International Journal of Computer Applications Technology and Research
Volume 15–Issue 02, 01 – 06, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1502.1001

Research on Multi-threaded Visualized Network Scan Sensing Method Based on TCP/IP Protocol Stack

Xin Feng
College of Communication Engineering,
Chengdu University of Information Technology,
Chengdu, China
fengxin0312@qq.com

Jianhua Zheng*
Key Laboratory of Knowledge Mining and Knowledge Services in Agricultural Converging Publishing, Agricultural Information Institute, Chinese Academy of Agricultural Sciences, Beijing 100081, China
zhengjianhua@caas.cn

Wenzao Li
College of Communication Engineering,
Chengdu University of Information Technology,
Chengdu, China

Bing Wan
School of Software, Chengdu Polytechnic, Chengdu 610225, China

Renhan Peng
College of Communication Engineering,
Chengdu University of Information Technology,
Chengdu, China

Abstract: Network scan sensing is a primary means to counteract cyber attacks. To this end, this paper focuses on the IP addressing and routing forwarding mechanism at the network layer, the TCP/UDP port status detection logic at the transport layer, and the service interaction protocol characteristics at the application layer within the TCP/IP protocol stack. It proposes and implements a low-cost, multi-threaded software scan sensing method with visualized results. This method integrates multi-source data analysis strategies including IP address traceability and target port access characteristics, and achieves accurate perception of port scanning behaviors through a dynamic threshold model and multi-dimensional risk assessment rules. Based on the perception of a certain range of ports in a specific region by this method from the 26th to the 28th, data analysis shows that under the preset abnormal judgment rules, abnormal scans account for 18.4%-19.1% of the total scan volume. The period from 22:00 to 24:00 every day is the peak period, with attacks concentrated on ports such as 443/TCP, 80/TCP, and 53/UDP, and attack sources showing geographical aggregation characteristics. From the above results, it can be concluded that port scanning behaviors have the common characteristics of concentration in time, ports, and attack sources.

Keywords: Network Port Scanning, Multi-feature Fusion, Real-time Detection, Data Visualization, Dynamic Threshold, Geographic Identification

1. INTRODUCTION

1.1 Background and motivation

With the deep integration of big data and Internet of Things(IoT) technologies, cyber attack methods have shown a trend of being stealthy and large-scale. As a pre-detection link of cyber attacks, port scanning has become a core means for hackers to locate method vulnerabilities and launch targeted intrusions [1]. According to the report of the State Grid Cyber Security Monitoring Center (SGCSMC), the annual growth rate of cyber security incidents caused by exposed high-risk ports reached 42% from 2023 to 2025 [2]. However, most traditional tools only have scanning capabilities, making it difficult to cope with the real-time processing of massive scanning data and multi-dimensional feature mining.

The aim of this paper is to develop a port scanning monitoring method integrating dynamic traffic threshold detection, multi-threaded detection and precise geographic identification. By conducting visual analysis of scanning data from November 26 to 28, 2025, this paper explores the core information such as temporal patterns, geographical distribution and port characteristics of attack behaviors. Based on dynamic traffic threshold detection, the method combines multi-threaded technology to improve port detection efficiency, and integrates multiple IP geographic interfaces to achieve precise geographic positioning, ultimately providing targeted decision support for cyber security protection [3].

1.2 Limitations of prior work

At present, there exist various port scanning tools and detection methods, but all of them have specific limitations. For example, Nmap, a mainstream scanning tool, can realize port detection, service identification and version detection, but it only focuses on port status collection, lacks the ability of intelligent judgment of malicious scanning, and cannot distinguish between normal detection and malicious attack behaviors. Its output results are in plain text format, lacking multi-dimensional visual analysis functions, making it difficult for users to quickly extract core attack features. The detection method based on fixed traffic threshold only judges maliciousness through a single indicator of port access frequency, without combining key features such as IP region and active time period, resulting in weak ability to identify

slow scanning and distributed scanning. Security personnel need to manually process various data to discover security risks and form evaluation reports, and conduct data matching and classification notification on a quarterly basis, which is time-consuming and labor-intensive [4].

