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

Thien Xuan Phan [1]

[1] The Graduate University for Advanced Studies, Japan

Kensuke Fukuda [2]

[2] National Institute of Informatics, Japan

SUMMARY

Detecting and preventing the Internet traffic anomalies are crucial tasks to maintain the network services. Traditional network anomaly detection approaches are typically based on the conventional network architecture that demands heavy processing to extract feature information needed for traffic analysis, which results in the rather large amount of delay time to detect anomalous traffic in case of network attacks. In addition, the lack of a flexible network controlling infrastructure/mechanism in conventional network leads to the inflexibility in reaction against network attacks. Recent approaches base on Software-Defined Network (SDN) [1] show their flexibility and efficiency since they exploit the network management flexibility of SDN for anomaly detection and mitigation. However, these approaches can not deal with large number of flows and scalability issue is still unsolved. We propose an architectural approach for anomaly detection and mitigation which solve those limitations. We extend the current SDN switch with our minor extension module to support it perform efficiently with monitoring task, together with exploit the SDN infrastructure and protocol for anomaly detection/mitigation solution.

WHY SDN

- Fast query of flow-level statistics by SDN's Southbound API (OpenFlow) [2].
- Easily and quickly drop desired packets/flows by well-defined action sets -> mitigation becomes faster and simpler.
- SDN's network programmability and ability of applying changes for network controlling rules in real-time bring flexibility for our detecting system (easier for deploying, flexible in controlling/ modifying network behaviors for detection/mitigation).

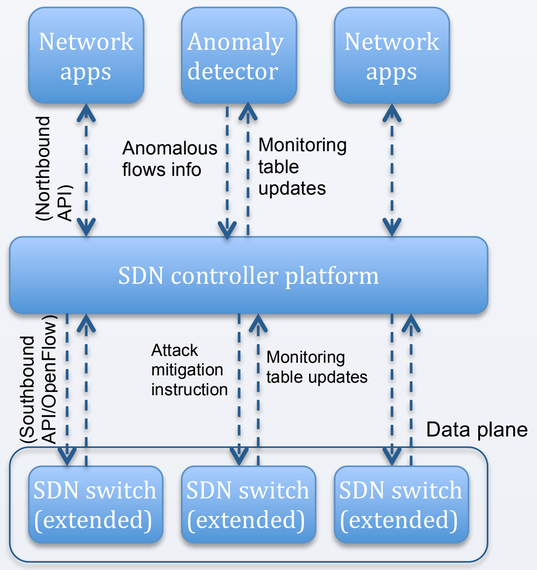
PROBLEM STATEMENT

- Current SDN-based proposals can not handle large number of flows in SDN switches.
- Heavy processing at controller in case of detecting large number of SDN switches.
- Rather large control-bandwidth consumption due to large frequency of control-messages and amount of data exchange between SDN switches and controller when querying network statistics for detection.

