OpenFlow Random Host Mutation: Transparent Moving Target Defense using Software Defined Networking

Jafar Haadi Jafarian, Ehab Al-Shaer, Qi Duan

2012 Proceedings of the first workshop on Hot topics in SDN

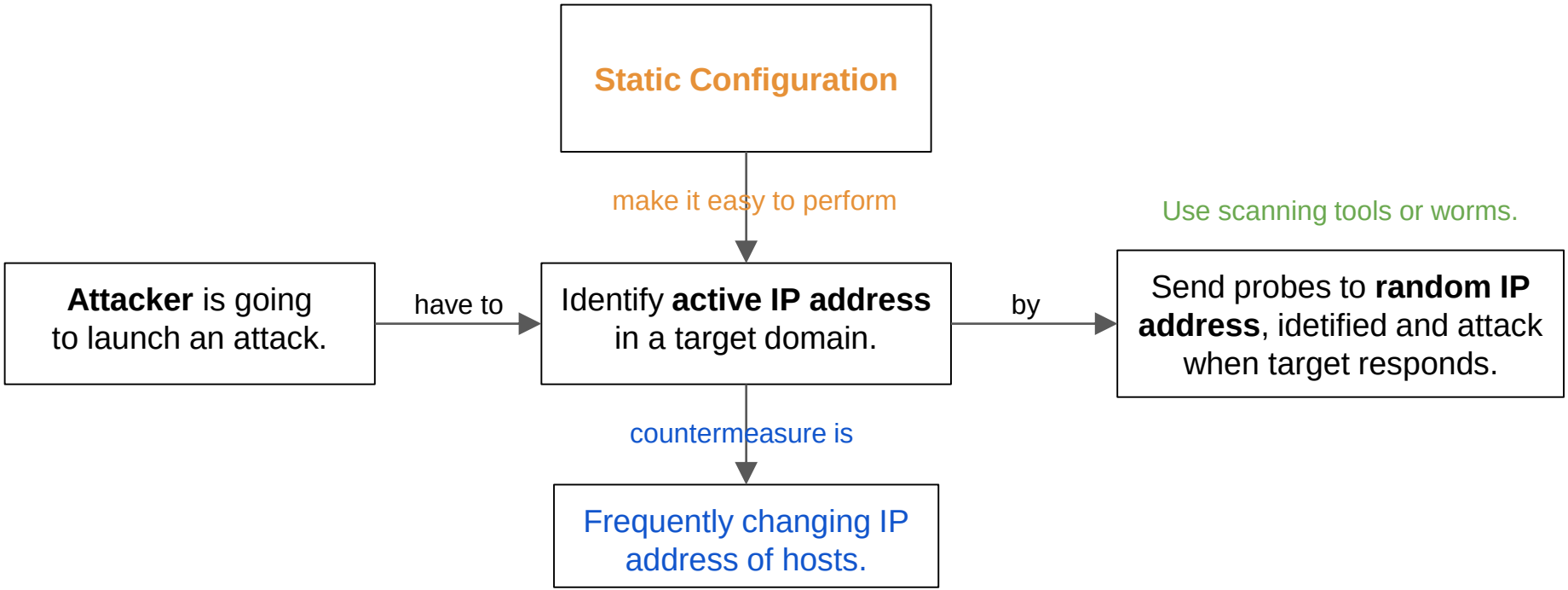
R05922009 資工所一 Wen,Sheng-Han

Outline

- Introduction
  - What is “moving target denfense” (MTD)?
- Overview of OF-RHM
  - Objectives
  - Related Works
- Design Details of OF-RHM
  - Range allocation & vIP mutation

Introduction

Introduction



Proactive Moving Target Defense (MTD)

Introduction

Moving Target Defense (MTD)

Enterprise networks sometimes have many public and private hosts accessible from outside.

→ Become targets of most of the attackers.

How about DHCP and NAT?

Ans: Insufficient to provide poactive countermeasure because IP mutation is infrequent and traceable.

