http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (23): 7193-7200, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.7193.7200

Research on the Network Security Supervision Practical Guide Mode Based on Network Resource

Gaofeng Luo, Tongcheng Huang and Zijuan Shi
Hunan Provincial Key Laboratory of Information Service in Rural Area of Southwestern Hunan,
Shaoyang University, Shaoyang, 422000, China

Abstract: The problem of network security has attracted the attention of the entire world, because network security problems annually give a lot of network users resulting in loss of life and economic. This study improves the PDRR safety monitoring model and proposes a network security monitoring system model of DOM security data tag tree, finally its model is studied experimentally. Through the study found, DOM security data label tree network monitoring system can ensure the smooth transmission of data which can effectively block the malicious attacks and compared to the previous PDRR, it has good clustering and dividing partition function, improving the efficiency of network security protection. Through the network data transmission security testing, we found that the most obvious effect is the intercept on the IP fraud, before the improved is 18 times and after the improved drops to 1 which verify the effectiveness of network security monitoring system, to provide a theoretical reference for the study of network security monitoring scheme.

Key words: Network security monitoring, DOM data, PDRR data monitoring model, IP fraud, malicious attack

INTRODUCTION

With the rapid increase of network users, the network security problem has become a research focus of current information security research field (Jin and Lin, 2010) Many experts and scholars at home and abroad put forward some solutions for the problems of network security monitoring and one of more common is PDRR safety supervision model, this model is primarily oriented with dynamic time, the spatial distribution traverses each web page node, to protect the network through the encryption and data recovery and other functions (Lin and Qian, 2011; Pu *et al*., 2010; Lu *et al*., 2011). At present, the main problem is lower efficiency of many network securities monitoring system and is prone to vulnerabilities. Based on this, this study proposes a new DOM digital label tree network monitoring model, it will improve the efficiency of network monitoring through the data clustering and dividing and the effectiveness of the safety supervision system is also verified by experiment.

COMPUTER SECURITY SUPERVISION RESEARCH

Network security problems have attracted national attention. For the network security problem, this study mainly deals Asia region to launch a research, at the same time network attack categories are also summarized (Wang and Zhang, 2011).

Network security research: According to the international consulting service agencies newly released data, it shows that there are more than 70% Asian companies that have been subjected to network security attacks, in which the most serious attack project is divided into five analogy, including e-mail, web forums, communication equipment, multimedia tools, data sharing etc (Wang and Zhang, 2011; Xu and He, 2011). In view of the different enterprise, the five attack projects launch the research of computer internet security systems. Finally, data are carried out the analysis of mathematical statistics as shown in Fig. 1.

In Fig. 1, it can be seen that not taking any measures' enterprises have reached 21.8% and only 5% enterprises

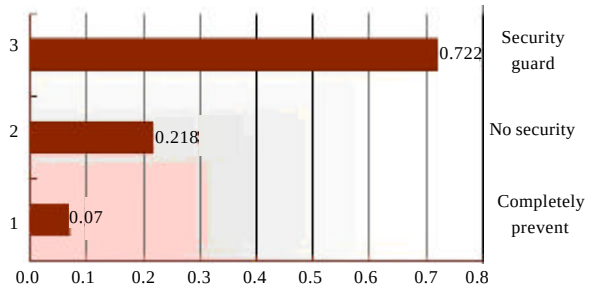

Fig. 1: Investigation results of Asian companies network monitoring system

Corresponding Author: Gaofeng Luo, Hunan Provincial Key Laboratory of Information Service in Rural Area of Southwestern Hunan, Shaoyang University, Shaoyang, 422000, China

