Performance Evaluation for Group Key Rekeying

Tsukasa Igarashi s1080014 Supervised by Prof. Hiroshi Toyoizumi

Abstract

This paper evaluated the performance for group key rekeying that is important for computer security. Group key is the encryption key that used among particular group members and rekey means to change from an old group key to a new one. There are three rekeying processes proposed: immediate, batch and periodic. Immediate rekeying is a process that rekeying is done once someone joins or leaves a group. Batch rekeying is a process that is used when the total number of members that joins or leaves a group increases. Periodic rekeying is a process that rekeying is used in the constant period, regardless whether the total number of members joins or leaves a group. As a result of comparison of these three rekeying processes, according to the condition, we need to change rekeying processes.

1 Introduction

Computer security is one of the most important things in computer science. For example, when a conference is held among specific group members, the information of the conference must be kept in a secret. It is possible to realize this with group keys. Using group keys, a group member can access information, but a non-group member can not access information. So group keys are necessary for computer security, especially for group security.

Group key is generated by group controller and transmitted to each group member through a one to one secure channel. In addition, group keys must be periodically replaced because of prevention to access to a non-group member. The replacement is called 'rekey'. Rekey is good method to prevent illegal access, but this method has some problems on the performance. It is the problem that there are possibility group key is decrypted by the person that he was previously a group member. Researchers of group keys searched how group keys cope with illegal access by hackers using sub-group keys, thinking a role of the group key server [1]. On the other hand, I searched how group keys are updated more effectively, according to the number of group members.

The purpose of this study is to do performance evaluation for effective group key rekeying.

2 What's Group Key and Rekey?

2.1 Public Key

Before the explanation of group keys is held, public key cryptosystem of fundamental cryptosystem is explained. Public key cryptosystem is the cryptosystem that done using a public key and a secret key between a sender and a receiver. As you see in Figure 1, [2]

1. A receiver generates a public key and a secret key.
2. A receiver sends only a public key to a sender.
3. A sender gets a public key.
4. A sender encrypts a data with it.
5. A sender sends an encrypted data to a receiver.
6. A receiver gets an encrypted data and decrypts it with a secret key and he can watch the data.

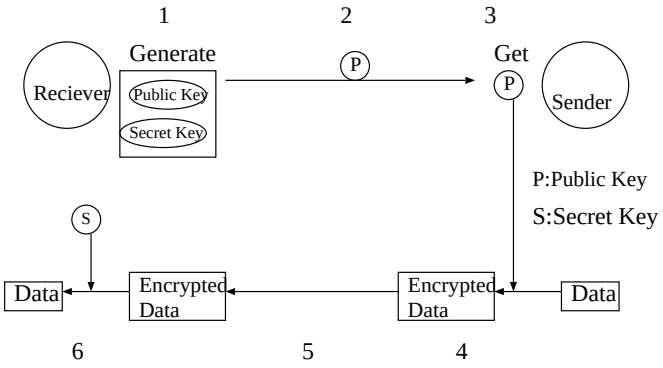

Figure 1: Public Key Cryptosystem

2.2 Group Key

On the other hand, group key is an encryption key that is used among particular group members. As you see in Figure 2, a group key is used on one to many communications. For example, it is used on TV pay programs (Wowow, SkyPerfecTV, or for etc.), and in particular conferences in a company. In the former, it plays a role that a person who was not officially join the TV program can not watch the pay program. In the latter, it plays a role that the person who was not take part in the conference can not know the detailed information.

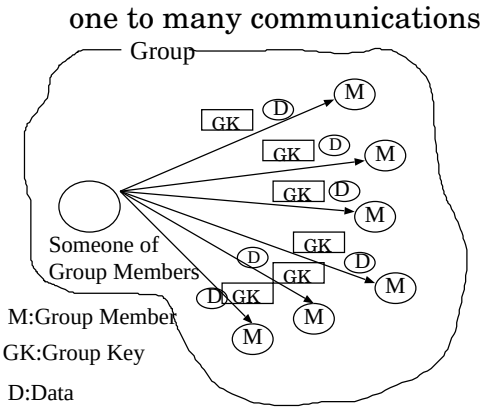

Figure 2: Group Key

2.3 Rekey

Rekey is the process changing from an old group key to a new one. Without rekey, illegal access increase because the key become old and the encryption key is decrypted by the person that he was an ex-group member. To prevent this access, a rekeying is done. Three rekeying methods are immediate, batch and periodic [3], and are compared about relation between the number of group members joining or leaving a group and the time of spending in a group below.

