The Flow-Reduced Malware Detection System by Controlling Inactive/Activr Timeout

Jae Kyu Lee*, Hyeon Yang*, Kyeong Ho Park**,Si Young Lee**,Seong Gon Choi*

**Broadband Network Lab., Chungbuk National University, Korea*

***Xabyss Inc., Korea*

princeljk@cbnu.ac.kr, adieu@cbnu.ac.kr, khpark@xabyss.com, edward.lee70@xabyss.com, choisg@cbnu.ac.kr

***Abstract*—This paper shows the flow reduction effect of malware detection system through inactive/active timeout control. In the gigabyte network environment, the DB search speed of the malware detection system that processes high-speed, largecapacity data is affected by the number of stored flows. Therefore, it is necessary to reduce the number of stored flows. The malware detection system captures network data with the First-N technique and adjusts the session length by modifying the inactive/active timeout. A drill-down mechanism is used for malware inspection of network data stored in DB. Inactive/active timeout is adjusted to verify that the number of flows decreases as the session length increases.**

***Keyword*—First-N, Inactive/Active Timeout, Drill-Down Search, Flow Count, Storage Efficiency**

Jae Kyu Lee received B.S degree in the College of Electrical & Computer Engineering, Chungbuk National University, Korea in 2017. He is currently an M.S. candidate in School of Electrical & Computer Engineering, Chungbuk National University. His research interest is network security.