Introduction

OpenFlow Random Host Mutation (OF-RHM)

A MTD architecture implementation utilizing OpenFlow.

With high unpredictability and rate while mataining configuration integrity and minimizing operation overhead.

Overview of OF-RHM

Overview of OF-RHM

OpenFlow Random Host Mutation (OF-RHM)

mutates the IP addresses of end-hosts “randomly” and “frequently”

Two objectives:

i. IP mutations must be transparent to the end-hosts.

ii. IP mutations must be performed with high unpredictability and speed.

Overview of OF-RHM

Related Work

APOD

Uses **hopping tunnels** based on address and port randomization.

Require cooperation of both client and server. → Not transparent.

NASR

Based on DHCP frequent updates.

Not transparent to end-hosts. (require reconfiguration for hosts.)

Overview of OF-RHM

Two objectives of OF-RHM

i. IP mutations must be transparent to the end-hosts.

By associated each host with random, short-lived virtual IP address (vIP) at regular interval.

Q1: What's the translation mechanism of rIP and vIP?

Q2: How to design the architecture to attain such a mechanism?

ii. IP mutations must be performed with high unpredictability and speed.

Overview of OF-RHM

Two objectives of OF-RHM

i. IP mutations must be transparent to the end-hosts.

ii. IP mutations must be performed with high unpredictability and speed.

By selecting mutated vIP randomly from entire unused address space in the network.

Q3: How to find unused IP address?

Q4: How to assign vIPs to hosts to satisfy the constraints:

Overview of OF-RHM

Q1: What’s the translation mechanism of rIP and vIP?

Q2: How to design the architecture to attain such a mechanism?

Q3: How to find unused IP address?

Q4: How to assign vIPs to hosts to satisfy the constraints?

mutation unpredictability.

minimum required mutation rate of all hosts.

Overview of OF-RHM

Q4: How to assign vIPs to hosts to satisfy the constraints:

mutation unpredictability.

minimum required mutation rate of all hosts.

Answer:

Formalize the problem as **constraint satisfaction problem** and use **SMT** solver to solve the problem.

But how to formalize?

Design Details of OF-RHM

Problem Definition & Formalization

In OF-RHM, each host is associated with an unused address range based on specific requirement.

At each mutation, a vIP is choose from this range for each mutation interval.

Q3: How to find unused IP address?

Problem Definition & Formalization

Q3: How to find unused IP address?

Given used address **A1, A2, … Am**

The unused address is determined by simply masking the full network address space **A** as follc

$$A_{unused} = A \cap \neg(A_1 \cup A_2 \cup \ldots \cup A_n)$$

Problem Definition & Formalization

Main problem

Suppose each host belong to a subnet.

Given unused ranges **{r1, r2, …, rm}** and subnet **{s1, s2, …, sn}**, what is the appropriate assignment scheme such that the following objectives are achieved:

Objective 1: the range assigned to the subnet must include enough IP address to satisfy minimum required mutation during interval T.

Objective 2: Unpredictability and mutation rates must be maximized by allocating all unused address ranges.

Problem Definition & Formalization

Mutation Rate Constraint

based on objective1

$$\forall k, \left(\sum_{1 \le i \le n} c_{ik} R_i \right) * T \le \sum_{1 \le j \le m} b_{jk} |r_j|$$

The total number of vIPs of all hosts in subnet **sk** during **T** must less than the aggregate size of all ranges assigned to **sk**

Range Allocation Constraint

based on objective2 & routing constraint

$$\forall j, \sum_{1 \le k \le z} b_{jk} = 1$$

Each range must be assigned to one exactly one subnet.

Range Distribution Constraint

$$\forall k, P_k = \frac{T * \sum_{1 \le i \le n} c_{ik} R_i}{\sum_{1 \le j \le m} b_{jk} |r_j|}$$

Range must be assigned to subnets proportionate to their total required mutation rate.

