An Enhanced Adaptive Grey Verhulst Prediction Model for Network Security Situation

Yu-Beng Leau[†] and Selvakumar Manickam[††]

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia

Summary
Situation prediction is an increasingly important focus in network security. The information of incoming security situation in the network is important and helps the network administrator to make good decisions before taking some defense remedies towards the attack exploitation. Although Grey Verhulst prediction model has demonstrated satisfactory results in other fields but some further investigations are still required to improve its performance in predicting incoming network security situation. In order to attain higher predictive accuracy of the existing Grey Verhulst prediction models, this paper tends to seek an enhancement of the adaptive Grey Verhulst security situation prediction model by forecasting the incoming residual based on the historical prediction residuals. The proposed model applied Kalman Filtering algorithm to predict the residual in the next time-frame and closer the deviation between the predicted and actual network security situation. Benchmark datasets such as DARPA 1999 and 2000 have been used to verify the accuracy of the proposed model. The results shown that the enhanced adaptive Grey Verhulst prediction model has better prediction capability in predicting incoming network security situation and also achieved a significant improvement compared to other Grey Verhulst prediction models.

Key words:
Network security situation prediction, Grey Verhulst, Kalman Filtering, Residual prediction

1. Introduction

In this globalization era, the Internet has become an important part of our lives offering convenient services and information sharing. The number of Internet users worldwide has mushroomed to reach 3.17 billion which is almost 40% of the world population in 2015 [1]. Unfortunately, the immense popularity of the Internet and prevalent use of online applications has made the Internet a breeding ground for malware and cyber criminals. The local area networks (LANs) are the building blocks of the Internet. LAN is crucial for computing operations within the boundaries of the organization. Since LAN is also connected to the Internet, it is vulnerable to infiltration and attacks from outside the organization. For instance, in Malaysia, the published incident statistics for year 2014 indicate that 11918 cases were reported to Malaysia Computer Emergency Response Team (MyCERT) with different types of attacks such as denial of service, intrusion attempt, malicious codes, spamming and etc [2]. Besides that, in a security report published by Arbor Network in 2015, it revealed that Distributed Denial of Service (DDoS) attack was the most frequently observed threat in an enterprise with an average of 21 attacks in a month. The situation became worse when more than 33% of organizations had their intrusion prevention system devices experience failure during the attack [3]. Consequently, the organizations have to bear the big loss caused by the incident. As an information security breaches survey conducted by PricewaterhouseCoopers on United Kingdom (UK)'s businesses, it discovered that 90% and 74% of large and small organizations respectively had a security breach in the year 2014 and it caused losses of £1.46 million - £3.14 million average in the year [4]. This phenomenon brings serious challenges and problems to network security.

Due to the rising number of threats, detection alone is no longer able to provide an organization a reliable network. Prevention before an incident occurs should be in place. As preventing an incident requires careful analysis and planning, network security communities are constantly on the alert to know the incoming security situation in their networks before any precautions could be taken. Figure 1 illustrates the network security landscape which consists of promising online applications, new emerging network threats, current alarming situation and main components in situational awareness.

2. Grey Verhulst Prediction Model

The Verhulst model was first introduced by a German biologist, Pierre Franois Verhulst in 1837 to describe the increasing process like S-curve which has a saturation region, namely the process increases slowly at initial stage, then speeds-up and finally grows slowly or stop growing [5]. Grey Verhulst model is superior in small samples. The Grey Verhulst model can be defined as follows [6]:

Step I:

Suppose that the original raw data series $x^{(0)}$ with n samples is expressed as:

$$X^{(0)} = \{x^{(0)}(1), x^{(0)}(2), \dots, x^{(0)}(n)\}, \quad n \geq 4 \qquad (1)$$

Manuscript received May 5, 2016
Manuscript revised May 20, 2016

and

$$X^{(0)}(k) \geq 0, k = 1, 2, \ldots, n; \quad (2)$$

Step II:

A new series $X^{(1)}$ is generated by applying Accumulating Generation Operation (AGO)

$$X^{(1)} = \{x^{(1)}(1), x^{(1)}(2), \ldots, x^{(1)}(n)\}, n \geq 4 \quad (3)$$

where

$$x^{(1)}(k) = \sum_{i=1}^{k} x^{(0)}(i), \ k = 1, 2, 3, \ldots, n \quad (4)$$

From the Equation (4), it is obvious that original series $X^{(0)}$ can be easily recovered from $X^{(1)}$ as

$$X^{(0)}(k) = \begin{cases} x^{(1)}(k) - x^{(1)}(k-1), & k \neq 1 \\ x^{(1)}(k), & k = 1 \end{cases} \quad (5)$$

where $X^{(1)}(k) \in X^{(1)}$. This operation is called Inverse Accumulated Generation Operation (IAGO).

