High Camouflage Intrusion Detection Method for Structured Database Based on Multi Pattern Matching

Dawei Song1,*, Xun Zhu1, Fengjuan Ma1

1Weifang Vocational College of Engineering, Qingzhou City, Shandong, China, 262500

*Corresponding author e-mail: daweis@wfec.edu.cn

Abstract. with the rise and rapid development of mobile communication, intelligent terminal and data system, we are entering the era of mobile Internet. In recent years, more and more data need to be processed and transmitted in daily life, and structured data is becoming more and more important. Among them, multi-mode matching technology can search data in a wider range. Matching for multiple patterns at a time avoids unnecessary matching, accelerates the matching process, and helps to find longer matching information and obtain higher accuracy. This paper mainly introduces the high camouflage intrusion detection method of structured database based on multi-mode matching. This paper uses the high disguised intrusion detection method of structured database based on multi-mode matching, collects sensitive information of wireless access points and stations through the communication of WLAN in multimodal matching, then intercepts and forges data packets to initiate replay attack. Replay attack is characterized by abnormal traffic in the network, which can be detected by statistical analysis. The experimental results show that the high camouflage intrusion detection method based on multi-mode matching makes the camouflage intrusion detection rate increase by 23%. The limitations of the design and research of camouflage intrusion detection are analyzed, discussed and summarized, so as to enrich the academic research results.

Keywords: Multi Mode Matching, Structured Database, High Disguised Intrusion Detection, Wireless Local Area

1. Introduction

In recent years, masquerade detection has been widely studied in the academic and industry, and plays a huge role in information security engineering: some masquerade intrusion detection systems also show convincing performance [1-2]. However, there are still some problems to be solved in the design
and implementation of camouflage intrusion detection system (hereinafter referred to as "detection system"), when the learning features are too single: most detection systems only care about the individual behavior of users, but some user groups will have aggregation in some behaviors, thus interfering with the detection results [3-4].

With the progress of science and technology and the rapid development of the Internet, the design of indoor path planning algorithm in complex environment is enhanced. Due to the openness of the wireless channel, the wireless LAN realizes data transmission by sending wireless signals to all sides without any difference, which not only achieves high flexibility, but also brings many insecurity factors [5-6]. Li Y analyzed the relationship between intrusion detection signal and database and their conversion algorithm [7]. Zhang g thinks that the existing conversion algorithms only consider how to completely preserve the semantics and structure of intrusion detection signal documents, but there are still many problems in data type, binary data processing, character set and so on. There may be insert, delete and update exceptions in the database generated in this way [8]. The use of wireless media eliminates the physical access of wired network cable, and also loses a layer of effective isolation for intruders. In addition, WLAN also uses TCP / IP protocol and IEEE protocol, which has its own defects, making WLAN not only subject to the same attack against TCP / IP protocol as wired LAN, but also subject to the invasion threat against WLAN data link layer [9-10]. However, there are errors in their experimental process, resulting in inaccurate results.

The innovation of this paper is to propose a high camouflage intrusion detection method for structured database based on multi pattern matching. In this paper, the method of Intrusion Detection Based on multi-core structured database pattern matching is studied in detail. That is to use the results of each match to dynamically establish a structured database. Then, the fixed size data block is read from the file, multi pattern matching preprocessing is carried out, all the patterns in the database are searched, and the matching data (including matching location and matching length) is obtained. The matching data is used to output coding and improve the tree. The purpose of this study is to find a new way for the development of high camouflage intrusion detection in structured database.

2. Structural database analysis of multi pattern matching

2.1. Multi matching pattern analysis

With the development of Internet technology, intrusion detection signal, as a form of Web data, becomes more and more important in data exchange of Internet and e-commerce. Camouflage intrusion means that the attacker embeds virus into the user's system in advance, so as to obtain the permission to operate the user's system and carry out illegal operation. These two kinds of intrusion behavior will cause serious threat to system security, and may cause organizations or individuals to disclose key data, which will bring economic and reputation damage.

The multi pattern matching structured database detection terminal is specially designed for intrusion detection and response. The detection terminal is equipped with two network cards. The wireless network card randomly monitors the wireless network communication of all frequency bands in the coverage area, and the wired network card is responsible for the communication with the control center. Wireless network detection terminal includes data acquisition module, protocol analysis module, intrusion detection module and response module. The detection terminal is an embedded system running Linux operating system, which has the advantages of low cost, small size and flexible configuration in practical application. The device management module is responsible for organizing all the device information in the local wireless LAN and storing it in the database structurally. The device information is provided to the intrusion detection module. The administrator can view, add and manage legitimate devices through the device management module. Local application of this function
can design an effective algorithm in the structured database, which has the following forms.

\[
\min f(X) = w_1f_1(X) + w_2f_2(X) + ... + w_if_i(X), X \in \Omega
\]

The formula is as follows:

\[
3I_{01} = I_{d1} + I_{g1} + I_{c1} = 3U_{0j} \sigma C_{01}
\]

The following formula shall be used for the test:

\[
g_k(X) \geq 0(i = 1.2.3...k)
\]

2.2. Structured database

The attacker obtains relevant sensitive information through eavesdropping, and then deploys fake access point near the target access point. If the signal noise ratio of the fake access point is higher than the legitimate access point, the victim computer will automatically select the counterfeit equipment with strong signal to access, and lure the legitimate station to connect to the fake access point incorrectly, and the attacker can collect key data such as user name and password, then, the illegal site can log in to the legitimate access point by collecting the information.

