Journal of Computer Sciences

Original Research Paper

An Adaptive Assessment and Prediction Mechanism in Network Security Situation Awareness

[1]Yu-Beng Leau, [2]Ali Abdulrazzaq Khudher, [3]Selvakumar Manickam and [3]Samer Al-Salem

[1]Faculty of Computing and Informatics, Universiti Malaysia Sabah, Malaysia
[2]Department of Computer Science, Cihan University-Sulaimaniya, Iraq
[3]National Advanced IPv6 Centre, Universiti Sains Malaysia, Malaysia

Article history
Received: 21-12-2016
Revised: 16-04-2017
Accepted: 20-05-2017

Corresponding author:
Yu-Beng Leau
Faculty of Computing and Informatics, Universiti Malaysia Sabah, Malaysia
Email: leauyubeng@gmail.com

Abstract: Network intrusion attempts have reached an alarming level. Cisco's 2014 Security Report indicated that 50,000 network intrusions were detected and 80 million suspicious web requests were blocked daily. Hence, Intrusion Prevention System (IPS) had been chosen as a defence mechanism in many organizations. However, the University of South Wales reported that seven big-brand IPS had failed to detect and block 34-49% of attacks in web-based applications. The accuracy of IPS can be improved if the network situation is also considered in preventing intrusion attempts. Knowledge about current and incoming network security situation is required before any precaution can be taken. Situation assessment and prediction are two main phases of Network Security Situation Awareness. This paper presents a network security situation assessment and prediction mechanism that proposes an Entropy-based situation assessment scheme to assess current network security status with the aid of the Analytical Hierarchy Process and the introduction of an adaptive situation prediction mechanism based on Grey Verhulst and Kalman Filtering to predict the incoming security situation. The effectiveness of the mechanism is evaluated using National Advanced IPv6 Center (NAv6) 2015 dataset. The findings demonstrated that Entropy-based Network Security Situation Assessment (E-NESSAS) assessed more comprehensively network security situation by using Entropy concept. Meanwhile, Adaptive Grey Verhulst-Kalman Network Security Situation Prediction (AGVK-NESSIP) provided high predictive accuracy with accuracy of 82.77%. The results clearly revealed that the proposed mechanism could assess current security situation systematically by E-NESSAS and was able to predict the situation more accurately by AGVK-NESSIP regardless of the time intervals and behaviour of the data sequence.

Keywords: Situation Assessment, Situation Prediction, Grey Verhulst, Kalman Filtering, Analytical Hierarchy Process

Introduction

The Internet infiltrates our lives with offering convenient services and information sharing. It raises the number of Internet users worldwide to reach 3.17 billion which is almost 40% of the world population in 2015 (ITU, 2015). 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. In 2014, Symantec had encountered a 40% increase in phishing attacks compared to previous year, 2013 (Symantec, 2015). Meanwhile, Arbor Network had also 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 (Anstee, 2015). Based on a survey conducted on United Kingdom (UK)'s businesses 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 (PricewaterhouseCoopers, 2015). 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 monitor the current and incoming security situation in their networks before any precautions could be taken. Endsley (1988a) has introduced a concept of situation awareness to the world which covers the capabilities of security situation assessment and prediction in his 3-hierarchical framework.

Concept of Network Security Situation Awareness

Situation awareness is defined as the observation of changing critical factors in a complex global network within a time and space interval, the understanding of those factors mean according to the operator's goals and the projection of their status in next interval (Endsley, 1988b). It consists of three stages which are event detection, current situation assessment and future situation prediction (Endsley, 1995). Event Detection is a basic process which mainly to identify the abnormal and malicious activity in the network and translates them into logical format. Current Situation Assessment is a process to evaluate the security situation of the entire network by using the information obtained from the detected alerts in the event detection then Future Situation Prediction uses the current and historical network security situation status to forecast the future network security tendency according to the current and historical network security situation status. In 1999, these stages have been adapted in cyberspace called as Network Security Situation Awareness (NSSA) (Bass and Gruber, 1999).

The governments, enterprises and other stakeholders are seeking appropriate strategies with this kind of capability to manage their information and control system. For instances, the Australia Government established a Cyber Security Operations Centre (CSOC) within the Department of Defense to provide a 24/7 cyber situation awareness capability to facilitate operational responses to cyber security events of national importance (AAGD, 2009). In United States (US), President Barack Obama sealed a strategy plan to share situational awareness of network vulnerabilities and risks among the public and private sector networks and to work with other countries (between government and industries) in order to expand the international network in building a greater global situation awareness and incident response (WH, 2011). The United Kingdom (UK) Cyber Security Strategy clearly stated that they will continue to improve their detection and analysis of sophisticated cyber threats especially in the UK's critical national infrastructure as well as to pool knowledge and situational awareness when appropriate with their partners across all businesses to build a genuinely national response (CO, 2011). One of the main responsibilities of The German National Cyber Response Centre is to alert the crisis management staff whenever the cyber security situation reaches the level of an imminent or already occurred crisis (FMI, 2011). In Malaysia, the National Cyber Security Policy addressed the need to develop effective cyber security incident reporting mechanisms capable of disseminating vulnerability advisories and threat warnings in a timely manner so as to strengthen the National Computer Emergency Response Teams (CERTs) in monitoring the situation of critical national information infrastructure (MOSTI, 2012). From the effort of aforementioned countries in their strategic planning, it obviously reflected a concerted concern that NSSA is very much in demand at the top level of cyber security strategic plan.

Proposed Mechanism

The proposed mechanism called Network Security Situation Assessment and Prediction (NESSAP) mechanism which aimed to assess the entire network security situation by considering the tangible and intangible criteria and predict the incoming network security situation on next time-interval by using historical and current situation. In NESSAP, it comprises four main modules: (1) Data Preparation, (2) Data Normalization, (3) Entropy-based Network Security Situation Assessment (E-NESSAS) and (4) Adaptive Grey Verhulst-Kalman Network Security Situation Prediction (AGVK-NESSIP). Each module contains several components. The suspicious alerts are collected from Intrusion Detection Systems, as example, Snort in this research and flow into NESSAP mechanism. Figure 1 depicts the overall modules and flows in proposed mechanism.

Data Preparation Module

Data Preparation Module is the first module in NESSAP mechanism. The purpose of this module is to prepare appropriate data in proper format for the mechanism. The generated alerts from different alert detection engines may have different format. It is difficult for the mechanism to identify all possible formats for the alerts. Therefore, before the generated alerts have been used in the mechanism, they are required to be standardized in a specific format. Alert

Procurement is the first component in Data Preparation Module. It used to collect the alerts from multiple alert detection engines and save them into a text file. Meanwhile, Alert Formatting is a component to extract the features in each alert from the text file (output of Alert Procurement) and save them in a Comma Separated Value (CSV) type file. The features are loaded in a table which consists of number of rows and columns. There is a column called Alert_Score has been added into the table. The value of it is based on the priority value which able to represent the severity of this particular alert.

Data Normalization Module

Data Normalization module is responsible to categorize the alerts in specific groups based on their features and eliminate the redundant alerts which might lengthen the processing time. In this module, Alert Fusion is the component to gather the alerts in several groups based on the timestamp and destination address. In this context, user is required to define the time-interval which can be in minute basis to segment the alerts from a bunch of alerts for this particular time period. After that, the alerts within this time-frame will be classified based on its destination address. The alerts which have same destination address will be grouped under the same cluster. The fused alerts will be flowed to the next component, Alert Filtering. The process flow of Alert Fusion is depicted in Fig. 2.

After receiving the fused alerts from previous component, Alert Filtering is used to filter out the redundant alerts in the group. In this stage, fields such as IP destination, rules and priority in each alert are compared regarding its similarity. The similar alerts which have same features except the time are grouped. A counter is responsible to calculate the number of alerts in each group before these redundant alerts to be eliminated. The process flow of this component is demonstrated in Fig. 3. The alert types with its frequency will be fed into next module, Network Security Situation Assessment Module.

