International Journal of Pure and Applied Mathematics
Volume 117 No. 21 2017, 1-9
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Group Key Agreement for Secured Group Communication

Sriram TK[1] , Yoga Vignesh B[2] , Suji Helen L[3]
[1,2]Department of ComputerScience, Sathybama University,Chennai,India
[3]Assistant Professor,Department of ComputerScience,Sathyabama University,Chennai
[1]sriramtk@gmail.com
[2]yogavignesh06@gmail.com
[3]sujihelen@gmail.com

Abstract

Modern group oriented applications mostly involves communication upon wireless networks. In today's networks, communication among group members must be secure and efficient. Group key agreement is widely employed such that group communications can be done in a secure manner in the modern group oriented applications. In existing group oriented application there is a problem of third party to enter the group without admins knowledge and can gain the information. Even sometimes the admin may change dynamically. So by studying the drawbacks a model is being proposed here which deals with the group key agreement in which group keys are creating an encryption key while each member will be having a secret decryption key. Only by knowing the key for encryption can the text be encrypted so that only the members of the group can decrypt.

Keywords : Nodes, Group Key,Encryption,Decryption.

1. Introduction

In this modernised world all the transactions are basically based on the net starting from shopping to transferring money and what not. When a transaction is being processed then a crucial aspect is security as there are some which involve or mostly involve monetary issues. For such circumstances there is an issue of security involved. This is where the method of encryption comes in handy. The best way of handle data security is **Encryption**. In order pursue an encoded document it is very necessary for the reader to either have a security key or the password with which the file had initially been encrypted with an ambition in mind to unscramble it. The encrypted files are alluded to as Cipher content and the ones without encryption are alluded to as plain text. Under similar circumstances when a group communication occurs then people in a group are supposed to talk to each other keeping in mind the end goal to communicate. Let us take the example of a what's app group where lets' say that there is an admin and the others are just participants in the gathering. Now if we look at our model and this model is replacing these people with nodes and the communication is done on a wired LAN connection. A key will be generated by the admin and hence encrypts the procedure of communication. The message when enters into the node for the node to properly understand the message it has to be unscrambled and hence the process of deciphering comes into play. The procedure of taking an encrypted text and converting it into the normal text which can be caught on easily by the node and can be read is known as **Decryption.** The model being proposed here has 3 modules namely Node Initialization, Key generation, Message Sending.

2. Related Work

Discussion will now be focused on a few of the related works that have been done by various inventors on the same domain. Firstly is **Hierarchical Identity Based Encryption (HIBE) with Constant Size Ciphertext**[1][4]where the system is used wherein the encrypted text has only three elements to be grouped and the deciphering requires only two computations on a map, without considering the hierarchy. Encryption here is efficient. The security issue in the standard model and in addition the irregular prophet demonstrates has been proved where in the first case there is only selective id security and in the second case it has full security. Its applications include: Effective forward secure open key and character based cryphertexts, conversion of the NNL broadcast system encryption into a efficient public key broadcast system, finally it also has a efficient mechanism for future encryptions.

Next we have **Identity Based Authenticated Key Agreement Protocols from Pairings[2]** where an investigation is done on a lot of issues in relation to the verified key understanding protocols which make efficient use of the Weil or Tait pairings. Such issues describe the procedure of making efficient protocols; here avoiding key escrow by a Trust Authority (TA) which is in charge of issuing identity based private keys especially for the users, it even describes to the users based on how the users should use various trusted authorities. A few authenticated protocols have been described and is given with a key confirmation where the protocols are modified from Smart's AK(Authenticated Key) protocol. Heuristically the security protocols are studied and are proved using a few security methods. Finally the inventors state that their AK protocol is resistant to any kind of attacks.

Last but not the least is **Entity Authentication and Key Distribution[3]** where the authentication of an entity and in addition key distribution are the crucial problems that are being faced in a conveyed framework with respect to cryptography. One of the main disadvantages here is that incorrect and inefficient protocols have gone up the charts hence reducing efficiency. The first treatment of such issues have been discussed by the inventors in the paper where complexity of modern cryptography has been taken into consideration. Two such problems namely symmetric, two-party setting: shared validation and confirmed key trade have been tended to in detail by the authors of this paper. A definition is presented along with the protocols and finally a proof that the protocols meet all its goals thinking about the minimal postulation of a pseudorandom function. When this theorization is instantiated properly, the protocols which are generated are not only efficient but practical as well.

