International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

Prediction of Network Security Based On Grey Theory Technique

Abhijeet V. Sagare , Mr. S.K. Pathan
[1] *M.E.student , Computer Department , SKNCOE Pune , Maharashtra, India*
[2] *Asst. Professor , Computer Department, SKNCOE Pune , Maharashtra , India*

Abstract - ***Network Security situation is the important part of any wired or wireless network. Network intrusion attacks, threats are increasing day by day. Whole network security status includes current situation evaluation and to forecast future situation.***

This paper presents network security situation assessment and prediction. The objectives are to present security situation assessment scheme to assess current network security status, to design Grey Verhulst mechanism to forecast incoming network security situation and to identify the salient asset in the network. This proposed system is expected to reduce the possibility of taking action against false alerts. The findings of this research are projected to significantly rise up the network security.

Key Words: *network security situation, situation prediction, grey theory, grey Verhulst model*

1. INTRODUCTION

Nowadays computer network has become integral part in any organization providing services and information sharing. The number of Internet users worldwide has reached in millions which has made network to undergo viruses , threats. Due to the increasing number of the threats, its very difficult to ignore the current security situation and its future prediction. Endsley introduced the "Situation awareness (SA)is the perception of the elements in the environment within a volume of time and space". In 1998, Heu wei [1] introduced the SA process into network security field, and put forward cyberspace network problems. Furthermore, Dong [7] discussed the related issues and introduced the grey theory into the network situation prediction. The network security situation evaluation system (NSSES) developed by BIT-ISA Lab provided the situation evaluation and prediction for users.

viewing at the limitations of existing system's in the prediction model based on conventional grey verhulst model, this paper presents robust framework for forecasting of network security and gives alert to n/w admin to take efficient remedies against threats.

1.1 Basic Concept

Network Situation awareness is defined as change of critical assets in network within a time and space interval, the understanding of those assets mean according to the operator's goals and the projection of their status in next interval (Endsley, 1988). In other words, the concept of Network Security Situation (NSS) actually originates from situation awareness . Based on Rongzen Fan et al [4], a security situation can be referred as to which extents of the network devices have been compromised . In computer network, NSS Awareness can be defined as the forecasting of future network security. In general, situation awareness can be divided into three phases which are event detection, current situation assessment and future situation prediction (Endsley, 1995). These phases can be adapted in NSS Awareness.

phase 1: Threat detection is a basic process of situation awareness. This stage mainly to identify the abnormal and malicious activity in the network and translates them into logical format.

phase 2: Current Situation evaluation is a process to evaluate the security situation of the entire network by using the information obtained from the detected alerts in previous stage.

phase 3: Future Situation forecasting is aimed to forecast the future network security tendency according to the current and historical network security situation status

Grey theory was invented by Deng in 1982. It makes use of sequence generated by accumulated generating operation (AGO) for reducing the randomicity existing in the original data sequence. The measure makes to find out the variation in the sequence and use the regularity to forecast

Presently, grey theory is widely used for priorities because it captures dominance at small data sample and better precision in short-term period forecasting by dong[7].

2. Verhulst Model

It is a non-linear differential equation

$d / dt [p(t)] = x\, p(t) - y [p(t) * p(t)]$

where x ,y are model constants

p(t) is original data sequence

2.1 Accumulated Generating Operation (AGO) :

Serve the sample data of network, collected from admin as original input data set given below.

$V(0) = \{ V(0)(1), V(0)(2), ..., V(0)(n) \}$

Then, a new accumulated row matrix $V(1)$, generated by the first-order Accumulated Generating Operation (1-AGO) as

$V(1) = \{ V(1)(1), V(1)(2), ..., V(1)(n) \}$

$V(1)$ is called the 1-AGO of $V(0)$.

$$V_{(1)(1)} = V_{(0)}(1)$$

$$V_{(1)(i)} = \sum_{k=1}^{i} V_{(0)}(k)$$

For all i = 1,2,...n

Then the grey Verhulst model is achieved as ,

$d/dt [V(1)(k)] + a\, V(1)(k) = b [V(1)(k)]$

where a is constant and b is grey input

3 . Proposed System

As previously stated, it requires to develop a robust and efficient system for evaluating the current security situation and forecasting the future situation based on current and previous security situation which obtained from detected intrusion alerts. The **specific characteristics** of this proposal are as follows.

1. Network security situation evaluation module to assess the current security status of the network.
2. A modified Grey Analysis algorithm in identifying the most salient asset in the network.
3. To design Grey Verhulst prediction mechanism to forecast the network security situation.
4. To evaluate the performance of the proposed system by implementing a novel prototype with real data.

The proposed system includes 4 modules. There are Data capture module, Data sequencing module, NSSE Module, Network Security Situation (NSS) Forecasting Module.

