EL-SEC: ELastic Management of SECurity Applications on Virtualized Infrastructure

Nabeel Akhtar Ibrahim Matta Ali Raza Yuefeng Wang
Boston University

Abstract

- The elastic management of a Network Function (NF) refers to load management across the virtual network function (VNF) instances and the autonomic scaling of the VNF instances as the load on the NF changes.
- EL-SEC is an autonomic framework to elastically manage security NFs on a virtualized infrastructure.
- EL-SEC uses Software Defined Networking (SDN) and Network Function Virtualization (NFV), along with a modular approach for the different EL-SEC components which can be easily extended.
- Use case: Snort IDS deployed on the GENI testbed using EL-SEC.
- Results:
    - Control theoretic ***Elastic Manager*** can effectively manage resources for NFs.
    - Elastic resource management enables quicker detection of attacks.

EL-SEC Components (Fig. 1)

- **MONITORING APPLICATION:** Monitoring application gathers VFs state information and provide it to the different components of the EL-SEC system.

- **ELASTIC MANAGER:** Elastic Manager is responsible for adding/removing VF instances as the load on the system changes. Moreover, it balances load across current VF instances.

- **ATTACK ANALYZER:** Attack Analyzer gathers state information of VFs running security functions and analyzes it to identify and block attackers' traffic.

- **FORWARDING CONTROLLER:** Forwarding Controller gets the load balancing information from the Elastic Manager and attackers' information from the Attack Analyzer. It uses this information to install the forwarding rules in the network to either balance load across VFs or block the attackers' traffic.

Use Case: (Fig. 2) Instantiating EL-SEC on GENI

- **RINA MONITORING APPLICATION:** RINA monitoring application is used to gather the CPU load and Snort alerts from the VF instances and provide this information to the *Elastic Manager* and *Attack Analyzer.* It uses the Pub-Sub model to gather this information.

- **PI/PID CONTROLLER:** Elastic Manager is implemented using *Proportional Integral (PI)* and *Proportional Integral Derivative (PID)* Controller.

  - PI Controller:

$$x_{i+1}(t) = x_{i+1}(t-1) + K_i \; e_i(t) \qquad i \geq 1 \qquad (1)$$

where $e_i(t) = L_i(t) - T_i$: Error in load value

$L_i(t)$: Load on VNF i

T_i : Target load on VNF i

$x_{i+1}(t)$: Fraction of flow diverted to VNF i + 1

K_i : Controller's gain

  - PID Controller:

$$x_{i+1}(t) = x_{i+1}(t-1) + K_i^p e_i(t) + K_i^d \Big(e_i(t) - e_i(t-1)\Big) \quad (2)$$

- **ATTACK ANALYZER:** Attach Analyzer uses application state information of the VNF instances to detect attacks on the system. The Snort IDS alerts are processed by the Attack Analyzer and the attackers' list is provided to the OVS controller to block the attack traffic.

- **OVS CONTROLLER:** RYU OVS controller adds the forwarding rules to the OVS switch to:
  - Balance the load across the VNF instances
  - Block the attack traffic

- **TRAFFIC GENERATION:** Background traffic is generated using the *nping* application. This generates load on the system. With background traffic, the port scanning attack is generated using the *nmap* application.