In contrast, the multi-dimensional fusion monitoring method proposed in this paper can not only realize the full collection of port scanning behaviors, but also realize the intelligent identification of malicious scanning through dynamic traffic threshold, accurate IP geographic identification and multi-feature weighted judgment. For example, it can accurately distinguish between malicious and normal traffic by combining multi-dimensional features such as scanning frequency, geographic attributes and active time periods; it can intuitively present the time distribution, geographic origin and port characteristics of attacks through visual charts; it provides network security managers with full-process support of "detection-judgment-statistics-visualization", helping them quickly formulate defense strategies.

1.3 Challenges and solution

The application of multi-dimensional integrated technology in port scan monitoring faces various challenges. Firstly, there is the adaptability issue of traffic threshold detection. Fixed thresholds are difficult to cope with scan behaviors in different network environments, making them prone to false positives or false negatives. Secondly, there is the efficiency issue of multi-protocol port detection. The detection mechanisms of TCP and UDP ports are inherently different, and single-threaded processing is difficult to balance comprehensiveness and real-time performance of detection. large-scale port detection tasks may lead to response delays in the implementation of the method. Finally, there is the issue of standardized acquisition of geographical information. The return formats of different IP geographic interfaces are inconsistent, and information such as country codes and region names lacks unified identification, affecting subsequent geographical distribution analysis.

To address the above challenges, this paper proposes corresponding solutions: adopt a dynamic traffic threshold mechanism, adjust threshold parameters according to real-time network traffic, and improve detection adaptability; use multi-threaded technology to realize parallel detection of TCP and UDP ports, and allocate detection tasks through thread pool management to improve the efficiency of large-scale port detection [5]; integrate multiple geographic information interfaces such as Taobao IP and ipinfo, establish a priority call mechanism, standardize the returned results, uniformly output information such as country codes and region names, and ensure the accuracy of geographic identification [6].

1.4 Contributions and organization

In this paper, a port scanning monitoring method model integrating traffic threshold detection, multi-threaded port collection and precise geographic identification is proposed. The aim of this paper is to comprehensively collect data such as traffic data, source IP and target ports of port scanning behaviors, calculate detection thresholds through dynamic traffic threshold formulas, and identify high-frequency scanning behaviors [7]. Based on this logic, this paper expands the method functions, conducts multi-dimensional analysis of the time distribution, geographic attribution and port types of scanning data, and evaluates the risk level of attack behaviors by calculating multi-dimensional risk scores.

(1).Improving Improving the adaptability and accuracy of traffic threshold detection: Traditional port monitoring methods mostly adopt fixed traffic thresholds, which are difficult to adapt to different network environments. The proposed method effectively reduces the probability of false positives and false negatives by adjusting detection parameters based on real-time traffic through a dynamic traffic threshold mechanism.

(2).Realizing full collection and correlation analysis of multi-dimensional data: Traditional monitoring methods mostly focus on single-dimensional information collection. The proposed method integrates multi-dimensional data such as traffic, ports, and geography, and reveals the potential patterns of attack behaviors through correlation analysis, providing a more comprehensive basis for the formulation of defense strategies.

(3).Provide a cyber security defense tool: The method provides network security managers with a dynamically adaptive monitoring tool implemented based on Python [8], enabling them to formulate more effective defense strategies according to current information and improve the level of cyber security protection.

The subsequent structure of the paper is organized as follows: Section 2 provides a review of related work, while Section 3 elaborates on the proposed method in detail. Section 4 presents the implementation process of core technologies through formulas and logical derivation. For specific details regarding the solutions and their validation, refer to Section 5.

2. RELATED WORK

2.1 Research on port scan detection

Port scan detection technology is a core component of network security protection, with the primary goal of quickly identifying abnormal scanning behaviors, distinguishing between legitimate access and malicious attacks, and providing a basis for subsequent defensive responses. Existing detection technologies are mostly optimized for specific scenarios or based on single-index judgment, exhibiting significant limitations in adaptability and comprehensive analysis.

