

Application of hospital information security based on Intelligent Intrusion Detection System

Xingshan LI ^a, Yifan ZHANG, Min XU

Luohe medical college, Luohe, 462000, China

^aemail:604141388@qq.com

Keywords: Intelligent intrusion, detection system, NPRIM new algorithm

Abstract. The intelligent improved NPRIM algorithm is applied to the new hospital in intrusion detection system, and has done a lot of experiments on simulation data sets, design a high detection rate and low false detection rate based on clustering and the boundary point detection of intelligent intrusion detection system model.

Introduction

The description and treatment of hospital information system includes the processing data state of the network system in the hospital information network system, the real-time traffic of the network processing data, the internal operation of the medical system and so on. More detailed contents is the detailed time of medical behavior, medical staff's personal data and information, the types of medicine and health care system of medical, health event details of specific diagnosis and treatment[1]. In order to guarantee the normal operation of the hospital information system, ensure the safety of the medical information and patient information, the intelligent intrusion detection system model based on clustering and boundary point detection was designed to applied in hospital information system, effective to detect the invasion of the hospital information system, at the same time record invading the source IP address, specific illegal types of external network attack, attack time, attack ability and purpose, fast and make alarm and record[2].

Design of intrusion detection model based on clustering and boundary points detection

NPRI algorithm of clustering and boundary detection wse applied to intrusion detection system[3], the whole process is shown in fig. 1.

Can be seen from the overall flow chart1 of intrusion detection model, the intrusion detection system of the project group is mainly composed of data processing, clustering analysis, intrusion detection, intrusion response, and storage of five parts [4] [5].

