**Journal of Computer Science 10 (2): 325-329, 2014**
ISSN: 1549-3636

doi:10.3844/jcssp.2014.325.329 Published Online 10 (2) 2014 (http://www.thescipub.com/jcs.toc)

# OPTIMIZING BATCH REKEYING INTERVAL FOR SECURE GROUP COMMUNICATION BASED ON QUEUING MODEL

**Vasanthi, A. and T. Purusothaman**

Department of Computer Science and Engineering, Government of College of Technology, Coimbatore, India

Received 2012-07-02, Revised 2013-11-02; Accepted 2013-11-20

## ABSTRACT

Rapid growth of Internet spawns many group oriented multicast applications like Internet pay TV, news dissemination and stock quote system. The fortes of these applications are the support of dynamic, scalable group membership and group members are geographically divergent. As members of the group move in and out, an imperative cryptographic rekeying model should be applied to preserve the confidentiality of the group. A symmetric key called as session key is employed to defend the group communication data during transit. Forward and backward secrecy is attained by updating the session key for every change in group membership. Depends on the application immediate rekeying or batch rekeying can be used employed. The problem with the batch rekeying algorithm is to determine the pertinent batch size and the optimal time for rekeying process. The main aim is to propose a mathematical model based on queuing theory principles by considering the request for rekeying as Poisson process, rekeying service as an exponential distribution. The performance of the proposed model is analyzed using Java based simulator. By varying the arrival rate and rekeying service rate the optimal batch size can be attained. The optimal rekeying interval improves the performance of the group when the group membership grows dynamically. Reduces the long waiting time of the rekeying requests and find the best batch size for the rekeying. Proposed mathematical model analyses the various control parameters for batch rekeying and locates the best values for the batch size and interval time using the M/M/1/K model queues.

**Keywords:** Group Communication, Batch Rekeying, Queuing Theory

## 1. INTRODUCTION

The ubiquity of communication networks fortifies the progress of many group oriented applications like Internet Education, Internet Pay TV and Stock quote system. Multicasting is the cost effective means of data transfer for group communication. Multicasting exercises less network resources compared with unicasting. The group should allow the members to join and leave randomly and it must be scalable. Because Internet is opened to all, anyone joining in the group can access the group services. It is predominate to secure the group communication from various threats. The security of the group is ensured by encrypting the packets anticipated for the group with a shared secret called as session key. The foremost task of multicast key management system is the generation, distribution and updation of the session key intended for the group. The session key must be delivered securely only to members who are participating in the session. Forward secrecy assures that a submissive challenger who knows a contiguous subset of old session keys cannot ascertain any subsequent session key. While backward secrecy ensures that a submissive challenger cannot ascertain former session key by knowing only the present session key. Forward and backward secrecies are ensured by changing the keys labeled as group rekeying operations. Due to the dynamics of group members, rekeying results in high computation and communication overhead to the network and also causes out of synchronization problem. The Rekeying methods are

**Corresponding Author:** Vasanthi, A., Department of Computer Science and Engineering, Government of College of Technology, Coimbatore, India

classified as immediate rekeying and batch rekeying. Applications which require strict forward and backward secrecies should employ only immediate rekeying which updates session key whenever there is a change in group membership. In some applications like Pay TV group secrecies may be relaxed which may use batch or periodic rekeying. The main issues behind batch rekeying algorithms are the relationship between rekeying interval and the rekeying request. Short rekeying interval does not give a better benefit and also the long rekeying interval violates the group security issues. The main problem to be addressed in batch rekeying algorithm is an optimized rekeying interval. In order to reduce the communication overhead of rekeying, the group should be well structured. The large dynamic group is divided into sub groups and each subgroup works collaboratively. This study focuses on the main issue of group communication i.e., finding of the suitable rekeying interval for batch rekeying.

