Impact Analysis of Cheating in Application-Level Multicast

Masayuki Higuchi s1090176 Supervised by Hiroshi Toyoizumi

Abstract

Therefore this paper researches the impact of cheating nodes in application-level multicast overlay trees, and focuses on selfish nodes acting independently, cheating about their distance measurements during the control phase building or maintaining the tree in HBM protocol. Group communication over the Internet is very important for various service, and an application-level multicast is efficient communication technology. A technique whereby hosts or end-nodes are organized into an overlay distribution tree without any specific support from the network. It is used efficiently in the peer-to-peer streaming service, Sharecast, Skype and so on, but also it has some problems. It causes unfair for the users by the node's position in the tree. As a result, the impact in cheating were different according to the tree structure. Also this paper researches countermeasures against cheating.

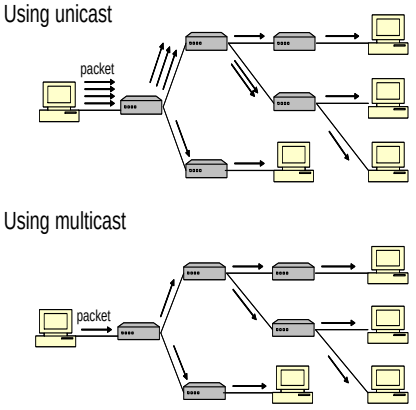

Figure 1: Comparison of unicast with multicast. In unicast, stream duplicate data in network, but in multicast only sender to transmit a single copy of data.

1 Introduction

Recently, communication technology in the Internet is very important for various service in the Internet, satellite TV distribution, software distribution, stock quote streaming, Web caching, and multimedia conferencing. These are examples of applications that require one-to-many or many-to-many group communication, and so efficient and safe communication is needed.

Communication over network has three kinds of forms, unicast (one-to-one communication), multicast (one-to-many communication), and broadcast (one-to-many communication). Multicast transmits the same data to plural hosts called a multicasting group in a network. On the other hand, broadcast transmits data toward many and unspecified partners. Figure 1 shows comparison of unicast with multicast.

Multicast enables efficient group communication by allowing the sender to transmit a single copy of data, with network elements such as routers and switches making copies as necessary for the receivers. Thus multicast reduces the computational load at the sender, as well as the number of copies of data on the network, so it is possible to communicate at a high baud rate.

We identify multicast security as one of the important problems to solve for the successful deployment of group communication applications. For example, investors would like a guarantee that the stock quotes being delivered via multicast are indeed authentic. In summary, popular applications of multicast require data integrity, access control, and privacy [6]. Also, multicasting technique is used efficiently in the peer-to-peer service, Sharecast [7], Skype [1], and so on.

This paper, through simulation, focuses efficiency on group communication.

2 Multicast

2.1 IP Multicast

Generally multicast refers to the IP multicast [5]. IP multicast is a system with which a receiver establishes a delivery path and receives data distribution. Between a sender and a receiver, the duplicate of data and a channel setup are performed by each multicast router under the delivery tree which consisted of multicast routers, so all routers that perform multicasting must be multicast routers, but maintenance of an infrastructure is difficult. Also, it is unreliable because of the best-effort communication by IP layer.

2.2 An Application-Level Multicast

An application-level multicast [2] can solve problems in IP multicast. Application-level multicast is a technique whereby hosts or end-nodes are organized into an over-

lay distribution tree without requiring any specific support from the network, has been proposed mainly as a way to palliate to the lack of deployment of native IP multicast in production networks.

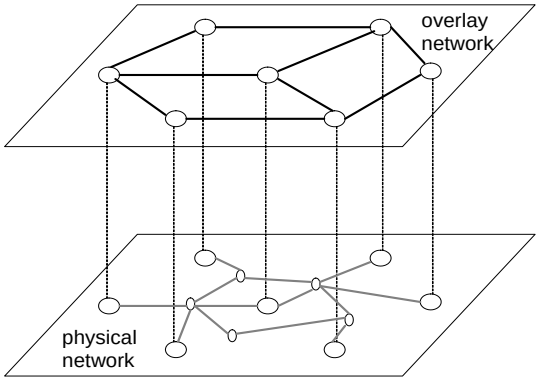

Figure 2: Overlay network and Physical network

The overlay network is an important mechanism in the feature of application-level multicast, and it is a virtual link constructed with the transport level. Even when the link between nodes cuts in physical network, the packet can be received from another link. Figure 2 shows difference between overlay network and physical network.