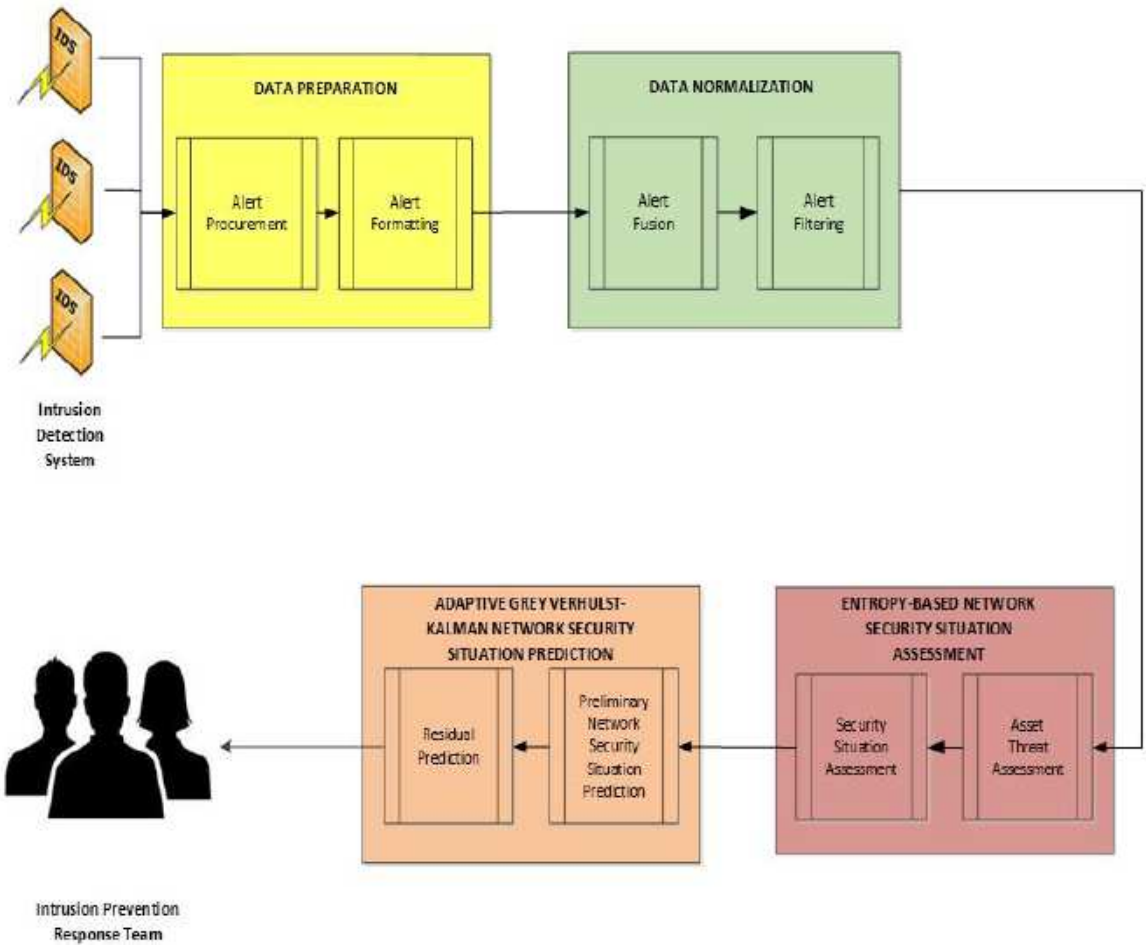

Fig. 1. Overview of network security situation assessment and prediction mechanism design

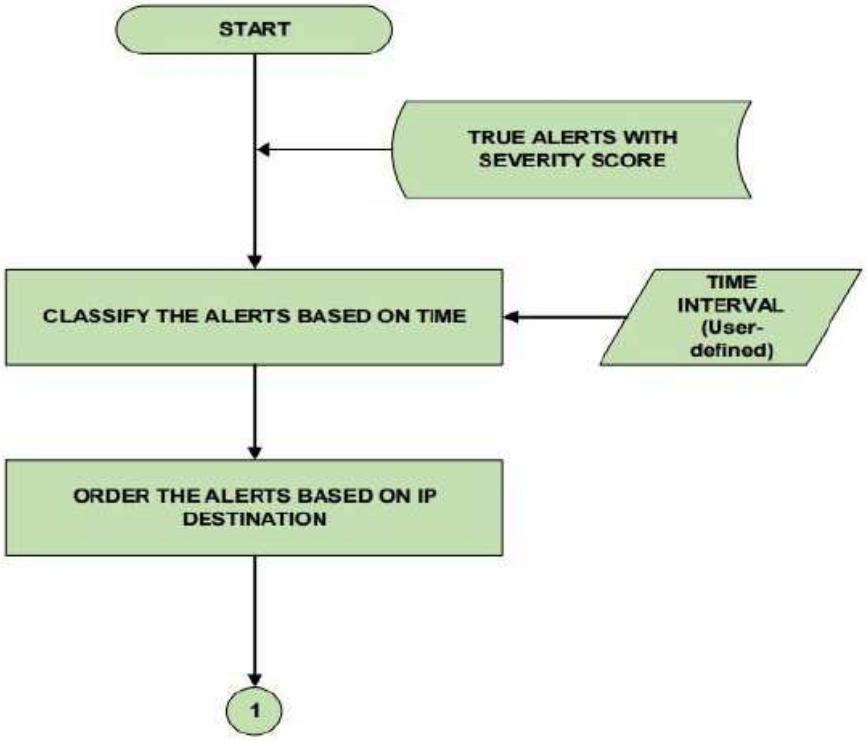

Fig. 2. Process flow of alert fusion

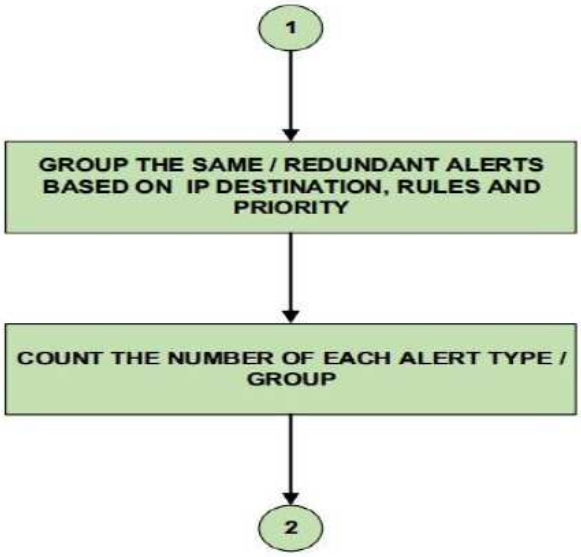

Fig. 3. Process flow of alert filtering

Entropy-based Network Security Situation Assessment Module

Entropy-based Network Security Situation Assessment module is one of the core methodologies of the proposed mechanism. Its main function is to assess the current security situation in entire network and provide this useful information to the security administrator. Instead of assessing the security situation of network in overall, threat of every single asset has been evaluated in the first step. Asset Threat Assessment is responsible to evaluate the threat of every asset in the network. It is a prerequisite process for next component to assess the whole network security situation. In a network, different asset has different function. Thus, it brings them a different threat value based on their importance in a particular network. As example, a printer may have different threat value as a server in the same attack. With the aid of Analytic Hierarchy Process, a weight with range from 0 to 1.0 has been determined and assigned to the assets after considering their implication of particular attack which relatively measured as its loss on confidentiality, integrity, availability, damage and response cost as well as likelihood of occurrence. This weight assignment represents the importance value of particular asset in the network. It can be done when any new network asset has been added into the network. Asset Threat Assessment has four main process as described in Fig. 4. The well-format and non-redundant alert types from previous module are ready to be used for assessment. Based on the IP destination address in an alert, the importance value of asset involved has been identified by referring to the list of network assets and their weight.

