PROJECT 1 CHECKPOINT

Team Members: Sriram, Aditya, Rakesh,Vikas

Work done so far

****

1. Design

- Our system will have 4 administrators talking to the SDN / OpenFlow Control. All of them will have the same view of the Network. The communication would be on TCP over SSL.
- Voting would be done using Apache Zookeeper. Each Administrator on Link failure will send a configuration file with a confidence score. The confidence score will be a combination of End to End Delay, Packet Loss and Achievable Bandwidth. These metrics are verified by the switch intelligence layer. Only Voters / Administrators that claim to have a higher confidence score would be allowed to vote in subsequent epochs. This reduces the amount of time the Administrators take to come to a consensus.
- We have discussed our design with Professor Porter and have received feedback.

2. Configured OpenFlow on Mininet.

What Next

****

1. Implement the adversary model, switch intelligence layer and the distributed voting mechanism.
2. Inspired from Pathlets, we will evaluate our Algorithm against 2 topologies - random graphs and an internet like graph.
3. We got some good food for thought from Prof Porter on how much should each metric contribute to the confidence score. We would like to play around with that.

What results will we show in our Poster - Graph Description

****

PRIMARY GRAPH

****

In both the topologies, we would like to measure the effect of the number of malicious administrators and voting epoch durations on the time overhead of the voting protocol.
Our first graph will be a plot between the number of malicious administrators (X axis) and the duration from link failure detection to agreement on a fix (measured in seconds). This would be done for both the topologies and while we will plot the exact values for upto 4 malicious administrators, we would do an asymptotic analysis for higher numbers. Qualitatively we expect that a higher number of malicious administrators will lead to more routing rounds on average. This graph will help us quantitatively estimate on how much can a higher ratio of malicious administrators do in delaying the computation of the alternate route.

SECONDARY GRAPHS (Based on Time)

****

In this plot we would like to study the relationship between the confidence score complexity and epoch interval time. As we incrementally add different metrics to determine the best route the epoch interval would increase as the switch intelligence layer will have to do more work in validating the confidence score. We will study the effect of adding new metrics with respect to the voting epoch length.

The plot is similar to the primary graph described above.
X axis:- Number of malicious administrators
Y axis:- The duration from link failure detection to agreement on a fix (in s).
We will have multiple plots corresponding to different combinations of metrics and different voting epoch lengths.

We would also like to address one crucial concern that was raised during the discussion of our approach with Prof Porter. Each Administrator sends a scalar quantity as a confidence score rather than a vector which would indicate the confidence in each of the required metrics. There is a possibility that several vector combinations yield the same scalar score which in turn leads to complications when aggregating results and summarizing conclusions. We would like to address this issue by helping Network Administrators advertise vectors and come up with an algorithm that prioritizes the vector based on the needs of the application.