Malware Risk Analysis on the Campus Network with Bayesian Belief Network

Aliyu Mohammed, Haitham A. Jamil, Sulaiman Mohd Nor, Muhammad Nadzir Marsono
Department of Microelectronic and Computer Engineering
Universiti Teknologi Malaysia
Faculty of Electrical Engineering,
Skudai, 81310, Johor Malaysia
maliyyu@fkegraduate.utm.my, sulaiman@fke.utm.my, nadzir@fke.utm.my
haithamjamil@gmail.com

ABSTRACT

A security network management system is for providing clear guidelines on risk evaluation and assessment for enterprise networks. The threat and risk assessment is conducted to safeguard enterprise network services to maintain system confidentiality, integrity, and availability through effective control strategies. In this paper, based on our previous work in analyzing integrated information security management and malware propagation on the campus network through mathematical modelling, we proposed Bayesian Belief Network with inference level indicator to enable the decision maker to understand and provide appropriate mitigation decisions on the risks posed. We experimentally placed monitoring sensors on the campus network that gives the threat alert priority levels and magnitude on the vulnerable information assets. These methods will give a direction on the belief inferred due to malware prevalence on the information security assets for better understanding.

KEYWORDS

Network security; malware propagation modelling; Bayesian Belief Network; risk and threats

1. INTRODUCTION

Most available malicious software (adware and spyware) affect users' productivity, compromise their privacy, and modify (damage) system assets. We determine relations between the infection distribution and also the status of the infected system to estimate the general effect on the enterprise network. The methodology presented within this paper determines and discusses the following concepts: (i) Infections and probability types of occurrences triggered by malware. (ii) Risk computation with uncertainty compensation of infection and recovery models based on Bayesian Belief Network. The risk evaluation is based on the relationships among the most critical assets, and threats that are likely to those assets and their vulnerability impacts. This findings can then be applied for mitigation and control countermeasures for the organizations infrastructural assets being at risk[1].

The prevalence of malware propagation on the Internet and the campus network in general has caused the loss of data and vital information. Experts in information security agree that data breaches are one of the inherent costs of doing business online[2]. Organizations must take necessary steps to safeguard customer information and provide proper risk management processes that could be carried out should a data breach occur. The recent data breach report indicates that the Federal Trade Commission (FTC - US) brought suit against hospitality giant Wyndham Worldwide in late June 2012 for allegedly exposing 619,000 consumer payment account numbers

to a domain in Russia. This is despite the FTC claims on the defendants' failure to maintain reasonable security allowing intruders to obtain unauthorized access. This results in $10.6 million fraudulent charges dating back to 2008 according to court documents. The FTC reported that identity theft and other scams cost Americans $1.52 billion in 2011. This is despite all efforts to combat such theft, it is still on the rise[2].

Bayesian Belief Network provides the understanding to enable the containment of malware propagation based on the risk posed by the malware threat. The BBN has both the quantitative and qualitative abilities to effectively measure the prevalence of the malware risk factor on the vulnerable assets. The BBN inference support system is a tool that correlates and give causal relationships that exist between risk factors and risk key indicators with their associated operational attributes [3].

The paramount question that is always being asked is how do we effectively understand the magnitude of malware propagation and prevalence on the network assets? How do we present an understandable risk assessment to the decision maker for easy decision? To answer these questions we have to look at the inner operations of BBN and the enterprise risk assessment and evaluation with a view to understand the effects of malware prevalence on network assets.

Risk assessment handles the evaluation of the current risk factor status that is based on the probability and also the consequence of occurrence. It suggests that when the Bayesian Network model is built, it allows the organization to have the understanding of various choices in the network structure. This network probability updating will not only continuously cuts down on the data uncertainty, it offers the enterprise the risk scenario with real-time and up-to-date analysis[4].The composite risk probability concept for the generation of attack data, as well as connected risk assessment approach utilizing a homogeneity method for fast evaluation of large systems needs to be considered[5]. A technique for lifecycle information security risk assessment which provides helpful guidance just before beginning a risk assessment process is desirable. At the moment, within our knowledge, research regarding how to utilize Bayesian Belief Network (BBN) inference using both available data and evidence based information on malware prevalence on the network infrastructure is very limited. However, there is an increasing curiosity about how we can apply Bayesian Network (BNs) using both data plus some evidence information to understand the magnitude of malware propagation prevalence and damages to network infrastructure[6].A good example of decision analysis of statistical distribution denial-of-service (DoS) flooding attacks was presented by Li et.al[7].

The remainder of this paper is structured as follows. Section II describes briefly the mathematical modelling and tools for the malware propagation capture and analysis. The section also describes the basic principles of Bayesian Belief Network (BBN). This includes the probabilistic conditional inferences and decision analysis on risk due to threats and vulnerability issues. Section III discusses the implementation of Bayesian Belief Network and its application towards the prevalence of malware on the network. This is to assess risk as a factor of threat, vulnerability and cost impact on the enterprise assets; based on the malware propagation prevalence on the campus network. Finally, some concluding remarks for future works is made in section IV.