Step III:

A series $Z^{(1)}$ is generated by applying the MEAN operation to $X^{(1)}$.

$$Z^{(1)} = \{z^{(1)}(1), z^{(1)}(2), \ldots, z^{(1)}(n)\}, \quad (6)$$

where $z^{(1)}(k)$ is the mean value of adjacent data such as

$$z^{(1)}(k) = 0.5x^{(1)}(k) + 0.5x^{(1)}(k-1), \quad (7)$$

$k = 2, 3, \ldots n$

In order to predict the S type curve, the non-linear difference equation in Grey Verhulst model is defined as below.

$$x^{(0)}(k) + az^{(1)}(k) = b(z^{(1)}(k))^2 \quad (8)$$

and its whitening equation is

$$\frac{dx^{(1)}(k)}{dt} + ax^{(1)}(k) = b(x^{(1)}(k))^2 \quad (9)$$

in which a is defined as the development coefficient and b is defined as the grey input. The parameter matrixes are

$$\hat{a} = \begin{bmatrix} a \\ b \end{bmatrix} = (B^T B)^{-1} B^T Y \quad (10)$$

where

$$B = \begin{bmatrix} -z^{(1)}(2) & (z^{(1)}(2))^2 \\ -z^{(1)}(3) & (z^{(1)}(3))^2 \\ \vdots & \vdots \\ -z^{(1)}(n) & (z^{(1)}(n))^2 \end{bmatrix} \quad (11)$$

and

$$Y = \begin{bmatrix} x^{(0)}(2) \\ x^{(0)}(3) \\ \vdots \\ x^{(0)}(n) \end{bmatrix} \quad (12)$$

By calculating Equation (9), the solution of $x^{(1)}(t)$ at time k is

$$x_p^{(1)}(k+1) = \frac{ax^{(0)}(1)}{bx^{(0)}(1) + (a - bx^{(0)}(1))e^{ak}} \quad (13)$$

In the Equation (13), $x^{(0)}(1) = x^{(1)}(1)$. It is assumed that the n-dimension data sequence is selected to fit the model.

When $k \geq n$, the fitted model can be used to predict the future value as

$$x_p^{(0)}(k+1) = x_p^{(1)}(k+1) - x_p^{(1)}(k) \quad (14)$$

where

$$x_p^{(0)}(1), x_p^{(0)}(2), x_p^{(0)}(3), \ldots, x_p^{(0)}(n)$$

are called Grey Verhulst fitted sequence, while

$$x_p^{(0)}(n+1), x_p^{(0)}(n+2), x_p^{(0)}(n+3), \ldots, x_p^{(0)}(n+t)$$

are called Grey Verhulst predicted values.

In Grey Verhulst model, a and b are the key parameters to guarantee the precision of the model. Their values can be obtained by applying least square method into the generation sequences $Z^{(1)}$ as Equation (7). This feature only allows the Grey Verhulst model to generate appropriate parameters in the small time interval and the AGO curve varies smoothly.

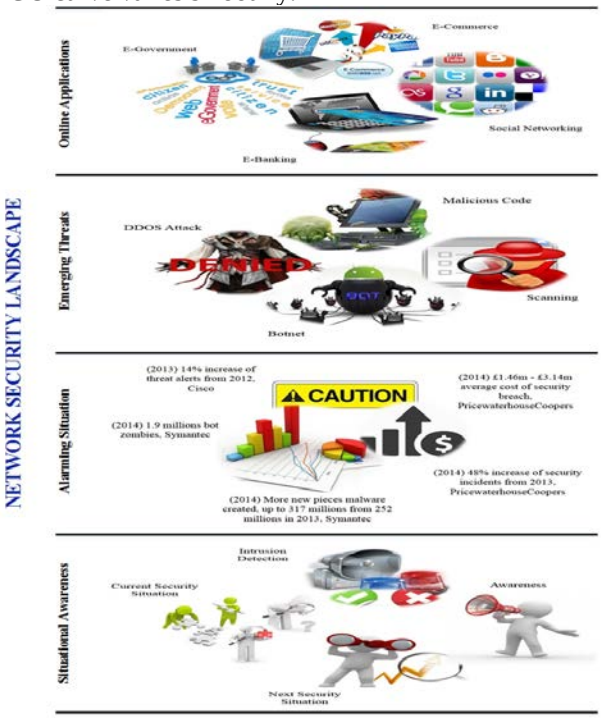

Fig. 1 Network Security Landscape.

