Global Network Modelling Based on Mininet Approach. *

Vitaly Antonenko
Moscow State University
Applied Research Center for Computer Networks
Moscow, Russian Federation
anvial@lvk.cs.msu.su

Ruslan Smelyanskiy
Moscow State University
Applied Research Center for Computer Networks
Moscow, Russian Federation
smel@cs.msu.su

Categories and Subject Descriptors

C.2.5 [**Computer-Communication Networks**]: Local and Wide-Area Networks—*Internet*; C.2.4 [**Distributed Systems**]: Network Operating Systems

Keywords

Network simulation, Mininet, rapid prototyping, emulation, virtualization, malware propagation, network worms

1. INTRODUCTION

The problem of the Global network operation analysis has a variety of applications. For example, it occurs to evaluate the effectiveness of the network topology, the location determining of network security tools, rapid prediction of malware attacks propagation. In this paper, we focus on a prediction of malware propagation analysis.

Nowadays malware propagating is a big problem for the Global Network (under this term we will mean what usually call Wide Area Network). In this paper we focus on network worm propagation. The network worms activity has a wide spectrum from just copying itself through network upto organizing DDoS attacks on the particular resources and implementing spying activity.

Based on experience of network worm propagation analysis [1], the main requirement for network model is scalability. Network size covered by model must be 10^5 - 10^6 at least. For example, classic worm epidemic - CodeRed has infected more than 200 thousand hosts [5]).

This paper proposes a possible solution of this problem that satisfies all the named requirements, based on network prototyping system Mininet [2].

*This work was supported by the Russian Foundation for Basic Research under Grant 10-0144/01 dated 25.03.2010, and by the Skolkovo Innovation Center under Grant 79 dated 02.07.2012.

HotSDN'13, August 16, 2013, Hong Kong, China.
ACM 978-1-4503-2178-5/13/08.

2. MININET CE DESCRIPTION

Mininet is a rapid prototyping system. The major goal of the system is fast development of OpenFlow controller applications. OpenFlow controller is a core of Software-Defined Networking [3]. Mininet represents a new approach in network modelling. The emulation based on network virtualization techniques provides brand new possibilities for network structure and network operation simulation.

However, the fine-grained packet processing is the only one requirement for the malware propagation analysis. Other one is a scale of modelling network. The native limitation of Mininet having up to 2000 nodes in the emulated network makes an original version of Mininet hardly applicable to the considered of malware propagation analysis in the Global network.

The main idea of Mininet CE is to develop the upper level software over Mininet that could combine several separate instances of Mininet into one Cluster.

Mininet CE Supervisor Console is the analog of Mininet console but it can configure, send commands and show output from several instances of Mininet via SSH. For implementation the SSH session with each Mininet instance in Mininet CE Paramiko library is used.

Mininet CE cluster node is a virtual or physical machine with Linux operating system (we use Ubuntu 12.10) with three packets for the public repository.

Also Mininet CE cluster node must have two active Ethernet interfaces. The first one is to communicate with Mininet CE supervisor console, the other one is to communicate with the other cluster nodes.

The connection among Mininet instances in the cluster makes it possible to use an extra external interface mechanism described in "examples/hwintf.py" in Mininet distribution.

3. EXPERIMENT METHODOLOGY

There is the scenario of network operation that will be performed by Mininet CE. Such scenario has to be described in a special module, which is a part of Mininet CE supervisor console. In this scenario, malware propagation process should also have been described.

Malware propagation simulation divided into steps. One propagation step is one full life cycle of malware, which described in detail in first section of this paper. Briefly, we could describe malware propagation step as follow (see Figure 1). For malware propagation step simulation we need a description of network worm. In this experiment we simulated the Sasser worm [4].

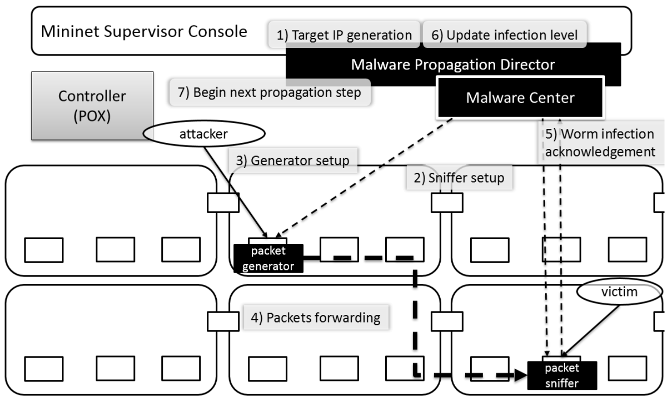

Figure 1: Malware propagation simulation scheme.