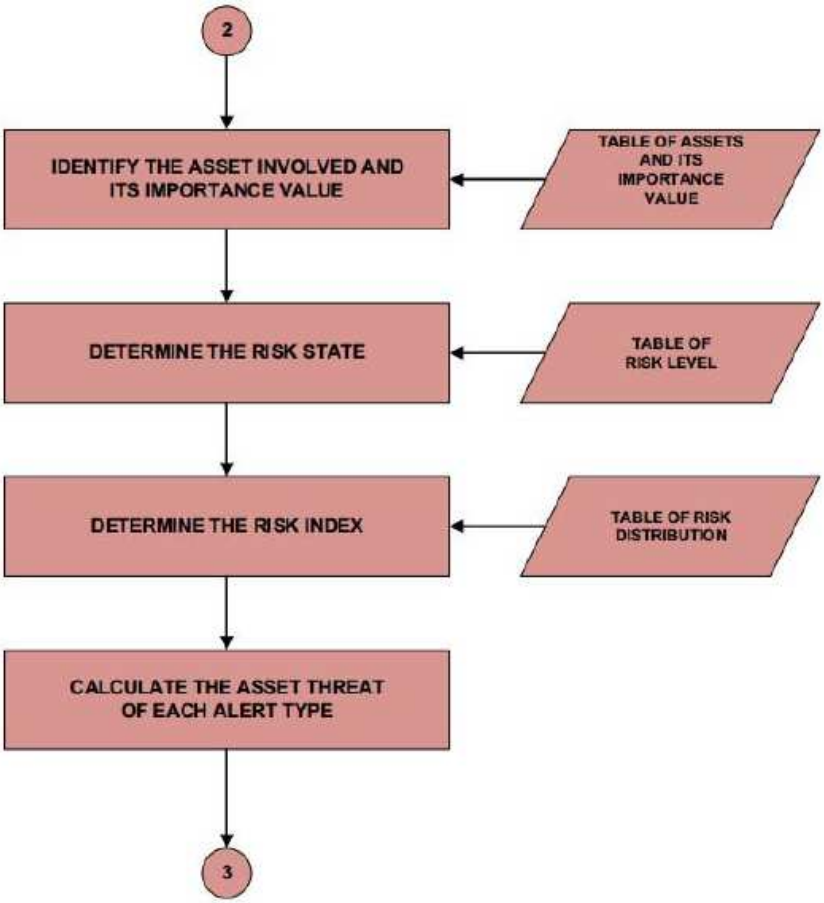

Fig. 4. Process flow of asset threat assessment

Then, with the importance value of network device and alert score of each alert type, a risk state can be calculated by using the Equation 1:

$$Risk\ State\left(RS_n\right) = Alert\ Score\left(AS_k\right) \times Importamce\ value\ of\ Asset\left(AW_n\right) \quad (1)$$

where, AS_k is k^{th} type of Alert Score ($0.0 \leq AS_n \leq 1.0$) and k is the number of Alert Type. After that, a table called Table of Risk Level is used to identify the level of risk of each alert based on its risk state. There are 10 different levels of risk in this research, Extreme (E), Highest (HT), Much Higher (MH), Higher (HR), High (H), Moderate (M), Low (L), Lower (LR), Much Lower (ML) and Lowest (LT). The risk state (range from 0 to 1.0) has been divided into 10 segments which symbolize different risk level of the alert type as depicted in Table 1.

Once the risk level of alert has been pinpointed, Risk Index (RI) of the alert also can be determined by using Table of Risk Index as presented in Table 2. The range of RI is from 0.1 to 1.0.

Table 1. Table of risk level

Risk state, *RS*	Risk level
$0 \leq RS < 0.1$	Lowest (LT)
$0.1 \leq RS < 0.2$	Much Lower (ML)
$0.2 \leq RS < 0.3$	Lower (LR)
$0.3 \leq RS < 0.4$	Low (L)
$0.4 \leq RS < 0.5$	Moderate (M)
$0.5 \leq RS < 0.6$	High (H)
$0.6 \leq RS < 0.7$	Higher (HR)
$0.7 \leq RS < 0.8$	Much Higher (MH)
$0.8 \leq RS < 0.9$	Highest (HT)
$0.9 \leq RS < 1.0$	Extreme (E)

Table 2. Table of risk index

Risk level	Risk Index (RI)
Extreme (E)	1.0
Highest (HT)	0.9
Much Higher (MH)	0.8
Higher (HR)	0.7
High (H)	0.6
Moderate (M)	0.5
Low (L)	0.4
Lower (LR)	0.3
Much Lower (ML)	0.2
Lowest (LT)	0.1

After obtaining the risk index of every type of alerts, Asset Threat, AT for each is also calculated by using Equation 2. Adapted the concept of grade calculation for security situational index (Xiaorong *et al*., 2012), in this research, different severity of alert is corrected by 10^{AS_k} where aggravate the seriousness of an attack that causes severe consequence on the asset:

$$AT_k = 10^{AS_k} \times RI \tag{2}$$

where, AT_k is k^{th} type of Asset Threat.

Security Situation Assessment acts as a center of assessment module to consider the situation of all the assets in the network in order to determine the security situation for the whole network. With the Asset Threat, AT in all detected alerts from previous component, Security Situation Assessment applied the concept of information entropy to measure the uncertainty degree of the network assets. As the nature of network alerts from environments that are characterized as unknown, high entropy, non-stationary and noisy (Tan, 2013), the concept of information entropy is useful in measurement of the uncertainty in a random variable. In general, the more uncertain or random the event is, the more information it will contain. In this research, the greater the entropy, the more serious the security situation of this asset is. Figure 5 demonstrates the processes in Security Situation Assessment.

By using the Asset Threat, AT, Information Entropy, E of each asset is calculated as Equation 3 and 4.

For $k = 1$:

$$E_n = AT_k \tag{3}$$

and for $k>1$:

$$E_n = -\sum_{k=1}^{K} AT_k \, p\left(AT_k\right) \log p\left(AT_k\right) \tag{4}$$

where:

$$p\left(AT_k\right) = \frac{f_k}{F} \tag{5}$$

Where:
n = n^{th} asset
E_n = Entropy of n^{th} asset
AT_k = Asset Threat of k^{th} alert type
f_k = Frequency of k^{th} alert type in particular asset
F = Total of frequency of all alert types in particular asset

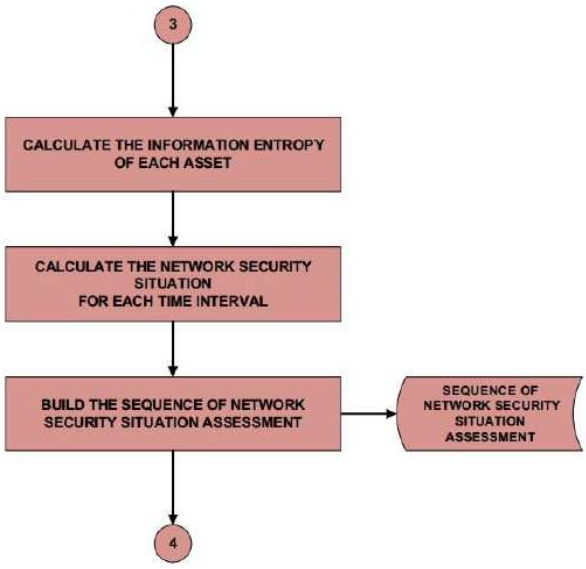

Fig. 5. Process flow of security situation

After calculating the Information Entropy of all the assets, the value of Network Security Situation Assessment (NESSAS) for each time interval can be evaluated. This value is the sum of security situation assessment for all the assets, which can be determined by multiplying Information Entropy with the importance value of asset in the network (AW). The formula to calculate the value of NESSAS is as follows:

$$NESSAT\left(T_i\right) = \sum_{n=1}^{N} ASSE_n\left(T_i\right) = \sum_{n=1}^{N} AW_n \times E_n\left(T_i\right) \tag{6}$$

where:

$$ASSE_n\left(T_i\right) = AW_n \times E_n\left(T_i\right) \tag{7}$$

Where:
T_i = i^{th} time-interval
AW_n = Importance value of nth asset
$ASSE_n$ = n^{th} Asset Security Situation Entropy

Once the network security situation assessment has been computed, a sequence of situational values from E-NESSAS module is built in order based on the time interval.

Adaptive Grey Verhulst-Kalman Network Security Situation Prediction Module

Adaptive Grey Verhulst-Kalman Network Security Situation Prediction module is also a core methodology in the proposed mechanism. Its purpose

is to predict the incoming network security situation and then taking some preemptive actions before an incident occurs. The module is constructed by two main processes in different components which are Preliminary Network Security Situation Prediction and Residual Prediction. To increase the precision of prediction, the value of forecasted network security situation in this module is a combination of preliminary situation prediction and its residual prediction in a particular time interval.