Problem Definition & Formalization

Since the problem of assigning ranges to subnet is **NP-hard.**

After formalizing the problem with several constraint, we solve the assigning problem with **SMT (Satisfiability Modulo Theories) solver**.

If no solution is found, we relax constraint value, and assert the constraints

$$\forall k, P_k = \frac{T * \sum_{1 \le i \le n} c_{ik} R_i}{\sum_{1 \le j \le m} b_{jk} |r_j|}$$

$$P_a = \frac{T * \sum_{1 \le i \le n} R_i}{\sum_{1 \le j \le m} |r_j|}$$

$$\forall k, |P_k - P_a| < \delta$$

relax this value

Overview of OF-RHM

Q1: What's the translation mechanism of rIP and vIP?

Q2: How to design the architecture to attain such a mechanism?

~~Q3: How to find unused IP address?~~

~~Q4: How to assign vIPs to hosts to satisfy the constraints?~~

~~mutation unpredictability.~~

~~minimum required mutation rate of all hosts.~~

Design Details of OF-RHM

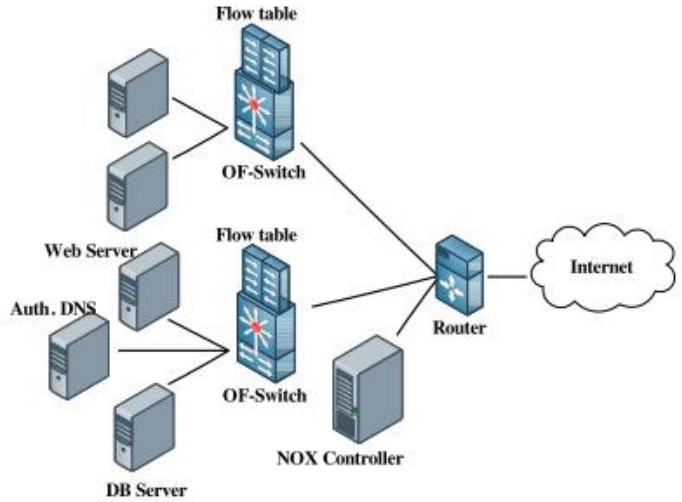
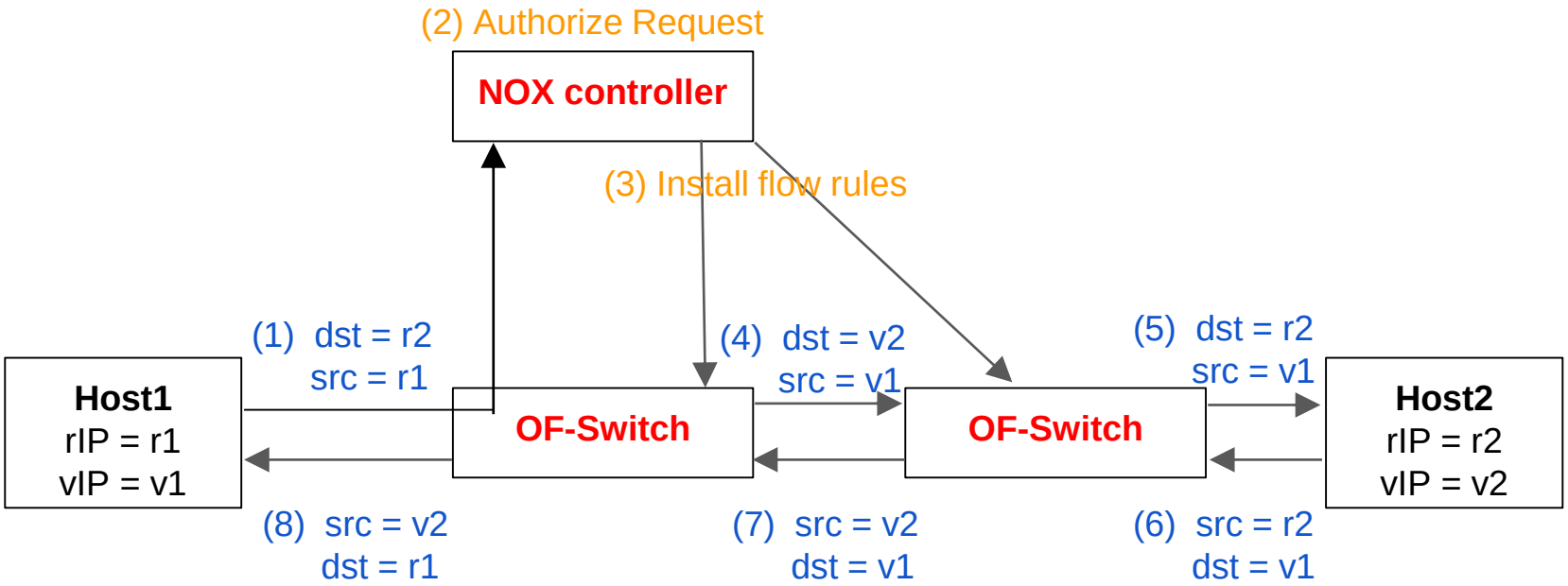


