Network Security Swarm-Intelligence Application Design Based on Collaborative Defense Technology

Dongmei Bin(✉), Chunyan Yang, and Songming Han

Electric Power Research Institute of Guangxi Power Grid Co., Ltd., Nanning 530023, Guangxi, China
wyyx022023@126.com

Abstract. This paper proposes a collaborative defense of network security based on Swarm intelligence Framework. This technology is based on joint detection and collaborative response, Relying on the swarm intelligence technology, the scheme can recognise the complete attack chain and perceive the global network from the perspective of a cyber-kill-chain timeline, achieving collective and precise defence of multiple network security entities, thus further improving the capability to recognise, defend, and dispose of the advanced and complex security threats. But Swarm intelligence technology is not yet mature. The design of communication messages needs to carry out various experiments according to different network attack characteristics, and in-depth research is required to form practical and scalable technical achievements.

Keywords: integrated learning · collaborative defense · swarm intelligence

1 Introduction

In the context of high-intensity network confrontation, implementing effective network security defense has become the focus of network attack and defense field. New attack methods represented by automation and intelligence have greatly changed the pattern of network security games. However, the multi-point collaborative defense technologies at both home and abroad are still in the early stages and lack a universal collaborative method and mechanism.

Therefore, the CTM (Collaborative Threat Management Device) is proposed based on the existing computer network security technology of UTM unified defense threat management, which aims to add collaborative defense and control functions on the basis of UTM. The main idea is to set CTM collaborative defense devices at key points like network nodes, and apply built-in firewall and other security components, so to monitor and collaboratively defend the traffic obtained by the detection system, thus achieving the intelligent, practical, and automated network security collaborative defense.

F. Huang et al. (Eds.): ICAIE 2023, AHCS 15, pp. 537–543, 2024.
https://doi.org/10.2991/978-94-6463-242-2_66

2 Network Security Collaborative Defense Framework Based on Swarm-Intelligence Technology

The framework of network security collaborative defense based on swarm-intelligence includes modules of data access and sharing, proactive prevention, joint sensing, collaborative response, etc. The modular structure can help to establish intelligent spatiotemporal correlation for information among various network security components, thus giving out accurate analysis result of the attack event; on the other hand, it can also dispose the network attack in encircling suppression manner by the linkage of multiple components.

The data access and sharing module is the basis to achieve collaborative sensing. It is mainly used to collect, store, parse, and restrict the information of specific security components, and finally share the information with other security components. The attacks that the network may suffer can be summarized by the swarm-intelligence-based network security proactive prevention technology, so to generate the network attack graph, based on which, the key attack path can be figured out through the swarm-intelligence algorithm, thus providing theoretical reference to support the joint sensing and collaborative response. By combining with swarm-intelligence technology, intelligent joint perception technology used among various network security components, more accurate security analysis result can be concluded for complex network attack event through the spatiotemporal correlation of information among various network security components. And by the collaborative response technology among multiple network security components, complex network attacks can be interrupted by the "encircling suppression" disposing formed by multiple security components.

3 Collaborative Detection Technology for Network Security Based on Ensemble Learning

Though the artificial intelligence algorithm has been used to detect the network attacks and obtained certain achievements, the single-detector algorithm still has shortcomings like large error, slow operation speed, and low generalization capability [1]. It is quite necessary to study and build an ensemble model for network detection which is not only accurate but also capable in generalization. Therefore, in this paper, an ensemble learning algorithm with dynamic adjustment and collaboration strategy is studied and used in the attack detection model to improve the detection accuracy.

3.1 Ensemble Learning Algorithm

Ensemble learning generates multiple detectors according to certain rules, and then combines them by a certain ensemble strategy to make a comprehensive judgment and output the final result [1]. Boosting algorithm is a new type of machine learning algorithm that emerges in artificial intelligence field during recent years. It can reduce bias in supervised learning and form a strong detector by continuously changing the sample distribution and weighting & stacking weak detectors, so to reduce the generalization error [2]. The algorithm continuously trains the unstable and weak detectors to generate

a sequence of weak detectors, adjusts the probability distribution of the training sample subset of the current sub-detector by the error of the previous generation sub-detector, and obtains different generations of sub-detectors through different training sample subsets. Finally, the strong detector can be formed by composing the weighted sub-detectors. Given a detection algorithm and training set as input vectors, it corresponds to a certain category label of the detection problems [3]. At the time of initialization, equal weights are assigned to each training sample, and then the weak detector algorithm is used to train the training set. After each training, larger weights are assigned to the training samples that fail in training, so to obtain a sequence of prediction functions. The prediction function with better prediction effect has a larger weight, and vice versa [4].

