# Modeling of Infection Phenomenon and Evaluation of Mitigation Methods for IoT Malware Mirai by Agent-Oriented Petri Net $PN^2$

Shingo Yamaguchi and Hiroaki Tanaka
Graduate School of Sciences and Technology for Innovation, Yamaguchi University
2-16-1 Tokiwadai, Ube 755-8611, Japan
Email: {shingo, w902ff}@yamaguchi-u.ac.jp

***Abstract*—In September 2016, an unprecedented massive DDoS attack was launched by IoT devices. This attack was caused by a new type of malware called *Mirai*. IoT devices are characterized by the large volume, pervasiveness, and high vulnerability. Thus such a DDoS attack tends to become massive and disruptive. In this paper, since Mirai can produce copies of itself, we modeled the infection phenomenon of Mirai with agent-oriented Petri net $PN^2$. Using the model, we also evaluated the cost-performance of mitigation methods which use reboot and/or a worm *Hajime* without DDoS capabilities.**

## I. Introduction

A new type of malware called *Mirai* primarily targets IoT devices such as IP cameras and home routers. IoT devices are characterized by the large volume, pervasiveness, and high vulnerability [1]. Thus a DDoS attack launched by IoT devices tends to become massive and disruptive. Addressing the threat of Mirai is an urgent issue.

In November 2016, US-CERT [2] provided a mitigation method for DDoS threat posed by Mirai and other malware. Since Mirai exists in dynamic memory, rebooting the infected device enables us to remove it. The devices have to be changed from the default password to a strong password, otherwise they would be reinfected. This requires us to analyze the cost-performance of the mitigation method using reboot.

In October 2016, a new type of worm called *Hajime* was found [3]. Hajime can produce copies of itself like Mirai, but currently does not have any DDoS capabilities. In addition, Hajime blocks ports which Mirai uses to infect an IoT device. Thus Hajime is considered as one of mitigation methods for Mirai. Like Mirai, Hajime exists in dynamic memory, thus it would be lost as rebooting the infected device. The device is also exposed to reinfection. This requires us to analyze the cost-performance of the mitigation method using not only reboot but also Hajime.

In this paper, we construct a mathematical model representing the infection phenomenon of Mirai. We regard the phenomenon as multi-agent system, and express it with agent-oriented Petri net $PN^2$. Using the model, we also analyze the cost-performance of the mitigation methods using reboot and/or Hajime.

## II. Mirai and Agent-Oriented Petri Net $PN^2$

*a) Mirai:* Mirai's attack consists of two steps. The first step is to infect an IoT device and then to make it a bot. There are more than 100,000 IoT devices which use easy-to-guess password. By using the password, Mirai intfects those devices one after another. The second step is to perform DDoS attack.

*b) Agent-Oriented Petri Net $PN^2$:* $PN^2$ is an extended model of Petri nets proposed by Hiraishi [4] to theoretically analyze multi-agent systems. Intuitively, a $PN^2$ is a Petri net (called as *environment net*) whose each token is a Petri net (called as *agent net*). An agent net represents an agent. An environment net represents an environment in which agents interact and move. Each transition of the environment net is synchronized with one or more transitions of agent net. It is called as *transition binding*. The increase and decrease of tokens on the environment net respectively represent the duplication and vanishment of agents. Our research group [5] is developing a tool for editing and simulating $PN^2$.

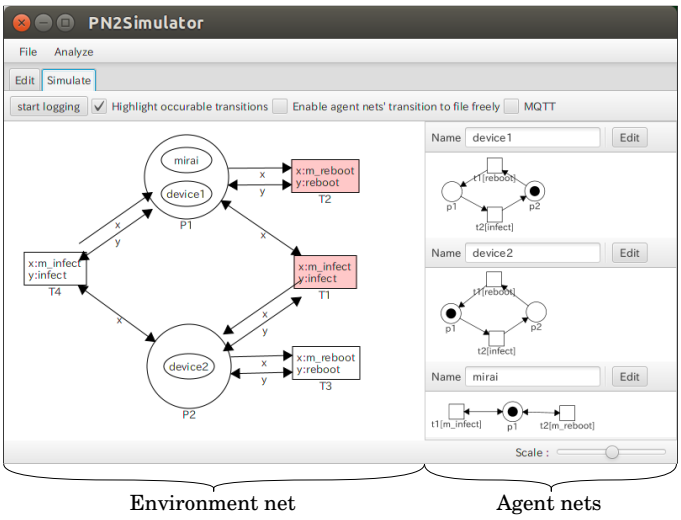
## III. Modeling of Infection Phenomenon

