SDN based Scalable MTD solution in Cloud Networks

MTD 2016

Ankur Chowdhary, Sandeep Pisharody,
Dijiang Huang
Arizona State University

Index

- Introduction
- Background
- System Architecture and Contribution
- Motivating Example
- MTD approach
- Complexity and Performance Evaluation
- Conclusion Future Work

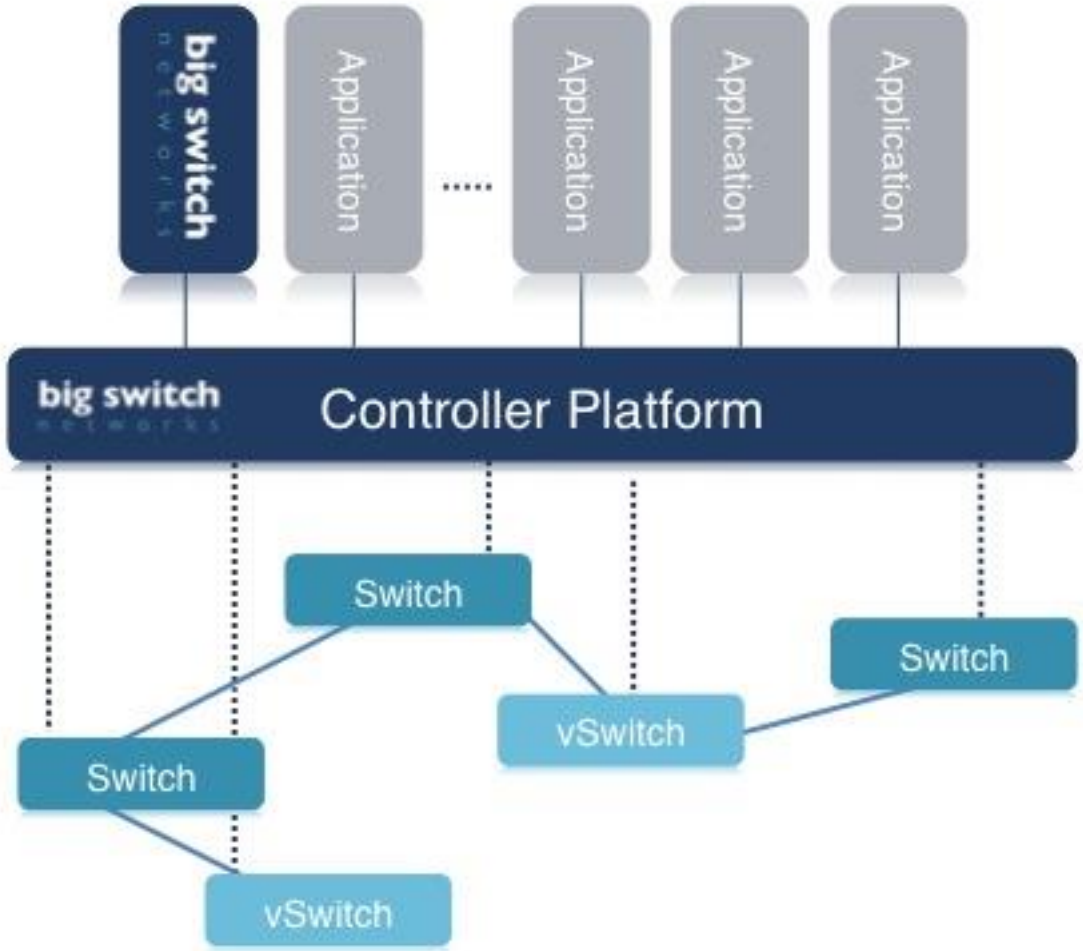
Introduction

- There are many critical assets in a network which can be compromised by a malicious attacker through a multistage attack.
- SDN separates data and control plane, which provides network administrator better visibility and policy enforcement capability compared to traditional networks.

Introduction

- Moving target defenses have been proposed as a way to make it much more difficult for an attacker to exploit a vulnerable system by changing aspects of that system to present attackers with a varying attack surface.
- We use the SDN controller to assess the attack scenarios through scalable Attack Graphs (AG) and select necessary countermeasures to perform network reconfiguration to counter network attacks.

