Sampling of the Group Membership in RTP

Ali Gulabi
gulabi_a@etech.haw-hamburg.de
Overview

• INTRODUCTION
• RTP
  – RTP Header
  – RTP Applications
• RTCP
• Group size
• Basic Operation
• Sampling
  – Corrective Factors
  – Binning Algorithm
  – Comparison
• Security issues
• References
• Questions
Introduction

• In large multicast groups, the size of the group membership table maintained by RTP (Real Time Transport Protocol) participants may become unwieldy.
• Particularly for embedded devices with limited memory and processing power.
• This document discusses mechanisms for sampling of this group membership table in order to reduce the memory requirements.
• Two mechanisms are proposed, and the performance of each is considered.
RTP

• provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio or video.
• RTP packet consists fixed RTP header, a possibly empty list of contributing sources and the payload data
• Does not address resource reservation.
• Does not guarantee quality-of-service for real-time services.
• independent of the underlying transport and network layers.
RTP header

<table>
<thead>
<tr>
<th>Version</th>
<th>Padding</th>
<th>Extension</th>
<th>Contributing Source Count (CC)</th>
<th>Marker</th>
<th>Payload Format</th>
<th>Sequence Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Timestamp

Synchronization Source Identifier (SSRC)

Contributing Source Identifier (CSRC)

Optional Header Extension

- Monotonically Increasing
- Media Specific
- Original Source or Mixer Identifier
- Mixers may combine multiple senders
RTP header (cont.)

- Version (2 bits) identifies the version of RTP
- Padding (1 bit) packet contains one or more additional padding octets
- Extension (1 bit) the fixed header must be followed by one header extension
- CSRC Count (4 bits) contains the number of CSRC identifiers that follow the fixed header Marker (1 bit) the packet contains marker bits
- Payload Type (7 bits) identifies the format of the RTP payload
- Sequence number (16 bits) increments by one for each RTP data packet sent, and may be used by the receiver to detect packet loss and to restore packet sequence.

<table>
<thead>
<tr>
<th>V</th>
<th>P</th>
<th>X</th>
<th>CC</th>
<th>M</th>
<th>PT</th>
<th>SEQUENCE NUMBER</th>
</tr>
</thead>
</table>

Ali Gulabi
gulabi_a@etech.haw-hambur.de
RTP header (cont.)

- Timestamp (32 bits) reflects the sampling instant of the first octet in the RTP data packet.
- SSRC (32 bits) field identifies the synchronization source.
- CSRC list (0 to 15 items, 32 bits each) identifies contributing sources for the payload. The number of identifiers is given by the CC field.

<table>
<thead>
<tr>
<th>TIME-STAMP</th>
<th>SYNCHRONIZATION SOURCE IDENTIFIER (SSRS)</th>
<th>CONTRIBUTING SOURCE IDENTIFIERS (CSRC)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
RTP Applications

• Designed for **multiparty multimedia conferences**
  – Storage of continues data
  – Interactive distributed simulation
  – Control and measurement applications
RTP control protocol (RTCP)

- For an RTP session there is typically a single multicast address; all RTP and RTCP packets belonging to the session use the multicast address.

- RTP and RTCP packets are distinguished from each other through the use of distinct port numbers.
RTCP (cont.)

- Periodic transmission of control packets to all participants in session
- Works in conjunction with RTP.
- Each participant in RTP session periodically transmits RTCP control packets to all other participants.
- Each RTCP packet contains sender and/or receiver reports
  - report statistics useful to application
- Statistics include number of packets sent, number of packets lost, interarrival jitter, etc.
- Feedback can be used to control performance
  - Sender may modify its transmissions based on feedback
Group size

• The group size is obtained by storing a table, containing an entry for each unique SSRC seen in RTP and RTCP packets.

• As members leave or time out, entries are deleted, and as new members join, entries are added.

• The table is thus highly dynamic.

• For large multicast sessions, such as an mbone broadcast or IP-based TV distribution, group sizes can be extremely large, on the order of hundreds of thousands to millions of participants.
Group size (cont.)

• There are three major scalability problems with RTP;

  1. Congestion due to floods of RTCP packets in highly dynamic groups;
  2. Large delays between receipt of RTCP packets from a single user;
  3. Large size of the group membership table.

