Exploration of Key Technologies for Network Security Monitoring Based on Distributed Artificial Intelligence

Qu Hongfeng[1], Xuan Yang[1,*], and Sun Shuo[2]

[1] Guangxi Vocational & Technical College, Nanning, Guangxi, 5302262, China
[2] Dalian Jiaotong University, Dalian, Liaoning, 116028, China
Email: 784701970@qq.com (X.Y.)
*Corresponding author
Manuscript received May 14, 2025; accepted August 4, 2025; published October 24, 2025.

***Abstract*—In order to explore the key technology of network security monitoring based on distributed artificial intelligence, the method of combining theory with practice is adopted, based on the relevant overview of distributed artificial intelligence, the application of distributed artificial intelligence in network security monitoring is analyzed, and the application effect is discussed with the practical cases. The analysis results show that the network security monitoring technology based on distributed artificial intelligence can accurately monitor complex network security attacks through distributed architecture, multi-source data integration, real-time monitoring, and collaborative work, etc. The monitoring results can provide necessary references and guidance for the solution and treatment of security risks, so as to improve the level of network security protection.**

***Keywords*—distributed artificial intelligence, network security monitoring, system architecture, distributed data acquisition**

I. Introduction

Under the environment of cloud computing, Internet of Things (IoT) and 5G technology's rapid development, cyber-attacks are characterized by distribution, intelligence and concealment, resulting in network security facing unprecedented severe challenges. Traditional centralized network security monitoring means in dealing with large-scale, distributed network attacks, there are limited data processing capacity, slow response speed, difficult to adapt to dynamic changes in the network environment and other issues. Distributed artificial intelligence, as an emerging technology paradigm, can provide new solutions for network security monitoring. Reasonable application of distributed AI technology in network security monitoring can distribute the intelligent perception, learning and decision-making capabilities of AI to each node of the network, realizing real-time monitoring, rapid response and efficient processing of network security threats, thus enhancing the security of the network environment, which is worthy of wide-scale promotion and application.

II. An Overview of Distributed Artificial Intelligence

Distributed AI is an important branch in the field of artificial intelligence, which can be regarded as a more advanced AI technology, and compared with AI, distributed AI mainly researches the use of collaboration and interaction between multiple intelligences to complete complex AI tasks under a distributed computing environment (the work process of the intelligent body is shown in Fig. 1).

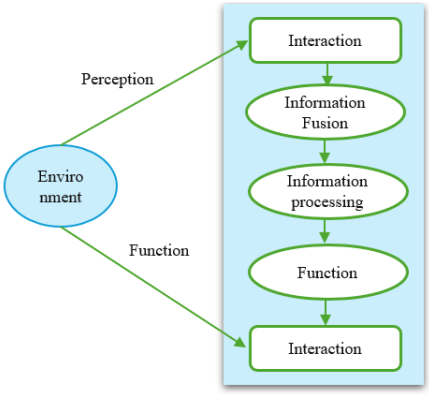

Fig. 1. Working process of the intelligent subject.

In a networked environment intelligences may be distributed on different nodes, communicating and sharing information through the network, thus solving problems that are difficult for a single intelligence to handle. It has the following characteristics:

A. Distributability

Intelligents in a computer network environment are distributed over multiple physical locations or computing nodes, e.g., for a cloud-based distributed AI system, the intelligents can be distributed over different servers or edge devices. And each intelligence has its unique local sensing and processing capabilities, working in parallel with each other, and is not concentrated in a centralized processor.

B. Collaboration

Each intelligent body needs to collaborate with each other to complete the task, and such collaboration can be simple task allocation or complex joint decision-making. In a scenario where multiple robots collaborate to accomplish a complex task, the robot intelligences have to negotiate their respective action paths, task division, etc., through communication to ensure the efficient completion of the entire task.

C. Autonomy

Each intelligent body has the ability to make autonomous decisions, and can make decisions based on its own goals, knowledge and local environment without global control. For example, if distributed artificial intelligence is applied to network security monitoring, each intelligent body can adjust the relevant parameters autonomously according to the operational characteristics of the network and the security problems it faces, and collaborate with other intelligent bodies to realize real-time monitoring of network security.

III. Distributed Artificial Intelligence in Cybersecurity Monitoring

A. System Architecture

Distributed AI-based network security monitoring system usually adopts a layered architecture. The schematic diagram of the specific structure is shown in Fig. 2.

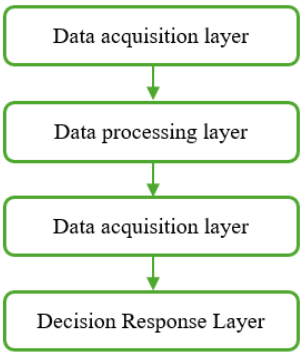

Fig. 2. Schematic diagram of layered architecture of distributed AI-based network security monitoring system.

