A Novel Adaptive Grey Verhulst Model for Network Security Situation Prediction

Yu-Beng Leau, Selvakumar Manickam
National Advanced IPv6 Centre (NAv6)
University of Science Malaysia
Penang, Malaysia

***Abstract*—Recently, researchers have shown an increased interest in predicting the situation of incoming security situation for organization's network. Many prediction models have been produced for this purpose, but many of these models have various limitations in practical applications. In addition, literature shows that far too little attention has been paid in utilizing the grey Verhulst model predicting network security situation although it has demonstrated satisfactory results in other fields. By considering the nature of intrusion attacks and shortcomings of traditional grey Verhulst model, this paper puts forward an adaptive grey Verhust model with adjustable generation sequence to improve the prediction accuracy. The proposed model employs the combination methods of Trapezoidal rule and Simpson's 1/3rd rule to obtain the background value in grey differential equation which will directly influence the forecast result. In order to verify the performance of the proposed model, benchmarked datasets, DARPA 1999 and 2000 have been used to highlight the efficacy of the proposed model. The results show that the proposed adaptive grey Verhulst surpassed GM(1,1) and traditional grey Verhulst in forecasting incoming security situation in a network.**

***Keywords*—Grey Theory; Network Security Situation Prediction; Adaptive Grey Verhulst Model; Adjustable Generation Sequence; Prediction Accuracy**

I. INTRODUCTION

Internet has become an impeccable necessity in our life providing services such as information sharing, communication, social interaction and etc. The acceleration of countries modernization and proliferation of mobile devices utilization has boost up the Internet users to reach 3.17 billion in 2015 [1]. The growth of Internet is further driven by new technologies such as cloud computing and Internet of Things (IoT). However, the immense popularity of the Internet and prevalent use of online services has made Internet a breeding ground for malware and cyber criminals. New security challenges are emerging while people are enjoying to sharing their resources borderlessly. In 2014, Symantec has encountered a 23% and 40% increase in data breaches and phishing attacks respectively compared to previous year [2]. This alarming situation brings serious challenges to network security worldwide.

Prevention is better than detection and recovery. Due to the rising number of the threats, network security communities nowadays crave to know the incoming security situation in their network before any precaution taken. Unfortunately, countering attacks in an Intrusion Prevention System (IPS) with a complete list of responses is insufficient. Surprisingly, in a study done by University of South Wales in 2013 on nine big-brand IPS systems, they found that seven out of them failed to detect and prevent up to 49% of attacks that target vulnerabilities especially in web-based application [3]. Therefore, predicting the incoming security situation in an entire network is desired to facilitate IPS to be more intelligent in in aspect of preventing the problem from growing and in returning the system to a healthy mode. Coincidentally, security situation prediction capability was considered as one of the main components in situation awareness when the concept has been introduced by Endsley [4] to the world. The idea then has been first adapted in the cyberspace by Tim Bass [5] with 3-hierarchical phases network security situation awareness (NSSA) which consists of event detection, current security situation assessment and future security situation prediction.

Recently, the governments, enterprises and other stakeholders started to adapt the concept of NSSA and seek some appropriate strategies especially in predicting incoming security situation in their network before any incident occurred. For instance, in Germany, the National Cyber Response Centre is responsible to alert the crisis management staff whenever the cyber security situation reaches the level of an imminent or already occurred crisis [6]. Meanwhile, in Malaysia, the National Cyber Security Policy addressed that there is a need to develop effective cyber security incident reporting mechanisms which capable of disseminating vulnerability advisories and threat warning in a timely manner in order to strengthen the National Computer Emergency Response Teams (CERTs) in monitoring the situation of critical national information infrastructure [7]. From the efforts of aforementioned countries in their strategic planning, it obviously brings us a significant motion that future network security situation prediction is very much in demand at the top level of cyber security strategic plan.