big switch networks



3

Open source integration layer

2

Open APIs to program the network

1

Open standards such as OpenFlow

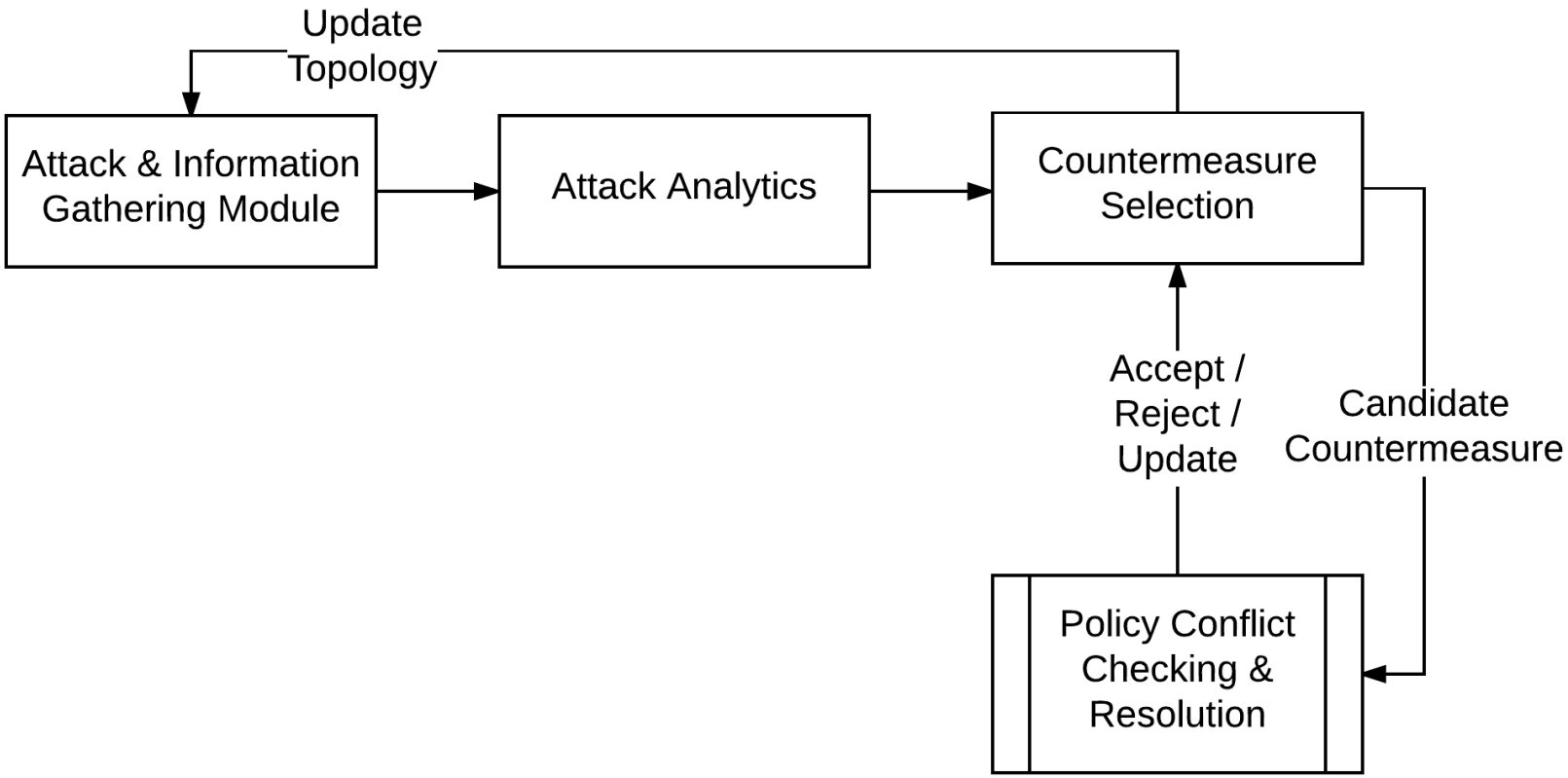
Background

- Attack Graph is a succinct representation of network nodes including hosts, ports, services, connectivity and vulnerability information.
- Using the information from the attack graph the analysts can take preventive measures before the attacker can exploit the system weakness.