GM(1,1) and Grey Verhulst are theories to deal with indeterminate and incomplete system with their superiority in small sample. Unfortunately, they have similar problem in overshoots which caused by the non-monotonic time series data (Yao *et al*., 2013). The background value, $z^{(1)}(t)$ of both theories can be written as Equation 8:

$$z^{(1)}(t) = \alpha x^{(1)}(t) + (1-\alpha)x^{(1)}(t-1) \tag{8}$$

In fact, the background value is a crucial factor that influences the adoption of Grey theories and their forecasting result. The value of developing coefficient, a and the precision of the model will be affected by different background values (Yeh *et al*., 2009). In Grey Verhulst, the Grey differential equation is written as Equation 11:

$$x^{(0)}(t) = \alpha z^{(1)}(t) = b\left(z^{(1)}(t)\right)^2 \tag{9}$$

where background value, $z^{(1)}(t)$ can be obtained through Equation 8.

From the Equation 9, background value has direct influences on the precision of the Grey Verhulst. Its value is determined by α which range $0 \leq \alpha \leq 1$. In traditional Grey theories, α is always set as 0.5 to equalize the importance of each data (Yao *et al*., 2003; Wen *et al*., 2000; El-Fouly *et al*., 2007). In this context, the ignorance of data characteristic has produced more prediction errors (Yeh *et al*., 2009; Lin *et al*., 2009).

In order to improve the performance of Grey theories especially in Grey Verhulst, the error term resulted from the background value calculation needs to be eliminated. In other words, finding a suitable background value for the model is an essential subject to improve the prediction accuracy. The most suitable background value should be located in between $x^{(1)}(t-1)$ and $x^{(1)}(t)$ (Li and Lin, 2013). Figure 6 illustrates the possible area of background value located. Due to the developing coefficient will direct affect the background value, thus the newer data should be emphasized by assigning a larger value of a (Yeh *et al*., 2009). In fact, setting the value of a is a process to search the optimal solutions within the value space. The time series dataset should be regarded as several different populations (Lin *et al*., 2010). Hence, the value of a should be adaptable at each timescale with different adjustable background values as Fig. 7.

The possible error which might degrade the precision of Grey Verhulst can be identified prior to its elimination. The whitening equation of Grey Verhulst model is:

$$\frac{dx^{(1)}(t)}{dt} + ax^{(1)}(t) = b\left[x^{(1)}(t)\right]^2 \tag{10}$$

By integrating both side of Equation 10:

$$\int_{t-1}^{t} \frac{dx^{(1)}(t)}{dt}dt + a\int_{t-1}^{t} x^{(1)}(t)dt = b\int_{t-1}^{t}\left[x^{(1)}(t)\right]^2 dt \tag{11}$$

where:

$$\int_{t-1}^{t} \frac{dx^{(1)}(t)}{dt}dt = x^{(1)}(t) - x^{(1)}(t-1) = x^{(0)}(t) \tag{12}$$

Thus, Equation 11 can be written as:

$$x^{(0)}(t) + a\int_{t-1}^{t} x^{(1)}(t)\,dt = b\int_{t-1}^{t}\left[x^{(1)}(t)\right]^2 dt \tag{13}$$

By comparing the Equation 9 and 13, the background value can be determined as Equation 14:

$$z^{(1)}(t) = \int_{t-1}^{t} x^{(1)}(t)\,dt \tag{14}$$

From the Equation 14, the error is exist if there has an inequality equation as follows:

$$\int_{t-1}^{t} x^{(1)}(t)\,dt \neq \alpha x^{(1)}(t) + (1-\alpha)x^{(1)}(t-1) \tag{15}$$

where:

$$z^{(1)}(t) = \alpha x^{(1)}(t) + (1-\alpha)x^{(1)}(t-1) \tag{16}$$

In other words, 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:

$$\int_{t-1}^{t} x^{(1)}(t)\,dt \tag{17}$$

Indeed, Equation 17 is the area underneath a curve which can be represented as in Fig. 8.

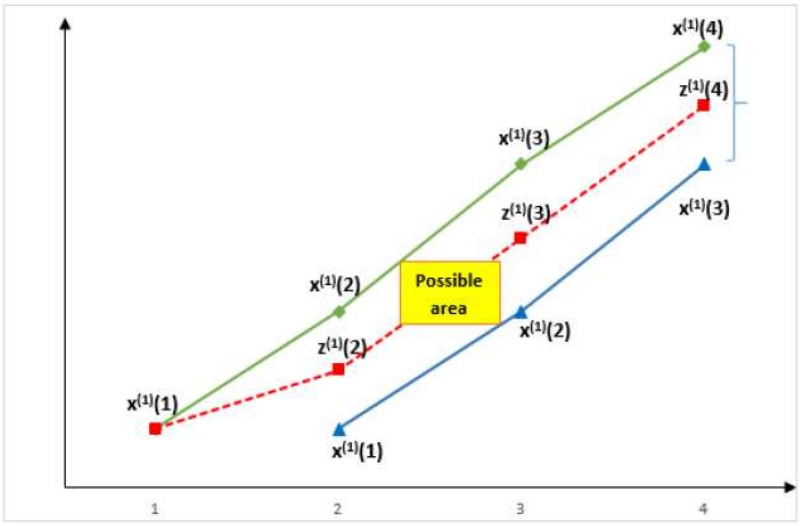

Fig. 6. Possible area of background values

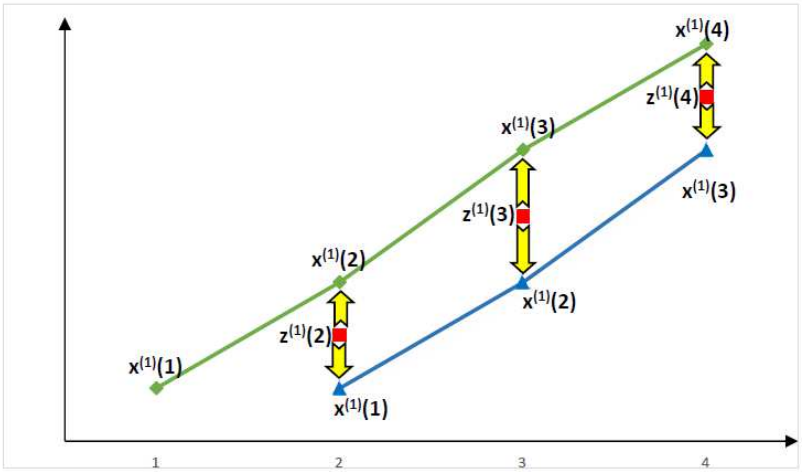

Fig. 7. Distribution of the adjustable background values

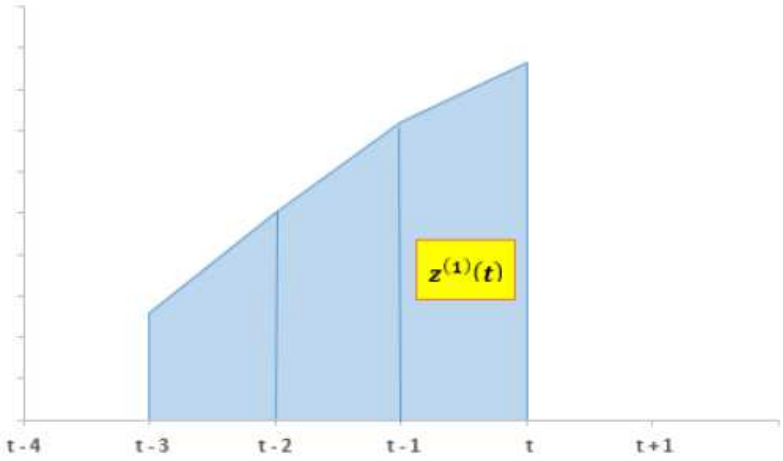

Fig. 8. Area under a curve

Since the curve function is unknown, the background value, $z^{(1)}(t)$ is calculated by the combination methods of Trapezoidal Rule and Simpson's Rule. These rules are used to determine the area underneath a graph. 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 rule is an extension of Trapezoidal rule where the integrand is approximated by a second order polynomial. Simpson's Rule is able to approximate more accurately the area under a curve but it limited to even number of region divisions. Therefore, the combination of Trapezoidal Rule, which can be used in any number of region divisions and Simpson's Rule are chosen to find the area under a curve in this research.