The rest of this paper is structured as follows: the authors first discuss some limitation of existing prediction models. Then, the author present a novel adaptive grey Verhulst model with the approach of calculating its adjustable generation sequence in the following section. Next, the authors demonstrate the grey prediction models with benchmarked datasets, The Defense Advanced Research Project Agency (DARPA) 1999 and 2000 (LLS DDOS1.0 and LLS DDOS 2.0.2). To verify the performance of the proposed model, the authors compare the accuracy of prediction result of our model

with traditional GM(1,1) and grey Verhulst models from the aspects of their Mean Absolute Percentage Error (MAPE) and Root Mean Square Deviation (RMSD). Finally, the authors summarize our work with a conclusion.

II. Limitation of Existing Prediction Models

A considerable amount of work has been published on designing network security situation prediction models. These studies can be categorized into three groups, i.e. Machine Learning, Markov Model and Grey Theory [8]. Prediction based on machine learning such as neural network and support vector system is commonly used in situation prediction due to its high convergence rate and strong fault tolerance capacity. But it requires a large amount of training data to gain the appropriate parameters and establish self-learning neurons. Furthermore, the method is unsuitable for small-scaled data as less input information will slower the convergence. Markov model, on the other hand, is also to be used to perform the prediction in various time series such as series of network situation. Nevertheless, the model is complex and difficult to build due to its difficulties in making assumption on all possible states and transitions especially in a network which is highly heterogeneous in nature. Since data pertaining to network situation may be inconsistent and incomplete, grey theory especially First-order One-variable grey model (GM(1,1)) has been widely used to provide better prediction in short-term forecasting with small sample data without any training required. Regrettably, the method is only limited to linear time series and it is not suitable for non-stationary random sequence. Apparently, the generation sequence with mean is only limited to small time interval and it depresses the model precision with delay error. In fact, Grey Verhulst, a type of small sample predicting model in Grey Theory which able to forecast the situation with single peak of data sequence. However, the model failed to apply some related influencing factors which will degrade its performance [9]. Observing the chronology of an intrusion attack as illustrated in Figure 1, the authors argue that an adaptive Grey Verhulst model with its adjustable generation sequence is best suited to predict the incoming network security situation which behaves as a non-linear time series.

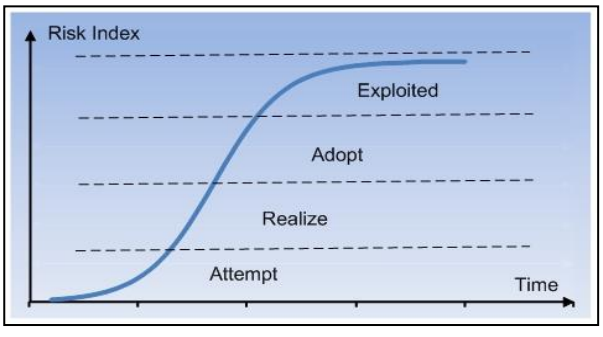

Fig. 1. The chronology of an intrusion attack

III. Proposed Adaptive Grey Verhulst Model

GM(1,1) and Grey Verhulst are theories to deal with indeterminate and incomplete system with their superiority in small sample. Nonetheless, they have similar problem in overshoots which caused by the non-monotonic time series data [10]. In addition, the generated sequence also make the prediction generate the advance or delay error which will depress the model precision [11]. Hence, this paper attempts to show that adaptive determination of grey parameters in grey Verhulst model is able to guarantee the precision. The adjustable generation sequence in this adaptive grey Verhulst model is not only suitable to forecast a stochastic time series such as incoming network security situation but also to handle multiple-peak situation variation which is inherent in network behavior [8].

In order to predict the incoming network security situation, a sequence of current and historical assessment of network security situation is used as input to the model. Figure 2 depicts the process flow of adaptive grey Verhulst model.

