International Conference on Information and Communication Technology and Its Applications (ICTA 2016)
Federal University of Technology, Minna, Nigeria
November 28 – 30, 2016

Dynamics of SCADA System Malware: Impacts on Smart Grid Electricity Networks and Countermeasures

Adeyinka A. Falaye[1], Oluwafemi Osho[2], Maxwell I. Emehian[3], and Seun Ale[4]
[1]Department of Computer Science, Federal University of Technology, Minna, Nigeria
[2]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria
[3,4]Department of Mathematics, Federal University of Technology, Minna, Nigeria
{[1]falaye.adeyinka, [2]femi.osho}@futminna.edu.ng

***Abstract*—Supervisory Control and Data Acquisition (SCADA) system malware have contributed to the degradation of most critical installations across the globe, especially the power grids. This study seeks to investigate the dynamics of spread of malware targeted at SCADA systems on smart-grid electricity networks. We develop a mathematical model for the propagation of SCADA malware. The infectious-free and endemic equilibrium are obtained, with the former tested and found to be locally asymptotically stable. We investigate using numerical simulations the effects of antivirus, and the combination of vulnerability scanning and security patches. Our results emphasize the importance of the proposed countermeasures at reducing or eliminating the risks posed by the SCADA system malware.**

Keywords – SCADA; Smart Grid; Reproduction Number; Local Stability; Programming logic controller

I. INTRODUCTION

According to the 2016 Digital Cyber Crime Unit of Microsoft Corporation, malware attacks cost global economy an estimated 3 trillion US Dollars annually [1]. This is higher than entire GDP estimate of Africa in 2015 [2], [3], and approximately the external reserve of the People's Republic of China which stood at about 3.17 trillion US Dollars as at September 2016 [4].

In this modern era, there is an increasing spate of dependency on the effectiveness and efficiency of a well-structured electric power system, a major infrastructure in the economic development of a country or society and also a backbone to the proper functioning of other critical infrastructures, which very much need electric power to function at full capacity. These include infrastructures such as telecommunications, internet, water, air traffic control and transportation [5]. Though these infrastructures can operate without main power supply for a short period of time, in the long run, longer and larger outages in power may put them in jeopardy, and as a result, creating a crippling effect on the economy. These power outages can be as a result of technical or/and operational faults. However, over the years, they have also been caused by targeted malware attacks on the Supervisory Control and Data Acquisition (SCADA) systems, which control the flow of data and information on most modern power grids.

Control systems such as SCADA systems are structured to achieve/maintain set goals by reducing the probability of unwanted behavior, to meet demand of the critical infrastructure the system is controlling, and to obtain maximum production profit. SCADA systems are mostly found in critical national infrastructures such as the electric power grid, transportation systems and oil and gas distributions. And it is because of their critical nature that these SCADA systems remain at high risk of attack from an instantaneously growing set of attackers, who are highly skilled and motivated. SCADA systems consist of several components including programming logic controllers (PLCs)/remote terminal units, which communicate with the SCADA servers and perform most of the supervisory and overriding controls, such as controlling continuous flow of signals, and providing enabling conditions for fault detention.

To effectively run a functional power grid, there is a strong dependency on SCADA systems. But keeping the systems secure and immune to malware attacks from external forces, as well as internally generated errors, is very essential in avoiding outages. This is a massive challenge because of the complexity of the SCADA systems and their operation on real-time, as well as their connectivity to the internet, all of which makes the systems perform their various duties.

Malware attacks have over time evolved from the more common internet worm and virus attacks to more precise attacks on target systems. While there have been significant damages by these internet worms and virus attacks, present set of malware are designed to specifically steal information which are considered confidential, take control of systems for malicious purposes, create pathways (backdoors) through which other attacks can be launched or cause complete breakdown of targeted infrastructures. A typical example of such malware is Stuxnet [6].

Malware attacks on SCADA systems vary from mere invasive forms (e.g. to steal confidential information or to analysis the traffic of power supply by the system) to more invasive forms (e.g. to take control of the system or to cause

a disruption in the normal functions of the systems) [7]. Figure 1 depicts a SCADA system malware attack.

In this paper, we investigate the effectiveness of existing control strategies for SCADA system malware, specifically, the use of antivirus signatures, and also propose a new control strategy, which combines vulnerability scanning and implementation of security patches.