From Figure 11, the area underneath the curve from time interval t-3 to t can be determined as below:

$$\int_{t-3}^{t} x^{(1)}(t)\,dt = \int_{t-3}^{t-1} x^{(1)}(t)\,dt + \int_{t-1}^{t} x^{(1)}dt \tag{18}$$

Rearrange the Equation 18:

$$\int_{t-1}^{t} x^{(1)}(t)\,dt = \int_{t-3}^{t} x^{(1)}(t)\,dt - \int_{t-3}^{t} x^{(1)}(t)\,dt \tag{19}$$

By applying the Trapezoidal rule and Simpson's rule, the Equation 19 can be further simplified as follows:

$$\int_{t-1}^{t} x^{(1)}(t)\,dt = \frac{t-(t-3)}{2(3)}\left[\begin{array}{l} x^{(1)}(t-3) \\ +2\left(x^{(1)}(t-1)+x^{(1)}(t-1)\right)+x^{(1)}(t)\end{array}\right] \tag{20}$$
$$-\frac{(t-1)-(t-3)}{3}\left[x^{(1)}(t-3)+4x^{(1)}(t-2)+x^{(1)}(t-1)\right]$$

Hence, the background value, $z^{(1)}(t)$ is:

$$z^{(1)} = x^{(1)}(t-1)+\frac{1}{6}x^{(0)}(t-1)-\frac{1}{6}x^{(0)}(t-2)+\frac{1}{2}x^{(0)}(t) \tag{21}$$

where, t = 3, 4,……,n.

Preliminary Network Security Situation Prediction is the first part in this module to forecast the incoming security situation according to the previous and current situation assessment. This component adaptively modified Grey Verhulst algorithm which is more suitable to be used in predicting intrusion attack situation with its S-Shape behavior. The sequence of Network Security Situation Assessment, output from the Security Situation Assessment has been used as input in this prediction component. The process flow of Preliminary Network Security Situation Prediction is shown in Fig. 9.

First, a sequence of situational values, $X^{(0)}$ is retrieved from Security Situation Assessment:

$$X^{(0)} = \left\{x^{(0)}(1), x^{(0)}(2), ..., x^{(0)}(n)\right. \tag{22}$$

where:

$$x^{(0)}(t) \geq 0, t = 1,2,.....,n$$

With this sequence, a new sequence of accumulated data is built by applying the 1-Accumulated Generating Operation (1-AGO) to it. The accumulated data sequence, $X^{(1)}$ is as Equation 23:

$$X^{(1)} = \left\{x^{(1)}(1), x^{(1)}(2), ..., x^{(1)}(n)\right\} \tag{23}$$

where:

$$x^{(1)}(t) = \sum_{i=1}^{t} x^{(0)}(i)$$

for $X^{(0)}$ (i)≥0 and t = 1, 2,……, n.

Second, a sequence of adaptive background value, $Z^{(1)}(t)$ is generated by considering the consecutive (before and after) neighbors of $x^{(1)}$:

$$Z^{(1)}(t) = \left\{z^{(1)}(1), z^{(1)}(2), ..., z^{(1)}(n)\right\} \tag{24}$$

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, ……, n.

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

$$x^{(0)}(t)+az^{(1)}(t) = b\left[z^{(1)}(t)\right]^2 \tag{25}$$

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 the parameter matrix $A = \begin{bmatrix} a \\ b \end{bmatrix} = (B^TB)^{-1}B^TY$ and the matrixes of B and Y as below:

$$B = \begin{bmatrix} -z^{(1)}(2) & \left(z^{(1)}(2)\right)^2 \\ -z^{(1)}(3) & \left(z^{(1)}(3)\right)^2 \\ \vdots & \vdots \\ -z^{(1)}(n) & \left(z^{(1)}(n)\right)^2 \end{bmatrix} \tag{26}$$

$$Y = \begin{bmatrix} x^{(0)}(2) \\ x^{(0)}(3) \\ \vdots \\ x^{(0)}(n) \end{bmatrix} \tag{27}$$

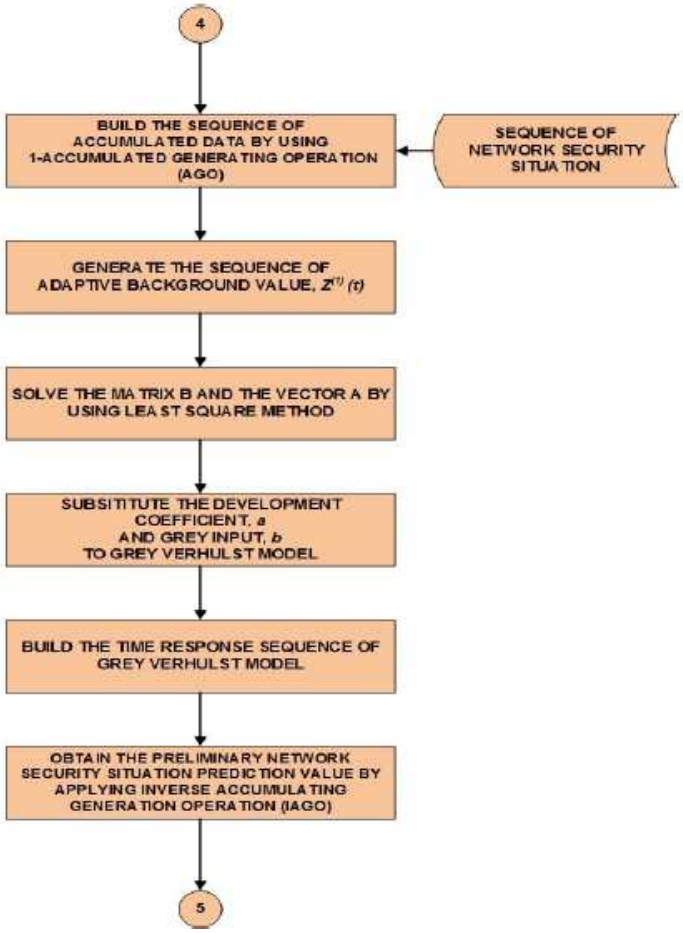

Fig. 9. Process flow of preliminary network security situation prediction

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 Equation 28 and 29:

$$a = \frac{DH - GE}{FG - D^2} \tag{28}$$

$$b = \frac{FH - DE}{FG - D^2} \tag{29}$$

where:

$$D = \sum_{t=3}^{n}\left[z^{(1)}(t)\right]^3 \tag{30}$$

$$E = \sum_{t=3}^{n}\left[z^{(1)}(t)x^{(0)}(t)\right] \tag{31}$$

$$F = \sum_{t=3}^{n}\left[z^{(1)}(t)\right]^2 \tag{32}$$

$$G = \sum_{t=3}^{n}\left[z^{(1)}(t)\right]^4 \tag{33}$$

$$H = \sum_{t=3}^{n}\left[z^{(1)}(t)\right]^2 x^{(0)}(t) \tag{34}$$

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:

$$x_g^{(1)}(t+1) = \frac{ax^{(0)}(1)}{bx^{(0)}(1) + \left(a - bx^{(0)}(1)\right)e^{at}} \tag{35}$$

where, $x^{(0)}(1) = x^{(1)}(1)$.

Finally, to obtain the preliminary network security situation prediction value, $x_g^{(0)}(t+1)$, 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:

$$x_g^{(0)}(t+1) = x_g^{(1)}(t+1) - x^{(1)}(t) \tag{36}$$

and:

$$x_g^{(0)}(1) = x^{(1)}(1) = x^{(0)}(1) \tag{37}$$

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

For Residual Prediction, it is second part in the Network Security Situation Prediction Module. It mainly focuses on forecasting the next prediction deviation based on the previous prediction residual. This component intent to ensure the predicted value closer to its actual value in a particular time-interval. In this research, Kalman filtering has been applied to achieve this intention. In general, Kalman filtering is an optimal estimator which can provide an efficient recursive computation means to infer the state of a process in order to minimize the mean of the squared error (Welch and Bishop, 2004). It has some significant features such as less parameters, simple calculation and convenient in real time processing (Lin *et al*., 2014). Thus, it has been chosen to forecast the incoming residual of adaptive grey Verhulst prediction in the research. The process flow of residual prediction is depicted in Fig. 10.