Figure 1: The architecture of OF-RHM network

Design Details of OF-RHM

Q1: What's the translation mechanism of rIP and vIP?



Protocol of OF-RHM

Protocol: Supporting two scenarioes, communicate using **host IP** or **host name.**

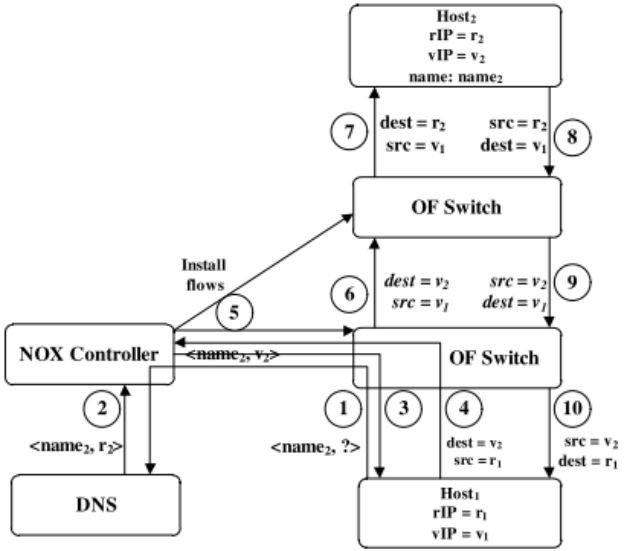


Figure 2: Communication via name

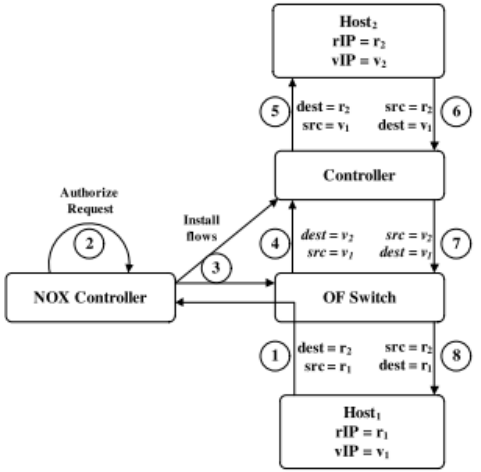


Figure 3: Communication via rIP address

Overview of OF-RHM

~~Q1: What's the translation mechanism of rIP and vIP?~~

Q2: How to design the architecture to attain such a mechanism?

~~Q3: How to find unused IP address?~~

~~Q4: How to assign vIPs to hosts to satisfy the constraints?~~

~~mutation unpredictability.~~

~~minimum required mutation rate of all hosts.~~

Architechture of OF-RHM

Implementation of this technique requires two major components:

a. Subnet gateways to perform **rIP-vIP translation** (OpenFlow switch)

b. A central management authority which **coordinates mutation across network.** (OpenFlow Controller)

These components are **costly** in tradional network. (That’s why they choose SDN.)

a. Realtime global configuration.

b. synchronization problem in decentralized environment.

