INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

# GROUP KEY MANAGEMENT SERVICES FOR NEXT GENERATION BROADCAST NETWORKS: IPTV

**A.Vasanthi[1], T.Purusothaman[2]**

1. Department of CSE, BVRITH, Hyderabad, India, Vasanthi_gct@yahoo.co.in
2. Department of CSE&IT, Government College of Technology, Coimbatore, India, purushgct@yahoo.com

Author Correspondence: Associate Professor, BVRITH, Hyderabad, 8885510777, vasanthi_gct@yahoo.co.in

## Abstract

The next generation broadcasting networks is expected to be ruled by Internet Protocol Television (IPTV). IPTV uses IP Multicasting to disseminate multimedia contents to its large set of audience. Secure group communication plays a vital role in ensuring only the authorized customers receive the multimedia data. Key management is the indispensable defy in secure multicasting. Group key or session key is to be updated for every change in group membership. Applications like IPTV faces frequent change in membership. Batch rekeying can be an ideal solution. This paper concentrates on developing an ideal prototype for transmitting multimedia contents through secure multicasting. Queuing model based rekeying policy is proposed to reduce computational and communicational overhead.

**Keywords:** Batch Rekeying, IPTV, Group Key Management, Queuing Model, Secure Multicasting

## 1. Introduction

Predominantly the next generation television broadcasting is expected by means of packet switched network. The technological changes of communication and computing has stimulated increasing interest in the deliverance of TV services via the Internet Protocol (IP) Networks globally and the service is coined as Internet Protocol Television (IPTV). The triple play package which coalesce digital data, television broadcasting and data services together. When the data is transferred over the public network the security remains unanswered part. Adding with the triple play package it provides an interactive environment for the customers by promoting applications like CollaboraTV. The most exigent errand for IPTV, is broadcasting of the scheduled multimedia programs as per the subscription of user and broadcasting of on demand multimedia contents. Secure group communication plays a vital role to ensure the audio and visual contents are transmitted only to the subscribers. The different phases of broadcasting of multimedia contents in IPTV is shown in fig.1.1

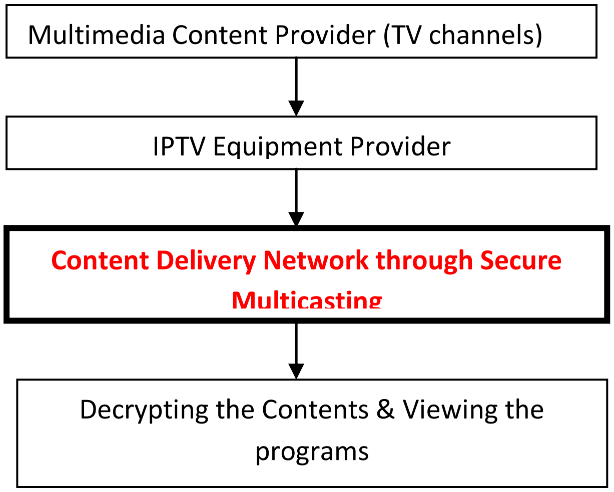
Multimedia Content Provider (TV channels)
IPTV Equipment Provider
Content Delivery Network through Secure Multicasting
Decrypting the Contents & Viewing the programs

Fig 1.1 Transmission of IPTV Program

Telecommunication and broadcasting industry rushes into IPTV epoch. The contents delivery network of IPTV system uses IP Multicast for broadcasting its program to group of receivers at once. To ensure only the authorized customers receive the program needs admission supervisory mechanisms. This can be attained with the proper usage of group communication services. The customers who paid for the same channel can be grouped and the contents of the channel are to be encrypted using a common key called as group key or session key. Since the membership of the group is highly dynamic for IPTV with more number of customers joining and leaving the channel frequently, robust rekeying scheme is indispensable to ensure forward and backward secrecy. Forward secrecy guarantees that the departed or evicted customer should not be allowed to receive any further broadcasting messages. Backward secrecy ensures that a newly joined customer should not be able to view the programs telecasted before the join. The process of maintaining forward and backward secrecy is depicted as group rekeying. Immediate rekeying or batch rekeying can be adopted based on the type of group membership and services. Since the group membership is highly dynamic batch rekeying is the suitable solution for IPTV group services.

IPTV transmission requires the scalability of group membership. In order to reduce the overhead involved in rekeying and to increase the scalability the concept of subgroup is introduced. Finding the optimal size of subgroup is major issue in IPTV. If the subgroup is optimal, it reduces considerable number of encryptions. This paper focuses on identifying optimal number of subgroups by applying the principles of queuing theory. Whenever a new member pays for the channel and becomes member of the group or existing paid customer leaves the group due to subscription expiration raises rekeying request. Rekeying request is consider being a pure random Poisson process with the arrival rate as λ. A content delivery group is assumed to have N subgroups in order to reduce the number of encryptions required for rekeying.

