Group Key Exchange Management in Delay Tolerant Network

Muktesh Gupta
Assistant Professor
Department of Computer
Science and Engineering
University Institute of Technology,
RGPV Bhopal

ABSTRACT
Existing group key management scheme may not be applied effectively in Delay tolerant network where transmission between nodes (users) has the characteristics of irregular connectivity and long communication delay. In Previous proposed schemes, Group key is regenerated every time whenever new user joins or leave form the existing group, in order to maintain backward secrecy and forward secrecy and therefore the overhead to broadcast new group key to all member of group increases. In this proposed scheme which is based on Chinese remainder theorem constraint to broadcast new group key generated by server in case of user join as well as user leave is removed thus making the complexity constant in both scenario. Simulation is done in Opportunistic Networking Environment(ONE) Simulator and the result shows that Key update , Receiving success rate and key update success rate is better than Logical key Hierarchy LKH as well as Chinese remainder group key (CRGK) schemes.

Keywords
Delay tolerant network; Group key management ; Chinese Remainder Theorem; Logical Key Hierarchy; Opportunistic Networking Environment ; Modified Chinese reminder group key.

1. INTRODUCTION
Delay Tolerant Network (DTN) [1] is a environment where transmission between nodes(users) is done based on the store, carry and forward paradigm. Examples of such networks are Sensor networks, mobile networks in extreme terrestrial environments, or planned networks in space. In these kinds of networks effective end to end reliable connectivity is not possible [2]. In DTN sometime situation may arise where the communication between two node is possible only via user which is not authorized in a networks [3] and also in some cases there is no next receiver node available to transmit message for long time in these situations messages are stored in the buffer of the sender node for a long time therefore it become extremely difficult to have secure communication in these type of networks.

Group Communication is very useful and effective way of communication in a scenario where some information has to be shared between group of node in DTN. In Group Communication Network [4] all the node which are authenticated by the group server have a common group key which is used to decipher the message broadcast by some node, if any unauthorized node receive this broadcasted message it may not be able to decipher it. But the challenge in maintaining group key is a difficult task in these networks.

Need of confidentiality of group communication grows significantly as the popularity of group oriented applications are increasing day by day. While there are many secure protocols already available in peer to peer communication, in DTN where dynamic changing members are there it become extremely difficult to have efficient agreement on group key specially when user join or leave the group. In past many group management protocols are proposed based on the hierarchical structure but required about O(log n) [5] of keys to be received, decrypted or computed, and stored by each individual group user for a group of n users.

This paper proposes Modified version of Chinese reminder theorem based on DTN Group key management. By shifting more computing load onto the key server, this scheme optimize the number of re-key broadcast message. This scheme do not required to broadcast any key update message in case of user join and well as in case of user leave thus making it very efficient scheme for having secure communication in DTN Networks.

2. RELATED WORK
Existing Group key management scheme (LKH) logical key hierarchy[6] is based on centralized key generation in which members of a group are arranged in a tree like structure with a constraint that it should be balanced binary tree. In this scheme root node of tree contains group key and all leave node contain group members. Main overhead in these types of scheme is to maintain balance tree for smooth functioning. In DTN network as there is high intermitted connectivity between nodes, sometimes network will face a situation that simultaneously many node join and also leave the group therefore it become extremely difficult for the above scheme to work efficiently because major overhead is to maintain the balance tree. Moreover Group key is derived by computation of many logical keys which are in the path of root node to the leave node. The drawback in this scheme is that whenever user join or leave the group structure of tree has to be rearranged and logical key at each ancestor node has to be computed again and therefore it requires O(log n) complexity. Further logical key hierarchy is a stateful scheme and is not suitable for Delay Tolerant Network.

Another Scheme based on Chinese reminder theorem (CRGK) Chinese remainder group key theorem [7] in which communication overhead in case of user join phase is O (1).In CRGK Scheme Group key $GK_{i,j}$ contain two tuple <i,j> which indicate i-th random group key and j-th hash operation on that key. Every time when new user join the group, server changes the group key of same series by using forward has function, as the existing node are already have the group key with same series they also compute the next group key of same series by

using forward hash function and therefore no need of broadcast of key update message is required. But in case of user leave server has to change the series of group key and therefore for successful communication of already existing node the key update message has to be broadcast by the sever because user may not able to get group key of same series as randomly generate by the sever, therefore at the time of user leave key message has to be broadcast and the complexity will depend on the number of user present in the group which in O(n) where n is the number of users in a group.