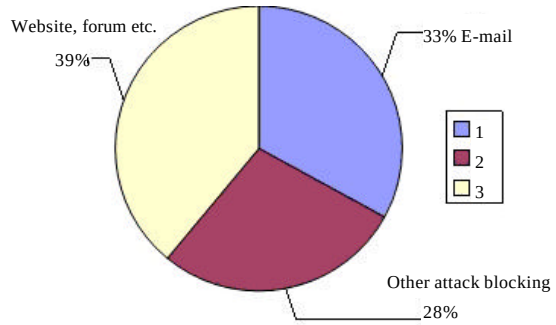

Fig. 2: Effectiveness of safety measures

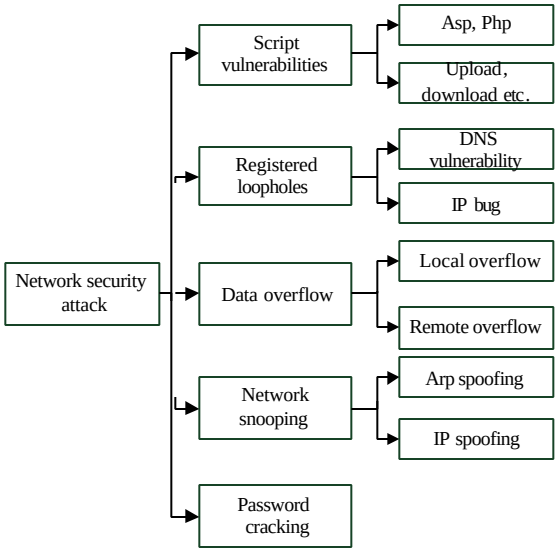

Fig. 3: Network security attack classification

have received considerable attention to five attack analogies, the remaining enterprises only carry out prevention for a network security attacks analogy.

Figure 2 shows the investigation results of network security monitoring system, we can be seen that after the implementation of network security measures, there are more than 39% for the interception rate of website and forum malicious attack, there are more than 33% for the interception rate of e-mail malicious attacks and the interception rate of other categories attacks are 28%. For the network virus attacks, there are a variety of forms. Through the investigation, the forms of attack are summarized as follows.

It can be seen from Fig. 3, the main types of network security attacks are divided into five categories, in which the security threat level of scripting vulnerability, registered vulnerability and network Qiekui are relatively high, so we should take safety precautions, to prevent the harm of malicious network attack (Liu and Meng, 2013).

Fig. 4: Schematic diagram of PDRR model

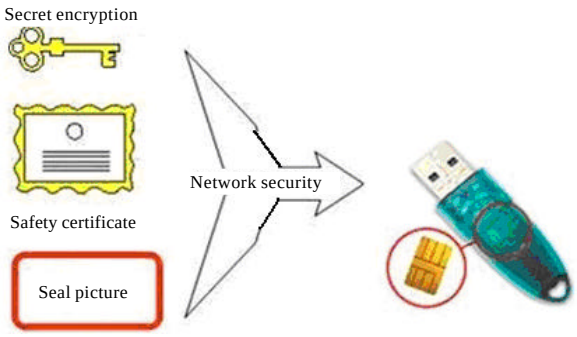

Fig. 5: Network security measures

Network security monitoring system: Network security monitoring system has many kinds, the most commonly used is the PDRR model based on time dynamic, it can use the form of encryption and recovery to carry out the protection of database (Kiewitz *et al*., 2012; Ho and Le-Ngoc, 2012). After the main principle of PDRR carries out the traversal of data, data can be restored when they destroy the attacks as shown in Fig. 4.

In addition to Fig. 4 describes the guarding model of network security, there are also safety certificate, digital signature and other many measures, to protect the safety performance of network as shown in Fig. 5.

From the above analysis, we can see that network security measures are mainly concentrated in the interception of the malicious attack and data encryption. However, if data encryption and data recovery function uses the ordinary algorithm, they will result in low efficiency, validation error etc. The network security system is improved as shown in Fig. 6.

It can be seen from Fig. 6, this study uses the DOM numerical model in the computer security monitoring system, to establish the computer security system.