Reference

https://github.com/akhtarnabeel/ELSEC

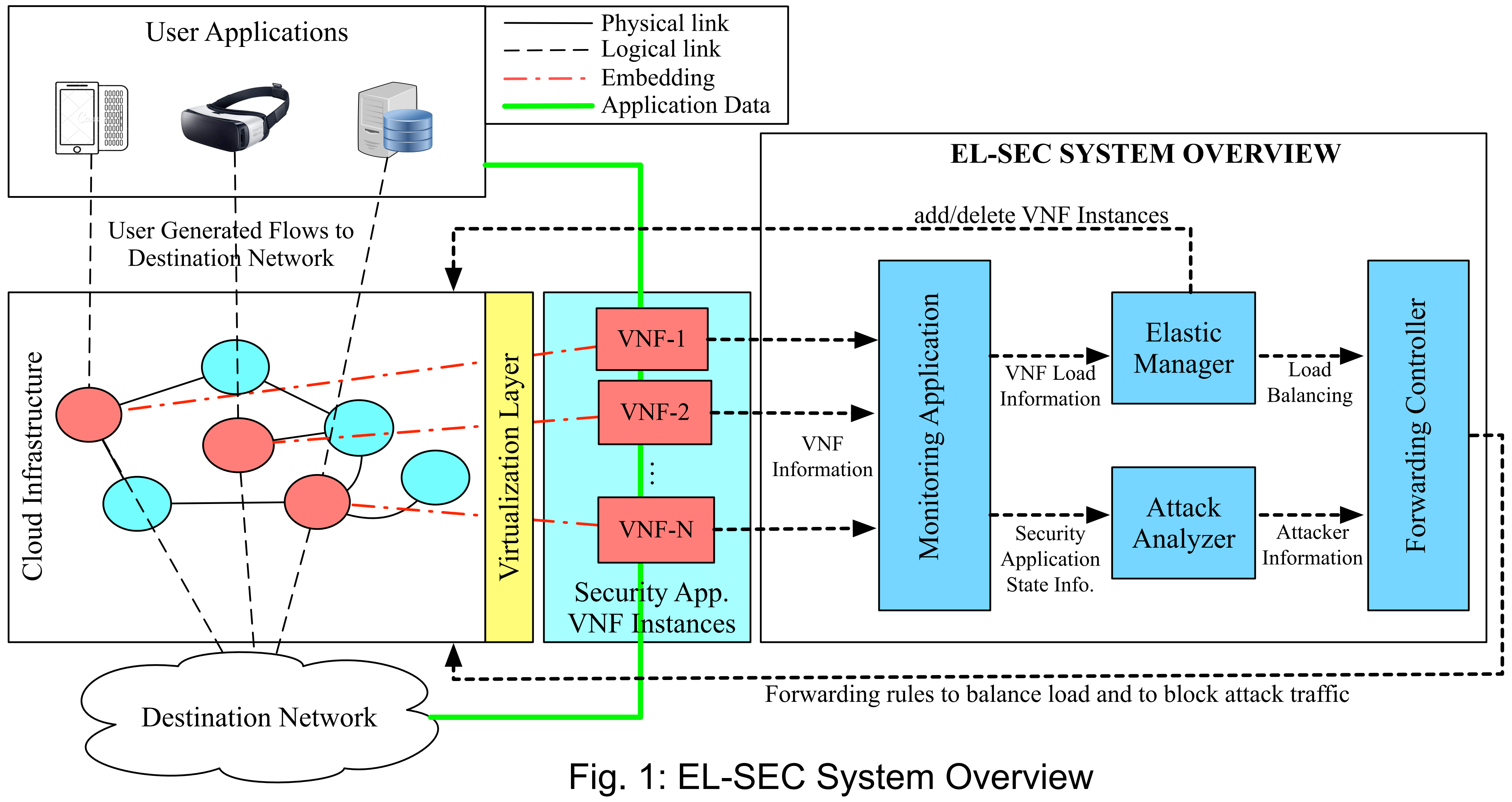

Fig. 1: EL-SEC System Overview

