Experiment on repetitive exchanging of heterogeneous routers for router metabolism

Rei ISHIOKA[†], ***Student Member***, **Yuya SUGA**[††], ***Nonmember***, ***and*** **Junichi MURAYAMA**[†], ***Member***

SUMMARY Future cyberattacks may infect routers with malware. If these routers are exchanged periodically with initialized ones, even undetectable malware can be removed. However, these routers may infect the same-type malware again. To solve this problem, we have proposed a repetitive exchanging scheme between heterogeneous-type routers. This paper evaluates this exchanging scheme through four experiments. The summaries of the results are as follows. (1) Even heterogeneous routers can be exchanged in a hitless manner by using VRRP. (2) A centralized priority controller can control heterogeneous routers by means of the dynamical attachment of their command interpreters. (3) Router-priority control achieves repetitive router-exchanging without packet forwarding interruption. (4) A repetitive malware infection can be suppressed by means of heterogeneous-router exchanging. According to these results, it is expected that the router metabolism utilizing heterogeneous routers can mitigate malware infection damage effectively.

key words: *router metabolism, router exchange, heterogeneous, hitless, repetitive*

1. Introduction

Recent cyberattacks use malicious software called malware. Malware causes much damage, such as Distributed Denial of Service (DDoS) attacks or phishing scams [1] [2] [3]. It may infect routers as well as servers [4]. Due to progressing obfuscation technology, malware detection using its signature information becomes difficult [5] [6]. If a router is initialized periodically, even undetectable malware will be removed. However, this router will be infected again with the same malware.

To solve this problem, we have proposed a repetitive exchanging scheme for heterogeneous routers [7] [8]. In this scheme, heterogeneous routers are combined as a redundant system. These routers are exchanged periodically by way of the Virtual Router Redundancy Protocol (VRRP) [9].

Each router forwards packets during the master state. On the other hand, its software configuration is initialized during the backup state. A router's state is changed periodically between those two states. For repeating this change semi-permanently, the router's exchanging priority is controlled periodically using a centralized priority controller [7]. When heterogeneous routers need to be controlled, a command interpreter function for each router is attached to the controller or the router [8].

This paper evaluates this scheme by experiment. The evaluation comprises the following four experiments: hitless exchange of heterogeneous routers, centralized priority control of heterogeneous routers by deploying command interpreter function, periodical exchange of heterogeneous routers, and protection of malware infection by means of exchanging heterogeneous routers.

In the first experiment, using VRRP, even heterogeneous routers were exchanged within 1 millisecond. Next, in the second experiment, deploying command interpreters dynamically within a priority controller, priority levels of heterogeneous routers were controlled without interruption of packet forwarding. Then, in the third experiment, a centralized router-priority control achieved periodical hitless router-exchanging. Finally, in the last experiment, the exchange of heterogeneous routers suppressed repetitive infection with the same malware. Consequently, we can say that our concept of heterogeneous router metabolism is promising as one of the anti-malware countermeasures.

The rest of this paper is organized as follows: Sect.2 shows an overview of our scheme for achieving heterogeneous router metabolism. Then, Sect.3 evaluates our scheme by experiment. Finally, Sect.4 shows the conclusion of this paper.

2. Overview of our proposed scheme

This section presents our exchanging scheme of heterogeneous routers [8]. A configuration of our scheme is depicted in Fig.1. A redundant router system comprises two heterogeneous routers. These routers are combined redundantly using VRRP, and they are exchanged periodically. When a router becomes the backup router, its software configuration is initialized immediately. Thus, even undetectable malware can be deleted from the router. However, the same-type malware may try to infect the current master router again. Such an attempt may be prevented by means of changing the master router's software to be different from the backup router's one. If this changing is repeated, the routers will be kept malware-free for a long time.

For repeating the router exchange, the router's priority needs to be changed periodically [7]. This change is performed in a unified manner using a centralized controller. Here, the controller needs to control heterogeneous routers. Thus, a command interpreter function for a new-type backup router needs to be attached dynamically to either the controller or the router [8].

Ultimately, this system is implemented within a single hardware router, and thus elements are implemented as

[††]The authors are with Tokai University, Minato-ku, Tokyo, 108-8619 Japan.

