World Scientific Research Journal Volume 9 Issue 3, 2023
ISSN: 2472-3703 DOI: 10.6911/WSRJ.202303_9(3).0017

Current Status of Collaborative Intrusion Detection Research

Jianyang Deng[1, a, *], Yijia Lin[2, b]

[1]Bloco China Sociedade Unipessoal Limitada, Macao, China

[2]Faculty of Finance, City University of Macau, Macao, China

[a]ryan.y.deng@gmail.com, [b]F19090107186@cityu.mo

Abstract

The paper discusses the advantages of Collaborative Intrusion Detection Systems (CIDS) in detecting distributed cooperative attacks and dealing with large-scale network intrusions. The main research topic is how to improve detection performance while achieving decentralization. Recent research achievements in CIDS are reviewed, focusing on detection methods, data aggregation and trust management. The challenges of decentralization are analyzed, and the future development direction of CIDS based on blockchain technology is discussed. Finally, the paper looks forward to the potential applications of CIDS in emerging fields such as cloud computing and the Internet of Things.

Keywords

Intrusion detection; Collaborative intrusion detection; Deep learning; Federal learning; Blockchain technology.

1. INTRODUCTION

The rapid advancement of technology has fundamentally transformed various aspects of people's lives, including microgrid [1], Internet of Things [2], and enhanced power systems [3]. In addition, computer science and technology have emerged as a key development trend and a prevailing force in modern society [4]. Notably, Artificial Intelligence (AI), a burgeoning field within computer science, is dedicated to developing intelligent machines that can mimic human thinking and behavior [5]. While bringing many conveniences to people's lives, network security incidents also emerge in endless streams, and the network security situation is becoming increasingly severe. In terms of cloud platform security, the proportion of various network security incidents that occur on China's cloud platform is still high. In terms of industrial control system security, systems with high-risk vulnerabilities involve key industries such as coal, oil, electricity, and urban rail transit, covering enterprise production management, enterprise operation management, government supervision, and industrial cloud platforms.

Intrusion detection technology, that is, intrusion detection system, is a dynamic security technology that monitors and analyzes system activity, analyzes and extracts intrusion behavior characteristics, and responds to intrusion behavior in real time. It usually includes monitoring system behavior, auditing system faults and structures, analyzing and monitoring intrusion behavior and issuing alarms, statistical analysis of abnormal behavior, evaluating system and data integrity, and other functions.

In 1998, the Common Intrusion Detection Framework Architecture (CIDF) working group proposed an intrusion detection framework, dividing the intrusion detection system into four components: event generator, event analyzer, event database, and response unit.

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202303_9(3).0017

2. THE CONCEPT OF COLLABORATIVE INTRUSION DETECTION

Collaboration refers to the process or ability of two or more individuals to achieve the same goal. In IDS, collaboration can be understood as the ability of multiple detection components to work together to complete intrusion detection tasks, which can be collaborative on data collection or data processing. The concept of collaboration was introduced into IDS to improve the overall detection rate through multi-source data collection and multi-party collaborative processing.

The concept of CIDS was first proposed by Wu et al. [6], who implemented an efficient distributed intrusion detection system by setting up three data collectors that can collect data from different sources and one data processor. Since then, research on CIDS has shown an upward trend year by year. Essentially, CIDS belongs to a type of DIDS. Currently, scholars generally define CIDS as a comprehensive intrusion detection system in which two or more independent detection entities with certain independent detection capabilities work together through collaborative work in data collection, detection analysis, and alert response to achieve intrusion detection objectives.

3. CURRENT RESEARCH STATUS OF COLLABORATIVE INTRUSION DETECTION

Since its birth, CIDS has the inherent advantage of decentralization compared with traditional IDS and is the future direction of IDS development. This chapter will focus on the current research status of CIDS detection methods, data aggregation, and trust management mechanisms.

3.1. Detection methods

In early IDS, the module responsible for detection completed the detection and classification of data by matching predefined rules and policies. The built-in rules were inflexible, had low detection accuracy, a long optimization process, and slow growth rates. This method is no longer suitable for the current complex network environment. In recent years, the flourishing development of artificial intelligence technology has promoted the combination of intrusion detection technology research and machine learning algorithms, which has changed the limitation of manually extracting features and enabled nodes to detect complex attacks. Machine learning-based intrusion detection methods are currently a mainstream research direction. In the field of collaborative intrusion detection, independent nodes that use machine learning algorithms to detect attacks can share information to perform more complex operations. Servin et al. [7] proposed a Multi-Agent CIDS based on reinforcement learning, which uses Q-Learning algorithm to achieve an intelligent detection system. Louati et al. [8] designed an intrusion detection model based on adaptive agents, which uses Autoencoder, Multilayer Perceptron, and K-Nearest Neighbor algorithms to implement a high-precision hybrid distributed CIDS.

3.2. Data aggregation

Compared with traditional IDS, the advantage of CIDS is that it can detect large-scale distributed and coordinated attacks, such as network scanning, worm viruses, and distributed denial-of-service attacks (DDoS). Through data sharing, CIDS can improve detection methods and increase intrusion detection accuracy, which involves the issue of data aggregation. Data aggregation refers to the process of detecting, analyzing, and correlating multiple sources of data to obtain more descriptive and meaningful results.