By building a structured database, intrusion signals can be detected effectively. The server mainly stores the received ciphertext in the database in the data storage stage: when the user sends the retrieval request, it is responsible for matching the records in the database that meet the retrieval conditions, and returning the ciphertext record set to the client. The database has the characteristics of addition homomorphism and multiplication homomorphism. When the data needs to be averaged and summated, it is not necessary to perform decryption operation first, then encrypt the result of plaintext operation, but can directly operate ciphertext and database operation, which greatly reduces the cost and efficiency of encryption and decryption operation and data transmission; on the other hand, it can protect important or sensitive data, so that users can operate the data and get the required results. In the traditional encryption method of leaking data details, when users use their own key to encrypt data, the same ciphertext results will be generated when the same value of plaintext is encrypted. If the number of attribute values of a field in a database is relatively small, the number of ciphertext generated after encryption is limited. At this time, the attacker can attack statistics based on frequency, thus threatening the security of ciphertext database.

3. Intrusion detection analysis in multi matching mode

3.1. Multi matching algorithm

Since the pattern string information in the multi-mode matching algorithm has been known and stored in a container with continuous address before pattern matching, a complete binary search tree can be realized by an array. The array stores the index value of the pattern string in the container. The subscript range of the array is 1 to N, where n is the number of nodes in the binary tree. If the subscript of the current node in the array is I, the subscript of the left child node of the current node is 2x, and the right child node of the current node is 2xi + 1. The algorithm constructs the complete binary search tree based on the array in recursive way. The first element of ordered sequence must be the leftmost child node of binary search tree, and the second element must be the parent node of the left child node. Therefore, the elements can be added to the array during the middle order traversal of the tree in the
form of array.

3.2. Abnormal detection signal in detection system

Compared with misuse detection, anomaly detection has certain detection ability for unknown intrusion behavior, but the error detection rate is higher when the detection environment changes greatly. The misuse detection is based on the known intrusion characteristics, and the detection accuracy is high, but it has a greater dependence on the system. The most significant difference between wireless network and wired network is the transmission medium, especially in security. The mobile characteristics of wireless network bring many vulnerabilities that are not existed in the wired network, which makes many effective security measures in the wired environment invalid in the wireless environment. The open transmission of wireless signal is one of the root causes of additional threats to WLAN (relative to wired network), and also the main reason that affects the development and application of wireless technology. Therefore, it is very important to do well in wireless security prevention and develop new intrusion detection structure and mechanism to protect wireless network.

The intrusion detection system is mainly centralized and decentralized in application form. The core of the centralized system is the control center, which usually connects multiple wireless detectors to collect data, and the information is transmitted to the control center after preliminary processing, and further processed by the control center. The status and function of each device node of decentralized system are the same, and can independently complete the intrusion detection function. Because of its convenience of management and less investment, it is suitable for small-scale wireless network. The specific results are shown in Table 1.

|                         | Very important | general | Very unimportant |
|-------------------------|----------------|---------|------------------|
| Personal literacy       | 63%            | 31%     | 0%               |
| Personal effort         | 57%            | 27%     | 2%               |
| Personal hobbies        | 44%            | 32%     | 11%              |
| Practice participation level | 38%      | 27%     | 35%              |

4. Wireless local area model in intrusion detection system

4.1. WLAN analysis

WLAN usually needs to cover a large area, and it often needs to configure multiple wireless access points. There are two ways of detector deployment: distributed deployment and accompanying deployment. Distributed deployment can cover the wireless network with the least detectors, but due to the transmission characteristics of wireless signal, it can not guarantee that there is no detection dead angle. If the deployment mode of detector and wireless access point is adopted, the monitoring range and wireless access area can be completely overlapped and covered, so that the detection system can achieve the goal of full coverage of wireless access range and no blind area detection, and improve the intrusion detection rate. Intrusion detection system has the following characteristics: robustness. There should be multiple monitoring points in the whole system, and the failure of the whole system can not be caused by the failure of one monitoring point. System configuration is simple, each part of the system should be able to meet a variety of needs configuration; adaptability. The judgment
standard of network events should adapt to the changes of computer and network environment and be easy to expand. It has the ability to expand its own monitoring range, and the new host and other equipment can be added into the system. Concurrency analysis ability; multiple different events of multiple hosts can be monitored at the same time, and multiple modes can be comprehensively analyzed to determine whether the intrusion behavior; high efficiency, less occupation of host resources, less impact on network performance. The specific results are shown in Figure 1. The abscissa is the synchronization number model, and the ordinate is the absolute value of the error. The experimental results show that the error decreases exponentially with the increase of intrusion detection times.