3 Modeling of Rekey Process

3.1 Pollaczek-Khinchin Formula

Pollaczek-Khinchin Formula [4] is the formula that is essential in M/D/1 of waiting line theory. With this formula, we can lead the expression of M/D/1. M/G/1 queue is the queue that arrival rate is Poisson process and service time is general. M/G/1 queue is expressed as follow.

$$E[N] = \rho + \frac{\rho^2 + \lambda^2\sigma_s^2}{2(1-\rho)} \quad . \tag{1}$$

where E[N] is the expectation of the total number of customer that exist in the system. ρ is the the utilization in the system. λ is the arrival rate to the system. σ_s is the variance of the service time in the system.
Using above expression, we can lead the expression of rekey processes.

3.2 Immediate rekeying

Immediate rekeying is a process that rekeying is done once someone joins or leaves a group. Immediate rekeying is active according to join or leave a group. If the total number is too many number, a new group member must wait since after the new comer's rekey is completely finished, the next new comer's rekey is started. So that, when a new comer arrives, if the previous rekey is not finished, he must wait particular time and his rekey starting time will be delayed. Please see in Figure 3.

1. When #1 arrived a group, none rekey was done, so his rekey (S1) could be done immediately.
2. When #2 arrived a group, #1 rekey (S1) did not finish, so #2 must wait until #1 rekey finished (W2).
3. When #3 arrived a group, #1 and #2 rekey (S1 and S2) did not finish, so #3 must wait until #1 and #2 rekey finished (W3). When both S1 and S2 finished, #3 rekey (S3) could be started.

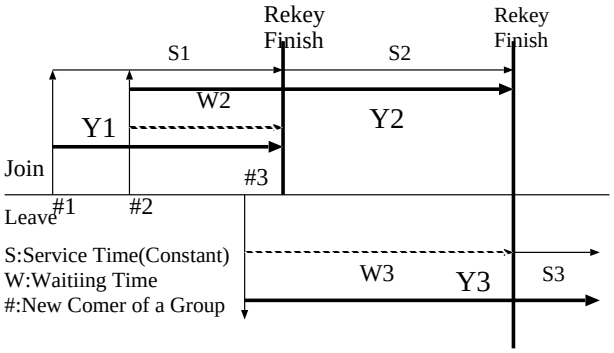

Figure 3: Immediate Rekeying

Immediate rekeying is a type of M/D/1 queues [5] that is one of the formulas for waiting line theory [6], and also M/D/1's service time (in this case, service time is the time required for rekey) is constant. S is the service (sojourn) time in the system. W is the waiting time in the system. Waiting time means that from the time a new comer arrives a group to the time his previous member's rekey completely finishes. In (1), σ_s is the variance of the service time, so σ_s is zero in this case. Hence we calculate E[N] of immediate rekey with (1) the below.

$$E[N] = \frac{\rho(2-\rho)}{2(1-\rho)} \quad .$$

By Little's formula ($E[N(t)] = \lambda E[T]$), we have

$$E[Y] = \frac{1}{\lambda}E[N] \quad .$$

So

$$E[Y] = \frac{1}{\lambda} * (\frac{\rho(2-\rho)}{2(1-\rho)}) = \frac{\rho(2-\rho)}{2\lambda(1-\rho)} \quad .$$

Namely,

$$E[Y] = \frac{\rho(2-\rho)}{2\lambda(1-\rho)} \quad . \tag{2}$$

where E[Y] is the mean of Y. Y is the time from a customer arrives in the system to a customer leaves in the system. Of course, Y includes service time.

In this case (immediate rekeying) , λ is the join or leave rate (number). So 2λ is the total rate, ρ means the product between 2λ and S (rekey time).
Hence E[Y] is expressed below. With (2),

$$E[Y] = \frac{S(1-\lambda S)}{1-2\lambda S} \quad . \tag{3}$$

Also ρ is the utilization, so this value must be smaller than one, hence

$$S < \frac{1}{2\lambda} \quad . \tag{4}$$

This is the assumption for immediate rekeying. If S is bigger than and equal to $1/2\lambda$, this process is not approved and E[Y] diffuses to ∞ and ρ converges one.

In immediate rekeying, when the number of members is increase, rekey's delay time is also increased. E[Y] becomes ∞. But when the total number of members joins or leaves a group is few, this process is useful because new comers do not need to wait.

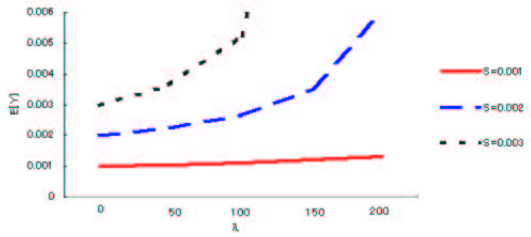

Figure 4: Immediate Rekeying Graph

Figure 4 is the relation between λ and E[Y]. As λ is bigger, E[Y] is bigger and (4) is not approved and E[Y] become ∞. (For example, when S is 0.003, E[Y] diffuses to ∞ at λ is 200).