2.MODELLING OF MALWARE PROPAGATION AND STATISTICAL CAPTURE TOOLS

2.1 Identifying Threats to Information Assets

The question to ask when conducting a risk analysis on how to prevent information theft is, "What can happen to our information?" The answers are long but broadly classified to include the following: (i) Virus infecting server that stores the data and tries to corrupt the files (ii) Trojan horse copying sensitive and personally identifying information to be transmitted to an attacker's FTP site. (iii) Staff leaving a backdoor in an application to steal or destroy information, (iv) Employee can lose a laptop with vital information; (v) Denial of Service (DoS) attacks can affect key database and applications. Enterprises must protect the privacy of information regardless of where or how it is stored. Figure 1 shows a typical scenario for a campus network on how sensors are placed with other articulated control measures and mitigation strategies. We are interested to know in this typical scenario, how malware propagates through a campus network. With appropriate mathematical SIR (susceptible, infectious and recovered) epidemiological model parameter analysis will allow for observing the propagation trend as explained in the next section.

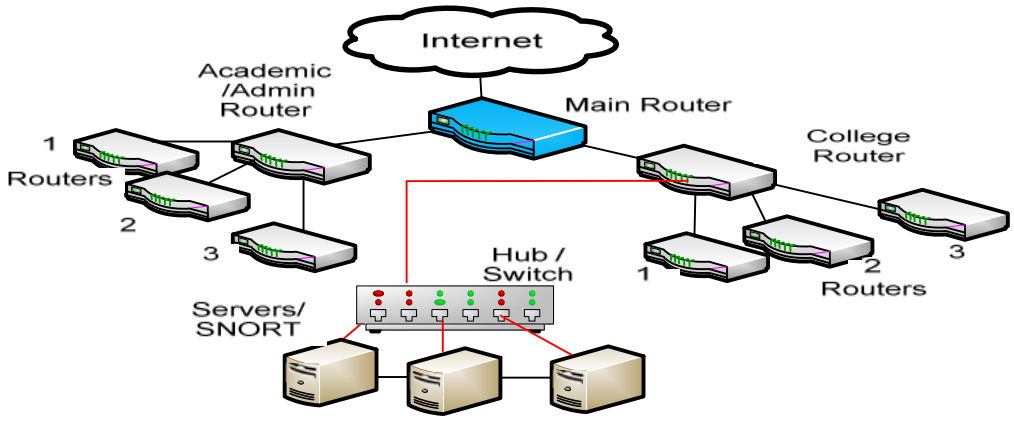


Figure1. Tools for statistical data collection on the campus network

2.2 Modelling of Malware Propagation on the campus network

The simplest SIR model that was described by Kermack and Mckendrick in 1927[8] is regarded as the most famous mathematical model for the spread of infectious disease. The population is grouped into three: susceptible (*S*), infected *(I)*, and recovered *(R)*. A susceptible host *(S)* is a host in which the operating system, applications and anti-virus are not updated and thus is vulnerable to attacks. With the right code triggered, a susceptible host can be changed to be in the infected state easily. This happens when the user (host) visits a malicious web site, when a malware is transferred to the rest via a thumb drive or re-infected via the network (including mail attachment). An infected host *(I)* will remain in this state until the host is cleaned. The prerequisite for the host to be cleaned is that the signature must be available and the host scanned and cleaned of the malware. This will move the host from the infected state to the recovered state. The recovery state *(R)* takes place when the host has now recovered and is cleaned from the particular malware type. The recovery is through the use of end-user antivirus, updates and patch management. At this stage it is assumed that the host is immune from this malware. However, the host is still considered susceptible from other malware especially zero-day malware. The SIR model is easily written using ordinary differential equation which implies a deterministic model

with continuous time. The SIR model for spread of disease was considered and based on the background of the virulent new strains. The population is assumed fixed during the epidemic in the SIR model. Based on this, the modelling is to first identify the independent and dependent variables, where the independent variable is time *t* to be measured in days or weeks. Further modelling works that consider the two-factor model is discussed in[9-11] while the handling of removal rate with effects of quarantine is discussed in [12,13].

The parameters used for the SIR modelling are described as: *Sn (t)* is the number of susceptible hosts at time *t, In (t)* is the number of infected hosts at time *t, Rn (t*) is the number of recovered hosts at time *t, β* is the average number of adequate contacts (i.e. Contacts sufficient for infection) of host per unit time. Thus, *β* is also known as the infection rate, *r* is the recovery rate, t is the unit time and *N* is the total number of host on the network with *n* as the infinitesimal increase in the total population of hosts[14,15]. Thus, the SIR model ordinary differential equations are:

$$\frac{dS_n}{dt} = -\beta \frac{S_n}{N_1} \tag{1}$$

When rationalized with n changes to *(i)* susceptible, thus

$dS = -\beta \frac{S_i}{N_i} dt$, and the susceptible increases from *i to i+1*

$$S_{i+1} = S_i - dS_i$$

Also the infectious hosts are differentiated with respect to S_n/N_1

$$\frac{dIn}{d\left(\frac{S_n}{N_1}\right)} = \beta \frac{S_n}{N_1} - r \frac{N_1 - S_n}{N_1} \tag{2}$$

Rationalizing from n==i, and i+1==n

$$dI = \left(-\beta \frac{S_i}{N^2_i} - r \frac{N_i - S_i}{N_i^2} \right) d\frac{S_i}{N_i}$$

Where $I_{i+1} = I_i + dI$

$$\frac{dRn}{dt} = In - r \frac{N_1 - S_n}{N_1} \tag{3}$$

$$dR_i = \left(I - r \frac{N_i - S_i}{N_i} \right) dt$$

where $R_{i+1} = R_i + dR_i$

2.3 The Bayesian Belief Network Principles

The essence of the Bayesian approach is to provide a mathematical rule explaining how it should change existing beliefs in the light of new evidence. In other words, it allows scientists to combine new data with their existing knowledge or expertise.

