**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 3, Issue. 7, July 2014, pg.848 – 853*

**RESEARCH ARTICLE**

# Secure Member Key Management in Cooperative Group based Communication

**K.ChandraSekhar [1], T.Venkataramana [2]**

[1] Student, of CSE, Madanapalle Institute Of Technology & Science, JNTUA University, A.P, India

[2] Associate professor, Department of CSE, Madanapalle Institute Of Technology & Science, JNTUA University, A.P, India

chandu0540@gmail.com, venkataramana.t@gmail.com

***Abstract - In group communication the information is broadcasting from the multiple nodes at time. In the existed papers we can't achieve the fast transmission and communication we study on those problems of broadcasting. As to overcome these problems we used the various proven security algorithms and group key communication from some group. In that group we select any one node based on priority to send the secrete key distribution between sender and receivers. The existing key management system did not deal with these problems effectively and securely. In this it is easy to change the keys form cluster-head nodes to sub-nodes each and every intended nodes different keys are generated. Once we share the data first we can distribute the key from the head node to sub-nodes in this process we avoid the collisions and provide the security.***

***Keywords – Ad hoc networks, key generation, key distribution, broad casting, encryption and decryption***

## I. INTRODUCTION

MANET is a system made of wireless mobile nodes. These mobile nodes have wireless communication networks. MANETs have been projected those effective networking system providing the information exchange between the mobile nodes even without standard infrastructure. Mobile ad-hoc networks important to support group oriented communication in wireless nodes. In the above group communication, the sender enables to provide securely broadcast messages to the cooperative group. The solution to this problem the sender can be dynamic and may cross various networks in clearly open secure network before reaching the neighbor nodes. The group member may be limited, sender must choose the subset nodes/ intended nodes.

MANET is a type of Ad-hoc network that can change the positions and configure itself on the fly. MANETs are mobile nodes, they used to connect various networks. Thus can be a standard Wi-Fi connections.

 

Mobile ad hoc networks are a kind of networks that it can modify location and classify self-scheduled the fly. Ad hoc networks are mobiles utilize wireless connections to add to various network. It preserve exist a standard Wi-Fi connection or a new average such because a cellular's or protectorate message.

Mobile ad hoc network are unfinished to a limited region of wireless strategy such as a collection of laptops computer as others may be associated to the Internet. Because of the active life of mobile ad hoc network are usually not extremely protected it is significant to be careful what data is send more a mobile ad hoc network.

The router connectivity may modify normally, primary in the direction of the multi hop statement model allow message without the use of BSAP and give option relations within hotspot cell. MANET is type of ad hoc networks it can modify locality with arrange self on top of the fly. Every node in this network system is mobile and they use wireless connections to communication with different network

Routings are single of center troubles network used for deliver information beginning node to the additional. WAN are also called Mobile ad hoc multichip networks without fixed topology before personal organize. MANET can be characterizing as have a active, multi hop, potentially quick change topologies. The plan of such network is to supply communications capability to area by incomplete before no accessible message infrastructure.

Mobile ad hoc network is typically shaped through cellular phone node with wireless infrastructure. It use a peer to peer multi hop routed in its place of a fixed network communications to presents network connectivity.

The key agreement is easy to apply wireless sensor networks, mobile Ad-hoc networks, and cell phones. The key management technique is one of the challenging security issues in wireless sensor network and mobile Ad-hoc networks. Therefore, the energy efficient security will be a complicated issue. In order to generate multiple common secrete keys between the group communications.

## II. RELETED WORK

The main security problem in group-oriented communications with entry power is key management. The offered key management system is mainly proposed with two techniques they are group key agreement method and group key distribution system. Both are dynamic research areas in group networks. The group key agreement method allow group of keys exchanged by one node to another node. In the key agreement method allow a group of users to share a private key apprehensive network. Here any member can encrypt data and secret messages with the shared private key and only grouping members can decrypt the data. In This way, a secret intragroup broadcast channel can be recognized without relying on a central key server to create and distribute secrete keys to the possible nodes. In the existing system allow capable member joins or removes but the cost for a member remove is still relatively elevated. Hierarchy key arrangement has been further planned and enhanced to reach improved effectiveness for user joints and leaves. The hypothetical analysis improves the tree based group key agreement method.