In general the group key management (Devi and Padmavathi, 2010; Sakarindr and Ansari, 2010; Steiner *et al*., 2000) can be divided into three categories based on the key update mechanism as, (a) Centralized key management (b) Distributed key management and (c) Decentralized key management.

In Centralized key management, an entity called as Group Controller manages the whole group. The crucial problem with this technique is the single point of failure. In the distributed subgroup approach the bigger group is cracked into small subgroups. Different controllers are used to oversee each subgroup, diminishing the problem of the work getting intense at a single place. In decentralized key management approach, the central group controller is eliminated. All the members are enabled to perform access control. The group key is generated in a contributory style where all the members contribute their own share to compute the group key.

Batch rekeying is employed in many multicasting applications where security can be relaxed for a while like IPTV. It is proved that in batch rekeying based group communication (Li *et al*., 2001) rekeying interval was in inverse proportion to the potential number of members in group. Using the birth-death Markovian principles (Liang and Xuan, 2004) a model is developed to address the issue of rekeying interval. The main drawback of all these methods are lack of optimal batch size based on rekeying request and the group size.

## 2. MATERIALS AND METHODS

The structure of the rekeying interval has two methods (a) Static (b) Dynamic. The static method is simple and less flexible. Dynamic method based on change of the requests time, the rekeying will process when the number of rekeying requests either by new join or leave should reach 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 considers as a single batch. The main characteristics of this study are:

- Member's arrival or departure is deemed as rekeying request
- Rekeying service process is the rekey server process rekeying in a period
- Rule of Rekeying that every request waits after arrival until the number of requests reaches the threshold k these characteristics gives a path to apply the queuing theory principles to optimize the rekeying interval

### 2.1. Model Description

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. The input i.e., rekeying request is modeled as poisson process with the parameter $\lambda$ and the service done by the rekey server is exponentially distributed for various rekeying request with the service rate as $\mu$. The threshold to start the rekey server is k 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:

- Rekeying request to the system is assumed to be Poisson process with rate $\lambda$. k is the maximum numbers of the customers in the system
- After buffering the rekeying requests to the queue service begins by the time t with the density function $d(t) = \alpha^{e-\alpha t}$, $t \geq 0$, $\alpha > 0$ where $\alpha$ is the rate of time T.
- 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:

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

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

By applying the limits to Equation 1 another with respect to the system state as follows

When no rekeying request n = 0:

$$\lambda P_0 = \mu P_1$$

When only one rekey request n = 1:

$$\lambda P_1 + \mu P_1 = \lambda P_0 + \mu P_2 \Leftrightarrow (\lambda+\mu) P_1 = \lambda P_0 + \mu P_1$$

When only two rekeying request n = 2:

$$\lambda P_2 + \mu P_2 = \lambda P_1 + \mu P_3 \Leftrightarrow (\lambda+\mu) P_2 = \lambda P_0 + \mu P_3$$

When three rekeying request n = 3:

$$\lambda P_3 + \mu P_3 = \lambda P_2 + \mu P_4 \Leftrightarrow (\lambda+\mu) P_3 = \lambda P_2 + \mu P_4$$

When k rekeying request arrives n = k:

$$\mu P_k = \lambda P_{k-1} \Leftrightarrow \mu P_k = \lambda P_{k-1}$$

Solving these simultaneous equations the values of $P_0$, $P_1..P_k$ can be obtained:

$$P_1 = (\lambda/\mu) P_0$$
$$P_2 = (\lambda/\mu)^2 P_0$$

So the probability that the group has n rekeying request is:

$$P_n = (\lambda/\mu)^n P_0 \quad 0 \le n \le k-1$$

The initial probability can be calculated as:

$$\sum_{n=0}^{k} P_n$$
$$\sum_{n=0}^{k} (\lambda/\mu)^n$$
$$P_0 \sum (\lambda/\mu)^n = 1$$
$$\text{So } P_0 = 1-(\lambda/\mu)/1-(\lambda/\mu)^{k+1} \qquad \lambda \neq \mu$$
$$P_0 = 1/k+1 \qquad \lambda = \mu$$

The probability that there exists k rekeying request is:

$$P_n = (\lambda/\mu)^n 1-(\lambda/\mu)/1-(\lambda/\mu)^{k+1} \qquad \lambda \neq \mu$$
$$P_0 = 1/k+1 \qquad \lambda = \mu$$

The member's statistical deed can be portrayed by an embedded Markov chain (Baccelli and Bremand, 1994). Usage of markov chain has basic advantage of predicting member's rekeying request based on its previous states.