Mathematically, the Bayes' rule states

$$Posterior = \frac{Likelihood * prior}{marginal \cdot likelihood}\ ;\ P(R=r \mid e)=\frac{P(e \mid R=r)P(R=r)}{P(e)} \quad (4)$$

Where $P(R=r \mid e)$ denotes the probability that random variable *R* with value *r* given the evidence *e.* The factor in the denominator is just a normalizing constant that ensures that the posterior adds up to *1*. These can be computed by summing up the numerator over all possible values of *R*; meaning that:

$$P(e) = P(R=0,e) + P(R=1,e) + .. = sum_r P(e \mid R=r)P(R=r) \quad (5)$$

This procedure in equation (5) is termed as the marginal likelihood (as we have marginalized out over *R*) and provides the prior probability of the evidence. Thus, the concept of the child, parent, consequence and the conditionality's are as depicted through the deduction and abduction process as in [16] and discussed further in [16,17].

Bayesian Belief Network inference System is a theory that complements reasoning under uncertainty by delivering a coherent framework to create a decision in compliance while using preferences from the decision manager [18]. Decision theories provided an axiomatic reason for preferences and represented graphically by decision trees and influence diagrams. The influence diagram includes probabilistic dependencies between variables, such as the Bayesian Belief Network. However, influence diagrams contain decision nodes that provide choices and value nodes that provide utility measures.

A Bayesian network consists of a graphical structure that encodes domain variables, were the qualitative and quantitative relationships between them provides for the encoding probabilities over the given variable[19]. According to Heckerman [20],a Bayesian network can be considered as a set of variables *X* that relates to network structure S that tries to encode a set of conditional independence factors about the variables in *X*, and a set of *P* being a local probability distributions associated with each set of the variable. Conditional independencies in *S* encodes that there are no arcs that relate them. In a given structure S, the joint probability distribution for *X* can be depicted by the equation:-

$$p(x) = \prod_{i-1}^{n} p(x_i \mid pa_i) \quad (6)$$

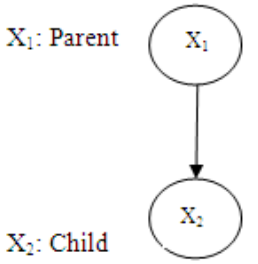
These local probability distributions P corresponds to the terms of the products indicated in equation 6 above. This show the pair of (*S, P*) are the joint distribution of p(x).
These Bayesian Network can be defined as follows: -

$$BN=(S,P)\ S = \{(X_j, X_i) \mid X_i \in X, X_j \in pa_i\};\ P = \{p(X_i \mid pa_j) \mid X_i \in X\} \quad (7)$$

The quantitative aspect of Bayesian Belief networks enables for accommodating subjective judgments (expert opinions) as well as probabilities that are based on objective data[21]. In general, we use the Bayesian network typically to compute all probabilities of interest since a Bayesian network for *X* determines a joint probability distribution for *X*. For example, *P* (f | *a, b, c, d, e),* is the probability of *f* following the observations of the other variables *(a, b, c, d, e),* and can be computed as follows:

$$P(f \mid a,b,c,d,e)=\frac{P(a,b,c,d,e,f)}{P(a,b,c,d,e)} = \frac{P(a,b,c,d,e,f)}{\sum_{f} P(f',a,b,c,d,e)} \quad (8)$$

2.3.1 Modelling Process in Bayesian Network



P(X1)	
X1=0: false	X1=1: true
0.5	0.5

Conditional Probability Table (CPT)

X1	P(X2/X1)	
	X2=0: false	X2=1: true
0: false	0.98	0.02
1: true	0.45	0.55

$P(X_2/X_1)$: Conditional probability of X_2 given that X_1 has occurred.

Figure2. Modelling parameter with Bayesian Network.

Figure2 shows concise principles of Bayesian network. It indicates the relations that exist between two variables X_1 and X_2. The two variables are in binary structure whose values ranges from *0* (false) or 1 (true). The causality response that exists between each node is represented through a conditional probability table (CPT). The table brings out the relationship between the parent node X_1 and the child node X_2 with an arrow that shows their relationship.

Given the value of the variable $X_1=1$ on the parent node, the conditional probability effect of the child node $P(X_2/X_1)$ is determined through the CPT. Based on the marginalization process outlined by authors in[22], the probability of $P(X_2=1)$ can be derived and computed from the equation 9 as:

$$P(X_2=1)=\frac{\sum_{X_1=0}^{1} P(X_2=1/X_1)*P(X_1)}{\sum_{X_1=0}^{1}\sum_{X_2=0}^{1} P(X_2/X_1)*P(X_1)} \quad (9)$$

In this case the causal relations between risk events can be defined with Bayesian network with only two or more nodes. This includes the two nodes of Figure 2 as minimum units. The conditional probability of the target node will be improved based on additional observation on the information from the parent or the child nodes. Further details on Bayesian network modelling can be found in [22][3].