First, a sequence of network security situation assessment, $X^{(0)}$ is channeled into the model and a new sequence of accumulated data is built by applying the 1-Accumulated Generating Operation (1-AGO).

$$X^{(0)} = \left\{x^{(0)}(1), x^{(0)}(2), \ldots\ldots, x^{(0)}(n)\right\}$$

$$X^{(1)} = \left\{x^{(1)}(1), x^{(1)}(2), \ldots\ldots, x^{(1)}(n)\right\}$$

where

$$x^{(1)}(t) = \sum_{i=1}^{t} x^{(0)}(\mathrm{i}),\ X^{(0)}(\mathrm{i}) \geq 0,\ \ \mathrm{t} = 1, 2, \ldots\ldots, \mathrm{n}.$$

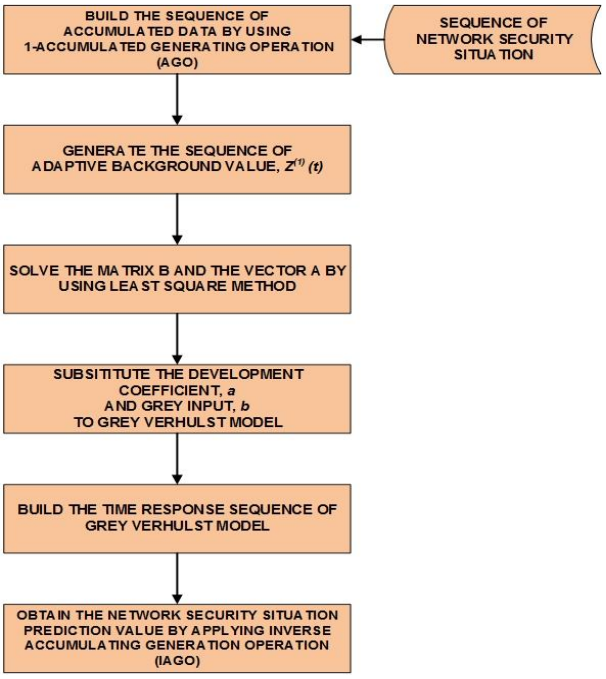

Fig. 2. Process flow of adaptive grey Verhulst model

Next, a sequence of adaptive background value, $Z^{(1)}(t)$ is generated by considering the consecutive (before and after) neighbors of $x^{(1)}$. The detail of calculating $z^{(1)}(t)$ is explained in the following section.

$$Z^{(1)}(t)=\left\{z^{(1)}(1),z^{(1)}(2),\ldots\ldots,z^{(1)}(n)\right\}$$

where

$$z^{(1)}(t)=x^{(1)}(t-1)+\frac{1}{6}x^{(0)}(t-1)-\frac{1}{6}x^{(0)}(t-2)+\frac{1}{2}x^{(0)}(t),$$

and $t=3,4,\ldots\ldots,n$.

The value of $z^{(1)}(t)$ is substituted into Grey Verhulst model below.

$$x^{(0)}(t)+az^{(1)}(t)=b\left[z^{(1)}(t)\right]^2$$

where a is development coefficient which its size reflects the growth rate of the sequence $X^{(0)}$ and b is the role of vector which is grey input in Grey Verhulst model. After that, the equations are rearranged into matrix form $Y=B\hat{a}$ with

$$A=\begin{bmatrix}a\\b\end{bmatrix}=(B^TB)^{-1}B^TY$$

the parameter matrix and the matrixes of B and Y as below.

$$B=\begin{bmatrix}-z^{(1)}(2) & \left(z^{(1)}(2)\right)^2\\ -z^{(1)}(3) & \left(z^{(1)}(3)\right)^2\\ \vdots & \vdots\\ -z^{(1)}(n) & \left(z^{(1)}(n)\right)^2\end{bmatrix}\qquad Y=\begin{bmatrix}x^{(0)}(2)\\ x^{(0)}(3)\\ \vdots\\ x^{(0)}(n)\end{bmatrix}$$

In order to find the value of a and b, the matrix B and vector A have been solved by using matrix method, $A=(B^TB)^{-1}B^TY$. The value of a and b can be obtained through the formulas below:

$$a=\frac{DH-GE}{FG-D^2}\qquad b=\frac{FH-DE}{FG-D^2}$$

where

$$D=\sum_{t=3}^{n}\left[z^{(1)}(t)\right]^3,\qquad E=\sum_{t=3}^{n}\left[z^{(1)}(t)x^{(0)}(t)\right],$$

$$F=\sum_{t=3}^{n}\left[z^{(1)}(t)\right]^2,\qquad G=\sum_{t=3}^{n}\left[z^{(1)}(t)\right]^4,$$

$$H=\sum_{t=3}^{n}\left[z^{(1)}(t)\right]^2x^{(0)}(t)$$

With the value of a and b, the predicted time response sequence of Grey Verhulst model, $x_g^{(1)}(t+1)$ is calculated by substituting them into the solution of Verhulst model.