Firstly, the sequences of actual value and adapted grey Verhulst predicted value of network security situation are used to build a sequence of prediction error, *E*. The value of prediction error in each time interval, *e* can be obtained through Equation 38:

$$e(t) = x^{(0)}(t) - x_g^{(0)}(t) \tag{38}$$

where:

$$Actual\ value = \left\{x^{(0)}(1), x^{(0)}(2), x^{(0)}(3), \ldots\ldots\ldots, x^{(0)}(t)\right\} \tag{39}$$

$$\begin{aligned} &Adaptive\ Grey\ Verhulst\ Predicted\ Value \\ &= \left\{x_g^{(0)}(1), x_g^{(0)}(2), x_g^{(0)}(3), \ldots\ldots\ldots, x_g^{(0)}(t)\right\} \end{aligned} \tag{40}$$

Then, the initial estimated state, $\widehat{r_o}$ and estimation error covariance, P_0 have to be set. The value of $\widehat{r_o}$ 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:

$$\widehat{r_o} = e(t) = x^{(0)}(t) - x_g^{(0)}(t) \tag{41}$$

The more meaningful variables to be initialized, the faster convergence will be achieved. Then 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 below are used respectively. The model is assumed constant, therefore $F_{t+1} = 1$ for any $t \geq 0$. Control variables are not being used, so $B = 0$ and $u = 0$:

$$\widehat{r_{t+1|t}} = \widehat{r_{t|t}} \tag{42}$$

$$P_{t+1|t} = P_{t|t} + Q_{t+1} \tag{43}$$

After completing the time update equations, the first task during the measurement update is to compute the Kalman gain, K_{t+1} as Equation 44. Due to the same scale of state estimate, $\hat{r}$ has been used in the measurement, therefore in this research, $H = 1$:

$$K_{t+1} = P_{t+1|t}\left(P_{t+1|t} + R_{t+1}\right)^{-1} \tag{44}$$

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, $\widehat{r_{t+1|t+1}}$:

$$\widehat{r_{t+1|t+1}} = \widehat{r_{t+1|t}} + K_{t+1}\left(y_{t+1} - \widehat{r_{t+1|t}}\right) \tag{45}$$

where:

$$y_{t+1} = \widehat{r_{t|t}} = x^{(0)}(t) - x_p^0(t) \tag{46}$$

the deviation from real value on previous network security situation prediction. The final step is to update the posteriori error variance estimate through Equation 47:

$$P_{t+1|t+1} = \left(1 - K_{t+1}\right)P_{t+1|t} \tag{47}$$

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

In order to acquire the predicted value for incoming network security situation, preliminary network security situation prediction value, $x_g^{(0)}(t)$ which computed by using adaptive grey Verhulst model and residual prediction value $\widehat{r_{t+1|t+1}}$ which obtained from Kalman Filtering model have been combined. Figure 11 presents the process flow for acquiring the final network security situation prediction in the proposed mechanism.

Thus, the calculation of final predicted network security situation, $x_p^{(0)}(t+1)$ as Equation 48:

$$x_p^{(0)}(t+1) = x_g^{(0)}(t+1) + \widehat{r_{t+1|t+1}} \tag{48}$$

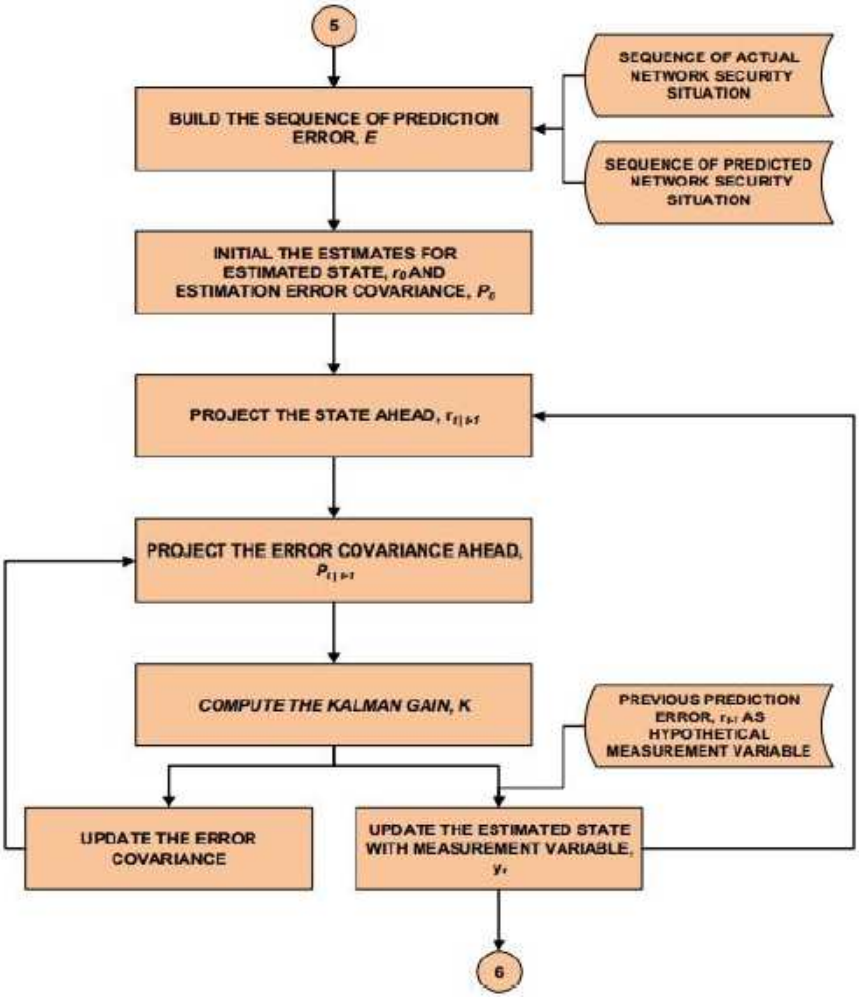

Fig. 10. Process flow of residual prediction

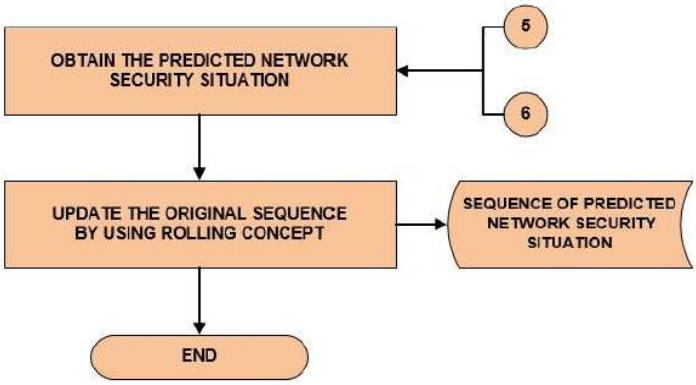

Fig. 11. Process flow of final network security situation prediction

Then, the result obtained will sent back to the predicted network security situation sequence for updating purpose. Lastly, all the processes in the proposed mechanism will be repeated and the sequences are keep updating timely.

Case Study and Results

A new NAv6 2015 Intrusion Detection Dataset has also been generated and used for testing purpose as the model takes into account the importance of

network assets in assessing the security situation. A testbed which simulates NAv6 Centre's network environment was designed and implemented in order to generate the test set as the input for NESSAP mechanism. Figure 12 illustrates the testbed for NAv6 2015 dataset generation.

The testbed was created by using VMware vSphere. There are three components in this testbed topology which are attacker machines, intrusion detection system and victim servers. Attack machines were designed to launch the probing and malicious payload attacks which can be detected for evaluating the performance of the proposed mechanism. Meanwhile, intrusion detection system was created to detect the attack packets from outsiders (attack machines) in a particular time period and victim machines which represent the servers in NAv6 Centre such as web server, database server, mail server and Domain Name System (DNS) server were connected to the outsiders (attack machines) through intrusion detection system and they act as attack targets in this testbed.

