ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

An Efficient Transmission over Cooperative Groups Using Hybrid Scheme

K.Banupriya[1]

M.E CSE, M.A.R College of Engineering and Technology, Trichirapalli, Tamilnadu, India[1]

ABSTRACT- The growth of group applications triggers the need for group-oriented security mechanisms over insecure network channels. The applications include IP telephony, collaborative work spaces, secure conferences, as well as dynamic coalitions common in law enforcement and disaster rescue scenarios. Standard security services required in such group settings, e.g., confidentiality of group-wide broadcasts can be very efficiently achieved if all group members share a group-wide secret key. The existing key management system used two approaches. One is Group key Agreement and another one is Key Distribution. Both approaches provided an unsecured data transmission and also very difficult to join a member in a remote system. It cannot deals with re-keying concept. In this paper, I proposed Hybrid of Group key agreement and public key broadcast encryption to Effective and Secure transmission of data to the remote cooperative groups. It provides fully secure data transmission and easy to join a new member in the existing system. In this approach, update the session key in a group easy.

KEYWORDS-Group key agreement, key distribution, cooperative groups, session key, and broadcast.

I. INTRODUCTION

As a result of the increased popularity of group-oriented applications and protocols, group communication occurs in many different settings: from network layer multicast to application layer tele- and video-conferencing. Regardless of the underlying environment, security services are necessary to provide communication privacy and integrity. In many newly emerging networks, there is a need to broadcast to remote cooperative groups using encrypted transmission. Examples can be found in access control in remote group communication arising in wireless mesh networks (WMNs), mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), etc.

The common problem is to enable a sender to securely transmit messages to a remote cooperative group. A solution to this problem must meet several constraints. First, the sender is remote and can be dynamic. Second, the transmission may cross various networks including open insecure networks before reaching the intended recipients. Third, the communication from the group members to the sender may be limited. Also, the sender may wish to choose only a subset of the group as the intended recipients. Furthermore, it is hard to resort to a fully trusted third party to secure the communication. In contrast to the above constraints, mitigating features are that the group members are cooperative and the communication among them is local and efficient, and also reduces the computation overhead and the communication costs are independent of the group size. The paper is simple that contains the efficient member deletion/ addition and also contains the rekeying concept. This paper exploits these mitigating features to facilitate remote access control of group-oriented communications without relying on a fully trusted secret key generation center.

A. Related Work

The major security concern in group oriented communications with access control is key management. The existing key management systems used two approaches. One is Group key agreement (or group key exchange by some

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

authors) which allows a group of users to negotiate a common secret key via open insecure networks. Then, any member can encrypt any confidential message with the shared secret key and only the group members can decrypt. And another one is key distribution systems (or the more powerful notion of broadcast encryption). In a key distribution system, a trusted and centralized key server presets and allocates the secret keys to potential users, such that only the privileged users can read the transmitted message. The early key distribution protocol [21] does not support member addition/deletion.

B. Contribution

Three aspects are important in our contribution. First, we formalize the problem of secure transmission to remote cooperative groups. We observe that the existing key management approaches do not provide effective solutions to this problem. On one hand, group key agreement provides an efficient solution to secure intragroup communication, but for a remote sender, it requires the sender to simultaneously stay online with the group members for multiple rounds of interactions to negotiate a common secret session key before transmitting any secret contents. On the other hand, broadcast encryption enables external senders to broadcast to noncooperative members of a preset group without requiring the sender to interact with the receivers before transmitting secret contents, but it relies on a centralized key server to generate and distribute secret keys for each group member. This implies that: 1) before a confidential broadcast channel is established, numerous confidential unicast channels from the key server to each potential receiver have to be constructed; and 2) the key server holding the secret key of each receiver can read all the communications and has to be fully trusted by any potential sender and the group members

Second, we propose the new approach is a hybrid of group key agreement and public-key broadcast encryption. In our approach, each group member has a public/ secret key pair. By knowing the public keys of the members, a remote sender can securely broadcast a secret session key to any intended subgroup chosen in an *ad hoc* way and simultaneously, any message can be encrypted to the intended receivers with the session key. Only the selected group members can together decrypt the secret session key and hence the encrypted message. In this way, the dependence on a fully trusted key server is eliminated. Also, the dynamics of the sender and the group members are coped with because the communication between the sender and the receivers before the transmission of messages is avoided and the communication from the group members to the remote sender is minimized.

