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. 2, February 2014, pg.197 – 201

RESEARCH ARTICLE

A New Key Management Paradigm for Fast Transmission in Remote Co-operative Groups

M.VIJAYAKUMAR[#1] **V.PRIYA DHARSHINI**[#2] **Dr.C.SELVAN**[#3]

[1]Student, Department of CSE, Sri Eshwar College of Engineering, Coimbatore, India

[2]Student, Department of CSE, Sri Eshwar College of Engineering, Coimbatore, India

[3]Associate Professor, Department of CSE, Sri Eshwar College of Engineering, Coimbatore, India

[1] vijayakumarmecse@gmail.com, [2] priyaviswa31@gmail.com, [3] selvan.coimbatore@gmail.com

Abstract-In Emerging technology Mobile adhoc network (MANET) is widely used many areas, successfully to achieve fast transmission and communication. But it cannot achieve fast transmission /broadcasting in Remote Area. To overcome this problem new key management paradigm technique is used. In this proposed method the new key management paradigm form some group. In that group select any one of the node / system based on that priority to send the secret key distribution between sender and receiver to improve fast data transmission in remote Area. Each and every data transmission, secret key will be generated and also should be updated. In that remote area hackers should theft the data, so give protection against the unauthorized person. Using key updating method transmit the data fast, reliable and more securable manner. To create Co-operative groups using a new Key management paradigm in Remote Area. The Computation overhead and Communication Cost are independent of group size. Using rekeying strategies efficient way to achieve any number of addition / deletion process will be carried out and as well as strong security against the collision in that remote Area.

Index Terms – Key Management, Manet, Secret Key, Cooperative Groups, Rekey

I.INTRODUCTION

MANETs are planned to function good networking system facilitating information exchange between mobile devices without fixed infrastructures. It's most important to support group-oriented applications, audio/video conference and one-to-many data dissemination in battlefield or disaster rescue scenarios. Wireless network communication is broadcast and a certain amount of devices can receive transmitted messages, the risk of unsecured sensitive information being intercepted by unintended recipients is a real concerned. So MANET, VANET having in same near future.

This network communication is hard to resort hard to resort to a fully trusted third party to secure the communication. And then the group members are cooperative and the communication among them is local and efficiently. A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. The traffic types in ad hoc networks are quite different from those in an infrastructure wireless network [3].

A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. A Mobile ad hoc Network (MANET) is a self-configuring infrastructure network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose".

II.RELATED WORK

Bo Rong et al [9] describes in mobile ad hoc networks (MANETs), many application secure group-oriented computing among a large number of nodes in an adversarial environment. To deploy these large scale cooperative applications, secure multicast service must be provided to efficiently and safely exchange data among nodes.

Yamir Amir et al [8] describes each secure group has a trusted key server responsible for generating and securely distributing keys. Specifically, the trusted server knows user set *U*, key set *K*, and user–key relation *R*. Every user in *U* has a key in *K* called its individual key, which is shared only with the trusted server for pair wise confidential communication with the trusted server. There is a group key in *K* shared by the trusted server and all the users in *U*. The group key can be utilized by each user to confidentially send messages to other members of the group. Keys other than the individual key and group key are named auxiliary keys.

Group-oriented computing in MANET a typical scenario of dynamic multicast, since wireless nodes are free to move and are thus likely to frequently join or leave the cooperation domain. The second issue requires a successful deployment of security protocols, which further depends on the underlying key management solution. A number of key management schemes have been proposed for single-security-level group communication

III.PROPOSED TECHNIQUE

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 cluster head node is a globalised node for all subgroup nodes. It should contain all subgroup nodes private and public keys. 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.The cluster head will notify whether the node is eligible to add the sub group or not. In proposed techniques have following technique

System Model, Key Management, Member Organization, Key Pre distribution Phase in dynamic key management

System Model

In this Module create nodes and made ad hoc network. Each and every node has to generate public and secret key. And allocate a certificate authority person to provide certificate for public key during data transmission but he does not have secret key, receiver only have that secrete key. The remote sender can retrieve the receiver's public key for checking and validate through certificate authority.