This proposed paper is on new scheme based on Chinese reminder theorem for DTN network. Proposed scheme removed the drawback of the CRGK scheme by reducing the complexity on user leave from O (n) to constant. Further proposed scheme maintains both forward and backward secrecy. In MCRGK scheme, Key is generated every time in user join and user leave therefore it is not vulnerable to collusion attack also.

3. PROPOSED WORK

3.1 Group Initialization

Suppose there are m group at in time of initialization user $U_1,U_2,.....U_m$ in initial phase. Authentication of user which are present in the group has to be done. While authenticating user the server assign one symmetric key (SK_i) and one positive integer (n_i) to the user. The positive integer(n_i) selected by server is also known as Chinese remainder parameter as it is pair wise relatively prime with all other positive integer assigned by server at time of authentication for other user i.e. $gcd(n_i,n_j)=1(1\leq i,j\leq m\ i\neq j)$. At the time of group initialization server also generate one group key (GK_i) which is not known of any user.

With the above parameters the server establish a congruence equation as shown

$$X\equiv SK_1\ (GK_1)\ mod\ (n_1)$$

$$X\equiv SK_2\ (GK_1)\ mod\ (n_2)$$

.....

$$X\equiv SKm\ (GK_1)\ mod\ (n_m)$$

where GK_i is the Group key generated by the server when user join or leave the group. SK is the symmetric key and n_i is the Chinese reminder parameter which is secretly known by server and the individual user at the time of authentication.

Now According to Chinese reminder theorem, the solution of congruence equation have only one solution[8] Z (Let) which is unique. Taking this as a advantage the solution of above equations can be calculated as

$$Z=\sum_{i=1}^{m} Bi\ Xi\ SK_i$$

Where Bi can be calculated as B/Bi (B=n1*n2*....nm)

For calculation of Xi concept of modulo inverse is used and it can be calculated using following equation given below

$$B_iX_i=1(mod\ n_i)$$

Server calculate the unique solution Z for the congruence equations and at the time of message broadcast the server will encrypt the message using group key which is not known to any user. Server broadcast encrypted message along with the unique solution of congruence theorem i.e. Z, authenticated user on receiving the message along with the Z perform 1 modulo arithmetic and 1 XOR operation and will easily derive the group key and decrypt the message.

3.2 User Join

In proposed Scheme User join will take place in a constant time, server will update the parameter of the newly join user in the previously existing congruence equation and again compute the Z value. As the congruence equation contains new parameter the Z value changes as it includes the parameter of the newly join node given by server at the time of authentication. It will add following to congruence equation

$$X\equiv SK_1\ (GK_2)\ mod\ (n_1)$$

$$X\equiv SK_2\ (GK_2)\ mod\ (n_2)$$

.....

$$X\equiv SK_m\ (GK_2)\ mod\ (n_m)$$

$$X\equiv SK_{new}\ (GK_2)\ (mod\ n_{new})$$

(added because of new node)

Z value is calculated by adding the parameter of new user in the following equation given below

$$Z=\sum_{i=1}^{m} B_i\ X_i\ SK_i + B_{new}X_{new}SK_{new},$$

Note in every user join phase, change of group key is required in order to maintain Backward Secrecy i.e. new node may not be able to encrypt message which are generated before it got authentication by the server. When the encrypted message is received new user having group key GK2 it will able to decrypt it because the congruence equation contains parameters of new user at the time of calculating Z value.

3.3 User leave

At the time of user leave as soon as the server will get the information about the user which wants to leave, in order to ensure forward security i.e. the user will not decrypt any message generated after it leaves the group, server has to immediately remove user parameter from the congruence equation so that in future attempt to get the group key based on its CRT parameter it won't be able to do so because the new congruence theorem doesn't contain its CRT parameter.

$$X\equiv SK_1\ (GK2)\ mod\ (n_1)$$

$$X\equiv SK_2\ (GK2)\ mod\ (n_2)$$

~~$X\equiv SK_3\ (GK2)\ mod\ (n_3)$~~

~~$X\equiv SK_4\ (GK2)\ mod\ (n_4)$~~

.....

$$X\equiv SK_m\ (GK2)\ mod\ (n_m)$$

So in above congruence equation user U_3 and U_4 leaves from the group therefore their parameters are removed from the congruence equation . After Removal of the leaved user parameter server again has to change group key in order to maintain forward secrecy the new congruence equation is as shown

$$X\equiv SK_1\ (GK_3)\ mod\ (n_1)$$

$$X\equiv SK_2\ (GK_3)\ mod\ (n_2)$$

.....

$$X\equiv SK_m\ (GK_3)\ mod\ (n_m)$$

Z value is updated accordingly. Now when the message is broadcasted by the server , all the authenticated node present in a group will able to decrypt the message successfully

because the Z value is calculated by the congruence equation in which their parameters are present.