The ensuing contents of this paper are organized thus: Section II describes related works. Section III introduces the proposed model, as well as its variables and parameters. In Section IV, the equilibrium points, effective reproduction number and the local stability of the infectious-free equilibrium point are presented. Section V presents the numerical simulations and analysis of obtained results. The study is finally concluded in Section VI.

II. RELATED WORKS

The need to fully grasp the dynamics of the spread of various malwares has over the years necessitated the formulation of various models. The use of epidemiology in many of the models has been inspired by the near similarities which the spread of malware share with biological virus [8]. Mathematically, epidemiology has developed quite rapidly since the mid 20th century [9].

One main procedure used in epidemiology is application of a compartmental model, where the population is divided into various sectors according to their epidemic status. Another important procedure entails the use of a system of differential equations.

Many existing models of malware propagation find their root in some classical classic epidemiology models including [10]–[13], and often consider malware attacks on computer systems. For instance, [9] developed an SIR model to determine the dynamics of malware attacks on computer networks. Misra, Verma and Sharma [14] also focused on computer network. Their model considered two states: infected and susceptible. The effect of anti-malware was equally investigated. Liu, Liu, Liu, Cui, and Huang [15] proposed a new compartmental model. They however investigated the effect of heterogeneous immunization on the spread of the malware. Piqueira, Vasconcelos, Gabriel and Araujo [16], on their part, considered more states. Specifically, using simple systems identification techniques, they developed a model named SAIC (Susceptible, Antidotal, Infectious, Contaminated), based on the SIR model [10]–[12]. In [17], the SIS model was modified to include what was termed a re-introduction parameter, which represents the re-introduction of an existing computer virus or the introduction of a new virus.

Few studies have considered spread of malware on other systems. One of these is the work of [18]. They combined generic epidemiological models with graph theory to model and monitor the evolution of malware that target telephony networks, specifically, the Private Branch eXchanges (PBX).

In modeling attacks on SCADA systems, studies have considered different SCADA systems, and focused on various attacks. While many have modeled other attacks few studies have attempted malware attacks on SCADA networks.

On smart-grid/electric power systems, [19] presented a framework that models a category of cyber-physical switching vulnerabilities. Chopade, Bikdash, and Kateeb [20] proposed a flexible and extensible framework for survivability of smart –grid and SCADA systems. They considered survival under severe emergencies, vulnerabilities and WMD attacks. The work of [21] focused on the development of a novel hierarchical method applied to Petri nets to model coordinated attacks on smart grid, while that of [22] entailed the simulation and evaluation of the impacts of data integrity attacks on automatic generation control.

Regarding other SCADA systems, [23], focusing on stealthy deception attacks, proposed some enhanced hydrodynamic models which were used for detection of physical faults and cyber attacks to automated canal systems; while an aspect-oriented model for evaluating the security of automotive cyber-physical systems was proposed by [24]. They focused on four attacks: man-in-the-middle, fuzz, interruption and replay attacks.

On the other hand, in modeling attacks that affect any type of SCADA system, [25] and [26] proposed models for intrusion detection. While in the former, the models were Modus/TCP-based, in the latter study, behavioral modeling was applied. Another study, by [27], entails a SCADA security framework which includes real-time monitoring, anomaly detection, impact analysis, and mitigation strategies, and the proposal and evaluation of a new algorithm which considers both password policies and port auditing for evaluating cybersecurity.

One of the few studies, however, that considered malware propagation on SCADA networks is [28]. The authors modeled Stuxnet attack using Boolean Logic Driven Markov Processes (BDMP).

III. FORMULATION OF MODEL

A model formulation involves a process whereby the basic assumptions of the model are clearly stated while relating these assumptions from the real world to the mathematical model [12]. The assumptions of the proposed model include:

- The entire population is divided into four (4) states i.e. the Vulnerable Class, the Infectious Class, the Immune Class and the Recovered Class; all based on their epidemiological status.
- Every new PLC added to the network is considered to be vulnerable, while a few of them are considered to be infected.
- The rate at which new PLCs are added to the network and existing ones which die due to non-infectious reason is assumed to be constant.
- The active population includes all the PLCs.
- There is a vertical transmission into the infectious class as a result of connectivity to the internet.
- It is assumed that there is an external factor i.e. a Universal Serial Bus (USB) device that can be introduced into the smart grid network, as mountable devices, to transfer and copy files.
- All model parameters are constant.
- All interactions within the network occur homogeneously.