The remainder of this paper is structured as follows. Part II of this paper focuses on the literature. Part III concentrates on construction of mathematical model for the content delivery network of IPTV in order to reduce the number of encryptions. Fourth part of this paper gives a conclusion and the future scope of group key management schemes in broadcasting networks.

## 2. Related Work

### A. *IPTV Architecture*

The bureaucrat description accepted by the International Telecommunication Union focus group on IPTV (IPTV-T FG IPTV) is “IPTV is defined as multimedia services such as television/video/audio/text/graphics/data delivered over IP based networks managed to provide the required level of quality of service and experience, security, interactivity and reliability”. Fig 1.2 shows the overall functional view of IPTV broadcasting from the multimedia content provider to customer who availed the services.

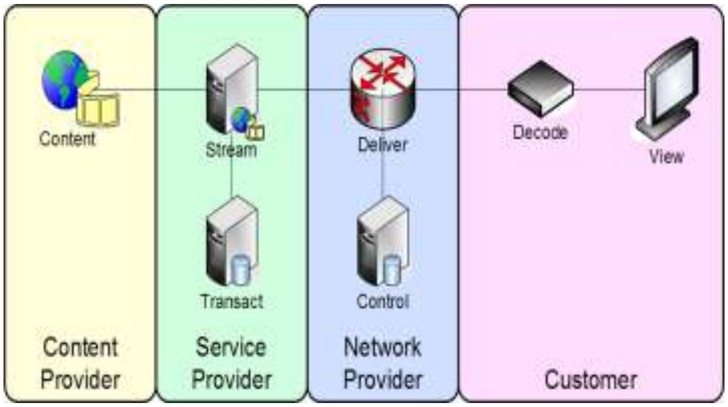

Fig 1.2 Architecture of IPTV proposed by ITU-T

In general television networks uses broadcasting as the transmission technique. The specialty of IPTV is the usage of multicasting for its content delivery. Internet Group Management protocol is the key protocol used for IPTV. The broadcasting of TV programs only to the subscribed customers is the key challenge in front of the IPTV industry. Secure group communication plays a vital role in multicasting multimedia contents to the subscribed customers.

### B. *Secure Multicasting*

Secure multicasting is the technique to instigate group confidentiality service. Confidentiality ensures that only subscribed customers are able to access the multimedia contents. Multimedia contents are encrypted by a common key called as group key or session key shared only by the members of the group. Change in group membership occurs either by new arrival of the member or by the departure member. The procedure of distributing a new group key for each membership change is named as Rekeying. Individual rekeying refers the process of changing the session key for change in every membership. Since IPTV application experiences heavy change in group membership individual rekeying is not an optimal solution. Batch rekeying can be an ideal solution. In batch rekeying the key server waits for a period of time called as rekeying interval, collects the entire join and leave requests during the interval process them as a single rekey request.

In group dynamics, it is compulsory to change the session key to enforce the following security requirements:

(i) Forward secrecy - It assures that an evicted member cannot decrypt the future contents of the group using the older session key.

(ii) Backward secrecy - It ensures that a newly joined member cannot decrypt the past communication with the current group key.

(iii) Collusion Resistance – Unfeasibility for any two or more former group members who have been expelled, to gain access to future group keys even if they collude and put their keying material jointly.

(iv) Though, there is no change in group membership, the session key should be refreshed periodically to increase the difficulty level for the attackers.

### C. *Queuing Principles*

In order to mathematically investigate the attributes needed for the rekey server which is the main part of the content delivery network of the next generation broadcasting network. A Mathematical model must be formulated in which such phenomena are expressed. This can be done using a branch of mathematics known as *queuing theory*. In queuing theory, models are studied of systems in which “customers” (randomly) arrive at a “service station” in order to be “served”; since there may be other customers ahead of them, they may need to wait in a buffer or “queue”. Queuing models are characterized by the probability distribution of the time between arrivals, the probability distribution of the time needed to serve a customer, size of the buffer space (if finite), queuing policy (e.g., first come first served), etc.

In general queuing model is represented in Kendal’s notation i.e. A/B/C/D/E.