The rest of this paper is structured as follows: the authors first explain the basic concepts of Grey Verhulst and Kalman Filtering. Then, the authors discuss about an adaptive Grey Verhulst prediction model in the following section. Next, the authors present a Kalman's Residual prediction model as a complement to the adaptive Grey Verhulst prediction model and demonstrate the proposed model with benchmark datasets. In order to verify the performance of the model, the authors compare its predictive accuracy with other Grey Verhulst models in the aspects of Mean Absolute Percentage Error (MAPE) and Root Mean Square Deviation (RMSD). At the end of

this paper, the authors summarize the results with a conclusion.

3. Kalman Filtering

Kalman Filtering is a recursive solution published by R. E. Kalman in 1960 to handle the problems in discrete signal and linear filtering [7]. It is an optimal estimator which consists of a set of mathematical equations that can estimate efficiently the state of a process in order to minimize the mean of the squared error [8]. It infers the parameters of interest from indirect, inaccurate and uncertain observations. It has some significant features such as less parameters, simple calculation and convenient in real time processing [9]. Recently, the applications of Kalman Filtering are widely used especially in solving estimation problems [10]. It has been used in various fields such as weather forecasting [11, 12], stock market prediction [13, 14] , navigation [15, 16], tracking objects [15, 17] as well as network security situation prediction [9].

Basically, Kalman Filtering estimates a state by using a form of feedback control. It determines the optimal filtering gains through a complete description of the probability distribution of its estimation error [10]. As such, the equations in Kalman Filter fall into two groups: time update equations (predictor equations) and measurement update equations (corrector equations). The time update equations are responsible to obtain the priori estimates for next time interval by projecting forward the current state and error covariance estimates. Meanwhile, the measurement update equations handle the feedback which incorporate the new measurement into the priori estimates in order to get an improved posteriori estimate [8]. The complete operation in Kalman Filtering is illustrated in Figure 2.

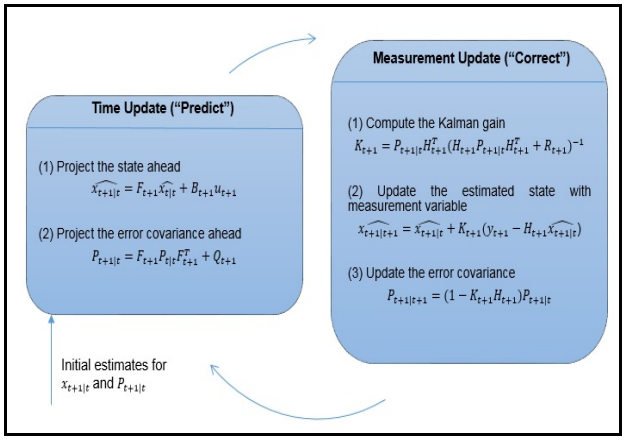

Fig. 2 A Complete Picture of the Operation in Kalman Filtering.

where

$\hat{x}$: Estimated state
F : State transition matrix
u : Control variables
B : Control matrix
P : State variance matrix
Q : Process variance matrix
y : Measurement variables
H : Measurement matrix
K : Kalman gain
R : Measurement variance matrix
$t+1|t+1$: Next time period
$t|t$: Current time period
$t+1|t$: Intermediate steps

In the equations, the *n x n* matrix *F* relates the state, *x* at time step t to the state at step $t+1$ in the absence of process noise, the *n x l* matrix B relates the control input to the state *x* and the matrix *m x n* matrix *H* relates the state to the measurement, y_{t+1} which is the actual measurement. The discrepancy between the predicted and actual measurements is called the residual and it can be calculated by finding the difference of them as $y_{t+1} - H_{t+1}\widehat{x_{t+1|t}}$. In order to find a posteriori state estimate, $\widehat{x_{t+1|t+1}}$, a linear combination of a priori estimate and a weighted residual will be formed as $\widehat{x_{t+1|t}} + K_{t+1}(y_{t+1} - H_{t+1}\widehat{x_{t+1|t}})$. The weight in this case is a *n x m* matrix called Kalman gain, K_{t+1} which obtained from previous process. It is used to minimize the posteriori error covariance.