The traffic threshold-based detection method is currently the most widely used technical approach. The traffic threshold detection method proposed by Wang Longye et al. can quickly identify high-frequency scanning behaviors within a short period due to its simple principle and easy deployment [11]. However, fixed thresholds struggle to adapt to dynamically changing network environments: false positives are likely to occur during enterprise business peak hours, while attackers can easily evade thresholds through slow scanning, distributed scanning, and other strategies, leading to missed detections. Additionally, relying solely on access frequency as the only indicator fails to fully characterize the malicious nature of scanning behaviors.

To address the specific needs of high-speed network environments, Wu et al. designed a slow scan attack detection algorithm based on the Sketch data structure, enabling efficient analysis of massive high-speed traffic through lightweight data processing [9]. Nevertheless, this algorithm relies on specific hardware acceleration modules and complex network topology adaptation, resulting in high hardware costs

and operational difficulties. It is difficult to promote on a large scale in general environments such as small and medium-sized enterprise networks and edge computing nodes. Moreover, its functional coverage is limited to slow scanning in high-speed scenarios, failing to address diverse attack forms such as multi-protocol collaborative scanning.

2.2 Research on geographical information fusion

The core application of geographical information fusion technology in the field of network security is to parse the geographical attributes (country, region, city, etc.) corresponding to IP addresses, providing a basis for attack source tracing and risk grading, and serving as an important support for improving the accuracy of port scan monitoring. Existing geographical information acquisition and application schemes have obvious deficiencies in data standardization, accuracy, and deep integration [10].

Current mainstream IP geographical information acquisition relies on third-party interfaces, but the return formats of different interfaces lack a unified standard: some interfaces return core fields such as country codes and region names, while others only provide vague geographical descriptions. Inconsistent field naming rules and data formats require additional data cleaning and format conversion for subsequent geographical distribution analysis,increasing the complexity of the method's implementation. Meanwhile, single interfaces have limitations in coverage: domestic interfaces have low accuracy in parsing overseas IPs, while overseas interfaces struggle to accurately identify domestic sub-regions. The lack of effective fault-tolerance mechanisms when interface calls fail also affects the reliability of geographical information acquisition.

Existing research utilizes geographical information to a relatively low extent. Most schemes only use it as auxiliary display data and do not deeply integrate it with core features such as scanning frequency and active time periods. As an important dimension for assessing attack source risks, the correlation analysis between geographical information and other features can significantly improve the accuracy of malicious attack judgment. However, existing schemes fail to give full play to this role. Furthermore, some schemes lack standardized processing of geographical information, resulting in chaotic naming formats for different regions, which prevents statistical analysis and visual display of geographical distribution, limiting its application value in defensive decision-making.

3. SOFTWARE-BASED SCAN MONITORING SCHEME

In this paper, a port scanning monitoring method integrating dynamic traffic threshold detection, multi-threaded port collection, and precise geographic identification is designed. The aim of this paper is to construct a full-process closed-loop monitoring method of "data collection - suspected marking - risk assessment - visualization display".This paper comprehensively collects key information such as traffic data, source IPs, target ports, and access timestamps of port scanning behaviors, realizing accurate identification of high-frequency scanning behaviors and scientific assessment of attack risks, so as to provide efficient and implementable technical support for network security management.

The method is supported by multi-threaded technology to ensure the efficiency and stability of large-scale port monitoring: through the multi-threaded port collection module, it parallel processes TCP/UDP protocol data, synchronously collects core basic information of scanning behaviors, avoids efficiency bottlenecks caused by single-threaded processing, and adapts to the demand of large-scale port scanning data collection in complex network environments. Meanwhile, it integrates a precise geographic identification module, calling multi-interface IP geolocation services such as ip.cn, Taobao IP, and ipinfo. Through a multi-interface fault-tolerance mechanism and data caching strategy, it obtains geographic attributes such as the country, region, and city of the attack source, ensuring the accuracy and acquisition efficiency of geographic information and providing basic data support for subsequent multi-dimensional risk assessment.