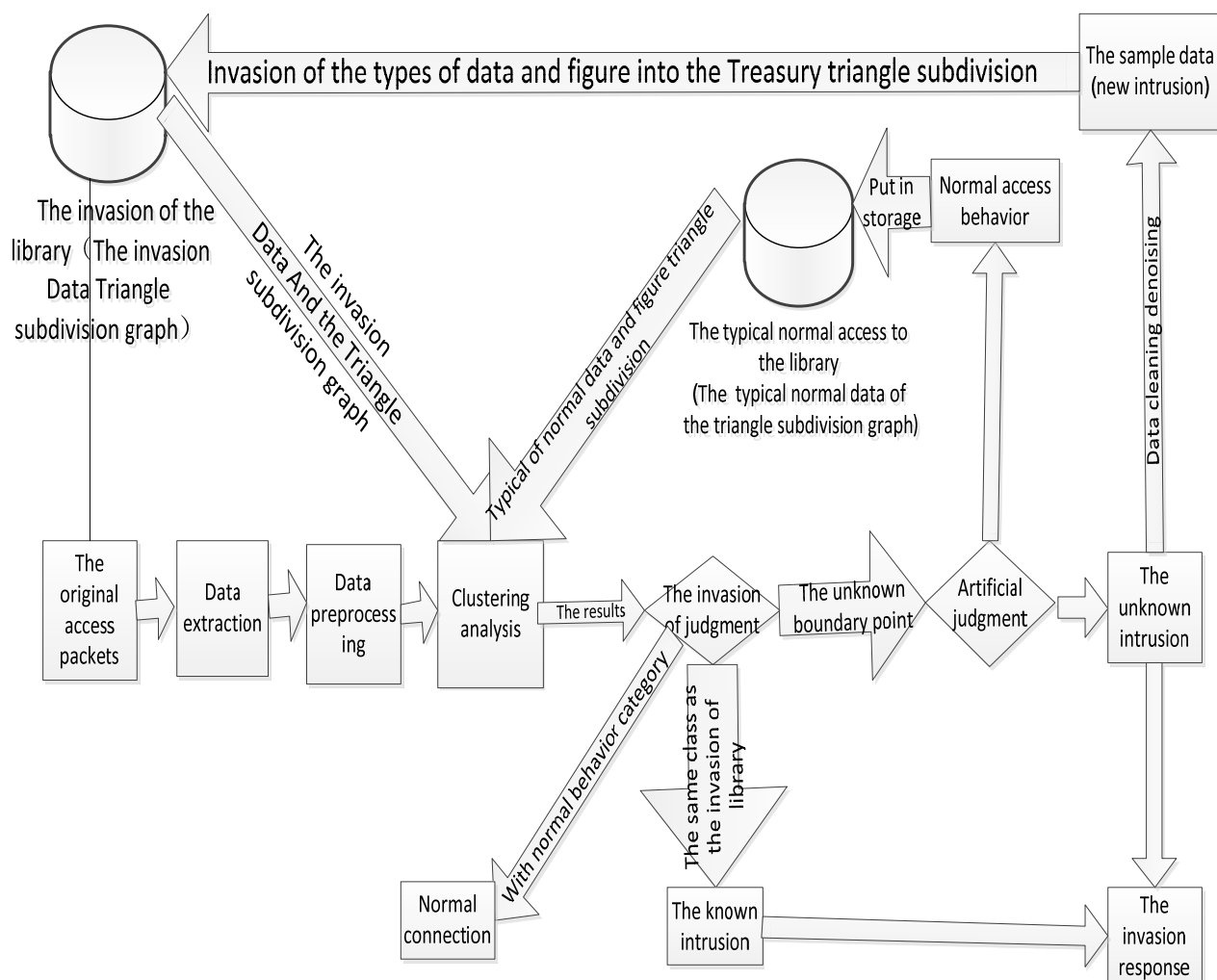


Fig. 1 The overall flow chart of intrusion detection model

Safety status of experimental hospital

In order to verify the effect of intelligent intrusion detection model based on clustering and boundary points detection in hospital information system, the project team worked with the A, B, C three different levels of hospital. A is the Luohe hospital of traditional Chinese medicine, it is in the south of Henan Province is a large-scale financial medical of third-level grade-A hospital, including teaching, research, prevention, care, rehabilitation, B is the fifth people's hospital of Luohe City, it is a set of medical, teaching, research, prevention, rehabilitation in one of three general hospital, C is the third affiliated hospital of Luohe Medical college, it is a Urban secondary general hospital , including teaching, scientific research, prevention and health care. Three hospital information system security measures are shown in the following table:

safety precautions hospital	A	B	C
firewall	with	with	with
VPN Vlan	with	with	without
intrusion detection	with	without	without
log management	with	with	without
Security audit	with	without	without

As can be seen from the above table, a hospital security measures are complete in hospital A, but the intrusion detection is not intelligent. Hospital B and C security measures are less and intrusion detection was not used.

Validation results

In order to not affect the normal operation of hospital information system, effective verification the applying of intelligent intrusion detection model based on clustering and boundary point detection was done in the hospital information system at the same time, the team used alone a server for intelligent intrusion detection system [6]. Configuration of the server: Intel Xeon E5-2420 CPU, 16G memory, 900GSASA hard disk. Each hospital detection time for two months, the results shown in the following table:

	Attack number of times with intelligent intrusion detection system	Attack number of times without intelligent intrusion detection system
A	610	490
B	391	0
C	129	0

From the test results can be seen, the more attack of the number of times the larger hospital at the same time, At the same time, the intelligent intrusion detection system developed by the project team in the case of less manual participation in the detection of the number of the invasion is higher than the ordinary intrusion detection system, and the detection accuracy is high, the false detection rate is low.

Evaluation of experimental hospital

In order to improve the security of hospital information system, and improve the intelligent level of intrusion detection, the hospital work with the team of intelligent intrusion detection technology of the development and application of information security from May to July in 2016, try to use the project development of intelligent intrusion detection system, usage is as follows:

(1) System operation is simple, easy to use, is conducive to the safety of the administrator to learn and use.

(2) Compared with the original detection system in our hospital, the detection accuracy of the system is high and the false detection rate is low.

(3) The system has adaptive learning ability, in the detection process, for known intrusions, no need for manual participation can quickly make the corresponding, and for the new unknown intrusion behavior, can be effectively detected, issued a warning and reported to the administrator.

This system has great application value in the hospital information system security, the project team hopes to redouble their efforts in the detection speed of the system, to further improve the system interface etc.

Summary

This paper introduces the intelligent intrusion detection system based on improved NPRIM algorithm in the application of hospital information security, by introducing the present situation of the hospital, the results of verification, validation, the evaluation of hospital three aspects to introduce the project team in the applications of intelligent intrusion detection system to work in the hospital information system.