To run the testbed, two Ubuntu-based Linux attacker hosts were created and BackTrack 5 R3 was installed on them. The attackers typically launch the attacks on victim servers which represented the assets in the network. Meanwhile, Snort was deployed to capture the suspicious packets from the attackers. The log file generated by Snort was stored and used as input for evaluating the performance of NESSAP mechanism.

Asset Weight for NAv6 2015 Dataset

A new dataset had been generated for overall evaluation of the mechanism, i.e. NAv6 2015 dataset. This dataset was captured under the simulation of NAv6's network environment. The dataset consists of 861 intrusion alerts generated by Snort by analyzing probing attacks and malicious payload attacks. The dataset was generated by capturing network activity laced with attacks over a period of 36 h and it involved four main servers in NAv6, web server, database server, main server and DNS server.

The weight assignment of NAv6 2015 dataset was based on the concept of Analytic Hierarchy Process (AHP). A set of AHP table forms for each type of attack had been filled up by the network administrator from NAv6 Centre based on his knowledge and experience as well as business policy of the Centre. An average priority which represents the importance of the servers for each attack types such as probing attack, denial of service attack, remote to user attack and user to root attack have been calculated. Then by averaging all average priority values of each server for every type of attack, the asset weight which represents the importance of servers in this dataset is calculated as illustrated in Table 3.

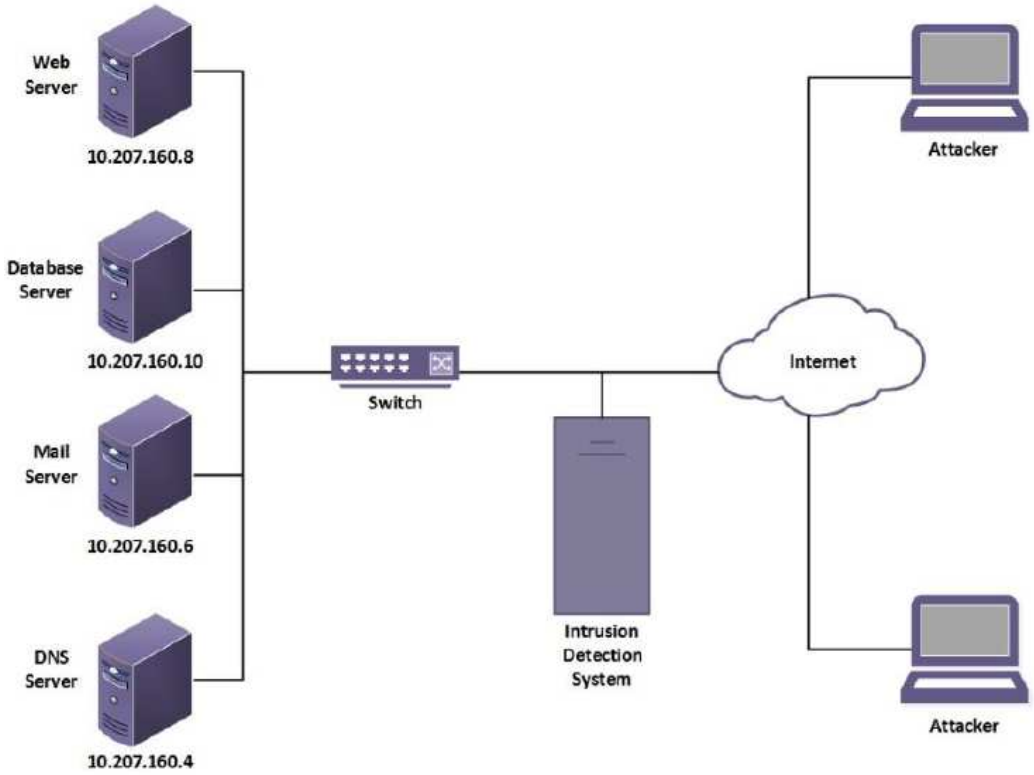

Fig. 12. Testbed for NAv6 2015 dataset generation

Assessment Result for NAv6 2015 Dataset

In order to examine the flexibility of the proposed E-NESSAS module in assessing security situation in various length of time interval, NAv6 2015 dataset had been divided based on 2 h time interval and it has 18 time frames in total. The NAv6 2015 dataset was then channeled into the E-NESSAS prototype to test the capability of proposed module in assessing the security situation. The situational value obtained from the experiment which represents the tendency of security situation with tangible and intangible criteria consideration on each asset in real environment is shown in Table 4.

The result showed that the situational value of network security situation in NAv6 Centre during the attacks in this dataset was between 0.07 and 0.26. The network situation started with low situational value and grew up steadily throughout the period from 11:01 to 17:00. During the increment, the servers, in this experiment were vulnerable to attacks by the attackers outside the network through the probing attacks. The graph showed that there was a slightly drop of situational value at time frame 17:01-19:00 and reverted to reach 0.2574 in the following hours. The changes were matched with the attack launched in the experiment. The attacker stopped the probing attack that time-frame and started the malicious payload attack at the last 4 hours in the experiment. By observing the changes of situational values which illustrate the trend movement of these values are matched with the attacks launched by attackers in particular time period. Therefore, it proved that the proposed E-NESSAS module can assess the security situation in any time interval with the aid of AHP in determining the importance of assets.

Prediction Result for NAv6 2015 Dataset

The experiment was conducted to evaluate the predictive accuracy performance of proposed grey prediction model. It used a set of 2 h time interval situational values which was generated by E-NESSAS model as input to channel into the developed prototype. The first 11 situational values were used to predict the last 7 situational values in NAv6 2015 dataset.

Prediction Results

In this section, the performance of AGV-NESSIP and AGVK-NESSIP models were evaluated. The purpose of this evaluation is to determine the appropriateness of considering the previous prediction error in the situation prediction. The results obtained are presented in Table 5.

Table 3. Weight of assets in NAv6 dataset 2015

Asset IP Address	Asset Weight
10.207.160.8	0.2681
10.207.160.4	0.2644
10.207.160.10	0.1977
10.207.160.6	0.2698

Table 4. Situational value for NAv6 2015 dataset

Date	Time frame	Situational value
10 June 2015	11:01-13:00	0.0755
13:01-15:00	0.0822	
15:01-17:00	0.0810	
17:01-19:00	0.0987	
19:01-21:00	0.1087	
21:01-23:00	0.1113	
23:01-01:00	0.1184	
11 June 2015	01:01- 03:00	0.1284
03:01-05:00	0.1348	
05:01-07:00	0.1521	
07:01-09:00	0.2013	
09:01-11:00	0.2129	
11:01-13:00	0.2223	
13:01-15:00	0.2453	
15:01-17:00	0.2477	
17:01-19:00	0.2247	
19:01-21:00	0.2574	
21:01-23:00	0.2356	

Table 5. Predicted situational values of proposed models for NAv6 2015 dataset

		Grey prediction models			
		Proposed AGV-NESSIP model		Proposed AGVK-NESSIP model	
Time frame	Real value	Predicted Value	RPE (%)	Predicted Value	RPE (%)
0901-1100	0.2129	0.1463	31.28	0.1728	18.86
1101-1300	0.2223	0.1605	27.80	0.1949	12.33
1301-1500	0.2453	0.1699	30.74	0.2078	15.27
1501-1700	0.2477	0.1732	30.07	0.2047	17.38
1701-1900	0.2247	0.1700	24.33	0.2052	8.68
1901-2100	0.2574	0.1608	37.55	0.2008	22.00
2101-2300	0.2356	0.1467	37.73	0.1740	26.12
MAPE (%)			31.36		17.23
RMSD			0.08		0.04

