Autoencoder ensembles for network intrusion detection

Chun LONG[ab], JianPing XIAO[ab], Jinxia WEI [a], Jing ZHAO[ab], Wei WAN[ab], Guanyao DU[ab]

a *Computer Network Information Center, CAS (Chinese Academy of Sciences), China*

b *University of Chinese Academy of Sciences, China*

anquanip@cnic.cn, xiaojianping@cnic.cn, weijinxia@cnic.cn, jingzhao@cnic.cn, wanwei@cnic.cn, duguanyao@cnic.cn

***Abstract*—Machine learning methods have been widely used in the field of intrusion detection. However, most methods require labeled data sets, and the overhead is very high. Network data is often high-dimensional and has the problem of data imbalance, which makes many techniques unable to adapt to the real network environment. In this paper, we propose a network intrusion detection model based on autoencoder ensembles. This model uses a recursive feature addition algorithm to select the optimal subset of features, which can significantly reduce the training time of classifiers, and improve the performance of intrusion detection system. After feature selection, the feature subset is grouped, and then each group is mapped to an autoencoder. Multiple such autoencoders ensembles form the detection model. Only normal samples are used for training. The detection model is unsupervised, which improves the efficiency of detecting known and unknown attacks. The experimental results show that feature selection can effectively reduce training and detection time. Our model has high detection accuracy and strong adaptability.**

***Keyword*—Autoencoder, Feature Selection, Machine Learning, Network Intrusion Detection System, Recursive Feature Addition**

Chun LONG is currently a full engineer in Computer Network Information Center, Chinese Academy of Sciences, China. He received Ph.D. degree in Computer Software and Theory from University of Chinese Academy of Sciences. He developed Compound Attack Prediction Method based on the Attack Graph and Multi-source Security Event Fusion method based on EA-DS Evidence Theory. His research interests include Information Security, Cyber Security, Cyber Risks and Web Vulnerabilities.

Jianping XIAO is currently a postgraduate student in Computer Network Information Center, Chinese Academy of Sciences, China. He received B.S. degree in Network Engineering from Beijing University of Posts and Telecommunications, and he is currently studying for M.S. degree in University of Chinese Academy of Sciences, majoring in Cyberspace Security. His research interest is Cyber Security.

Jinxia WEI is currently a full engineer in Computer Network Information Center, Chinese Academy of Sciences, China. She received Ph.D. degree in Cryptography from Beijing University of Posts and Telecommunications. Her current research interests include network security situation awareness, security big data analysis, and cloud computing security.

Jing ZHAO is currently a full engineer in Computer Network Information Center, Chinese Academy of Sciences, China. She received M.S. degree from Beijing University of Posts and Telecommunications, and she is currently studying for Ph.D. in University of Chinese Academy of Sciences, majoring in Computer Software and Theory. Her current research interests include network security situation awareness, security big data analysis, and cloud computing security.

Wei WAN is currently a full engineer in Computer Network Information Center, Chinese Academy of Sciences, China. He received Ph.D. degree in Computer Software and Theory from University of Chinese Academy of Sciences. He has presided over and participated in many national projects. Moreover, he developed Investigation of state division in botnet detection model, Botnet detecting method based on activity similarity and so on. His research interests include Information Security, Cyber Risks and Web Vulnerabilities.

Guanyao DU is currently a full engineer in Computer Network Information Center, Chinese Academy of Sciences, China. She received Ph.D. degree from Beijing Jiaotong University. Her current research interests include network security situation awareness, security big data analysis, and cloud computing security.