Advances in Artificial Intelligence, Big Data and Algorithms
G. Grigoras and P. Lorenz (Eds.)

doi:10.3233/FAIA230841

Data Flow Risk Monitoring for Novel Power System Based on Bidirectional Interactive Protocol Traffic

Jianqiao SHENG[1], Yuan FANG[2], Guannan ZHANG[3], Xin DING[4]
Information and Communication Branch, State Grid Anhui Electric Power Co., Ltd., Hefei, China

Abstract—In response to the challenges brought by the significant increase in data volume and the proprietary and closed nature of business protocols in the highly coordinated and interactive "source-network-load-storage" system of the new power grid, this study proposes a technology for analyzing abnormal behavior in bidirectional interactive protocols. A risk monitoring scheme for data flow is designed, incorporating both trigger detection and deep detection. The scheme proposes an improved cumulative sum algorithm (SSUM algorithm) for risk monitoring by real-time tracking of multidimensional sequences and their cumulative deviations based on statistical characteristics, achieving coarse-grained risk monitoring of the entire network flow. Then, time window features are introduced and the AdaBoost ensemble learning algorithm is used for fine-grained deep detection of abnormal traffic. Finally, the presence of data flow risk is determined. Experimental results show that the detection accuracy of the AdaBoost algorithm is better than that of other classification algorithms, reaching 97.7%. The joint monitoring scheme has the advantages of low cost and low false alarm rate.

Keywords-Smart grid, data flow, risk monitoring, bidirectional interactive protocol traffic, risk assessment

1. Introduction

The new power system integrates advanced power electronic technology, information technology, and intelligent management technology to enable the interconnection of distributed energy collection devices, energy storage devices, and various loads, forming a network of new energy nodes. This network facilitates bidirectional energy flow, energy-equivalent exchange, and resource sharing. The interaction and interconnection among the intelligent power grid, power sources, and customers are strengthened. The power grid and energy internet continuously introduce new models and formats for resource sharing, integrating new technologies with traditional businesses. However, the

[1] Corresponding author: Jianqiao SHENG, Information and Communication Branch, State Grid Anhui Electric Power Co., Ltd., e-mail: 86503739@qq.com
[2] Yuan FANG, Information and Communication Branch, State Grid Anhui Electric Power Co., Ltd., e-mail: 657362916@qq.com
[3] Guannan ZHANG, Information and Communication Branch, State Grid Anhui Electric Power Co., Ltd., e-mail: 56102201@qq.com
[4] Xin DING, Information and Communication Branch, State Grid Anhui Electric Power Co., Ltd., e-mail: 1137401560@qq.com

new power system's complex structure, communication network environment, and frequent bidirectional interaction pose heightened security risks.

In recent years, there has been significant attention focused on monitoring data flow risks. This article primarily focuses on studying the detection schemes deployed in the controllers of the new power system. Several research studies have proposed detection schemes based on traditional statistical theory [1-8]. For example, Tao proposed utilizing entropy as a key feature to characterize network traffic [1]. Researchers such as Song and Gao have discussed the decrease in the randomness of destination IP address distribution during DDoS attacks [2-3]. By measuring the entropy value of the destination IP address, the randomness of the distribution can be evaluated, enabling the detection of such attacks [5-8]. Tee and Xiao proposed schemes based on the CUSUM control chart to track changes in feature quantities for anomaly detection [9-11]. Liu developed a model for automatic detection of abnormal values [12]. However, the algorithm's dependency on pre-simulated attack experiments limits its adaptability and portability [13]. Moreover, establishing a comprehensive flow model remains challenging, leading to limited detection accuracy. To address these challenges, researchers like San and Ye have applied machine learning technologies such as support vector machines, logistic regression, K-nearest neighbor, naive Bayes, and neural networks for detection algorithms [14-16]. Braga analyzed statistical information related to DDoS attacks and proposed the "six-tuple" flow-based feature [17]. The self-organizing map algorithm was used to identify malicious traffic based on the "six-tuple." However, the slow convergence of the SOM algorithm resulted in extended training times and increased system overhead [18-20].