2.4 Effects of Connectivity and control countermeasures

The malware propagation ability can be understood through the factor of connectivity and control as it relates to cause effect consequences. The connectivity is the measure of rate of propagation of the malware on the network that results in determining the risk due to the threats posed on the network. In order to understand and appreciate the cause effect due to connectivity and control measures, we employ the Bayesian Network modelling tool *GeNIe.* This is indicated with the cause (trigger), the risk event (effect) and the consequence (resulting factor). The magnitude is checked through the control measure as in Figure 3.

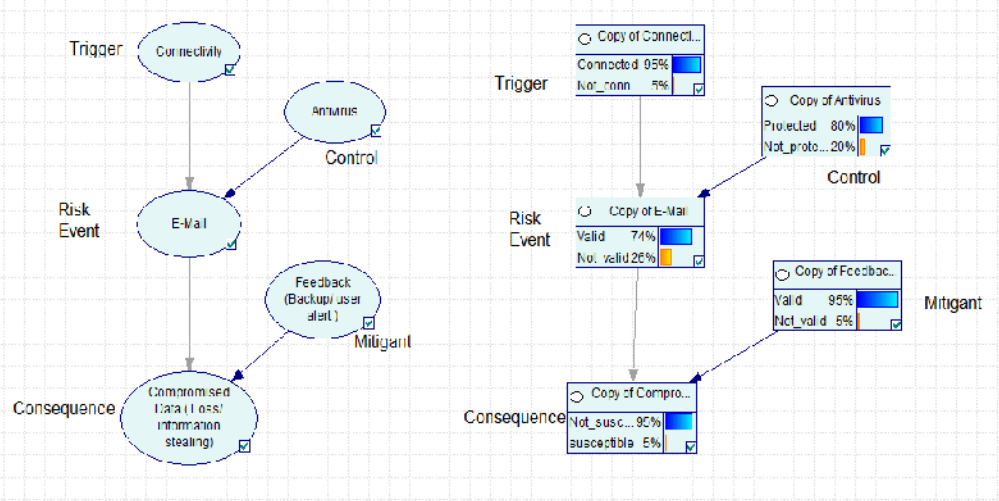


Figure 3. E-mail connectivity through cause effect factor

The issue of control is a measure of effectiveness of the available countermeasure that can be applied to reduce the impact before it happens. While mitigation process takes place after the consequence in order to proffer for possible remedy. The cause, effect, and consequence depicted in the Figure 3 through the use of the rate of propagation parameter considered in the modeling section. The mitigation helps to finding remedy for the aftermath effect.

3.Implementation using Bayesian Belief Network System to Model Malware Risk

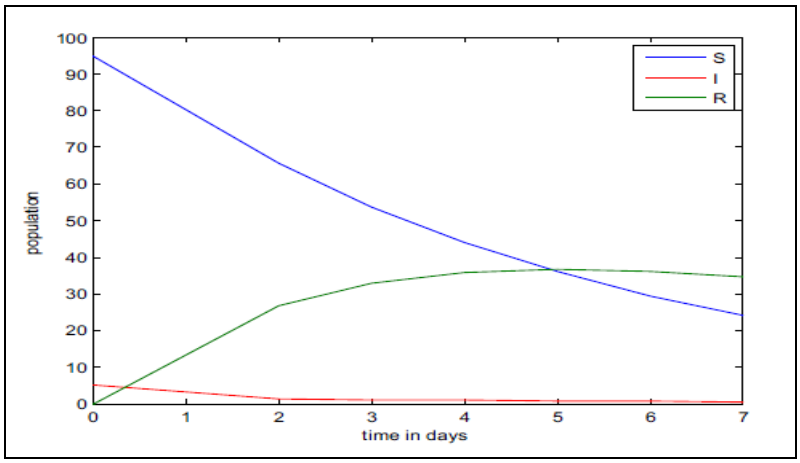
The Bayesian Belief Network is effective and has adequate technique for modelling, measuring and to a certain extent managing the characteristics of malware propagation risk on the network environment. This is with a view to protect the campus information assets. This is achieved through the use of prior knowledge of the causal risk factors and the possible probabilistic reasoning concept of the systems. In a nut shell, the Bayesian Belief analysis is to allow for improving the prior determined factors values in the effect of any additional information obtained about the variables in the network. This is for building the conditional probability table (CPT), when such similar information's are not available; the tables could be built based on opinion results. The assets risk models might be readily developed utilizing a graphical Bayes internet editor like the *GeNIe* application program [23].

Let's look at a situation when a Trojan malware propagates through a network of nodes. A model developed with the basic SIR model based on the typical epidemic modelling is considered and applied. The epidemic models generally explain the rapid outbreak that occurs in the network environment for a period of less than one year. While it becomes endemic if the scenario persist and extend to a longer period. The present situation is that we based our study on situation that the propagation malware attack in the analysis is a single class type. The experimental modelling simulation of worm propagation based on the SIR model is discussed in the next section.