$$x_g^{(1)}(t+1)=\frac{ax^{(0)}(1)}{bx^{(0)}(1)+\left(a-bx^{(0)}(1)\right)e^{at}}$$

where $x^{(0)}(1)=x^{(1)}(1)$. Finally, to obtain the prediction value of next network security situation, $x_g^{(0)}(t+1)$, the Inverse Accumulating Generation Operation (IAGO) has been applied. As $x^{(1)}(t+1)=x^{(1)}(t)+x^{(0)}(t+1)$, the $x_g^{(0)}(t+1)$ can be determined by using the formula below.

$$x_g^{(0)}(t+1)=x_g^{(1)}(t+1)-x_g^{(1)}(t)$$

and

$$x_g^{(0)}(1)=x^{(1)}(1)=x^{(0)}(1)$$

where $t=2,3,\ldots\ldots,n$.

IV. Adaptive Background Value Generation

Background value, $z^{(1)}(t)$ is a crucial factor that influences the adoption of grey theories and theirs forecasting result. The value of developing coefficient, a and the precision of the model will be affected by different background values [12].

In traditional grey Verhulst, the grey differential equation can be written as

$$x^{(0)}(t)+az^{(1)}(t)=b\left(z^{(1)}(t)\right)^2 \tag{1}$$

where

$$z^{(1)}(t)=\alpha x^{(1)}(t)+(1-\alpha)x^{(1)}(t-1)$$

Observed from the differential equation, background value has direct influences on the precision of the Grey Verhulst. Its value is determined by α which range $0\le\alpha\le1$. On the basic of traditional grey theories, α is always set as 0.5 to equalize the importance of each data [10, 13, 14]. In this context, the ignorance of data characteristic has produced more prediction errors [12, 15]. Thus, to improve the performance of grey theories especially in grey Verhulst, the error term resulted from the background value generation have to be eliminated. In other words, finding a suitable background value for the model is an essential subject to improve the prediction accuracy.

Based on [16], the most suitable background value should be located in between $x^{(1)}(t-1)$ and $x^{(1)}(t)$ as illustrated in figure 3. Due to the developing coefficient will direct affect the background value, thus the newer data should be emphasized by assigning a larger value of α [12]. In fact, setting the value of α is a process to search the optimal solutions within the value space. The time series dataset should be regarded as several different populations [17]. Hence, the value of α should be adaptable at each timescale with different adjustable background values as depicted in figure 4.

The possible error which might degrade the precision of grey Verhulst can be identified prior to its elimination. In grey Verhulst, the whitening equation of grey Verhulst model is written as

$$\frac{dx^{(1)}(t)}{dt} + ax^{(1)}(t) = b\left[x^{(1)}(t)\right]^2 \tag{2}$$

By integrating both side of equation (2),

$$\int_{t-1}^{t} \frac{dx^{(1)}(t)}{dt}dt + a\int_{t-1}^{t} x^{(1)}(t)dt = b\int_{t-1}^{t}\left[x^{(1)}(t)\right]^2 dt \tag{3}$$

where

$$\int_{t-1}^{t} \frac{dx^{(1)}(t)}{dt}dt = x^{(1)}(t) - x^{(1)}(t-1) = x^{(0)}(t)$$

