PROBLEM STATEMENT

We propose to address the malicious administrator problem in SDN's, where a network administrator mis-configures a correctly functioning controller in a way that adversely affects network performance. This is a serious problem as it could have serious cost / availability implications. In cases where there is a performance issue without a network outage this problem is harder to detect.

APPROACH

We consider an adversary model where k administrators out of n have gone rogue. These malicious administrators create policies to choose undesirable paths for packet forwarding. We consider a recent SIGCOMM paper - Fleet for inspiration. There are two main approaches mentioned in the paper. The single configuration approach where n-k administrators agree on a single configuration. The second approach described is a multi-configuration model which deals with each administrator having his own configuration to deal with link failures. The paper gives results only for the first approach. The model proposed by fleet for the single configuration approach involves each of the network administrators proposing their configuration to circumvent the detected link failure and all the other administrators are required to vote for or against the proposal within a designated interval of time termed epoch. In our model, we try and obligate the voting process and automate the configuration selection by intelligently evaluating the configurations against predefined network metrics and eventually choosing the best possible configuration in less time.

RELATED WORK

FORTNOX, FRESCO and VeriFlow deal with security policies in order to prevent rule conflicts. Avant-guard focuses on identifying and preventing DoS attacks in SDN. TopoGuard detects attacks that poison the controller's view of the network topology. SPHINX is an SDN application to prevent various attacks launched by malicious end hosts and compromised SDN switches. We plan to use the existing work to give us a better understanding of the various solutions possible and if needed incorporate some of the techniques used in these works to improve our proposed solution.

PLAN OF ACTION

We try and implement our model using Openflow SDN controller installed on a mininet network simulation environment. We develop an intermediate layer between the controller and the switches known as the switch intelligence layer which is responsible for evaluating the proposed configurations against the current network metrics using P4. We can then analyse if the configuration chosen by the switch layer was indeed the best one among all proposed configurations. We then perform network diagnostics and compare the performance and efficiency of our proposed model against Fleet's model.

SCHEDULE

11/03/2015: Configuration of Openflow on mininet and network diagnostics protocol using P4

11/24/2015: Implementation of Fleet algorithm and analysis.

12/08/2015:Implementation of our proposed algorithm and comparison with Fleet