4. Adaptive Grey Verhulst Prediction Model

Generally, Grey Verhulst is designed to deal with indeterminate and incomplete system with their superiority in small sample. Nonetheless, it has problem in overshoots which caused by the non-monotonic time series data [18]. Furthermore, the generated sequence also make the prediction generate the advance or delay error which will depress the model precision [19]. Due to this, an adaptive Grey Verhulst model which adaptively determine the parameters in the prediction model was proposed in our previous paper [20]. The adaptive Grey Verhulst model is not only able to guarantee the precision in forecasting a stochastic time series such as a series of network security situation, but also able to handle multiple-peak situation variation which is inherent in network behavior [21].

The current and historical network security situation assessment sequence, $X^{(0)}$ is used as input to predict the incoming network security situation. First, the sequence is fed into the model to generate a new sequence of accumulated data by applying the 1-Accumulated Generating Operation (1-AGO).

$$X^{(1)} = \left\{x^{(1)}(1), x^{(1)}(2), \ldots\ldots x^{(1)}(n)\right\} \quad (15)$$

where

$$x^{(1)}(t) = \sum_{i=1}^{t} x^{(0)}(i) \text{ for } X^{(0)}, t = 1, 2, \ldots\ldots n$$

Instead of using mean generation sequence as in Equation (7), the model generates a sequence of adaptive background value, $Z^{(1)}(t)$ by considering the consecutive (before and after) neighbors of $x^{(1)}$.

$$Z^{(1)}(t) = \left\{z^{(1)}(1), z^{(1)}(2), \ldots\ldots z^{(1)}(n)\right\} \quad (16)$$

where

$$z^{(1)}(t) = x^{(1)}(t-1) + \frac{1}{6}x^{(0)}(t-1) - \frac{1}{6}x^{(0)}(t-2) + \frac{1}{2}x^{(0)}(t),$$
$$t = 3, 4, 5, \ldots\ldots n.$$

After that, the value of $Z^{(1)}(t)$ is then substituted into the Equation (8) in Grey Verhulst model. The equation then is arranged into matrix form $Y = B\hat{a}$ with the parameter matrix as Equation (10). By using the Least Square Method, the values of *a* and *b* are obtained through the formulas below:

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

where

$$D = \sum_{t=3}^{n}\left[z^{(1)}(t)\right]^3, \quad E = \sum_{t=3}^{n}\left[z^{(1)}(t)x^{(0)}(t)\right],$$
$$F = \sum_{t=3}^{n}\left[z^{(1)}(t)\right]^2, \quad G = \sum_{t=3}^{n}\left[z^{(1)}(t)\right]^4,$$
$$H = \sum_{t=3}^{n}\left[z^{(1)}(t)\right]^2 x^{(0)}(t).$$

With the values of *a* and *b*, the predicted time response sequence of Grey Verhulst model, $x_g^{(1)}(t+1)$ as in Equation (13) is calculated. Finally, by applying Inverse Accumulating Generation Operation (IAGO), the predicted value of next network security situation, $x_g^{(0)}(t+1)$ is obtained.

$$x_g^{(0)}(t+1) = x_g^{(1)}(t+1) - x_g^{(1)}(t) \quad (17)$$

and

$$x_g^{(0)}(1) = x^{(1)}(1) = x^{(0)}(1) \quad (18)$$

where t =2, 3, ……,*n*..

5. Proposed Kalman's Residual Prediction Model

In order to enhance the predictive accuracy with closer predicted value to the actual value in a particular time-interval, a residual prediction algorithm by using Kalman Filtering method is proposed as an additional process in the adaptive Grey Verhulst model. The algorithm focuses on forecasting the next prediction deviation based on the previous prediction residual. The output, which is residual prediction value then will be combined with the preliminary network security situation prediction value which computed by using adaptive Grey Verhulst model to form a final prediction value for incoming network security situation. Figure 3 depicts the process flow of residual prediction in the adaptive Grey Verhulst model.

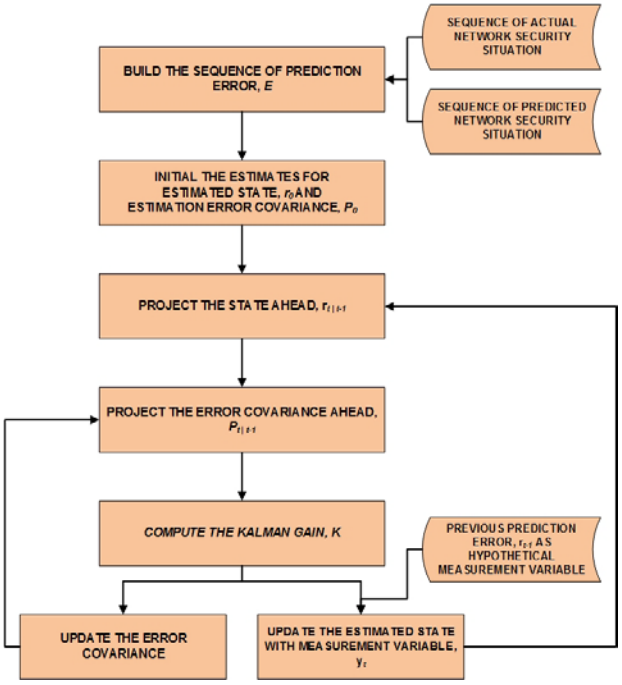

Fig. 3 Process Flow of Residual Prediction.