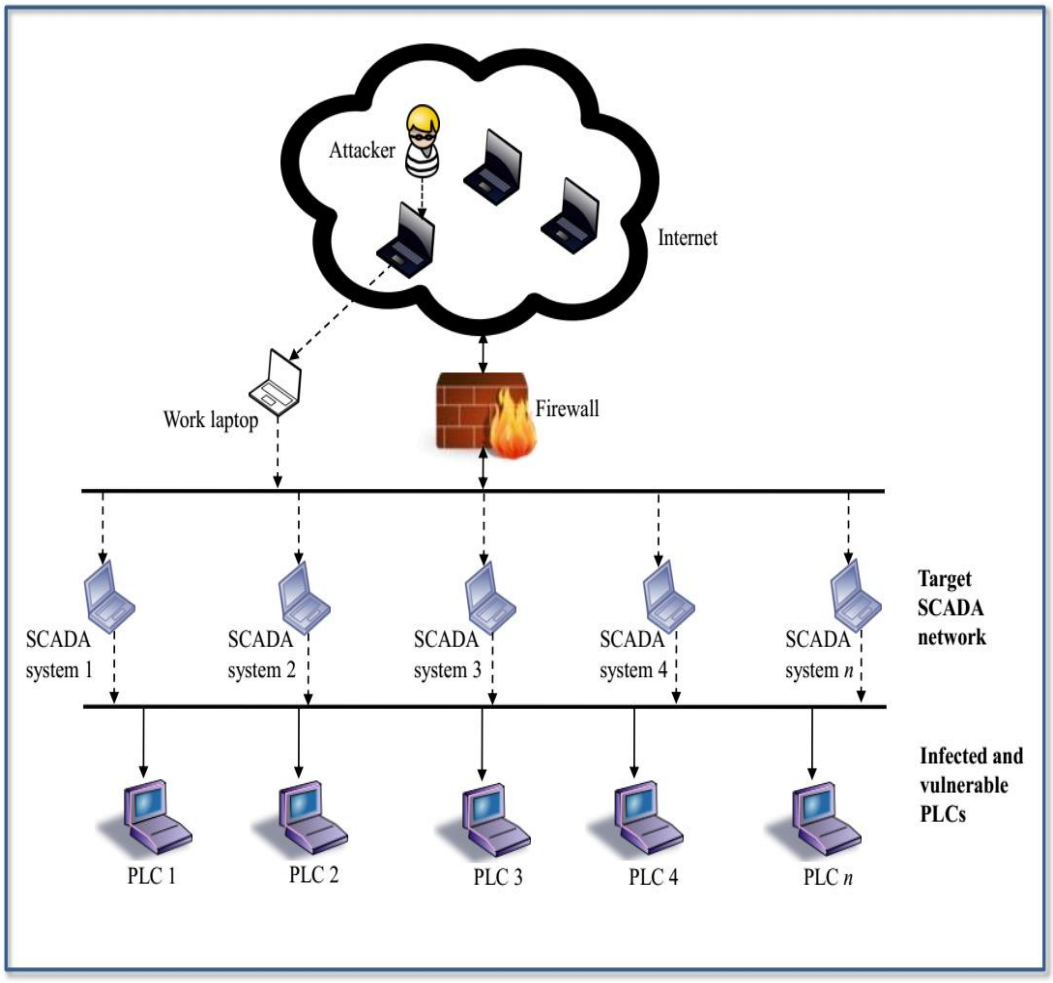

Figure 1. Model of a SCADA system malware attack

Another basic procedure of modelling is the description of the various notations, as well as the parameters used in the formulation of the model.

The various notations are described below:

- V(t), which represents the number of vulnerable SCADA PLCs/software-based remote terminal units (RTUs) within each substations over an electric smart grid network at time, t, after connection has been established.
- I(t), which represents the number of infectious SCADA PLCs/RTUs within each substations over an electric smart-grid network at time, t, after connection has been established.
- IMUN(t), which represents the number of immune SCADA PLCs/RTUs within each substations over an electric smart grid network at time, t, after connection has been established.
- R(t), which represents the number of recovered SCADA PLCs/RTUs within each substations over an electric smart grid network at time, t, after connection has been established.
- USB(t), which represents the number of Universal Serial Bus (USB) devices used by employees on any of the substations within an electric smart grid network at time, t, after connection has been established.
- N(t), which represents the total number of SCADA PLCs/RTUs within each substations over an electric smart grid network at time, t, after connection has been established.

