2009 International Conference on Environmental Science and Information Application Technology

# The Design of an Active VoIP Security Defense Model Based on Dynamic Self-adaptive Diffluence

Zhaoyang Qu[1,2]
1: North China Electric Power University,
Baoding City, Hebei Province, China
2: School of Information Engineering,
Northeast Dianli University,
Jilin City, Jilin Province, China
E-mail: qzywww@mail.nedu.edu.cn

Wei Yang
School of Information Engineering,
Northeast Dianli University,
Jilin City, Jilin Province, China
E-mail:yw4198126@126.com

*Abstract*—**This paper designs an active Voice over Internet Protocol (VoIP) security defense model, aiming to cope with various attack problems that the network is confronting. Based on the model, a dynamic self-adaptive diffluence algorithm that can be applied to the VoIP Gateway was proposed. It combines advantages of UBS selection strategy and weighted Bayesian classification algorithm, the algorithm can accurately, quickly complete the task of intrusion detection through using few high-quality training sample for learning. Experimental results demonstrate the algorithm is more accurate under the smaller training set.**

*Keywords-VoIP; active security defense model; dynamic self-adaptive diffluence algorithm; network security*

## I. INTRODUCTION

VoIP is a voice communications technology based on IP inter-connection, VoIP applications are emerging today as an important component in business and communication industry. With the rapid development of the internet technology, it is becoming more and more outstanding in application for the problem of network security [1]. The security threats to VoIP network mainly include Denial of Service (DoS) attacks, invalid access, toll fraud, eavesdropping and sending SPIT [2] et al. At present, there are the following three aspects in the major measures of VoIP: (1) keeping VoIP network and data network separate, it is the most effective action to minimize the risks, (2) encrypting the data packet and authenticating the traffic, which can protect the conversation from attack, and (3) using firewall and intrusion detection system to assure VoIP security. At present, the solutions require sacrifice some related performance to ensure safety, the most of defensive measure is passive defense, the encryption measure needs a process of coordination in different manufacturers and the most of intrusion detection methods [3] are based on data mining algorithm, such as the intrusion detection model based on Support Vector Machine (SVM) algorithm and the intrusion detection method based on multi-classification support vector machine, all of the testing results are better in some extent, but they depend on a larger training data set. Actually, it is a demanding task for searching network attack and marking them for training, because it is time-consuming both in terms of the human resources and physical resources.

In order to solve the problems of the defensive measures and assure VoIP network safety, an active VoIP network security defense model is designed. Simultaneously, there are still some unresolved and scarcely addressed classifiers to model the attack patterns, the data acquisition task is always time-consuming and greatly relies on the domain experts [4] et al. A dynamic self-adaptive diffluence algorithm that is designed can classify alarm messages effectively and has also its own advantages to reduce the sample complexity.

## II. ACTIVE VOIP NETWORK SECURITY DEFENSE MODEL DESIGH

In order to find out the safety risk and threats quickly, an security network is required to respond quickly to the attack behavior. An active VoIP network security defense model is shown in the Figure 1.

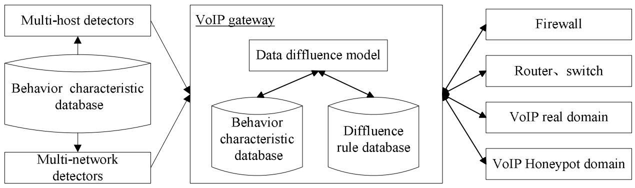

Figure 1. Active VoIP network security defense model.

The basic idea of the security defense model use multi-intrusion detection systems to cooperate. Through intrusion detection, intrusion deception, hole-scanning security problems can be found in time. It can provide evidences that make the

Fund Project: Grants of Jilin Provincial Technology Development project (No.20080322); "The Eleventh Five-Year Plan" Science and Technology Education research project of Jilin Provincial Department of Education (2008 (41) ) .