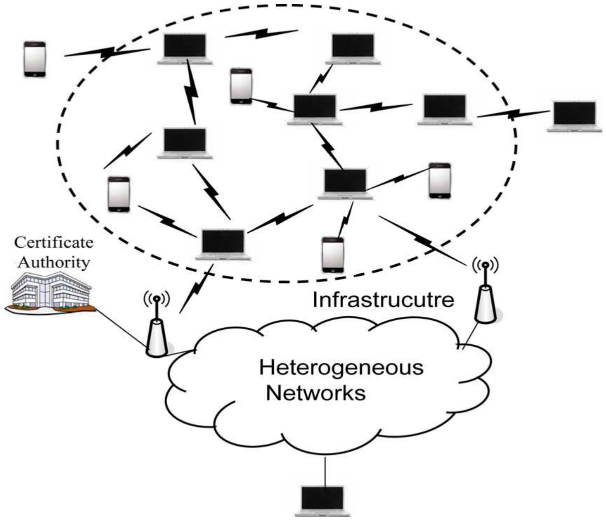


Figure 1. System Model Architecture

Key Management

The major security concern in group-oriented communications with access control is key management. The key management paradigm al-lowing secure and efficient transmissions to remote cooperative groups by effectively exploiting the mitigating features and circumventing the constraints. This system 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 simultaneously encrypt any message under the session key, and only the intended receivers can decrypt.

Member Organization

Organize the nodes in the network. Each and every node should managed by Group Manager. Whenever the nodes want to move from one place to another place, they can easily move with the permission of group manager. Any node want to add in the network or group, the group manager should allow the new node in the group. Doing this process, we can easily manage the network members and avoid unwanted nodes.

Key Updating Process

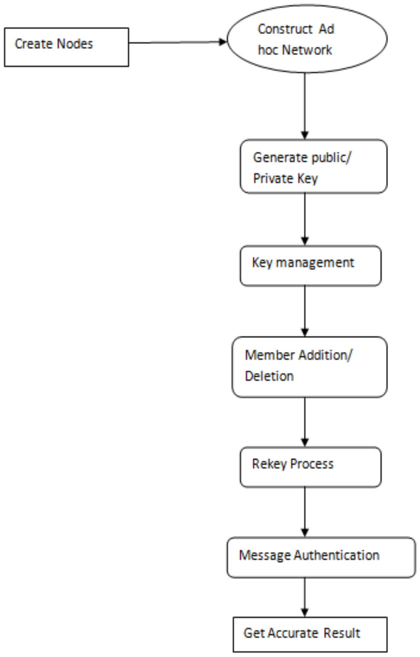
In this process, whenever happened nodes addition and deletion, the key should rekey in the group and the network. Updating the long-term secret key of a member causes more overhead than updating her session key or her group decryption key, although the long-term secret key update process described is still much more efficient than a completely new run of the protocol.

Key Pre distribution Phase in dynamic key management

In proposed scheme an authentication key *K*CHAuth is a pair of public/private key *K*pt/*K*st and a certificate CertCHt signed by the base station are pre distributed in each cluster head. The authentication key *K*CHAuth is used to verify member sensor node identities. *K*CHAuth is known to all cluster heads and the base station. The public/private key pair *K*pt/*K*st is used to establish pair wise keys among cluster heads. An authentication key *K*Authi and the public key *K*PBS of the base station are pre distributed in each member sensor node. *K*PBS is used to verify the certificates of the cluster heads. *K*Authi can be calculated by the following hash function:

$$\boldsymbol{K\text{Authi} = H\ (\text{ID}i||K\text{CHAuth})}$$

System Design Flow Diagram



In this process first we create node and then generate pair wise key .The pair wise key include private and public keys. The cluster head generate key management. It will independent on membership addition and deletion of the node. If incase the pair wise key not satisfy the cluster head key generation means ,The cluster head will intimated to the particular node to perform the rekey strategies. Now the information is authenticated and transfer in secure manner.