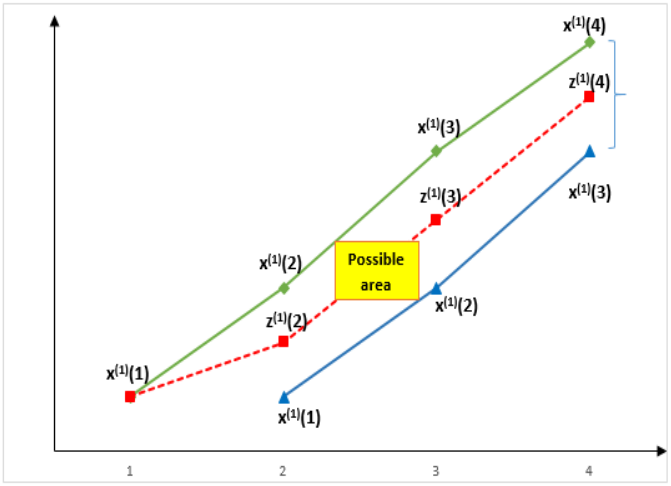

Fig. 3. Possible area of background values

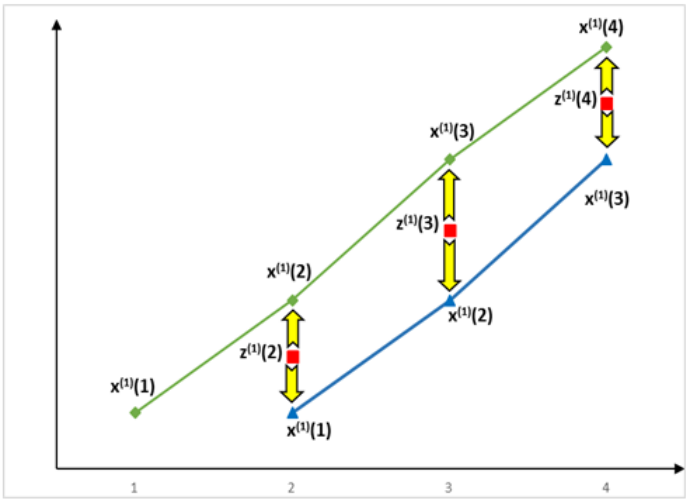

Fig. 4. Distribution of the adjustable background values

Thus, equation (3) can be written as

$$x^{(0)}(t) + a\int_{t-1}^{t} x^{(1)}(t)dt = b\int_{t-1}^{t}\left[x^{(1)}(t)\right]^2 dt \tag{4}$$

By comparing the equation (1) and (4), the background value can be determined as below.

$$z^{(1)}(t) = \int_{t-1}^{t} x^{(1)}(t)dt \tag{5}$$

From the equation (5), the error is exist if there has an inequality equation as follows.

$$\int_{t-1}^{t} x^{(1)}(t)dt \neq \alpha x^{(1)}(t) + (1-\alpha)x^{(1)}(t-1)$$

where

$$z^{(1)}(t) = \alpha x^{(1)}(t) + (1-\alpha)x^{(1)}(t-1)$$

Therefore, to eliminate the error, the background value must be equal to the integration of $x^{(1)}(t)$ from two consecutive time interval $t-1$ to t.

$$\int_{t-1}^{t} x^{(1)}(t)dt \tag{6}$$

Indeed, equation (6) represents an area under a graph function as presented in figure 5.

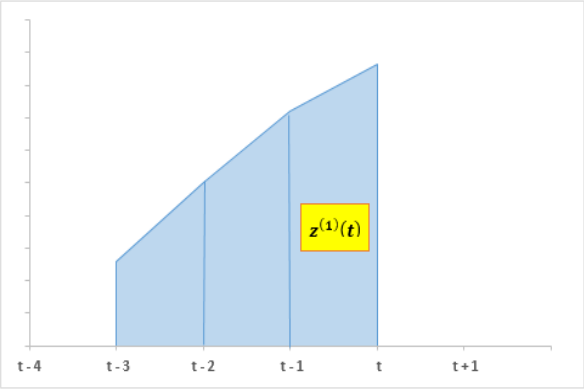

Fig. 5. Area under a graph function

Due to the curve function is unknown, in our proposed adaptive grey Verhulst model, the background value, $z^{(1)}(t)$ is calculated by the combination methods of Trapezoidal rule and Simpson's 1/3rd rule. These rules are used to determine the area under a graph without knowing its function. Trapezoidal rule is based on approximating the integrand by a first order polynomial and then integrating the polynomial in the interval of integration while Simpson's 1/3rd rule is an extension of Trapezoidal rule where the integrand is approximated by a second order polynomial. From figure 5, the area under the curve from time interval $t-3$ to t can be determined as below.