In key sharing, the person is dependable for providing the creating and distribute the group key is either a remote node, such as a suitably elected group node. In the key distribution systems a TTP key server presents and allocate the private or secrete keys to the possible nodes, such that only the certified user can read the transmit data or transmit messages. The existing distribution method does not support the node joins/leaves after the structure is deployed.

This process was consequently evolve to permit the dispatcher to early choose the proposed recipients subset of the primary group, which is generally referred to as transmit encryption. The transmit encryption is needed for key management system distribution. Transmit encryption schemes classified into two types. One is symmetric key transmit encryption and another one is unrestricted key transmit encryption. In the symmetric key transmit encryption, only the trusted third party creates the all the secrete keys and transmit the messages to the users, here the key production hub can be act as a sender. In the public key transmit encryption the secrete keys for each users, the trusted party also generates a public keys for the all users so any one can collaborate the major role of dispatcher. Similarly to the set key agreement, hierarchy based key structure were consequently proposed to recover the efficiency in transmit encryption systems.

The public key transmit encryption scheme was presented that has more difficulty in key range, cipher text size, and calculation cost, where is the highest number of allowable possible receivers. The present method reduces the range of key and the cipher texts.

## III. CONTRIBUTION

Wireless mobile ad-hoc networks have newly recommended as a high speed internet access. Each user in the wireless network directly communicates with the other nodes without backbone network. The key management model can't access to the group key. So the neighboring nodes easy to access the information. Unavailability of a trusted third party keys.

In Proposed system the new key management paradigm Algorithm technique is used. Discrete Logarithm Attack-It is very difficult to deal with discrete logarithm problem based on the security of the key exchange.

Man In The Middle Attack -The access can be done between source and destination with the help of the intermediates. The intermediates who alter the original message received from the source and sends to the destination. The proposed scheme will overcome the problem in the existing system. In Network Security the several techniques are used to provide the security threats. New key management paradigm is one of the techniques. Set of mobile nodes form subgroup. The Diffie-Hellman key exchange is a key exchange protocol and not used for encryption. The cluster head node is a globalized node for all subgroup nodes. It should contain all subgroup nodes private and public keys. The cluster head node encrypts the data and the intended nodes decrypt the data using public keys. In this process CA distribute the public keys to sub-

 

nodes. The communication of subgroup nodes are all comes under the cluster head node knowledge. So there is no attack possible to enter while the communication between the nodes.

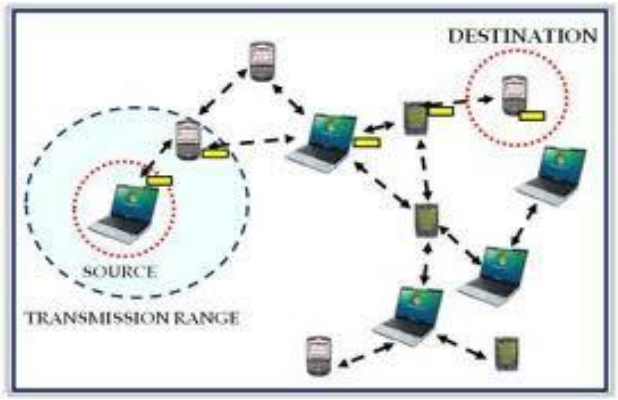


**FIG 1: Architecture**

- The dispatcher is isolated and can be energetic.
- The secrete key is distributed between the group nodes and sub group nodes and sub-sub group nodes but not used for encryption and decryption.
- The broadcast may cross a variety of networks including open apprehensive networks before getting the proposed recipients.
- Easy to change the rekeys or update the keys.
- Each node share energy levels automatically.
- Data compression techniques are applicable.

