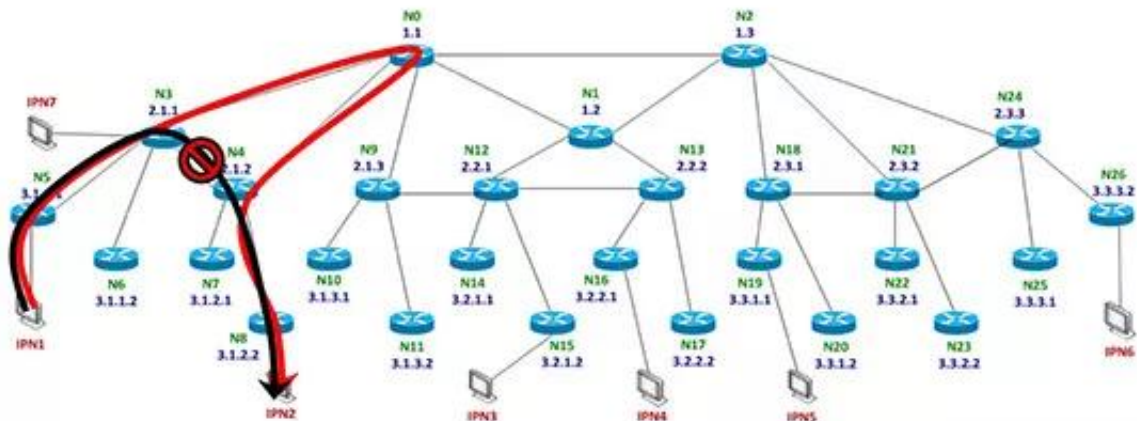# Team creates high-speed internet lane for emergency situations

May 22 2017, by Scott Bureau

RIT researchers developed a faster, more reliable network protocol that can be used for emergency situations. In the image, the black line represents the original path the data takes, the red circle with a line through it indicates the link that was broken, and the red line is the updated path that the protocols learn after updating themselves. In a demo, the newly created MNLR protocol recovered six times faster than the older protocol. Credit: Rochester Institute of Technology

In a disaster, a delay can mean the difference between life and death.

Emergency responders don't have time to wait in traffic—even on the congested information superhighway.

That's why researchers at Rochester Institute of Technology are developing a faster and more reliable way to send and receive large amounts of data through the internet. By a creating a new network protocol, called Multi Node Label Routing protocol, researchers are essentially developing a new high-speed lane of online traffic, specifically for emergency information.

The project, funded by a grant from the National Science Foundation and US Ignite, aims to improve the information flow between emergency responders at the scene of an incident and decision-makers at the office of emergency management.

"Sharing data on the internet during an emergency is like trying to drive a jet down the street at rush hour," said Jennifer Schneider, the Eugene H. Fram Chair in Applied Critical Thinking at RIT and co-principal investigator on the project. "A lot of the critical information is too big and data heavy for the existing internet pipeline."

Schnieder said data-dense information sharing was a major issue during recent disasters, including Hurricane Irene and Hurricane Sandy. Emergency responders were not able to quickly share critical information. That's why RIT students studying environmental health and safety—several of whom are actual responders themselves—worked with emergency professionals to gather data and create scenarios that support research into this real-world problem.

For example, in a flood event, emergency responders may need to share LIDAR mapping images, 911 requests and deployments, cell phone location data, video chats, voice recordings and social media communications. When that information has to compete with civilians

tweeting about the disaster and messaging loved ones, the network is taking on more than it can handle.

"It is normal to have links and routers fail, and as the network topography changes, packets can be delayed, rerouted or lost," said Nirmala Shenoy, a professor in RIT's Information Sciences and Technologies Department and principal investigator of the project. "This unreliability and delayed information can render loss of important data in the LIDAR images and other information."

To solve this problem, Shenoy, along with co-principal investigator Erik Golen, a visiting assistant professor in RIT's Information Sciences and Technologies Department, and a team of five graduate students created the Multi Node Label Routing (MNLR) protocol. It is designed with an immediate failover mechanism—meaning that if a link or node fails, it uses an alternate path right away, as soon as the failure is detected. The new protocol runs below the existing internet protocols, allowing normal internet traffic to run without disruption.

The new protocol does not depend on routes discovered by either Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF). It discovers routes based on the labels assigned to the routers. The labels in turn carry the structural and relational connectivity information among routers.

"The new protocol is actually of very low complexity compared to the current routing protocols, including BGP and OSPF," Shenoy said. "This is because the labels and protocols leverage the connectivity relationship that exists among routers, which are already sitting on a nice structure."

In a demo this May, the team put the protocol to the test over the U.S. GENI (Global Environment for Network Innovation). The group transferred data using BGP and the new MNLR protocol. They ran the

data between 27 nodes representing the network of the incident control center, the 911 call center and the office of emergency management.

While BGP took about 150 seconds to recover from a link failure, MNLR recovered in less than 30 seconds. The recovery metrics showed that the new MNLR protocol transferred information faster and more reliably than existing protocols in the event of network failures and topology changes.

"While BGP has a recommended default keep alive message interval of 60 seconds, MNLR is not so constrained," said Shenoy. "In fact, MNLR can detect failure with one missing keep alive message as the failure or topology change information will be flooded internet wide, which can be expected in certain cases with BGP."

Shenoy said that the main issue with current protocols stems from the fact that they were invented several decades ago and not for the type of network scenarios experienced in current internet. Thus, BGP and OSPF are unreliable and that manifests when a link fails, she said."If you receive an email five minutes late, that is still acceptable," Shenoy said. "But in an emergency situation, the implicit impact of these serious network problems truly come to light."

In an emergency situation, information becomes too old after about eight minutes, adds Schneider, who leads RIT's Collaboratory for Resiliency and Recovery. "We are on the cusp of generating and collecting all this great technical information, but we need to be able to share it and create the situational awareness decision-makers need."

The team is continuing to develop and enhance the MNLR protocol. In the future, the team plans to test and implement the protocol in emergency situations.