Firstly, a sequence of prediction error, *E* which represents the difference between the adaptive Grey Verhulst predicted value and actual network security situation value is built. The value of prediction error in each time interval, *e* can be obtained through Equation (19).

$$e(t) = x^{(0)}(t) - x_g^{(0)}(t) \quad (19)$$

where

Actual value

$$= \{x^{(0)}(1), x^{(0)}(2), x^{(0)}(3), \ldots\ldots, x^{(0)}(t)\} \quad (20)$$

Adaptive Grey Verhulst predicted value

$$= \{x_g^{(0)}(1), x_g^{(0)}(2), x_g^{(0)}(3), \ldots\ldots, x_g^{(0)}(t)\} \quad (21)$$

Prior to the process, some parameter values such as process noise, Q, measurement noise, R and initial estimation error covariance, Po and initial residual, ro have to be set. The value of $\hat{r}_0$ is the deviation of real value, $x^{(0)}(t)$ and predicted adaptive grey Verhulst value, $x_g^{(0)}(t)$ during previous time-interval while the value of P_0 is based on the knowledge about the initial state. The more

meaningful variables to be initialized, the faster convergence will be achieved. In the experiment, the process noise, Q has been set as $Q = 0.0001$ because the proposed model is assumed reliable and is able to provide a good estimation of the true process. The measurement noise, R was set as low as 0.0001 because the value of measurement is directly taking from the deviation of previous prediction and actual values, thus it is almost free of any error from measurement. Meanwhile, the initial error of estimation, Po was set as Po =100. It is assumed to be a high variance due to lack of knowledge about the initial state. The value of residual, ro was initialized as $\hat{r}_0 = 0$ as the previous residual is completely unknown in the early stage.

The process will be started from time update equations. To project the state, $\widehat{r_{t+1|t}}$ and error covariance, $P_{t+1|t}$ ahead, the equations (22) and (23) are used respectively. The model is assumed constant, therefore $F_{t+1} = 1$ for any $t \geq 0$. Control variables are not been used, so $B = 0$ and $u = 0$.

$$\widehat{r_{t+1|t}} = \widehat{r_{t|t}} \quad (22)$$

$$P_{t+1|t} = P_{t|t} + Q_{t+1} \quad (23)$$

After completing the time update equations, the first task during the measurement update is to compute the Kalman gain, K_{t+1} as Equation (24). In this experiment, the measurement is same scale as state estimate, $\hat{r}$, therefore $H = 1$.

$$K_{t+1} = P_{t+1|t}(P_{t+1|t} + R_{t+1})^{-1} \quad (24)$$

With the Kalman gain, the next step is to measure the process to obtain measurement variable, y and then to generate a posteriori state estimate, $\widehat{r_{t+1|t+1}}$.

$$\widehat{r_{t+1|t+1}} = \widehat{r_{t+1|t}} + K_{t+1}(y_{t+1} - \widehat{r_{t+1|t}}) \quad (25)$$

where

$$y_{t+1} = \widehat{r_{t|t}} = x^{(0)}(t) - x_p^{(0)}(t) \quad (26)$$

the deviation from real value on previous network security situation prediction. The final step is to update the posteriori error variance estimate through Equation (27).

$$P_{t+1|t+1} = (1 - K_{t+1})P_{t+1|t} \quad (27)$$

The process is repeated with the previous posteriori state estimate to project the new priori estimates after completing each time and measurement update pair.