### *A. Group key Generation Algorithm*

Step 1: Select two prime numbers p and q.

Step2: calculate n such that n=pq.

Step3: find the totient of n, $\phi(n)$

$$\phi(n)=(p-1)(q-1).$$

Step4: choose an e such that $1 < e < \phi(n)$.

Step5: determine d(modular arithmetic) which satisfies the congruence relation

$$De \equiv 1 \pmod{\phi(n)}.$$

### *B. Key Distribution Algorithm*

Step1: can't be used to exchange an arbitrary message

Step2: rather it can establish a common key

Step3: known only to the two participants

Step4: whose value depends on the participants

Step5: based on exponentiation takes $O((\log n))^3$

Step6: nb discrete logarithms takes $O(e^{\log n \log \log n})$ operations.

## IV. IMPLEMENTATION ISSUES

### A. Network Environment Setup Module:

In the first module, we create the network environment setup with nodes, certificate authority. Network environment is set up with nodes connected with all and using socket programming in java.

### *B. Certificate Authority Module:*

In this module, each receiver contains public/private key pair. This public key is certified by the CA but private key is kept only maintain the receiver. Each and every member trusts the Certified Authority and can verify the CA's signature, each and every member can also assume that the certain public keys indeed belongs to whoever is identified in the certificate. The certificate authority(CA) works as an organization that stores public keys and their owners and every party in a communication trusts this organization. Which shows that no direct communication from the sender to the receivers is necessary, then the sender can send the secret information to the receivers.

### *C. Key Broadcast Module:*

In this module formally define the model of group key agreement protocol. In this module the public key is shared by intended group members only. Implicitly, group key agreement protocol provides the mutual group key authentication and the authentication is direct between the group members. Rather than directly broadcast the data into qualified members, broadcast key schemes distribute keying information that permits only qualified members. The remaining members do not receive the distributed key, these members are not qualified. Because in group communication key distributes qualified members only. In this module, the third party in our key management model is only partially trusted. In other words the third party knows public keys and certifies the public key of each group member. This type of partial trusted third parry implementation is known as public key infrastructure(PKI) in open secure networks. In this key broadcasting increases any attacker's needed effort, the key should be frequently changed each and every intended group communication. The key should be broadcasted to each and every group member.

 

### *D. Group Key management*

Group key management means managing the keys in a group communication. Mostly the group communications used in multicast communication so that the message is send by single sender and received my multiple users at a time. The main problem in multicast group communication is it's security so in order to improve the security we use the discrete logarithmatic problem and key distributing protocols. Here we are distributing the single key into the intended nodes or subgroup nodes. In multi group communication the cluster head node is responsible for generating and updating keys. The cluster members receiving the keys and broadcasting the data into one cluster node to another cluster nodes. In group key agreement protocols, the sender has to stay on the online with the receivers and the direct communication between the receivers to sender is required. This is difficult for cluster head node. But in our new key paradigm there is no direct communication between the receivers to the sender because the sender receives the public keys from the third party so here there is no direct communication. This module also shows the node/member addition and deletion.

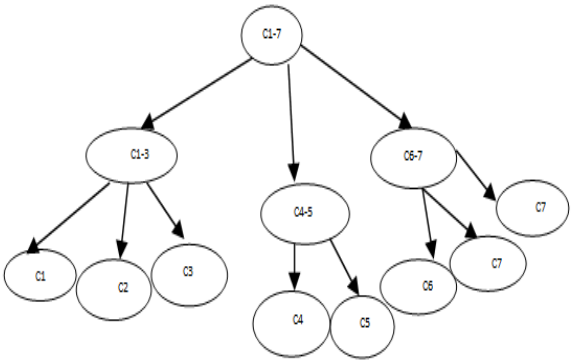


**Fig 2: hierarchical key structure**

### *E. Encryption and Decryption*

Conversion of data into a secret code. The encryption is the effective way to achieve data security. To read these encrypted file, you must access to a secrete key . The unencrypted data is called plain text ,and encrypted data is called cipher text. Encryption is essential for ensured and trusted delivery of sensitive information

There are two types of encryption techniques: asymmetric encryption and symmetric encryption. The asymmetric encryption is also known as public key encryption. In this encryption the public key known to everyone and private/secrete key known only the recipient of the message. Symmetric encryption where the same key is used to encrypt and decrypt the message. This is differs from asymmetric encryption. The encryption technique is commonly used in protecting the information within the many civilian systems.