1) Data acquisition layer

The main role of the data collection layer is to collect raw data from the network, including network traffic, logs, and anomalous behavior. Tools such as distributed sensors like Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems are utilized to comprehensively collect data from every node on the network. Network traffic data includes all the data going in and out of the network, such as source IP address, destination IP address, port number, protocol type, and so on. Log data, on the other hand, records information about the operational status of network devices (e.g., routers, servers, etc.), user login activities, and so on. Abnormal behavior data are those that deviate from normal network activity patterns, such as a sudden large number of external connection attempts or abnormal logins by a particular user during non-working hours. Through extensive collection of these data, it can provide basic data for subsequent network security analysis.

2) Data processing layer

Reduce data transmission overhead by utilizing edge computing and federated learning for local data analysis. The data collected at the data collection layer can be used by edge computing to complete the initial processing close to the data source. Thus, a large amount of raw data is avoided to be directly transmitted to the central server, reducing the data transmission overhead. Federated learning, on the other hand, belongs to a machine learning technique that allows different local devices to jointly train models without sharing raw data, and to utilize data from each device for more effective analysis while protecting data privacy. Joint application of these two techniques allows for efficient preliminary processing of data locally, extracting valuable features and transferring key information to the intelligent analytics layer.

3) Intelligent Analytics Layer

Deep learning (e.g., LSTM, GNN) and Reinforcement Learning (RL) can be used in the Intelligent Analysis Layer for cybersecurity threat modeling in order to provide a more systematic and comprehensive analysis of cybersecurity.

LSTM is more suitable for processing data with time-series characteristics, and network traffic varies at different points in time, using LSTM techniques to capture long-term dependencies in the data in order to better identify potential threat patterns [1]. GNN is suitable for dealing with data related to network structure, where the network itself can be viewed as a graph structure, nodes represent devices in the network, and edges represent connections between devices.GNN can analyze the structure of the graph and node attributes to discover abnormal network connections or device behaviors. RL can be used to learn optimal strategies by letting intelligences learn through trial-and-error in the environment, which can be applied to cyber security to optimize defense strategies. Threat modeling can optimize defense strategies by dynamically adjusting resource allocation to deal with different types of threats.

4) Decision response layer

The decision response layer is the execution layer of the distributed artificial intelligence-based network security monitoring system, which can respond in time according to the results of the intelligent analysis layer. Common response methods include: dynamically adjusting firewall rules, blocking malicious IPs, or triggering emergency response. Dynamically adjust firewall rules. If it is found that an IP address frequently carries out malicious scanning, the access of the IP address can be blocked by modifying the firewall rules. Blocking malicious IP is a direct and effective defense measure to protect network security, which can prevent malicious attackers from further invading the network. Triggering an emergency response is a series of measures taken when a serious threat is detected, which can be done by notifying the security administrator, starting a backup system, or quarantining the infected network area, etc., in order to minimize the damage and protect the security of the network.

B. Key Technologies

1) Distributed data acquisition techniques

In order to realize the comprehensive collection of data affecting security in the network and give full play to the role and advantages of distributed artificial intelligence in network security monitoring, distributed sandbox technology can be applied to collect malicious code traffic during data collection. When applying distributed sandbox technology in the collection of malicious code traffic, each sandbox node can be organized in a distributed way, and the effective scheduling of tasks between nodes can be achieved through cross-node task scheduling to collect malicious code traffic, thus realizing the comprehensive collection of distributed malicious code traffic. Adopting this technique in network malicious code traffic collection can decentralize the data collection task to each node in the network, avoiding a single point of failure and improving the reliability and comprehensiveness of data collection [2]. For example, in a large data center network, distributed sandbox technology can be applied in each rack or server cluster for data collection, and the collected data can be sent to the central data aggregation node or directly transmitted to the distributed storage system.

2) Collaborative and federated learning techniques

The application adopts the federated learning algorithm, which can prompt each intelligent agent to train the model

locally using its own data, and then upload the model parameters to the central server for aggregation, and the central server will then distribute the updated global model parameters to each intelligent agent, so as to realize the updating and optimization of the model. The model training process for federated learning is shown in Fig. 3:

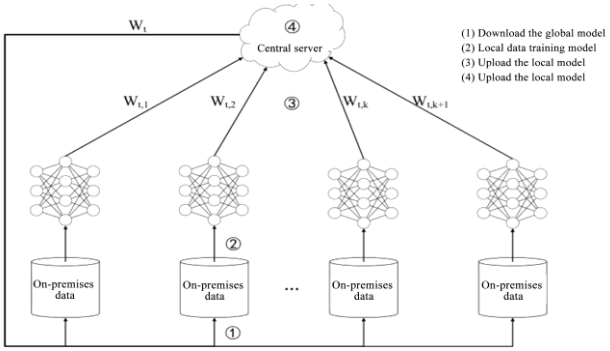

Fig. 3. Schematic diagram of the federal learning process.