978-0-7695-3682-8/09 $25.00 © 2009 IEEE
DOI 10.1109/ESIAT.2009.88

system respond more quickly, so that the system will be transformed from static defending to dynamic protection. When any abnormity appears, it can be respond quickly according to the security strategy.

VoIP gateway is the core of the whole defending model. It is an interface between IP network and telephone network. We can connect IP gateway via Public Switched Telephone Network (PSTN) local loop, it is responsible for transitioning analog into digital signals, compressing the packets, transferring the IP packet speech signal over the internet, then traveling through the internet to called party side, it is unpacked, unzipped, decoded and reverted to recognize analog voice signal for IP packets by VoIP gateway. Finally, it can be sent to the called party side via PSTN [5]. All the traffics that intend to enter into VoIP real domain should be checked to achieve the destination. The prototype of data diffluence module on the VoIP gateway are mainly responsible for diffluence of message according to certain strategies, the strategies of diffluence are to determine whether the visiting is normal or not according to the checking of data packets. If it is normal visiting, the data packet will be transmitted to VoIP real domain. Otherwise, data packet will be sent to VoIP honeypot domain. A honeypot has a specific value in attack detection and deflection [6]. The honeypot concept can become very useful as specific component of an active VoIP network security defense model. It is completely logically and physically separated by the real one where we continuously monitor activity. Physical separation is necessary in order to avoid that an attacker breaking into the VoIP honeypot domain.

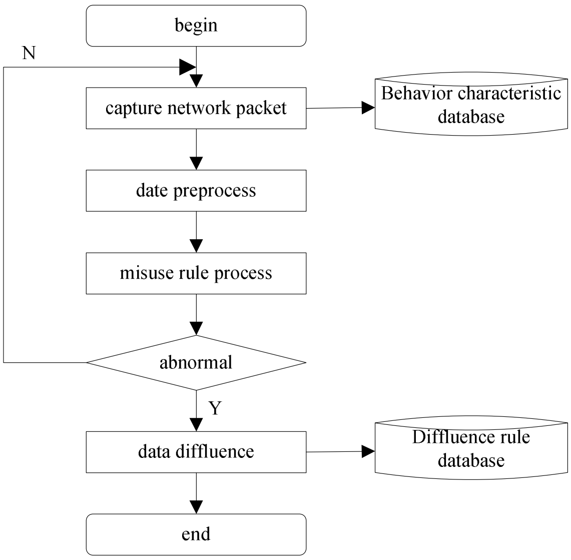

Figure 2. Data diffluence procedure.

Date diffluence procedure is shown in Figure 2. Capturing packets on the VoIP network, it will implement intercept and analyze them and write behavior characteristic into database. The original captured data packets need to be processed further by using data preprocess module, including the packet of decoding, slicing and mattering rearrangement, filtering the inaccurate and the same data, and then producing related characteristic value as input value of the misuse rules processing module. The module of misuse rule processing implements misuse detection based on rules, when the module detect attack behavior to send directly to result. If not, data packet will be sent to the data diffluence module, and determine whether the packet is normal or not, and process the result in the end.

## III. DYNAMIC SELF-ADAPTIVE DIFFLUENCE ALGORITHM REALIZE

In order to deal with suspicious traffic more reasonably, a dynamic self-adaptive diffluence algorithm that can be applied to the VoIP Gateway was proposed. The idea of the model is to realize data of diffluence through the self-adaptive, dynamic and circulatory in the classification of training samples learning process, it can be realized in three steps:

Step 1: In order to distinguish between the abnormal traffic from normal [7], this paper selects the training data set in alarm database and marks it, the selection of the selector functions is based on UBS selection strategy. The concrete process is as follows.

