CHAPTER 5

OPTIMIZATION OF SUB GROUP SIZE

5.1 INTRODUCTION

IP based broadcasting service is one among the key service for the next generation broadcast networks. IPTV service is to transmit the multimedia contents through IP network. It employs multicasting to transmit the contents to many receivers concurrently. By using the multicast communication, the deployment of multimedia application can be facilitated greatly. The two most important benefits of using multicast are: it reduces the load on the server as servers send only one packet instead of multiple packets to the receivers and it reduces the overall bandwidth consumption as only one data packet is transmitted wherever possible. IPTV can further benefit Internet users by entertainment, social and business values, but IPTV faces more challenges of scalability, privacy and service quality. So in order to provide resilient IPTV service proper secure multicast mechanism is indispensable.

IPTV system needs to ensure only the paid subscribers called as authorized subscribers should receive the multimedia contents. While any unauthorized subscribers, who have not paid the subscription amount should not be able to enjoy any of the IPTV services. The ideal solution is to enforce the secure access control mechanism in IPTV is group key management
schemes. For instance, IPTV can group the authorized subscribers for a specific channel and assign a secret key called as session key. The broadcast server of IPTV can encrypt the multimedia programs with the session key known only to its subscribers and transmits the program. The performance of the group key management scheme heavily depends on the number of group members and the frequency of membership changes. Specifically, the individual rekeying which performs rekeying whenever membership changes occur introduces a large overhead to the entire systems. Because subscribers frequently change the TV channels they view, individual rekeying is not suitable for IPTV systems.

When a group membership changes most frequently, individual rekeying cannot yield a better performance. Batch rekeying can be an ideal solution for application like pay per view or IPTV. However, it can improve the performance when the selection of control parameters is appropriate. Batch rekeying technique improves the performance but to improve the communication overhead of IPTV broadcast server the dynamic subscribers group is to be managed well (Min-Ho Parl et al 2013).

IPTV uses IP multicast to transmit the multiple video channels as IP packets to the subscribers. The subscribers are sub grouped based on the choice of viewing such as classical bundle, movie bundle, or the kids bundle etc. By subscribing to a particular bundle or combination of bundle authenticates the subscribers to receive the multimedia contents related to that bundle.
The biggest challenge in IPTV is the maintenance of enormous subscribers and also the subscriber’s subscription bundle simultaneously. This chapter concentrates on the architecture of key server and the effective management of subscribers group.

5.2 ARCHITECTURE OF IPTV BROADCAST SYSTEM

The major components of IPTV broadcast system are conditional access subsystem, middleware application server and the content delivery network (Zhu Y & Jue J 2009). The conditional access subsystem consists of encryptor system both online and offline streaming, and key server responsible for all cryptographic keying material supplied to the IPTV...
system. The high-level structure of a secured broadcast server is shown in the Figure 5.2.

![Figure 5.2 Structure of a secured broadcast server](image)

From the architecture of IPTV system, it is very clear that the rekey server present inside the broadcast server is responsible for the complete subscriber group key management mechanisms. Nevertheless, practically considering the subscriber strength will be enormous and the offered list of channel by the provider may be high (Mythili G M 2014). The subscribers are allowed to select the bundle of channels. During the subscription period, the viewing of the subscribed channel should not be disturbed. At the same time, the channel bundles are to be viewed only by the authorized subscribers. To achieve this goal hierarchical group structure is proposed. The structure of subscriber group is shown in the Figure 5.3.
The subscribers of the IPTV are grouped based on their subscription. Each bundle is managed separately. All the subscribers’ bundles are managed by the conditional access subsystem present in the broadcast server. Subscriber can belong to only one bundle or group of bundle at any time. The computation and communication load of IPTV broadcast server increases heavily because of enormous number of active subscribers. In order to reduce the complexity of IPTV system the subscriber group management should be administered properly. The architecture used in IPTV system is centralized architecture (Donghyun Choi et al 2013). The broadcast server is responsible for transmission and management of subscriber group (Minming Li et al 2009). The encryptor and rekey server is responsible for ensuring the multimedia content security. The overall performance of IPTV system can be

Figure 5.3 Structure of subscriber group in IPTV
improved by analyzing the maximum number of subscriber’s subgroup bundle and the upper bound for number of members in each subgroup. Since the subscriber joining and leaving can happen at any moment, the prediction-based model is most suitable for estimating the performance of the IPTV system. To improve the performance of batch rekeying, queuing based prediction model is proposed to identify the optimal rekeying interval and optimal batch size in the previous chapter. In this chapter a prediction based queuing model to manage the subscribers is illustrated with the complete analysis.

5.3 IDENTIFICATION OF OPTIMAL SUB GROUP SIZE

The potential subscribers of IPTV system are massive. Most often, the subscriber’s membership changes. To guarantee the security of IPTV system the multimedia contents are transmitted by encrypting with a common shared key known as session key. To facilitate the basic requirement of the group communication such as forward and backward secrecy the session key needs to be updated. The communication cost can be reduced drastically by adopting hybrid architecture for IPTV system.