In Fig. 3, $w_{t,k}$ represents the local model update of the kth client in the tth iteration, and w_t represents the global model update in the tth iteration. In the specific training, we need to assume that the current iteration round is t, and then iterate according to the following process.

As a first step, the client needs to establish a connection with the central server when the Federal Learning System is launched. To ensure the stability and reliability of the connection, a network-based protocol (e.g., TCP/IP) can be used for this purpose. After the connection is established the client sends a request to the central server indicating that it is ready to receive the global model after the last iteration and download the global model after the last completed iteration w_{t-1}.

In the second step, the client k can train the local dataset on w_{t-1} after receiving the global model w_{t-1}. The local dataset is a data resource specific to the client k, and the local dataset has unique distribution characteristics [3]. In order to ensure that the local dataset can be better adapted to w_{t-1}, it is also necessary to pre-process the data, through data cleaning (removing noise, outliers, etc.), data standardization (converting the eigenvalues of the data to specific intervals), etc., and then the pre-processed local dataset will be applied to the global model downloaded from the central server to be trained again, to obtain the local model $w_{t,k}$.

In the third step, each client sends the extracted local model updates to the central server, but it should be noted that advanced encryption techniques can be applied in the uploading process in order to protect the privacy and security of the data. Homomorphic encryption can be used to ensure that the central server can perform aggregation operations on the encrypted model updates without decryption.

In the fourth step, after the central server receives the model updates from each client, it also needs to weight and aggregate them according to the pre-set weights. The weights need to be determined based on a variety of factors, such as: the size of the client's dataset, the quality of the data, or the importance of the client in the whole federated learning system, etc. By weighting the clients with the weights and then performing the aggregation process, a new global model can be obtained w_t .

Step 5, continue steps 1 through 4 until the end of the training.

Federated learning solves the data privacy and security problems in traditional centralized machine learning through distributed training and privacy protection mechanisms. Its core process includes model downloading, local training, update uploading, aggregation updating and iterative training, and the reasonable application of this approach in network security monitoring can make full use of the data resources of each node in the network to improve the accuracy and generalization ability of the model under the premise of protecting data privacy [4]. For example, in network security monitoring, the network traffic data collected by different intelligent agents may have different feature distributions, and through federated learning, the local models of each agent can be integrated to obtain a global model applicable to the entire network environment.

3) Adaptive defense strategies

In order to give full play to the advantages of distributed artificial intelligence in network security monitoring, it is also necessary to strengthen the application of reinforcement learning based on MITRE's CALDERA framework, so as to be able to automatically adjust the defense strategy to deal with APT attacks to better protect network security. CALDERA is an open-source automated adversarial simulation platform developed by MITRE that can simulate real attack scenarios to enable network security monitoring to more comprehensively understand and master attacker behavior and techniques, thereby improving its detection and response capabilities. Reinforcement learning, on the other hand, is a machine learning method that learns optimal strategies through the interaction of intelligences with their environment. Reinforcement learning in the CALDERA framework enables automatic adjustment of defense strategies, and the specific implementation process is as follows:

The first step is state representation. The network security state is represented as a state in reinforcement learning, including network topology, device status, user behavior and other information. This state information can be collected by distributed sensors and transmitted to a central server for processing.

The second step is action selection. Define a series of defense actions, such as adjusting firewall rules, blocking malicious IPs, triggering emergency response, etc., and through reinforcement learning intelligences can select the best defense actions according to the current network security state [5].

Step 3, reward design. Design a reasonable reward mechanism to guide the intelligent body to learn the best defense strategy. For example, if APT attacks are successfully detected and blocked, positive rewards are given to the intelligent body; when a security event occurs, negative rewards are given.

Step 4, strategy optimization. Intelligent bodies can learn the best defense strategy by continuously interacting with the environment. In the process of adaptive prevention strategy optimization, the intelligent body can adjust its behavior according to the reward feedback and gradually optimize the defense strategy.