Where
A- Inter arrival distribution
B- Service Distribution
C- Server Capacity
D- Queue Capacity
E- Queue discipline

Whenever a new subscriber joins or leaves from the group, a rekeying request is initiated immediately. Assume the group consists of $n$ subscribers ($G_1$, $G_2$, $G_3$, .., $G_n$). Since the join or leave is pure random event can be considered as Poisson process with the rekeying request rate of λ.

### D. *Categorization of Group Key Management Schemes*

In general the group key management [1, 2, 3] can be divided into three categories based on the key update mechanism as,

1. Centralized key management
2. Distributed key management and
3. Decentralized key management.

In centralized approaches [4] [5] [6], there would be a central server controlling the whole group. This group controller would not rely on any auxiliary entity to perform access control and key distribution. The crucial problem with this technique is the single point of failure. But with the group controller stanchly designed, the centralized system is more suitable for supporting small and medium dimension group members. The most popular conventional centralized approaches are:-

1. Group Key Management Protocol
2. One –way Function Tree
3. Logical Key Hierarchy
4. Key Graph and
5. Key Management using Boolean Function Minimization (KM-BFM) Technique.

In the distributed subgroup approach [7], there is no explicit manager and the members themselves do the key generation. All members can perform access control and the generation of the key can be rather contributory, meaning that all members contribute some information to generate the group key or done by one of the members. The distributed protocols have a scalability problem in case of key update, since they require performing large computations and they are characterized by large communication overheads. Further, they need all group members to have powerful resources. Basically in a distributed approach, there is no centralized server and the group key is to be formed from the contribution of all members

In decentralized subgroup approach, the large group is split into small groups. Different controllers are used to manage each sub group, minimizing the problem of concentrating the work on a single place. Some of the popular distributed subgroup approaches such as (i) IOLUS (ii) Dual Encryption Protocol and (iii) Hybrid Re-keying Mechanism are the most standard algorithms.

### *E. Group Rekeying*

The process of enforcing the security requirements of the group is termed as Group Rekeying. Group Rekeying are classified as immediate rekeying and batch Rekeying. Applications which require strict forward and backward secrecy should employ only immediate or individual rekeying. Applications where security can be relaxed for a while can employ batch rekeying. Immediate rekeying is highly secure but affected by out of sync problem and scalability issues. In batch rekeying re-keying request are grouped and the rekey is done only after the threshold is reached or time out. Selection of immediate or batch rekeying depends on the type of application and level of security needed for that application. Applications like IPTV does not require strict secrecy levels so batch rekeying can be applied. The most dominating factor in the implementation of batch rekeying is the rekeying interval or rekeying threshold.

It is proved that in batch rekeying based group communication [7] rekeying interval was in inverse proportion to the potential number of members in group. Using the birth-death Markovian principles [8, 9] a model is developed to address the issues of rekeying interval.

## 3. Proposed Model

IPTV uses secure multicasting for the transmission of multimedia contents. To enforce security group key or session key is to be updated periodically or whenever there is a change in group membership. The process of updating keys is named as rekeying. If optimization techniques are not applied the communication cost of rekeying increases heavily which may disturb the content delivery network of IPTV [1]. To reduce the communication complexity the total subscriber group is divided into various subgroups depending on the programs offered by the subscribers. Since the subscriber data cannot be clearly predicted at the server side, the subgroups are introduced based on the period of pay per view. According to the prediction the subgroups are classified into fixed time, short expelled time and variable expelled time.

For fixed time subgroup subscribers the sojourn time (Difference between join time and departure time of the subscriber) is very minimal and well known. Short expelled time talks about the subscriber's subscription for short duration but not predicted. Variable expelled time talks about the unpredictable sojourn time but may be evicted by the controller due to security reasons or left the group after long time voluntarily.

The structure of the rekeying interval has two methods a) Static and b) Dynamic. The static method is simple and less flexible. Dynamic method based on change of the requests time. In this the rekeying will process only when the number of rekeying requests either by join or leave reaches the threshold called as batch size. In general group member's arrival and departure is completely random and the join and departure request are collected cumulatively for a period of time and considered as a single batch. The foremost characteristics are

- Member's arrival or departure is deemed as rekeying request.
- Rekeying service process is the period during which the rekey server performs the rekeying as a batch. And
- Rule of Rekeying is that every request waits after arrival until the number of requests reaches the threshold ƙ

These characteristics give a path to apply the queuing theory principles [10, 11] to optimize the rekeying parameters for batch rekeying.