In order to acquire the final predicted value for incoming network security situation, the residual prediction value, $\widehat{r_{t+1|t+1}}$ will be combined with preliminary network security situation prediction value, $x_g^{(0)}(t+1)$ which computed by using adaptive grey Verhulst model. Thus, the calculation of final predicted network security situation, $x_p^{(0)}(t+1)$ as Equation (28). Figure 4 presents the process flow for acquiring the final network security situation prediction.

$$x_p^{(0)}(t+1) = x_g^{(0)}(t+1) + \widehat{r_{t+1|t+1}} \quad (28)$$

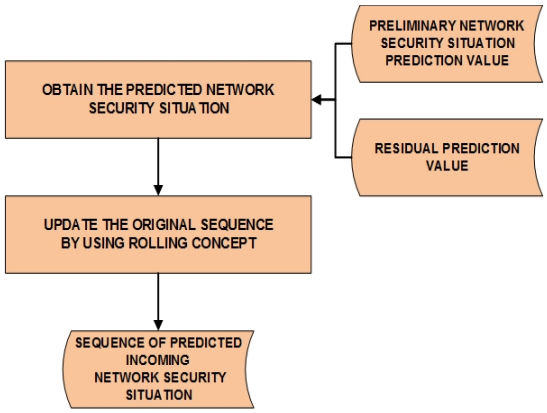

Fig. 4 Process Flow of Final Network Security Situation Prediction.

6. Practical Results

In this paper, benchmark datasets such as DARPA 1999 and 2000 (LLS DDOS 1.0 and LLS DDOS 2.0.2) Intrusion Detection Evaluation Datasets have been used to assess the performance of prediction models and also do the comparisons with other grey prediction approaches. The datasets consist of various attacks and there had been categorized into five main classes namely, Probe, Denial of Service (DoS), Remote to Local (R2L) and User to Remote (U2R) and the Data attacks [22]. Literature have shown that these datasets had been widely used to evaluate the prediction model [23-28]. For DARPA 1999 Intrusion Detection Evaluation Dataset, the only data generated on April 6, 0800 to April 7, 0600 was used in the research because there were more attacks compared to other days and it was more dangerous to the network situation [29].

The datasets first had been divided into several time-slots in minutes basis and evaluated by Entropy-based network security situation assessment model proposed by Beng and Selva [30]. Then, 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. Evaluation metrics such as Mean Absolute Percentage Error (MAPE), Root Mean Square Deviation (RMSD) and Relative Percentage Error (RPE) have been applied to measure the predictive accuracy of the models. Mean Absolute Percentage Error (MAPE) is a measure of accuracy of a method for constructing fitted time series values in statistics, specifically in trend estimation with treating all the errors with the same weight [20],while Root Mean Square Deviation (RMSD) measures the differences between predicted and actual value by penalizing variance with more weight to the errors [31]. Meanwhile, Relative Percentage Error (RPE) is a measurement of how large the error is in relation to the

correct value. It is a ratio of the absolute error of the measurement to the accepted measurement.

Table 1, 2 and 3 present the prediction results of traditional GM(1,1) model, traditional Grey Verhulst model, Adaptive Grey Verhulst (AGV) model and Adaptive Grey Verhulst-Kalman (AGVK) model for each datasets. The numerical results show that Adaptive Grey Verhulst-Kalman model has better prediction in all the datasets with the lowest MAPE and RMSD amongst other prediction models. The average MAPE and RMSD of AGVK model are 16.09% and 0.04 compared to AGV model which are 31.39% and 0.05 as well as 36.45% and 0.06 for traditional Grey Verhulst model. It denotes that AGVK model can predict incoming network security situation with 83.91% predictive accuracy while AGV and traditional Grey Verhulst models are only able to achieve 68.61% and 63.55% respectively. The results prove that Adaptive Grey Verhulst-Kalman prediction model is able to predict more accurately the incoming network security situation regardless of the datasets which symbolize the current security situation in a network.

Table 1: Prediction Result for DARPA 1999

Time /h	Real Value	GREY PREDICTION METHODS					
		Traditional Grey Verhulst Model		AGV Model		Proposed AGVK Model	
		Predicted Value	RPE (%)	Predicted Value	RPE (%)	Predicted Value	RPE (%)
13	0.2206	0.2467	11.86	0.2557	15.92	0.2251	2.08
14	0.1871	0.2183	16.70	0.2349	25.57	0.2314	23.69
15	0.2056	0.1853	9.89	0.2071	0.75	0.2030	1.28
16	0.2151	0.1517	29.49	0.1761	18.14	0.1471	31.62
17	0.1806	0.1206	33.23	0.1451	19.64	0.1356	24.88
18	0.1706	0.0936	45.12	0.1165	31.69	0.1549	9.16
19	0.2056	0.0714	65.29	0.0916	55.43	0.1341	34.79
20	0.2160	0.0537	75.16	0.0709	67.17	0.0968	55.20
21	0.1956	0.0399	79.59	0.0542	72.30	0.1083	44.65
22	0.1835	0.0295	83.94	0.0410	77.65	0.1354	26.23
MAPE (%)			45.03		38.43		25.36
RMSD			0.10		0.09		0.06