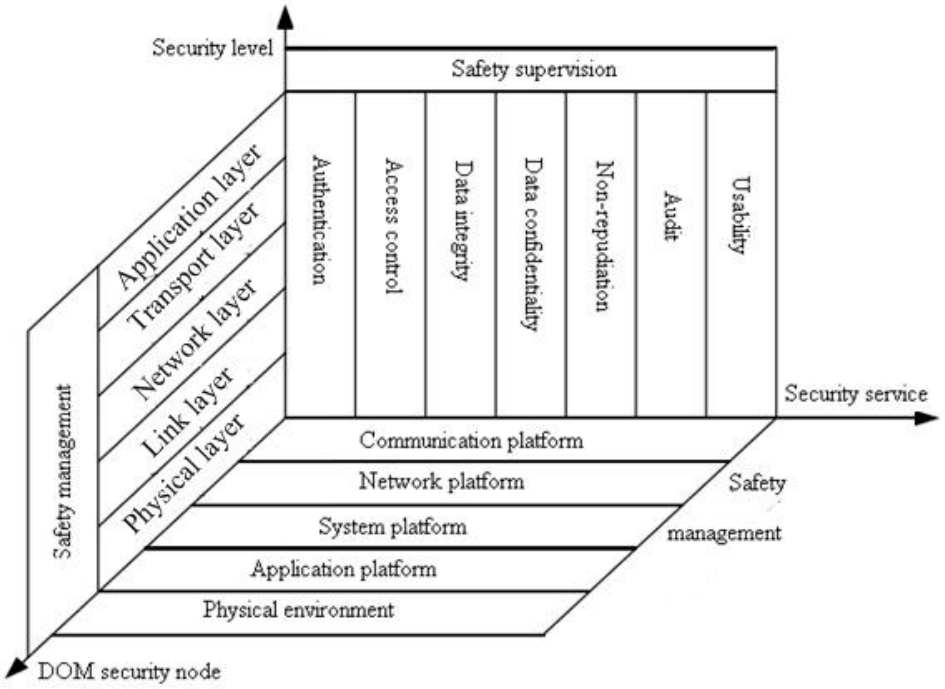

Fig. 6: Computer security supervision coordinate model

COMPUTER SAFETY MONITOR SYSTEM MODEL

Computer security monitoring model's establishing idea mainly depends on the Internet node link database to solve the security problem. Through the data model of DOM tag number, the network security supervise system is improved.

Safety supervision system clustering model: Web clustering structured framework model is the focus of study and this study uses the Libwww database that is the page analysis database provided by W3C. When the network is subjected to virus attacks, network security monitoring system needs to extract the tag feature data engine. DOM tag tree is the best model of data traversing, it can carry out regional block analysis for the each node of Internet engine and finally its integrating results will be returned from the system. The safety supervision clustering model is shown in Fig. 7.

ASP, PHP and JSP are the main basis of currently generation Internet web page code, another is form of a static HTML language generation and these languages are marked with labels which can be modified for the page through a certain form. In order to detect page needs, we can go through the system labeling and detection on the label, finding webpage page existing vulnerabilities. We can use the relationship between brothers and father and son that is said the parallel and nested relations in label, the number of tags is shown in Eq. 1.