[†]The authors are with the graduate school of Tokai University, Minato-ku, Tokyo, 108-8619 Japan.

software [10]. Specifically, the elemental routers are implemented as virtual routers (VRs) [11]. In addition, the controller is implemented on a virtual machine (VM). These elements are connected with each other using virtual switches (VS) [12].

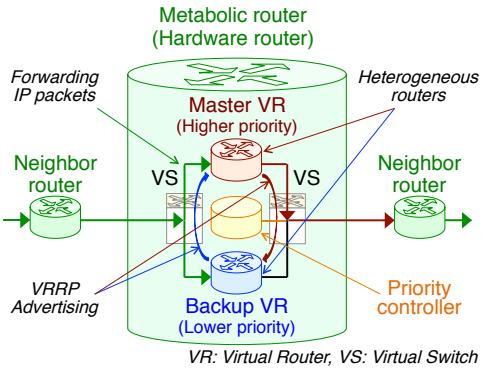

Fig. 1 Heterogeneous router system

3. Experiment

We evaluated our proposed scheme through the following four experiments: hitless exchange of heterogeneous routers, centralized priority control of heterogeneous routers using command interpreter functions, periodical exchange of heterogeneous routers, and protection of malware infection through exchanging heterogeneous routers. This section presents these experiments.

3.1 Hitless router-exchanging

Routers' exchanging periods were measured using an experiment system depicted in Fig.2. In this system, each element router is emulated by a hardware router, and thus a metabolic router is configured as the redundant hardware-routers system. In Fig.2, Controller, Router1, and Router2 are located in the center top, the center middle, and the center bottom, respectively. In addition, Host1 and Host2 are on the left and the right upper. Here, Host3 on the right lower was not used in this experiment. Specifications of Router1 and Router2 are summarized in Table 2 and Table 3, respectively. Their specifications were exchanged occasionally. In addition, those of Host1, Host2, and Controller are summarized in Table 1. As Switch1 and Switch2, Gigabit Ethernet switches were used [12].

Table 1 Specification of Host1, Host2 and Controller

CPU	Intel Core i7-10710U
Memory	64GB
Storage	1TB
OS	Linux Ubuntu 20.04

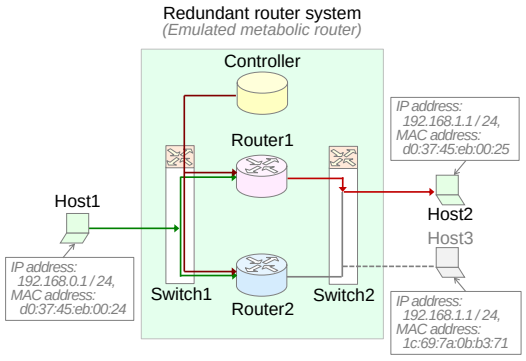

Fig. 2 Experiment system configuration

Table 2 Specification of Router1

CPU	Intel Core i7-10710U
Memory	64GB
Storage	512MB
OS	VyOS version 1.4-rolling-202206161834 [11]

Table 3 Specification of Router2

Model	CISCO 1812J
CPU	MPC8500
Memory	128MB
Storage	32MB
OS	IOS version 12.4

In the first stage, Controller initially implemented command interpreters for Router1 and Router2. Then, through SSH [13] control by Controller, the VRRP priority levels of Router1 and Router2 were set to 253 and 252, respectively. Next, Host1 and Host2 communicated with each other using Linux's ping command. The payload length of each IP packet was set to 84 bytes, and the packet transmission interval was set to 1 millisecond. Here, the packet length was set shorter in order to measure router-exchanging latency rather than packet forwarding throughput. In this condition, Router1 (master) forwarded all packets without packet loss.

In the second stage, during the ping communication, Router2's priority level was changed from 252 to 254. Accordingly, the master router was changed from Router1 to Router2. Here, all ping packets were forwarded without loss.

From this result, we can conclude that even heterogeneous routers can be exchanged with each other within 1 millisecond using VRRP.

3.2 Centralized priority control

Priority levels of heterogeneous routers were controlled dynamically in a centralized control manner. In this experiment, Controller in Fig.2 was configured as shown in Fig.3. It comprised Control Program (CP), Command Script (CS), Interpreter1, and Interpreter2.

Although CP and CS were installed initially, Inter-

preter1 and Interpreter2 were installed on demand when Router1 and Router2 were added to the system, respectively. The specifications of Router1 and Router2 are described in Table 2 and Table 3, respectively. In addition, those of Host1, Host2, and Controller are in Table 1.