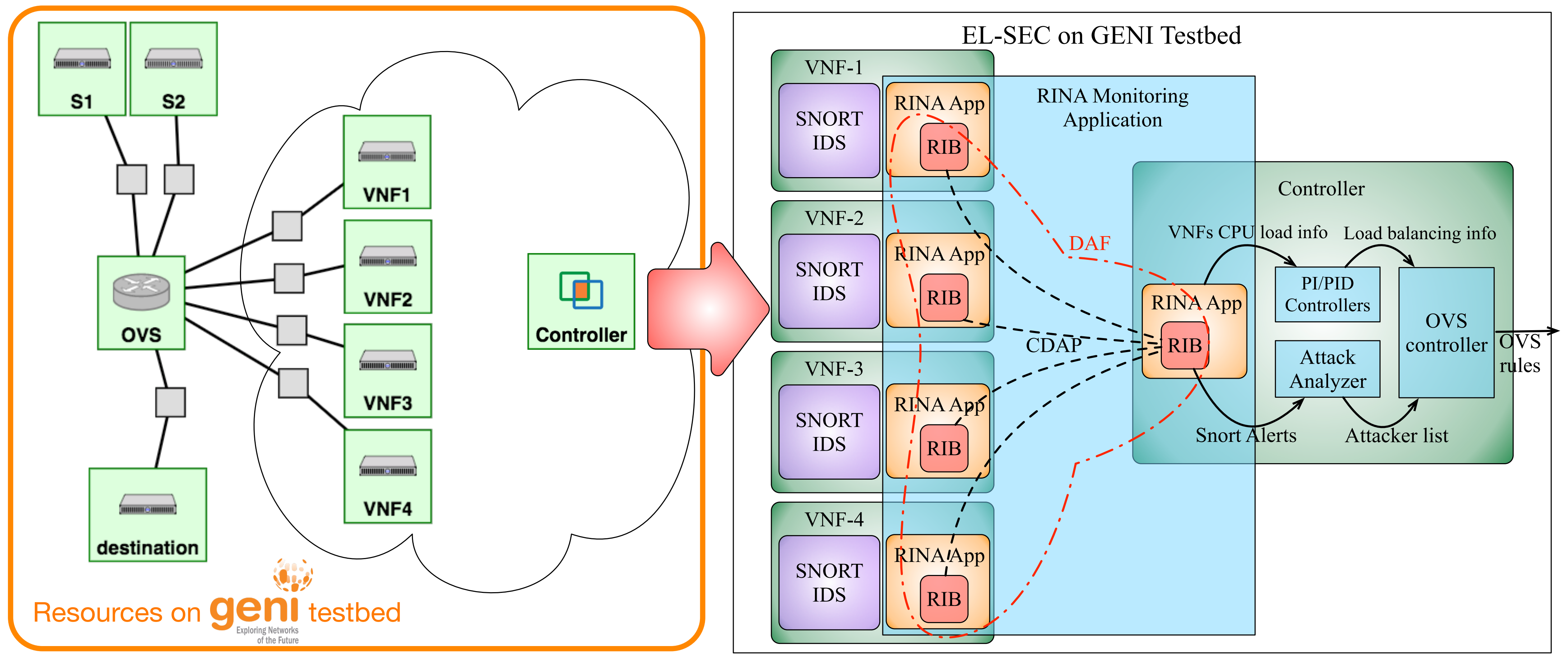

Fig. 2: EL-SEC use case: IDS on the GENI testbed

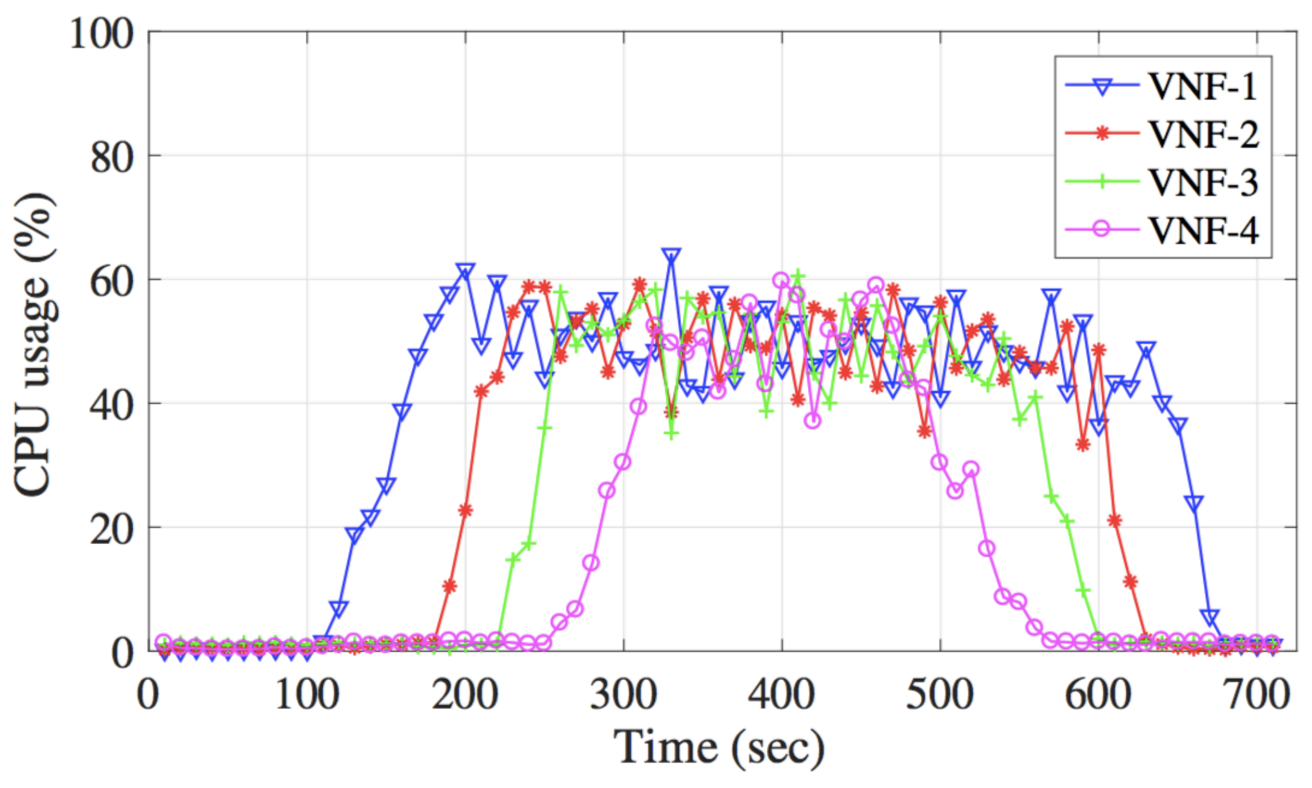

