Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 13 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Comparative Study of Group Communication Protocol over Mobile Network

By Amin Ul Haq
National university of Modern Languages, Pakistan

Abstract - Peer to Peer Network for mobile is not centralized but self managing network with no specific topology. Topology of the Peer to Peer Network for mobile is change with change in time. In Mobile Peer to peer network various group communication protocols exists for multiparty conferencing. A mobile Peer to Peer network consisted of many security risks such as Decentralization of data storage, unusable connections, unauthorized access of data storage, provide connection to temporary IP address, Possess significant or total autonomy from central servers. Both file sharing and instant messaging are unsecure due to unavailability of encryption in both ends sender as well as receiver site in different peer to peer mobile network protocols. In this research our goal is to compare different group communication protocols in peer to peer mobile networks. and to suggest an efficient and secure protocol for group communication over peer to peer mobile network.

Keywords : *communication protocol, peer to peer network, file sharing, instant messaging.*

GJCST-E Classification : *C.2.2*

Strictly as per the compliance and regulations of:

Comparative Study of Group Communication Protocol over Mobile Network

Amin Ul Haq

Abstract - Peer to Peer Network for mobile is not centralized but self managing network with no specific topology. Topology of the Peer to Peer Network for mobile is change with change in time. In Mobile Peer to peer network various group communication protocols exists for multiparty conferencing. A mobile Peer to Peer network consisted of many security risks such as Decentralization of data storage, unusable connections, unauthorized access of data storage, provide connection to temporary IP address, Possess significant or total autonomy from central servers. Both file sharing and instant messaging are unsecure due to unavailability of encryption in both ends sender as well as receiver site in different peer to peer mobile network protocols. In this research our goal is to compare different group communication protocols in peer to peer mobile networks. and to suggest an efficient and secure protocol for group communication over peer to peer mobile network.

Keywords : communication protocol, peer to peer network, file sharing, instant messaging.

I. Introduction

a) Introduction to Peer - Peer Networks

Peer to Peer Networks are that type of Architecture in which computer share a portion of their resources such as disk storage, processing power, printing facilities and hard drive etc. These required resources are provided directly to other participants, because this method involves system serving other system. Peer-peer networks have no central resources. Peer-peer networks participants are both suppliers and providers of resources. A.Friedman (2008):

b) Background Study

Peer to Peer Networks are evolving throughout the world in many areas, such as audio, video, conferencing, games, online chatting programs and file sharing etc. Peer to Peer Networks is a special type of computer network that it is self organized symmetric communication and distributed control architecture. Self organization means that there are no typical centralized resources. As a result, link capacity is distributed throughout peer in the network, and as a result control is distributed as well. Peer to Peer networks have two important features that distinguish them from a more standard client-server model of information distribution. Peer to peer networks are overlay networks in which each node has unique name spaces. Peer to Peer system link different, possibly heterogeneous system as peer's, and allow them to interact on top of existing network configurations. It does this by defining unique relationship to that system, usually in the form of a topology by which systems are linked. The research on peer to peer communication can be divided into four groups. i.e search, storage, security and applications. Here in this work we will discuss security with respect to efficiency in detail while the other groups are out of the scope of this work.

c) Peer to Peer Security Issues and Risks

Peer to peer networks architecture have lot of advantages that's way all over the world communication is turning toward peer to peer communication instead of client-server architecture. Peer to peer networks communication are also facing some problems in security. The security risk can be divided into three categories i.e. security, legal and infrastructure risk. Here in this work we have focused on security risk. Peer to peer protocols have been designed with a lot of features but it does not focus on security measurements. They take advantage of:

1. Decentralized data storage.
2. Operate in an environment of unstable connections.
3. Unauthenticated access to data storage.
4. Provide connection to temporary IP addresses.
5. Possess significant or total autonomy from central servers; and avoiding filtering and security policy control.

Most peer to peer applications, both file sharing and instant messaging have week or easily cracked measure to protect user identities. There is no encryption of any communication sent or received via most peer to peer protocols.

Objectives of the Study

1. To compare different group communication protocols in the field of peer to peer networks.
2. To suggest an efficient and secure protocol for group communication via peer to peer networks

II. Research Methodology

The main steps in this research work are given below.

1. Read and review the research papers related to peer to peer group communication

Author : National university of Modern Languages Peshawar Pakistan. E-mail : aminkhan_2008@yahoo.com

2. Review the research critically.
3. Do the effective designing of network using visual studio.NET 2005 which reflects the real network.
4. Stimulate the network and collect results.
5. Report the result in the thesis to complete the requirement of MS.

a) Tools Used

The tools used for the protocol in this work are visual studio.NET 2005 and a supporting tool is SQL Server for keeping important data in a Database. It has the ability to test this protocol for a LAN/ WAN of approximately 100 machines that could be Pc, Laptop, mobile devices and we computed the performance of these machines based on the following factor.