Next, we give a brief overview of application-level multicast protocol, a host-based multicast (HBM). HBM protocol [3] is example of a centralized approach to application-level multicast. They have a session controller node which gathers distance information from all of the group nodes and calculates the overlay tree which it uses to inform each node of its neighbors.

In HBM, the construction and maintenance of the overlay tree is under the control of a single host, the rendezvous point (RP) or controller. Periodically and asynchronously, each group member measures its distance to all the others (or a subset of them) and reports these to the RP which thus knows the identity of each group member and the communication costs between them. The RP is then responsible for the overlay topology calculation and its dissemination among the group members.

Although HBM is a general protocol that does not restrict the properties of its overlay topology, the topology used in this study is a degree-bounded shared tree of minimum cost, based on RTT distance metrics.

2.3 Sharecast: An Example of Multicast Service

Multicast technology is used in peer-to-peer streaming service. The service which deliveries the video/audio streaming data is desired with the increased spread of broadband environment in the Internet. In the ordinary client-server model, the bottleneck of a streaming server's processing power actualizes and it is in the tendency for a service provider's burden to become large. In order to solve such a problem, the new type of distributed streaming data delivery architecture based on the concept of peer-to-peer system was developed, in which streaming data are relayed among user-nodes in cascade manner. Sharecast [7] is one of the peer-to-peer system (see Figure 3: Sharecast). When join to the service, new member send IP address, MAC address, channel ID that want to see, and version to administrator, and administrator send back access node lists. Finally, new member request a connection to relay-node that administrator has send.

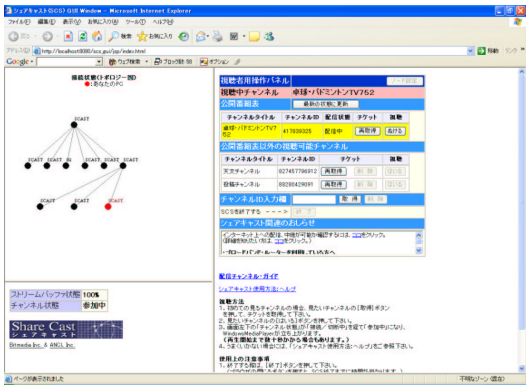

Figure 3: Sharecast: multicasting service

3 Cheating Method

3.1 Reasons of Cheating

In Sharecast, many users on the Internet receive, view and listen to streaming data, and streaming data are relayed towards other users at same time, so it can use without high performance server. However the user relay streaming data, and the load hangs to user's machine. If one node has to relay streaming data to many users, the user's machine become very busy. In other words, users don't want to be root or sub root, that is, user that relay to many users may cheat distance information, and try to be node that only receive streaming data. Therefore this paper believes that cheating nodes have a great impact, through simulations, focuses the impact of cheating nodes.

3.2 Simple Cheating Method

An HBM cheat always reports a distance of 5 to the source, and adds 10 seconds to the RTT distances it mea-

sured to the rest of the group. An HBM cheat also delays by 10 seconds any measurement probes it receives from any other group member. This probe delaying action is mandatory since otherwise the RP could easily detect cheats by comparing the *A* to *B* and *B* to *A* RTT measurements. If they differ significantly, the RP could easily conclude that one of *A* and *B* has a suspect behavior. Then, after cross-checking with other metrics evaluations where *A* and *B* are implicated, the RP could easily determine which node is cheating.

The cheat is thus aiming to become one of the source's children, while having no children at all.

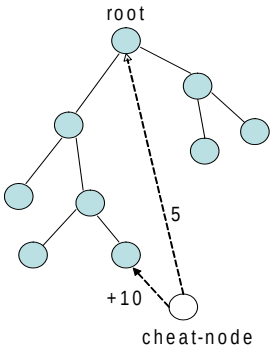

Figure 4: Example of cheating method in the tree

3.3 Performance Measures for Application Level Multicast

Several indicators are widely used to evaluate the performance of application-level multicast protocol. Two such classical performance indicators [4] are the link stress and the relative delay penalty (RDP).

3.3.1 The link stress

The link stress is a measure of the network efficiency of the application-level multicast protocol and is defined as the number of redundant copies of a data packets carried on a network link. For example, if a node have to relay to three nodes, the link stress is three. The maximum stress is therefore the maximum number of duplicates seen by any single network link, while the average stress is the sum of duplicates divided by the total number of network links making up the branches of the tree. A major goal of all application-level multicast protocols is, of course, to keep the value of these stress indicators as small as possible, since higher network stress levels (especially maximum stress) indicate higher risks of network congestion.