The core operational logic of the method follows a closed-loop process: first, complete basic data collection and geographic attribute parsing through the multi-threaded collection module; second, dynamically determine detection criteria based on recent network traffic characteristics and screen out suspected attack sources through specific calculation rules; then, quantify the attack risk level through multi-dimensional risk assessment rules; finally, draw time distribution line charts, geographic distribution pie charts, and port characteristic bar charts through visualization technology to intuitively present core features such as attack peak periods, high-risk geographic regions, and high-frequency attack ports. The entire method realizes full-process automated processing from data collection to risk interpretation, which not only adapts to dynamically changing network environments but also provides clear and intuitive attack situation references for security managers, helping them quickly grasp the attack status and risk characteristics of port scanning.

4. MULTI-DIMENSIONAL RISK CALCULATION METHOD

This section will detail the calculation rules of the dynamic traffic threshold and the design details of the weighted summation of multi-dimensional risk scores, providing a standardized implementation basis for the suspected marking of port scanning behaviors and the quantification of malicious risks.

The dynamic traffic threshold is the core basis for identifying high-frequency scanning behaviors, and its design goal is to adapt to the dynamic fluctuations of the network environment and avoid false positives or false negatives caused by fixed thresholds. This rule is based on a time window, selecting the past 5 minutes as the traffic statistical cycle. It defines μ as the mean value of network traffic during this cycle (reflecting the benchmark level of normal network access) and σ as the standard deviation of network traffic during this cycle (reflecting the degree of dispersion of traffic fluctuations). The calculation rule of the dynamic traffic detection threshold (T) is shown as Equation (1). This equation takes the recent traffic mean as the benchmark and superimposes 2 times the standard deviation as the judgment boundary for high-frequency scanning behaviors. It not only accommodates traffic fluctuations during normal business peak periods but also effectively distinguishes between legitimate access and continuous, large-scale scanning behaviors. During method operation, the traffic statistical cycle is updated in real-time, and the threshold is dynamically adjusted. The method compares the real-time scanning traffic of each IP with the current threshold, and marks it as a suspected attack source if the threshold is exceeded, providing basic data for subsequent multi-dimensional assessment.

International Journal of Computer Applications Technology and Research
Volume 15–Issue 02, 01 – 06, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1502.1001

$$T = \mu + 2\sigma \quad (1)$$

For the marked suspected attack sources, a weighted summation calculation rule is adopted to quantify the contribution of three core features to the judgment of malicious attacks, forming a comprehensive risk assessment result. Three core features—traffic, time, and geography—are selected as evaluation indicators, with clear scoring criteria for each indicator: the traffic indicator (F) directly reflects the intensity of scanning behavior, scoring 50 points if the dynamic threshold is exceeded and 0 points otherwise, serving as the core basis for judging malicious scanning; the time indicator (T) combines the temporal rules of attack behaviors, scoring 30 points for scanning behaviors occurring during the nighttime period of 22:00-23:00 (a high-incidence period for port scanning) and 0 points for other periods, reflecting the temporal correlation of attack behaviors; the geographic indicator (G) is based on the geographic attributes of the attack source, with overseas IPs initiating scanning behaviors considered to have higher malicious risks, thus scoring 20 points for overseas IPs and 0 points for domestic IPs or local area network IPs, enhancing the geographic traceability value of the attack source. The calculation rule of the risk total score (R) is shown as Equation (2), which highlights the importance of different features through weight allocation, ensuring the scientificity and rationality of the assessment results.

$$R = 0.4F + 0.3T + 0.3G \quad (2)$$

Where R represents the multi-dimensional risk total score (ranging from 0 to 100 points), 0.4, 0.3, and 0.3 are the weight coefficients of the traffic indicator, time indicator, and geographic indicator respectively, F represents the traffic score, T represents the time period score, and G represents the geographic score.