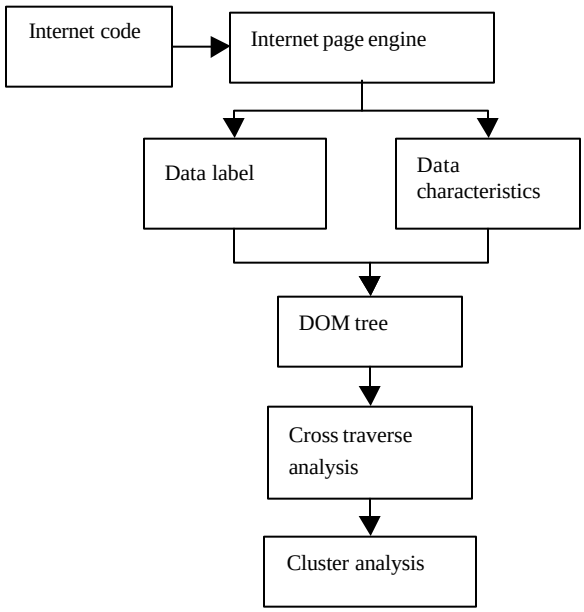

Fig. 7: Network security supervise clustering model

$$BIG\text{-}THREE = (U, R) \quad (1)$$

Among them, the node of labels tree can be expressed in U; the relationship between labels can be expressed in R, through a systematic data analysis of Internet web pages, we can get the DOM tag tree.

Regional block partition: For the information of Internet pages, it can carry out the feature classification panel through the information characteristics, the feature same or similar components can be carried out block statistics. According to the block feature, feature module can be expressed as shown in Eq. 2:

$$S = (B, L) \quad (2)$$

In which, S is the page block features; B = (B1, B2,...Bn) is said block collection.

Definition 1: The number of DOM cross label nodes is block combination for:

$$P = (P1, P2,...Pn) \quad (3)$$

In Eq. 3, Pi has the data set of similar or identical characteristics node, $PNi \cap PNj = PN$:

$$PN1 \cup PN2 \cup ..... \cup PNj = \phi(i \neq j)$$

Definition 2: After the regional blocking, clustering labels can be written as the feature similar or same tag set in different blocks which is expressed as:

$$Ci = (PNi, R), i <= n \quad (4)$$

In Eq. 4, R denotes the similar characteristics value set of different blocks.

The main algorithm of clustering nodes' extraction and block are as follows:

```
Get_Node-Feature (Node) {
If (Node.BUG = NULL)
Extract Node Feature from NODE
ELSE
Extract Node Feature from NODE of Node.BUG
endif
}
AreaPartition (BUG—Tree) {
Relevance,
Areald =1
For each Leaf Node of BUG—Tree
IfNode.bProcessed == false
ListTreeAndGetArea (Node)
Else
Continue
Endif
Endfor
      }
```

RLC crawling algorithm: Q-Learning algorithm is a computer security monitoring system that can strengthen memory detection algorithm, in which it can estimate the tag tree function with Q (f, h) and state as well as action value, the error between the two memories is reduced by iterative method. The basic expressions can be represented as shown in Eq. 5.

$$Q_y(f,h) = R(f,h) + \alpha \sum T(f,h,f_t) \max_{h_t} Q_y(f_t,h_t) \quad (5)$$

In which, Q_y expresses the optimal return value when found loopholes h in the optimal mode f. The definition of optimal supervision function value is V_f, choosing the best strategy θ when the network is the way of f. So, there are:

$$V_f = \max_h Q_y(f,h) \quad (6)$$

Optimization strategies are shown in Eq. 7:

$$\theta = \arg\max_h Q_y(f,h) \quad (7)$$

When the conversion coefficient $\alpha = 0$, it is called immediately optimal return value, the optimal value is not affected. The expression formula is shown in Eq. 8.

$$Q_y(f,h) = R(f,h) \quad (8)$$

When $0<\alpha<1$, it can be the optimal value of future returns, Internet web webpage has certain influence on later link, it is shown in Eq. 9:

$$Q_y(f,h) = R(f,h) + \alpha \sum T(f,h,f_t) * \max_{h_t} Q_y*(f_t,h_t) \quad (9)$$

According to the Fig. 8, it can be seen that the main algorithm of RLC capture is as follows:

```
Initialize:
set the lowest return: R
Input:
queue of URL
for each URL in queue do
massage = Query( URL);
If FormExist(massage) == TURE
form = ExtractFonn(massage );
RecordFonii(term);
end if
urlset = ExtractUrl(massage );
```