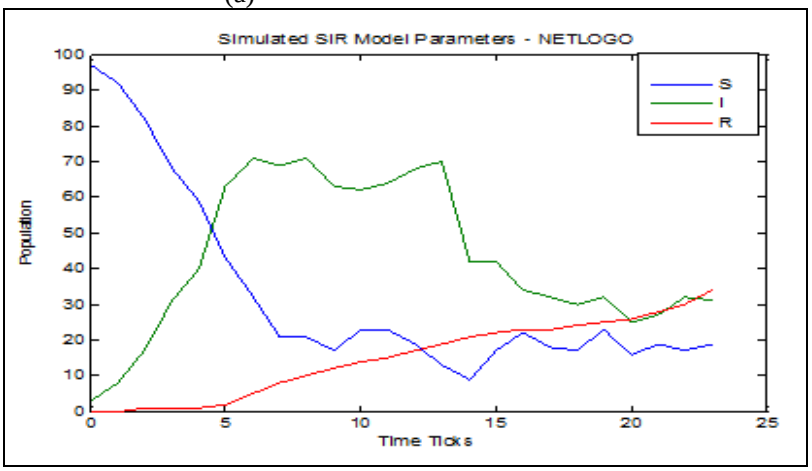
3.1 Worm Propagation based on SIR Model Simulation

The three worm propagation parameters *S*, *I*, and *R* derived from equations (1), (2) and (3) were coded with MATLAB simulation. The parameters were based the experimental data obtained

from Snort sensors placed on the campus network. The Experiment was for a period of seven days. The propagation rate parameter β and r are infection rate and removal rate respectively were determined through the generated data from the sensor and simulated. The same parameters were simulated using the Netlogo system software to provide for similarity understanding as shown in Figures 4 (a) and (b). The initial condition for the parameters is as follows: - $\Delta t = 1$; $t = 1:7$; $S_i = 50$; $I_i = 0$; $R_i = 0$; $N = 100$; $\beta = 50$; $r = 0.2$. While the initial values are based on the campus network segment with N number of hosts, time t is for seven days. The infection rate and removal rate are conceptualized for the purpose of simulation based on the population considered during the experiment. Further details on the campus network worm propagation modelling can be found in [24].



(a)



(b)

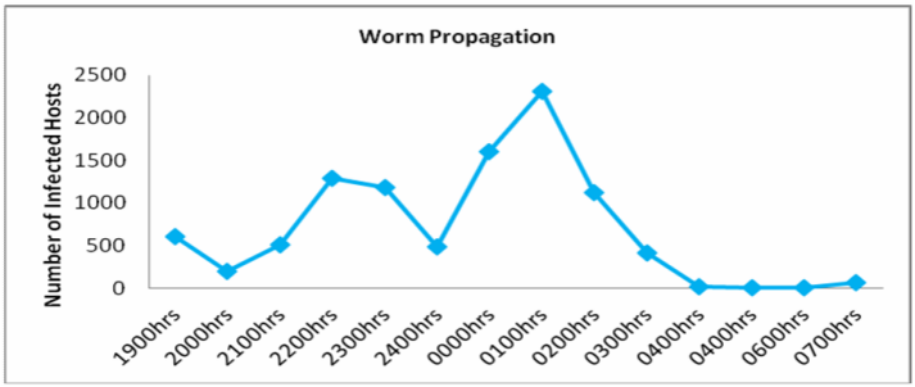
Figure4. (a) Mathematical and (b) Simulation Model Parameters

The Figures 4(a, b) above shows the typical worm spread observed for a period of some days on the campus network environment. The Snort sensor was used on the various campus network segments, which includes the colleges, academic areas, and the administrative environment. The results are analyzed to see the effect as it applies to the topological trend of the network. The characteristics for the worms are based on the propagation effect for a period of seven days in Figure 4(a), and that of (b) is for a time tick scenario. The parameters of the model was used and

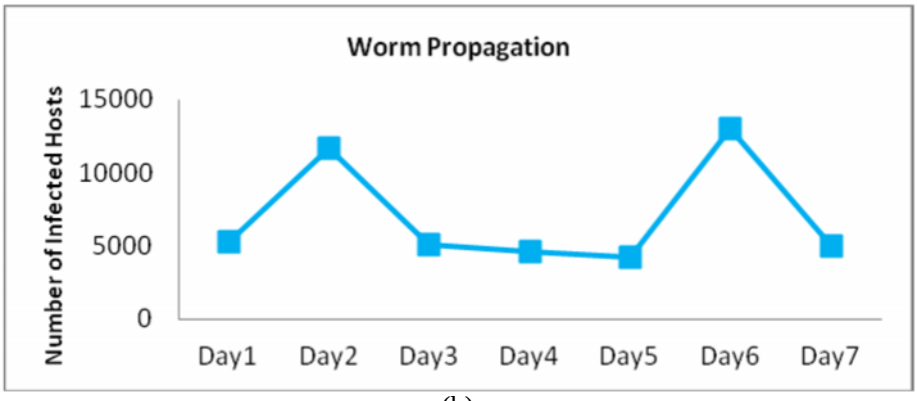
translated into the parameters in the Netlogo software. This is through observing the trend of the propagation parameters in comparison to what was obtain from the Matlab simulation. The propagation characteristics of the parameters applied with Netlogo provides a similarity trend that indicates consistency in the shape of the three varying factors SIR. The propagation parameters (infection rate, removal rate, magnitude, and impact) will be translated and rationalized into fitting it with the Bayesian network for inference. Thus risk as a result of the threat posed by the malware will be determined and presented for easier understanding and to allow for providing mitigation strategies.

3.1.1 Malware alert from monitoring sensor

The monitoring sensor snort IDS was configured for a period of time on the campus network segment during the experimental phase. The malware alert recorded shows the class types of worm variants that are infecting hosts on the network. The trend was observed and a typical malware labelled as *ET Trojan TinyPE* will be used in this study to understand the likely risk it will pose based on the rate of infection and impact on the assets.