3.2 Network Attack Detection Technology Based on Ensemble Learning Algorithm

The biggest advantage of ensemble learning algorithm is that it can obtain high-precision detection models through repeated iterative training of weak detectors. Boosting algorithm can significantly improve the accuracy of unstable detection algorithms like the decision trees, neural networks, and support vector machines [5]. Each training of the algorithm can obtain a sub-detector, and each sub-detector is improved based on the calculation results of the previous generation sub-detector. Therefore, viewing from the perspective of training, the training of Boosting is a process of continuous optimization, that is, the process of the detector changing from unstable to stable state. For the attack event detection technology based on ensemble learning algorithm, it uses Boosting algorithm to conduct iterative training of the data sample sets and obtains a sequence of weak detectors that meet the error requirements [6], and then conducts weighted sum of the weak detector sequence to obtain a strong detector [7].

4 Multi-security-Component Collaborative Response Technology Based on Artificial Bee Colony Algorithm

In the field of cyberspace security, the attack response process can be deemed as a non-cooperative game process between attack and response. Since there are lots of uncertain factors during this game process, the response decision-making not only relies on the security response system itself, but also on the attack strategy used by the attackers. In such context of strategies interdependence, how to select effective and rational security response strategy is actually an issue that is worthy of being studied. The specific steps of multi-security-component collaborative defense based on artificial bee colony algorithm are as follows.

(1) Make all entities of network security intelligent and able to basically interact with other network security entities of the same or different types.
(2) Establish mechanism to achieve communication among multiple network security entities

All network security entities shall be designed into entities that can periodically and spontaneously exchange messages. In order to minimize the complexity of the

communication protocol, the way of designing active message, Update message, and abstract message is used to achieve communication among network security entities. For the messages communicated among network security entities.

(3) Share the detected network threat information among multiple entities of the same type. Complex network attacks are often composed of multiple atomic attacks, so the response requires collaboration of multiple components. When an entity detects a network threat or abnormal event, it can automatically send update or active messages to entities of its same type, which are also its physical and logical neighbors. And when the physical and logical neighbors receive such updates and active messages, they will continuously forward the information to entities of their own physical and logical neighbors, and the like. Eventually, each entity can receive all the updates and active messages sent by its surrounding physical and logical neighbors, and can conduct data fusion for the received messages, which will be further resent to surrounding physical and logical neighbors again automatically. This can help achieve information iteration and re-convergence. If the level of concern in the active message exceeds the set threshold, it will trigger the information transmission with different types of network security entities, i.e. go to Step (4).
(4) Transfer and share network threat information among multiple entities of different types. Complex network attacks often involve multiple network security entities, such as terminals, servers, network gateways, and network security perception platforms. When the level of concern of a certain entity in a certain type exceeds the set threshold, it will automatically send messages to other types of entities. For example, information can be shared among terminals, servers, networks, gateways, and network security perception platforms by this method. Then, go to Step (5).
(5) The network security perception platform generates collaborative response security policies. As the control center of the entire network information system, the network security perception platform formulates and generates polices related to network security by comprehensively analyzing the information reported by various security entities. In order to effectively tackle the network threats initiated by attackers, especially some complex attack threats, it is necessary to issue corresponding defense strategies to multiple entities in order to block or cope with network attacks.
(6) Response strategies and collaboration for multiple entities of a same type to dispose network threat. For example, if a certain server is infected with a worm, the corresponding strategy for the same type of entities to take to achieve collaborative defense is: first, isolate the server infected with the worm virus and disconnect itself from the network; then, disconnect the infected server from other servers; after that, use relevant security software to kill the worm virus on the server; finally, install patches on servers deployed around the infected server in the network to fix vulnerabilities and close relevant network ports.
(7) Response strategies and collaboration for multiple different types of entities to dispose network threat. In the case that a certain server is infected with a worm, the corresponding strategy to be taken by different types of entities to achieve collaborative defense is: first, filter the traffic generated by the worm propagation in the network and host by firewalls at all levels; second, set corresponding access control

