Quick Blocking Operation of IDS/SDN Cooperative Firewall Systems by Reducing Communication Overhead

Akihiro Takai*, Yusei Katsura**, Nariyoshi Yamai*, Rei Nakagawa*, and Vasaka Visoottiviseth***

* Institute of Engineering, Tokyo University of Agriculture and Technology, Tokyo, Japan

** Graduate School of Science and Technology, Nara Institute of Science and Technology, Nara, Japan

*** Faculty of Information and Communication Technology, Mahidol University, Nakhon Pathom, Thailand

s224164x@st.go.tuat.ac.jp, katsura.yusei.ky6@is.naist.jp, nyamai@cc.tuat.ac.jp,
rnakagawa@go.tuat.ac.jp, vasaka.vis@mahidol.edu

Abstract—**An Intrusion Detection System (IDS) / Software Defined Networking (SDN) cooperative firewall system has attracted much attention recently because it has many advantages of dynamic network configuration with SDN and scalable IDS hosts. In the IDS/SDN cooperative firewall system, an SDN switch relays traffic between a client and a server and mirrors traffic from a client to an IDS host. The IDS host monitors the mirrored traffic and notifies the SDN switch to block malicious traffic according to the detection of the attack. At this point, malicious packets reach the server until the IDS detects the attack and notifies it. In this paper, we propose a method to speed up mirroring and notification by integrating IDS and SDN switch hosts as a method to shorten the blocking time and compare it with existing methods. The experimental system was constructed using Raspberry Pi3 B+ and 4B boards. As a result, it was confirmed that the proposed method completes the blocking operation faster than the existing method. We also investigated the breakdown of the blocking time to confirm the effect of the proposed method.**

Keywords— **Firewall, Intrusion Detection System, Software Defined Network, OpenFlow**

Akihiro Takai was born in Japan in 1999 and received his B.E. from Tokyo University of Agriculture and Technology (TUAT), Japan in 2022. Currently, he is a master's student at Tokyo University of Agriculture and Technology, Japan. His research interests include computer networks.

Yusei Katsura was born in Japan in 1996 and received his B. Info. Env. degree from Tokyo Denki University, Japan in 2019, and his M. S. degree in computer engineering from Nara Institute of Science and Technology (NAIST), Japan in 2022. He was a research student at Tokyo University of Agriculture and Technology (TUAT), Japan in 2019-2020. He is currently a Ph.D. student at Nara Institute of Science and Technology. His research interests include computer networks.

Nariyoshi Yamai was born in Japan in 1961 and received his B.E. and M.E. degrees in electronic engineering and Ph.D. degree in information and computer science from Osaka University, Japan in 1984, 1986, and 1993, respectively. Currently, he is a professor at the Institute of Engineering, Tokyo University of Agriculture and Technology (TUAT), Japan. His research interests include distributed systems, network architecture, network security, and the Internet.

Rei Nakagawa was born in Japan in 1993, received his B.S. and M.S. degrees from the Tokyo University of Science, Japan, in 2016, and 2018 respectively, and a Ph.D. degree in informatics and engineering from the University of Electro-Communications (UEC), Japan, in 2021. He has been an assistant professor at the Institute of Engineering, Tokyo University of Agriculture and Technology (TUAT), Japan since April 2021. His research interests include network architecture, video streaming technology, software defined network, and information centric networking.

Vasaka Visoottiviseth was born in Thailand in 1975, received her M.E. and B.E. degrees from Tokyo University of Agriculture and Technology (TUAT), Japan in 1999 and 1997, respectively, and received her Ph.D. degree in computer engineering from Nara Institute of Science and Technology (NAIST), Japan in 2003. Currently, she is an associate professor at Mahidol University, Thailand. Her current research interests include mobile and wireless computing, network security, and digital forensics.