A Secure and Efficient Conference Key Distribution System[5], Diffie-Hellman system[8] behaves contrary to the how it is supposed to behave then the system acts secure using an interactive practical conference key distribution system based on the public keys. This system allows the users to send their own conference keys after authenticating the users. All the users in this group have to work the same amount as well as communicate the same amount.

6.**An Efficient Group Key Agreement Protocol for Ad Hoc Networks[6]"**, a collection of autonomous nodes that communicate with each other by forming a wireless network is referred to as an ad hoc network. The resources available for this ad hoc method is limited. So when construction of a group node is under progress then the cost of the resources have to be minimized in such networks. Hence in this paper the goal is to be achieved using an efficient group key agreement which is based on a circular hierarchical group model, referred

as CH-ECC. The group key agreements minimizing the cryptographic computations. There has been a sharp increase in the past few years due to the network delay in the WANs as one of the primary concerns for the negative impacts on the key agreement protocols[7]. asymmetric encryption scheme that is chosen-ciphertext secure in the random oracle model. Here firstly the conversation from generic formation from an asymmetric arbitrary one way encryption scheme to one that is of a secure one.

Communicate the each other nodes, unwanted node also will communicate to neighbor node. Under the circumstance of a sender who needs to safely transmit messages to a gathering of recipients. The issue is the manner by which the sender can do this in a situation with the accompanying limitations:

1) A completely trusted merchant to produce keys for the gathering individuals is not available;

2) It is hard to estimate who will send scrambled messages to the members of the gathering;

3) The system is key independent.

4) The group is dynamic, that is, a user may join or exit the gathering. A similar function to the AGKA (Authenticated Group Key Agreement) is performed during broadcast encryption.

However, in a broadcast encryption system, the maintanance of the group is fully dependent on the dealer. There are still a few systems that are free from trusted dealers, they cannot offer forward secrecy and/or key escrow freeness.

3. Proposed System

In this proposed model the problems still existing in the existing system are dealt with. The main aim here in this proposed model is to generate key for the group and ensure authentication of its noes using the group key.

Initially we first have to formalize the idea of a dynamic Identity Based Authenticated Asymettric Group Key Agreement (IBAAGKA) without the usage of key escrow. For the generation of private keys to all the members of the gathering a trusted Key Generation Center (KGC) is identified and is allotted the work of distribution of keys to all its group members. On successful accomplishment of this can the members establish a public group encryption key so they can receive messages which are in the encrypted form with the help of the group key encryption technique. Moreover users are allowed to enter and exit the group.

A strong and sturdy stateful Identity Based Batch Multi Signatures (IBBMS) scheme is made in a manner that it cannot be forged in any way, where the static protocol in the existing system is turned into a dynamic Identity Based Authenticated Asymettric Group Key Agreement (IBAAGKA members of the group protocol without key escrow. Using the dynamic protocol the crucial requirement is that the group manager has to record the messages which are being sent to the gathering.Fig.1 shows the overall architecture of the proposed system.