(a)



(b)

Figure5 (a, b). *ET Trojan TinyPE* Worm Propagation (1:2008576:3)

3.2 Probability Factor Analysis with BBN

In order to estimate the risk posed by this particular worm, we will start by looking at risk and its dependencies. As we know, risk is a function of threat, vulnerability and cost. In this case, the

threat will be caused by this worm. We then consider factors that influence the threat (i) the severity level of the worm and (ii) the rate by which the worm is propagating in the network. Vulnerability is a measure of the degree of exploits that is available to the threats. The causes are as mentioned, unpatched system, antivirus with non updated signatures etc. Costs in this case will be the degree of loss incurred after the exploits has taken place.

Thus the initial equation of risk,

Risk = *f* (threat, vulnerability, cost), becomes

Risk = *f* (severity level, rate of propagation, vulnerability, cost)

A host can only be infected if it is vulnerable. The degree of vulnerability together with the rate of worm propagation will generate the rate by which the hosts will be infected. Thus the above equation can be simplified to be

Risk = *f* (severity level, rate of infected hosts, cost)

The rate can be number of hosts infected per minute, hour or day. This rate will depend on how fast we want to update our BBN model.

Based on this, in the BBN model the CPT factors that will be used in the calculation of the risk are:

(1) Severity level
(2) Rate of infected hosts
(3) Cost

Next, we will determine the parameter ratings that will be used for each of the factor mentioned above. We will use a simple BBN model to illustrate this idea. Also in the illustration, the BBN Model is used for the effects of a single worm. In reality we will have to consider the joint effects of multiple malware. This will be discussed in some other paper.

Severity level:
The severity level of a particular malware will be based on the severity level assignment given by Snort. Snort assigns a seventy level of I, II, Ill and IV, I being the most severe and IV the least. We assign a probability of 0.4 to I, 0.3 to II, 0.2 to III and 0.1 to IV to reflect the degree of severity.

Rate of infected hosts:
Rate of host infected is obtained from the propagation parameter of Trojan malware captured for the period of seven days as shown from the graph in the paper. Figure 5b, indicates that the total host population on the segment is = 15000, while the infected host for one day is = 5000. Therefore rate of infected host = 5000/ 15000 = **0.33** for that particular day. This is updated for following days.

Cost:
To simply the discussion, the cost impact rating for a particular segment is either **0 or 1**. **0** implies the segment does not have important and critical assets whilst **1** is the reverse. We can assign a more fine grain level, e.g. network segment with critical servers would be assigned the highest value, segment with admin group a second level until the lowest least critical segment.

Using the above, we now proceed to develop the BBN risk model and study few scenarios. These scenarios include the extreme case of all metrics in the above factors having the highest values

where we expect the risk generated to be the highest to all low where the risk will be the lowest and in between.

The following is the BBN model with the CPT and the resulting risks.

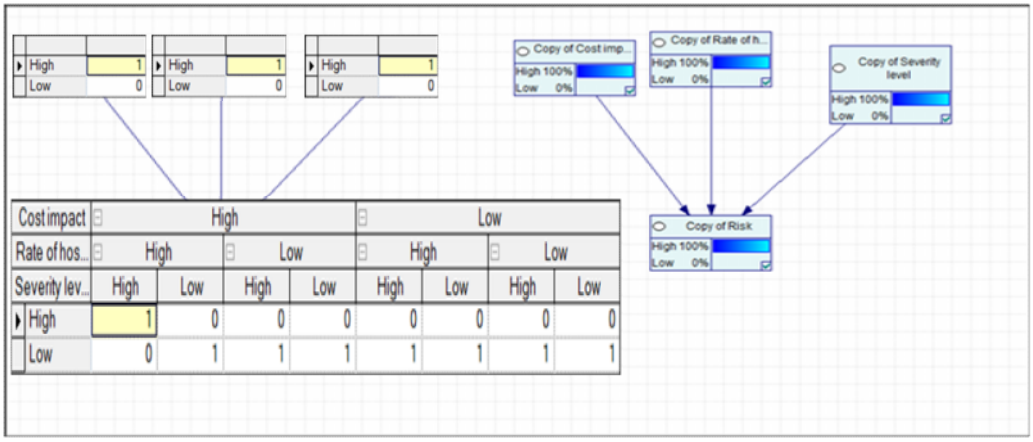


Figure 6a. BBN Malware Propagation Risk Analysis (highest risk)[23].

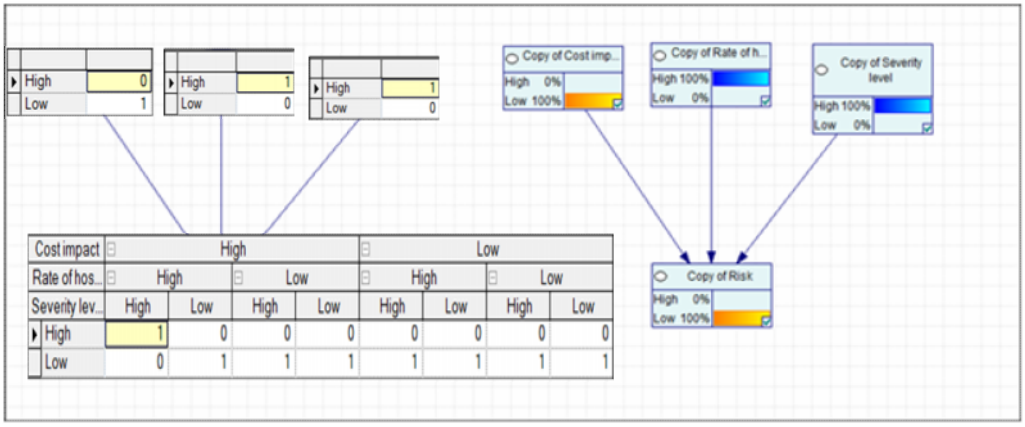


Figure 6b. BBN Malware Propagation Risk Analysis (lowest risk)

