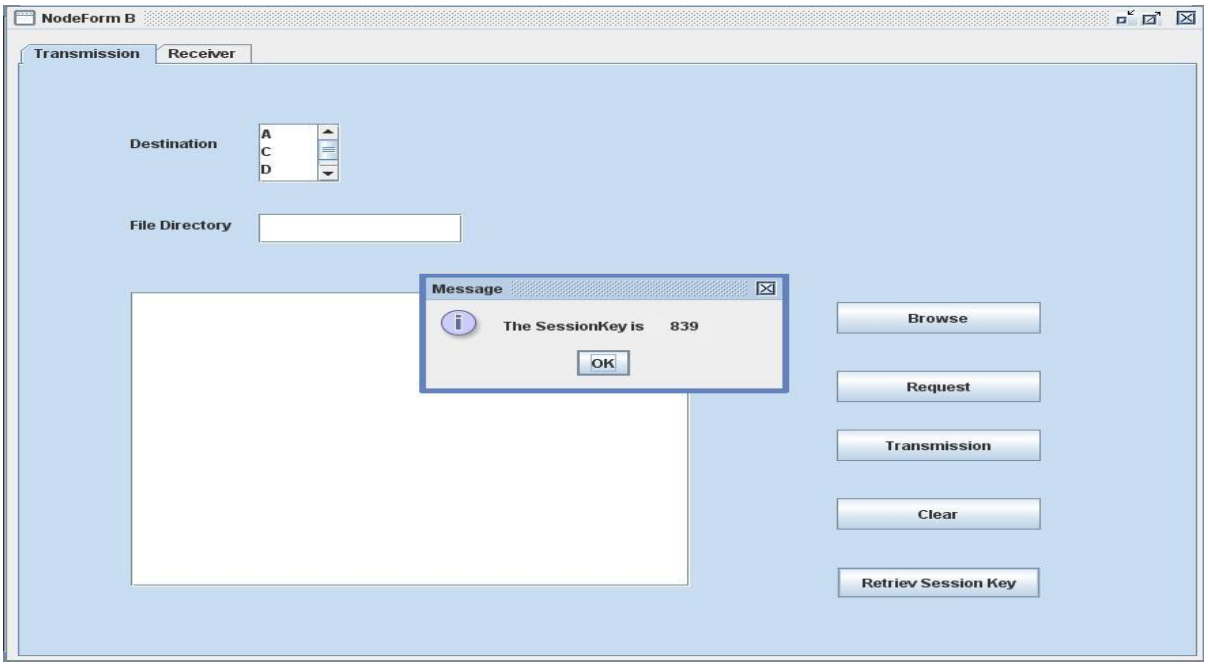

Fig. 4.8: Decryption of message using the new common session key.

The following Fig. 4.9 shows the message obtained at user B after decryption.