Architechture of OF-RHM

In OF-RHM, the **controller** performs the following task:

a. coordinates mutation process across OpenFlow switch.

b. determination optimal set of vIPs using SMT solver.

c. manages active connections by installing flows.

d. handles DNS updates

In OF-RHM, the **switch** performs

a. perform rIP-vIP translations.

Overview of OF-RHM

~~Q1: What's the translation mechanism of rIP and vIP?~~

~~Q2: How to design the architecture to attain such a mechanism?~~

~~Q3: How to find unused IP address?~~

~~Q4: How to assign vIPs to hosts to satisfy the constraints?~~

~~mutation unpredictability.~~

~~minimum required mutation rate of all hosts.~~

Evaluation

Evaluation

Environment setting

Create a network of OpenFlow switches by **Mininet**.

Routing was handled by NOX controller.

Evaluation Target

Random external scanner

Worms

Overhead

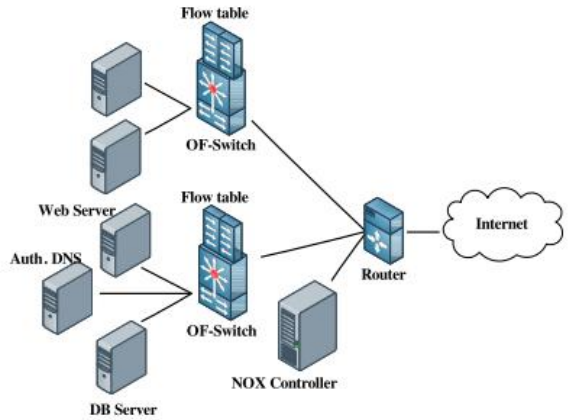


Figure 1: The architecture of OF-RHM network

Evaluation

Random external scanner

Most attacker use scanning tools such as **Nmap** to discover active hosts.

```
nmap www.hinet.net
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-10-02 08:09 CST
Nmap scan report for www.hinet.net (202.39.253.11)
Host is up (0.0034s latency).
rDNS record for 202.39.253.11: 202-39-253-11.HINET-IP.hinet.net
Not shown: 998 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed ident
Nmap done: 1 IP address (1 host up) scanned in 6.05 seconds
```

Evaluation

Random external scanner

Run 100 Nmap scan on the Mininet network, which consists of 2^{10} hosts.

Compare the results with ground truth (by initial scan).

Results

Not more than 1% vIP address are discovered in any scan.

Evaluation

Random external scanner

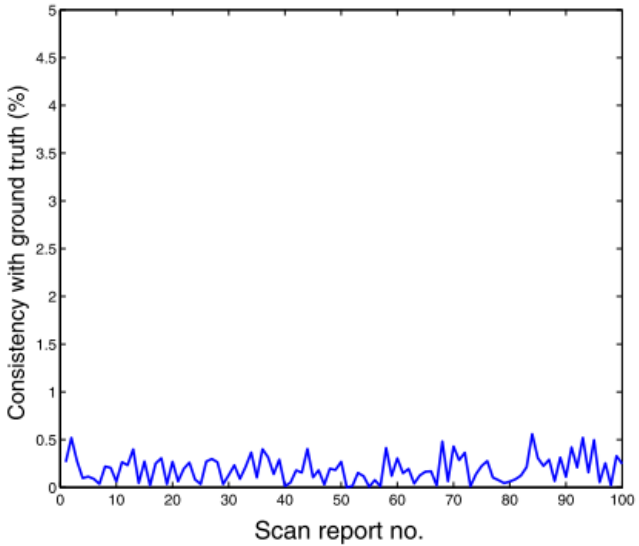


Figure 4: Consistency of consecutive Nmap scan reports with ground truth

Evaluation

Worms

The effectiveness of a scanning strategy is determined by **decreasing** the probability of multiple scanning of a specific IP.