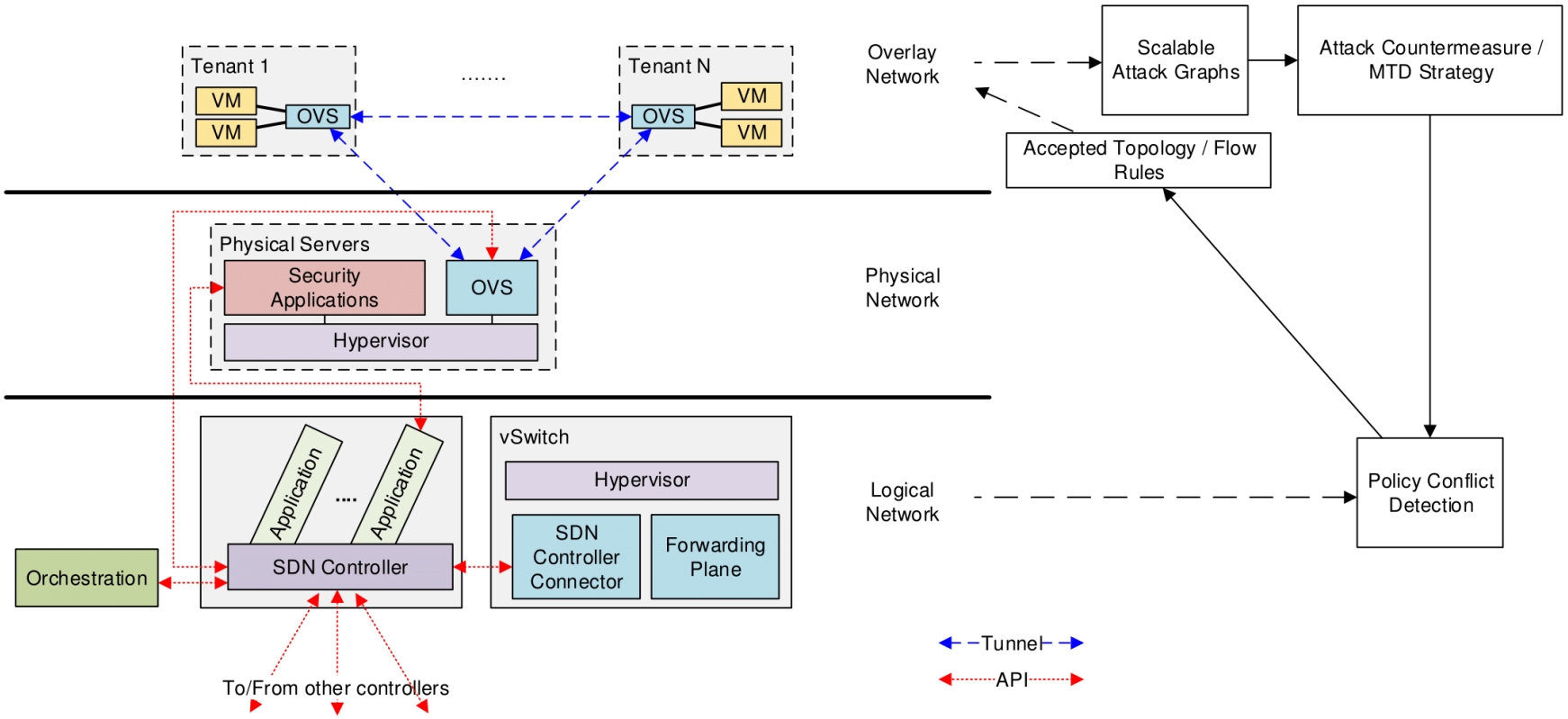
Background

- Most of the works that have used AG in past face scalability challenges.
- We employ distributed hypergraph partitioning algorithm to handle scalability issues inherent in representing security states of entire network.