## Theorem 3.1

The embedded Markov chain rekeying model is an ergodic Continuous-Time Markov Chain, if it satisfies the required properties of the steady-state probability vector, i.e., time-homogeneous, irreducible and aperiodical.

There are a total of n states, denoted by Si, i = 0, · · · , n. In static condition the group exists in a specific state Si, when the member arrives or departs the state either increases or decreases depends on the size of the group. Using embedded Markovian chain this can be symbolized as shown in **Fig. 1**.

The parameters which decides the optimal batch are:

- Expected number of rekeying request in a batch of size k. ($N_q$)
- Expected number of rekeying request in the group. ($N_s$)
- Expected waiting time for rekeying request to process in the group ($W_s$)
- Expected waiting time for rekeying request to process in the batch ($W_q$)

By applying little's law the various control parameters can be calculated:

$N_s = (\lambda/\lambda-\mu) - (k+1)(\lambda/\mu)^{k+1} / 1-((\lambda/\mu)^{k+1}$
$N_q = N_s - \lambda'/\mu$ where $\lambda' = \mu(1-P_0)$
$W_s = 1/\lambda' N_s$
$W_q = 1/\lambda' N_q$

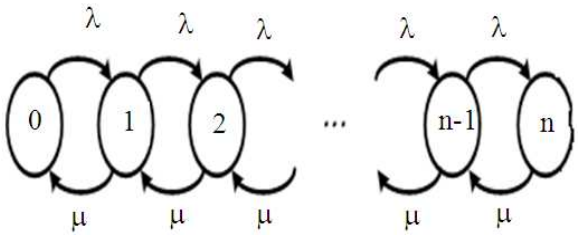


**Fig. 1.** Markov chain model of request and service

The optimal rekeying interval ($RI_{opt}$) is defined as the difference between start of current batch rekeying process to the next batch rekeying process. This can be calculated by adding the expected waiting time and the rekeying time by the rekey server:

$$RI_{opt} = W_s + \mu$$

$RI_{opt}$ can calculated by varying the arrival rate and the service time taken by the rekey server. The rekeying time mainly depends on the kind of rekeying algorithm used by the rekey server. In general rekeying algorithms are evaluated based on three parameters:

- Communication cost
- Computation cost
- Storage cost

By considering these three parameters the suitable rekeying algorithm can be applied. The rekeying algorithm which is used is the key factor to determine the rekeying service rate. The rekeying interval and batch size is mainly depends on the type of rekeying algorithm employed.

## 3. RESULTS

In dynamic environment, members join or leave randomly so that a lot of rekeying messages are created. Number of rekeying messages reduces significantly for batch rekeying system with the compromise to strict forward and backward secrecy and also it avoids out of sync problem. To optimize the rekeying interval a queuing theory based model is used.

The proposed model is simulated using Java based simulator called Java Modeling Tools which is mainly to simulate the various queuing models. The suitable rekeying model is identified by changing various system parameters like rekeying request rate, rekeying service rate and batch size.