• The reconsideration algorithm helps to alleviate the first of these. This document addresses the third, that of large group size tables.
Basic Operation

• Each participant maintains a key, $K$, of 32 bits, and a mask, $M$, of 32 bits.
• Mask = $m*1$ bits + 0 (the rest) bits
• When an RTCP packet arrives with some SSRC, $S$, rather than placing it in the table, it is first sampled.

$$D = (K*M == S*M)$$  (1)

* : AND
== : test for equality
D : the sampling decision

• If inequality (1) holds, the SSRC is stored in the table. If not, the SSRC is rejected.

*The key can be anything, but is usually derived from the SSRC of the user who is performing the sampling.*
SSRC's used by session participants are chosen randomly, and distribution is uniform.

\[ L = N \times 2^m \]

\[ p = \frac{1}{2^m} \]

L : group size estimate

m : the number of bits in the mask, M, which are 1

p : sampling probability
Performance

• the ratio of the standard deviation to mean of the estimate $L$ (coefficient of variation) is:

$$\sqrt{\frac{2^m - 1}{G}}$$

$G$ : actual group size

• if the target is a 1% standard deviation to mean, the sampling probability $p=2^{-m}$ should be no smaller than .5 when there are ten thousand group members.

• More generally, to achieve a desired standard deviation to mean ratio of $T$, the sampling probability should be no less than:

$$p > \frac{1}{1 + G \times T^2}$$
Increasing the Sampling Probability

- The above simple sampling procedure would work fine if the group size was static. However, it is not.
- The sampling probability must be made dynamic, and will need to increase and decrease as group sizes vary.
- The procedure for increasing the sampling probability is to start mask with $m=0$. Every received SSRC will be stored in the table, so there is effectively no sampling.
- At some point, the value of $m$ is increased by one. This implies that approximately half of the SSRC already in the table will no longer match the key under the masking operation.
when to increase \( m \)

- Let's say an RTP participant has a memory with enough capacity to store \( C \) entries in the table.
- The best estimate of the group is obtained by the largest sampling probability. This also means that the best estimate is obtained the fuller the table is.
- A reasonable approach is therefore to increase the number of bits in the mask just as the table fills to \( C \). This will generally cause its contents to be reduced by half on average. Once the table fills again, the number of bits in the mask is further increased.
Reducing the Sampling Probability

• When the group size decrease, the number of one bits in the mask must decrease as well.
• Not doing so will result in extremely poor estimates of the group size!!!
• When the number of bits decreases, the user should theoretically add back those users whose SSRC now match.
• However, these SSRC are not known, since the whole point of sampling was to not have to remember them.
• To compensate for this, some kind of algorithm is needed.
1- Corrective Factors

\[
fi(t) = \begin{cases} 
0 & , \quad t < ts \\
\frac{ts + cL(ts-) - t}{L(ts-) - L(ts+)} & , \quad ts < t < ts + cL(ts-) \\
0 & , \quad t > ts + cL(ts-) 
\end{cases}
\]

and the multiplicative factor as:

\[
gi(t) = \begin{cases} 
1 & , \quad t < ts \\
\frac{ts + 2cL(ts-) - t}{L(ts-) - L(ts+)} & , \quad ts < t < ts + cL(ts-) \\
1 & , \quad t > ts + cL(ts-) 
\end{cases}
\]

actual group size estimate \(L(t)\):

\[
L(t) = \sum fi(t) + N*(2**m) \quad , \text{additive factor}
\]

\[
L(t) = \prod N*(2**m)*gi(t) \quad , \text{multiplicative factor}
\]

C: the average RTCP packet size divided by the RTCP bandwidth for receivers

\(L(ts-)\): the group size estimate just before the change in the number of bits in the mask at time \(ts\)

\(ts-\): the time right before the reduction

\(ts+\): the time after reduction
2- Binning Algorithm

- There are 32 bins, same as the number of bits in the sample mask.
- When an RTCP packet from a new user arrives whose SSRC matches the key under the masking operation, it is placed in the $m^{th}$ bin (where $m$ is the number of ones in the mask) otherwise it is discarded.
Binning Algorithm (cont.)