STUDY ON THE ACTUAL PRACTICE OF COMPUTER SECURITY SUPERVISION

In order to verify the proposed DOM digital tree safety monitoring system, this study uses the

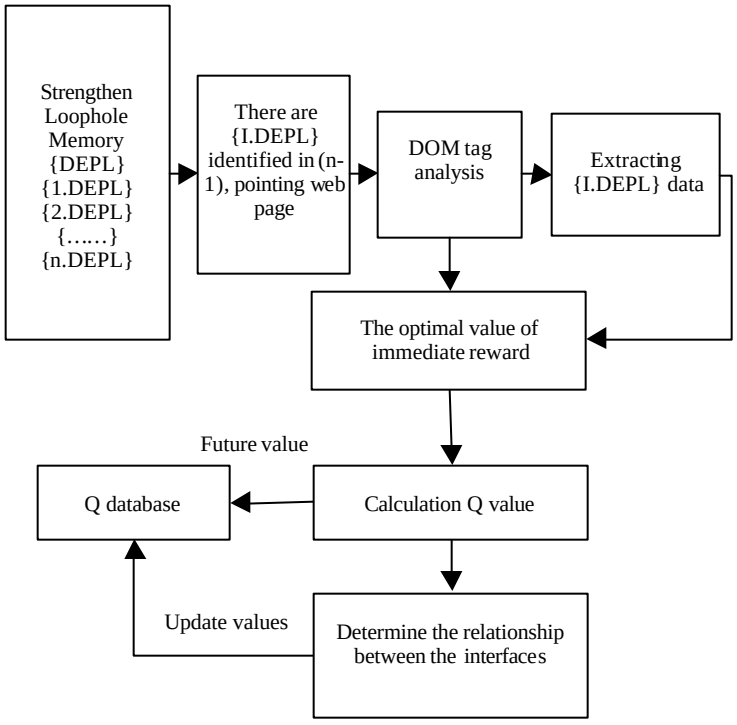

Fig. 8: RLC extraction model

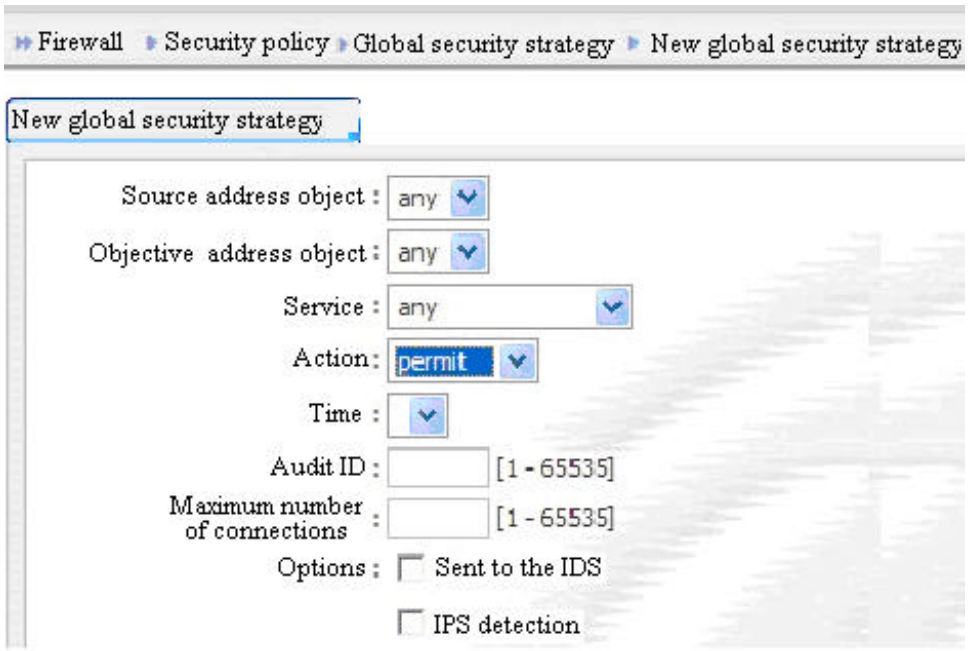

Fig. 9: Schematic diagram of VPN and firewall function

DCFW-1800S UTM software in the verification experiment, the software's most important function is VPN and firewall. The configuration is shown in Fig. 9.