The following are the parameters used in the model:

- α is the constant rate at which new PLCs are, on the average, added to the electric smart grid network.
- p is the probability of recruiting PLCs from α number of PLCs.
- β is the constant rate of interaction of the vulnerable class with the infectious class.
- γ is the natural death rate or death due to non-infectious reason.
- a_1 is the proportion of time of scanning due to implementation of vulnerability scanning of the network.
- a_2 is the rate of the effectiveness of detection of vulnerabilities due to vulnerability scanning of the network.
- a_3 is the rate of removal of vulnerabilities due to implementation of security patches on the network.
- θ is the rate of vertical transmission of infected PLCs into the network.
- μ is the rate of recovery due to application of antivirus.

- δ is the death rate due to SCADA malware attack on the electric smart grid network.
- φ is the rate of natural recruitment of Universal Serial Bus (USB) devices into the network.

A VIMR (Vulnerable Class, Infectious Class, Immune Class and Recovered Class) model, depicted in Figure 2, is proposed to explain the dynamics of spread of malicious codes. The total size of the population is N, where N = V + I + M + R, and varies with time.

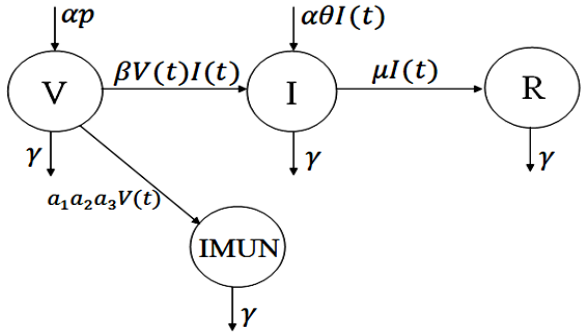

Figure 2. The Flow of Malicious Codes into a Smart Grid Network

Our main aim is to study the dynamics of SCADA system malware and based on our assumptions in the smart grid network, the dynamics of the SCADA system malware consists of the following system of ordinary differential equations:

$$\frac{dV(t)}{dt} = \alpha p - \beta V(t)I(t) - \gamma V(t) - a_1a_2a_3V(t)$$

$$\frac{dI(t)}{dt} = \alpha\theta I(t) - \beta V(t)I(t) - \mu I(t) - \delta I(t) - \gamma I(t)$$

$$\frac{dIMUN(t)}{dt} = a_1a_2a_3V(t) - \gamma IMUN(t)$$

$$\frac{dR(t)}{dt} = \mu I(t) - \gamma R(t) \quad (1)$$

An external factor was also considered but do not constitute part of the population of the entire system, i.e.

$$\frac{dUSB(t)}{dt} = \varphi USB(t) - \mu USB(t)$$

Thus, the total population of SCADA system PLCs is given as

$$\frac{dN(t)}{dt} = \alpha - \gamma N - (\delta - \alpha\theta)I(t)$$

Letting

$$IMUN(t) = M(t);\ USB(t) = U(t);\ and a_1a_2a_3 = a$$

The system in (1) above as well as the external factor becomes

$$\frac{dV(t)}{dt} = \alpha p - \beta V(t)I(t) - \gamma V(t) - aV(t)$$

$$\frac{dI(t)}{dt} = (\beta V(t) + [\alpha\theta - \mu - \delta - \gamma])I(t)$$

$$\frac{dM(t)}{dt} = aV(t) - \gamma M(t)$$

$$\frac{dR(t)}{dt} = \mu I(t) - \gamma R(t) \quad (2)$$

And

$$\frac{dU(t)}{dt} = (\varphi - \mu)U(t)$$

IV. INFECTIOUS-FREE AND ENDEMIC EQUILIBRIUM POINTS AND EFFECTIVE REPRODUCTION NUMBER

Points whereby the SCADA systems and electric smart grid configuration do not change with time or when no force is acting on the system, are known as the equilibrium points. We obtained the equilibrium points and also tested for stability of the equilibrium points.