An IoT system is a network of devices. We regard the devices/Mirai and the network as agents and an environment, and express the infection phenomenon of Mirai with $PN^2$. When a device is infected with Mirai, it becomes a bot. When the infected device is rebooted, it returns to normal. We model this behavior as the agent net shown in the upper right of Fig. 1 (a). Mirai repeatedly infects IoT devices. Mirai vanishes when an infected device is rebooted. We model this behavior as the agent net shown in the lower right of the figure. We model the network as the environment net shown in the left side of the figure. Each place represents a node identified by an IP address, and has a single device as a token. Mirai is also represented as a token. The IoT system of Fig. 1 (a) consists of two devices. The device `device1` of `P1` has been infected with Mirai, while the device `device2` of `P2` is normal.

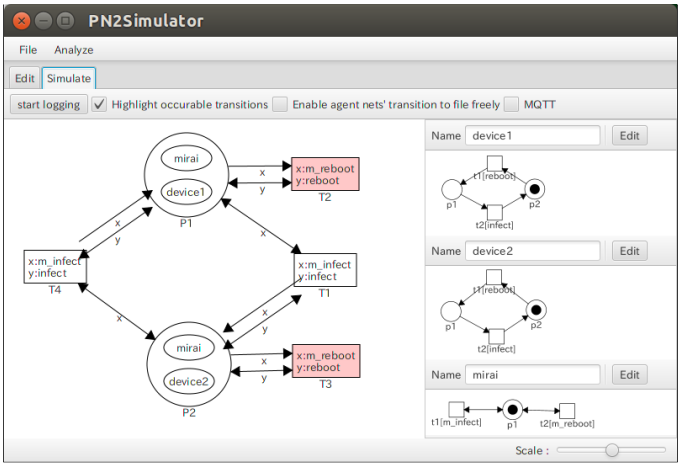
We regard an infection as an interaction between Mirai and an IoT device, and express it with a transition binding. In the state shown in Fig. 1 (a), transition `T1` is firable. This means that the Mirai of `P1` can infect the device `device2` of `P2`. A firing of `T1` produces a copy of Mirai into `P2` and changes `device2` to a bot (See Fig. 1 (b)).

## IV. Evaluation of Mitigation Methods

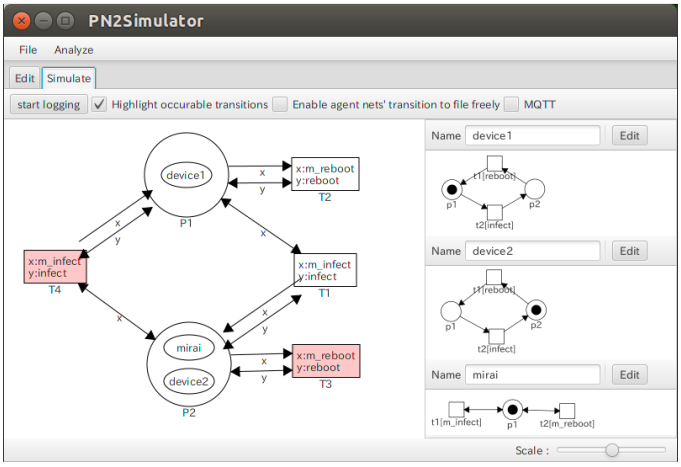
We add the mitigation methods that use reboot and Hajime into the $PN^2$ model. We regard rebooting an infected device as an interaction between Mirai and the device, and express it with a transition binding [6]. In the state of Fig. 1 (b), transition




(a) The initial state. The device `device1` of `P1` has been infected with Mirai, while the device `device2` of `P2` is normal.