4. PROTOCOL ANALYSIS

4.1 Performance Evaluation

In user join phase as well as user leave phase the server does not need to broadcast any key update message, it simply add or remove the Chinese Remainder Parameter from the Congruence theorem and Broadcast Message along with the unique Solution obtained from Theorem. If the user is present at the time of computation of the congruence theorem then its parameter are present in calculation of unique solution (Z) and therefore at the time of message received which is broadcasted by the server, user may able to decrypt it easily. Same in case of user leave phase [9] when the user leave from group its parameter is removed from the congruence theorem and therefore at later stage it may not be able to decrypt the massage broadcasted by server . This whole scheme requires periodically update of Group key in both scenario i.e. when user join or leave from the group in order to main both forward and backward secrecy. Shifting more computation on the server side actually the complexity of communication between the users is reduced.

4.2 Security Analysis

4.2.1 Forward Security

Evicted member are not allowed to compute newer group key which means that after leaving the group user will not be able to access new information of the group. In MCRGK scheme, when the user leave the group its CRT parameter are immediately removed from congruence equation by server and there for it will not be able to get new information of the group.

4.2.2 Backward Security

When new member joins the group it may not able to compute older group keys which means they are unable to access previous information in the group. In MCRGK scheme as the older group key does not contain the parameter of new member therefore they are unable to get older group key.

5. SIMULATION AND RESULT

For simulation use of Opportunistic Network Environment simulator[10] is done in which epidemic Routing protocol is used. The area of spam selected is around 5km^2 , the interface type is "Bluetooth" interface for all nodes making btInterface.type = SimpleBroadcastInterface with the Transmit speed of 2 Mbps = 250kBps, Range of transmission (in meter) is 10. The Mobility model for all the nodes is Random Way point.

5.1 Result for Joining Phase

Comparing the key update in the joining phase with the three schemes one is Logical key hierarchy, Chinese Reminder Theorem and the third is proposed Modified Chinese Reminder theorem , Taking x axis as the number of nodes in the joining phase in the interval of 5 node at each simulation and y axis as Delay in key update in joining in second.

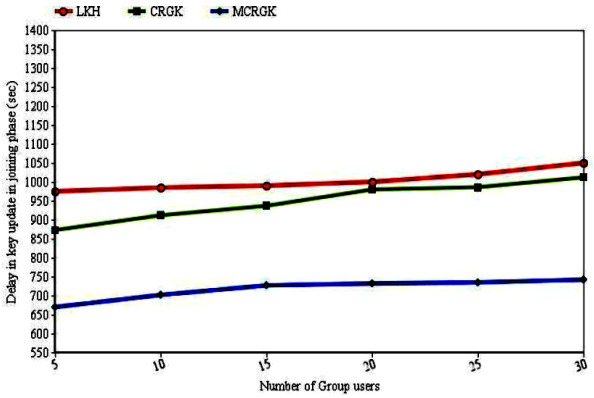

Fig 1: Comparison of key update in joining

Thus MCRGK key update is taking much more less time the previously proposed schemes as the computation of the key generation is reduced. The reason is that the server does not need to send a message when the new user join, and only sends one key update message when the node leaving, so the average update delay is least.

5.2 Result for leaving phase

On user leave phase also MCRGK scheme work efficiently as compare to Logical key hierarchy and also Chinese remainder theorem.