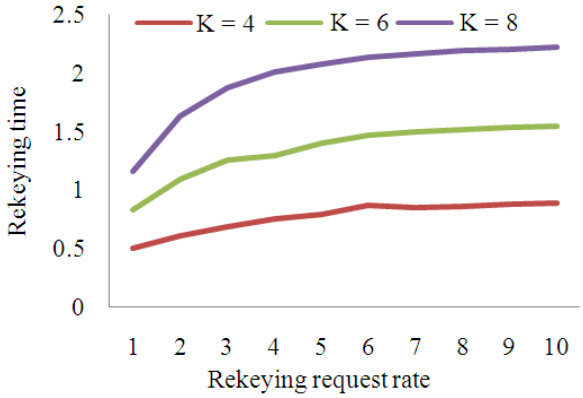


**Fig. 2.** Optimal rekeying interval when k = 4, 6,8

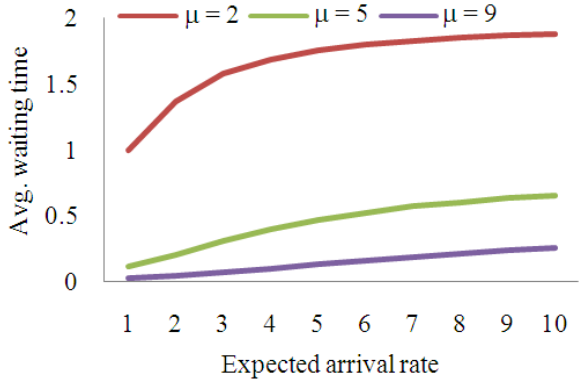


**Fig. 3.** Average waiting time when μ = 2, 5, 9

Group size of 1000 members is considered. The group controller performs the rekeying operation with rekeying service rate (μ) as 5 sec/req. The rekeying request follows poisson distribution. The graph shows relationship between batch size and rekeying request rate.

Association between the rekeying interval and rekeying request rate for various batch size is clearly given in **Fig. 2**. Optimal rekeying interval when k = 4,6,8.

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 chart 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.

## 4. DISCUSSION

This paper mainly focuses the user behavior for the next generation IPTV networks. A queuing theory based model is proposed to analyze the user session and the time to rekey. Finding of the optimal rekey interval time is one among the important parameter for any rekeying server. This works mainly for bulk leaving.

## 5. CONCLUSION

Generally periodic or batch rekeying policies are the suitable rekeying policies for applications like Pay TV. The problem associated with batch rekeying is selection of suitable batch size and appropriate rekeying interval. Queuing theory based rekeying model is proposed to solve the selection of optimal batch size and rekey interval. The proposed queuing model uses model 4(M/M/1/K) queue to accumulate the rekeying request. By varying the queuing system parameters like arrival rate, service rate and batch size the optimal rekeying interval is obtained. The study can be extended in future for the optimal division of the group into subgroups which reduces the complexity of rekeying process.

## 6. REFERENCES

Baccelli, E. and P. Bremand, 1994. Elements of Queueing Theory: Palm-Martingale Calculus and Stochastic Recurrences. 2nd Edn., Springer-Verlag, Berlin, ISBN-10: 3540533478, pp: 256.

Devi, D.S. and G. Padmavathi, 2010. Secure Multicast Key Distribution for Mobile Ad Hoc Networks. Int. J. Comput. Sci. Inform. Security, 7: 218-222.

Li, X.S., Y.R. Yang, M. Gouda and S.S. Lam, 2001. Batch rekeying for secure group communication. Proceedings of the ACM 10th International World Wide Web Conference, (WWC' 01), Hong Kong, pp: 525-534.

Liang, D.K. and Z. Xuan, 2004. Birth-death model of IP multicast group behaviour. J. T. Sinhra, Univ. Sci. Tech., 1: 134-134.

Sakarindr, P. and N. Ansari, 2010. Survey of security services on group communication. IET Inform. Security, 4: 258-272. DOI: 10.1049/iet-ifs.2009.0261

Steiner, M., G. Tsudik and M. Waidner, 2000. Cliques: A new approach to group key agreement. IEEE Trans. Parallel Distributed Syst., 11: 769-780. DOI: 10.1109/71.877936