$$\int_{t-3}^{t} x^{(1)}(t)\,dt = \int_{t-3}^{t-1} x^{(1)}(t)\,dt + \int_{t-1}^{t} x^{(1)}(t)\,dt \tag{7}$$

Rearrange the equation (7),

$$\int_{t-1}^{t} x^{(1)}(t)\,dt = \int_{t-3}^{t} x^{(1)}(t)\,dt - \int_{t-3}^{t-1} x^{(1)}(t)\,dt \tag{8}$$

By applying the Trapezoidal rule and Simpson's 1/3rd rule, the equation (8) can be further simplified as follows.

$$\int_{t-1}^{t} x^{(1)}(t)\,dt =$$

$$\frac{t-(t-3)}{2(3)}\left[x^{(1)}(t-3)+2\left(x^{(1)}(t-2)+x^{(1)}(t-1)+x^{(1)}(t)\right)\right]$$

$$-\frac{(t-1)-(t-3)}{6}\left[x^{(1)}(t-3)+4x^{(1)}(t-2)+x^{(1)}(t-1)\right]$$

Finally, the background value, $z^{(1)}(t)$ can be obtained through the equation below.

$$z^{(1)}(t) = x^{(1)}(t-1) + \frac{1}{6}x^{(0)}(t-1) - \frac{1}{6}x^{(0)}(t-2) + \frac{1}{2}x^{(0)}(t) \tag{9}$$

Where $t = 3,4,\ldots\ldots,n$.

V. Case Study and Results

The DARPA/MIT Lincoln Lab evaluation datasets 1999 and 2000 have been published and widely used in evaluating the performance of prediction models [18-22] recently. In these datasets, there are various attacks found and there can be categorised into five main classes namely, Probe, Denial of Service (DoS), Remote to Local (R2L) and User to Remote (U2R) and the Data attacks [23].

In order to verify the performance of our proposed adaptive grey Verhulst in predicting network security situation, these three benchmarked datasets, DARPA 1999 and 2000 (LLS DDOS 1.0 and LLS DDOS 2.0.2) have been used in our model as well as traditional GM(1,1) and grey Verhulst models. These datasets were divided into several time-slots based on hours or minutes, and be evaluated by using entropy-based network security situation assessment approach in [24]. The values of situation assessment for each time slots have been used as input for the prediction models to forecast the next network security situation. Table 1, 2 and 3 present the prediction results from each dataset for the three models of grey theory aforementioned.

From the computational results aforementioned, Mean Absolute Percentage Error (MAPE) and Root Mean Square Deviation (RMSD) are used as evaluation metrics to determine the performance of prediction models in term of its accuracy. MAPE is a measure of accuracy of a method for constructing fitted time series values in statistics especially in trend estimation while RMSD is frequently used to measure the differences between the values predicted by a model and the values actually observed. The numerical results show that adaptive grey Verhulst model has attained average 93.3% of prediction accuracy while GM(1,1) and traditional grey Verhulst models has only achieved 87.3% and 92.0% respectively. Compared to both traditional GM(1,1) and grey Verhulst model, the lower MAPE and RMSD values produced have further prove the proposed prediction model is more reliable in forecasting incoming security situation in a network.