The hybrid architecture shown in Figure 5.3 reduces the control overhead by splitting it into subgroups. The notion of introducing the concept of subgroups is to reduce the computation and communication complexity. The number of encrypted rekey messages to communicate the new key is the mechanism to measure the computation complexity.

Assume a group consists of 15 subscribers. In the first case, the subscribers are treated independently without any subgroups. The complexity varies for join and leave. When a new subscriber joins the group, session key is to be changed. The new session key is to be encrypted with the old session key and communicated to the existing subscribers. For the new subscriber it is
encrypted with its own secret and sent as a unicast message. The total computation and communication overhead involved is only two. At the same time when a subscriber leaves from the group, to update the session key, the new session key is encrypted by the individual shared secret and transmitted. The communication complexity is 14 i.e. the number of subscribers in the group.

In the next case, assume that the subscribers are divided into three different subgroups as shown in the Figure 5.4. If any subscriber joins the system three rekey messages are transmitted for communicating to the existing subscribers and one more message for the new subscribers. When a subscriber leaves from the group, the session key is updated with the existing subgroup key for the subscribers who belong to other subgroups. The subgroup where the leaving subscriber belongs to should be communicated individually. Total complexity is seven rekeying messages.

![Figure 5.4 Structure of Group of size 15](image-url)
Table 5.1 and 5.2 shows the clear picture of computation complexity in case of join and leave without subgroups and with subgroups. The total cost of computation is significant for large groups.

Table 5.1  Computation cost for varying number of subscribers without subgroup

<table>
<thead>
<tr>
<th>No. of Subscribers</th>
<th>Join</th>
<th>Leave</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>2</td>
<td>15</td>
<td>17</td>
</tr>
<tr>
<td>32</td>
<td>2</td>
<td>31</td>
<td>33</td>
</tr>
<tr>
<td>64</td>
<td>2</td>
<td>63</td>
<td>65</td>
</tr>
<tr>
<td>512</td>
<td>2</td>
<td>513</td>
<td>515</td>
</tr>
<tr>
<td>1024</td>
<td>2</td>
<td>1023</td>
<td>1025</td>
</tr>
<tr>
<td>4096</td>
<td>2</td>
<td>4095</td>
<td>4097</td>
</tr>
<tr>
<td>8192</td>
<td>2</td>
<td>8191</td>
<td>8193</td>
</tr>
</tbody>
</table>

Figure 5.5 Computation complexity without subgroup
Table 5.2  Computation cost for varying number of subscribers with sub group

<table>
<thead>
<tr>
<th>No. of Subscribers</th>
<th>Sub group Size</th>
<th>Join</th>
<th>Leave</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>12</td>
</tr>
<tr>
<td>32</td>
<td>4</td>
<td>6</td>
<td>10</td>
<td>16</td>
</tr>
<tr>
<td>64</td>
<td>8</td>
<td>10</td>
<td>33</td>
<td>43</td>
</tr>
<tr>
<td>512</td>
<td>16</td>
<td>18</td>
<td>46</td>
<td>64</td>
</tr>
<tr>
<td>1024</td>
<td>32</td>
<td>34</td>
<td>62</td>
<td>96</td>
</tr>
<tr>
<td>4096</td>
<td>64</td>
<td>68</td>
<td>191</td>
<td>259</td>
</tr>
<tr>
<td>8192</td>
<td>64</td>
<td>130</td>
<td>255</td>
<td>385</td>
</tr>
</tbody>
</table>

Figure 5.6 Computation complexity with sub group
In order to analyze the performance improvement of sub grouping, the number of subgroups and total subscribers in each subgroup is to be formulated in IPTV.

5.3.1 System Model Description

The total subscribers group is divided into M subgroups, $SG_{i=1..M}$. The total members inside the subgroup $i$ at time $t$ is denoted as $N_i(t)$. The subscriber’s arrival process is a Poisson process with the arrival rate $\lambda$. The number of subscribers arrives during the time $(t, t+s)$ only depends on the length of the time period $s$ but has no relationship with the start time $t$. A Poisson process is a sequence of events ‘randomly spaced in time’ as shown in Figure 5.7

![Figure 5.7 Subscribers interarrival time](image)