In order to verify the functions of DOM digital tag tree in VPN, its interface needs to modification. By adding adaptive model DOM digital label number

Physical interface | VLAN interface | VSI interface

#	Name	Interface state	IP/ bit mask	Security domain	Link mode	Working mode	Management IP
1	eth0			l2-trust	Adaptive	Transparent	
2	eth1			l2-untrust	Adaptive	Transparent	
3	eth2				Adaptive	Route	
4	eth3				Adaptive	Route	

Fig. 10: VPN digital label tree interface

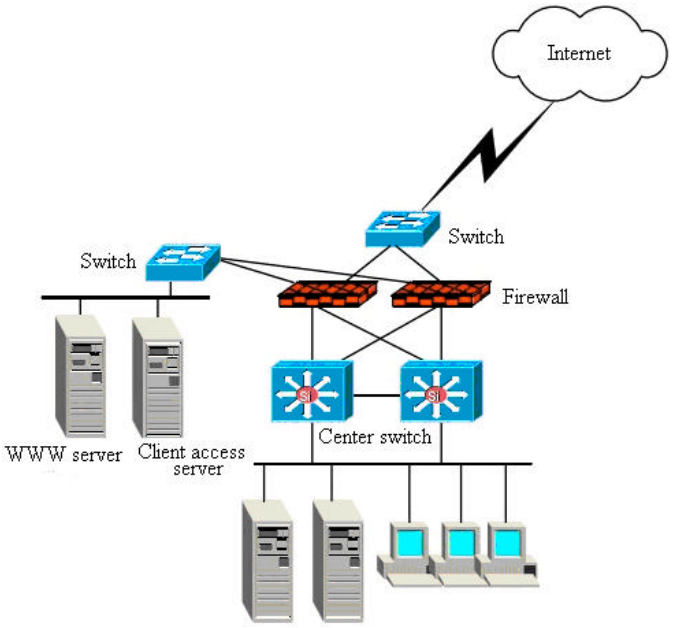

Fig. 11: Network topology

strategies, in which act is only permitted by the "permit", refusing "deny", it is shown in Fig. 10.

In order to improve the general applicability of experimental performance and proving network monitoring system, the safety supervision system is divided into three parts, including firewall system, VPN system and other auxiliary safety system. In this system, the study join up 4 gigabit network interface, network topology can be represented as shown in Fig. 11.

It can be seen from Fig. 11, the four interfaces as a unit can configure a DOM digital label number VPN firewall which respectively connect Internet through web and internal network through the center switch. The network interface of two firewalls is connected by a switch and external network.

The connection diagram of VPN and computer is shown in Fig. 12. After connecting the VPN and computer, they need to allocate static address, so we can pass the IP test to see whether VPN is connected to the computer. Through the test experiment, IP address 210.34.212.2 is assigned by VPN, we can see that the VPN are successfully connected by computer.

In order to verify the universal property of safety supervision system, this study selects different industries' all kinds of network to carry on verification. Through the improvement of network security monitoring system, before and after test improvement's data transmission situation, finally we can get the curve as shown in Fig. 9 and Table 1.

It can be seen from Fig. 13, after PDRR scheme is improved, it has greatly improved for the protection function of data transmission. With the change curve of time, the improved scheme allows data to be stationary transmission.