System Architecture



System Architecture



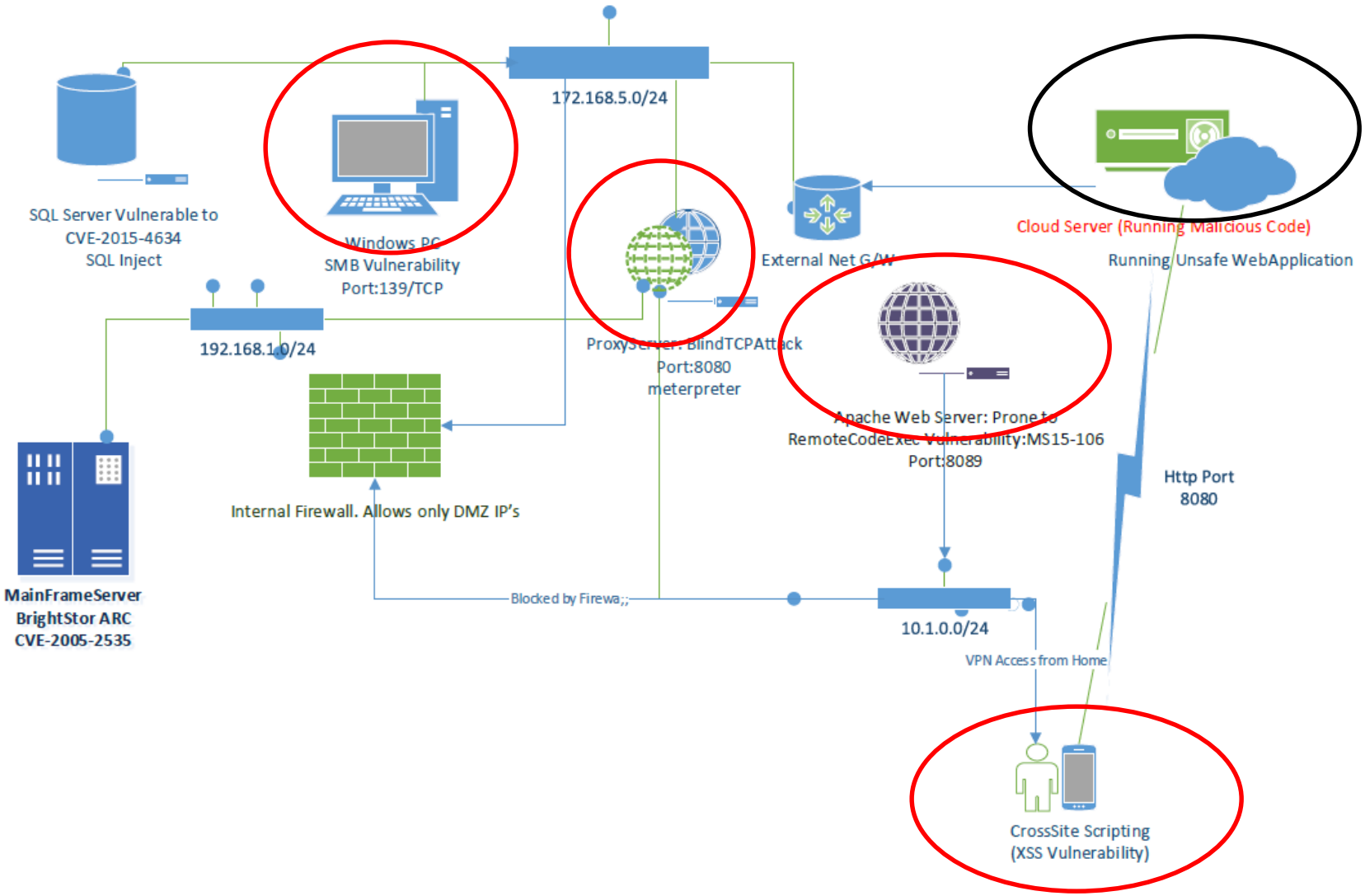
Contribution

- We automate dynamic system reconfiguration safely by leveraging scalable AG and cross-layer security policy checking. It requires no involvement by network operators.
- We are able to successfully implement a framework that does real-time network reconfiguration either pro-actively, or reactively to any abnormal events in the environment.