- CPU Response time.
- Data storage (RAM size and HDD size) for maintaining stack of group controllers and key tree.
- Communication cost (The no of uni-cast and multi-cast messages).
- Current traffic load.
- No of allowable / possible group number registered with group controller.
- Maximum distance.

b) Proposed Solution

STGDH stand for stack and tree based group daffi-hellman is a new group key agreement protocol, it solves all those problems that were faced by researcher before this work. However two main problems faced by researcher i.e. computational complexity of generating the group key in terms of computational cast, another problem faced was tree maintenance. In this protocol both of these issues will be solve very efficiently. To solve the first problem, this protocol will choose the best performance group members as a group controller whenever membership operation is performed and for this purpose our new designed algorithm called GC Algorithm is executed to choose the highest performance member.

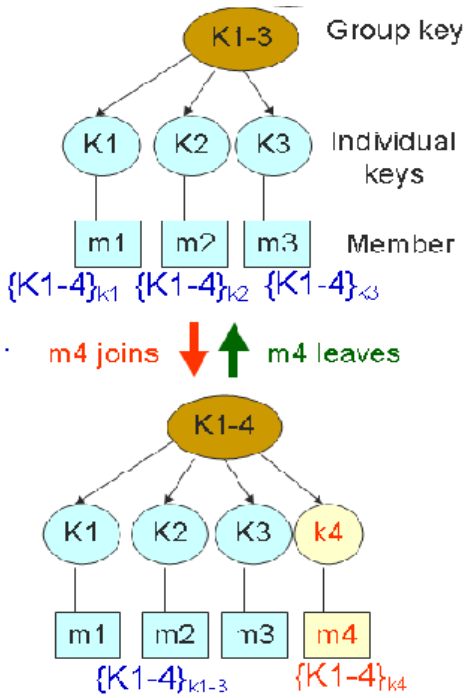


Figure 1 : Tree Based Group key and Individual key management Protocol

Group key and individual key management protocol is basically used to encrypt different messages and also used to verify the identification of each member.

c) Rekeying Message

It is basically used to keep information when members any key altered or keep track of new key information.

Join

It encrypt new group key with old group key and multicast to group, also it also encrypt new group key with new user's individual key and unicost to the joining user. But in join time complexity for rekeying messages is O(1).

Leave

It encrypt new group key with each user individual key and send it to remaining users one by one. Time complexity for rekeying messages in leave is O(n).

But main problem in the leave users is scalability.

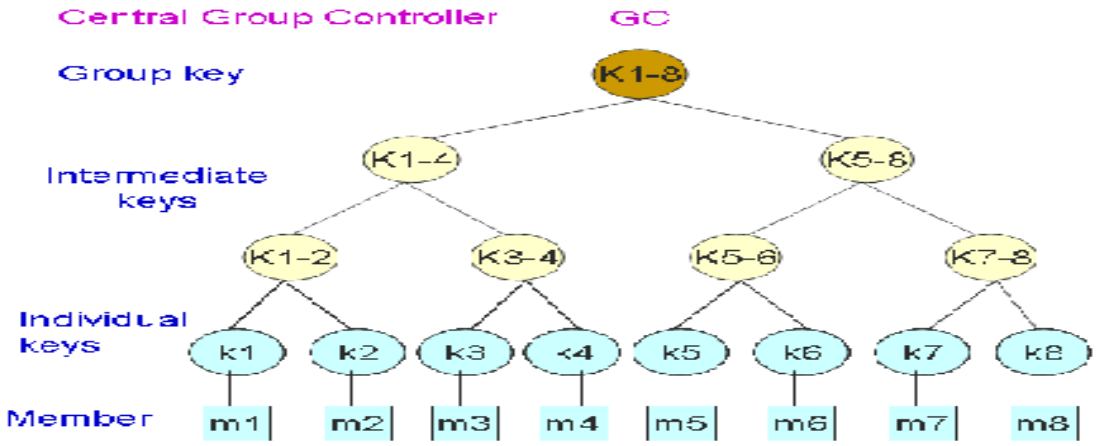


Figure 3 : Group key, intermediate key and individual key Management protocol

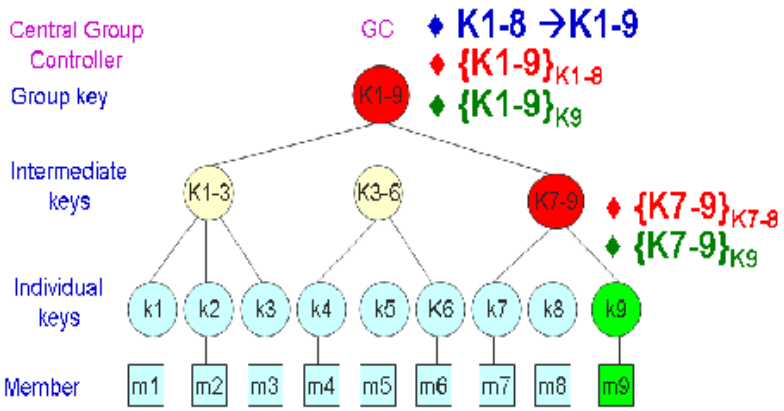
In the above fig(2.5) intermediate key is used to encrypt other keys instead of actual data. In group key, intermediate key and individual key management protocol tree each member stores the key information from leaf to the root. We can represent each member path for key storage as:

m1 ⟶ {k1, k1-2, k1-4, k1-8}
m2 ⟶ {K2, k1-2, k1-4, k1-8}
m3 ⟶ {k3, k3-4, k1-4, k1-8}
m6 ⟶ {k6, k5-6, k5-8, k1-8}

d) Join

In join tree approach when path is change also key need to be change and it is encrypted with the old key. It multicast the old group member which is shown in the fig.