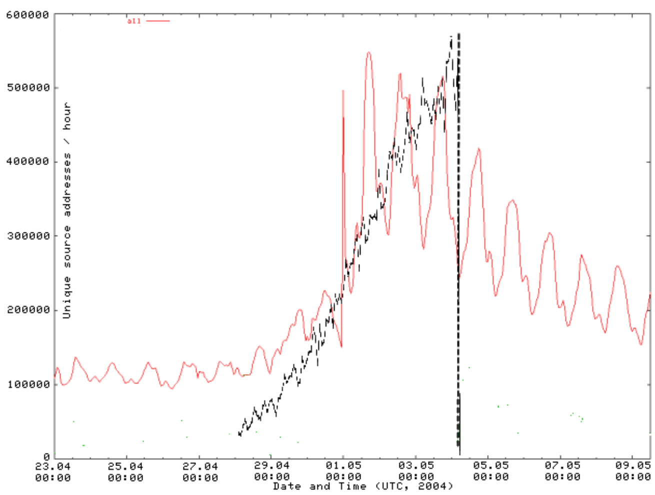

Figure 2: Comparison simulation results to real data of Sasser worm activity.

To complete preparations for our experiment we took as input data target selection algorithm and network activity data of the simulated worm. The network activity of Sasser worm instance data [4] is used for packet generator and packet sniffer, to simulate self-copping process of Sasser worm.

4. EXPERIMENT RESULTS AND DISCUSSION

During the experiment the model network segment was built, its topology consist of 7500 nodes. The initial population of the worm consisted from 394 hosts in experimental network. The propagation speed was one try to propagation for one propagation step simulation.

We compared the simulation result to growing activity on port 445 that was observed during the real Sasser worm propagation in 2004 (Figure 2). Black vertical line shows the period when Microsoft patch that fix the vulnerability the used by Sasser worm was installed in observed network. The black graphic is the graphic Sasser propagation speed.

The combination of Mininet CE and Malware Propagation module produce the close infection dynamics. The experimental results are consistent with the expected results, so the experiment can be considered as successful.

5. CONCLUSION

There was described the new version of Mininet for computer cluster, that allow us reproduce the network with such amount of nodes that hardly was possible before. The possible size of network topology in Mininet CE depends on number of cluster nodes with Mininet instances. One cluster node could simulate more than thousand hosts, and an modern server could execute at least 15 cluster nodes: we get about 15 thousands hosts by server. In collaboration that Mininet CE is well scaled system on we could simulated really big networks.

By the architecture, Mininet CE saves features of Mininet, so it do not become clear simulation system, it stay a network prototyping system. That means that we could trust the results of such simulation and there is no need to prove correctness and adequacy of built model.

We are very thankful to Nick McKeown, professor in the Electrical Engineering and Computer Science departments at Stanford University, who attracted our attention to network simulation by Mininet.

6. REFERENCES

[1] Su Fei, Lin Zhaowen, and Ma Yan. A survey of internet worm propagation models. In *Broadband Network Multimedia Technology, 2009. IC-BNMT '09. 2nd IEEE International Conference on*, pages 453–457, Oct.

[2] Bob Lantz, Brandon Heller, and Nick McKeown. A network in a laptop: rapid prototyping for software-defined networks. In *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, Hotnets-IX, pages 19:1–19:6, New York, NY, USA, 2010. ACM.

[3] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. Openflow: enabling innovation in campus networks. *SIGCOMM Comput. Commun. Rev.*, 38(2):69–74, March 2008.

[4] Doi Norihisa Terada Masato, Takada Shingo. Proposal for the experimental environment for network worm infection. *Transactions of Information Processing Society of Japan*, 46(0):2014–2024, 2005.

[5] Cliff Changchun Zou, Weibo Gong, and Don Towsley. Code red worm propagation modeling and analysis. In *Proceedings of the 9th ACM conference on Computer and communications security*, CCS '02, pages 138–147, New York, NY, USA, 2002. ACM.