Real-time monitoring of SDN networks using non-invasive cloud-based logging platforms

Bartlomiej Siniarski & Cristian Olariu. Supervised by: Prof. John Murphy

1 Research Problem & Motivation

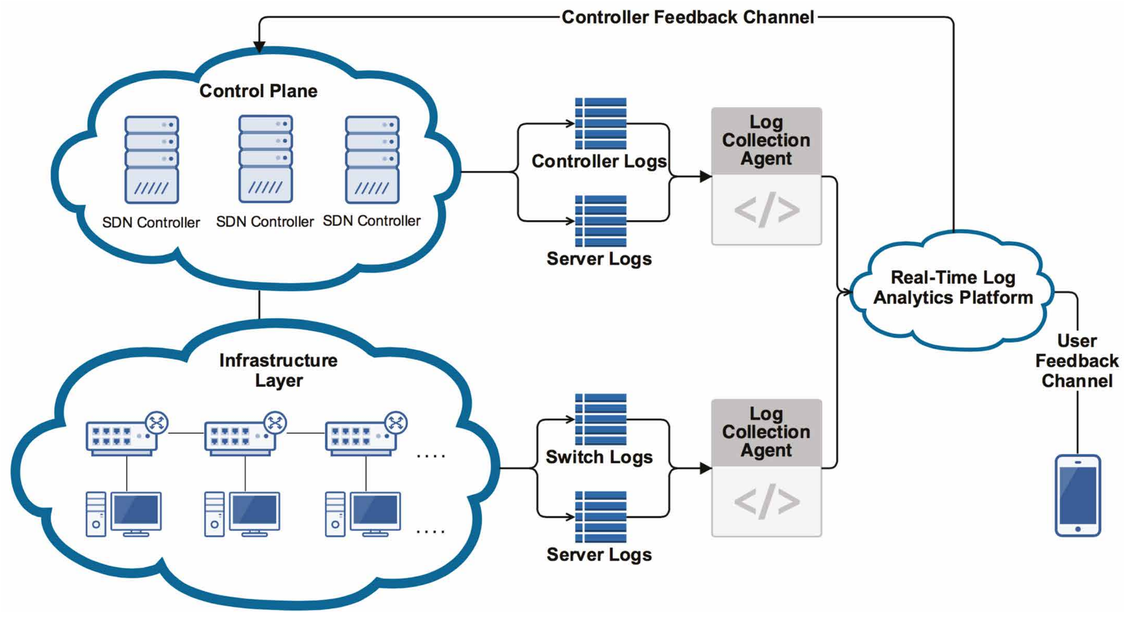
» The Software Defined Networking paradigm enables quick deployment of software controlled network infrastructures, however regardless of their size, monitoring SDN networks should be centralized and reliable to enable network administrators to get an instant feedback on a network's health.

» Research in the field of SDN security confirms that new methods and techniques must be considered and explored in order to enable the dynamic configurations in SDN security monitoring, detection, prevention and recovery capabilities.

» System health monitoring, overload detection and sophisticated alerting needs to be an integral part of any SDN network infrastructure in order to aid network managers in troubleshooting and early detection of potential problems.

» Monitoring should be "service aware" so that the network health can be mapped to its ability to carry the services required.

