Yang CHEN, Hong-chao HU, Guo-zhen CHENG, 2019. Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties. *Frontiers of Information Technology & Electronic Engineering*, 20(2):238-252. https://doi.org/10.1631/FITEE.1800516

Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties

Key words: Intranet defense; Software-defined network; Multi-dimensional maneuvering

Corresponding author: Hong-chao HU
E-mail: 13633833568@139.com
ORCID: Yang CHEN, http://orcid.org/0000-0001-7806-2066

Motivation

1. The means of attack have become more complex, e.g., advanced persistent threat (APT), social engineering attacks, and zero-day exploits. Their attack behavior cannot be effectively detected by the traditional security detection system.

2. The boundaries of the enterprise network tend to be blurred, especially in recent years. With the development of the mobile Internet, bring your own device (BYOD) has become a new model for workplaces. While this model reduces enterprise costs, attackers can easily penetrate the internal resources through these devices.

Main idea

1. System architecture design:

   (1) Design principles;

   (2) General framework;

   (3) Maneuvering mechanism;

2. Implementation of cyber defense solution (SPD):

   (1) Communication protocols;

   (2) Packet classification;

   (3) IP allocation;

   (4) Path maneuvering.

1. System framework

Data plane:
This plane enforces packet forward according to the dynamic transform rules.

Management plane:
This plane is responsible for the initial system configuration and network operational status.

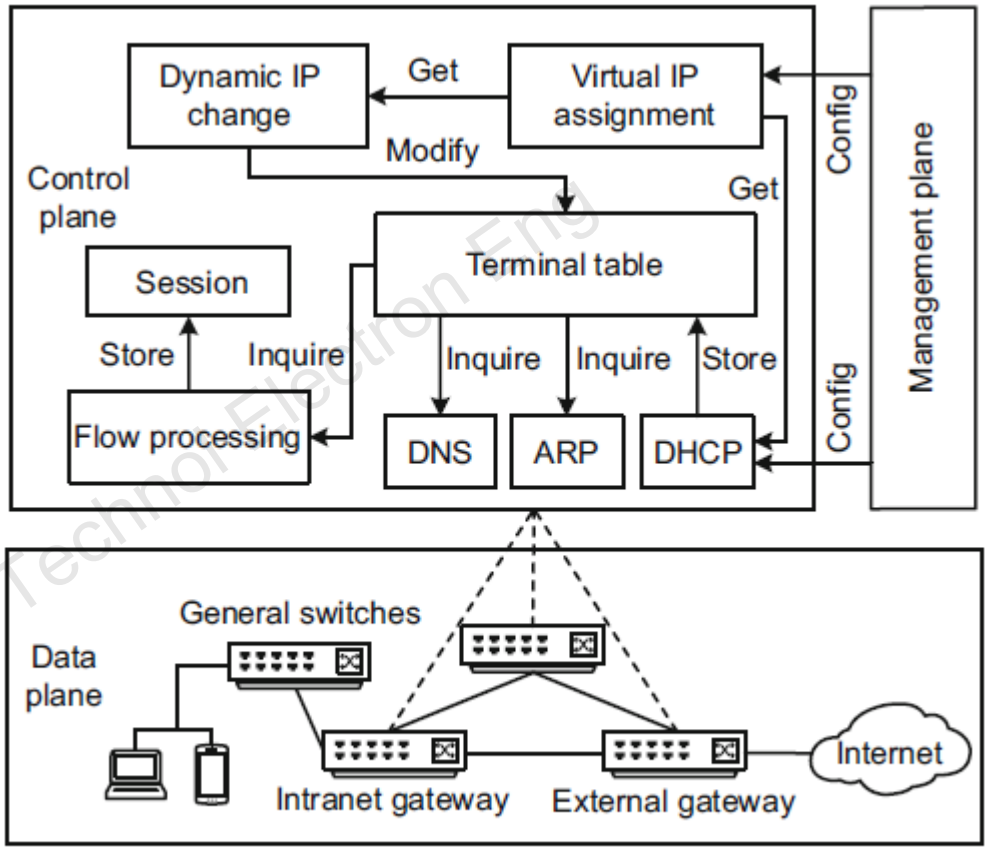


Fig. 1 System framework

Control plane:
(1) Configure resources for hosts and maintain a dynamic virtual configuration;
(2) Establish a session and a transmission path for communication, and maintain a dynamic external network port.