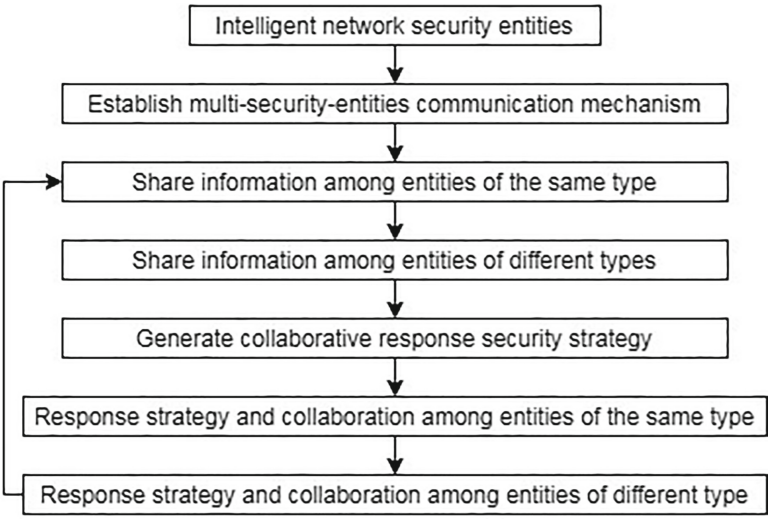

Fig. 1. Collaborative Process of Multiple Security Components based on Swarm Intelligence

policies on switches, routers, and firewalls to isolate the infected host from the network; finally, feedback the characteristics of the worm attack to intrusion detection devices and application firewalls, etc. After completing Step (7), it needs to return to Step (3) to continuously iterate and share the information and response collaboration among network security entities, as shown in Fig. 1. In actual application deployment, it is necessary to design more complete and compatible communication protocols, neighborhood policies, and rank functions according to the actual network security data and security defense systems.

5 Conclusion

In this paper, the complex multi-step network attack is simulated to conduct relative experiments to verify the joint sensing technology and collaborative response technology. Details are shown as follows:

5.1 Verification of Joint Sensing Technology

The attack simulation tool is used to simulate complex network attack in the established simulation environment, mainly including 3 types of complex network attacks: (1) suspected behaviors that can be observed on multiple security components but have no high risk nature; (2) suspected behaviors that can be observed by a same security component at multiple time points but have no high risk nature; (3) attack type having the nature of the above two types.

The data access and sharing technology is applied to store, parse, restrict, and distributively share the security information collected by multiple security components

within a period of time. And the swarm intelligence security analysis engine is taken to conduct spatiotemporal correlation security analysis, and verify if the analysis result conforms to the actual network attack or not.

5.2 Verification of Collaborative Response Technology

First of all, the network security analysis result is input into the response strategy generating module to obtain the optimal response strategy; secondly, the control module generates dispatching command according to the response strategy, and distributes to all relating security components; finally, all security components operate according to the commands, so to observe if the complex network attack is fully blocked or not.

This paper proposes a collaborative defense of network security based on Swarm intelligence Framework. This technology is based on collaborative detection and collaborative response, but Swarm intelligence technology is not yet mature. The design of communication messages needs to carry out various experiments according to different network attack characteristics, and in-depth research is required to form practical and scalable technical achievements.

References

1. WOLD S, ESBENSSEN K, GELADL P. Principal Component Analysis [J]. Chemometrics & Intelligent Laboratory System, 1987, 2(1): 37–52
2. YAN Qiao, YU FR, GONG Qingxiang, et al. Software-defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Sur-vey, Some Research Issues, and Challenges[J] IEEE Communications Surveys$ Tutorials, 2015, 18(1): 602–622.
3. SAHAY R, BLANC G, ZHANG Zonghua, et al. Towards Autonomic DDoS Mitigation Using Software Defined Networking [EB/OL]. https://hal.archives-ouvertes.fr/hal-01257899, 2019-9-10.
4. BRAGA R, MOTA E, PASSITO A. Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow [C]// IEEE. IEEE Local Computer Network Conference, October 10–14, 2010, Denver, CO, USA. NewJersey: IEEE, 2010: 408–415.
5. SYLVESTER EV A, BENTZEN P, BR ADBU RYIR, et al. Applications of Random Forest Feature Selection for Fine-Scale Genetic Population Assignment Evolutionary Applications, 2018, 11(2): 153–165
6. HART PE. The Condensed Nearest Neighbor Rule [U]. IEEE Transactions on Information Processing Systems, 2018, 31(3): 6638–6648.
7. JORDAN M I, BISHOP C. Neural Networks [J]. ACM Computing Surveys, 1996, 28(1): 73–75.