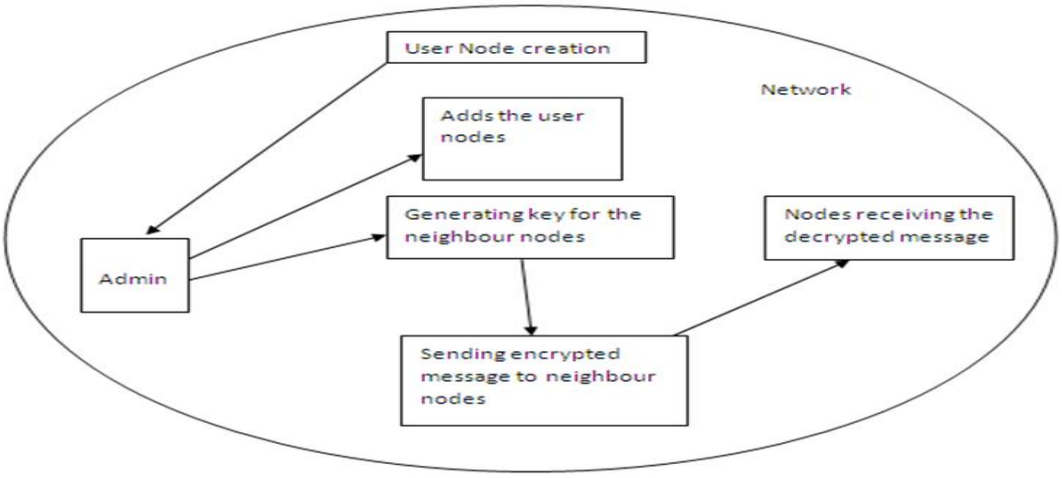

Fig1. An overall show of the model

3.1 **Methods:**

In this proposed model we have three modules namely:

- **Node Initialisation**
- **Key Generation**
- **Message Sending**

3.2 Node Initialization

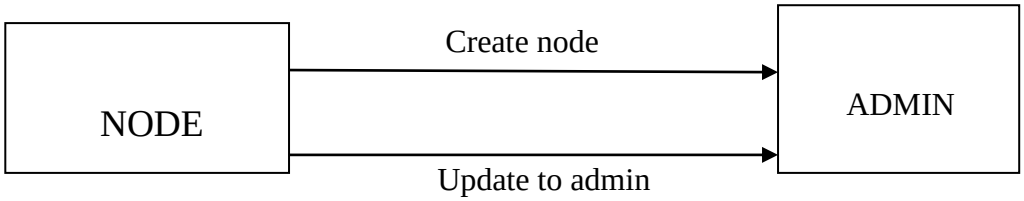

Fig.2 Creation of node and updation of the nodes are being done

In a group if a part wants to enter the group messaging state then a node has to be initialised. This is simple terms means that a new node will be added to the group of all the existing nodes. Using the phenomenon of node initialization nodes are added to the group. All the groups information is handled by the group head, so in any cicumstances if any updateation is to be done then it is firstly stored in the group head first. There are two types of nodes that are available here namely Admin node, and Mobile ad hoc networks (MANET) node.

MANET nodes: These are a group of solo nodes which have the ability to communicate with each other over radio waves. The nodes which are in the range of the radio waves then the nodes require a mode of transportation which in this model is a LAN wire.

Admin Nodes: There is only one node which is the administrator of the entire group messaging process where these nodes are the sole authority for allowing a group member to leave or to join the communication of the gathering. All information are saved in this admin node and this node also has the responsibility of storing and recording all the messages which are being sent to the gathering members. Fig 3. The Home Page where both admin and node creation are available. Fig. 4 and Fig.5 shows creation of new node with distance and group establishment.