• When the number of bits in the mask is to be increased, those members in the bin who still match after the new mask are moved into the next higher bin.
• Those who don't match are discarded.
• When the number of bits in the mask is to be decreased, nothing is done. Users in the various bins stay where they are.

However, when an RTCP packet for a user shows up, and the user is in a bin with a higher value than the current number of bits in the mask, it is moved into the bin corresponding to the current number of bits in the mask.

Finally, the group size estimate $L(t)$ is obtained by:

$$L(t) = \sum_{i=0}^{31} B(i) \times 2^i$$

Where $B(i)$ are the number of users in the $i^{th}$ bin.
To Compare

<table>
<thead>
<tr>
<th>Time</th>
<th>No Sampling</th>
<th>Binned</th>
<th>Additive</th>
<th>Multiplicative</th>
</tr>
</thead>
<tbody>
<tr>
<td>20000</td>
<td>5001</td>
<td>5024</td>
<td>5024</td>
<td>5024</td>
</tr>
<tr>
<td>20250</td>
<td>4379</td>
<td>4352</td>
<td>4352</td>
<td>4352</td>
</tr>
<tr>
<td>20500</td>
<td>3881</td>
<td>3888</td>
<td>3900</td>
<td>3853</td>
</tr>
<tr>
<td>20750</td>
<td>3420</td>
<td>3456</td>
<td>3508</td>
<td>3272</td>
</tr>
<tr>
<td>21000</td>
<td>3018</td>
<td>2992</td>
<td>3100</td>
<td>2701</td>
</tr>
<tr>
<td>21250</td>
<td>2677</td>
<td>2592</td>
<td>2724</td>
<td>2225</td>
</tr>
<tr>
<td>21500</td>
<td>2322</td>
<td>2272</td>
<td>2389</td>
<td>1783</td>
</tr>
<tr>
<td>21750</td>
<td>2034</td>
<td>2096</td>
<td>2125</td>
<td>1414</td>
</tr>
<tr>
<td>22000</td>
<td>1756</td>
<td>1760</td>
<td>1795</td>
<td>1007</td>
</tr>
<tr>
<td>22250</td>
<td>1476</td>
<td>1472</td>
<td>1459</td>
<td>582</td>
</tr>
<tr>
<td>22500</td>
<td>1243</td>
<td>1232</td>
<td>1135</td>
<td>230</td>
</tr>
<tr>
<td>22750</td>
<td>1047</td>
<td>1040</td>
<td>807</td>
<td>80</td>
</tr>
<tr>
<td>23000</td>
<td>856</td>
<td>864</td>
<td>468</td>
<td>59</td>
</tr>
<tr>
<td>23250</td>
<td>683</td>
<td>704</td>
<td>106</td>
<td>44</td>
</tr>
<tr>
<td>23500</td>
<td>535</td>
<td>512</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>23750</td>
<td>401</td>
<td>369</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>24000</td>
<td>290</td>
<td>257</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>24250</td>
<td>198</td>
<td>177</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>24500</td>
<td>119</td>
<td>129</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>24750</td>
<td>59</td>
<td>65</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>25000</td>
<td>18</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Security Considerations

- The use of SSRC sampling does not appear to introduce any additional security considerations beyond those described in [1]. In fact, SSRC sampling, as described above, can help somewhat in reducing the effect of certain attacks.
- RTP, when used without authentication of RTCP packets, is susceptible to a spoofing attack.
- Attacker can send many packets, each with different SSRC, that match the key. This would cause the group size to inflate exponentially.
- However, with a random hash applied, an attacker cannot guess those SSRC which will match against the key.
- In fact, an attacker will have to send \(2^{**m}\) different SSRC before finding one that matches, on average.
References

• RFC 2762       RTP Sampling       February 2000
  – Authors' Addresses
    Jonathan Rosenberg
dynamicsoft
200 Executive Drive
West Orange, NJ 07052
USA
EMail: jdrosen@dynamicsoft.com

Henning Schulzrinne
Columbia University
M/S 0401
1214 Amsterdam Ave.
New York, NY 10027-7003
USA
EMail: schulzrinne@cs.columbia.edu

• MULTIMEDIA SYSTEMS, IREK DEFEE
• Multicast Services, Lawrence A. Rowe, University of California, Berkeley
Questions

???