*1) using n-dimensional feature vector table* $X=\{x_1,x_2,\ldots,x_n\}$ *of to describe the properties of the sample data. Determined k classifications* $C_1,C_2,\ldots,C_k$ *given an unknown sample X, bayesian classification will take the unknown samples to* $C_i$*, if and only if*

$$P(C_i\mid X)>P(C_j\mid X),1\le j\le k,j\ne 1 \tag{1}$$

*In the former formula,* $C_i$ *is the largest of* $P(C_i\mid X)$ *called the largest posterior hypothesis. By definition the bayesian*

$$P(C_i\mid X)=\frac{P(X\mid C_i)P(C_i)}{P(X)} \tag{2}$$

$P(C_i)=s_i/s$ , $s_i$ *is sample size of* $C_i$ , $s$ *is samples amount, so only compute maximum value for* $P(X\mid C_i)$.

*2) According to independent the conditions of n properties and to get*

$$P(X\mid C_i)=\prod_{k=1}^{n}p(x_k\mid C_i) \tag{3}$$

*The probability of* $P(C_1\mid X_i),P(C_2\mid X_i),\ldots,P(C_n\mid X_i)$ *is evaluated by training samples, in* $P(X_j\mid C_i)=s_{ij}/s_i$, $s_{ij}$ *is training samples amoun of* $C_i$ *in* $A_j$ *property and the value is* $x_j$, $s_i$ *is the training samples amoun of* $C_i$.

*3) Each value of P and sample probability size phase correspondence, the values of P are ordered by descending* *and the two highest values: $P_j$ and $P_k$ . It can be get suppose $P_j > P_k$, so the final classification result is j class. $P_j$ shows the sample's credibility of j and $P_k$ shows the confidence. When the $P_j$ gets bigger and $P_k$ gets smaller show the classification result accurate and reasonable, make $P_j$ close to 1 and make $P_k$ close to 0 possibilities. When using the P-value pair, there are four possibilies as follows:*

*a) When $P_j$ is high and $P_k$ is low: the predictable result shows that credibility and confidence are both higher.*

*b) When both of $P_j$ and $P_k$ are high: the predictable result shows that confidence higher and credibility lower.*

*c) When both of $P_j$ and $P_k$ are low: the predictable result shows that confidence lower and credibility higher.*

*d) When $P_j$ is low and $P_k$ is high: the predictable result shows that credibility and confidence are both lower.*

*The a) is the most accurate and certain in the predictable result and When $P_j \approx P_k$, the result is the worst. According to the UBS selection strategy, adjust the P-value pair dynamically, use the selector functions as follows:*

$$C(i) = \left|P_j - P_k\right| \tag{4}$$

*$C(i)$ is absolute deviation degree for P-value pair, when $C(i)$ is a very small real number and close to 0, indications show that the classification is the most accurate result, mark the sample and then learn the next.*

Step 2: During the implementation of the algorithm, we often need to use corresponding strategies to end it. The purpose is to reduce the sample selection of the execution time and so that the sample set achieve the best learning effect after the algorithm is suspended. The Mean Squared prediction Error (MSE) is used for conference index, and aimed at predication function $f^*$ that is the training set $T$ under the test sample $x$ . The MSE can be defined as follows:

$$MSE\left(f^*(x,T)\right) = bias^2\left(f^*(x,T)\right) + \text{var}\left(f^*(x,T)\right) \tag{5}$$

$bias\ \left(f^*(x,T)\right) = \left(f\ (x,T)\right) - E\left(f^*(x,T)\right)$ , $f$ is bayesian classification algorithm and $bias$ function reflects selected sensitivity the training set $T$ for the predication function $f^*$, the value is the square of the predictable classification subtract from actual classification of all the samples in the test sample $x$ , the function var shows the sensitivity the predication function for the training set $T$, and the value grows with the training set choice. In order to get lower MSE, we need to get low-bias and variance.

Step 3: When P is determined, we can get the classification model which had been constructed by training. Select the test data from the alarm database and component the test group $T$. The correctness testing were selected randomly to the test sample $x$ from $T$ , the model for forecasting generated in each classifier $C_i$ send to the voting module, the class of the most vote-getting as the classification, and then make the weigh plus 1 which is the classification corresponding the same classification method belong to $x$ . The step 3 repeated until the finally classification model is produced.

