УДК 004.9

MULTI-TASK DEEP LEARNING-BASED INTRUSION DETECTION MODEL FOR IOT NETWORK

Huiyao Dong (ITMO University)
Scientific adviser – PhD, Kotenko Igor Vitalievich
(ITMO University; St. Petersburg Federal Research Center
of the Russian Academy of Sciences)

Introduction. The Internet of Things (IoT) connects physical and virtual entities using recent and emerging information and communication technologies. It allows network properties to automatically analyse certain scenarios or surroundings, benefiting all network environments with electronics, software, sensors, actuators, and internet connectivity [1]. As it has become the current technology trend and is applied in self-driving automobiles, smart healthcare, and smart cities, IoT vulnerabilities and the intrusion threats it faces can lead to considerable damage to devices or the system. IoT intrusion detection systems (IDSs) must be researched and enhanced to adapt to modern network attacks. This paper proposes a Multi-task Deep Learning-based approach for network traffic classification in IoT environment for detection of rare network intrusions with sparse data.

Body. The proposed method solves the following issues: (1) Network data are usually high-dimensional and have a great volume of samples, while much information is irrelevant. (2) Real life data has a skewed distribution, and many rare but crucial attacks lack samples. (3) Minimising false alarms while maximising detection rates is critical for IDS. Multi-Task Learning utilises the valuable information obtained in many related relevant tasks to enhance the performance on all. One of the main approaches is to learn the feature relationship for multiple tasks and computes common feature representations [2]. In data pre-processing stage, we utilise Elastic Net Regularization for input dimension reduction, then resampling methods for class balancing: Synthetic Minority Oversampling Technique (SMOTE) to increases minority weights and Edited Nearest Neighbours (ENN) down sampling for deep data cleaning. The DNN-based model is designed to be vertically deep with fully connected deep layers with two functional modules. It contains the common layers to learn feature representation and inter-task correlations; the task-specific layers for classification of different network attacks. Inspired by the architecture proposed in [3], the model assigns each tasks a SoftMax gating network to optimise tasks' weights and Dropout layer to eliminate irrelevant information, then task-specific networks receive knowledge from its own subnetwork and other related tasks. To compare the performance of STL and MTL, we build DNN-based STL, hard parameter sharing and soft parameter sharing MTL models, with same parameters set for DNN layers.

Findings. Though all constructed with DNN layers, both of the MTL models outperforms STL, and their false alarms are acceptable. Besides, soft parameter sharing MTL have better capability for anomaly detection than the hard parameter sharing when corresponding samples are limited.

Sources used:

1. Denisenko Ruiz J.F., Harjani R., Maña A., Desnitsky V., Kotenko I., Chechulin A. A methodology for the analysis and modeling of security threats and attacks for systems of embedded components // The 20th Euromicro International Conference on Parallel, Distributed and Network-Based Processing. – 2012. pp. 261–268.
2. Zhang Y., Yang Q. A Survey on multi-task learning // IEEE transactions on knowledge and data engineering. – 2022. – № 12. pp. 5586-5609.
3. Ma J., Zhao Z., Yi X., Chen J., Hong L., Chi, E. Modeling Task Relationships in Multi-task Learning with Multi-gate Mixture-of-Experts. – 2018. pp. 1930-1939.

Dong H. (author)	Signature
Kotenko I. (supervisor)	Signature