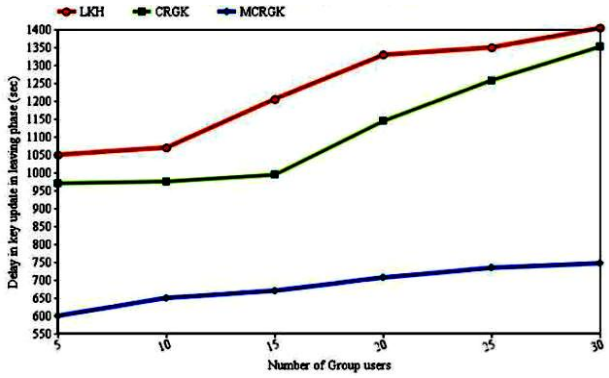

Fig 2: Comparison of key update in Leaving

Comparison between the ratio of the key update success with respect to the number of user, MCRGK scheme do not need to broadcast a message when the node joins, so it has the highest success rate. The LKH is a state full scheme, when key update message is lost, will lead to subsequent key cannot be received successfully, so the rate is the lowest.

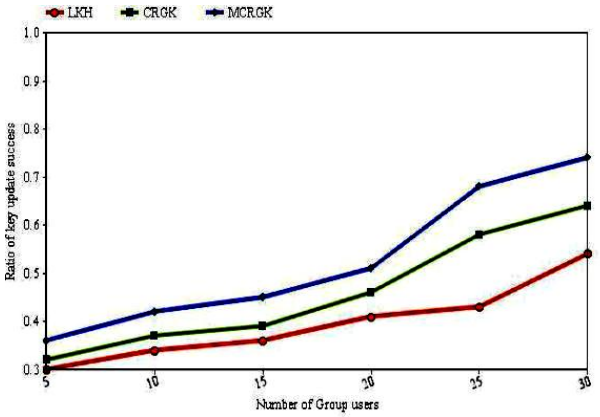

Fig 3: Comparison of key update success rate

Overall comparison of LKH, CRGK and the Proposed scheme MCRGK is done base of the above statistic

Table1. Comparison of LKH, CRGK and MCRGK

Schemes	**LKH**	**CRGK**	**MCRGK**
User Join	O (log n)	O (1)	O (1)
User Leave	O (log n)	O (n)	O (1)
Secrecy	Both Forward and backward	Both Forward and backward	Both Forward and backward
Security	Venerable to collusion attack	Not Venerable to collusion	Not Venerable to collusion

6. CONCLUSIONS AND FUTURE WORK

Key Management in dynamic scenario is the major part of proposed protocol, where user join or leave the group any number of time at their ease. Different schemes are proposed but security in the network is directly proportional to complexity as security increases the complexity also increase. MCRGK scheme reduces the complexity on user leave phase thus making this scheme efficient in Delay tolerant network. Still there is need to reduce the computation complexity of the server as computation and length of key update messages in MCRGK are direct proportion to the number of users in the group, so the scheme is only suitable for small and medium size DTN group communication.

Next step is to expend the concept for large group of DTN network by distributing the load of server to some of the sub server so the computation of congruence theorem become fast and also parallel computation is also possible .

7. REFERENCES

[1] R. S. Mangrulkar "Design and Development of Delay Tolerant Network : A Case Study" Nirma University International Conference on Engineering (NUiCONE) IEEE 2012

[2] Harminder Singh Bindra, Amrit Lal Sangal "Considerations and Open Issues in Delay Tolerant Network'S (DTNs) Security" Scientific Research August 2010

[3] Sofia Anna Menesidou and Vasilios Katos "Authenticated Key Exchange (AKE) in Delay Tolerant Networks" Springer Berlin Heidelberg 2012

[4] H. Harney, C. Muckenhirn Group Key Management Protocol (GKMP) Architecture RFC 2094, IETF Network Working Group, July 1997..

[5] Muhammad Yasir Malik "Efficient Group Key Management Schemes for Multicast Dynamic Communication Systems" 2012

[6] H. Harney and E. Harder, "Logical key hierarchy protocol," draft-harney-sparta-lkhpsec00.txt, IETF Internet Draft, 1999.

[7] Guoyu Xu, Xingyuan Chen, Xuehui Du, Zhengzhou "Chinese Remainder Theorem Based DTN Group Key Management" IEEE January 2012

[8] Yuke Wang "New Chinese Remainder Theorems" IEEE 1998

[9] Xinliang Zheng,Chin-tser Huang "Chinese Remainder Theorem Based Group Key Management"citeseer 2007

[10] Ari Keränen, Jörg Ott, Teemu Kärkkäinen "The ONE Simulator for DTN Protocol Evaluation" ICST 2009
.