Effect of Intermittent Interval Sampling on Software-Defined DMZs

Richard Habeeb, Ethan Koch, Zachary Throneburg, Haotian Wu, Dr. Caterina Scoglio, Dr. Dan Andresen, Dr. Don Gruenbacher

Electrical and Computer Engineering

Kansas State University

Background

Past studies at K-State show that campus network performance can be improved through the introduction of a software-defined demilitarized zone (DMZ) [1]. software-defined dynamic DMZ configurations typically trust traffic based on a whitelist or fuzzy logic; however, not all traffic in dynamic DMZs is guaranteed to be benign. Thus, research is needed to expand the security of software-defined DMZs.

Intermittent sampling of intervals of flows could potentially increase security confidence. While, Dividing or splitting a flow contradicts the design of OpenFlow (OF, an industry standard for SDN), redirecting a flow for a short interval could be an effective way to sample packets and improve security. In order to evaluate the viability of this method, **we analyzed how much packet loss would occur during flow redirection at large bandwidths.**

Topology

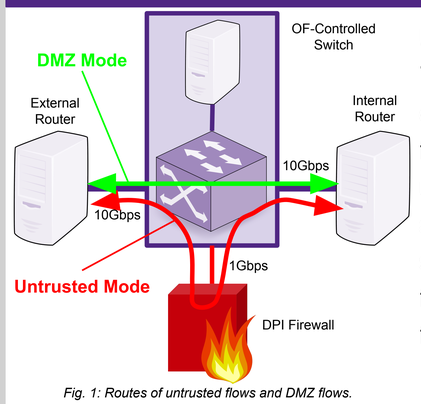

Fig. 1: Routes of untrusted flows and DMZ flows.

Untrusted Mode:

This routing path is the default for all new traffic flows in the OF switch. In untrusted mode all packets are routed from client to server through the DPI firewall bottleneck. See figure 1.

DMZ Mode:

After a flow has been deemed acceptable to enter the DMZ, it is redirected through the switch, this greatly improves the performance of the flow but has potential drawbacks.

Interval Sampling Design

To realize intermittent interval sampling, we used an OF controller software called POX. Our application, built on POX API, automatically redirects flows in an out of the DMZ based on programmable criteria (we used flow-size for our experiments). Additionally, our application will time out DMZ mode flows, switching them back to untrusted mode after a certain time period. This allows the DPI firewall device to effectively sample traffic, thus increasing security measures.

Hypothesis

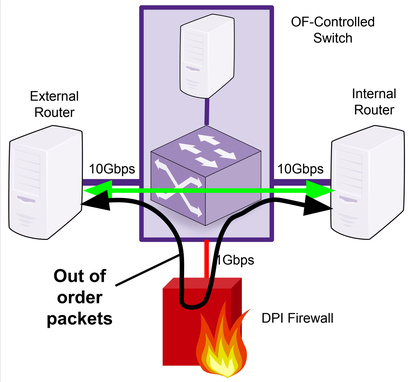

Fig. 2: Cause of lost packets during redirection.

Our hypothesis is that some out of order packets would occur during redirections into DMZ mode, but not into Untrusted mode. This is because we can estimate the expected, worst-case retransmission count in DMZ redirections. This is computed based on the round-trip time (RTT) between the switch and the DPI firewall. Because of that time, the packets transferred through the firewall immediately before a redirection are expected to be out order (see figure 3). Figure 4 contains a chart of this calculation. Because these out of order packets are scattered through 1 RTT of traffic, all this traffic may be retransmitted in worst-case scenarios of the H-TCP congestion control protocol.