The higher the risk total score, the higher the malicious risk. A score of 100 points indicates an extremely high risk (with strong aggressive characteristics), 0 points indicates no risk (legitimate access), and 60 points is the critical value for judging malicious attacks. When the total score is ≥ 60 points, the scanning behavior is judged as a malicious attack, requiring focused attention and defensive measures. In summary, the multi-dimensional risk calculation method realizes accurate screening of suspected attack sources through the dynamic traffic threshold judgment rule, and quantifies attack risks with standardized scoring and weighted rules. It not only ensures the scientificity of the assessment but also has strong engineering implementability, providing clear and quantitative risk references for network security managers and helping them quickly lock in high-risk attack sources and formulate targeted defensive strategies[12].

5. SMULATION AND RESULT

This paper adopts the designed port scan monitoring method to collect network data in a specific area from November 26 to 28, and conducts geographic attribution analysis on all abnormal IPs during the monitoring period. The results are shown in Figure 1:

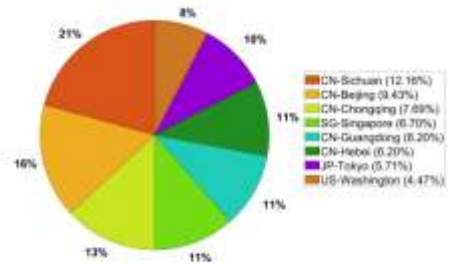

Figure 1. Geographic Distribution Proportion of Abnormal IPs

The core feature of this figure is that abnormal IPs exhibit significant geographic aggregation. Among domestic regions, Sichuan has the highest proportion (12.16%), while Beijing, Chongqing and other regions also account for a certain proportion; overseas, they are concentrated in network hub nodes such as Singapore and Tokyo, Japan.

During the monitoring period, we also analyzed the overall threat level of all IPs and calculated the proportion of daily abnormal IPs in the total scan volume. The results are shown in Figure 2:

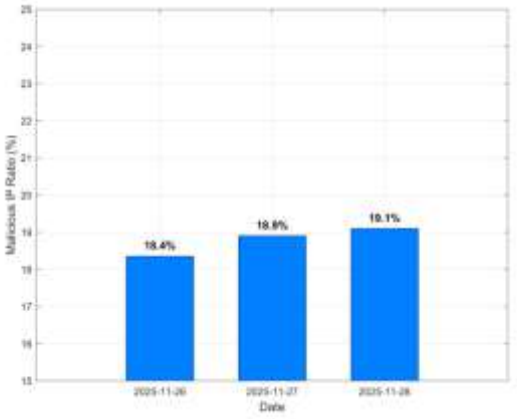

Figure 2. Proportion of Abnormal IPs in Total Scans (Nov 26-28)

This figure clearly presents the fluctuation trend of the proportion of abnormal IPs during the monitoring period: the proportion was 18.4% on November 26, 18.9% on the 27th, and 19.1% on the 28th. It remained within the range of 18.4%-19.1% overall, with no significant fluctuations.

We also analyzed the time distribution law of abnormal IP scans. Using the hourly abnormal IP data collected by the port scan software mentioned in this paper from the 26th to the 28th, the results are shown in Figure 3:

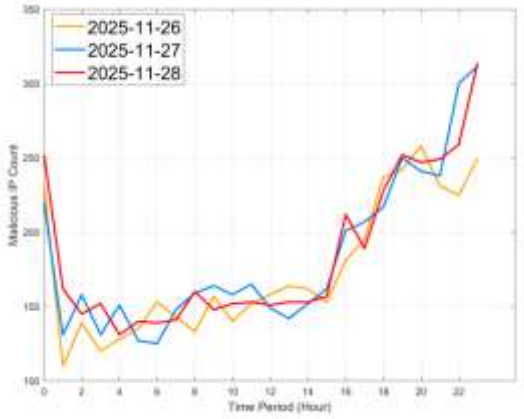

Figure 3. 24-Hour Trend Chart of Malicious IP Count Across Multiple Dates

It can be seen from the figure that the number of abnormal IPs reaches an obvious peak between 22:00 and 24:00 every day, maintains a stable medium level from 2:00 to 16:00, and the time distribution trend is highly consistent across the three days from the 26th to the 28th. This law indicates that abnormal scanning behavior has significant temporal aggregation.