Fig. 3: Load balancing with the PID Controller

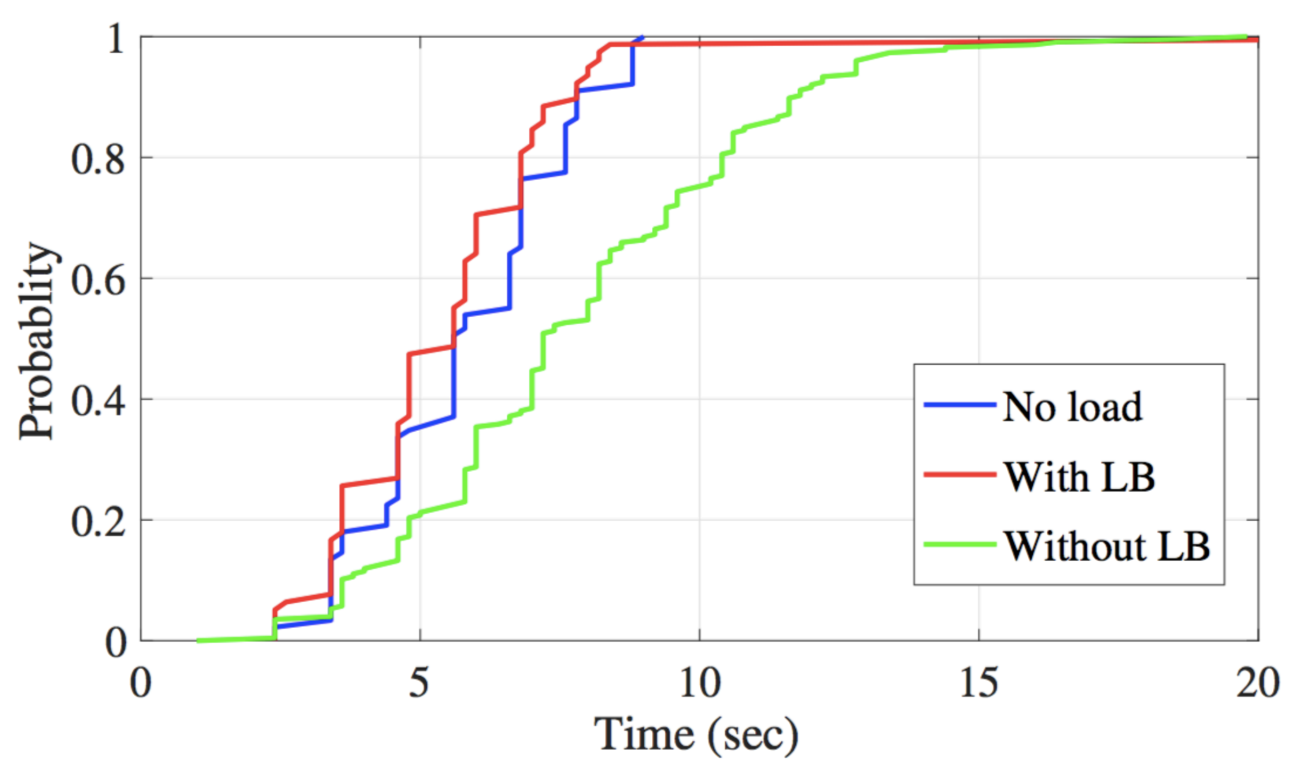

Fig. 4: Time to detect port scanning attacks