OpenFlow based Network Intrusion Detection System

Student: Sujayyendhiren Ramarao Srinivasamurthi

E-mail: sxr1043@rit.edu

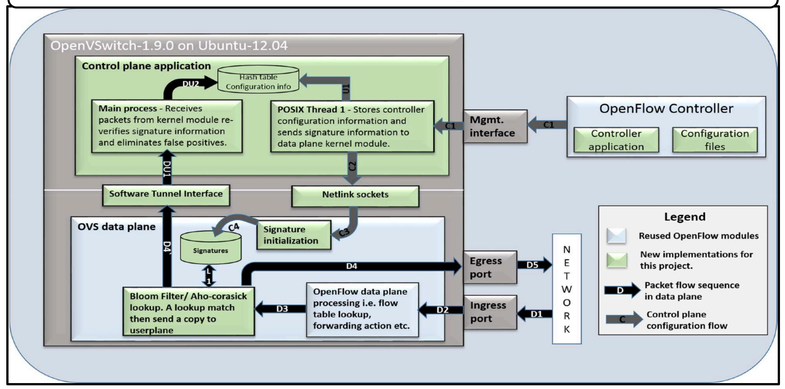
Advisor: Prof Minseok Kwon and Prof. Kaiqi Xiong

Email: jmk@cs.rit.edu and kxxics@rit.edu

Abstract

OpenFlow based Network Intrusion Detection System (NIDS) is an attempt to build an efficient security mechanism in a Software Defined Network (SDN). The data plane of this software switch comprises of Bloom filter (in approach-1) or Aho-corasick algorithm (in approach-2) that runs multiple pattern matching while OpenFlow provides a robust, efficient and modular framework for filtering and configuration in the data plane.

Architecture diagram



Components Of NIDS

Control Plane*:* Control plane receives, parses, and stores configuration information pertaining to the signatures received from the controller. Parsed configuration is stored at a hash table. Signature information is sent from control plane to the bloom filter via netlink interface.

Netlink Interface and tunnel interface**:** Signatures are sent from control plane process to the kernel module via Netlink sockets. Tunnel interface sends data packets from data plane (kernel) to control plane application.

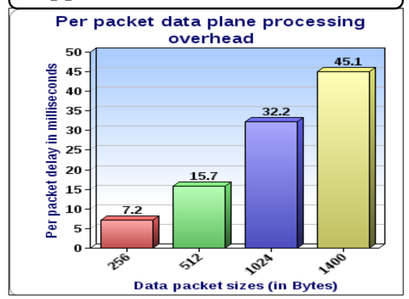
Data plane*:* Data plane receives signature information from control plane. Signature is inserted into Bloom filter. Data lookup with the filter is hooked in the OpenFlow data plane, which is a kernel module.

Controller: OpenFlow controller is embellished to transmit configuration information to the control plane.

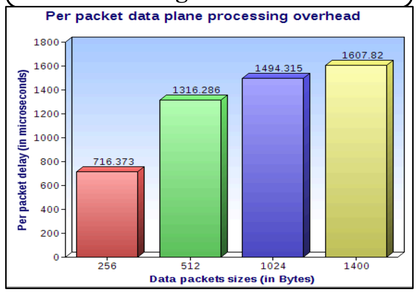
Key operation is the data plane execution:

1. All packets undergo OpenFlow flow table lookup.
2. Packets are scanned for pattern matches by a lookup into the data structure.
3. On a malicious pattern match normal forwarding is accompanied by a copy sent to control plane.
4. Control plane verifies with a hash table lookup.
5. Lookup success results in a action to drop or log and in case of false positive no action is performed.

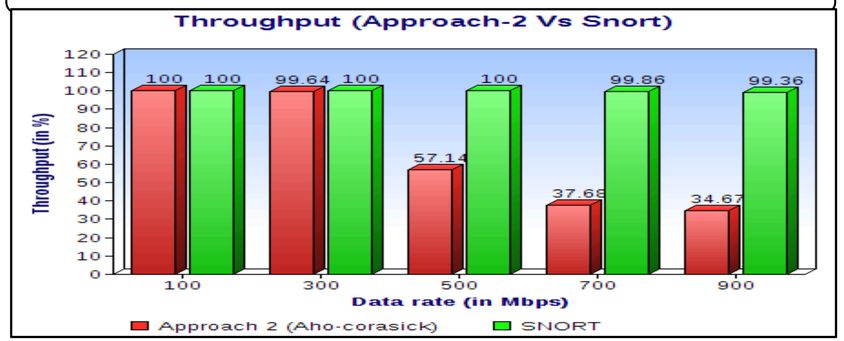
Approach-1 With Bloom Filters



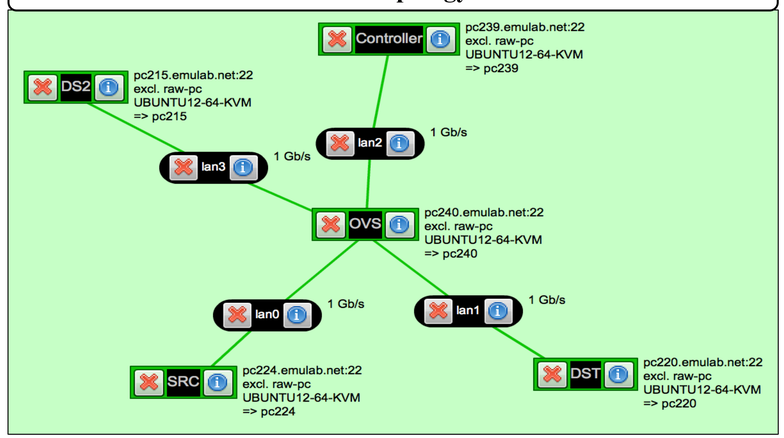
Approach-2 With Aho-corasick algorithm



Throughput - SNORT Vs Approach2



Test Topology



Test topology summary

The experimental setup comprises of minimum of four machines. OpenFlow controller acts as an administrator, it is named as 'Controller', this PC holds the NIDS signatures in the configuration files.

The machine placed at the center has the OVS kernel module (openvswitch.ko) with the a hook corresponding to the data structure in use, this is essentially the NIDS data plane. The NIDS control plane resides at the userspace on this machine.

The PC marked as 'Source' generates data plane packets for testing. All the data plane packets are destined to the PC marked as 'Destination.' Packet generator client transmits packets from 'Source' and is destined to 'Destination.'

Future Work

- Dynamic threat identification - Currently the threat is identified based on known signatures. In dynamic threat identification we may analyze the network traffic based on the network protocols and traffic activity patterns.
- This implementation may be ported to a hardware and introduced to real time traffic.

Conclusion

- NIDS is modular. It consumes less data plane memory. It can fit a number of hardware configurations and different kinds of networks.
- Our design eliminates any possibilities of false positives .

geni Exploring Networks of the Future

NETWORK SCIENCE AND ENGINEERING

National Science Foundation WHERE DISCOVERIES BEGIN