The choice of detection cycle poses a challenge due to the conflicting factors of system overhead and detection delay. Determining the appropriate length of the detection cycle is crucial for an effective detection scheme. Balancing these two factors becomes a challenging task as there is a trade-off between minimizing detection delay and optimizing system resources. Achieving an optimal detection cycle requires careful consideration and analysis of the specific requirements, constraints, and capabilities of the system, as well as the potential impact on the network's performance and security.

The feature extraction methods face certain limitations and areas that require improvement. Existing research often yields features with high similarity, such as the entropy of source and destination addresses. However, traffic changes are reflected in multiple dimensions, making it challenging to establish a comprehensive flow model using these existing schemes. There is a need to explore and incorporate additional diverse features that capture the various aspects of traffic dynamics. Furthermore, most research focuses solely on the current network state during feature extraction, neglecting the historical state. However, during network attacks, traffic changes exhibit a high degree of temporal correlation. Therefore, it is essential to consider the temporal characteristics of traffic changes by utilizing appropriate features that capture the dynamics over time. Incorporating temporal features into the extraction process can enhance the detection accuracy of the system by capturing the evolving patterns and trends of network traffic. Overall, improvements in feature extraction methods should involve exploring and incorporating diverse features that go beyond the existing similarity-based features. Additionally, considering the historical state and incorporating temporal features will enable a more comprehensive understanding of traffic dynamics and lead to improved detection accuracy and performance.

The main contributions of this paper are as follows:

- **Trigger detection**: A module that continuously operates within the network and performs real-time, coarse-grained risk monitoring using the SSUM algorithm. This module ensures extremely low false negative rates through parameter adjustments. It serves as an early warning system, detecting potential anomalies and alerting the system.
- **Deep detection**: A module that is activated after the trigger detection module raises an alarm. This module focuses on extracting finer-grained features using a time-window-based feature construction scheme. The high-precision AdaBoost algorithm is utilized to identify abnormal traffic patterns accurately.

2. Overall Structure

The architecture of the attack detection system consists of several modules, each serving a specific function, shown in Fig. 1:

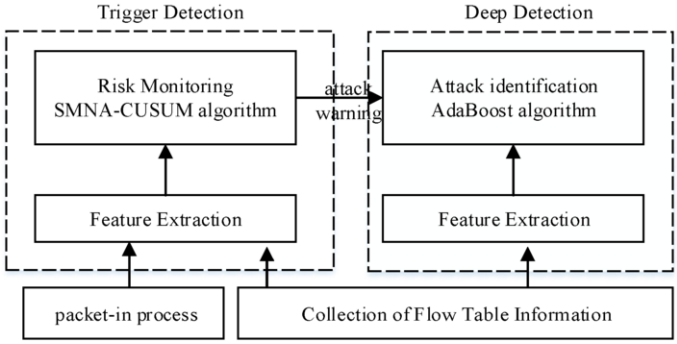


Figure 1. The overall architecture of the attack detection system

Trigger detection module: This module runs continuously in the network and performs coarse-grained risk monitoring. It collects network information from flow table information collection and packet-in message processing modules. The feature extraction module extracts four-dimensional feature vectors based on the collected information and constructs feature sequences. The risk monitoring module utilizes the SSUM algorithm to track and observe the feature sequence. If an anomaly is detected, it immediately issues an attack warning to notify the deep detection module.

Deep detection module: This module is activated upon receiving the attack warning from the trigger detection module. It focuses on extracting finer-grained features and uses the AdaBoost algorithm based on decision trees for attack identification. The feature extraction module obtains network information from the flow table information collection module. It extracts eight features that characterize network traffic status and constructs feature vectors based on sliding time windows. The attack identification module classifies the feature vectors in real-time using the AdaBoost algorithm and the trained model to make the final decision. If the decision indicates abnormality, it signifies the presence of anomalous attacks in the network.

Packet-in message processing module: This module passively receives and processes packet-in messages from the switches. It plays a crucial role in collecting network information, which is essential for anomaly detection and analysis.

Flow table information collection module: This module actively polls and collects all flow table information in the switches. It provides valuable network information required for the detection and monitoring processes.

These modules work together to provide a comprehensive approach for anomaly attack detection in the network. The trigger detection module acts as an early warning system, while the deep detection module focuses on precise identification and classification of attacks. The packet-in message processing and flow table information collection modules ensure the availability of relevant network information for effective detection and analysis.