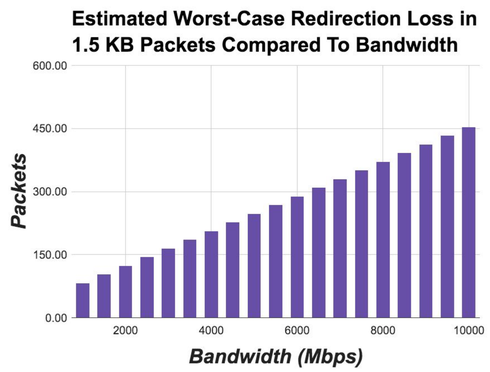

Fig. 3: Chart of expected redirection losses per bandwidth.

Thus, as bandwidth increases we expect the number of packets retransmitted to increase. Finally, we expected negligible losses for flow redirection out of the DMZ mode.

Methods

This experiment was conducted first by implementing a 10G SDN switch using Open vSwitch. The performance between client and server were then tuned to perform well at upwards of 9 Gbps traffic. We implemented the interval sampling POX controller, and further tuned the stability of the network. From there, we used a network performance tool called Nuttcp to generate our TCP flows in this experiment. An automation process conducted Nuttcp tests from 1 Gbps to 9 Gbps flows and parsed the bandwidth and retransmissions into a tabular format. Data from 24 switches was recorded per bandwidth.

Analysis of Results

The results from our experiments show high variance of packet losses. The scale of the two graphs (figures 4 & 5) indicate that packet loss is about 3 times less for redirections out of the DMZ; however, losses are still occurring. (analysis continued on next panel...)

Analysis of Results (Cont.)

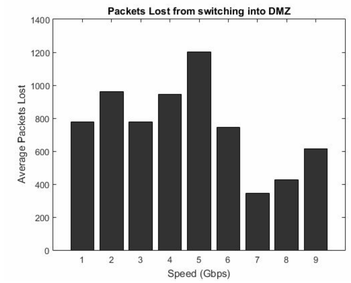

Fig. 4: Chart of measured switch-in losses per bandwidth.

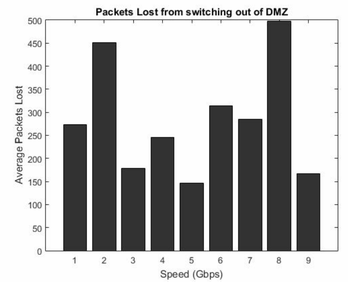

Fig. 5: Chart of measured switch-out losses per bandwidth.

Our measurements also show worst-case losses are far greater than our expectations. This observation indicates that unaccounted retransmissions are occurring during the switching process. Additionally, the worst case loss appears to trend downwards, contrary to our initial calculations.

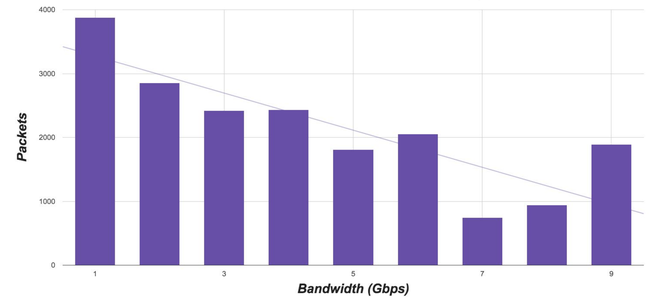

Fig. 6: Chart of expected redirection losses per bandwidth.

Conclusion and Future Work

This study provides evidence that other factors play into retransmission count and packet loss during redirection in this topology. This study also demonstrates how retransmission counts have high variance, and much more data is needed to show trends more clearly. Furthermore, our measurements show how intermittent interval sampling will be subject to some loss which could be significant for some applications. Finally, this study hints that intermittent interval sampling seems to perform at near 10 Gbps line speed well thus increasing network performance while allowing tunable security.

References & Acknowledgements

This research is based on work supported by the Electrical Power Affiliates Program (EPAP) at Kansas State University, and by the National Science Foundation under Grant No. 1341026. Experiments conducted using resources on Global Environment for Network Innovations (GENI) and equipment in the K-State Smart Grid Lab.