Table 2: Prediction Result for DARPA 2000 – LLS DDOS 1.0

Time /15 min	Real Value	GREY PREDICTION METHODS					
		Traditional Grey Verhulst Model		AGV Model		Proposed AGVK Model	
		Predicted Value	RPE (%)	Predicted Value	RPE (%)	Predicted Value	RPE (%)
9	0.1848	0.2281	23.42	0.2290	23.91	0.1870	1.18
10	0.1961	0.1926	1.77	0.1993	1.64	0.1643	16.20
11	0.1415	0.1423	0.59	0.1519	7.34	0.1375	3.05
12	0.1773	0.0952	46.29	0.1045	41.04	0.1185	33.14
MAPE (%)			18.02		18.48		13.39
RMSD			0.05		0.04		0.03

Table 3: Prediction Result for DARPA 2000 – LLS DDOS 2.0.2

Time /10 min	Real Value	GREY PREDICTION METHODS					
		Traditional Grey Verhulst Model		AGV Model		Proposed AGVK Model	
		Predicted Value	RPE (%)	Predicted Value	RPE (%)	Predicted Value	RPE (%)
7	0.0705	0.0971	37.72	0.1015	43.94	0.0845	19.85
8	0.0541	0.0569	5.09	0.0636	17.58	0.0369	31.80
9	0.0651	0.0273	58.13	0.0323	50.33	0.0432	33.66
10	0.0751	0.0118	84.26	0.0472	37.17	0.0623	17.06
MAPE (%)			46.30		37.25		25.59
RMSD			0.04		0.03		0.02

7. Conclusion

As a conclusion, this paper presents an enhanced adaptive Grey Verhulst network security situation prediction model with forecasting the residual based on the historical records. The authors have shown that the predictive accuracy of the Adaptive Grey Verhulst-Kalman prediction model was more promising with the improvement of 15.30% and 20.36% compared to traditional and adaptive Grey Verhulst prediction models correspondingly. Furthermore, the proposed model had also been proven that its capability to provide better incoming network security situation prediction in both single and multiple-peaks situation regardless to the time-interval allocation. In the nutshell, the proposed model is well-suited as a complement to the network prevention system in the organizations to ensure their network situation is always in a healthy and safety mode.

Acknowledgments

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] International Telecommunication Union. Internet Users. 2015 [cited 2015 25 August]; Available from: http://www.internetlivestats.com/internet-users/#trend.

[2] Malaysia Computer Emergency Response Team. MyCERT Incident Statistics Year 2014 2015 [cited 2016 2 March]; Available from: http://www.mycert.org.my/en/services/statistic/mycert/2013/main/detail/914/index.html.

[3] Anstee, D., et al., 10th Worldwide Infrastructure Security Report. 2015, Arbor Networks: United States p. 1-128.

[4] PricewaterhouseCoopers, Information Security Breaches Survey. 2015, Department for Business Innovation & Skills, PwC: London, United Kingdom. p. 1-52.