Module I: Data Capture: This module prepares data in the proper format. It manages threat detection alert and save them in a text file.
Module II: Data Sequencing*:* This module categorizes alerts in group depending on their similar features. It eliminates redundant alerts which may increase processing time. Alert Fusion and Alert Filtering are the components to accomplish the function of this module. In Alert Fusion component, with user-defined time-interval and same destination address, the formatted alerts in the file from previous module will be fused accordingly. Then, the redundant alerts in each cluster will be filtered out in the Alert Filtering component. A counter will be used to count the frequency of each type of alert.
Module III: NSSE *:* The module evaluates overall security situation in the network to make aware admin with current network status. Threat on each asset will be evaluated prior to the overall network assessment. After calculating the threat of each alert type, this module will apply the Entropy concept to measure the uncertainty degree of the network assets. The greater value of entropy implies more serious the security situation.
Module IV: NSS Forecasting: This module forecast the network security situation which able to alert admin before the attack onto network. For better precision, the predicted value of network situation is combined with its predicted error as well. Initial Network Security Situation Prediction component utilize a novel Adaptive Grey Verhulst algorithm to compute the predicted assessment of the network on next time-interval. Meanwhile, Error Prediction component calculate the predicted error based on the previous prediction errors.

3.1 Module Network Security Situation (NSS) Forecasting

Depending on the service, host and network security system in the threat situation provided by the target network, the situation assessment model can be established.

We only assess the security situation on the service.

Definition 1. The function *FS* said the security situation in the target network service status given as,

$$FS\ (\ S, C, N, D(t), t\ ) = N(t)\ .\ (\ 10\ ) \quad \ldots.\ (\ 1\ )$$

target network service status given as,

Where *S* represents a service the target network provided;

C indicates the type of service attacks ;

N is services by the number of attacks;

D is the severity of the attack;

$N(t)$ is the severity of attacks in t time;

$D(t)$ is the number of attacks occurred in t time.

Definition 2. The function *FH* said the security situation in the host status of the network given as,

$$FH\ (H, V, FS, t) = V\ .\ Fs(t) \quad \ldots.\ (\ 2\ )$$

Where *H* represents the target hosts on the network;

V indicates that the service's weight of all opened services.

Definition 3. Assuming in t (as small as possible) time period, select a state sequence from the state database, as the future network security situation prediction model of the input sequence, denoted by

$$X(0) = (x(0)1, x(0)2, \ldots, x(0)n)$$

Where , $x(0)\ t \geq 0$, $t = 1,2, \ldots, n$;

X(1) is 1-AGO sequence of X(0) , denoted as

$$X(1) = (x(1)1, x(1)2, \ldots, x(1)n)$$

the services available for the target network security situation prediction function module ,

$$Fs(t + (n+1)) = f\left(\sum_{i=1}^{n} Fs(t+i)\right) \quad \ldots \quad (3)$$

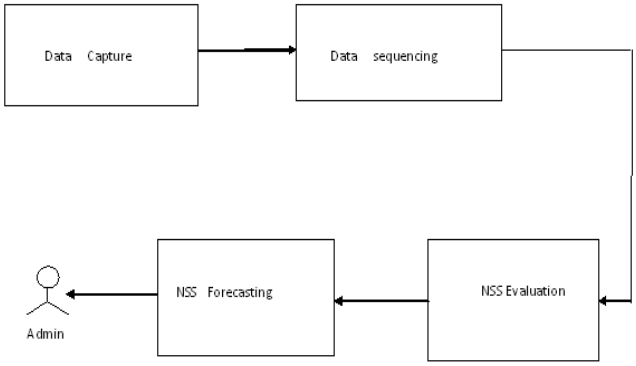

Fig-1 System architecture Of NSS evaluation & forecast

4. Model Experiment

The model can be implemented in PC equipped with

Linux machine with java platform.

Table I shows the operation condition involving

5 time intervals each 1 hour i.e. T1 ,T2 ,T3,T4,T5

TABLE I : Service operating conditions

Sr.No.	Table Column Head		
	Service Name	*Time*	*Service No.*
1	FTP, DNS , RPC	T1	3
2	DNS , SOCKET , HTTP, TELNET	T2	4
3	HTTP , FTP	T3	2
4	RPC , SOCKET , DNS	T4	3
5	TELNET , DNS , SOCKET	T5	3

From the above table, we can get the network security Situational value in five periods of time. The network security situation information of five periods as the original input data of forecasting module, then the forecasting value can be got by equation (3) for next period T6.

5. CONCLUSIONS

Our proposed system is expected to minimize the chances of network attack in the future and reduce the probability of taking reaction on false alerts. With the predicted value of security situation , it will acknowledge the network admin with a significant confidence level of the prediction to have a comprehensive plan in taking a more proper action against the incoming event. The findings of this research are also projected to significantly rise up the network security situation awareness. But , many of the key issues needs to be deepen and improved, such as the application of the model for a large number of discrete and not smooth sample points, the impact to the final model of residual error sequence selection can be implemented in future

REFERENCES

[1] Heu wei , Li Jian Hua, "Network Security Situation Prediction Based on improved Adaptive Grey Verhulst Model " , Springer 2010, 15(4):408-41

[2] Baris ulutas , "Grey system theory - based models in time series predicion" , Elsevier 2010 , ESA 37

[3] pallavi Vaidya, S.K.Shinde, "Application for network security situation awareness" ,IJCA 2012 , (0975 – 8887)

[4] Rongzen Fan, "Network security awareness and tracking method by GT" , JCIS 2013

[5] Xin wang,Yi xie," Modelling and analysis of network security situation prediction based on covariance neural" springer 2012

[6] Yan Wang, YongQi , " Network security risk assessment model and method based on situation awareness ", Springer 2012 , pp.191 – 204

[7] Jianfeng Dong,"The building of network security situation evaluation and prediction model based on Grey Theory " , IEEE 2010