3. Protocols Detail

A network that is under attack may exhibit the following characteristics:

- Burstiness: There is a sudden increase in the number of data packets in the network, indicating a burst of malicious activity.
- Latency: The network experiences severe congestion, leading to significant delays in packet transmission and communication.
- Asymmetry: There is a large number of half-connected data packets in the network, indicating an imbalance or irregularity in the traffic flow.

Dispersed source IP distribution of attack flow packets: The packets originating from an attack flow have a dispersed source IP distribution, meaning they come from a wide range of source IP addresses. However, there may be a concentrated distribution of destination IP addresses for these attack packets.

The paper focuses on extracting specific traffic features to characterize the above-mentioned characteristics of the system during abnormal data conditions. These features include: Burstiness feature: Extracting the changes in packet counts over time to identify sudden increases or bursts in network traffic. Latency feature: Analyzing the delays or increased round-trip times between communication endpoints to detect network congestion and potential attacks. Asymmetry feature: Examining the imbalances in the number of inbound and outbound packets to identify any irregular traffic patterns. Dispersed source IP distribution feature: Analyzing the distribution of source IP addresses of attack flow packets to detect any concentrated or dispersed patterns that indicate malicious activity.

The formula (1) provides a representation of the flow table entry by capturing information such as the switch ID, source and destination IP addresses, packet count, total bytes, and flow rate. These variables collectively describe the characteristics and statistics of network traffic associated with the specific flow table entry.:

$$C_i = [dpID_i, srcIP_i, dstIP_i, pkts_i, bytes_i, speed_i] \tag{1}$$

In the given formula, the variables have the following meanings. C_i represents a vector that contains the information of the i-th flow table entry. $dpID_i$ denotes the identifier (ID) of the switch where the flow table entry is located. $srcIP_i$ represents the source IP address associated with the matching field of the flow table entry. $dstIP_i$ signifies the destination IP address associated with the matching field of the flow table entry. $pkts_i$ indicates the number of packets that are matched with the specific flow table

entry. $bytes_i$ represents the total number of bytes that are transmitted by the packets matched with the flow table entry. $speed_i$ denotes the flow rate of the packets matched with the flow table entry.

We also introduce the concept of the entropy to measure the randomness of source and destination IP addresses in the network for detecting network attacks. When an attack occurs, a significant number of data packets are sent from compromised or "zombie" hosts. This results in an increased probability that the source IP addresses in the flow table statistical information belong to these compromised hosts. As a consequence, the randomness of the source IP addresses decreases. As the victim receives a larger volume of data packets, there is a more concentrated distribution of destination IP addresses, indicating a decrease in randomness. This shift in the distribution pattern of destination IP addresses is another characteristic of network attacks.

By leveraging the concept of entropy, which measures the randomness or uncertainty of a given set of data, one can quantitatively assess the level of randomness in the source and destination IP addresses. A higher entropy value suggests a more random and normal distribution of IP addresses, while a lower entropy value indicates a less random and potentially malicious distribution.

Therefore, by analyzing the entropy of the source and destination IP addresses, it becomes possible to detect deviations from the expected randomness and identify potential network attacks. The calculation method for information entropy is shown in formula 2:

$$H(dstIP) = \sum_{i=1}^{n} p_i \log p_i \tag{2}$$

Among them, n represents the total number of destination IP addresses, and p_i represents the probability of the i-th IP address appearing. The calculation method of p_i is in formula 3 and 4:

$$W = \{(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots\} \tag{3}$$

$$p_i = \frac{y_i}{n} \tag{4}$$

Where W repreents a set of purpose IP addresses collected within a certain time period. x_i represents a certain purpose IP address. y_i represents the number of times this address appears.

The following information is extracted from the flow table information as indicators to determine whether an attack has occurred, the formulas 5-9 show how to calculate these features:

- Total number of flow tables ($flowCount$): This represents the overall count of flow tables in the network and provides an indication of the network's activity.
- Total number of packets ($pktCount$): This denotes the total count of packets in the network and helps assess the volume of data being transmitted.
- Total number of bytes ($byteCount$): This indicates the total count of bytes in the network, providing insights into the overall data size and traffic intensity.

