SOSP: An Efficient Multicast Fault Isolation Scheme for Multi-Source Sessions

Heonkyu Park, *Student Member, IEEE*, Dongman Lee, *Member, IEEE*, Kyungran Kang, *Member, IEEE*, and Kilnam Chon, *Member, IEEE*

***Abstract*—This letter proposes a one-way source probing mechanism for fault isolation in multi-source multicast sessions. Routers involved in multicast record a routing path based on periodic probes from sources, and receivers isolate a fault region using the probes. We introduce a probe suppression mechanism to enhance the performance. The proposed scheme reduces message complexity and enhances fault isolation latency, which improves scalability. Furthermore, analytical formula is proposed to estimate suppression time, which provides maximum performance for a given network status.**

***Index Terms*—Computer networks, fault location, network fault diagnosis, protocols.**

I. Introduction

FAULT *isolation* is defined as a task of locating the on-tree router(s) or on-tree link(s) which is the origin of a fault [1]. We use the term *fault* when it results in a change to at least one receiver's path from the source. A fault may result from the network problems such as router crash, link failure, and significant packet loss. Fault isolation is a necessary activity for network operators or system administrators who are responsible for supervision of their corresponding network [2]. However, isolating a fault in multicast tree is a difficult task because of the dynamic nature of group membership, anonymity of members, and use of User Datagram Protocol (UDP) that provides no feedback [3].

Several models [1]–[4] have been suggested to diagnose a fault in multicast trees, but they are generally limited to single-source sessions. In practice, there are many multi-source multicast sessions, e.g., large-scale replicated database, large-scale multimedia conferencing, and Web cache protocols. If we apply the existing models to a multi-source multicast session, the number of control messages and time required to isolate a fault increases exponentially [5]. In this letter, we propose an efficient multicast fault isolation scheme for multi-source sessions, called *Suppressed One-way Source Probing* (SOSP). The main goal of the scheme is to isolate a fault in multi-source multicast sessions with short latency while maintaining low message complexity. For practical deployment, we present an analytical formula to estimate optimal suppression time in routers in the multicast tree in order to achieve short fault isolation latency.

Manuscript received February 13, 2004. The associate editor coordinating the review of this letter and approving it for publication was Dr. I. Fair.

H. Park and K. Chon are with the Korea Advanced Institute of Science and Technology (KAIST), Daejeon 305-701, Republic of Korea (e-mail: hkpark@cosmos.kaist.ac.kr; chon@cosmos.kaist.ac.kr)

D. Lee is with the Information and Communications University, Yuseong-gu, Daejeon, Republic of Korea (e-mail: dlee@icu.ac.kr)

K. Kang is with Ajou University, Suwon 443-749, Republic of Korea (e-mail: korykang@ajou.ac.kr)

Digital Object Identifier 10.1109/LCOMM.2004.835321

II. Proposed Scheme

A. Assumptions

The proposed scheme requires sources, receivers, and routers in the multicast routing tree for a given session to cooperate. The source is an end participant that sends data to the multicast address, the receiver is an end that joins the multicast address and receives the data from the sources, and a router is an internetworking device relaying source's traffic to next router or receiver. The sources send probes periodically and the receivers perform fault isolation by comparing consecutive probes. The routers in a given multicast routing tree compress the probes to avoid the probe implosion. Before explaining the proposed scheme in detail, we describe some important assumptions for the scheme.

- Every source maintains *probe timer*. This timer expires every *source probing interval*, which is a constant in a session.
- A *probe* consists of header and body. The header includes the number of paths and the hop count of each routing path it contains. The body contains routing paths each of which is a list of the addresses of the source and the routers that the probe has passed by.
- Each router maintains *suppression timer* per multicast address and combines the probes that are received during the *suppression time*.
- Each router maintains *path buffer* to store a routing path for each source from a probe that has been received during the suppression time.
- Every receiver maintains *history buffer* for each source. It is a time-stamped list of probes that the receiver has seen.

B. Fault Isolation Algorithm

In the beginning, each source multicasts data and starts the probe timer. Each router empties the path buffer and sets the suppression timer as not activated. Every receiver empties its history buffer. When probe timer at a source expires, the source multicasts to the receivers a probe that contains its address. Then, it restarts the probe timer.

When a router receives a probe, it activates its suppression timer if the timer is not activated. It extracts a routing path from the probe for each source, and stores it to the corresponding path buffer. If the buffer is not empty, then the router updates the timestamp of the stored one. When suppression timer at a router expires, the router appends its address to the end of each routing path stored in the path buffers. It combines routing paths