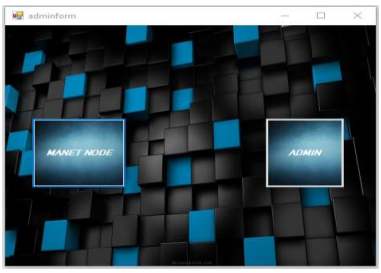

Fig.3 Home Page

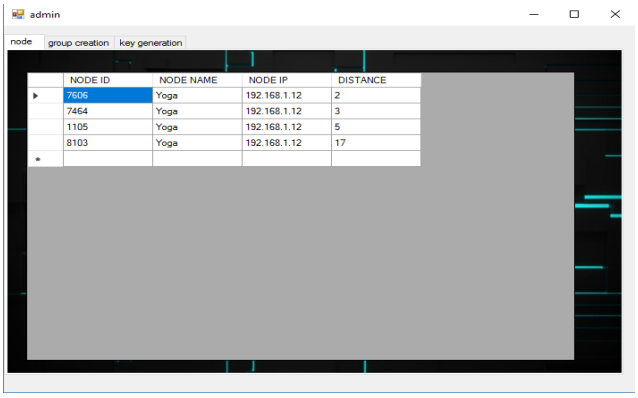

Fig.4 Creation of a new node with distance

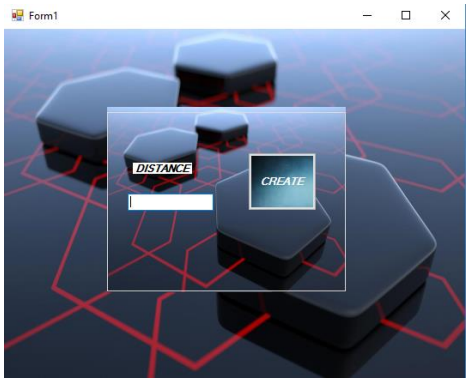

Fig.5 Group established

3.3 Key Generation

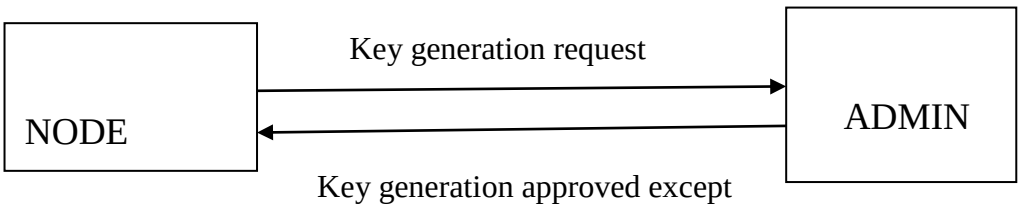

Fig.6 Node to Admin

Fig 6. A request being sent from the Node to Admin and the admin accepts the request and rejects one as it is out of scope

The first process here is to generate a group generation keyFig 7 and fig 8. For boosting the security both private key in accordance with the public keys are generated during the key generation process. Only after this process is done successfully then the private key and public key only generate a group key node which is essential for the group to

exchange messages amongst themselves in an encoded form shown in fig 9 , fig 10 and fig 11. The key being used here is mainly for safely encrypting and sending the message to a different node and on reaching the correct receiver the one with the authenticated keys then only can the message be unscrambled by the receiver in the gathering. All the transactions are recorded by the group admin node.