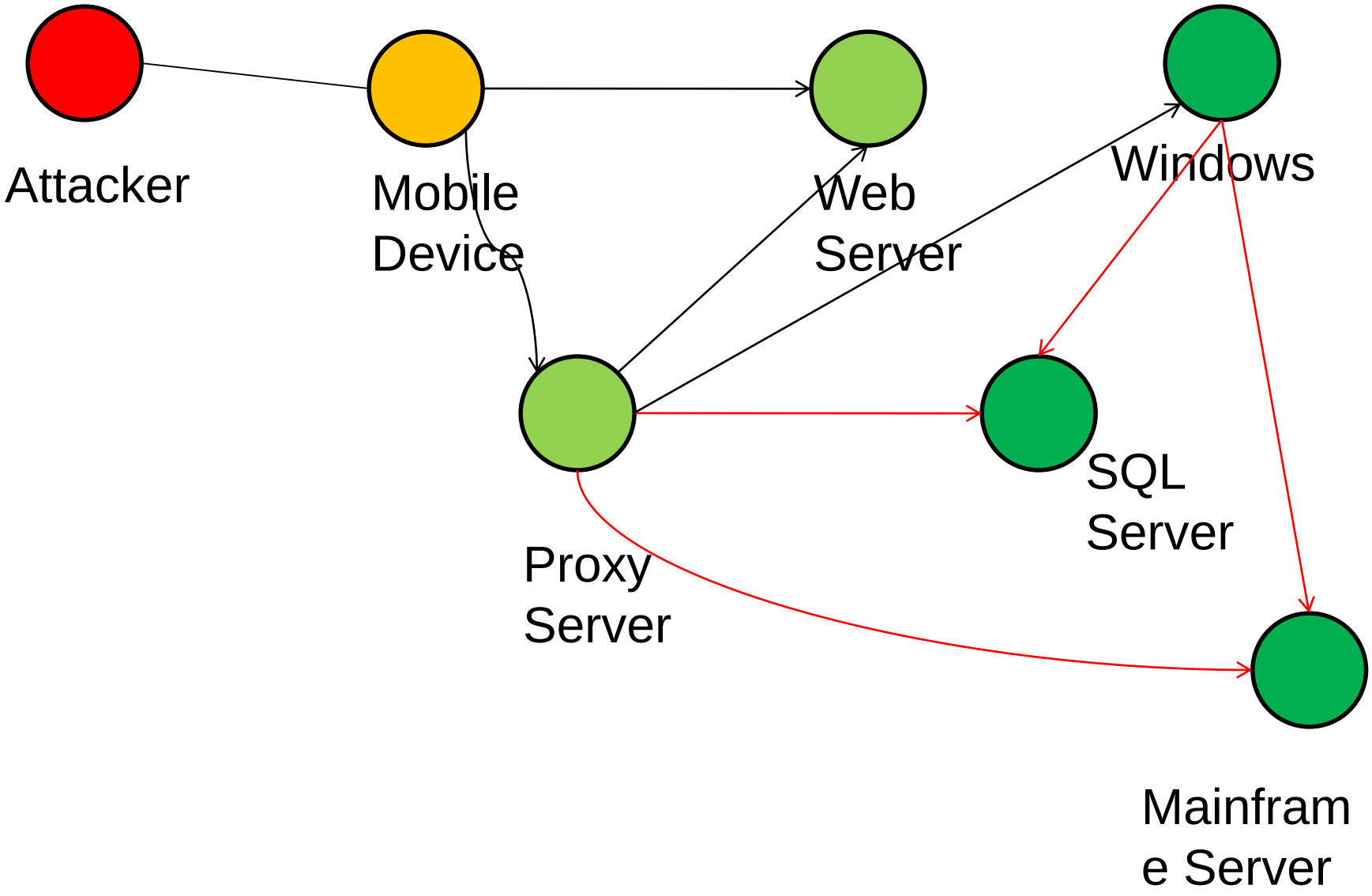
Contribution

- The reconfigured system is guaranteed to be compliant with security and SLA requirements of the organization.

