

# **MTREEDX: A MULTICAST NETWORK DIAGNOSIS TOOL**

**Jaiwant Mulik**

*Computer and Information Sciences Department  
Temple University, Philadelphia*

[jmulik@temple.edu](mailto:jmulik@temple.edu)

**Phillip Conrad**

*Computer and Information Sciences Department  
Temple University, Philadelphia*

[conrad@acm.org](mailto:conrad@acm.org)

**Brian Drake**

*Information Services and Advanced Technology Division  
Goddard Space Flight Center, NASA*

[brian.drake@gsfc.nasa.gov](mailto:brian.drake@gsfc.nasa.gov)

**Saroj Biswas**

*Electrical and Computer Engineering Department  
Temple University*

[saroj.biswas@temple.edu](mailto:saroj.biswas@temple.edu)

**Musoke Sendula**

*Electrical and Computer Engineering Department  
Temple University*

[hsendaul@nimbus.temple.edu](mailto:hsendaul@nimbus.temple.edu)

## **1. Introduction**

MTreeDx is a tool that is being developed to fulfill a gap in most currently available Multicast Network Management Tools. Specifically, this tool is being developed as an aid to diagnose problems in NASA's multicast network. Management of the NASA multicast network present several unique research challenges.

## **2. Motivation**

The images and other data acquired from space telescopes is distributed to research institutions using a multicast network. The network manager would like to prevent unauthorized hosts from joining the group. Detecting senders is

not difficult; the tool can simply listen for transmissions from unknown sources on the group. Detection of unauthorized receivers can be tricky. Unauthorized receivers on a subnet with no authorized receiver can be detected by the presence of an "extra branch" in the multicast distribution tree. We are investigating techniques to use mtrace [3] or similar tools to generate and display the current multicast tree. Guaranteeing the detection of unauthorized receivers on a shared media subnet with authorized receivers is provably impossible. We are investigating router-based techniques to detect unauthorized hosts.

The second problem is that of monitoring the multicast traffic. Several commercial and open source tools are available that require specific feedback from the network. For example, a multicast monitoring extension to a popular commercial network management system requires SNMP capability within the network. Mhealth [2] requires rtp reports to display loss statistics. In the absence of rtp sources or widespread SNMP support we are currently evaluating techniques that involve placing "monitoring stations" at strategic locations within the network. These stations could use techniques similar to those developed for the MINC [1] project.

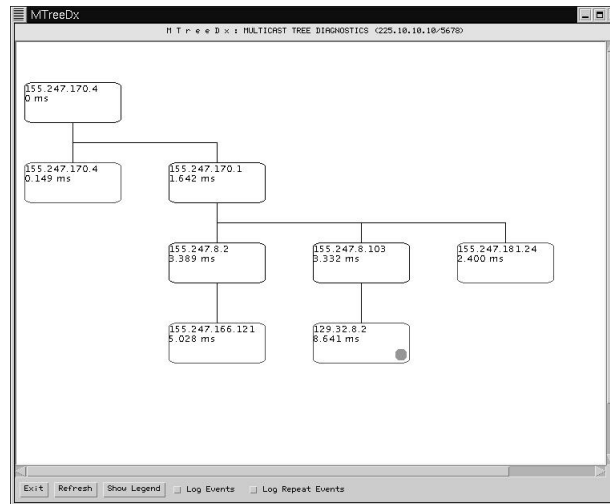
### 3. Features of MTreeDx

Currently, the main features of MTreeDx are:

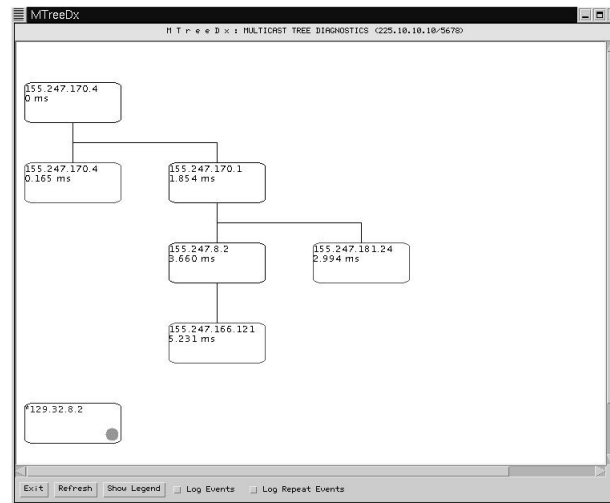
- 1 Displays the tree topology of group members from the perspective of the monitoring station [Fig. 1]. The group membership information is obtained from a pre-configured list of hosts. Each host display includes its IP address and the last measured round-trip time from the monitoring host. We are currently investigating router-based techniques to obtain group membership.
- 2 Provides visual information about all senders, active, and inactive.
- 3 Provides visual alarm, and logs identity of unauthorized sender [Fig. 3]. A list of authorized senders is pre-configured. Any sender not found in the authorized list is deemed unauthorized.
- 4 Provides visual information about authorized receivers.
- 5 Provides visual information about currently unreachable hosts [Fig. 2]. Unreachable hosts are moved from the tree display and displayed in a separate list.
- 6 Provides color-coded indications of the status of a node.
- 7 Multiple sessions of MTreeDx can be run in parallel.

Another challenge of creating a tool like MTreeDx comes from its requirement as an integrated tool for both security and traffic monitoring. We want to be able to create functionality that is common to both security and traffic

*MTreeDx: A Multicast NetworkDiagnosis Tool*



*Figure 1.* MTreeDx with one active sender



*Figure 2.* MTreeDx with an unreachable host

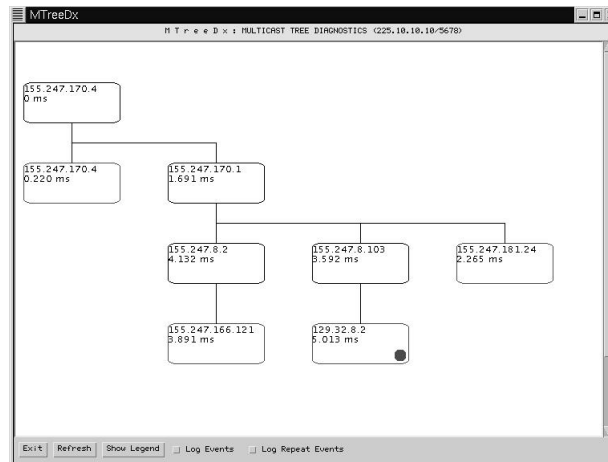


Figure 3. MTreeDx with one intruder

monitoring. For example, we are developing an intelligent display and logging system. Visual alarms are an important characteristic of both security and traffic monitoring. Given potentially large networks, we are developing intelligent interfaces that will allow the network administrator to prioritize, based customizable rules, portions of the network currently in view.

## References

- [1] Multicast-based inference of network-internal characteristics. <http://www-net.cs.umass.edu/minc/>.
- [2] Makofske D. B and Almeroth K. C. MHealth: A Real-time Multicast Tree Visualization and Monitoring Tool. Technical report, University of California, Santa Barbara. Makofske's Master Thesis.
- [3] Fenner W. and Casner S. A 'traceroute' facility for IP multicast. Technical report, IETF, August 1998. Work in progress.