The CP's role is to control Router1 and Router2 according to CS in which commands are written sequentially in the common language. In order to rewrite these commands in the native languages of Router1 and Router2, CP uses Interpreter1 and Interpreter2, respectively. Then, CP sends the rewritten commands appropriately to either Router1 or Router2. Examples of interpreted commands are shown in Table 4.

In the first stage of the experiment, the system was configured initially without Router1, Router2, Interpreter1, and Interpreter2. Then, Router1 and Interpreter1 were added to the system and Controller, respectively. Here, Router1's priority was set to 253, and thus Router1 acted as the master router.

In the second stage, Host1 and Host2 communicated with each other using Linux's ping command. The payload length of each IP packet was set to 84 bytes, and the packet transmission interval was set to 1 millisecond. Then, Router2 and Interpreter2 were added to the system and Controller, respectively. Here, Router2's priority was set to 252, and thus Router2 acted as the backup router. In this condition, Router1 (master) forwarded all packets without packet loss.

This result shows that heterogeneous routers and their interpreters can be added without packet forwarding interruption in our implementation scheme.

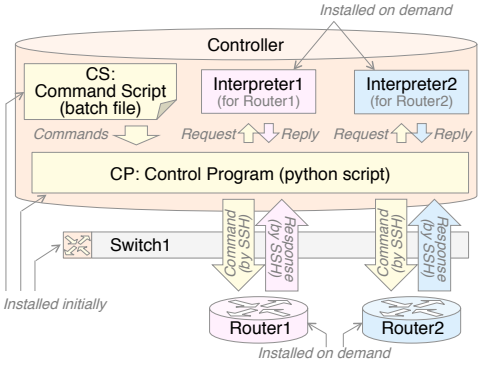

Fig. 3 Controller implementation

3.3 Periodical router-exchanging

Router-exchanging was repeated so as to keep a router's priority level within the limit.

In the first stage, the system was configured without Router2 in Fig.2. Consequently, Router1 acted as the master router and its priority level was initially set to 253.

In the second stage, by means of the centralized priority control scheme described above, Controller was added the command interpreter function for Router2. Then, Router2 was connected to the system. Its priority level was initially set to 252. Accordingly, Router2 acted as the backup router.

In the third stage, by means of the hitless router-exchanging scheme described above, Controller increased Router2's priority level from 252 to 254. As a result, the routers were exchanged immediately. Then, Controller decreased Router1's priority level from 253 to 252. Continuously, Controller also decreased Router2's priority level from 254 to 253.

In the fourth stage, Controller increased Router1's priority level from 252 to 254. As a result, the routers were exchanged again. Then, Controller decreased Router2's priority level from 253 to 252. Continuously, Controller also decreased Router1's priority level from 254 to 253.

Here, the system state was returned to that of the beginning in the third stage. This means that, in our proposed scheme, priority-level saturation can be avoided, and thus hitless router-exchanging will be repeated semi-permanently even between heterogeneous routers.

3.4 Protecting malware infection

A protective effect of our scheme against malware infection was examined using the system in Fig.2. In this experiment, Host1 and Host2 acted as a web client and its legitimate web server, respectively. Furthermore, Host3 was added as a fake web server. Host3 was assigned the same IP address as that of Host2, while their hardware MAC addresses are different from each other. Host settings are summarized in Table 5. In order to emulate repetitive attacks, a dummy malware file shown in Table 6 was set initially in both Router1 and Router2. This file was programmed to act on VyOS [11].

In the first stage, Router1 and Router2 acted as the master and its backup, respectively. Any malware file was not executed yet in this stage. Then, Host1 (web client) accessed Host2 (legitimate web server), as it intended. In addition, we verified that Router1's packet forwarding table had been set so as to resolve Host2's MAC address from Host2's IP address.

In the second stage, Router1 (master) executed the malware file. Consequently, Host1 (web client) accessed Host3 (fake web server) in place of Host2 (legitimate web server). In addition, we observed that Router1's packet forwarding table had been changed so as to resolve Host3's MAC address from Host2's IP address.

In the third stage, Controller changed the master router from Router1 (VyOS) to Router2 (IOS) using our scheme. Since Router2 did not execute the malware file yet, Host1 (web client) accessed Host2 (legitimate web server) again, as it intended. In addition, we observed that Router2's packet forwarding table had been set so as to resolve Host2's MAC address still from Host2's IP address.