2 Solving the problem

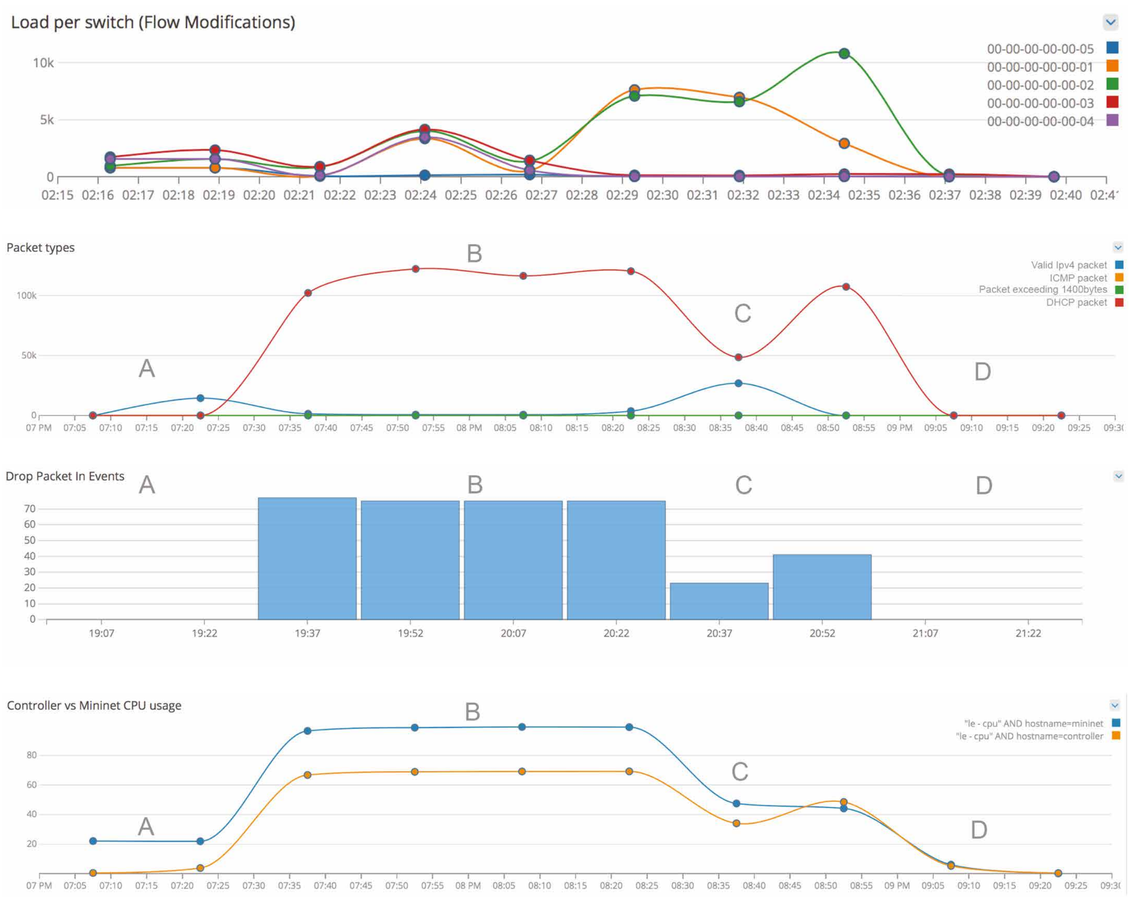


» Log events produced by a controller or a set of controllers can be collected by log management tool agent and periodically pushed to the log management and analysis platform deployed in the cloud.

» Additionally, all system metric logs produced by machines hosting SDN network components and controllers can be forwarded to the management tool. Logs from individual switches are also added in to the collection of log events for further correlation and analytics.

3 Approach

» Initial experiments use a virtualized network that can be controlled to create known problems.
» Analysis of log events from three unique locations: SDN controller, Open vSwitches and the servers hosting SDN controller.
» Correlate events with log data to yield an insight into the performance of the SDN network and its health.



4 Results

» Shown the usefulness of cloud-based log analysis engines for the evaluation of SDN network performance.

» SDN Network Health Metric was proposed to measure the health of SDN network based on symptoms gathered from log intelligence (0% - 100%)

» This work shows how to successfully identify when the network is being overloaded, identify malicious attacks and identify if the system has recovered successfully from an attack.

Future Work

» The preliminary work will be extended by enlarging the knowledge base of log events from system components

» Create the controller feedback channel to activate change

» Create a simple policy language that can be used with other SDN controllers.

» Generalize the approach for Service Aware SDN.

» Being able to get a rich insight into system performance, ultimately the work will form the basis of an automated feedback loop that can instruct the controller or switches to take protective steps to prevent system to collapse in the face of detected security violations.

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union
European Regional Development Fund
SOUTHERN Regional Assembly
Promoting our Region