The interarrival time is exponentially distributed. When a new subscriber joins the network it can be assigned to any one of the sub groups with an equal probability. The probability that the new subscriber $NS$ belong to subgroup $i$ is

$$P(NS_i) = P(NS_i \in SG_i) = \frac{1}{M} \quad (5.1)$$

For a Poisson process at the arrival $\lambda$, the distribution is

$$P(NS(t) = k) = e^{-\lambda} \frac{(\lambda t)^k}{k!}, k > 0 \quad (5.2)$$
The stationary increments $N(s+t) - N(s)$ is also Poisson with mean $\lambda$. Since the arrival is Poisson with the rate $\lambda$ and total number of subgroups are $M$, the Bernoulli trail to select one subgroup among is $\lambda/M$ at any time $t$. With the given parameters such as arrival and service, model 1 queue can be applied to measure the key parameters. The arrival to each subgroup is an independent identical Poisson distribution, the mean number of members in a subgroup $i$ can be obtained by

$$E(N_i(t)) = \frac{\lambda}{M\mu} \quad (5.3)$$

$$E(N(t)) = \sum_{i=1}^{N} N_i(t) = \frac{\lambda}{\mu} \quad (5.4)$$

The total group is sub grouped to reduce the communication and computation complexity. The communication complexity utilizes considerable bandwidth to distribute the new session key. The computation complexity measures the number of encryption and the decryption applied at the sender and receiver side to transmit the contents securely. With the optimal number of subscribers, the mean number of encryptions can also be calculated for subscribers joining and leaving. The purpose behind the calculation is to minimize the number of encryptions based on the size of the subgroup and number of subgroups.

5.3.2 Poisson Arrivals See time Average (PASTA) Property

PASTA is a property applicable to stochastic systems. The detailed explanation is given by Ronald W. Wolf (1982). In essence, it states that observations made of a system at time instants obeying a Poisson process, when averaged, converge to give the true value, that is to the average that an ideal observer would make when monitoring the system continuously over time (Francois Bacelli et al 2006). The PASTA property is one of the central
tools in queueing theory. Sometimes this property is referred to as ROP (Random Observer Property).

Consider an arbitrary system, which spends its time in different states $E_j$. Arrival to the system is a Poisson process with the rate $\lambda$. These arrivals include state transitions in the system as illustrated in Figure 5.8.

![System $E_j$](image)

**Figure 5.8 State of a system**

In equilibrium condition, the different probabilities associated with each $E_j$ is

1. The probability of the state as seen by an outside random observer ($\pi$)
2. The probability of the state seen by an arriving customer ($\pi^*$)

In general $\pi \neq \pi^*$

But due to the property of PASTA $\pi = \pi^*$

PASTA can be stated as the fraction of customers finding on arrival the system in some state $A$ is that the same as the fraction of time the system is in state $A$.

Since the subscribers join and leave are not known to key server, the system moves to the state of discontinuous changes, but due to the property of PASTA,

$$P(\text{subgroup at join is } k) = P(\text{subgroup at leave is } k)$$
5.3.4 Cost of Computation

To ensure the secrecy of the multimedia contents the session key is to be updated for the change in group membership. The updation of session key introduces additional overhead to the IPTV broadcast system. In order to minimize the overhead, the group is well managed with the help of subgroups. If the subgroups and members in the subgroup are optimal, the overhead also reduces.

The IPTV system follows the principle of queuing theory. The arrival of rekeying request can be due to either join or leave. Subscribers join is assumed as a random Poisson process. The rekey server service is exponentially distributed. Therefore, the IPTV system follows the principle of queuing theory (Tabari et al. 2012). Assume the cost of computation to distribute the new session key is $I_n$. The mean value of $I_n$ can be

$$E(I_n) = \text{No of subgroups} + E(\text{Subgroup where rekeying request is raised})$$

From the property of Poisson Arrivals See Time Average (PASTA), it is very clear that if the system allows only discontinuous changes of size one at join and leave then the probability distribution of number of subscribers in a system is equivalent to the one before the event.

$$P(N(\text{join})) = P(N(\text{Leave}) = k.$$ \hspace{1cm} (5.5)

Since the result is also a Poisson distribution, the average cost of computation is

$$E(I_n) = M + \frac{\lambda}{N\mu}$$ \hspace{1cm} (5.6)

The cost of computation can be minimized by solving the equation 5.6

$$I_n \min = \left(\frac{\lambda}{\mu}\right)^{1/2}$$ \hspace{1cm} (5.7)
5.4 PERFORMANCE ANALYSIS

The number of subgroups and members inside the subgroups are optimized based on the queuing theory principle. The structure of group and sub group changes upon the arrival and leave of the subscriber. For an example, assume subscribers group consists of 10,000 members and members are expected to be in group for 30 mins. The arrival rate is calculated as 10,000 /30 approximately 334.

Table 5.3 Sub group communication Cost

<table>
<thead>
<tr>
<th>S.no</th>
<th>No of sub groups</th>
<th>Encryption Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No Sub group</td>
<td>$3334 \times 10^3$</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>$300 \times 10^3$</td>
</tr>
<tr>
<td>3</td>
<td>50</td>
<td>$100 \times 10^2$</td>
</tr>
<tr>
<td>4</td>
<td>100</td>
<td>680</td>
</tr>
<tr>
<td>5</td>
<td>1000</td>
<td>38</td>
</tr>
</tbody>
</table>

![Figure 5.9 Encryption Rate](image.png)
Figure 5.9 depicts the average number of encryptions for different size of the subscribers. The results shows that when the number of subgroups are optimal, the rate of encryption reduces, which in turn reduces the computation cost. The cost of communication also reduces considerably with which the overhead of the rekey server is minimized.