TABLE I. Prediction Result for Darpa 1999

Time /h	Real Value	GREY PREDICTION METHODS					
		Traditional GM(1,1)		Traditional Grey Verhulst		Adaptive Grey Verhulst	
		Predicted Value	RPE (%)	Predicted Value	RPE (%)	Predicted Value	RPE (%)
13	0.2206	0.2641	19.75	0.2467	11.86	0.2557	15.92
14	0.1871	0.2751	47.01	0.2183	16.70	0.2349	25.57
15	0.2056	0.2864	39.32	0.1853	9.89	0.2071	0.75
16	0.2151	0.2983	38.68	0.1517	29.49	0.1761	18.14
17	0.1806	0.3106	72.05	0.1206	33.23	0.1451	19.64
18	0.1706	0.3235	89.67	0.0936	45.12	0.1165	31.69
19	0.2056	0.3369	63.86	0.0714	65.29	0.0916	55.43
20	0.2160	0.3508	62.41	0.0537	75.16	0.0709	67.17
21	0.1956	0.3654	86.78	0.0399	79.59	0.0542	72.30
22	0.1835	0.3805	107.35	0.0295	83.94	0.0410	77.65
MAPE (%)			62.69		45.03		38.43
RMSD			0.13		0.10		0.09

TABLE II. PREDICTION RESULT FOR DARPA 2000 – LLS DDOS 1.0

Time /15 min	Real Value	GREY PREDICTION METHODS					
		Traditional GM(1,1)		Traditional Grey Verhulst		Adaptive Grey Verhulst	
		Predicted Value	RPE (%)	Predicted Value	RPE (%)	Predicted Value	RPE (%)
9	0.1848	0.2458	33.00	0.2281	23.42	0.2290	23.91
10	0.1961	0.2795	42.58	0.1926	1.77	0.1993	1.64
11	0.1415	0.3179	124.63	0.1423	0.59	0.1519	7.34
12	0.1773	0.3615	103.95	0.0952	46.29	0.1045	41.04
MAPE (%)			76.04		18.02		18.48
RMSD			0.14		0.05		0.04

TABLE III. PREDICTION RESULT FOR DARPA 2000 – LLS DDOS 2.0.2

Time /10 min	Real Value	GREY PREDICTION METHODS					
		Traditional GM(1,1)		Traditional Grey Verhulst		Adaptive Grey Verhulst	
		Predicted Value	RPE (%)	Predicted Value	RPE (%)	Predicted Value	RPE (%)
7	0.0705	0.1051	49.06	0.0971	37.72	0.1015	43.94
8	0.0541	0.1142	111.01	0.0569	5.09	0.0636	17.58
9	0.0651	0.1240	90.46	0.0273	58.13	0.0323	50.33
10	0.0751	0.1347	79.36	0.0118	84.26	0.0472	37.17
MAPE (%)			82.47		46.30		37.25
RMSD			0.05		0.04		0.03

VI. CONCLUSION

In conclusion, this paper presents a novel adaptive grey Verhulst prediction model with its adjustable generation sequence. The authors have shown that the prediction accuracy of the proposed adaptive grey Verhulst was much better compared to GM(1,1) and traditional grey Verhulst models due to its remarkable features in forecasting next security situation in the network. With the capability to handle multiple-peaks situation and able to provide higher accuracy of prediction to network administrator, the proposed adaptive grey Verhulst is very well-suited to predict incoming network security situation of an organization. In the future, the author propose to investigate the prediction error of the adaptive grey Verhulst and design a residual prediction algorithm to complement it in order to improve the predictive accuracy in forecasting incoming network security situation.

ACKNOWLEDGMENT

The authors would like to thank Universiti Sains Malaysia for funding this research project entitled “A Framework for Analytic Hierarchy Process (AHP)-Entropy Network Security Situation Assessment and Adaptive Grey Verhulst-Kalman Network Security Situation Prediction in Intrusion Prevention System” under the RUI grant (1001/PNAV/811294).

REFERENCES

[1] Internet Users. 2015 [Available at: http://www.internetlivestats.com/internet-users/#trend]. Accessed on 25 August 2015.

[2] Internet Security Threat Report 2015, Symantec Corporation: United States, pp. 1-119, April 2015.

[3] Xynos, K., L. Sutherland, and A. Blyth, Effectiveness of Blocking Evasions in Intrusion Prevention System, University of South Wales, pp. 1-6, 2013.

[4] Endsley, M.R. Design and evaluation for situation awareness enhancement. in Proceedings of the Human Factors and Ergonomics Society Annual Meeting, SAGE Publications, 1988.