3.3 Batch rekeying

Batch rekeying is the process according to the probability of α, a rekey is performed. For example, in Figure 5, it is maintained at α is one third.

In batch rekeying, the rekey time is also the constant value S but the number that is rekeyed is different, so E[Y] is expressed as follows. With (2),

$$E[Y] = \sum_{n=0}^{\infty} \alpha(1-\alpha)^n \left(\frac{n}{\lambda} + \frac{S(1-\lambda\alpha S)}{1-2\lambda\alpha S}\right) \tag{5}$$

where n is the mean how many members behind a group member until the rekey starts. Also ρ must be

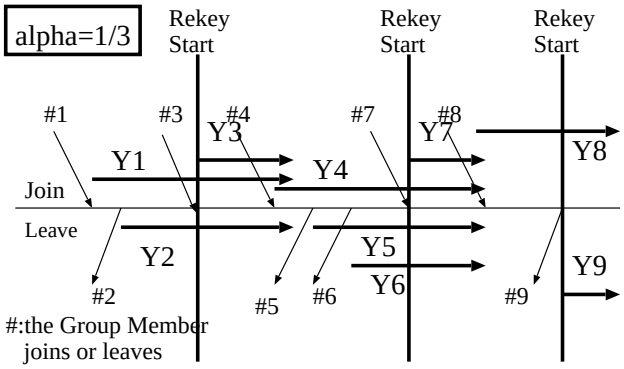

Figure 5: Batch Rekeying

smaller than one, hence

$$S < \frac{1}{2\lambda\alpha} \quad . \tag{6}$$

If (6) is not approved, E[Y] diffuses to ∞ and ρ converges one.

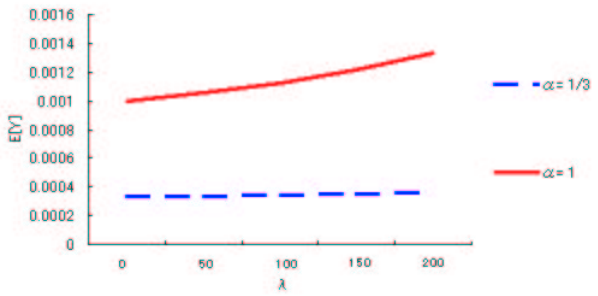

Figure 6: Batch Rekeying Graph

In batch rekeying, if α is smaller, E[Y] is also smaller and the increment is more slow. Please see in Figure 6. Also, according to α, E[Y] changes. As you can see in Figure 7, if α is small, E[Y] is also small.

3.4 Periodic rekeying

Periodic rekeying is the process that rekeying is used in the constant period, regardless the total number of members joins or leaves a group. The new comer's waiting time(W) is uniform distribution [7] and $E[W] = T/2$. So this process' E[Y] is expressed below.

$$E[Y] = S + \frac{T}{2} \quad . \tag{7}$$

where T is the constant period.
Also, S is the rekey time (also constant value), so S must

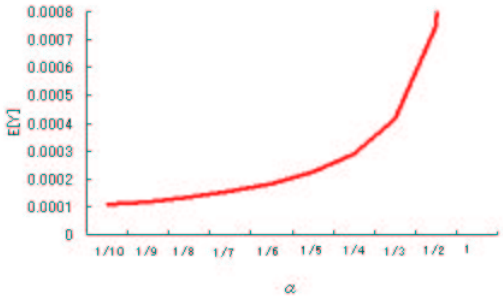

Figure 7: Batch Rekeying Graph

be smaller than and equal T. That is to say,

$$S \leq T \quad . \tag{8}$$

if (8) is not approved, E[Y] diffuses to ∞. Also periodic rekeying is not depend on λ and ρ. So, as you see in Figure 8, in spite of the number of # that means a new comer, if the constant time T passes, rekey is done.

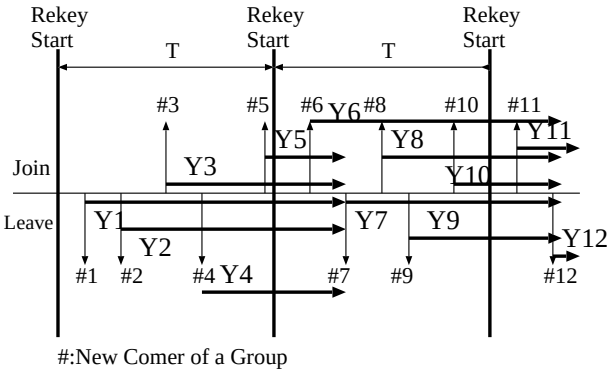

Figure 8: Periodic Rekeying

As you see in Figure 9, periodic rekeying's E[Y] is independent of λ.