OUR APPROACH

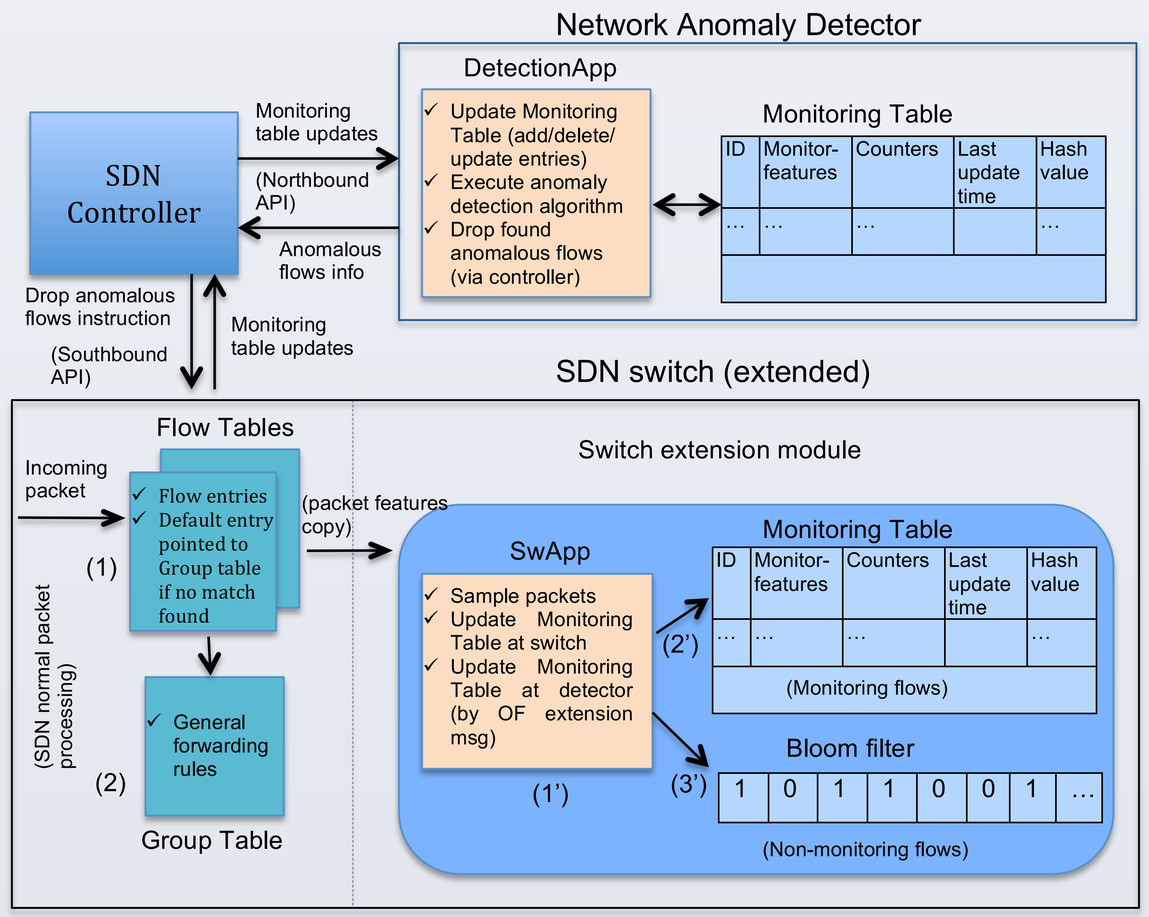
- Lightweight monitoring module at SDN switches that decrease amount of processing at controller and control bandwidth to achieve more scalability.
- Sampling mechanism at SDN switch allow it to handle large number of flows in anomaly detection.
- Conceptual architecture for anomaly detection and mitigation.

CONCEPTUAL ARCHITECTURE FOR ANOMALY DETECTION

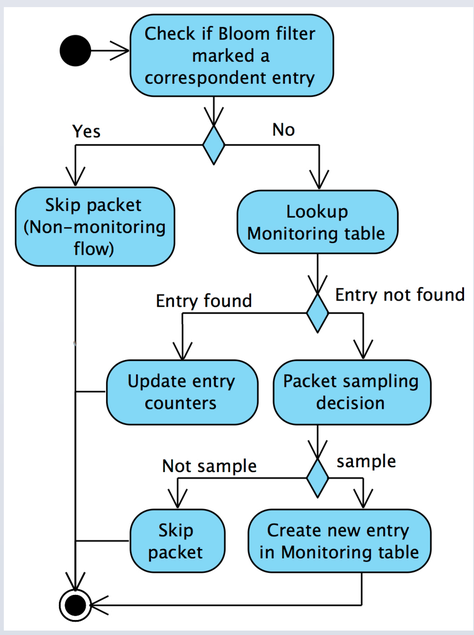


- Traffic flow monitoring at SDN switch (extended) via monitoring table/app.
- SDN switch send latest updates of monitoring entries to detector (through controller platform) in pre-defined frequency.
- Anomaly detection algorithm (e.g. [3]) executed in Anomaly detector to find out anomalous flows.
- SDN controller platform sends attack mitigation instruction (drop flows) based on anomalous flows information from detector.

SAMPLING AND MONITORING TRAFFIC FLOWS



- Incoming packet processed at flow tables, group table, meter table as usual.
- A copy of packet features passed through Switch extension module.
- Packet features for anomaly detection: {src addr, src port, dst addr, dst port, proto,...}.
- Monitoring table: monitor/update flow statistics.
- Bloom filter: mark non-monitoring flows.
- Sampling and monitoring workflow:



REFERENCES

[1] Open Networking Foundation, "Software-defined networking: The new norm for networks", ONF white paper, 2012.

[2] Open Networking Foundation, "OpenFlow switch specification – version 1.3.4", 2014.

[3] F. Silveira, C. Diot, N. Taft, R. Govindan, "ASTUTE: Detecting a different class of traffic anomalies", SIGCOMM 2010.

CURRENT PROGRESS AND FUTURE WORK

- SDN switch extension implemented on Lagopus switch.
- Experimental deployment: extended switch and Ryu controller.
- Evaluation of extended switch performance and detection system considered as future work.

National University SOKENDAI The Graduate University for Advanced Studies

Thien Xuan PHAN - Department of Informatics, 2-1-2 Hitotsubashi , Chiyoda-ku, Tokyo, Japan 101-8430 - Email: thien@nii.ac.jp