![Figure 1. Statistical table of sample library](image)

### 4.2. Camouflage data intrusion analysis

With the increase of camouflage data intrusion, the commonly used encryption protocols and security mechanisms of WLAN are constantly enhanced. Aiming at the characteristics of WLAN, this paper analyzes the defects of security mechanisms, lists the common threats and attacks, studies and summarizes a variety of DoS attacks, and analyzes their attack principles. Finally, it introduces the intrusion detection system, and analyzes the similarities and differences between wired and wireless; Finally, the paper evaluates the two data sources commonly used in WLAN intrusion detection technology, and gives the reasons. The open wireless signal transmission of WLAN physical layer brings many security risks, which directly affects the data security of data link layer. In addition, the device management of WLAN is mainly implemented in the data link layer, so ensuring the data security of the data link layer is a necessary condition to ensure the normal management and operation of the legitimate devices of WLAN, and also a necessary condition to realize the intrusion prevention and detection of WLAN. The specific results are shown in Table 2.

### Table 2. Statistical table of sample library

|                      | Normal | Ageing | Malfunction |
|----------------------|--------|--------|-------------|
| Number of Transformers | 43.11  | 4.54   | 4.81        |
| Total Sample         | 42.32  | 4.12   | 3.85        |
| Training Samples     | 40.52  | 3.79   | 2.63        |
| Validation           | 39.98  | 3.89   | 3.47        |
The attacker usually uses Aire play to launch ARP replay attack. Firstly, a large number of authentication cancellation frames are sent to disconnect the site from the wireless access point, while monitoring the network. When the site reconnects with the wireless access point after disconnection, it will send ARP requests, and Aire play will continuously send the captured ARP requests to the wireless access point, at this time, a large number of ARP request packets in the network will greatly increase the number of packets and fragile initialization vector (IV), so as to accelerate the speed of key cracking. The specific results are shown in Figure 2. When the number of attributes is the same, the detection efficiency of WLAN is significantly improved with the increase of the number of sample data.

![Figure 2. Questionnaire](image)

5. Conclusion

In this paper, there are still many shortcomings in the high camouflage intrusion detection method of structured database based on multi pattern matching. The database encryption and decryption algorithm designed in this paper is proposed on the premise of ensuring the security of the client, without considering the problem of key management, so the scheme needs to be further improved. This paper studies the security retrieval of structured database, and the security retrieval strategy of unstructured database is the next stage of research. Experiments and analysis verify the security and efficiency of the algorithm. There are still a lot of contents worthy of further study on the high camouflage intrusion detection method of structured database based on multi pattern matching. There are still many steps to study the high camouflage intrusion detection analysis of structured database, which are not involved due to space and personal ability. In addition, the experimental results of the algorithm design can only be compared with the traditional model in theory and simulation.

References

[1] Li Y, Tian S, Huang Y, et al. Driverless artificial intelligence framework for the identification of malignant pleural effusion [J]. Translational Oncology, 2021, 14(1):100896.

[2] Hassabis D, Kumaran D, Summerfield C, et al. Neuroscience-Inspired Artificial Intelligence [J]. Neuron, 2017, 95(2):245-258.
[3] Lu H, Li Y, Chen M, et al. Brain Intelligence: Go Beyond Artificial Intelligence [J]. Mobile Networks and Applications, 2017, 23(7553):368-375.

[4] Ng T K. New Interpretation of Extracurricular Activities via Social Networking Sites: A Case Study of Artificial Intelligence Learning at a Secondary School in Hong Kong [J]. Journal of Education and Training Studies, 2021, 9(1):49-60.

[5] Camerer C F. Artificial Intelligence and Behavioral Economics [J]. NBER Chapters, 2018, 24(18):867-71.

[6] Jia-zhan, Su, Xi-lun, et al. Full-scale bending test and parametric study on a 30-m span prestressed ultra-high performance concrete box girder: [J]. Advances in Structural Engineering, 2019, 23(7):1276-1289.

[7] Li Y, Yan L, Wang L, et al. Estimation of normal distribution parameters and its application to carbonation depth of concrete girder bridges [J]. Discrete & Continuous Dynamical Systems, 2019, 12(4&5):1091-1100.

[8] Zhang G, Wang J, Liu J, et al. Analysis of loss in flexural stiffness of in-service prestressed hollow plate beam [J]. International Journal of Structural Integrity, 2019, ahead-of-print(4):534-547.

[9] Needhi, Kotoky, Anjan, et al. Hybrid testing for evaluation of seismic performance of highway bridge with pier made of HyFRC - ScienceDirect [J]. Structures, 2019, 20:848-865.

[10] Yuanyao M, Ditao N. Effect of Vehicle Load on the Fatigue Performance of Corroded Highway Bridge [J]. Science of Advanced Materials, 2018, 10(6):845-852.