Third, The new key management paradigm and perform extensive experiments in the context of mobile ad hoc networks. In the proposed protocol, after extraction of the public group encryption key in the first run, the subsequent encryption by the sender and the decryption by each receiver are both of constant complexity, even in the case of member changes or system updates for rekeying. As to security, the proposal is shown secure against an attacker colluding with all the nonintended members. Even such an attacker cannot get any useful information about the messages transmitted by the remote sender. The proof is given under a variant of the standard Decision Diffie–Hellman (DDH) assumption.

II. PROBLEM STATEMENT AND SYSTEM MODEL

A. Problem Statement

A group composed of N users, indicated by $\{u_1 \ldots u_N\}$. A sender would like to transmit secret messages to a receiver subset S of the N users, where the size S of is $n \leq N$. The problem is how to enable the sender to efficiently and securely finish the transmission with the following constraints.

1) It is hard to deploy a key generation authority fully trusted by all users and potential senders in open network settings.

2) The communication from the receivers to the sender is limited, e.g., in the battlefield communication setting.

3) N might be very large and up to millions, for instance, in vehicular ad hoc networks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

4) Both the sender and the receiver sets are dynamic due to *ad hoc* communication.

According to the application scenarios, there are also some mitigating features that may be exploited for solving the problem.

1) n is usually a small or medium value, e.g., less than 256.

2) The receivers are cooperative and communicated via efficient local (broadcast) channels.

3) A partially trusted authority, e.g., a public key infrastructure, is available to authenticate the receivers (and the senders).

B. System Model

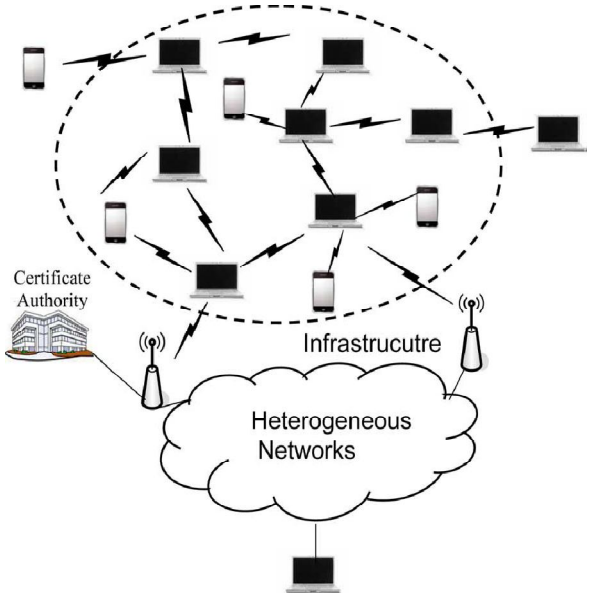

Fig. 1. System model.

The potential receivers are linked together with efficient local connections. Using communication infrastructures, they can also join to heterogeneous networks. Each receiver has a public/secret key pair. The public key is certified by a certificate authority, but the secret key is kept only by the receiver. A remote sender can get back the receiver's public key from the certificate authority and validate the authenticity of the public key by checking its certificate, which implies that no direct communication from the receivers to the sender is necessary. Then, the sender can send secret messages to any chosen subset of the receivers. We after that officially define the model of group key agreement based broadcast encryption. Since the heart of key management is to securely distribute a session key to the intended receivers, it is sufficient to define the system as a session key encapsulation mechanism. Then, the sender can at the same time encrypt any message under the session key, and only the intended receivers can decrypt.

III. KEY MANAGEMENT FOR TRANSMISSION TO REMOTE COOPERATIVE GROUPS

KeyGen: Each user i for i=1,..N randomly chooses $x_i \in z_p^*$ and computes $X_i = g^{x_i} \in G$

Encryption: Assume that a sender wishes to broadcast to users indexed by$\{i_1 .. i_n .\} \subseteq \{1 \dots N\}$. The sender runs the following algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

1) Randomly select $r, x_{i_0} \in z_p^*$ and compute
$$X_{i_0} = g^{x_{i_0}} \quad Y_{i_0} = \left(x_{i_1}/x_{i_n}\right)^{x_{i_0}} \quad c = g^r$$
2) Extract the public group encryption key $K = e(x_{i_1}, x_{i_2})e(x_{i_2}, x_{i_3}) \dots e(x_{i_{n-1}}, x_{i_n})$
3) Compute $S = ke(x_{i_n}, x_{i_0})e(x_{i_0}, x_{i_n})$
4) Compute the secret session key
$$k = S^r = e(g, g)^{xr}$$
5) Broadcast the header $Hdr = (X_{i_0}, Y_{i_0}, c)$

Decryption: The intended receivers run this algorithm as follows.