2. Communication protocols

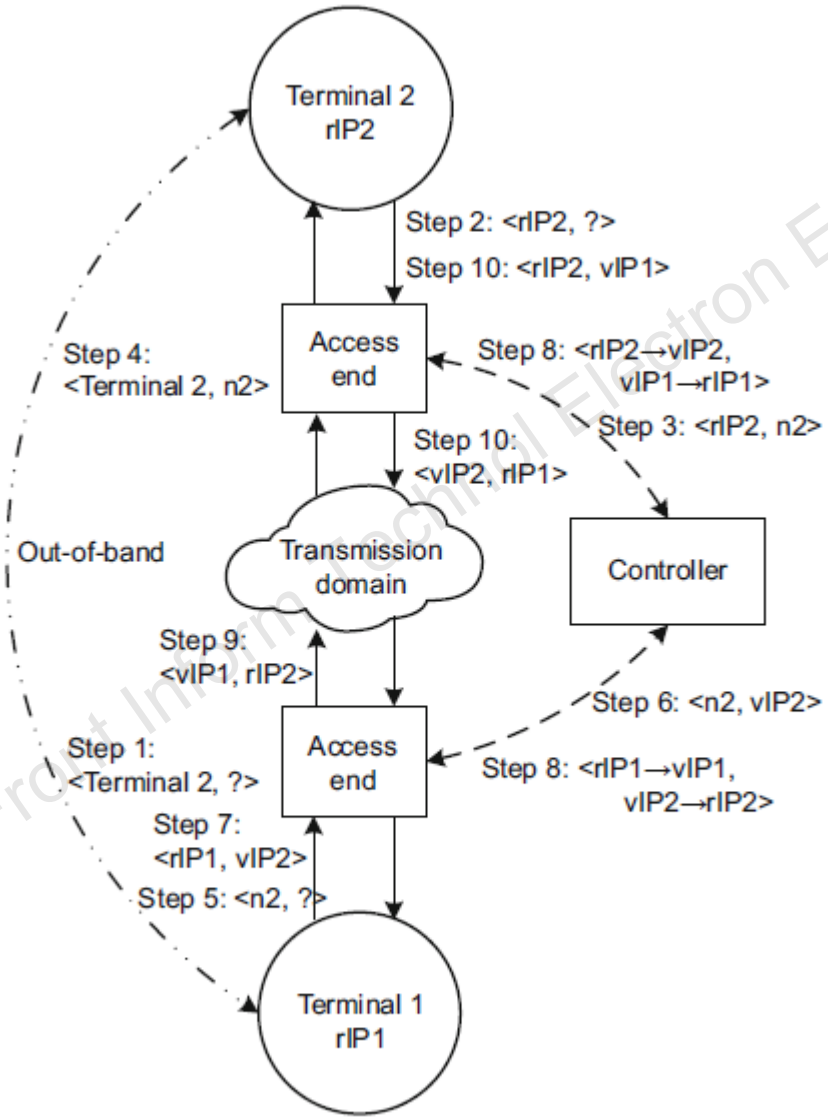


Fig. 2 Communication processing

3. Packet classification

When an IP packet is sent to the controller, the controller needs to determine to which type the packet belongs:

(1) The sender-to-access packet, the next hop is the receiving end;

(2) The sender-to-access packet, the next hop is not the receiving end;

(3) The message from the non-access end, the next hop is the receiving end;

(4) The message from the non-access end, the next hop is not the receiving end.

Algorithm 1 Communication processing

```
1: for all Packet p comes from the OF switch do
2:   if p.src is rIP and p is from the access end then
3:     if p.dst is vIP then
4:       R_1 ← the path from h_i to h_j
5:       for all switch s in R_1 do
6:         if s ∈ Type.A then
7:           f_i(h_i.rIP → h_i.vIP, h_j.vIP → h_j.rIP,
             dst_mac → h_j.mac, output : s.out)
8:           f_b(h_j.rIP → h_j.vIP, h_i.vIP → h_i.rIP,
             dst_mac → h_i.mac, output : s.in)
9:         else if s ∈ Type.B then
10:          f_i(h_i.rIP → h_i.vIP, h_j.vIP → h_j.rIP,
             dst_mac → h_j.mac, output : s.out)
11:          f_b(h_j.vIP, h_i.rIP, output : s.in)
12:        else if s ∈ Type.C then
13:          f_i(h_i.vIP, h_j.rIP, output : s.out)
14:          f_b(h_j.vIP, h_i.rIP, output : s.in)
15:        else if s ∈ Type.D then
16:          f_i(h_i.vIP, h_j.rIP, output : s.out)
17:          f_b(h_j.rIP → h_j.vIP, h_i.vIP → h_i.rIP,
             dst_mac → h_i.mac, output : s.in)
18:        end if
19:        flow_mod(f_i, f_b)
20:      end for
21:    end if
22:  end if
23: end for
```