A. Equilibrium Points

For equilibrium points, we have that

$$\frac{dV(t)}{dt} = \frac{dI(t)}{dt} = \frac{dM(t)}{dt} = \frac{dR(t)}{dt} = 0$$

We obtain Infectious-Free Equilibrium

$$E^0 = \left(\frac{\alpha p}{(\gamma + a)}, 0, \frac{a\alpha p}{\gamma(\gamma + a)}, 0\right)$$

And the Endemic Equilibrium

$$E^* = \left(\frac{\mu + \delta + \gamma - \alpha\theta}{\beta}, \frac{(a + \gamma)(\alpha\theta - \mu - \delta - \gamma) - \beta\alpha p}{(\alpha\theta - \mu - \delta - \gamma)\beta}, \frac{a[\mu + \delta + \gamma - \alpha\theta]}{\beta\gamma}, \mu\left[\frac{(a + \gamma)(\alpha\theta - \mu - \delta - \gamma) - \beta\alpha p}{\gamma(\alpha\theta - \mu - \delta - \gamma)\beta}\right]\right)$$

B. *Effective Reproduction Number and Local Stability*

A major procedure in modeling the dynamics of malware is the effective reproduction number denoted by $R_0$and it also helps in predicting part of the population which will not be infected.

System (2) has an infectious-free equilibrium whereby the infective part of the population is zero while the vulnerable and immune remain positive denoted by

$$E^0 = (V, I = 0, M, R = 0)$$

Thus, analyzing the local stability of the infectious-free equilibrium give the endemic point whereby there will be a rise or reduction to zero when a small number of infectious PLCs are brought into a highly vulnerable population.

Eliminating R, system (2) reduces to

$$\frac{dV(t)}{dt} = \alpha p - \beta V(t)I(t) - \gamma V(t) - aV(t)$$

$$\frac{dI(t)}{dt} = (\beta V(t) + [\alpha\theta - \mu - \delta - \gamma])I(t) \quad (3)$$

We obtain the effective reproduction number R_0 by investigating the local stability of the infectious-free equilibrium.

Theorem 1: The infectious-free equilibrium is locally asymptotically stable whenever $R_0 < 1$

We obtain the Jacobian of system (3) at infectious-free equilibrium

$$J = \begin{bmatrix} -(\gamma + a) & -\beta V(t) \\ 0 & \beta V(t) + [\alpha\theta - \mu - \delta - \gamma] \end{bmatrix}$$

Reducing the matrix to an upper triangular matrix, we have a characteristic equation as

$$J^0 = \begin{bmatrix} -\gamma - a & \frac{-\beta\alpha p}{\gamma + a} \\ 0 & \frac{-(-\beta\alpha p - \alpha\gamma\theta - a\alpha\theta + \gamma\mu + a\gamma + \delta\gamma + a\delta + \gamma^2 + a\gamma)}{\gamma + a} \end{bmatrix}$$

We assume our effective reproduction number to be the leading Eigen value, thus we assume

$$R_0 = \frac{-(-\beta\alpha p - \alpha\gamma\theta - a\alpha\theta + \gamma\mu + a\gamma + \delta\gamma + a\delta + \gamma^2 + a\gamma)}{\gamma + a}$$

Since $R_0 < 1$, thus we have a local stability, which implies that the malware can be curtailed through appropriate corresponding countermeasure parameters.

V. NUMERICAL SIMULATIONS AND ANALYSIS

We set out in Table I, variables and hypothetical values of our model.

Similarly, population-dependent parameter values usually have to be inputted based on computer malware epidemiology and population data. We set out in Table II parameters and corresponding values.