In the fourth stage, Router2 (new master) tried to execute the malware file. However, it failed because Router2 could not understand the program command. Thus, Host1 (web client) continuously accessed Host2 (legitimate web

Table 4 Example interpretations

Target	Command	Comment
Common	set interface ethernet eth1 vrrp vrrp-group 1 priority 253	Original source
Router1	set high-availability vrrp group 1 priority 253	VyOS native
Router2	vrrp 1 priority 253	IOS native

Table 5 Configuration of hosts

Host	Function	Software	IP address	MAC address
Host1	Web client	Firefox 85.0.1	192.168.0.1/24	d0:37:45:eb:00:24
Host2	Legitimate web server	Apache 2.4.41	192.168.1.1/24	d0:37:45:eb:00:25
Host3	Fake web server	Apache 2.4.41	192.168.1.1/24	1c:69:7a:0b:b3:71

server). In addition, we observed that Router2's packet forwarding table had not been changed.

Consequently, those results show that the exchange between heterogeneous routers can mitigate the effects of repetitive malware infection.

Table 6 Dummy malware program

```
ip neigh replace 192.168.1.1 lladdr 1c:69:7a:0b:b3:71 dev eth2
```

4. Conclusion

In this paper, for achieving router metabolism, we evaluated our heterogeneous router exchanging scheme through four experiments. In the first experiment, VRRP exchanged the master router with the heterogeneous-type backup one within 1 millisecond. In the second experiment, when the redundant router system deployed heterogeneous routers, a centralized priority controller was implemented their command interpreter functions dynamically without interruption of packet forwarding. In the third experiment, by means of the centralized priority control, router's priority level was suppressed not to reach the limited level, and thus the master router was exchanged repeatedly between heterogeneous routers. In the fourth experiment, by means of the heterogeneous router exchange, repetitive malware execution on the master router was obstructed. As the results of those four experiments, we can say that router metabolism utilizing heterogeneous routers is promising as one of the countermeasures against malware.

Acknowledgement

The experiments were assisted by Yuuki Tsubayama and Shota Kai, Tokai University. This work was supported by JSPS KAKENHI Grant Number JP19K11948.

References

[1] A. Sood et al., "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," IEEE Security & Privacy, vol.11, no.1, pp.54-61, Jan. 2013.
[2] N. An et al., "Behavioral anomaly detection of malware on home routers," 2017 12th International Conference on Malicious and Unwanted Software (MALWARE), pp.47-54, Oct. 2017.
[3] A. Stasinopoulos et al., "The weakest link on the network: Exploiting ADSL routers to perform cyber-attacks," IEEE International Symposium on Signal Processing and Information Technology, pp.000135-000139, Dec. 2013.
[4] K. Gajera et al., "A Novel Approach to Detect Phishing Attack Using Artificial Neural Networks Combined with Pharming Detection," 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), pp.196-200, Jun. 2019.
[5] P. O'Kane et al., "Obfuscation: The Hidden Malware," IEEE Security & Privacy, vol.9, no.5, pp.41-47, Sep. 2011.
[6] E. M. Rudd, et al., "A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions," IEEE Communications Surveys & Tutorials, vol.19, no.2, pp.1145-1172, Secondquarter. 2017.
[7] Y. Miyaoka et al., "A repetitive router-switching scheme for achieving a metabolic router," ICETC 2020, D1-2, Dec. 2020.
[8] Rei Ishioka et al., "A router metabolizing scheme using heterogeneous virtual routers," ICETC 2021, C3-5, Dec. 2021.
[9] S. Nadas, "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6," IETF RFC5798, Mar. 2010.
[10] M. Rosenblum et al., "Virtual machine monitors: current technology and future trends," IEEE Comp. Mag., vol.38, no.5, pp.39-47, May. 2005.
[11] "VyOS - Open source router and firewall platform," https://vyos.io/, Jan. 23, 2021.
[12] "IEEE 802.1d ethernet bridging - Browse Files at SourceForge.net," https://sourceforge.net/projects/bridge/files/, Jan. 23, 2021.
[13] T. Ylonen et al., "The secure shell (SSH) protocol architecture," IETF RFC 4251, Jan. 2006.