Early-stage anomaly detection and mitigation in large-scale networks

Thien Xuan Phan, Kensuke Fukuda

National Institute of Informatics, Japan

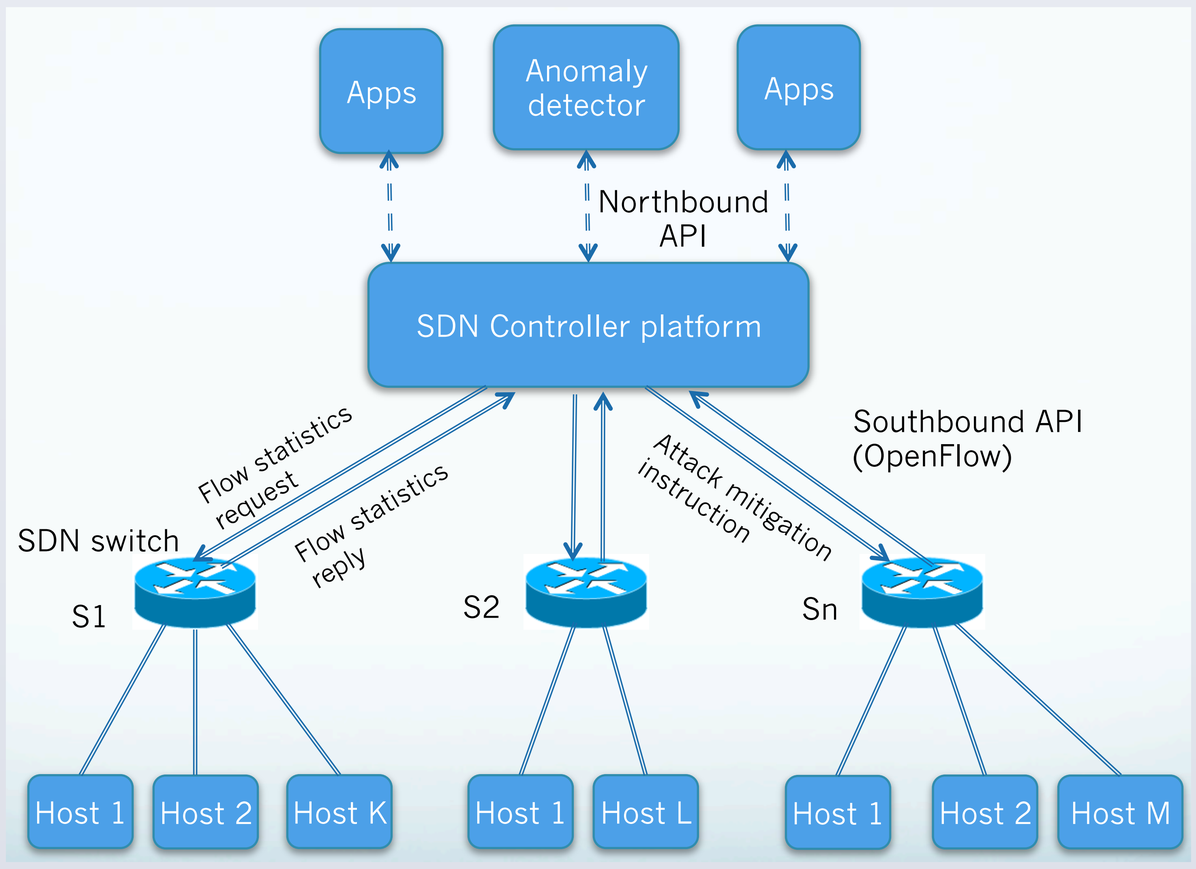
Motivation

- Increasing number of anomalies such as misconfiguration and remote attacks
- These Internet traffic anomalies cause a serious problem for the users and Internet service operators:
  - Affect directly availability of network services
  - Prevent legitimate users from accessing the networks resources
- Existing anomaly detection approaches:
  - Based on conventional network architecture
  - Heavy processing to extract features for traffic analysis
    - Delay time in detection
    - Inflexibility and latency in reaction
    - Even more challenged in large scales networks

Solution requirements and challenges

- Solution requirements:
  - Detect anomaly traffic in an early-stage
  - Quickly react to mitigate the possible attack
  - Be applicable for large-scale network including a number of distributed networks
- Challenges:
  - Similarity between abnormal traffic and normal traffic
  - Early-stage detection is challenging since retrieving data for analysis is time consuming
  - Challenges in implementation, deployment and experiment solution in large-scale networks

Proposed solution



- Anomaly detector:
  - Receive network traffic statistics from SDN controller platform
  - Analyze the statistics (based on 5 tuples: source IP, source port, destination IP, destination port, protocol)
  - Run anomaly detection algorithm to find out anomalies
  - Alert when anomalies were found
- SDN controller platform:
  - Query flow statistics from SDN switches by sending Flow Statistics Request to the switches
  - Pass the queried statistics through Anomaly Detector
  - Get alert from Anomaly Detector if anomalies were found
  - Mitigate attacks by blocking attack traffic (via Soundbound API)

Anomaly detection method

- 2 main phases:
  - Query statistics from switches
  - Calculate traffic volume changes in flows to find out anomaly
- Processing steps:
  - ① SDN switch forwards first packet of every flow to controller -> controller add a Flow Entry in which Match Field including 5 tuples {scr IP, src Port, dst IP, dst Port, Proto}
  - ② Detector creates a Monitoring Table to record traffic volume changes in flows, including fields: {5-tuples, packet count, byte count}
  - ③ For every time interval *M* minutes (M = {10, 15, 30,...}), repeat *N* times:
    - i. Controller sends an Individual Flow Statistics Request to switch
    - ii. Individual Statistics Reply from switch include a list of flow statistics of all flow entries existing in its Flow Table -> controller delegate it to Detector
    - iii. For each statistics in the list (correspond to a flow) -> Detector save information (as an item) to Monitoring Table (MT)
    - iv. For each item in MT, Detector calculate traffic volume change in that flow (using ASTUTE-based algorithm)

- ASTUTE-based algorithm (calculate changes of flow traffic volume):
  1) Substract packet-count of this query to packet-count of previous query (volume change is called δf,i)
  2) Assume F: number of observing flows, compute sample mean δi, sample standard deviation σi of volume changes -> computer the K' (Astute assessment value, AAV):

$$\hat{\delta}_i = \sum_{f=1}^{F} \frac{\delta_{f,i}}{F} \quad \therefore \quad \hat{\sigma}_i = \left[\sum_{f=1}^{F} \frac{(\delta_{f,i} - \hat{\delta}_i)^2}{F-1} \right]^{\frac{1}{2}} \qquad K' = \frac{\hat{\delta}_i}{\hat{\sigma}_i} \sqrt{F}$$

  3) Check if |K'| larger than K(p) -> mark observed flow as anomaly. Threshold K(p): examined through experiment, initial values: {3, 6, 9}

Evaluation plan

- SDN controller platform: Floodlight
- SDN network deployment: OpenvSwitch (software switch), Pica8 (physical switch)
- Evaluation metrics:
  - Detection time
  - Accuracy: detection rate (DR), false positive rate (FP)
  - Effectiveness of mitigation: time for react/recover network services after attack detected

Impact

- Potentially applied to build anomaly detection systems for large-scale networks
- Protect networks in real-life: organizational networks, company networks, research institutes, universities,...

Conclusion

- Anomaly detection architecture based on SDN
- Anomaly detection method
- Deployment and experiment plan for solution evaluation

SOKENDAI - 2015 International Communication Program