Stress_ratio = stress/stressref, where stressref is the corresponding stress observed when all receivers behave in an honest way.

We will be interested in the maximum stress ratio as a measurement of the impact of cheats on the underlying physical network. Indeed, maximum stress represents the highest load created by an application-level overlay tree on any network link, and thus the maximum stress ratio gives a good idea about the way risks of congestion evolve in the presence of cheats. Note that a stress ratio smaller (resp. greater) than 1 represents an improvement (resp. deterioration) compared with the case without any cheat.

3.3.2 The relative delay penalty

The relative delay penalty (RDP) is a measure of the penalty paid by a receiver for receiving data on an application-level tree rather than directly from the source. It is defined as the ratio TD/UD, where TD is the tree delay, that is the latency from the source to the receiver observed along the tree; and UD is the unicast delay, that is the networked delay resulting from direct communication from the source to the receiver. Figure 4 shows unicast delay and tree delay. The average RDP (over all the receivers) and maximum RDP (i.e. worse penalty) are therefore good indicators of the tree efficiency of the application-level multicast protocol.

RDP_ratio = RDP/RDPref, Where RDPref is the RDP of a receiver observed when all receivers behave in an honest way. Note that since the unicast delay is dictated by the physical topology and routing in the underlying network, it is independent of whether a receiver cheats or not, and we therefore have

$$RDP_{ratio} = \frac{(TD/UD)}{(TD_{ref}/UD_{ref})} = \frac{TD}{TD_{ref}}, \qquad (1)$$

since UD = UDref.

To have a better view of the influence of cheating in application-level multicast, we will segregate the receivers in a group of cheats and a group of honest receivers, and measure average, minimum and maximum RDP ratios in each group. This will allow us to not only study the impact of cheats on the performance observed by honest nodes, but also study the effects independent, selfish cheats have on each others. Note that as the overall goal is always to try and minimize RDP, a RDP ratio smaller (resp. greater) than 1 represents an improvement (resp. a deterioration), with a minimum ratio therefore representing the best improvement and a maximum ratio representing the worst deterioration.

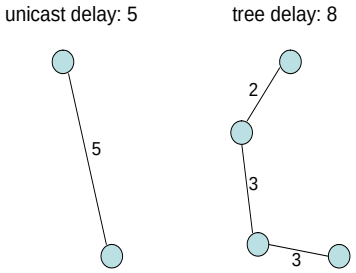

Figure 5: unicast delay and tree delay

4 Effects of cheating

4.1 In Sharecast

It caused unfair for the users by the node's position in the distribution tree. The first reason is that the gap was caused in the streaming, that is, the streaming was delayed seven seconds on the average between parents-node and child-node. Next reason is connected switch processing when the parents-node comes off. When the relay-node comes off, the nodes that exists in the subordinate position there cannot receive the streaming data until the distribution tree is restructured. It takes about one minute to change the connection in sharecast, so the user cannot see the video stream that flowed for the switch of the connecting.

4.2 Cheating in HBM

We used three types of distribution trees. First, showed example of the impact of cheating, and then showed worst impact of cheating. Finally, simulated in general.

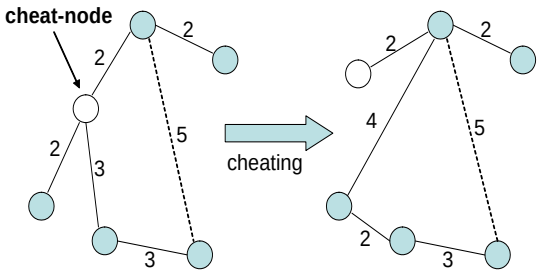

Figure 6: Example of cheating

	before cheat	after cheat
the link stress	2	3
the maximum RDP	8/5	11/5

Table 1: cheating in figure5

Table 1 shows impact of cheating in figure 5, and figure 5 shows that it is efficient tree, and the dotted line represents unicast delay. Before cheat, the cheat-node in figure 5 is the bad node of condition, because the node have to relay, but after cheat, the node can comfortable. For other nodes this cheating causes negative impact on the link stress and the RDP, so it has bad influence in network.

