BiLSTM-Ridge Regression Meta Learning Model for Few-Shot Logs Classification

Hanji Shen*, Jun Li **, Xiang FU ***

* Computer Network Information Center, Chinese Academy of Sciences, China

** University of Chinese Academy of Sciences, China

*** Blue Sky Frontier Science and Technology Innovation Center, Beijing, China

shenhanji@cnic.cn, jlee@cstnet.cn, fuxiangpku@163.com

***Abstract*—In the high threat attack classification detection task,, it is hard to find attack logs in the huge log set because the number of attack logs in the log set is particularly small, which is a major difficulty in the high threat attack classification detection task. This paper proposes a Meta learning classification model based on few-shot samples. Aiming at the uneven distribution of samples in the data set. Firstly, processing the source data set and enhance the data set to build a data set that can meet the C-way k-shot, then using fasttext to pre-train the data set samples, Finally, building a meta knowledge learner by using BiLSTM and support set meta training classifier by using ridge regression. The experimental results show that the proposed BiLSTM-Ridge regression model shows good results in the classification and detection of small sample attack logs on the real 335 attack log data sets of China Science and technology network. The accuracy of 5-way 3-shot can reach 66.47%, and the accuracy of 5-way 1-shot can reach 49.72%, which is improved compared with the typical small sample model.**

***Keyword*—Few shot, Meta Learning, BiLSTM, Ridge Regression, High threat attack**

Hanji Shen is currently a full engineer in Computer Network Information Center, Chinese Academy of Sciences, China. He received M.S. degree in Engineering in the field of Computer Technology from University of Chinese Academy of Sciences, and he is currently studying for a Ph.D. in University of Chinese Academy of Sciences, majoring in Computer Software and Theory. He has been an IEEE member since 2014. His research interest is Cyber Security.

Jun Li is currently a researcher, deputy chief engineer and doctoral supervisor in Computer Network Information Center, Chinese Academy of Sciences, China. He received Ph.D. degree in Computer System Structure from University of Chinese Academy of Sciences. He is one of the earliest experts engaged in computer network technology research in China. He has been engaged in scientific research and engineering practice in the field of computer network for a long time. His research interests include Network Architecture and Cyber Security.

Xiang Fu is currently a full-time engineer in Beijing Blue Sky Frontier Science and Technology Innovation Center. He received a Doctor of Science degree in the field of computer science from Peking University. His research interest is artificial intelligence.