Evaluation

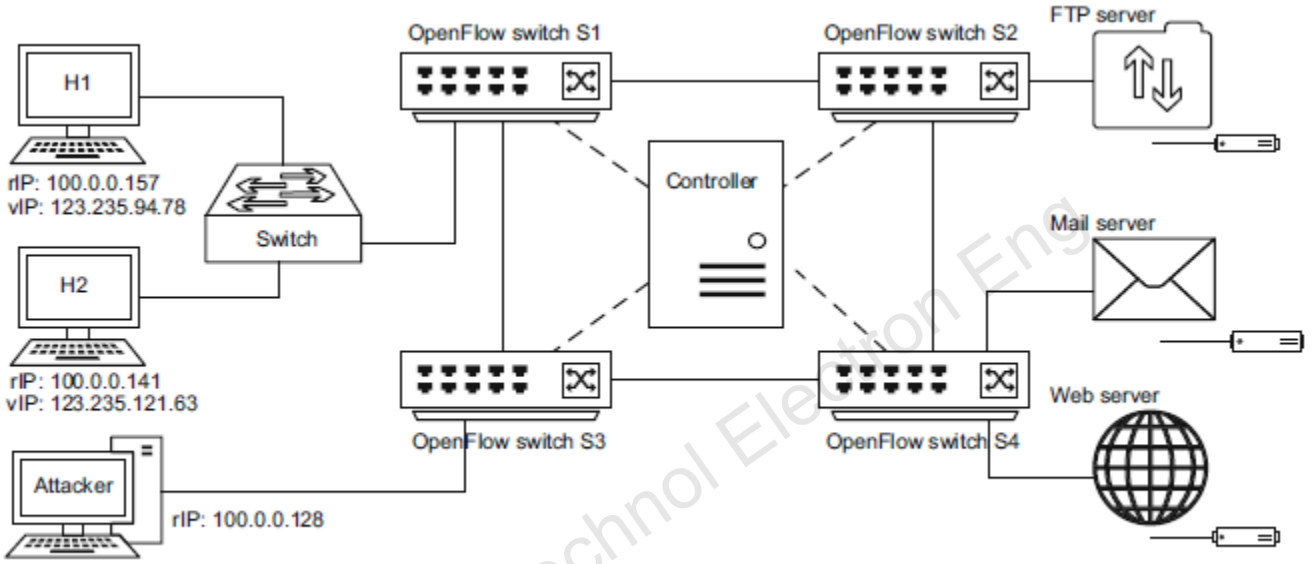
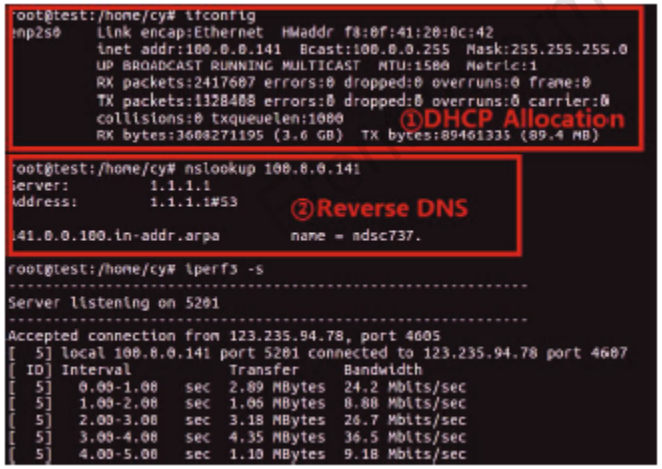
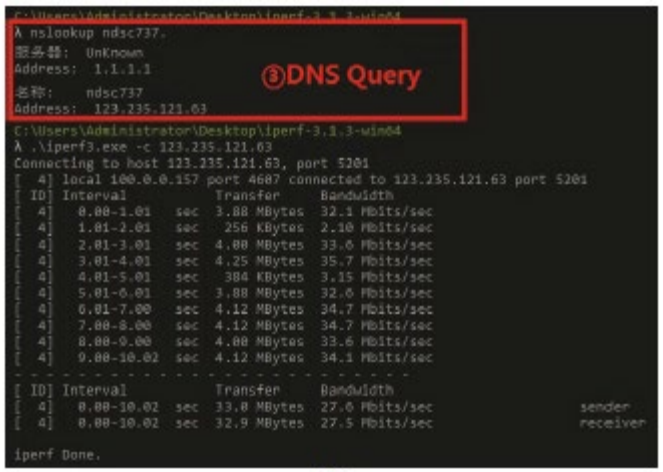


Fig. 4 Network topology



(a)



(b)

