Researchers at RIT seek to solve the problem of looping with Meshed Tree Protocol

August 14 2015, by Scott Bureau

A team of RIT computing security faculty and graduate students is creating Meshed Tree Protocol, the next standard for loop avoidance that will make our computer networks more reliable, faster and more secure against cyber attacks.

The next breakthrough in computing that will make our computer networks more reliable, faster and more secure against cyber attacks is being developed at Rochester Institute of Technology.

A team of computing security faculty and graduate students is creating Meshed Tree Protocol, the next standard for loop avoidance in network switching operations—one with near-zero failover time and an emphasis on cybersecurity. To develop and write the new standard, the RIT team has formed an IEEE working group. In the future, the team hopes to see its protocol used in industry as a superior alternative to current standards.

The new standard, called Meshed Tree Protocol, is designed to solve a problem of miscommunication commonly seen in a network of computers. All large computer networks must use some version of loop-avoidance in order to fix this miscommunication and function properly.

"Since the first loop avoidance protocol was invented in 1985, people have been trying to improve upon the process," said Nirmala Shenoy, a professor of computing security. "The significant reduction in convergence time, combined with its simplicity and security, indicates that Meshed Tree Protocol would be a superior candidate to resolve looping issues in switched networks."

The problem of looping normally arises in computer networks of more than five devices. Companies use network switches at layer 2 to link together computers and help receive, process and forward data to the right devices. In large networks, the arrangement of these links—also known as the topology—can change quite often. It is beneficial to have multiple links between switches, in case one of the links fails due to machine or human error.

However, when a message is fired off to a receiver that isn't functioning or doesn't exist, these redundant links can cause loops. The messages circulate forever, exponentially procreating, and can cause broadcast storms that slow down the network and negatively impact communications.

To prevent these loops, scientists created Spanning Tree Protocol and later Rapid Spanning Tree Protocol, a method of logically blocking certain bridge ports. However, the port blocking causes a failover, or a temporary network outage of 30 seconds or 100 milliseconds, respectively.

"One hundred milliseconds of network outage might not impact the typical home user, but it will make a difference at a research cluster or on the heart rate monitors at a hospital," said Bill Stackpole, RIT professor of computing security.

The spanning tree topologies also lack redundancy and the ability to balance traffic in the network. Newer protocols, including Shortest Path Bridging (SPB) and TRILL, work to alleviate these problems, but are complex and costly.

"Rather than having a failover that generates a pile of traffic that has to be unblocked, our solution actually precomputes every possible path," said Stackpole, "It's like missing a turn while you are driving and having your GPS automatically know a new route, without ever having to recalculate."

Meshed trees are novel in that they do not use the traditional single tree from one root concept. A meshed tree is a collection of all possible paths and because the pathways are already installed, failover time is immediate. The Meshed Tree Algorithm, created by the RIT team, also uses knowledge of the incoming ports and the structure of the meshed trees to detect attempts to modify or interfere with the topology.

From a security perspective, Meshed Tree Protocol will provide a mechanism to authenticate valid members of the meshed tree switch group—something that no existing protocol has offered to date. The protocol will feature four levels of security with different levels of

authentication and encryption.

"Loop avoidance protocols were never built with security in mind," said Daryl Johnson, professor of computing security. "People were always more concerned with actually making it work."

If someone could gain physical access to a port on your switch, he or she could theoretically generate a denial of service packet that can take down your infrastructure, Johnson said. The Meshed Tree Protocol is built with security in mind and has practices in place to prevent these kinds of breaches.

While most devices currently use Rapid Spanning Tree Protocol, the RIT Department of Computing Security group hopes that the speed, simplicity and security of Meshed Tree Protocol will incite a change in the industry.

More information: To learn more about Meshed Tree Protocol and the IEEE working group, go to standards.ieee.org/develop/wg/1910_WG.html

Provided by Rochester Institute of Technology