

Early Detection of LDDoS Attacks in IOT Utilizing Locality Sensitive Incremental TSVM Method

ZengGuang Liu*, XiaoChun Yin**, RuiPing Yang*, AnMing Dong***

*College of Computer Science and Engineering, ShanDong University of Science and Technology, QingDao, 266590 CN

**Blockchain Laboratory of Agricultural Vegetables, WeiFang University of Science & Technology, ShouGuang, 262700 CN

***School of Computer Science and Technology, Qilu University of Technology (Shandong Academy of Sciences), JiNan, 250353 CN

st.lzg@163.com, xiaochunvin@wfust.edu.cn, yrp9024@163.com, anmingdong@qlu.edu.cn

Corresponding Author: xiaochunvin@wfust.edu.cn, Tel: +86 18853688750

Abstract—The Mirai botnet and its variants has made Internet of Things (IOT) devices a powerful amplifying platform for Low Rate Distributed Denial-of-Service (LDDoS) attacks. In this paper, we investigate and develop a novel semi-supervised Locality Sensitive Incremental Transductive Support Vector Machine (LS-ITSVM) method. The proposed method maximizes the margins of different network flows by incorporating local frequency-domain features from the autocorrelation sequence of network flow into the regularization time-domain framework of TSVM. And it saves training and detecting time by incremental training support vectors and new added samples. The result of simulation proves the proposed method can distinguish abnormal network flows with higher detection accuracy, faster training and response time, and prevent abnormal network flow groups with less impaction.

Keyword—LDDoS, Internet of Things, Locality Sensitive Incremental TSVM, Frequency-Domain Features, Semi-Supervised Clustering



ZengGuang Liu was born in ShouGuang, China in 1982. He received the B.S. and M.S. degrees in computer science from the University of ShangHai for Science and Technology in 2005 and 2008 respectively. He is currently pursuing the Ph.D. degree in computer science at the University of ShanDong for Science and Technology.

From 2008 to 2016, he was a Senior Architecture Engineer in Core Network Department of Alcatel-Lucent. He had been a Principal AI Engineer of Hewlett Packard Enterprise since 2016. His research interests include big data, AI and network security areas.

He was a recipient of the Innovation Award of ShanDong for Excellence in 2011.



XiaoChun Yin (M'12) was born in ShouGuang, China in 1980. She received the B.S. degree in Education and Technology from QuFu Normal University in 2004, and received the M.S. degree in Education and Technology from Nanjing Normal University in 2007, and received the Ph.D. from Dongseo University in 2015.

From 2007 to now, she is an associate professor in Weifang University of Science & Technology. Her research interests include network security, IoT security, blockchain and AI areas.

Professor Yin was a recipient of the Science Research Innovation Award of Weifang University of Science & Technology in 2017 and 2018.



RuiPing Yang was born in Shandong, China in 1990. She received his B.Sc. (2014) degree and M.Sc. (2017) degree in mathematics from QuFu Normal University.

She is currently a Ph.D. candidate in the College of Computer Science and Engineering, Shandong University of Science and Technology. Her current research interests include machine learning, deep learning and neural networks.



Anming Dong received the B.E. degree in electronic information science and technology from Liaocheng University in 2004, the M.E. degree in communications and information systems from Lanzhou University in 2007, and the Ph.D. degree in communications and information systems from Shandong University in 2016.

He is currently an Associate Professor with the School of Computer Science and Technology, Qilu University of Technology (Shandong Academy of Sciences). His research interests include MIMO techniques, wireless communications, wireless machine learning, and application of optimization techniques for signal processing and wireless communications.

He was a recipient of the Excellent Doctoral Dissertation Awards of Shandong Province, in 2017.