4 Comparison

Assumption of three rekeying processes comparison
S is 0.001 (common), α is 1/10 and n is 10 (both in batch rekeying), T is 0.0011 (in periodic rekeying).

As you see in Figure 10, when the number of group members is small, immediate rekeying is the best rekeying process, batch rekeying is second best rekeying process and periodic is the worst rekeying process on the

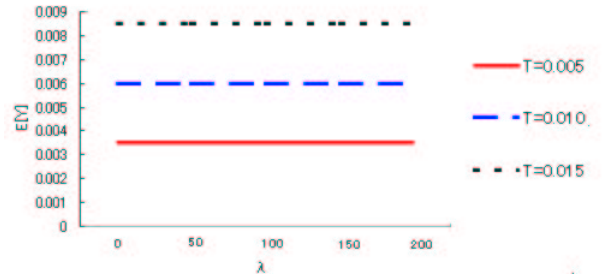

Figure 9: Periodic Rekeying Graph

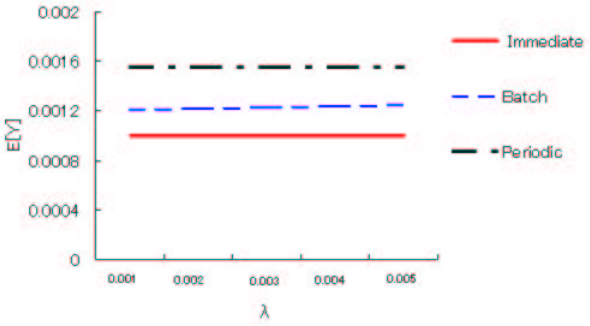

Figure 10: 3 Rekeying Comparison Graph(When λ is small)

performance. On the other hand, as you see in Figure 11, when the number of group members is big, periodic rekeying is the best rekeying process, batch rekeying is second best rekeying process and immediate rekeying is the worst rekeying process on the performance.

5 Conclusion

In many server systems, according to the number of that members and the purpose of use, the server's administrator will need to think a changing the rekeying processes. Also, batch rekeying has out-of-sync problem [8] between a key and a data. This problem is the problem that a user may receive a data message encrypted by an old group key, or it may receive a data message encrypted with a group key that it has not received yet. So we need to think this problem and select a rekeying process.

Acknowledgment

I thank Prof. H. Toyoizumi and Performance Evaluation Lab members very much.

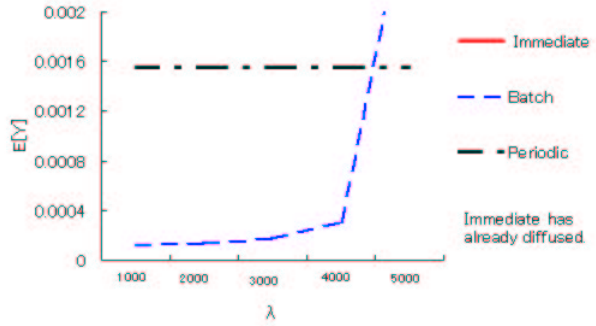

Figure 11: 3 Rekeying Comparison Graph(When λ is big)

References

[1] X. Li, Y. Yang, M. Gouda & S. Lam Department of Computer Sciences University of Texas at Austin, Batch Rekeying for Secure Group Communications retrieved from http://www10.org/cdrom papers/521/ on Jan 6, 2004.

[2] M. Itakura, What is Internet Security?, Tokyo: Nikkei BP Company. pp- 70-71, May 27, 2002.

[3] T. Hardjono & L. Dondeti, Multicast and Group Security, Norwood, MA: Artech House. pp- 129-134, June 1, 2003.

[4] H. Toyoizumi, Performance Evaluation Lecture Notes, April - July 2003.

[5] N. Ohsugi, Simulation Based Steady-stateAnalysis of M/M/1, M/D/1 and D/M/1 retrieved from http://www.aist-nara.ac.jp/%7Enaoki-o/homework/ims1/ims1_December-13-2001.doc on October 28, 2003.

[6] Blue Dreams, Queue Theory retrieved from http://www.ne.jp/asahi/license/ikawa17/info_soft/soft_main.html on September 18, 2003.

[7] S. Ross, Applied Probability Models With Optimization Applications, New York: Dover Publications Inc. pp- 17, 1992.

[8] X. Li, Y. Yang, M. Gouda & S. Lam, Batch Rekeying for Secure Group Communications retrieved from http://inrg.cse.ucsc.edu/280T/Winter2002/ReKeying.ppt on January 10, 2004.