The group is assumed to be very large. The member's arrival and departure is a pure random process which is coined as rekeying request. Since the rekeying request is a random process it can be modeled as poisson process [8, 9] with the arrival rate as λ and the service done by the rekey server is exponentially distributed for various rekeying request with the service rate as μ. The threshold to start the rekey server is ƙ called as batch size. The random variable $\beta_i$ indicates the rekeying request when a member i arrives or departs from the group. The rekeying request $\beta_1$, $\beta_2$, $\beta_3$ …. $\beta_i$ are independent and identically distributed. The assumptions made in the construction of rekeying model are

1. **1.** Rekeying request to the system is assumed to be Poisson process with rate λ. ƙ is the maximum numbers of the customers in the system
2. **2.** After buffering the rekeying requests to the queue service begins by the time t with the density function $d(t) = \alpha^{e\text{-}\alpha t}$, $t \geq 0$, $\alpha > 0$ where α is the rate of time T.
3. **3.** The rekeying server works on a first-come, first served (FCFS) discipline. Once service commences it always proceeds to completion. The service times are assumed to be distributed according to an exponential distribution with density function $s(t) = \mu e^{-\mu t}$ , $t \geq 0$, $\mu > 0$ where $\mu$ is the service rate.

If the rekeying requests and service are independent of time or if the behavior of the group is independent of time , the group is said to be in steady state. Otherwise it is said to be transient state. Let P(n) be the probability that there are n rekeying requests and one rekeying server in the group. The probability of the group having n rekeying request in t+Δt time is from one of the four mutually exclusive ways:

1. Presence of n rekeying requests at t and no member arrives or departs from the group in t+Δt time.
2. Presence of n-1 rekeying requests at t and one rekeying request from the group in t+Δt time.
3. Presence of n+1 rekeying requests at t and no member arrives or departs from the group in t+Δt time.
4. Presence of n rekeying requests at t and one rekeying request and one rekeying service in t+Δt time.

$$P_n(t+\Delta t) = P_n(t)(1-\lambda_n\Delta_t)(1-\mu_n\Delta_t) + P_{n-1}(t)\lambda_{n-1}\Delta_t \quad (1-\mu_{n-1}\Delta_t) + P_{n+1}(t)(1-\lambda_{n+1}\Delta_t)\mu_{n+1}\Delta_t + P_n(t)\lambda_n\Delta_t\mu_n\Delta_t$$

The subscriber's statistical deed can be portrayed by an embedded Markov chain. Usage of Markov chain has basic advantage of predicting member's rekeying request based on its previous states [1].

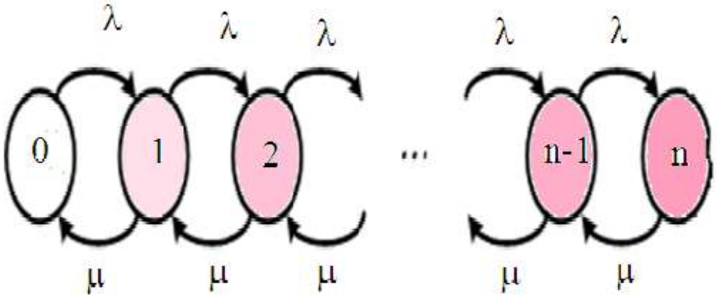

**Fig 1.2 Markov Chain model of Rekeying Request and Service**

The model is simulated using a special java based simulator called as Java Modeling Tools (JMT). The various parameter of the queuing network is given as input and the optimum rekeying interval and subgroup size is identified. Fig 1.4 shows the relation between rekeying interval and rekeying request for three different threshold value k=4, 6 and 8.

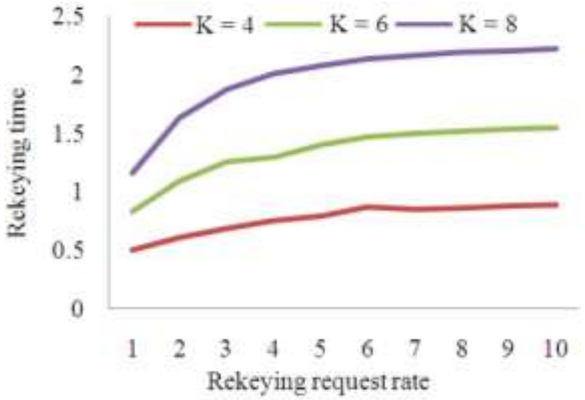

Fig 1.4 Relation between the rekeying interval and rekeying request rate

Certain applications like Pay TV, the members join or leave happens only at the beginning of the program and for short duration, group becomes static. The graph shows the relationship between expected rekeying request and the average waiting time when the value of batch size is five. The performance of the group mainly depends on the rekeying algorithm used. If the rekeying algorithm renders the service at the rate of μ=2, 5, 9 Fig. 3 shows the relationship between expected arrival rate and avg. waiting time.