Figure 4 : Join Tree approach



Where new member assigned the key through unicast. Time complexity for the rekeying message is $O(\log_k n)$. where in join approach m9 will joins the the following groups.

m9 ⟶ {k7-8, k7-9, k1-8, k1-9} and group controller should be.

GC: {m7, m8} ⟶ $\{k7\text{-}9\}_{k7\text{-}8}$
GC: {m1,……..,m8} ⟶ $\{k1\text{-}9\}_{k1\text{-}8}$
GC: {m9} ⟶ $\{k7\text{-}9, k1\text{-}9\}_{k9}$

Rekeying messages in the join approach is $2\log_k n$.

e) Leave

In leave tree approach when path is change then key is also need to be changed as shown in the fig(2.7).

In leave tree approach every changed key is encrypted with its child key and time complexity of this approach is $O(\log_k n)$.Where in leave approach m9 leaves the following groups.

m9 ⟶ K7-8 → K7-9, K1-8 → K1-9
GC : {m7}: $\{K7\text{-}8\}_{K7}$
GC : {m7}: $\{K7\text{-}8\}_{K8}$
GC : {m1, m2, m3}: $\{K1\text{-}8\}_{K1\text{-}3}$
GC : {m4, m5, m6}: $\{K1\text{-}8\}_{K3\text{-}6}$
GC : {m7, m8}: $\{K1\text{-}8\}_{K7\text{-}8}$

Rekeying messaging in leave approach is $k\log_k n$

III. Conclusion

A mobile Peer to Peer network consisted of many security risks such as Decentralization of data storage, unusable connections, unauthorized access of data storage, provide connection to temporary IP address, Possess significant or total autonomy from central servers. Both file sharing and instant messaging are unsecure due to unavailability of encryption in both ends sender as well as receiver site in different peer to peer mobile network protocols. To solve security issue in peer to peer multiparty conferencing we have selected Tree based STGDH protocol where STGDH stand for stack and tree based group Daffy- Hellman is a new group key agreement protocol, it solves all those problems that were faced by researcher before this work. However two main problems faced by researcher i.e. computational complexity of generating the group key in terms of computational cast, another problem faced was tree maintenance. STGDH is very efficient protocol then other protocols such as SDP(Session Description protocol), SGC(Subgroup Controller) Protocol and GC(Group Controller) Protocol. Tree based key structure reduces the rekeying messing and its time complexity is $O(\log_k n)$.it is suitable for multicast conference such as internet radio and stock estimation services

References Références Referencias

1. S. Hong, (2007, April). "Secure and Efficient Tree-based Group Diffie-Hellman Protocol",.
2. J.Li (2008). "A survey of Peer-to-Peer Network Security Issues".
3. A. Friedman. (2007, April). "Peer-to-Peer Security". "Peer-to-Peer Network Protocols".
4. N. Jasapara. (n.d.). "Group Key Agreement Protocols for Dynamic Peer Groups".
5. F.Otto, D.Patrick Mirembe (n.d.). "A model for data management in Peer-to- Peer systems".
6. H. Harney, C. Muckenhirn, (1997, July). "RFC2093 – Group Key Management Protocol (GKMP) Specification".
7. Y. Kim, A. Perrig, G. Tsudik *"Communication-efficient group key agreement".* Department of Computer Science on "A Secure P2P Video Conference System for Enterprise Environments".
8. B.Eun Jung (2006). "An Efficient Group Key Agreement Protocol" *10*.
9. M. Steiner, G. Tsudik, and M. Waidner, (2000). Key agreement in dynamic peer groups,. *11,* 769-780.
10. K. Y. Choi, J. Y. Hwang, and D. H. Lee, (2004). Efficient ID-based group key agreement with bilinear maps,. *Lecture Notes in Computer Science, 2947*.
11. F. Zhang and X. Chen, (2004). Attack on two ID-based authenticated group key agreement schemes from PKC. *In proc: Information Processing Lett., 91*, 191-193.
12. Y. Amir, Y. Kim, C. Nita-Rotaru, and G. Tsudik (2002, July). On the Performance of Group Key Agreement Protocols.
13. M. Burmester and Y. Desmedt, (1994, May). A secure and efficient conference key distribution system,.
14. Y.Kim, A.Perrig, G.Tsudik (2004). Group Key Agreement Efficient in communication. Key distribution protocol for digital mobile communication systems by M.Tatebayashi, N. Matsuzaki, Matsushita Electric Industrial Co Ltd Japan and D.B. Newman, Jr, the Jeorge Washington University, Washington DC. *53* (7), 905-921.