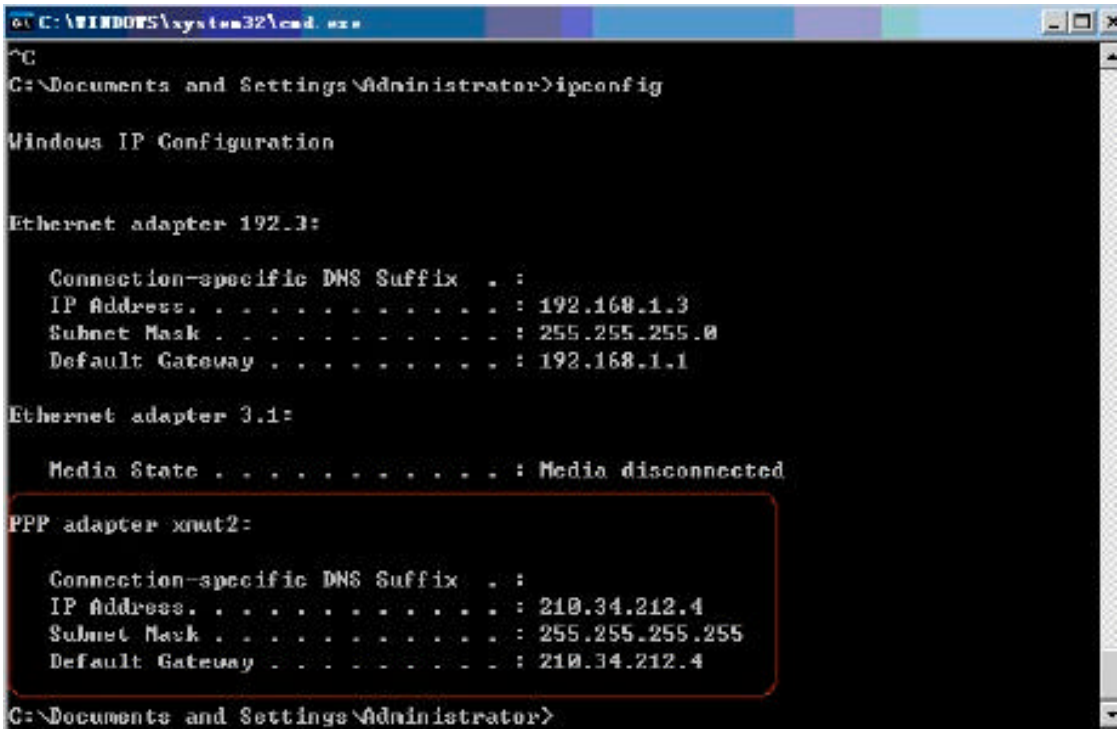

Fig. 12: Schematic diagram of the VPN link

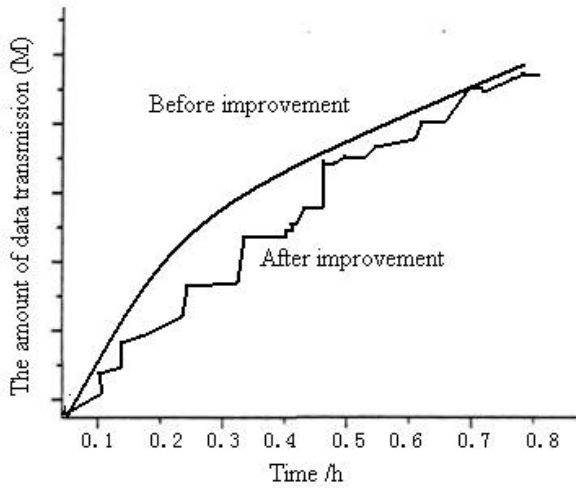

Fig. 13: Amount of data transmission with the time change curve

Table 1: Number and types of network supervision

Type of website	Number
Government network	30
Enterprise network	20
School network	40
Home network	50
Public network	10