1) For j=1,…n, each receiver $u_{i_j} \in S$ publishes $Y_{i_j} = \left(X_{i_{j+1}}/X_{i_{j-1}}\right)^{x_{i_j}} = g^{\left(x_{i_{j+1}} - x_{i_{j-1}}\right)^{x_{i_j}}} \in G$
2) Each receiver indexed by i_j can compute the secret decryption key $d = X_{i_{j-1}}^{(n+1)x_{i_j}} Y_{i_j}^n Y_{i_{j+1}}^{n-1} \dots Y_{i_{j-2}}$
3) Using d , each receiver extracts the session key k from by computing
k =e(d,c)

Hence, k=e (d, c) = e (g, g) ^{xr}. This completes the correctness proof of the scheme.

IV. IMPLEMENTATION ISSUES

A. Member Organization

Several key management schemes arrange the users in a tree-based structure. However, for our proposal, it is preferable to organize them in a sequence and then use the sender to close the chain to form a logical ring. The chain can be formed by ordering the users lexicographically by the least important bits of their distinctive public keys.

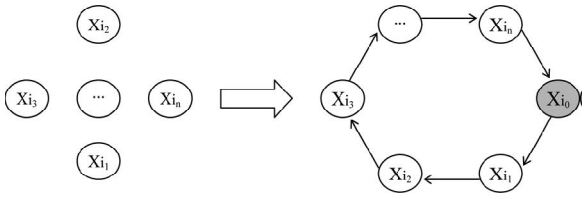

Fig. 2. Member organization.

A. Member Deletion/Addition and Group Partition/Merging
Member Deletion:

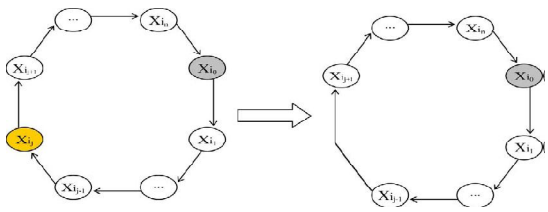

Fig. 3. Member deletion.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Encryption:

1) Randomly select $r', x_{i_0}' \in z_p^*$ and
$X_{i_0}' = g^{x_{i_0}'}, Y_{i0}' = \left(X_{i_1}/X_{i_n}\right)^{x_{i_0}'}, c = g^{r'}$
2) Compute the new public group encryption key $K' = \frac{Ke\left(X_{i_{j-1}}, X_{i_{j+1}}\right)}{e\left(X_{i_{j-1}}, X_{i_j}\right)e\left(X_{i_j}, X_{i_{j+1}}\right)}$
3) Compute $S' = K'e\left(X_{i_n}, X_{i_0}'\right)e\left(X_{i_0}', X_{i_1}\right)$
4) Compute the new secret session key $k' = (S')^{r'};$
5) Broadcast to the receivers the new header Hdr=X_{i_0}', Y_{i_0}', C'

Decryption:

1) According to Step 1 of the Decryption procedure of the basic protocol, receivers $u_{i_{j-1}}$ and $u_{i_{j+1}}$need to respond to the change in this step. They respectively publish $Y_{i_{j-1}}' = \left(X_{i_{j+1}}/X_{i_{j-2}}\right)^{x_{i_{j-1}}}$; $Y_{i_{j+1}}' = \left(X_{i_{j+2}}/X_{i_{j-1}}\right)^{x_{i_{j+1}}}$

2) Compute the new group decryption key
$d' = \left(X_{i_{t-1}}\right)^{nx_{i_t}}\left(Y_{i_t}'\right)^{n-1}\left(Y_{i_{t+1}}'\right)^{n-2} \ldots Y_{i_{t-2}}'$

3) Usingd', each receiver extracts the new session key $k'$from c' by computing $k' = e(d', c')$

Member Addition:

If the sender would like to include a new member u_{i^*}, the sender just needs to retrieve the public key $x_{i^*}$of this user and insert it into the public key chain of the current receiver set. Fig. 4 shows the addition of member u_{i^*}, to the receiver group.

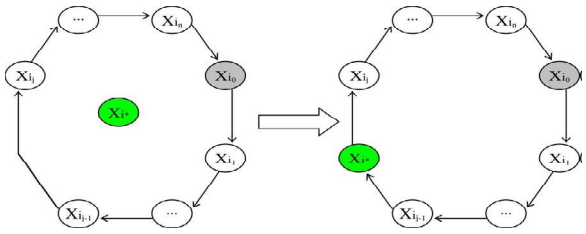

Fig. 4. Member addition.

