Research on Intrusion Detection Based on Incremental GHSOM Neural Network Model

Xiaoman Chi, Ximin Liu

Jilin Communications Polytecnic, Changchun, Jilin, 130012, China

Keywords: Incremental; Intrusion; Detection

Abstract: Compared with the traditional network intrusion detection method that uses the off-line method to train the intrusion detection model on the existing attack samples, even if the detection rate of the existing sample types is high, it is not effective for the new types of attack samples appearing in the network. Identification, such intrusion methods have problems such as slow speed and high cost of updating models, which is not conducive to detecting new types in the network[1]. This paper mainly focuses on the GHSOM neural network model and explores its incremental intrusion method.

1. Introduction

The key component of the information security integrated defense system is the intrusion detection system, and the second security defense line is the network intrusion detection system[2]. The network intrusion phenomenon can be identified by collecting and analyzing the traffic data of the key points of the network. The establishment of the traditional intrusion detection system detection model is based on the pattern matching method. With the rapid development of information technology, this kind of intrusion detection method can not meet the increasing demands of people. Therefore, it is necessary to conduct in-depth research on it. .

2. A Survey of the Research on Incremental GHSOM Neural Network Model in China

After learning new knowledge in the same learning system, most of the knowledge that was learned before is still an incremental learning algorithm. In the practical application process, this kind of learning algorithm can effectively improve the knowledge learned by the knowledge and update it accordingly, ensuring that the knowledge can be adapted to the updated data after the update, without re-learning the overall data. The method itself is not high in space and actual demand, and is more suitable for actual needs[3].

At present, the technicians who study the incremental learning algorithm have made good progress and results, such as the SVM incremental training algorithm, which is only used to retain the support vector after learning and remove the non-support vector; It may become a fast incremental learning algorithm used in the boundary vector of the support vector; improve the bias term for incremental training and so on. The disadvantage of these algorithms is that they leave the training sample mechanism support vector and start to crash. Seriously, information will be lost, which is not conducive to improving the learning accuracy rate.

The neural network learning algorithm is often used in intrusive detection environments with a large degree of variation because of its inherent fault tolerance and the advantages of large-scale nonlinear mapping and computation. The typical method in neural networks is self-organizing mapping, but the traditional SOM neural network algorithm itself has its own characteristics. It is mainly reflected in the fact that its neurons need to be clear before the clustering. Increased the difficulty of the work, and the probability of being able to achieve smoothly is not high, but this problem can be effectively solved by using the growth-type hierarchical self-organizing map neural network. The essence of GHSOM has a hierarchical structure as the SOM neural network. Expanding subnets and subnets for effective adjustment can also fully embody all the complex hierarchical relationships existing in the data, thus effectively solving the shortcomings of the fixed

  DOI: 10.25236/mmmce.2019.085

structure in the SOM neural network model. The GHSOM intrusion detection method itself has good adaptability to attack variants, but the traditional GHSOM network learning algorithm commonly used in the learning mode is batch, that is, if all the training samples can be obtained at one time, there is no need to Learn new knowledge[4]. It is obvious that the traditional GHSOM network model cannot effectively detect new types of attacks occurring in the network, and thus is limited in terms of the scalability and dynamic type of the intrusion detection itself.

In the process of in-depth exploration of incremental neural network learning methods, the more commonly used algorithm is SOM neural network, but this method can not be dynamically changed, which requires people to effectively adjust it by combining multiple learning algorithms. The researchers proposed self-organizing surface algorithms, evolutionary SOM, incremental network growth algorithms, and self-organizing incremental neural networks. These methods have the disadvantages of limited classification accuracy and overproduction matching training data when the new sample size is large.

3. Incremental GHSOM Learning Algorithm Effective Analysis

The incremental GHSOM learning process is carried out in the initial training and perfect GHSOM model by means of on-line detection and incremental learning, so as to dynamically update the GHSOM model during the detection process.

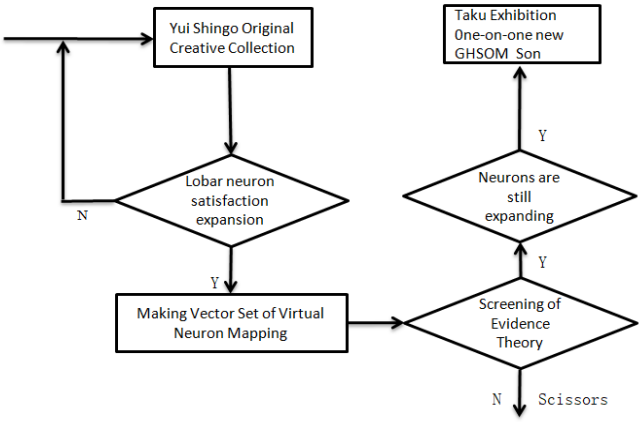

Fig.1. Schematic diagram of the incremental GHSOM dynamic learning process

As shown in the figure above, the incremental learning process diagram, in the incremental GHSOM network, uses the top-down layer expansion method for each online extraction detection mode vector to calculate and acquire the winning neurons in the examination[5]. Once the built-in mode vector and the winning neuron's homogeneous detection can be effectively fit, the output of the detection vector is the detection result, or else a new attack type appears, and the detection vector added in the incremental training set needs to be adjusted. After adjusting whether the incremental training set of the winning neuron is consistent with the requirement of the layer extension criterion, if the layer expansion condition is not satisfied, it means that the learning or detection process of the detection mode vector ends. Conversely, for the expansion of a subnet, the incremental training set has the same meaning as the initial training set, and the new subnet is trained until the structure is stable. Once the control requirements and dynamic growth of the neural network are the same, the immature subnets are removed and collected effectively, and then retrained and expanded to streamline the structure of the subnet itself[6].