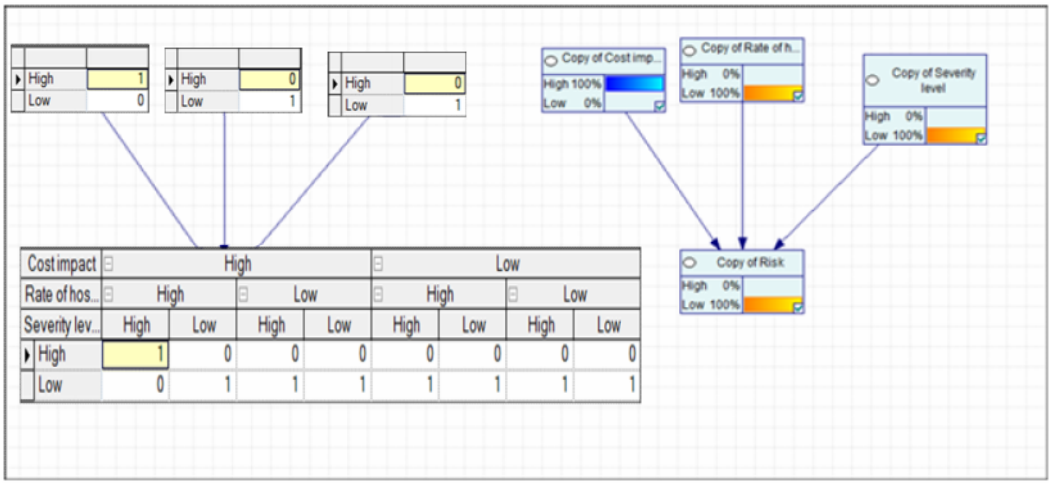


Figure 6c. BBN Malware Propagation Risk Analysis (lowest risk)

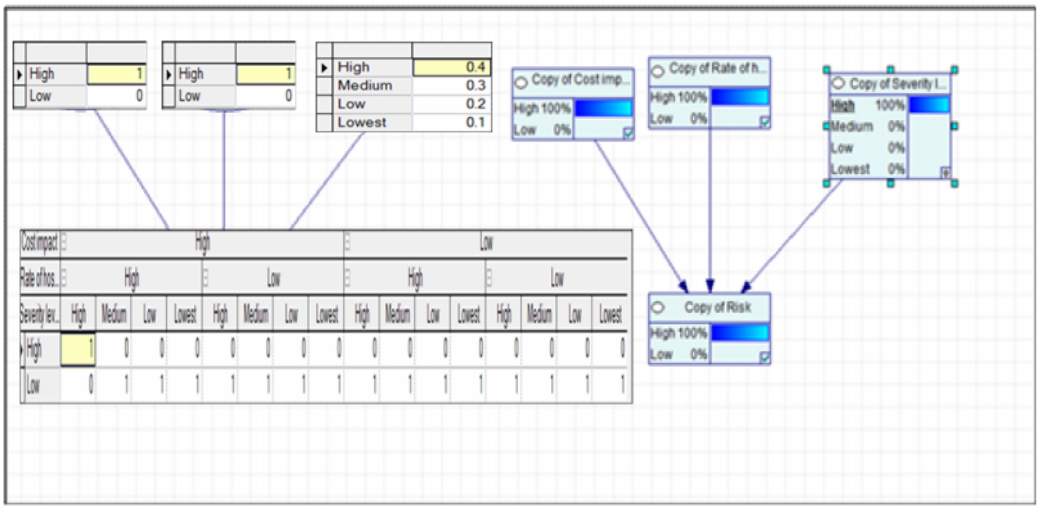


Figure 6d. The CPT with an evidence set at high severity level

3.3 Analysis and discussion

The results of the experiments presented in Figure5 (a, b) is the propagation characteristics of the malware variants as alerted by the monitoring snort sensor on the network. The threats posed by the malware are being determined based on the infection rate, severity, impact and the rate of the false positive factor. This is the criteria used for the calculation of the risk and threat rating factor. The use of Bayesian network with probabilities can be analyzed through the parameters that are critical to the risk factor for the particular vulnerable asset. The worm propagation parameter determines the level of threat; the vulnerability factors are based on the available control to the network infrastructural assets. Although, the result only considers a single type of malware and host IP with varying propagation rate on a particular network segment using BN. In future, we will consider multiple malware variants on various network segments on the campus network and use the result to determine the aggregated risk and threat rating in order to present a concise output on a dashboard. The work will be on the applications of the BN approach together with other decision support techniques to present an easily understandable output for the decision maker and security management team to view and provide for effective control and mitigation strategies. This specifically will be based on campus network infrastructural information security assets.