To study the port utilization preference of abnormal IPs, we collected and counted the number of open times of each port through this method. The results are shown in Figure 4:

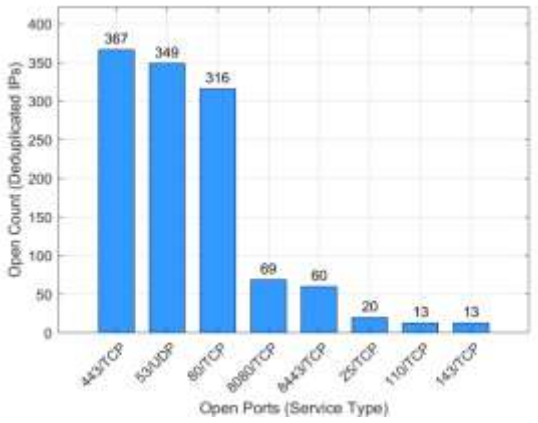

Figure 4. Statistics Chart of Open Ports by Malicious IPs

It can be seen from the figure that the number of open times of three types of ports, namely 443/TCP, 53/UDP, and 80/TCP, is significantly higher than that of other ports. Among them, the number of open times of 443/TCP reaches 367, making it the main attack target of abnormal IPs; while the number of open times of ports such as 25/TCP and 110/TCP is at a low level. This result indicates that abnormal scanning behavior has obvious port aggregation, and public service ports such as 443/TCP, 53/UDP, and 80/TCP are the key targeted objects of attacks.

6. CONCLUSIONS

By using the proposed port scan monitoring method, this paper collects and analyzes network data from a specific region from November 26 to 28, systematically revealing the core characteristic rules of port scan attack behaviors. The experimental results show that 22:00-24:00 daily is the peak period for abnormal IPs, with the number of abnormal IPs during this period accounting for 28%-31% of the total daily abnormal IPs. Moreover, the fluctuation trends of total scan volume and abnormal scan volume show a high degree of consistency, verifying the critical significance of port protection during nighttime. It is urgent to strengthen port access control and traffic monitoring strategies for this high-frequency attack window. Domestic abnormal IPs exhibit significant geographical aggregation characteristics, while overseas attack sources are mostly distributed relying on international network hub nodes, providing data support for the formulation of differentiated IP access thresholds in high-risk regions.

Port attack targets present obvious centralization features: the attack frequency of public service ports such as 443/TCP, 80/TCP, and 53/UDP is significantly higher than that of other ports, with the cumulative opening times exceeding 600 over three days. The security hardening of such basic service ports should be regarded as the core link in constructing network protection systems.

In summary, the proposed port scan monitoring method can extract multi-dimensional attack features from massive traffic, accurately match the temporal, geographical, and port targeting characteristics of attacks, provide strong technical support for formulating scientific defense plans, and significantly improve the accuracy and overall effectiveness of network security protection.

7. ACKNOWLEDGMENTS

Sichuan Province Science and Technology Department, Sichuan Province major science and technology project （No. 2024ZDZX0014）.Key Laboratory of Knowledge Mining and Knowledge Services in Agricultural Converging Publishing（2025KMKS05）. Meteorological Information and Signal Processing Key Laboratory of Sichuan Higher Education Institutes of Chengdu University of Information Technology, the fund of the Scientific and Technological Activities for Overseas Students of Sichuan Province (2022) and Funded by the Sichuan Provincial Department of Human Resources and Social Welfare" Researches on Key issues of Edge Computing Server Deployment and Computing task Offloading". Network and Data Security Key Laboratory of Sichuan Province, UESTC (No. NDS2024-3).Innovation Training Program of "Edge Perception and Decision-Making Platform Based on Embedded Neural Network"; Innovation Training Program of "Design of a Network Detection System Based on Scanning Perception.