Fig. 5 Communication verification: (a) terminal H2; (b) terminal H1

Evaluation

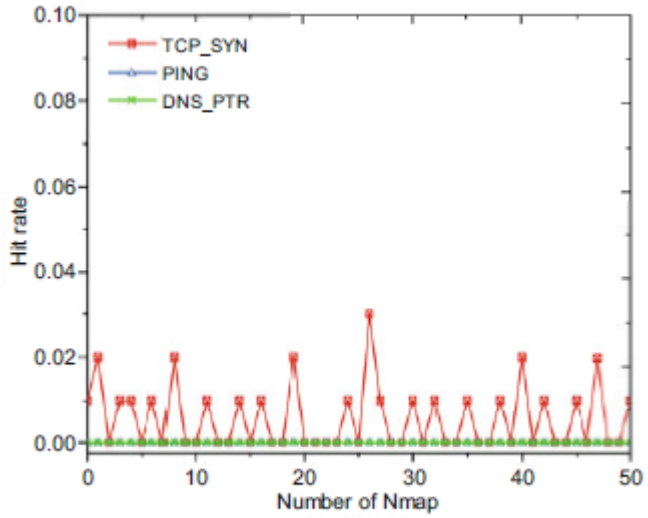


Fig. 6 Ratio of hits

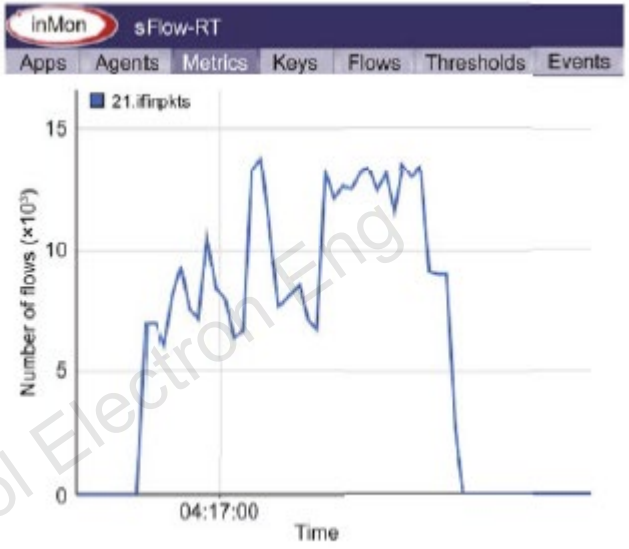


Fig. 7 Anti-denial-of-service (DoS) attack

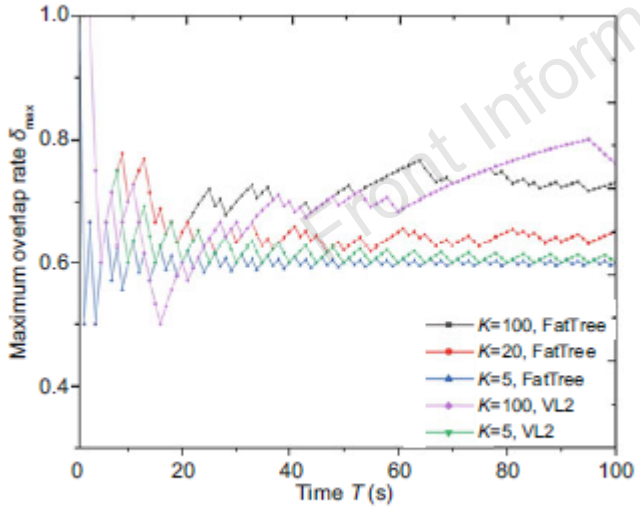


Fig. 8 Overlap rate of network

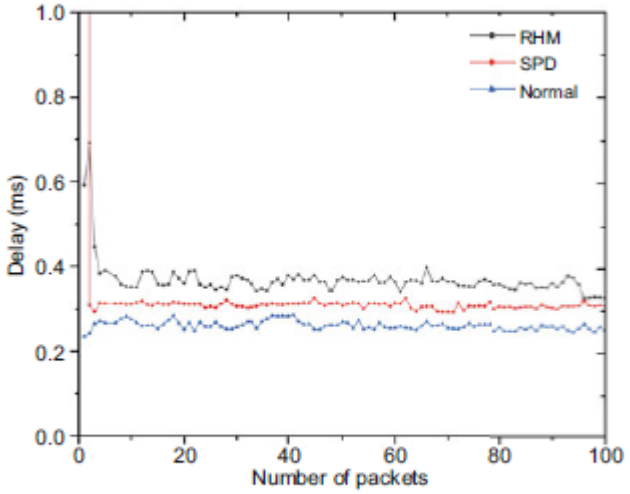


Fig. 10 Network delay caused by switch forwarding in RHM, SPD, and the normal modes

Conclusions

1. SPD with an appropriate alternation strategy can resist almost all network scanning attacks, and effectively intercept worms, DoS, and other unknown network attacks.

2. The flow overhead introduced by the system needs to be further optimized.