- Entropy of source IP addresses ($H(srcIP)$): This measures the randomness or uncertainty of the source IP addresses appearing in the flow table information. A decrease in entropy suggests a concentration of source IP addresses, indicating a potential attack.
- Entropy of destination IP addresses ($H(dstIP)$): This measures the randomness or uncertainty of the destination IP addresses in the flow table information. Similar to the entropy of source IP addresses, a decrease in entropy indicates a concentrated distribution of destination IP addresses, which could be indicative of an attack.

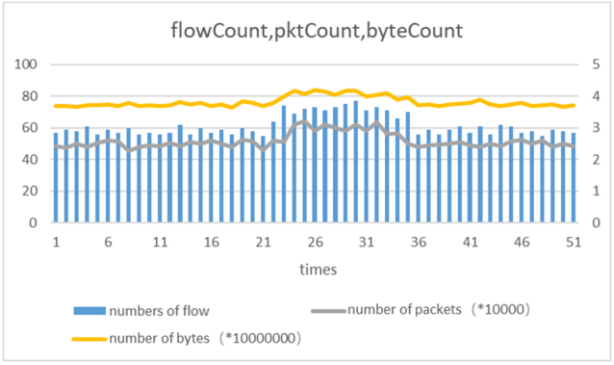
$$flowCount = n \tag{5}$$

$$pktCount = \sum_{i=1}^{n} pkts_i \tag{6}$$

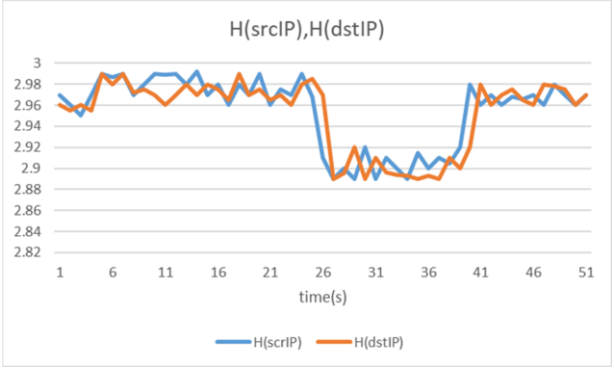
$$byteCount = \sum_{i=1}^{n} bytes_i \tag{7}$$

$$H(srcIP) = \sum_{i=1}^{n} p_i \log p_i \tag{8}$$

$$H(dstIP) = \sum_{i=1}^{n} p_i \log p_i \tag{9}$$



（a）The flow ,packet and byte count charactristics



(b) The source IP charactristic and destination IP charactristic

Figure 2. Changes in the five characteristic quantities during an attack

To further analyze the above features and observe their actual changes under normal and attack conditions, this paper simulates them in an SDN network. Fig. 2 shows the changes in network traffic features. Figures 2(a) and 2(b) respectively represent the five features. In the experiment, a TCP SYN Flood attack with a duration of about 80s was launched at 150s. Sub-table information was collected every 5s, and the information was collected for about 5 minutes in total.

4. Conclusion

In this paper, our main focus is the new power system. To address the challenge of determining the detection cycle, we propose a joint monitoring scheme that combines trigger detection and deep detection. The trigger detection module utilizes the low-cost SSUM algorithm for coarse-grained anomaly early warning. Deep detection incorporates the temporal characteristics of traffic changes to improve detection accuracy. The AdaBoost algorithm is selected for classification, showing superior performance with an accuracy of 97.7%. The joint monitoring scheme offers low cost and high detection accuracy.

Acknowledgement

This paper is supported by the funding of Anhui Provincial Electric Power Company's Technology Project of State Grid Corporation. (No. 521207220001, Research on Full-Chain Flow Analysis and Attack Traceback Technology for Secure Interaction in New Power System).

References

[1] Song, R., Gao, S., Song, Y., & Xiao, B. (2022, July). : A Traceable and Privacy-Preserving Data Exchange Scheme based on Non-Fungible Token and Zero-Knowledge. In 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS) (pp. 224-234). IEEE.

[2] Yang, L., Song, Y., Gao, S., Hu, A., & Xiao, B. (2022). Griffin: Real-time network intrusion detection system via ensemble of autoencoder in SDN. IEEE Transactions on Network and Service Management, 19(3), 2269-2281.