## IV. Experiment And AnAlysis

The dynamic self-adaptive diffluence method assure availability in training effect, simplify the training set and high-efficiency intrusion detection. When the same higher detection accuracy of intrusion detection conditions, the result of compared the sample number with dynamic self-adaptive diffluence method and random sampling method, as it is shown in Figure 3. Which they are the KDD Cup 1999 data sets has about 490000 data records. Under 99.6% detection accuracy of intrusion detection condition extracting 1980 normal data and 8996 attack data, dynamic self-adaptive diffluence method needs about 50 samples but random sampling method needs about 2000. This result demonstrate dynamic self-adaptive diffluence method is more availability under the circumstances that the smaller training set.

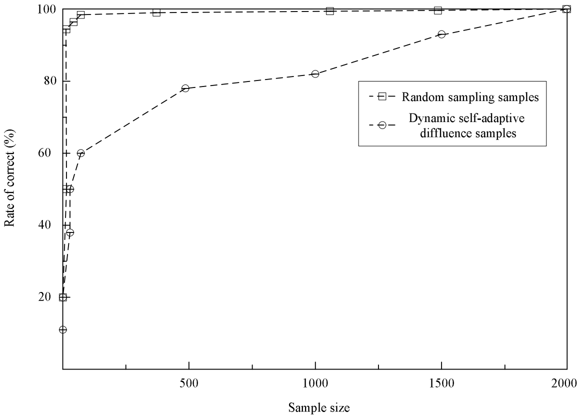

Figure 3. Experimental result.

In the process, it selects training samples at first, then uses the sample set complete the intrusion detection task. Along with the constantly changes of network traffic and the quality of the training samples changed, we need dynamic self-adaptive diffluence method to reselect the training samples, ensuring the quality of the sample and the performance of the related classification algorithm.

## V. CONCLUSION

This paper designs an active VoIP security defense model, and multi-intrusion detection systems that can be cooperate and complement to improve the security performance of the whole

VoIP network. The dynamic self-adaptive diffluence algorithm is applied to the VoIP Gateway that can select the training data and reduce the sample size, so it has greatly reduced the use of human resources, physical resources and computation. Experimental results show that this algorithm is more accurate under the smaller training sets. According to the actual application, the proposed method is needs to be improved and perfected in future.

## REFERENCES

[1] U. Roedig, R. Ackermann, R. Steinmetz. "Evaluating and imporoving firewalls for ip-telephony environments," in 1st IP telephony workshop, Berlin, Germany, April 2000.

[2] H. Abdelnur, R. State, I.Chrisment, C. Popi. "Assessing the security of VoIP Services," In the 10th IFIP/IEEE Symposium on Integrated Management (IM 2007), Munich, Germany, May 2007.

[3] J. P. Rouillard, "Real-tile Logfile Analysis Using the Simple Ecent Correlator (SEC)," In 18th USENIX System Administration Conference Proccedings, November 2004.

[4] Mohamed Nassar, Saverio Niccolini, RaduState, and ThiloEwald, "Holistic VoIP Intrusion Detection and Prevention System," In Third annual security workshop (VSW07).ACMPress,June2007.

[5] Supchai Tangwongsan and Labhidhorn Pangphuthipong. "A Model of Network Security with Prevention Capability by Using Decoy Technique," International Journal of Electrical, Computer and Systems Engineering, vol.1, No.4, 2007.

[6] M. Nassar, R. State, O. Festor, "VoIP Honeypot Architecture," In Proc.of 10th..IEEE/IFIP Symposium on Integrated Management,June 2007.

[7] T. Porter, "Practical VoIP Security," 800 Hingham Street, Rockland, MA02370: Syngress Publishing, March 2006.