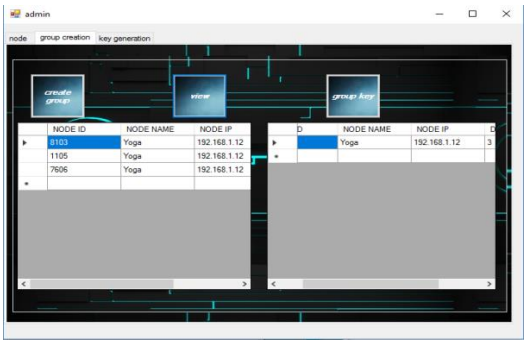

Fig 7. Creation of multiple nodes-three in a group and one ungrouped

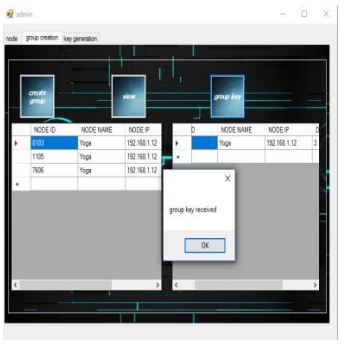

Fig 8. Group key created and sent to the nodes

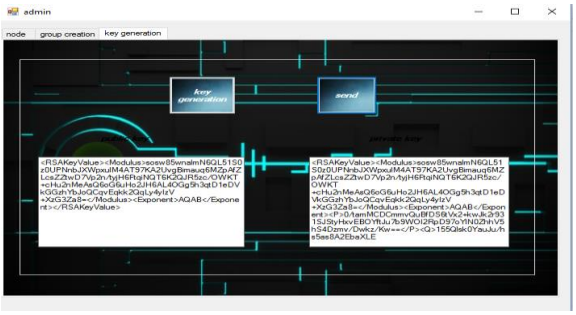

Fig 9. Key is being generated both- Public Key in accordance with Private Key

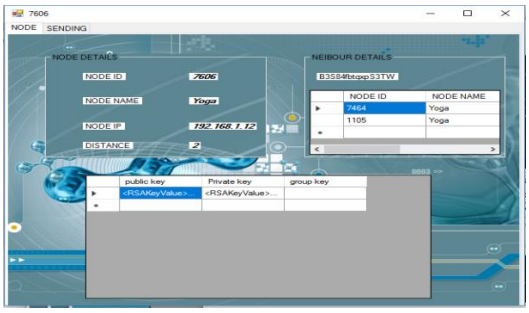

Fig 10. A Private and Public key is generated for the nodes

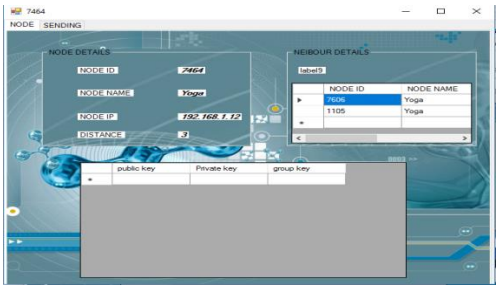

Fig 11. Key not generated for the ungrouped node

3.4 Message Sending

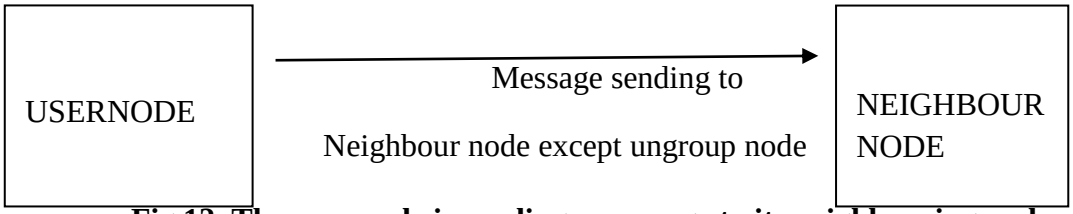

Fig 12. The user node is sending a message to its neighbouring node

Here the sending of the encrypted messages take place where encrypted messages are sent only to the group nodes shown in fig 12,fig 13 and fig 14. On receiving the message by the group nodes the message is in encrypted form and cannot be read by the received nodes, for solving that issue the message has to be decrypted. The message which is being transferred should not be sent to the nodes which are not a part of the group where the messages are being sent .

Fig 13. Message sending screen

Fig 14. A message is sent in the encrypted format

4. Conclusion

Hence in the above proposed model a group key is generated which is providing with secure message transfer during the entire group message transfer with the help of a group key generation which provides with both public keys and private keys which are provided by the admin nodes to the individual group nodes to ensure secure message transfer. Moreover the admin allows the addition as well as deletion of nodes as per the requirement of the process taking place.

5. References

[1] 'Dan Boneh','Hierarchical Identity Based Encryption with Constant Size Ciphertext" year, Lecture Notes in Computer Science, vol 3494, 2005.

[2] 'Liqun Chen1Hewlett', "Identity Based Authenticated Key Agreement Protocols from Pairings" Lecture Notes in Computer Science,springer, vol 4677, 2004.

[3] 'Mihir Bellare', 'Entity Authentication and Key Distribution',proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology,1993.

[4] 'Dan Boneh', ' Alice Silverberg', "Applications of Multilinear Forms to Cryptography" ACM workshop on Digital identity management, pages 63–72,2006.

[5] 'Mike Burmester'_Department of Mathematics Royal Holloway University of London, "A Secure and Efficient Conference Key Distribution System" Egham, Surrey TW20 OEX, 2006.

[6] 'Li Phing Zhang,Zhi Gang Yu', "An Efficient Group Key Agreement Protocol for Ad Hoc Networks*"*4th International Conference on Wireless Communications, Networking and Mobile Computing, pp 1-5,2008.

[7] 'Ongdae Kim', 'Adrian Perrig' , 'Gene Tsudik', "Communication-Efficient Group Key Agreement" "Proceedings of the 16th international conference on Information security: Trusted information: the new decade challenge", PP 229-244,2001.

[8] 'Lei Zhang', Qianhong Wu, Bo Qin, Josep Domingo-Ferrer "Provably secure one-round identity-based authenticated asymmetric group key agreement protocol"" Information Sciences: an International Journal", Volume 181 Issue 19, pp:4318-4329,October, 2011.