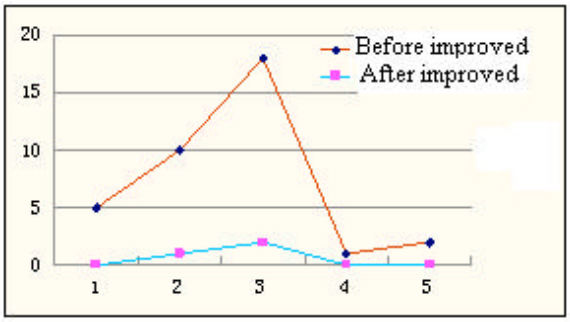

Fig. 14: Effect comparison chart

Table 2: Effect Table of supervision system after the improved

Attack name	Before improved system	DOM monitoring system after improved
ARP attack	5	0
IP conflict	18	1
Server crashes	10	2
Access interrupt	1	0
Access slow	2	0

In this study, the network security system of an enterprise is improved and DOM data tree scheme is applied to the network security monitoring scheme. After the scheme is implementation of 1 month, the effectiveness of program implementation will be drawn in Table 2 and Fig. 14.

From the Table 2 and the effect of comparison Fig. 14, they can be seen that DOM digital label tree network security detection system has much better than before improved for the interception performance of malicious attacks, in which the most obvious effect is the IP fraudulent interception, before improved is 18 times and after the improved drops to 1, this system has very good safety protective effect.

CONCLUSION

This study presents a DOM digital label tree network security monitoring scheme based on network resources, the effect test of supervision system is verified by computer network attack interception. Through the experiments verified, after the PDRR scheme is improved, the protection function of data transmission has greatly improved. With the change curve of time, data transmission quantity can be seen that the improved scheme allows data to be stationary transmission. For the effect of network interception, the most obvious effect is IP interception attack, before the improved is18 times, after the improved drops to 1, ARP attacks are reduced to 1 by 5 times, server crashes are reduced to 5 times by 10 times, access interrupt and access slow are respectively reduced to 0 times by 1 and reduced to 0 times by 2 times, they are no attack server access.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their helpful advices to improve this study. This work was supported in part by a grant from the Construction Program of the Key Discipline in Hunan Province of China and the Key Scientific Research Program of Department of Education of Hunan Province (NO.13A091).

REFERENCES

Ho, Q.D. and T. Le-Ngoc, 2012. Smart Grid Communications Networks: Wireless Technologies, Protocols, Issues and Standards. In: Handbook of Green Information and Communication Systems, Obaidat, M.S., A. Anpalagan and I. Woungang (Eds.). Academic Press, New York, pp: 115-146.

Jin, B. and J.J. Lin, 2010. Review of intrusion detection technology. J. East China Univ. Sci. Technol., 1: 45-46.

Kiewitz, C., S.L.D. Restubog, T.J. Zagenczyk, K.D. Scott, P.R.J.M. Garcia and R.L. Tang, 2012. Sins of the parents: Self-control as a buffer between supervisors' previous experience of family undermining and subordinates' perceptions of abusive supervision. Leadership Q., 23: 869-882.

Lin, M.J. and H.L. Qian, 2011. Intrusion detection system: Principle, intrusion hiding and countermeasures. Microelectron. Comput., 31: 102-103.

Liu, R.S. and X.H. Meng, 2013. Design and implementation of identity authentication system based on PKI. Manuf. Automation, 20: 112-113.

Lu, H.Q., F. Wang and Y. Song, 2011. The damage assessment system based on combating simulation. J. PLA Univ. Sci. Technol., 10: 139-143.

Pu, Y.F., W. Zhang, S.H. Teng and H.L. Du, 2010. The cooperative network intrusion detection based on decision tree. J. Jiangxi Normal Univ. (Nat. Sci. Edn.), 34: 302-307.

Wang, H.M. and Y. Zhang, 2011. Research on the model of joint operations simulation situation data. J. Syst. Simul., 20: 4186-4188.

Xu, Z.M. and J. He, 2011. The design and implementation of battlefield situation 3D graphics simulation system. Comput. Appl., 29: 313-316.