Table 6. Predicted Situational Values of Grey Models for NAv6 2015 Dataset

		Grey prediction models									
		Traditional GM (1,1) Model		Traditional grey verhulst model		EDGF verhulst model		Proposed AGV-NESSIP model		Proposed AGVK-NESSIP model	
Time frame	Real value	Predicted Value	RPE (%)	Predicted Value	RPE (%)	Predicted Value	RPE (%)	Predicted Value	RPE (%)	Predicted Value	RPE (%)
0901-1100	0.2129	0.1718	19.31	0.1548	27.29	0.4828	126.75	0.1463	31.28	0.1728	18.86
1101-1300	0.2223	0.1835	17.44	0.1653	25.61	0.5104	129.62	0.1605	27.80	0.1949	12.33
1301-1500	0.2453	0.2080	15.20	0.1694	30.95	0.5548	126.20	0.1699	30.74	0.2078	15.27
1501-1700	0.2477	0.2455	0.90	0.1663	32.89	0.6159	148.63	0.1732	30.07	0.2047	17.38
1701-1900	0.2247	0.2765	23.05	0.1565	30.34	0.6933	208.53	0.1700	24.33	0.2052	8.68
1901-2100	0.2574	0.3114	20.98	0.1417	44.97	0.7871	205.75	0.1608	37.55	0.2008	22.00
2101-2300	0.2356	0.3508	48.88	0.1237	47.49	0.8980	281.18	0.1467	37.73	0.1740	26.12
MAPE (%)			18.07		34.22		175.24		31.36		17.23
RMSD			0.06		0.08		0.44		0.08		0.04

The results showed that the MAPE of proposed AGVK-NESSIP and AGV-NESSIP models are 17.23 and 31.36% respectively. In other words, the prediction accuracy of AGVK-NESSIP model is almost 14% better than AGV-NESSIP model. As for AGVK-NESSIP model, it has a lower RPE than AGV-NESSIP model. It remains the RPE below 20% is at all the time frames except at 1901-2100 and 2101-2300. Due to this, AGVK-NESSIP model has smaller RMSD which is only 0.04 while AGV-NESSIP model has only 0.08 in this experiment. Hence, it showed that the proposed AGVK-NESSIP model has significant predictive accuracy compared with AGV-NESSIP model. Although there is a up and down in network situation between 1501 to 2101, but the result shows that AGVK-NESSIP model is still outperforms compared to AGV-NESSIP model in this situation. Therefore, it can be concluded the accuracy of prediction for the proposed prediction model can improve by adding residual prediction in the situation prediction.

Comparison with other Grey Prediction Models

For the purpose in claiming that the proposed grey prediction model has superior performance in forecasting incoming network security situation, a comparison test has been conducted among existing grey prediction models. Table 6 presents the predicted situational values generated by prediction models at every time interval.

The results showed that only traditional GM(1,1) and proposed AGVK-NESSIP models have achieved predictive accuracy above 80% while traditional grey Verhulst and AGV-NESSIP models only managed to achieve around 68 and 65% respectively. Although both traditional GM(1,1) and AGVK-NESSIP models have promising prediction results, but AGVK-NESSIP model has performed slightly better in this case with 0.84% lower MAPE and 0.02 smaller RMSD. In this experiment, EDGV Verhulst model has demonstrated the weakest performance due to its highest MAPE and RMSD compared with other prediction models. In this context, the assumption made in EDGF Verhulst model is considered inappropriate for the dataset. In other words, the performance of EDGF Verhulst is unconvincing and limited to certain network situations only. Meanwhile, compared with other prediction models, AGVK-NESSIP model behaves closer to the real value especially at 1701-1900. Hence, the results proved that the performance of AGVK-NESSIP model in the aspect of predictive accuracy surpassed other grey prediction models in forecasting incoming network security situation.

Conclusion and Future Work

The research commenced with an investigation into the concept of network security situation awareness, particularly exploring issues related to the network security situation assessment and prediction stages. The research proposed a mechanism in order to assess the current security situation in a network and to predict incoming security situation based on current and previous security situation. Within the proposed mechanism which included experiments by developing and implementing prototype of proposed assessment and prediction modules, this research has been successful.

In reality, a more intelligent and multi-functional intrusion prevention system is desired to complement intrusion detection system to secure the network. However, with the introduction of a more comprehensive network security situation assessment and an adaptive network security situation prediction models, this research has contributed in some significant degree to that domain. With more studies working to address the situation assessment and prediction, in the future, it is hoped that a better technology could improve the efficiency of the network security situation assessment and prediction models.

Author's Contributions

Yu Beng Leau: Propose the framework and implementing it to get the result. Analyze the results and compare with other existing methods. Writing this paper for publication purpose.

Ali Abdulrazzaq Khudher: Co-writing and editing the literature review.

Selvakumar Manickam and Samer Al-Salem: Co-implementing the proposed framework and analyzing the results.

Ethics

The authors confirm that this manuscript has not been published elsewhere and that no ethical issues are involved.

References

AAGD, 2009. Cyber security strategy. Australia Attorney-General's Department, Australian Government, Australia.

Anstee, D., 2015. 10th worldwide infrastructure security report. Arbor Networks, USA.

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

CO, 2011. The UK cyber security strategy-protecting and promoting the UK in a digital world. The Cabinet Office, UK.

El-Fouly, T., E. El-Saadany and M. Salama, 2007. Improved grey predictor rolling models for wind power prediction. IET Generat. Transm. Distribut., 1: 928-937. DOI: 10.1049/iet-gtd:20060564

Endsley, M.R., 1988a. Design and evaluation for situation awareness enhancement. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, (SAM' 88), SAGE Publications.

Endsley, M.R., 1988b. Situation Awareness Global Assessment Technique (SAGAT). Proceedings of the National Aerospace and Electronics Conference, May 23-27, IEEE Xplore Press, pp: 789-795. DOI: 10.1109/NAECON.1988.195097

Endsley, M.R., 1995. Toward a theory of situation awareness in dynamic systems. J. Human Factors Ergonom. Society, 37: 32-64. DOI: 10.1518/001872095779049543

FMI, 2011. Cyber security strategy for Germany. Federal Ministry of the Interior, Germany. p. 1-15.

ITU, 2015. International Telecommunication Union. Internet Users.

Li, D.C. and W.K. Lin, 2013. Employing GA-based adaptive grey model for learning with short-term sequence data. J. Grey Syst., 25: 96-106.

Lin, Y.H., P.C. Lee and T.P. Chang, 2009. Adaptive and high-precision grey forecasting model. Expert Syst. Applic., 36: 9658-9662. DOI: 10.1016/j.eswa.2008.12.009

Lin, Z., L. Xiujie, M. Jing, S. Wenchang and W. Xiufang, 2014. The prediction algorithm of network security situation based on grey correlation entropy Kalman filtering. Proceedings of the IEEE 7th Joint International Information Technology and Artificial Intelligence Conference, Dec. 20-21, IEEE Xplore Press, pp: 321-324. DOI: 10.1109/ITAIC.2014.7065059

Lin, Z., S. Li and Y. Ma, 2010. Real-time intrusion alert correlation system based on prerequisites and consequence. Proceedings of the 6th International Conference on Wireless Communications Networking and Mobile Computing, Sept. 23-25, IEEE Xplore Press, pp: 1-5. DOI: 10.1109/WICOM.2010.5601285

MOSTI, 2012. National cyber security. Ministry of Science, Technology and Innovation, Malaysia.

PricewaterhouseCoopers, 2015. Information security breaches survey. Department for Business Innovation and Skills, PwC, London, UK.

Symantec, 2015. Internet Security Threat Report 2015. Symantec Corporation, USA.

Tan, K.M.T., 2013. Learning and Prediction of Relational Time Series. 1st Edn., Naval Postgraduate School, pp: 236.

Welch, G. and G. Bishop, 2004. An introduction to the Kalman filter. UNC-Chapel Hill, Department of Computer Science.

Wen, J.C., K.H. Huang and K.L. Wen, 2000. The study of α in GM(1,1) model. J. Chinese Inst. Eng., 23: 583-589. DOI: 10.1080/02533839.2000.9670579

WH, 2011. International strategy for cyberspace-prosperity, security and openess in a networked world. The White House, USA.

Xiaorong, C., L. Su and L. Mingxuan, 2012. Research of network security situational assessment quantization based on mobile agent. Phys. Proc., 25: 1701-1707. DOI: 10.1016/j.phpro.2012.03.298

Yao, A.W., S. Chi and J. Chen, 2003. An improved grey-based approach for electricity demand forecasting. Electric Power Syst. Res., 67: 217-224. DOI: 10.1016/S0378-7796(03)00112-3

Yeh, C.W., C.J. Chang and D.C. Li. 2009. A modified grey prediction method to early manufacturing data sets. International MultiConference of Engineers and Computer Scientists, Mar. 18-20, Newswood Limited, Hong Kong.