[5] Bass, T. and D. Gruber, A glimpse into the future of id login: Special Issue Intrusion Detection. The USENIX Association Magazine, 1999.

[6] Cyber Security Strategy for Germany, F.M.o.t. Interior, Editor, Federal Ministry of the Interior: Germany, pp. 1-15, 2011.

[7] National Cyber Security, T.a.I. Ministry of Science, Editor, Ministry of Science, Technology and Innovation: Malaysia, pp. 1-9, 2012.

[8] Leau, Y.-B. and S. Manickam, Network Security Situation Prediction: A Review and Discussion, in Intelligence in the Era of Big Data, Springer, pp. 424-435, 2015.

[9] Cui, J., et al., Novel Grey Verhulst Model and Its Prediction Accuracy. Journal of Grey System, 27(2): pp. 47-53, 2015.

[10] Yao, A.W., S. Chi, and J. Chen, An improved grey-based approach for electricity demand forecasting. Electric Power Systems Research, 67(3): pp. 217-224, 2003.

[11] Hu, W., et al., Network security situation prediction based on improved adaptive grey Verhulst model. Journal of Shanghai Jiaotong University (Science),15(4): pp 408-413, 2010.

[12] Yeh, C.-W., C.-J. Chang, and D.-C. Li. A Modified Grey Prediction Method to Early Manufacturing Data Sets. in International MultiConference of Engineers and Computer Scientists, Hong Kong: Newswood Limited, 2009.

[13] Wen, J.C., K.H. Huang, and K.L. Wen, The Study of α in GM (1, 1) Model. Journal of the Chinese Institute of Engineers, 23(5): pp. 583-589, 2000.

[14] El-Fouly, T., E. El-Saadany, and M. Salama, Improved grey predictor rolling models for wind power prediction. IET Generation, Transmission & Distribution, 1(6): pp. 928-937, 2007.

[15] Lin, Y.-H., P.-C. Lee, and T.-P. Chang, Adaptive and high-precision grey forecasting model. Expert Systems with Applications, 36(6): pp. 9658-9662, 2009.

[16] Li, D.-C. and W.-K. Lin, Employing GA-based Adaptive Grey Model for Learning with Short-term Sequence Data. Journal of Grey System, 25(4): pp. 96-106, 2013.

[17] Lin, Y.-S. and D.-C. Li, The Generalized-Trend-Diffusion modeling algorithm for small data sets in the early stages of manufacturing systems. European Journal of Operational Research, 207(1): pp. 121-130, 2010.

[18] Man, D., et al. A combined prediction method for network security situation. in International Conference on Computational Intelligence and Software Engineering (CiSE), IEEE, 2010.

[19] GuangCai, K., W. XiaoFeng, and Y. LiRu. A fuzzy forecast method for network security situation based on Markov. in International Conference on Computer Science and Information Processing (CSIP), IEEE, 2012.

[20] SHI, Y., et al., An Immune-Based SCGM (1, 1) c Prediction Model for Network Security Situation⋆. Journal of Computational Information Systems, 9(11): pp. 4395-4406, 2013.

[21] Farhadi, H., M. AmirHaeri, and M. Khansari, Alert correlation and prediction using data mining and HMM. The ISC International Journal of Information Security, 3(2): pp. 77-101, 2011.

[22] Kholidy, H.A., A. Erradi, and S. Abdelwahed. Attack Prediction Models for Cloud Intrusion Detection Systems. in 2014 2nd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS), IEEE, 2014.

[23] Thomas, C., V. Sharma, and N. Balakrishnan. Usefulness of DARPA dataset for intrusion detection system evaluation. in SPIE Defense and Security Symposium, International Society for Optics and Photonics, 2008.

[24] Beng, L.Y., S. Manickam, and T.S. Fun, A Framework for Analytic Hierarchy Process-Entropy Network Security Situation Assessment and Adaptive Grey Verhulst-Kalman Prediction in Intrusion Prevention System. Australian Journal of Basic & Applied Sciences, 8(14): pp. 34-39, 2014