In CIDS, data aggregation refers to the method of collecting data from various distributed nodes and processing it through aggregation before analyzing attack behavior comprehensively.

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202303_9(3).0017

Through data aggregation, heterogeneous data from different detection methods and different IDS can be fused together to improve the system's detection accuracy, enhance system stability and reliability, and improve overall system performance. There are two main research directions based on different aggregation methods: centralized aggregation and alert correlation.

3.3. Trust management mechanisms

In peer-to-peer CIDS, the system is composed of a group of independent nodes with intrusion detection capabilities, and the system is able to detect advanced attacks by aggregating the alarm information of each node. Therefore, the system's detection capability relies on the information shared by the nodes, but due to the strong independence of the nodes, if there is a lack of system supervision, there may be internal attacks from malicious nodes. Malicious nodes can interfere with the normal operation of the intrusion detection system by sharing incorrect data.

An effective measure to prevent internal attacks in a distributed network is to establish a reputation system within the system. Under the reputation system, each node is supervised by the system and accumulates reputation value based on certain normal behavior rules. When a malicious node violates the rules, its reputation value will decrease. If the node's reputation value drops to a certain level, the system will consider the node untrustworthy and take certain measures to limit its participation in the collaborative network.

Khan et al. [9] proposed an intrusion detection model based on multi-agent and multi-level game algorithms. In this model, each node accumulates reputation by participating in communication. Nodes with low reputation are considered malicious and will be restricted from communication. This approach effectively prevents security risks within the network, improves intrusion detection accuracy, and increases network communication throughput through node competition. Gil Pérez et al. [10] proposed a reputation-based collaborative intrusion detection network that includes a Wise Committee (WC) in the system. The alarm information from each node must be evaluated and approved by the WC before it can be released, thus avoiding the impact of malicious alarms. The members of the WC rely on their interaction history with other nodes to evaluate their trustworthiness. Similarly, Ganesh et al. [11] introduced a reputation mechanism (CORE) in the nodes to ensure the trustworthiness of communication nodes by evaluating them through neighboring nodes. This approach has achieved a trustworthy collaborative intrusion detection system.

4. CONCLUSION

Collaborative intrusion detection plays an important role in current network security defense. This article analyzes the research status of CIDS from the aspects of detection methods, data aggregation, and trust management, and points out the existing problems, especially the great challenge faced in achieving complete decentralization. The emergence of blockchain technology provides a possible solution to these problems, as its tamper-proof, traceable, publicly transparent, secure, fault-tolerant, and non-repudiable properties can address the data aggregation and trust management issues in CIDS, laying the foundation for achieving complete decentralization. However, introducing blockchain technology may also bring new problems, such as additional communication and storage overheads and delays in blockchain validation, which need to be urgently addressed by researchers.

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202303_9(3).0017

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my family for their patience and support throughout the writing of this paper. Moreover, I would like to thank my friends and colleagues for their valuable feedback and suggestions.

REFERENCES

[1] J. Deng, C. -S. Lam, M. -C. Wong, S. -W. Sin and R. Paulo Martins "Instantaneous power quality indices detection under frequency deviated environment." IET Science, Measurement & Technology 13.8 (2019), pp. 1111-1121

[2] J. Deng, C. -S. Lam, M. -C. Wong, L. Wang, S. -W. Sin and R. Paulo Martins, "A Power Quality Indexes Measurement System Platform with Remote Alarm Notification," IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, 2018, pp. 3461-3465

[3] L. Wang, Y. Pang, C. -S. Lam, J. -Y. Deng and M. -C. Wong, "Design and Analysis of Single-Phase Adaptive Passive Part Coupling Hybrid Active Power Filter (HAPF)," IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, 2018, pp. 3615-3620

[4] Jianyang Deng. (2022) Modern Application of Computer Science and Technology. Advances in Computer and Communication, 3(2), 86-90.

[5] Deng, J., & Lin, Y. (2022). The benefits and challenges of ChatGPT: An overview. Frontiers in Computing and Intelligent Systems, 2(2), 81-83.

[6] Wu Y S, Foo B, Mei Y G, et al. Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS [C]// Proc of Computer Security Applications Conference. Piscataway, NJ: IEEE, 2003.

[7] Servin A, Kudenko D. Multi-Agent Reinforcement Learning for Intrusion Detection [C]// Proc of the 6th German Conference on Multiagent System Technologies. Berlin: Springer, 2008: 211–223.

[8] Louati F, Ktata F B. A Deep Learning-Based Multi-Agent system for intrusion detection [J]. SN Applied Sciences, 2020, 2 (4): 675-688.

[9] Khan B U I, Anwar F, Olanrewaju R F, et al. A novel Multi-Agent and multilayered game formulation for intrusion detection in Internet of Things (IoT) [J]. IEEE Access, 2020, 8: 98481–98490.

[10] Pérez M G, Mármol F G, Pérez G M, et al. RepCIDN: A Reputation- Based collaborative intrusion detection network to lessen the impact of malicious alarms [J]. Journal of Network and Systems Management, 2013, 21 (1): 128–167.

[11] Ganesh S S, Somasundaram K. A collaborative intrusion detection system for cognitive radio networks with trust and reputation management [J]. International Journal of Recent Technology and Engineering, 2019, 8 (2): 4489–4498.