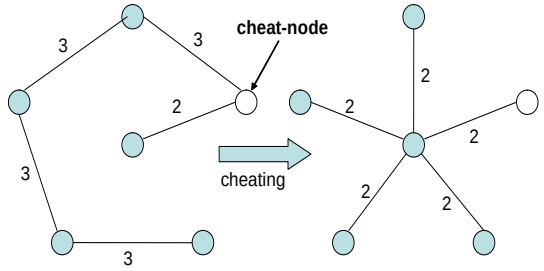

Figure 7: Impact of cheating in worst case

	before cheat	after cheat
the link stress	1	5
the maximum RDP	14/2	2/2

Table 2: cheating in figure 6

Table 2 shows impact of cheating in figure 6, and this cheating cause serious damage to network link, but it has positive impact in regard to the RDP. All node's RDP become UD in the tree like figure 6. Consequently, cheat-node stand to gain substantially in RDP when cheat in as far away from source as possible.

Table 3 shows impact of cheating in figure 7. When each node has the same number of children, off course, impact is negative on the link stress and RDP, and the influence power of the link stress is the same wherever cheat. In figure 7 the link stress increases in three links.

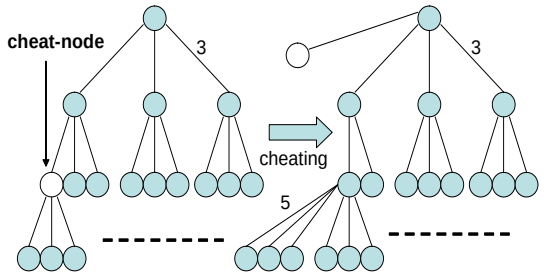

Figure 8: Impact of cheating in general

	before cheat	after cheat
the link stress	3	6
the maximum RDP	9/7	11/7

Table 3: cheating in figure 7

For the cheat-node it is most efficient cheating to cheat with n-1 when depth of tree is n, because the cheat-node that has the child, and the node that is the furthest from the source.

5 Counter Measures against Cheating

We understood cheating cause bad influence in network. Consequently, Countermeasures against cheating are described below.

1. Users receives the data from two or more nodes. As a result the influence at the switch of the connection can be decreased.

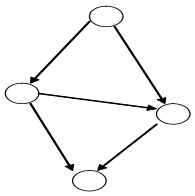

Figure 9: Counter measure; receive from two nodes

2. To detect the cheating, transmit ping to the router that connect one hop short of the cheat-node, and measure RTT metrics, and compare with RTT that cheat-node returned. However, when the distance between cheat-node and the router that connect one hop short of the cheat-node is very long, this counter measure is not effective.

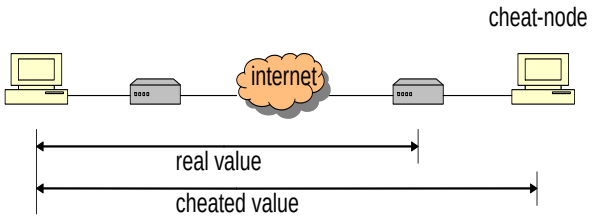

Figure 10: Counter measure; Compare the RTT metrics

6 Conclusion

In multicasting service, it caused unfair for the users by the node's position in the tree. The user wants to receives it to the source as much as possible at a near position, and don't want to become the relay-node, so the meaning exists in cheating. Then, evaluate the impact of cheats on the performance of the overlay trees, and found that the cheating has a great impact on network from two performance indicators. Also, the countermeasures is effective measures in theory. As a future work in this paper, through simulations, confirm the effectiveness of them.

Acknowledgments

I would like to thank Prof. Hiroshi Toyoizumi for his advice and Prof. Mark R. Freiermuth for his advice improving my English writing.

References

[1] S. Ikejima., "Gratis IP phone software, Skype," Nikkei Communications, No.428, no. 15, Dec. 2004, pp. 105-111 (in Japanese).

[2] L. Mathy, V. Roca, and A. El-Sayed, *A Survey of Proposals for an Alternative Group Communication Service*, IEEE Network, 2003.

[3] V. Roca and A. El-Sayed, *A Host-Based Multicast Solution for Group Communications*, IEEE intl. Conf. Networking, 2001.

[4] L. Mathy, N. Blundell, V. Roca, and A. El-Sayed, *Impact of Simple Cheating in Application-Level Multicast*, Dept. Computer Sciences, Univ. of Lancaster, UK, 2004.

[5] D. Kosiur, *The Handbook of IP Multicasting*, Ohmsha, Ltd, 1999 (in Japanese).

[6] T. Hardjono and L. R. Dondeti, *Multicast and Group Security*, Artech House, 2003.

[7] Sharecast, "Peer-to-Peer Streaming Service," http://www.scast.tv/scast/