[5] Wang, Z., Y. Dang, and Y. Wang. A new grey Verhulst model and its application. in IEEE International Conference on Grey Systems and Intelligent Services 2007. IEEE.
[6] Wen, K.-L. and Y.-F. Huang. The development of grey Verhulst toolbox and the analysis of population saturation state in Taiwan-Fukien. in IEEE International Conference on Systems, Man and Cybernetics. 2004. IEEE.
[7] Kalman, R.E., A new approach to linear filtering and prediction problems. Journal of basic Engineering, 1960. 82(1): p. 35-45.
[8] Welch, G. and G. Bishop, An Introduction to the Kalman Filter. 2004, UNC-Chapel Hill: Department of Computer Science.
[9] Lin, Z., et al. The prediction algorithm of network security situation based on grey correlation entropy Kalman filtering. in 2014 IEEE 7th Joint International Information Technology and Artificial Intelligence Conference (ITAIC),. 2014. IEEE.
[10] Mohinder, S.G. and P.A. Angus, Kalman filtering: theory and practice using Matlab. John Wileys and Sons, 2001.
[11] Che, Y., et al., A wind power forecasting system based on the weather research and forecasting model and Kalman filtering over a wind-farm in Japan. Journal of Renewable and Sustainable Energy, 2016. 8(1): p. 013302.
[12] Chen, K. and J. Yu, Short-term wind speed prediction using an unscented Kalman filter based state-space support vector regression approach. Applied Energy, 2014. 113: p. 690-705.
[13] Bisoi, R. and P.K. Dash, A hybrid evolutionary dynamic neural network for stock market trend analysis and prediction using unscented Kalman filter. Applied Soft Computing, 2014. 19: p. 41-56.
[14] Fang, Z., et al. Stock forecast method based on wavelet modulus maxima and kalman filter. in 2010 Fourth International Conference on Management of e-Commerce and e-Government (ICMeCG),. 2010. IEEE.
[15] Bistrovs, V. and A. Kluga, Combined Information Processing from GPS and IMU using Kalman Filtering Algorithm. Elektronika ir Elektrotechnika, 2009. 93(5): p. 15-20.
[16] Fakharian, A., T. Gustafsson, and M. Mehrfam. Adaptive Kalman filtering based navigation: An IMU/GPS integration approach. in 2011 IEEE International Conference on Networking, Sensing and Control (ICNSC). 2011. IEEE.
[17] Olfati-Saber, R. and P. Jalalkamali. Collaborative target tracking using distributed Kalman filtering on mobile sensor networks. in American Control Conference (ACC), 2011. 2011. IEEE.
[18] Yao, A.W., S. Chi, and J. Chen, An improved grey-based approach for electricity demand forecasting. Electric Power Systems Research, 2003. 67(3): p. 217-224.
[19] Hu, W., et al., Network security situation prediction based on improved adaptive grey Verhulst model. Journal of Shanghai Jiaotong University (Science), 2010. 15(4): p. 408-413.
[20] Leau, Y.-B. and S. Manickam, A Novel Adaptive Grey Verhulst Model for Network Security Situation Prediction. International Journal of Advanced Computer Science & Applications, 2016. 1(7): p. 90-95.
[21] Leau, Y.-B. and S. Manickam, Network Security Situation Prediction: A Review and Discussion, in Intelligence in the Era of Big Data. 2015, Springer. p. 424-435.
[22] Thomas, C., V. Sharma, and N. Balakrishnan. Usefulness of DARPA dataset for intrusion detection system evaluation. in SPIE Defense and Security Symposium. 2008. International Society for Optics and Photonics.
[23] Wang, Y., W. Li, and Y. Liu, A Forecast Method for Network Security Situation Based on Fuzzy Markov Chain, in Advanced Technologies, Embedded and Multimedia for Human-centric Computing. 2014, Springer. p. 953-962.
[24] 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). 2012. IEEE.
[25] Wu, R.-F. and G.-L. Chen. Research of network security situation prediction based on multidimensional cloud model. in 2012 Sixth International Conference on. 2012 Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). IEEE.
[26] Shia, Y., et al., A Chaotic Characteristics Identification Method for Network Security Situation Time Series⋆. 2012.
[27] Man, D., et al. A combined prediction method for network security situation. in International Conference on Computational Intelligence and Software Engineering (CiSE). 2010. IEEE.
[28] Shi, Y., et al., An Immune-Based SCGM (1, 1) c Prediction Model for Network Security Situation⋆. Journal of Computational Information Systems, 2013. 9(11): p. 4395-4406.
[29] Si, J., et al. Network threat assessment based on attribute recognition. in 11th International Conference on Advanced Communication Technology. 2009. IEEE.
[30] 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, 2014. 8(14): p. 34-39.
[31] Chai, T. and R.R. Draxler, Root mean square error (RMSE) or mean absolute error (MAE)?–Arguments against avoiding RMSE in the literature. Geoscientific Model Development, 2014. 7(3): p. 1247-1250.

Selvakumar Manickam is a senior lecturer and researcher at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He has authored and co-authored more than 100 articles in journals, conference proceedings and book reviews. He has graduated 3 PhDs and 1 MSc and currently supervising 9 PhDs and 1 Masters. He has given several key note speeches as well as dozens of invited lectures and workshops at conferences, international universities and for industry. His research interest includes Internet Security, Cloud Computing, Software Defined Network, IPv6, Internet of Things (IoT) and Open Source Technology.

Leau Yu Beng received B.S (Multimedia Technology) degree from Universiti Malaysia Sabah, Malaysia in 2004 and M.SC. (Information Security) from Universiti Teknologi Malaysia (UTM), Malaysia in 2007. Currently, he is a Ph.D candidate in National Advanced IPv6 Center (NAv6), Universiti Sains Malaysia (USM). His current research interests are intrusion alert detection and prediction. He is a member of Information Security Professional Malaysia (ISPA) and International Association of Computer Science and Information Technology (IACSIT). He is also a IBM Certified Academic Associate and Certified IPv6 Network Engineer.