TABLE I. HYPOTHETICAL MODEL VARIABLES AND POPULATION-DEPENDENT

S/N	Variables	Hypothetical values	Source
1	V	20	Assumed
2	I	5	Assumed
3	M	10	Assumed
4	R	0	Assumed
5	B	7	Assumed

TABLE II. HYPOTHETICAL MODEL POPULATION PARAMETERS

S/N	Parameter	Hypothetical Values	Source
1	a	Varies	Assumed
2	α	2	Assumed
3	δ	0.1	Assumed
4	β	0.1	Assumed
5	μ	Varies	Assumed
6	ψ	Varies	Assumed
7	θ	0.2	Assumed
8	γ	0.1	Assumed

Figure 3 shows the different rates of recovery due to application of anti-virus signatures with time i.e.($\mu = 0.1, 0.5, 0.9$), we discovered that if the anti-virus is used at the rate of 10% (i.e. on 1 out of 10 systems), the infectious class of PLCs continue to increase instantaneously from the initial population of 5,000 to above 15,000 in the first two days of interaction with the vulnerable class. The instant increase then tends to stabilize a bit, mostly due to the little effect of the disinfected PLCs. It then rises instantaneously, and after the next 5 days, rises to above 25,000, at 50% (i.e. on 2 out of 10 systems) it increases to about 10,000 in the next one and half days due to interaction with the vulnerable class of PLCs, before it starts decreasing gradually in the next two to five days to little below 5,000, mostly due to the positive effect of the anti-virus signatures; though this happens with a possibility of re-infection. But at 90% (i.e. on 9 out of every 10), the infectious population of PLCs increase minimally to about 7,000 in the first day due to the interaction with the vulnerable class before it gradually decreases mainly due to the very high effect of the antivirus signatures and the infectious population of PLCs will continually decline till it goes into extinction after 5days.

Figure 4 shows the variation in the rate of natural recruitment of the USB devices into the network. At 10% usage of USB devices for transfer and copying of files, there is an instant increase in the population of infectious PLCs from the initial 5,000 to above 10,000 after just one and half days due to interaction between the vulnerable class and the USB devices plugged into the system, which of course, some

are infected. But population of the infectious PLCs then stabilizes mostly due to the implementation of anti-virus signatures which at this point gradually detects infected USB devices. After the second day, the population of the infectious PLCs begins a rapid decline due to the disinfection of the infected USB devices by the anti-virus signatures until it the infected power line carries goes into extinction totally after five days.

Figure 5 shows the variation in the rate of vulnerability scanning, detection of vulnerability and implementation of security patches. At 10% vulnerability scanning, detention of vulnerability and implementation of security patches, the infectious population of PLCs increases from the initial 5,000 to above 14,000 in the one and half days due to the interaction with the vulnerable class, then it stabilizes a bit and decreases gradually to about 7,000 due to the implementation of the security patches. At 50% vulnerability scanning, detention of vulnerability and implementation of security patches, the population of the infectious PLCs increases to about 11,000 in one and half days due to the interaction with the vulnerable class but stabilizes and then decreases gradually to about 5,000 (the initial population) mainly due to the detection and implementation of the security patches. But at 90% vulnerability scanning, detention of vulnerability and implementation of security patches, the population of the infectious PLCs increase from the initial 5,000 to almost 10,000 in the first day mainly due to the interaction with the vulnerable class, then stabilizes a bit and gradually declines until it goes into extinction in the next 5 days, mainly due to the effect of the vulnerability scanning, detention of vulnerability and implementation of security patches.

From Figures 3, 4 & 5, it was discovered that there is always an instantaneous increase in the infectious class of the PLCs due to their interaction with the vulnerable class of the PLCs; and the consequences of this initial increase include power outages, damages to equipments, as well as financial losses. These are mainly due to the fact that these infectious PLCs can be used by interest groups or syndicates to carry out their agenda before such infections are detected and mitigated.

VI. CONCLUSION

We developed a model for the dynamics of SCADA system malware on smart-grid electricity networks for a population consisting of the Vulnerable, Infected, Immune and Recovered classes of PLCs or Remote Terminal Units. We also incorporated an external factor, the Universal Serial Bus (USB), and considered three control parameters: vulnerability scanning, detection from vulnerability scanning and the implementation of security patches.

Our findings highlight the necessity of control strategies, viz. antivirus, vulnerability scanning, and application of security patches, at mitigating malware spread on SCADA systems.

Future studies could consider other parameters including human behavior. Many studies have confirmed that many security breaches are the result of non-technical factors. In this study, the propagation was considered as a function of time. Propagation as a function of geographical spread and cost should be explored.