This decryption is jointly run by intended receivers to extract the secrete key through encryption back to its unencrypted form. The decryption may be accomplished automatically or manually. It is performed by set of keys received by the intended receivers.

## V. CONCLUSION

In group communication in Ad-hoc network is a challenging task. In this paper we provide the secure key management in group communication using key distribution protocol in ad-hoc networks. In this group communication we distribute the keys from cluster-head nodes to sub-nodes in ad-hoc networks this is one of the most important service in ad-hoc networks. Any challenge in secure group communication will reduce group rekeying. So how to modify group key securely and efficiently in secure group communication into the group key management paradigm.

## VI. FUTURE WORK

In future discuss the different types of nodes like leaving a subgroup. Sometimes cluster head node is leaving in cluster at that time we select the new cluster head node based on the above process and send the information to all the sub-nodes in Ad-hoc networks.

## References

[1] Quinhong Wu**,** Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Fellow and Jesus A.Manjon "Fast Transmission to Remote Cooerative Group: A New Key Management Paradigm," IEEE/ACM Trans. Netw., vol. 21, no. 2, April. 2013.

[2] W.Trappe, Y.Wang, andK. J. R.Liu**, "**Resource-aware conference key establishment for heterogeneous networks," IEEE/ACM Trans. Netw., vol. 13, no. 1, pp. 134–146, Feb. 2005.

[3] M. Abdalla, Y. Shavitt, and A. Wool**, "**Key management for restricted multicast using transmit encryption," IEEE/ACM Trans. Netw., vol.8, no. 4, pp. 443–454, Aug. 2000.

[4] B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu, and S. Guizani, "A pyramidal security model for large-scale group-oriented computing in mobile ad

 

hoc networks: The key management study," IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 398–408, Jan. 2009.

[5] 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.

[6] 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.

[7] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1569–1589, Oct. 2007.

[8] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," Adv. Cryptol., vol. 950, EUROCRYPT'94, LNCS, pp. 275–286, 1995.

[9] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The versakey framework: Versatile group key management," IEEE J. Sel. Areas Commun., vol. 17, no. 9, pp. 1614–1631, Sep. 1999.

[10] 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.

[11] A. Sherman and D. McGrew, "Key establishment in large dynamic groups using one-way function trees," IEEE Trans. Softw. Eng., vol. 29, no. 5, pp. 444–458, May 2003.

[12] 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.

[13] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," Trans. Inf. Syst. Security, vol. 7, no. 1, pp. 60–96, Feb. 2004.

[14] Y. Sun,W. Trappe, and K. J. R. Liu, "A scalablemulticast keymanagement scheme for heterogeneous wireless networks," IEEE/ACMTrans. Netw., vol. 12, no. 4, pp. 653–666, Aug. 2004.

[15] W.Trappe, Y.Wang, andK. J. R.Liu, "Resource-aware conference key establishment for heterogeneous networks," IEEE/ACM Trans. Netw., vol. 13, no. 1, pp. 134–146, Feb. 2005.

[16] P. P. C. Lee, J. C. S. Lui, and D. K. Y. Yau, "Distributed collaborative key agreement and authentication protocols for dynamic peer groups," IEEE/ACM Trans. Netw., vol. 14, no. 2, pp. 263–276, Apr. 2006.