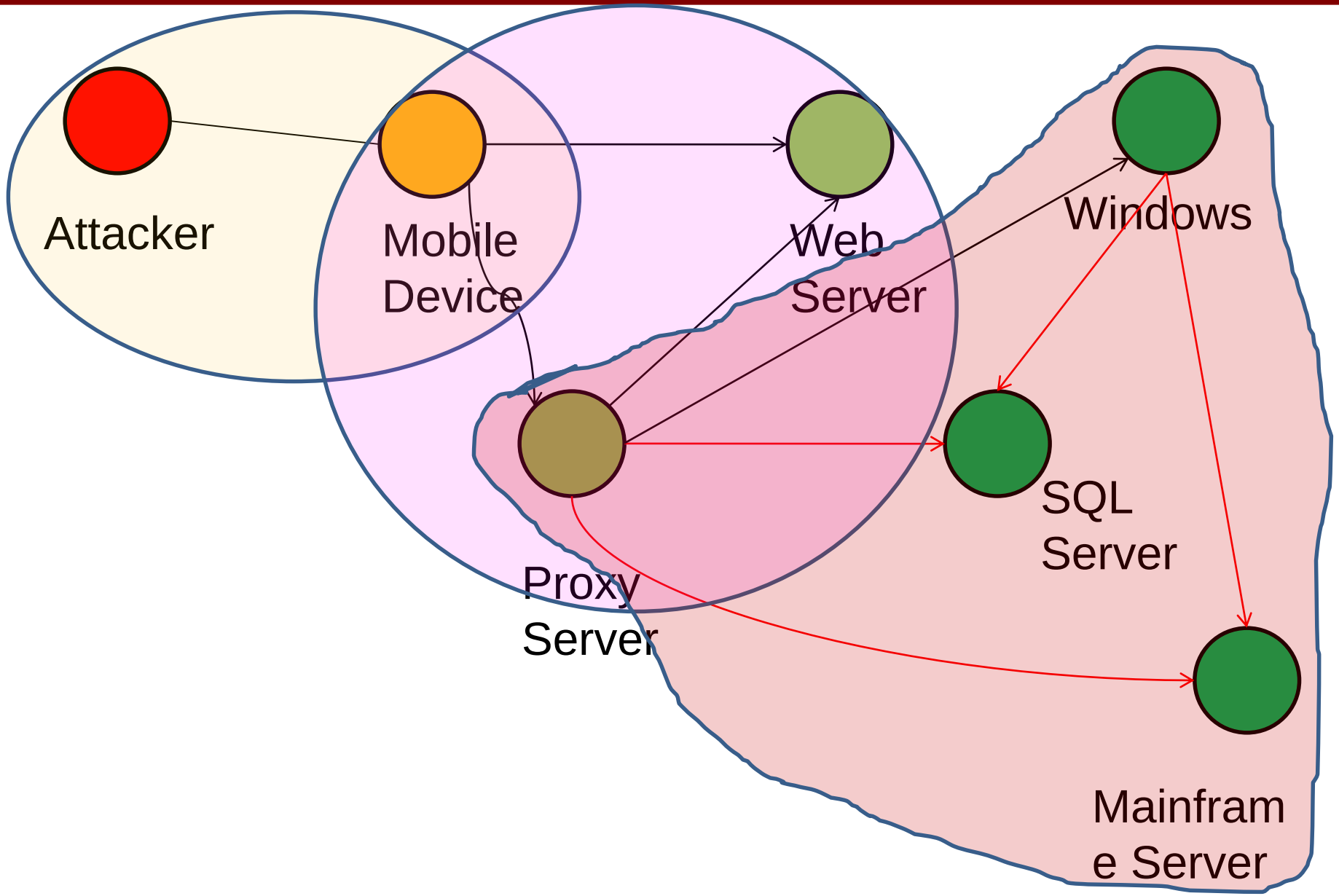
Motivating Example



Attack Graph



Equivalent Partitioned Hypergraph



Countermeasure Selection

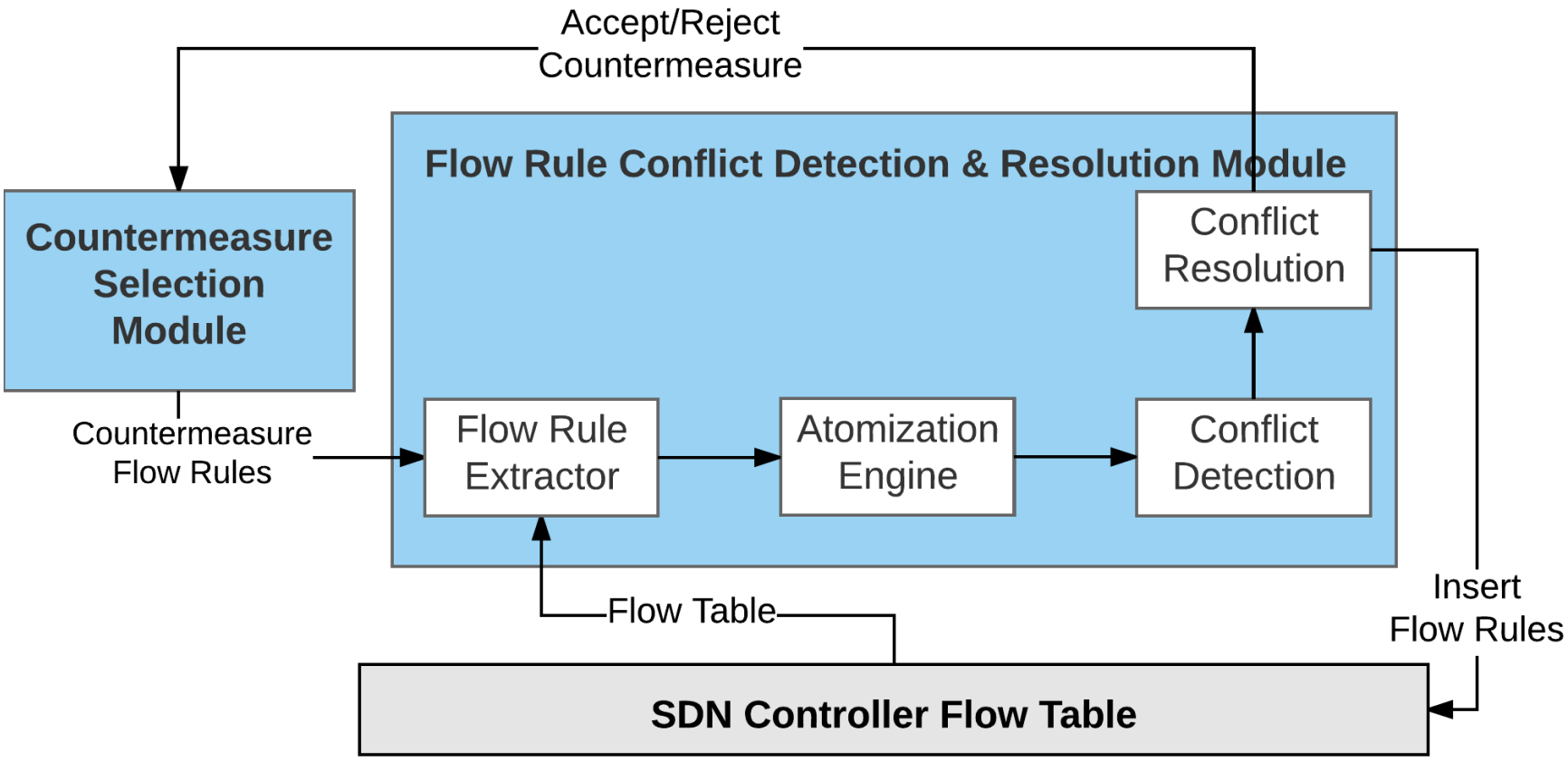
- Create an index of physical severs and their corresponding virtual server.
- For physical server PS_i calculate cumulative vulnerability score of each VS_j.