(b) The state after firing `T1`, in which the Mirai `P1` produced a copy of itself in `P2` and has changed `device2` to a bot.




(c) The state after firing `T2`, in which the Mirai vanished from `P1` and `device1` has returned to normal.

Fig. 1. PN$^2$ model of infection phenomenon of Mirai.

`T2` is firable. This means that the Mirai of `P1` can be removed by rebooting `device1`. A firing of `T2` removes the Mirai from `P1` and restores `device1` to normal (See Fig. 1 (c)). On the other hand, since Hajime has the same capabilities as

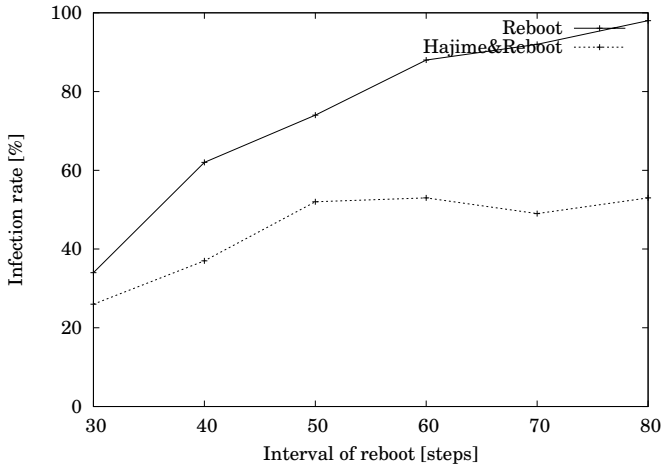



Fig. 2. Interval of reboot–infection rate of Mirai.

Mirai except for DDoS capabilities, we model Hajime as the same agent net as Mirai.

Using the model, we conducted an experiment to evaluate the cost-performance of the two mitigation methods. In the experiment, we used an IoT composed of 10 devices. The initial state was set to be that Mirai exists only in one node and every device is normal. Varying the expected interval of reboot for each device as $30, 40, \cdots, 80$ steps, we measured the infection rate of Mirai (= the number of infected devices / 10) after 1,000 steps. Figure 2 shows the result. The horizontal axis is the expected interval of reboot. The vertical axis is the mean of infection rate of Mirai for 10 trials. The solid line shows the result obtained in the case of the mitigation method that uses only reboot. The infection rate increases rapidly and reached 80% at 60 interval steps. The dashed line shows the result obtained in the case of the mitigation method that uses not only reboot but also Hajime. The infection rate increases slowly and was reduced to around 50%.

## V. Conclusion

In this paper, we constructed a PN$^2$ model representing the infection phenomenon of Mirai. Using the model, we also evaluated the cost-performance of the mitigation methods that use reboot and/or Hajime. As a future work, we are going to incorporate superiority of Mirai and Hajime into the model, and to evaluate the cost-performance of the mitigation methods.

## References


[1] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, "DDoS in the IoT: Mirai and other botnets," IEEE Computer, vol.50, no.7, pp.80–84, 2017.

[2] US Computer Emergency Readiness Team, "Heightened DDoS threat posed by Mirai and other botnets," https://www.us-cert.gov/ncas/alerts/TA16-288A, 2016.

[3] S. Edwards, I. Profetis, "Hajime: Analysis of a decentralized internet worm for IoT devices," https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf, 2016.

[4] K. Hiraishi, "A Petri-net-based model for the mathematical analysis of multi-agent systems," IEICE Trans. on Fundamentals, vol.E84-A, no.11, pp.2829–2837, 2001.

[5] K. Nakahori, S. Yamaguchi, "A support tool to design IoT services with NuSMV," Proc. of IEEE ICCE 2017, pp.84–87, 2017.

[6] H. Tanaka, S. Yamaguchi, "On modeling and simulation of the behavior of IoT devices malwares Mirai and Hajime," Proc. of IEEE ISCE 2017, #20, 2017.