[17] Y. Mao, Y. Sun, M. Wu, and K. J. R. Liu, "JET: Dynamic join-exittree amortization and scheduling for contributory key management," IEEE/ACM Trans. Netw., vol. 14, no. 5, pp. 1128–1140, Oct. 2006.

[18] W. Yu, Y. Sun, and K. J. R. Liu, "Optimizing the rekeying cost for contributory group key agreement schemes," IEEE Trans. Depend. Secure Comput., vol. 4, no. 3, pp. 228–242, Jul.–Sep. 2007.

[19] R. Dutta and R. Barua, "Provably secure constant round contributory group key agreement in dynamic setting," IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2007–2025, May 2008.

[20] J. Snoeyink, S. Suri, and G. Varghese, "A lower bound for multicast key distribution," Proc. IEEE INFOCOM, pp. 422–431, 2001.

[21] I. Ingemarsson, D. T. Tang, and C. K.Wong, "A conference on key distribution system," IEEE Trans. Inf. Theory, vol. 28, no. 5, pp. 714–720, Sep. 1982.

[22] M. Abdalla, Y. Shavitt, and A. Wool, "Key management for restricted multicast using broadcast encryption," IEEE/ACM Trans. Netw., vol. 8, no. 4, pp. 443–454, Aug. 2000.

[23] B. M. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting," Proc. IEEE, vol. 83, no. 6, pp. 944–957, Jun. 1995.

 

[24] J. Lotspiech, S. Nusser, and F. Pestoni, "Anonymous trust: Digital rights management using broadcast encryption," Proc. IEEE, vol. 92, no. 6, pp. 898–909, Jun. 2004.

[25] A. Fiat and M. Naor, "Broadcast encryption," Adv. Cryptol., vol. 773, CRYPTO'93, LNCS, pp. 480–491, 1993.

[26] C. K. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," IEEE/ACM Trans. Netw., vol. 8, no. 1, pp. 16–30, Feb. 2000.

[27] D. Halevi and A. Shamir, "The LSD broadcast encryption scheme," Adv. Cryptol., vol. 2442, CRYPTO'02, LNCS, pp. 47–60, 2002.

[28] J. H. Cheon, N.-S. Jho, M.-H. Kim, and E. S. Yoo, "Skipping, cascade, and combined chain schemes for broadcast encryption," IEEE Trans. Inf. Theory, vol. 54, no. 11, pp. 5155–5171, Nov. 2008.

[29] M. Naor and B. Pinkas, "Efficient trace and revoke schemes," in Proc. 4th FC, 2001, vol. 1962, pp. 1–20.

[30] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," Adv. Cryptol., vol. 3621, CRYPTO'05, LNCS, pp. 258–275, 2005.

[31] J.-H. Park, H.-J. Kim,M.-H. Sung, and D.-H. Lee, "Public key broadcast encryption schemes with shorter transmissions," IEEE Trans. Broadcast., vol. 54, no. 3, pp. 401–411, Sep. 2008.

[32] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," Adv. Cryptol., vol. 5479, EUROCRYPT' 09, LNCS, pp. 171–188, 2009.

[33] Q.Wu,Y.Mu, W. Susilo, B.Qin, and J. Domingo-Ferrer, "Asymmetric group key agreement," Adv. Cryptol., vol. 5479, EUROCRYPT'09, LNCS, pp. 153–170, 2009.

[34] Q.Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, and O. Farràs, "Bridging broadcast encryption and group key agreement," Adv. Cryptol., vol. 7073, ASIACRYPT'11, LNCS, pp. 143–160, 2011.

[35] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," Adv. Cryptol., vol. 1666, CRYPTO'99, LNCS, pp. 537–554, 1999.

[36] D. Boneh and M. Franklin, "Identity based encryption from the weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.

[37] E. Bresson, Y. Lakhnech, L. Mazaré, and B. Warinschi, "A generalization of DDH with applications to protocol analysis and computational soundness," Adv, Cryptol,, vol. 4622, CRYPTO'07, LNCS, pp. 482–499, 2007.

 