[3] Chen, Q., Song, Y., Jennings, B., Zhang, F., Xiao, B., & Gao, S. (2021, December). IoT-ID: robust IoT device identification based on feature drift adaptation. In 2021 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[4] Song, Y., Chen, B., Wu, T., Zheng, T., Chen, H., & Wang, J. (2021). Enhancing packet-level Wi-Fi device authentication protocol leveraging channel state information. Wireless Communications and Mobile Computing, 2021, 1-12.

[5] Song, Y., Geng, Y., Wang, J., Gao, S., & Shi, W. (2021). Permission Sensitivity-Based Malicious Application Detection for Android. Security and Communication Networks, 2021, 1-12.

[6] Chen, B., Song, Y., Zhu, Z., Gao, S., Wang, J., & Hu, A. (2021, June). Authenticating mobile wireless device through per-packet channel state information. In 2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W) (pp. 78-84). IEEE.

[7] Wu, T., Song, Y., Zhang, F., Gao, S., & Chen, B. (2021, June). My site knows where you are: a novel browser fingerprint to track user position. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.

[8] Ma, X., Song, Y., Wang, Z., Gao, S., Xiao, B., & Hu, A. (2021, June). You Can Hear But You Cannot Record: Privacy Protection by Jamming Audio Recording. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.

[9] Chen, B., Song, Y., Wu, T., Zheng, T., Chen, H., Wang, J., & Li, T. (2021). Enhancing Wi-Fi Device Authentication Protocol Leveraging Channel State Information. In Mobile Multimedia Communications: 14th EAI International Conference, Mobimedia 2021, Virtual Event, July 23-25, 2021, Proceedings 14 (pp. 33-46). Springer International Publishing.
[10] Song, Y., Zhou, K., & Chen, X. (2012). Fake bts attacks of gsm system on software radio platform. Journal of Networks, 7(2), 275.
[11] Song, R., Song, Y., Gao, S., Xiao, B., & Hu, A. (2018, December). I know what you type: Leaking user privacy via novel frequency-based side-channel attacks. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.
[12] Song, Y., Huang, Q., Yang, J., Fan, M., Hu, A., & Jiang, Y. (2019, May). IoT device fingerprinting for relieving pressure in the access control. In Proceedings of the ACM Turing Celebration Conference-China (pp. 1-8).
[13] Song, R., Song, Y., Liu, Z., Tan, M., & Zhou, K. (2019). GaiaWorld: a novel blockchain system based on competitive PoS consensus mechanism. CMC-COMPUTERS MATERIALS & CONTINUA, 60(3), 973-987.
[14] Shi, C., Song, R., Qi, X., Song, Y., Xiao, B., & Lu, S. (2020, June). ClickGuard: Exposing hidden click fraud via mobile sensor side-channel analysis. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
[15] Yang, L., Song, Y., Gao, S., Xiao, B., & Hu, A. (2020, December). Griffin: an ensemble of autoencoders for anomaly traffic detection in SDN. In GLOBECOM 2020-2020 IEEE Global Communications Conference (pp. 1-6). IEEE.
[16] Gao, S., Peng, Z., Xiao, B., Hu, A., Song, Y., & Ren, K. (2020). Detection and mitigation of DoS attacks in software defined networks. IEEE/ACM Transactions on Networking, 28(3), 1419-1433.
[17] R. Song, Y. Song, Q. Dong, A. Hu and S. Gao, "WebLogger: Stealing your personal PINs via mobile web application," 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 2017, pp. 1-6.
[18] Y. Song, X. Zhu, Y. Hong, H. Zhang and H. Tan, "A Mobile Communication Honeypot Observing System," 2012 Fourth International Conference on Multimedia Information Networking and Security, Nanjing, China, 2012, pp. 861-865.
[19] Y. Gala, N. Vanjari, D. Doshi and I. Radhanpurwala, "AI based Techniques for Network-based Intrusion Detection System: A Review," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 1544-1551.
[20] B. Charyyev and M. H. Gunes, "Locality-Sensitive IoT Network Traffic Fingerprinting for Device Identification," in IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1272-1281, 1 Feb.1, 2021.