IV .CONCLUSION

A new key management paradigm to enable send-and-leave broadcasts to remote cooperative groups without relying on a fully trusted third party. Our scheme has been proven secure in the standard model. A thorough complexity analysis and extensive experiments show that our proposal is also efficient in terms of computation and communication. These features render our scheme a promising solution to group-oriented communication with access control in various types of ad hoc networks. And also proposed key pre distribution in key management process for rekey when happened the nodes addition / deletion. During data transmission we were implemented crypto system and authentication process. This process makes an efficient and effective fast transmission in the Ad Hoc Network.

REFERENCES

[1] Bo Rong,Hsiao-Hwa Chen,Yi Qian,Kejie Lu,Rose Qingyang Hu,Sghaie Guizani ,” Peace: A Novel Privacy-Enhanced Yet Accountable Security Framework For Metropolitan Wireless Mesh Networks”, February 2010.

[2] L.Zhang , Q.Wu , A.Solanas ,and J.Domingo –Ferrrer, ” Balanced Trust worthiness safety and privacy in vehicle communications”, IEEE Trans, veh. Technol.., vol.59, no.4, pp.1606 – 1617, May 2010.

[3] M.Scott,”On the efficient implementation of pairing-based protocols”, 2011. Available :http://eprint.iacr.org/2011/334.pdf

[4] Patrick P.C Lee,John C.S.Lui,David K.Y.Yau ,” Distributed Collaborative Key Agreement And Authentication Protocols For Dynamic Peer Groups”, March 2010.

[5] Q.Wu.B.Qin,L.Zhang, J.DomingoFerrer,” & O.Farras, ”Bridging Broadcast Encryption & group key agreement”, Adv.Cryptol., vol.7073, ACIACRYPT 11,LNCS.pp 143-160.2011.

[6] Qianhong wu, Lei zhang & jesus A.Manjon , **“**Fast Transmission to Remote Cooperative Groups: A New Key Management Paradigm**”,** – IEEE / ACM transaction on Networking, Vol.21 , No .2, pp no 621-633 .April 2013.

[7] QianhongWu,Domingo-Ferrer,Gonzallez-Nicolas U “Balanced Trustworthiness, Safety, And Privacy In Vehicle-To-Vehicle Communications” , February 2010.

[8] Yamir Amir,Yongdae Kim,Criistina Nita-rotaru,John Schultz,Jonathan Stanton,Gene Tsudik,” Secure Group Communication Using Robust Contributory Key Agreement”,2004.

[9] Bo Rong , Hsiao-Hwa Chen, Yi Qian, Kejie Lu , Rose Qingyang Hu Sghaier Guizani “A Pyramidal Security Model for Large-ScaleGroup-Oriented Computing in Mobile Ad HocNetworks: The Key Management Study”,2009.

BIOGRAPHY

M. VIJAYA KUMAR He is pursuing M.E Degree in Computer science and Engineering in Anna University, Coimbatore, Tamil nadu, India. He received B.E Degree in Computer Science from Anna University, Chennai, India. He is a member of an IEEE Association. His Area of interest is Network Security.

V.PRIYA DHARSHINI she is pursuing M.E Degree from Sri Eshwar College of Engineering, Coimbatore, India .she received her B.E Degree from Karpagam University, Coimbatore, Tamil Nadu, India **.**she published two international journals and also an IEEE member . Her field of Interest is Network Security.

Dr.Selvan.C has been working as an Associate Professor in the department of CSE, in Sri Eshwar college of Engineering, Coimbatore since 2012. He is an IEEE member. He had been doing research in Government College of Technology, Coimbatore, Tamilnadu, India. He has published 5 papers in International Journals. His area of interest is Mobile Computing, Mobile communication and Data Mining.