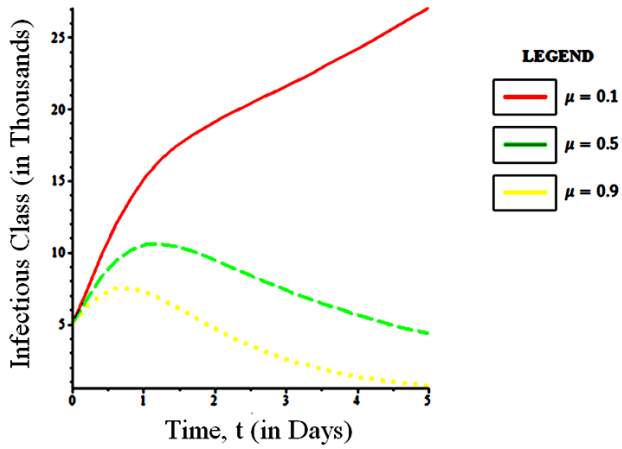

Figure 3. The Different Rate of Recovery due to Application of the Anti-Virus Signatures with Time

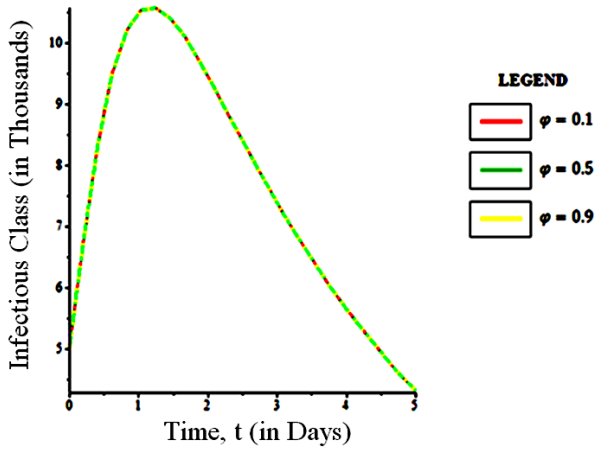

Figure 4. The Variation in the Rate of Natural Recruitment of USB Devices into the System

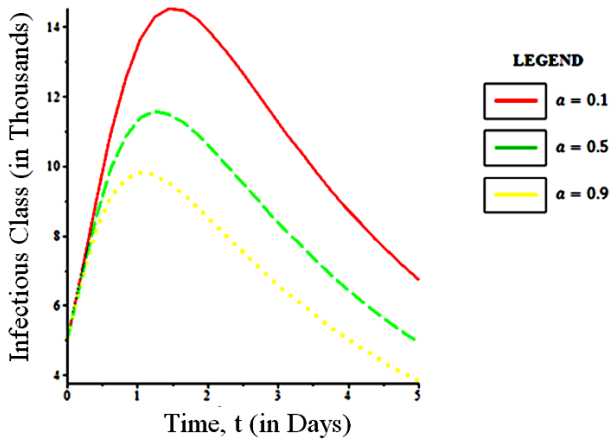

Figure 5. The Variation in the Rate of Removal of Vulnerability due to Vulnerability Scanning and Implementation of Security Patches

REFERENCES

[1] Microsoft, "Digital Crimes Unit Fact Sheet."

[2] Knoema, "IMF World Economic Outlook (WEO), October 2015." [Online]. Available: https://knoema.com/IMFWEO2015Oct/imf-world-economic-outlook-weo-october-2015. [Accessed: 22-Oct-2016].

[3] Knoema, "World GDP Ranking 2016 | Data and Charts | Forecast." [Online]. Available: https://knoema.com/nwnfkne/world-gdp-ranking-2016-data-and-charts-forecast. [Accessed: 22-Oct-2016].

[4] Trading Economics, "China Foreign Exchange Reserves 1980-2016." [Online]. Available: http://www.tradingeconomics.com/china/foreign-exchange-reserves. [Accessed: 21-Oct-2016].

[5] B. Les Cardwell and A. Shebanow, "The Efficacy and Challenges of SCADA and Smart Grid Integration," *J. Cyber Secur. Inf. Syst.*, vol. 1, no. 3, pp. 2–10, 2013.

[6] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," *IFAC Proc. Vol.*, vol. 18, no. PART 1, pp. 11271–11277, 2011.

[7] O. Gervasi, "Encryption Scheme for Secured Communication of Web Based Control Systems," pp. 609–618, 2010.