OF-RHM support blind mutation & weighted mutation, which make it effective against scanning worm.

Evaluation

Worms

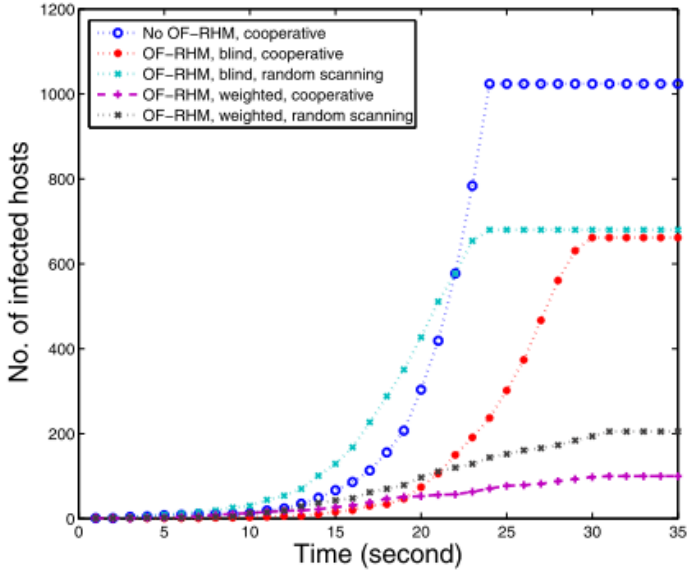


Figure 5: Worm propagation for various network setups

Evaluation

Overhead

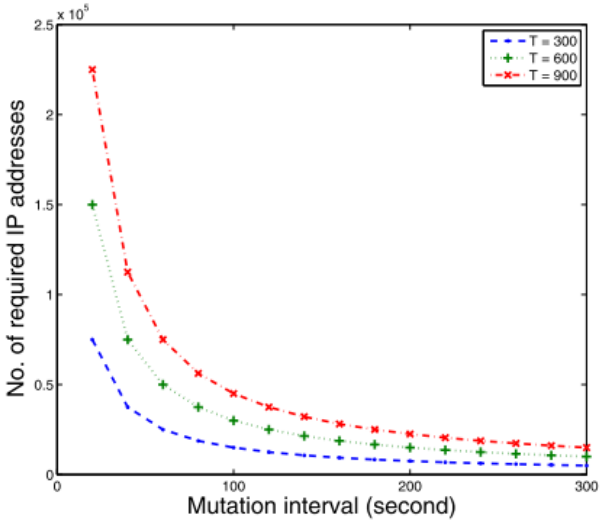


Figure 6: Required IP address size for various mutation intervals and number of hosts