- If th $$VS_i = Min\{10, \ln \sum \exp^{BaseScore(v)}\}$$ vulnerability score exceeds a pre-set threshold, migrate to another PS.

Policy Conflict Post-Countermeasures

- Change in network configuration induces new flow rules in environment.
- This can create new attack paths in network.
- We ensure these flow rules do not conflict with existing rules.
- We generate new attack graph for modified network configuration.

Policy Conflict Post-Countermeasures



System Safety and Liveliness

- P_{safe} = {~root(WS); ~localprivEsc(ftpServ)}
- P_{live} = {sshAccess(VM1; VM2); ftpAccess(VM1; ftpServ)}
- For the attack graph G, we check preconditions nodes described in attack analysis model satisfy $P_{safe} U P_{live}$

Complexity

- The time for Attack Graph generation $\mathcal{O}((N/p)^2) + \mathcal{O}(N/p) + \mathcal{O}(N \log p)$
- The time for countermeasure selection and policy conflict resolution

$$\mathcal{O}(|V| \times |CM|) + \mathcal{O}(n.r).$$

AG Performance Evaluation

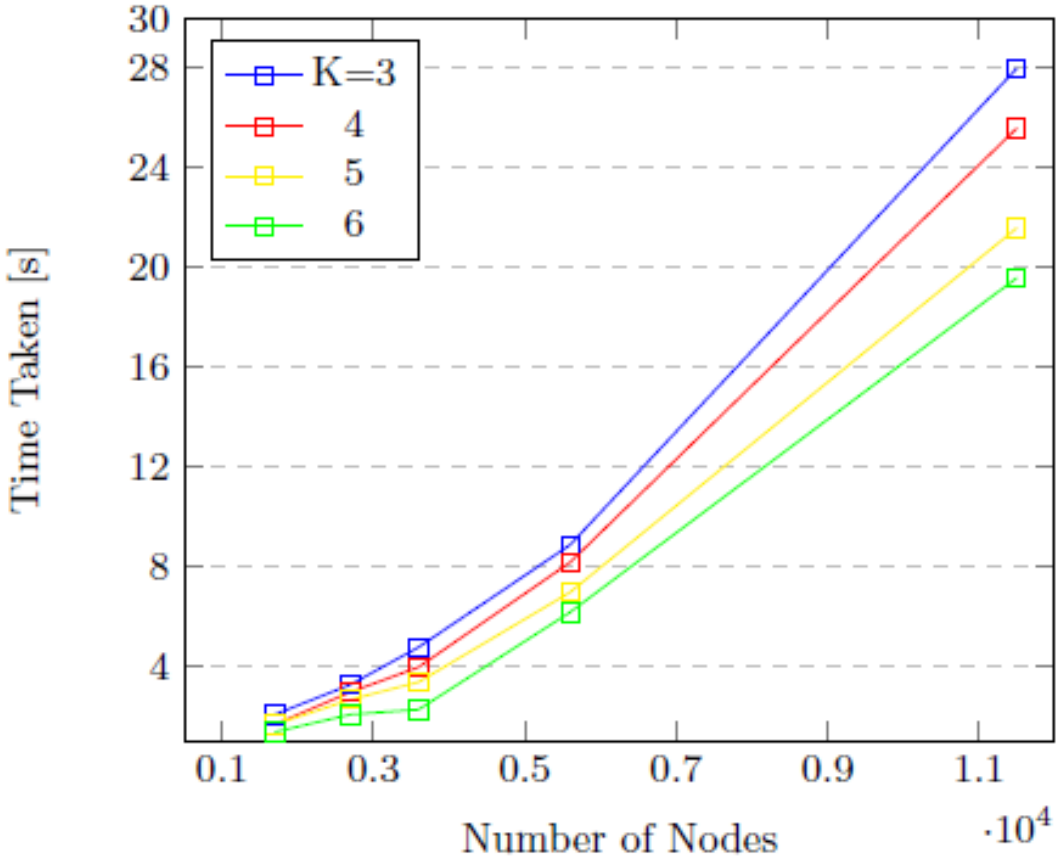
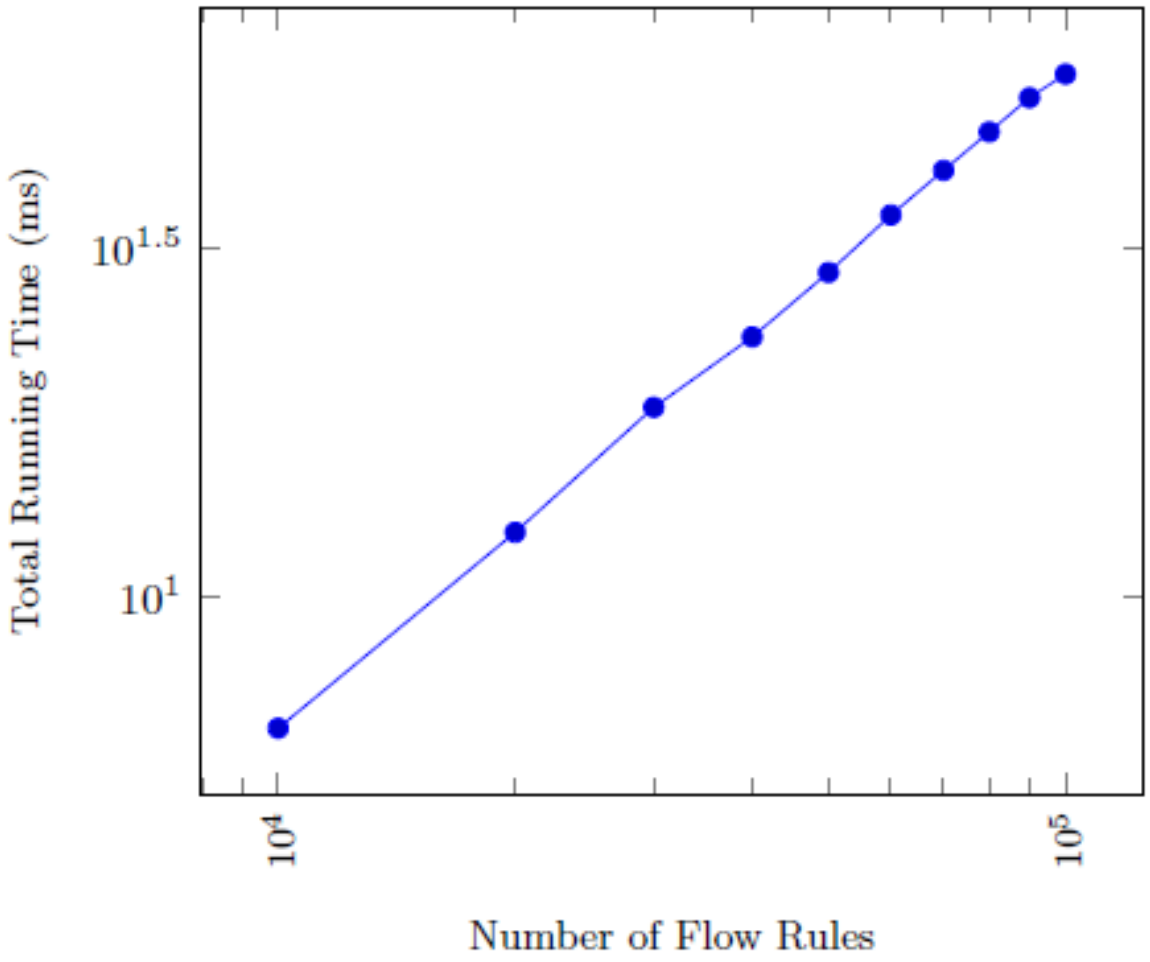


Figure 7: AG generation time vs Number of nodes

Flow Rule Conflict Resolution



Conclusion

- Our scalable AG solution is very useful in analyzing the security state of a large network, which would otherwise be difficult to interpret for a network administrator.
- Once we reconfigure the network using a countermeasure selection module, we ensure that there is no security policy violation or conflict in the adjusted network

Future Work

- Use of Game Theoretic Modelling to analyze the payoff of Attacker and Admin, so that admin can identify best possible countermeasures.
- Use of anomaly detection to detect malicious traffic, and identify zero day vulnerabilities.
- Employ regression and other statistical measures to ensure accuracy of anomaly detection methods.

Questions ???