4. CONCLUSION

The understanding of threat analysis methods provides effective ways of differentiating between what are actual and perceived risk on the network. Therefore, risk evaluation is a kind of challengeable task and is undoubtedly a long term issue to enable for the running of robust campus networks infrastructure. The evaluation result goes a long way in helping the management to improve on the levels of information security system of the organization. Clear understanding of malware and virus and their associated propagation mechanism structure that forms the attacks channels is a critical part in recognizing how effectively protecting against the overall threats and risks on the campus network environment. The security network management system based on Bayesian Belief system provides a clear understanding ability to inform for management policy implementation and pave way for a better decision making. We provided through analysis the ability to have a comparable concept of malware prevalence and impact through Bayesian Belief Network inference systems. The inference engines overall importance in

measuring and understanding of threats and information security risk management as a view point of enterprise and academic computing environment. These consequences provide the enabling ground for effective control and mitigation strategies to be in place. With this concept, it can provide for understanding whether organizational security investments paid off or not through a measure based on belief network inference decision[25]. As an on-going research activity, it is expected that we will extend the inference analysis and decision support system with the campus network assets assessment results through a comprehensive network security framework. The framework will aim at providing an enabling ground for effective control and safeguards of the infrastructural assets on the network.

REFERENCES

[1] O. Oriola, A. B. Adeyemo, and O. Osunade, "Network Threat Characterization in Multiple Intrusion Perspectives using Data Mining Technique," International Journal of Network Security & Its Applications (IJNSA), vol. Vol.4, No.6, 2012.

[2] K. Liyakasa, "Cracking the Code on cyber crimes," www.detinationCRM.com 2012.

[3] N. Fenton and M. Neil, "The use of Bayes and causal modelling in decision making, uncertainty and risk " 2011.

[4] P. Weber, G.Medina-Oliva, C.Simon, and B.Iung, "Overview on Bayesian networks applications for dependability,risk analysis and maintenance areas," Elsevier -Engineering Applications of Artificial Intelligence, 2012.

[5] S. Kondakci, "A Composite Network Security Assessment," The Fourth International Conference on Information Assurance and Security,IEEE, 2008.

[6] R. Bernard, "Information Lifecycle Security Risk Assessment: A tool for closing security gaps," Science Direct- Computers and Security, 2007.

[7] M. Li. and C. Chi., "Decision analysis of statistically detecting distributed denial-of-service flooding attacks," International Journal of Information Technology & Decision Making, vol. Vol. 2, No. 3, 2003.

[8] W. O. Kermack and A.G.Mckendrick, "Contributions of Mathematical Theory to epidemics,," proceeding of the Royal Society of London, vol. vol.141, pp. 94 - 122, 1933.

[9] C. Shin-Ming, A. Weng-Chon, C. Pin-Yu, and C. Kwang-Cheng, "On Modeling Malware Propagation in Generalized Social Networks," Communications Letters, IEEE, vol. 15, pp. 25-27, 2011.

[10] J. Wang, C. Xia, and Q. Liu, "A novel Model for the Internet Worm Propagation," IEEE, 2010.

[11] S. Fei, L. Zhaowen, and M. Yan, "Modeling and Analysis of Internet worm propagation," Scince Direct, vol. 17(4), pp. 63-68, 2010.

[12] Y. Yao, H. Guo, G. Yu, and F.-x. Gao, "Discrete-Time Simulation Method for Worm Propagation Model with Pulse Quarantine Strategy," Procedia Engineering, vol. 15, pp. 4162-4167, // 2011.

[13] C. C. Zou, W. Gong, and C. Towsley, "Worm Propagation Modelling and Analysis under Dynamic Quarantine Defense," ACM, 2003.

[14] M. G. Roberts and J.A.P.Heesterbeek, "Mathematical Models in Epidemology," In mathematical models, in Encyclopedia of ilfe Support System (EOLSS), 2003.

[15] Y. Wang, J. Li, K. Meng, C. Lin, and X. Cheng, "Modeling and security analysis of enterprise network using attack–defense stochastic game Petri nets," Security and Communication Networks, Published online in Wiley Library, 2012.

[16] A. Josang, "Conditional Reasoning with Subjective Logic," Journal of Multiple-Valued Logic and Soft Computing vol. 15(1), pp. pp. 5-38, 2008

[17] R. C. Stalnaker, "A theory of Conditionals," 1970.

[18] G. Yap, A. Tan, and H. Pang, "Explaining Inferences in Bayesian Networks," 2007.

[19] J. Pearl, " Probabilistic reasoning in intelligent systems " Morgan Kaufmann, San Mateo, CA, , 1988.

[20] D. Heckerman, "Bayesian Networks for Data Mining," Data Mining and Knowledge Discovery, 1997.

[21] A. Janjic, Z. Stajic, and I. Radovic, "A Practical Inference Engine for Risk Assessment of Power Systems based on Hybrid Fuzzy Influence Diagrams," Latest Advances in Information Science, Circuits and Systems, 2011.

[22] S. Russell and P. Norvig, Eds., Artificial intelligence: A modern approach. Prentice Hall, 1995.

[23] Decision Systems Laboratory, University of Pittsburgh, and N. B. f. Avenue, "GeNIe," 2007.

[24] A. Mohammed, S. M. Nor, and M. N. Marsono, "Network Worm Propagation Model Based on a Campus Network Topology," in Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, 2011, pp. 653-659.

[25] T. K. Tsiakis and G. D. Pekos, "Analysing and determining Return on Investment for Information Security," International Conference on Applied Economics – ICOAE, 2008.