Encryption:

1) Randomly select $r', x_{i_0}' \in z_p^*$ and
$X_{i_0}' = g^{x_{i_0}'}, Y_{i0}' = \left(X_{i_1}/X_{i_n}\right)^{x_{i_0}'}, c' = g^{r'}$
2) Compute the new public group encryption key $K' = \frac{Ke\left(X_{i_{j-1}}, X_{i_{j+1}}\right)e\left(X_{i^*}, X_{i_1}\right)}{e\left(X_{i_{j-1}}, X_{i_j}\right)}$
3) Compute $S' = K'e\left(X_{i_n}, X_{i_0}'\right)e\left(X_{i_0}', X_{i_1}\right)$
4) Compute the new secret session key $k' = (S')^{r'};$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

5) Broadcast to the receivers the new header Hdr=X'_{i_0}, Y'_{i_0}, C'

Decryption:

1) Only receivers$u_{i_{j-1}}, u_{i^*}$, and $u_{i_{j+1}}$ need to respond to the change in this step.

$$Y'_{i_{j-1}} = \left(X_{i^*}/X_{i_{j-2}}\right)^{x_{i_{j-1}}}$$

$$Y'_{i^*} = \left(X_{i_{j+1}}/X_{i_{j-1}}\right)^{x^*}$$

$$Y'_{i_{j+1}} = \left(X_{i_{j+2}}/X_{i_{j-1}}\right)^{x_{i_{j+1}}}$$

2) Compute the new group decryption key $d' = \left(X'_{i_{t-1}}\right)^{(n+2)x'_{iy}} \left(Y'_{i_t}\right)^{n+1} \left(Y'_{i_{t+1}}\right)^{n} \dots Y'_{i_{t-2}}$

3) Using d', each receiver extracts the new session key $k'$from c' by computing $k = e(d', c')$.

C. Re-keying

This approach can provide three levels of key update.

1. Session Key Update: This first level is to update the session key k. This key is used to encrypt digital contents to the receivers, and it expires after each session. To update the session key, the sender just needs to partially run Steps 1, 4, and 5 in the Encryption procedure. Receivers only need to execute Step 3 in the Decryption procedure. Note that Step 1 of is not necessary as the receivers have obtained d.

2. Group Decryption Key Update: The second level is to update the secret decryption key used by the receivers to compute the session key. To update the shared decryption key d, the sender only needs to run Steps 1 and 3–5 in the Encryption procedure.

Receivers only need to partially execute the three steps in the Decryption procedure.

3. Long-Term Secret Key Update: The third level is to update the secret key $x_i$of user u_i .

V.CONCLUSION

A new-fangled hybrid scheme is to allow send-and-leave broadcasts to remote cooperative groups without relying on a totally trusted third party. This scheme has been established secure in the normal replica. Methodical complexity psychoanalysis and extensive experiments show that this proposal is also efficient in terms of computation and communication.

REFERENCES

1. L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.
2. M. Burmester and Y. Desmedt, "A secure and efficient conference Key distribution system,"Adv. Cryptal.,vol.950, EUROCRYPT'94, LNCS, pp. 275–286, 1995.
3. M. Steiner, G. Tsudik, and M. Waidner, "Key agreement in dynamic peer groups," IEEE Trans. Parallel Distrib. Syst., vol. 11, no. 8, pp. 769–780, Aug. 2000.
4. M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The versa key framework: Versatile group key management," IEEE J. Sel. Areas Commun., vol. 17, no. 9, p. 1614–1631, Sep. 1999.
5. Q.Wu, J. Domingo-Ferrer, and U. González-Nicolás, "Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications," IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.
6. Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, "Secure group communication using robust contributory key agreement," IEEE Trans. Parallel Distrib. Syst., vol. 15, no. 5, pp. 468–480, May 2004.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

7. Y.-M. Huang, C.-H. Yeh, T.-I. Wang and H.-C. Chao, "Constructing Secure group communication over wireless ad hoc networks based on a virtual subnet model," IEEE wireless Commun., vol. 14, no. 5, pp. 71–75, Oct. 2007.

8. Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecture for multi-hop wireless mesh networks," IEEE J. Sel. Areas Commun, vol. 24, no. 10, pp. 1916–1928, Oct. 2006.