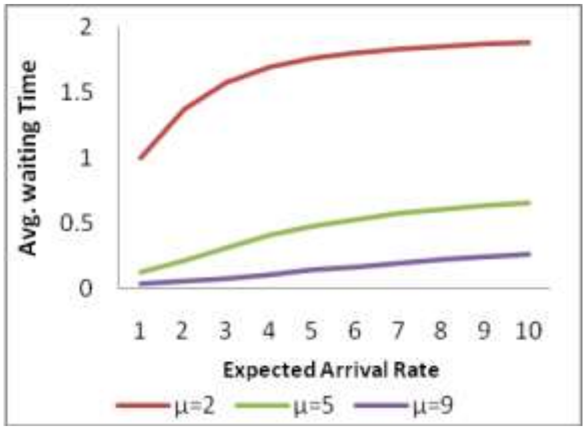

**Fig. 1.** Average Waiting Time for service rate μ=2, μ=5, μ=9

## II. CONCLUSION

## 4. Conclusion

This paper presents an overview of the batch rekeying algorithms and the various design parameters needed to construct the broadcast server of the next generation networks. Content delivery network for the next generation network is through secure multicasting. In order to enforce the security batch rekeying is applied. A queuing model based batch rekeying is proposed to solve various issues in batch rekeying applicable for broadcast networks.

## REFERENCES

[1] Vasanthi.A,T.Purusothaman, "Optimizing Batch Rekeying Interval For Secure Group Communication Based On Queuing Model", Journal of Computer Science 10(2): 325-329, ISSN: 1549-3636 © 2014 Science Publications . doi:10.3844/jcssp.2014.325.329 Published Online 10 (2) 2014 (http://www.thescipub.com/jcs.toc)

[2] S.Rafaeli, D.Hutchinson, A Survey of Key Management for Secure Group Communication, ACM Computing Surveys, 2003, Vol. 35, No. 3, pp 309-329.

[3] P.Sakarindr, N.Ansari, Survey of Security Services on Group Communication, IET Information Security, 2010, Vol. 4, Iss. 4, pp 258-272.

[4] H.Harney, C.Muckerhirn, Group Key Management Protocol Specification, IETF RFC 2093, July 1997.

[5] A.Sherman, D.Mc.Grew , Key Establishment in Large Dynamic Gropus using One Way Function Trees, IEEE Trans. Software Engineering, May 2003, Vol. 29, No. 5, pp 444-458

[6] C.K.Wong, M.Gouda, S.S.Lam, Secure Group Communication using Key Graphs, IEEE/ACM Trans. Networking , Feb 2000, Vol.8, No.1, pp 16-30.

[7] M.Steiner, G.Tsudik, M.Waidner, Cliques: A New Approach to Group Key Agreement, IEEE Trans. Parallel and Distributed Systems, Aug 2000.

[8] X.S.Li, Y.R. Yang, M.Gouda and S.S Lam, Batch Rekeying for Secure Group Communication, Proc. ACM 10th Intl. world Wide Web conference , May 2001

[9] Du.Ke.Liang, Zhang Xuan, Birth-Death Model of IP Multicast Group Behaviour, J.T.Sinhra, Univ Sci.Tech, 2004, Vol.1, pp 134.

[10] S.M.Ross, Stochastic Processes, John Wiley and Sons, 1996.

[11] E.Bacceili, P.Bremand, Elements of Queuing Theory, Springer – Verlag, 1994.

[12] B.Schneier, Applied Cryptography, John Wiley and Sons Inc., 1996.

[13] Hiroshi, Toyoizumi, Matsuyoshi Takaya, Performance Evaluation of Secure Group Communication, Journal of Operations Research Society of Japan, 2004, Vol.47, No. 1, pp 35-40.

**Dr.T.Purusothaman** : currently working as a Associate Professor (RD) in the department of Computer Science and Engineering and Information technology, Government College of Technology, Coimbatore. He has twenty three years of teaching experience. He has Completed Ph.D. in the area of Network Security and Grid Computing. He has presented a number of papers in various National and International conferences. Many of his papers were published in IEEE Explorer and reputed journal like Journal of Grid Computing, Springer. His research interests include Network Security, Grid Computing and Data Mining

**Vasanthi . A:** has completed her Bachelor of engineering from Madras University and post-graduation from Government College of Technology, Coimbatore. Presently she is working as an associate professor in BVRIT Hyderabad College of engineering for women, Hyderabad. Totally she has more than 10 years of experience in teaching. Currently she is pursuing her research in Anna University in the area of Network Security.

.