Usually, the problems faced in the incremental GHSOM learning process are the judgment of the winning neurons and the detection vector type, the flow schematic method of constructing the incremental training set, the new subnet expansion setting conditions, and the control method of the network dynamic growth scale. Wait. After interpreting the specific feelings of these contents, it is necessary to determine the similarity threshold. The winning neurons that can be used for detection

are the key to judge the same kind, and the knowledge of the previous learning is not destroyed, and the dynamic incremental neural network of GHSOM is detected. In the meta-element, the initial network, the extended network, and the non-overlay leaf neurons can be used. The comparison and judgment of the winning neurons and the types of detection vectors need to be performed after the detection is completed, and the weight vector is also determined by using the Euclidean distance method. The measure is compared with the check vector[7].

The emergence of a new type of attack will make the type of the detection vector and the winning neuron itself inconsistent. In this case, it is necessary to collect the new type of attack type in the incremental training set and apply it to the new subnet. The source of the incremental training set is not certain and needs to be designed for its construction mechanism. Each incremental training set has the same meaning as a leaf neuron. The coverage in the neuron fully reflects the concentration of the distribution mapping vector. It can reflect whether a certain neuron needs to be trained again and whether the clustering effect is fully reflected. Have serious effects and effects. For the dynamically increased incremental training set, after adding a large specific value, it will be expanded into a mature new subnet for training[8].

Schematic diagram of GHSOM dynamic layer neural network expansion, the initial network is represented by the implementation, the SOM subgraph is represented by the dotted line connection, the neurons are the dots in the graph, and the non-leaf neurons in the initial network GHSOM are in the figure. White dots, covering neurons are represented by black dots, and non-covering neurons are represented by gray dots.

GHSOM dynamic incremental neural network can be suitable for dynamic expansion when the input attack type is new enough. The network structure will not be able to control its scale because of expansion, resulting in system collapse, which requires an effective control system. The effective control of the size of the neural network is mainly to reduce the space loss, and to control the incremental GHSOM mode to gradually mature. The initial neural network of this model has matured itself, and the incremental network is divided into two types, immature self-network and mature network, based on neural network. For GHSOM incremental networks, it is impossible to change the mature network knowledge, but it can expand and extend its knowledge using dynamic learning methods. This is the neural network that reflects the excellent aggregation effect. Using dynamic learning methods can change the immature network. Knowledge, that is, a subnet that fully reflects the undesirable clustering effect. Once the immature subnet below the mature neuron node is removed, the mapping vector of the non-covered leaf neurons in the immature subnet and the covering neurons need to be effectively collected, and the increment of the mature neuron node itself The training set is reconstructed. The effective combination of dynamic expansion method dynamically expands a layer of SOM subnet and a virtual neuron in mature neurons under the premise of the incremental training set. This SOM subnet is a simplified SOM subnet obtained after removing the GHSOM subnet. The cover network also covers a layer of SOM subnet, thus increasing the strength of the control network, and the newly expanded network structure itself is becoming mature[9]. The data training can be carried out more fully and comprehensively, so as to effectively improve the inspection ability.

4. Conclusion

In summary, through the in-depth exploration and analysis of the incremental GHSOM algorithm, its specific advantages can be clarified, such as the simultaneous learning of incremental learning and detection, and the dynamic update of the GHSOM model during the detection process. The implementation of the intrusion detection test in the local area network means the amplification and adaptability of the incremental GHSOM model itself, and through the exploration of its more frequent problems, the detection and analysis can effectively solve the existing problems.

References

[1] Zhang Kenong; Lu Jiahua; Gao Ming. An FPGA-based Gigabit network intrusion detection

method and implementation. National Network and Information Security Technology Seminar '2015 Proceedings (Volume 1).

[2] He Yiqing. An intrusion detection method based on directed bipartite graph model and Bayesian network; Proceedings of the 27th National Computer Security Academic Exchange Conference, 2014.

[3] Zhang Wentao; Wlodek Kulesza. Firewall traffic prediction based on BP neural network; Proceedings of the 3rd National Conference on Information Retrieval and Content Security; 2017.

[4] Fan Wei. Improved ant colony algorithm combined with BP network for intrusion detection; Proceedings of the 5th Annual Conference of Fuzzy Information and Fuzzy Engineering Branch of China Operations Research Society.

[5] Hong Yang; Ge Zhenhua; Wang Jikai; Bao Peng; Zhang Qibin; Chen Zonghai;; Verification code recognition based on deep convolutional neural network; Proceedings of the 19th China System Simulation Technology and Applications Annual Conference (19th CCSSTA 2018), 2018.

[6] Liu Yang; Li Xiaofeng; Jiang Zhiyong; Hou Jincai; Chen Minghui;; Application of Dao Chemical Fire and Explosion Hazard Index Evaluation Method in Light Hydrocarbon Storage Tanks; Science Technology and Engineering, 2014(22).

[7] Wang Xingzhu; Yan Junxi; Zeng Qinghuai. Network intrusion detection based on mean clustering analysis and multi-layer core set aggregation algorithm, Computer Applications and Software, 2015(12).

[8] Zhao Hong; Wang Zongshui; Wang Wei; Fu Lijun. Application Research of Network Consumer Classification Based on Bloom Filtering; The 9th (2014) China Management Annual Conference-Marketing Sessions Proceedings, 2014.

[9] Doctor of Sociology, University of Minnesota, USA Senior Associate Research Fellow, National Strategic Planning and Analysis Research Center, Mississippi State University Chen Xinxiang; Maintaining innovative "neural network hardware"; China Teacher's Daily, 2014.