[8] M. H. R. Khouzani and S. Sarkar, "Dynamic malware attack in energy-constrained mobile wireless networks," in *2010 Information Theory and Applications Workshop, ITA 2010 - Conference Proceedings*, 2010, pp. 408–418.

[9] B. K. Mishra and A. Prajapati, "Dynamic Model on the Transmission of Malicious Codes in Network," *Int. J. Comput. Netw. Inf. Secur.*, vol. 10, pp. 17–23, 2013.

[10] W. O. Kermack and A. G. McKendrick, "A Contribution to the Mathematical Theory of Epidemics," *Proc. R. Soc. London. Ser. A, Contain. Pap. a Math. Phys. Character*, vol. 115, no. 772, pp. 700–721, 1927.

[11] W. O. Kermack and A. G. McKendrick, "Contributions to the mathematical theory of epidemics-III. Further studies of the problem of endemicity," *Proc. R. Soc. London. Ser. A, Contain. Pap. a Math. Phys. Character*, vol. 141, no. 843, pp. 94–122, 1933.

[12] W. O. Kermack and A. G. McKendrick, "Contribution to the Mathematical Theory of Edipemics. II. The Problem of Endemicity," *Proc. R. Soc. London. Ser. A, Contain. Pap. a Math. Phys. Character*, vol. 138, no. 834, pp. 55–83, 1932.

[13] N. T. J. Bailey, *The Mathematical Theory of Infectious Diseases*, 2nd ed. New York: Hafner Press, 1975.

[14] A. K. Misra, M. Verma, and A. Sharma, "Capturing the interplay between malware and anti-malware in a computer network," *Appl. Math. Comput.*, vol. 229, pp. 340–349, 2014.

[15] W. Liu, C. Liu, X. Liu, S. Cui, and X. Huang, "Modeling the spread of malware with the influence of heterogeneous immunization," *Appl. Math. Model.*, vol. 40, pp. 3141–3152, 2016.

[16] J. R. C. Piqueira, A. A. De Vasconcelos, C. E. C. J. Gabriel, and V. O. Araujo, "Dynamic models for computer viruses," *Comput. Secur.*, vol. 27, pp. 355–359, 2008.

[17] J. C. Wierman and D. J. Marchette, "Modeling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction," *Comput. Stat. Data Anal.*, vol. 45, pp. 3–23, 2004.

[18] I. Androulidakis, S. Huerta, V. Vlachos, and I. Santos, "Epidemic Model for Malware Targeting Telephony Networks," in *IEEE 23rd International Conference on Telecommunications*, 2016, pp. 1–5.

[19] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Top. Comput.*, vol. 1, no. 2, pp. 273–285, 2013.

[20] P. Chopade, M. Bikdash, and I. Kateeb, "Interdependency Modeling for Survivability of Smart Grid and SCADA network under severe emergencies, vulnerability and WMD attacks," *Southeastcon, 2013 Proc. IEEE*, no. April, pp. 1–7, 2013.

[21] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741–749, 2011.

[22] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system," *IEEE PES Gen. Meet. PES 2010*, pp. 1–6, 2010.

[23] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Cyber security of water scada systems-part II: Attack detection using enhanced hydrodynamic models," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1679–1693, 2013.

[24] A. Wasicek, P. Derler, and E. a. Lee, "Aspect-oriented Modeling of Attacks in Automotive Cyber-Physical Systems," in *2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2014, pp. 1–6.

[25] N. Goldenberg and A. Wool, "Accurate modeling of Modbus / TCP for intrusion detection in SCADA systems," *Int. J. Crit. Infrastruct. Prot.*, vol. 6, no. 2, pp. 63–75, 2013.

[26] A. Dolgikh, T. Nykodym, V. Skormin, and Z. Birnbaum, "Using behavioral modeling and customized normalcy profiles as protection against targeted cyber-attacks," in *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, 2012, pp. 191–202.

[27] C. W. Ten, G. Manimaran, and C. C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst. Man, Cybern. Part ASystems Humans*, vol. 40, no. 4, pp. 853–865, 2010.

[28] S. Kriaa, M. Bouissou, and L. Piètre-Cambacédès, "Modeling the Stuxnet attack with BDMP: Towards more formal risk assessments," in *7th International Conference on Risks and Security of Internet and Systems, CRiSIS 2012*, 2012, pp. 1–8.