Summary and outlook

This study first analyzes the information security of current hospital, intrusion detection system, data mining technology in the application of these three aspects in the field of intrusion detection research present situation and existing problems. On the basis of this, the clustering analysis technology and the application of boundary point detection technology in the field of intrusion detection are studied. Then based on the analysis of comparing the performance of clustering algorithms and the boundary point detection algorithm, the improvement of the existing clustering boundary point detection algorithm NPRIM without parameters, and set up based on clustering analysis and the boundary point detection technology of intrusion detection system model. Finally, the intelligent intrusion detection system model based on clustering analysis and boundary point detection technology is applied to the hospital information system.

This research report on the development and application of Intelligent Intrusion Detection Technology in hospital information security has done a lot of research and demonstration, the main work includes:

1. Research and analyze the research background of the project related to the project, Which mainly includes the hospital information system and its security, intrusion detection system, data mining technology, data mining technology in the application of intrusion detection.

2. The principle, advantages and disadvantages of all kinds of clustering analysis and boundary point detection algorithm are analyzed and compared in detail. These include a detailed analysis of the principle of the boundary point detection method based on partitioning, hierarchical, density, model based clustering analysis method and density based, grid, angle, and the advantages and disadvantages of the boundary point detection method.

3. In research NPRIM algorithm on the basis of the related concepts and NPRIM algorithm, according to the characteristics of the intrusion detection technology, the NPRIM algorithm was improved, and a large number of experiments to improve the results.

4. The application of improved NPRIM algorithm to intrusion detection system, and design a specific model of intrusion detection and clustering boundary point detection based on the experimental environment and the experimental results were compared and analyzed, further validation of the project group based on improved NPRIM algorithm is applied to intrusion detection is effective and feasible.

5. Improved NPRIM algorithm of intelligent intrusion detection system is applied to the hospital in the information security, this research report by introducing the present situation of the hospital, the results of verification, validation, the evaluation of hospital three aspects to introduce the project team in the applications of intelligent intrusion detection system to work in the hospital information system.

Next step

The research level of the project team is limited, and the research on some problems can not be improved. Therefore, the further research can be done in the following aspects.

1. Running speed needs to be optimized, Project development of intelligent intrusion detection system based on NPRIM algorithm in middle and small data set data set on the running speed is moderate, but in large data sets, especially in the larger volume of hospital inside probation, run slower, need to be further optimized.

2. The project team developed intelligent intrusion detection system, the unknown intrusion will be submitted to the security administrator, so that the administrator to deal with, therefore, the system in the use of the need to participate in the initial frequency of more. How to reduce the artificial participation, to further improve the level of intelligent intrusion detection is a direction of the next research.

3. This project is suitable for small and medium-sized hospitals, the project team needs to further study how to improve the performance of the system, it is applied to the large hospital information system.

Acknowledgement

In this paper, the research was sponsored by Medical Science Research project of Henan Province (Project No. 201404065).

Reference

- [1] Rakesh Agrawal, Johannes Gehrke, Dimitrios Gunopulos, etl. Automatic Subspace Clustering of High Dimensional Data for Data Mining Applications. Proc. of the ACM SIGMOD Int'l Conference on Management of Data. Seattle, Washington, June 1998, pp. 94-105.
- [2] Chih-MingHsu, Ming-Syan Chen. Subspace clustering of high dimensional spatiall data with noises[A]. PAKDD 2004, LNAI 3056. 31-40.
- [3] Baozhi QIU, Junyi SHEN. Based on extension and grid density clustering algorithm [J]. Control and Decision, 2006, 21(9):1011-1014
- [4] Baozhi QIU, Junyi SHEN. boundary treatment technology In the grid clustering [J]. Pattern Recognition and artificial Intelligence, 2006, 19(2):277-280
- [5] Estivill-Castro, V., Lee, I., 2000. AMOEBA: Hierarchical clustering basedon spatial proximity using Delaunay diagram. In Proc. 9th International Symposium on Spatial Data Handling, 2000,pp.7a.26-7a.41
- [6] Estivill-Castro, V., Lee, I., 2000. AUTOCLUST: Automatic clustering via boundary extraction for mining massive point-data sets. In: Proc. 5th Internat. Conf. on Geocomputation. Symposium on Spatial Data Handling, pp. 7a.26–7a.41.