8. REFERENCES

[1] R. Vadivel, S. Mayukha, Port Scanning Mitigation Strategies for Penetration Testing: Blue Team Perspective, 2022 International Conference on Engineering and Emerging Technologies (ICEET), Kuala Lumpur, Malaysia, 2022, pp. 1-6.

[2] Yang Andong, Jin Zaiquan, Peng Linfeng, Standardization and Batch Processing of Port Disabling Scripts for Secure Hardening of Independent Innovation Terminals, in Typical Cases, Solutions and Proceedings of Network and Information Security Technology Innovation in Electric Power Enterprises (2025), China Electronic Enterprise Association, Wuhu Power Supply Company, State Grid Anhui Electric Power Co., Ltd., 2025: 16-19..

[3] Cui Hongyuan, A Brief Discussion on the Relationship Between Ports and Network Security, Network Security Technology & Application, 2025, (03): 3-4.

[4] Qi Nannan, Sun Yuejie, Xue Dongliang, Development and Application of Network Security Risk Detection Technology System Based on Port Scanning, China Broadband, 2025, 21 (10): 79-81.

[5] Shi Zhiqiang, Shi Meijing, Research on TCP Port Scanning Technology Based on Multithreading, Modern Computer, 2023, 29 (24): 79-82.

[6] Sun Yang, Research on Spatial Distribution Characteristics and Influencing Factors of Global Cyber Attacks, World Regional Studies, 2025, 34 (09): 59-72..

[7] Hou Yinpeng, Zhou Xue, Zhang Sen, Research on Cybersecurity Defense System in Big Data Environment, Computer Knowledge and Technology, 2025, 21 (31): 81-83.

[8] Cao Wen, Hu Zhifeng, Dai Fei. Research and Implementation of Communication Network Security Vulnerability Scanning Technology Based on Python[J]. Computer Programming Skills & Maintenance, 2024.

[9] Ying Ming, Research on Detection Technology of Slow Port Scan Attacks in SDN Environment, Tianjin University of Technology, Tianjin, 2023.

[10] L. Yanyan, H. Shanhou, Application of Bayesian Optimization in Router Port Testing: An Improved Port Scanning Technique, 2023 IEEE 5th International Conference on Power, Intelligent Computing and Systems (ICPICS), Shenyang, China, 2023, pp. 98-103.

[11] Wang Longye, Luo Jie, Security Detection Method for Internet Port Scan Attacks, Information Security and Technology, 2016, 7 (02): 44-45+64.[12] Qi Nannan, Sun Yuejie, Xue Dongliang, Development and Application of Network Security Risk Detection Technology System Based on Port Scanning, China Broadband, 2025, 21 (10): 79-81.

[12] Li Qizhen, Research and Implementation of Network Scanning System for IoT Device Identification, Sichuan Normal University, Chengdu, 2024.[14] Sun Yang, Research on Spatial Distribution Characteristics and Influencing Factors of Global Cyber Attacks, World Regional Studies, 2025, 34 (09): 59-72..

[13] J. Huang, J. Chen, X. Lu, B. Mo, C. Zeng and S. Qiu, "Research on detection techniques for scanning attacks in software-defined network environments," 2023 4th International Conference on Computer Engineering and Application (ICCEA), Hangzhou, China, 2023.

[14] H. Wu, Z. Shao, G. Cheng, X. Hu, J. Ren and W. Wang, "Detecting Slow Port Scans of Long Duration in High-Speed Networks," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022.

[15] Xie Xiaomin, Research on Game Model for Port Mapping and Anti-mapping, Guangzhou University, Guangzhou, 2025.