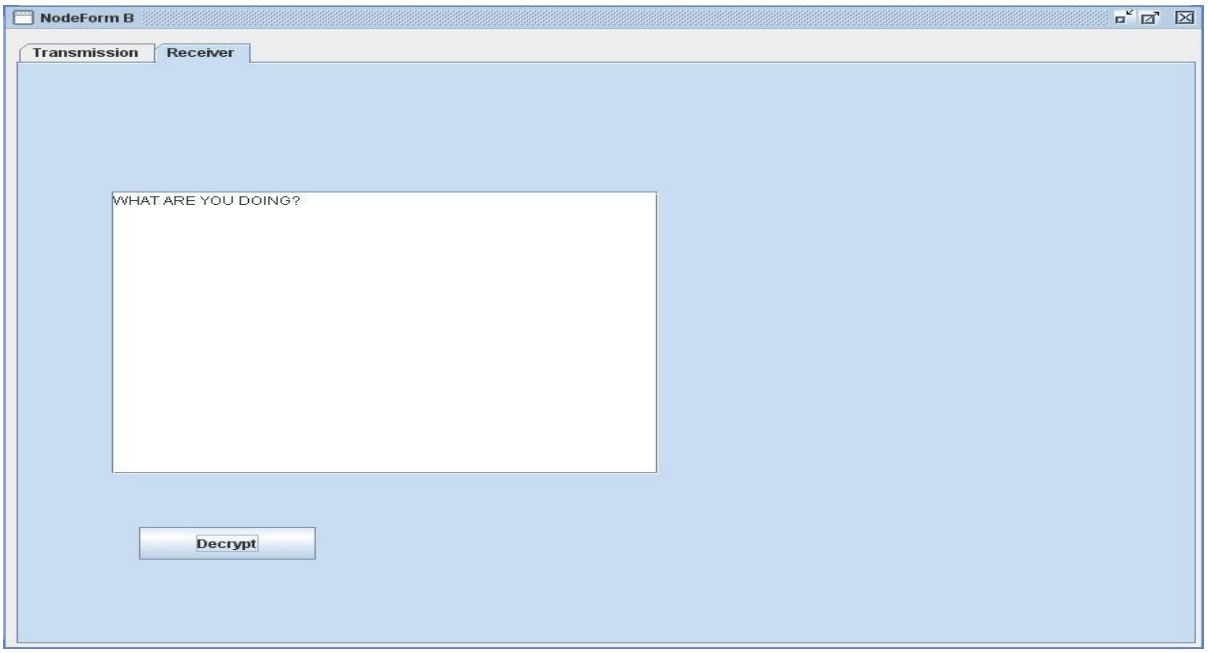

Fig. 4.9: The message obtained at user B after decryption.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The following Fig. 4.10 shows the identification of user D as unauthorized user as it is not included in the group for communication by the user A.

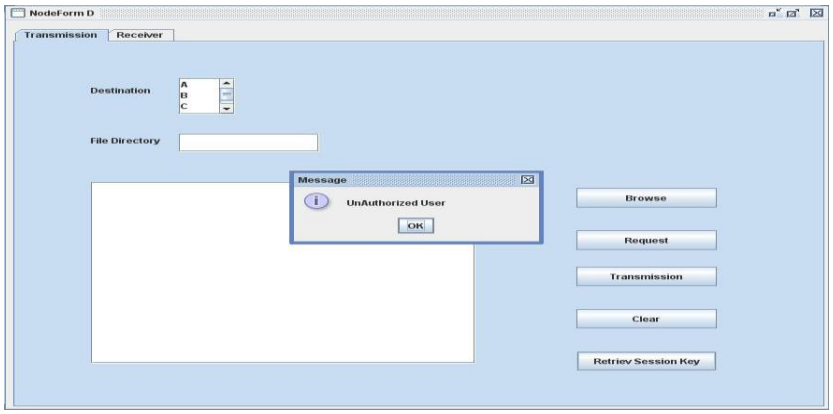

Fig. 4.10: Identification of unauthorised user.

V. CONCLUSION

We have proposed a novel key transfer protocol based on secret sharing scheme. Every user needs to register at the trusted KGC initially and preshare a secret with KGC. KGC broadcasts a set of key values to all group members at once by using the key transfer protocol. Only authorized group members can recover the set of key values and thus providing confidentiality and authentication. We have also proposed a method where the set of key values is used to generate multiple session keys which are used to encrypt / decrypt different messages during group communication, which is secure under chosen-plaintext attacks. The main security goals achieved by our system are key freshness, key confidentiality and key authentication.

REFERENCES

[1] R. Blom, "An Optimal Class of Symmetric Key Generation Systems," Proc. Eurocrypt '84 Workshop Advances in Cryptology, pp. 335-338, 1984.

[2] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly Secure Key Distribution for Dynamic Conferences," Information and Computation, vol. 146, no. 1, pp. 1-23, Oct. 1998.

[3] C. Boyd, "On Key Agreement and Conference Key Agreement," Proc. Second Australasian Conf. Information Security and Privacy (ACISP '97), pp. 294-302, 1997.

[4] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[5] A. Fiat and M. Naor, "Broadcast Encryption," Proc. 13th Ann. Int'l Cryptology Conf. Advances in Cryptology (Crypto '93), pp. 480-491, 1994.

[6] IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

[7] C. Laih, J. Lee, and L. Harn, "A New Threshold Scheme and Its Application in Designing the Conference Key Distribution Cryptosystem," Information Processing Letters, vol. 32, pp. 95-99, 1989.

[8] G. Saze, "Generation of Key Predistribution Schemes Using Secret Sharing Schemes," Discrete Applied Math., vol. 128, pp. 239-249, 2003.