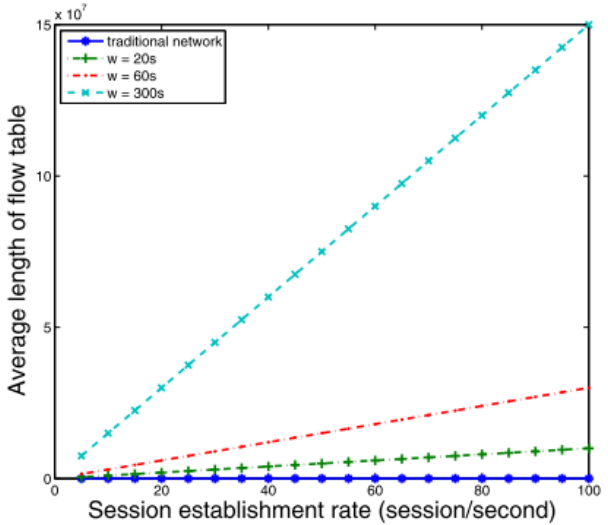
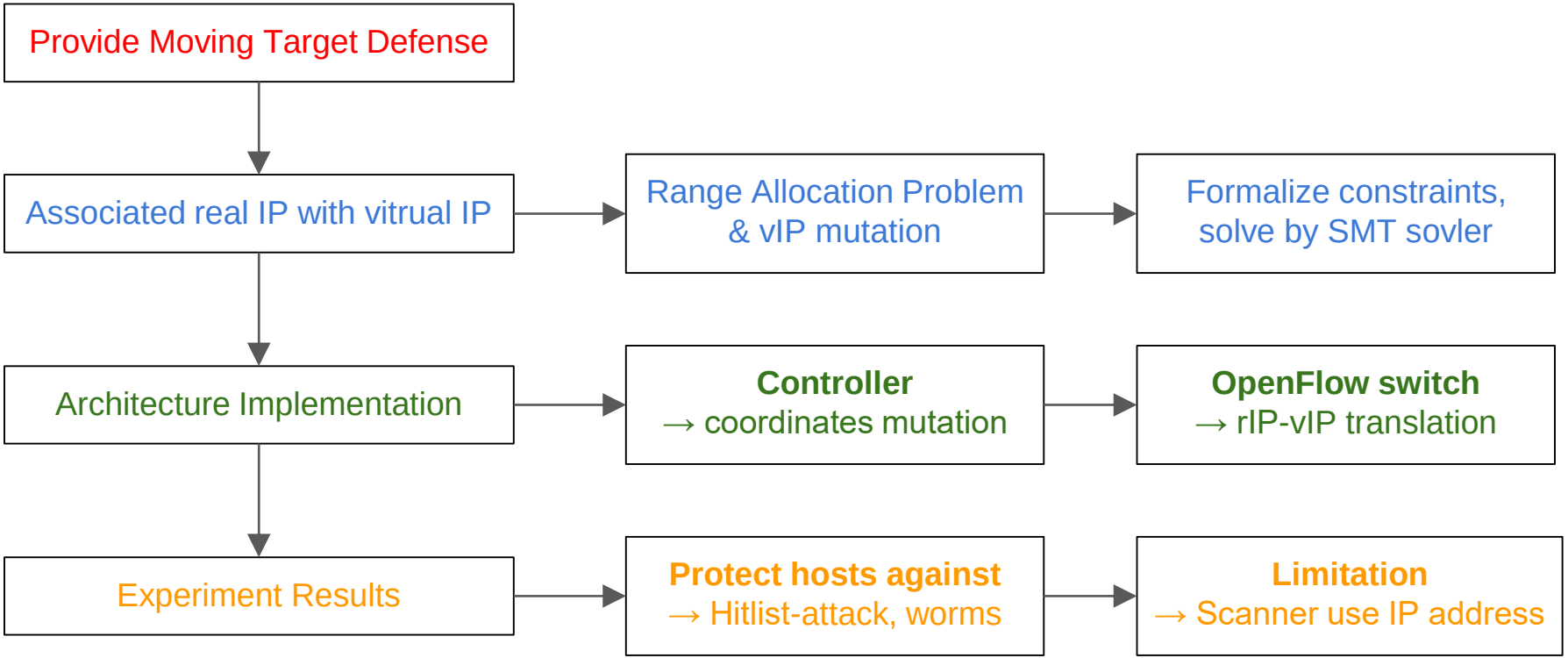


Figure 7: Flow table length for different session establishment rates and session durations

Summarize

Summarize


Provide Moving Target Defense
Associated real IP with vitrual IP
Range Allocation Problem & vIP mutation
Formalize constraints, solve by SMT sovler
Architecture Implementation
Controller → coordinates mutation
OpenFlow switch → rIP-vIP translation
Experiment Results
Protect hosts against → Hitlist-attack, worms
Limitation → Scanner use IP address

Conclusions

Conclusions

OF-RHM is a MTD architecture implementation utilizing OpenFlow.

With **high unpredictability and rate**, and is transparent to end-hosts.

The evaluation results show that OF-RHM can effectively prevent hosts from being scanning by **some external scanners and worms**.

Still weak to protect detection against external **scanners use IP address** to collect information.

Q & A

Thanks!