IV. Experiments and Case Studies

A. Experimental Design

A large enterprise campus network security monitoring project, the campus network has thousands of terminal devices, multiple server clusters and complex network applications. Before 2022, network security monitoring was mainly Snort (rule-based) + SVM (machine learning), but with the expansion of the network scale and the increasing complexity of the attack means, the traditional way is difficult to effectively respond. With the introduction of a distributed AI-based network security monitoring system after 2024, intelligent agents are deployed on each core switch, server cluster and some key end devices in the campus network. Intelligent agents collect network traffic data, system log data, and application program operation data through multi-source data collection techniques.

B. Experimental Process

The collected network traffic data, system log data and application operation data are cleaned, standardized and feature extracted. Especially for network traffic data, it is required to extract traffic statistics features and connection features, while for system log data, it is required to extract features such as event types and related user information. After the collected data processing is completed, the collaborative learning and decision-making mechanism between federated learning + LSTM, Multi-Intelligence Reinforcement Learning (MARL), etc. is used for network security monitoring. The federated learning algorithm is used to train the anomaly detection model, and each intelligent agent uses the local data to train the local model, and then the model parameters are uploaded to the central server for aggregation, and the global model is obtained and then distributed to each agent. In actual operation, if an intelligent agent detects anomalous traffic in the local network, it can automatically generate a security policy and send it down to the execution node based on the local processing results and decision-making suggestions from other agents and the center node ([6].). For example, when an IP address is detected as suspected of launching a DDoS attack, the intelligent agent will automatically generate a policy to block access to that IP address and send it down to the firewall for execution. The security policy enforcement node, in turn, will feedback the execution to the intelligent agent, which evaluates and optimizes the policy based on the feedback information.

C. Experimental Results

After 14 months of operation, the network security status of the enterprise campus network has been significantly improved. Compared with the traditional network security monitoring methods, the detection rate, false alarm rate and response speed of the distributed AI-based network security monitoring system for unknown attacks have been significantly improved, and the specific experimental results are shown in Table 1:

Table 1. Results of distributed AI-based network security monitoring applications

Norm	Snort	SVM	DAI (LSTM+FL)	DAI (MARL)
Detection rate (%)	85.2	89.7	96.3	98.1
False alarm rate (%)	12.5	8.9	3.2	2.1
Response time (ms)	120	95	45	30

V. Conclusion

In summary, combined with theoretical practice, the key technology of network security monitoring based on distributed artificial intelligence is explored, and the exploration results show that network security monitoring has strong complexity and is relatively difficult, and the traditional Snort (rule-based) + SVM (machine learning) network security monitoring technology has certain limitations in terms of the detection rate, false alarm rate, response time, etc., which makes it difficult to effectively respond to modern complex network security threats. The distributed AI application federated learning + LSTM, multi-intelligent body reinforcement learning (MARL) approach can decentralize the computation and data processing to multiple nodes, which can effectively respond to security threats in large-scale network environments. And it can also fully integrate data from different sources (e.g., network traffic, log files, user behaviors, etc.), enabling more comprehensive identification of potential threats. And its superiority is verified through experiments and case studies. Distributed AI not only improves the accuracy of threat detection, but also realizes adaptive defense, which can provide new solutions for future network security, and deserves to be widely promoted and applied in network security monitoring, so as to help the healthy and stable development of China's network industry.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Qu conceived and designed the research framework, drafted the initial version of the manuscript; Xuan revised the manuscript critically for important intellectual content; Sun compiled the literature review and discussion sections; all authors participated in the discussion of the research findings, provided comments on the manuscript; all authors had approved the final version.

References

[1] X. Flood, "Design of Kolla-based artificial intelligence and big data teaching experiment platform," *Software*, vol. 44, no. 02, pp. 119–122, 2023.

[2] W. G. Yu, Z. H. Yuan, J. Q. Chen *et al.*, "Distributed subspace locally linked random vector function link networks," *Journal of Shenzhen University (Science and Technology)*, vol. 39, no. 06, pp. 675–683, 2022.

[3] L. Huo, Y. H. Zhang, X. Chen, "Application of artificial intelligence in distributed energy storage technology," *Power Generation Technology*, vol. 43, no. 05, pp. 707–717, 2022.

[4] X. J. Zhao and Y. Chen, "Distributed training communication optimization strategy for artificial intelligence IoT," *Journal of Xi'an College of Arts and Sciences (Natural Science Edition)*, vol. 25, no. 04, pp. 27–31, 2022.

[5] D. Z. Meng, "Distributed systems and artificial intelligence in meta-universe finance," *China Business Journal*, vol. 14, pp. 80–82, 2022.
[6] L. F. Ding and G. F. Yan, "A review of security issues and defense mechanisms for multi-intelligent systems," *Journal of Intelligent Systems*, vol. 15, no. 03, pp. 425–434, 2020.