Quantitative Model for Dynamic Propagation and Countermeasure of Malicious Cyber Attack on the Mobile Wireless Network

Adeyinka A. Falaye
Department of Computer Science, Federal University of Technology FUTMINNA
Minna, Nigeria
falaye.adeyinka@futmina.edu.ng

Etuk Stella Oluyemi
Department of Information and media Technology, Federal University of Technology FUTMINNA
Minna, Nigeria
abiolastella@futminna.edu.ng

Seun Ale
Department of Mathematics, Federal University of Technology FUTMINNA
Minna, Nigeria
profgurujoe@gmail.com

Muhammad Bashir Abdullahi
Department of Computer Science, Federal University of Technology FUTMINNA
Minna, Nigeria
el.bashir02@futminna.edu.ng

Ugwuoke Cosmas Uchenna
Department of Computer Science, Federal University of Technology FUTMINNA
Minna, Nigeria
ask4cosmas@yahoo.co.uk

Femi Awogbemi
E-exam enter, Federal University of Technology FUTMINNA
Minna, Nigeria
awogbemifemi@gmail.com

***Abstract*—One major concern of network and data security consultants globally is the capabilities of infectious malicious cyber-attacks (Malware) to invade the entire population of the network terminals within few days of an outbreak of an attack to wreak havoc ranging from identity theft, financial fraud to systemic digital assault on critical national assets. It is known that when the vulnerable mobile device communicates with the infected nodes, it becomes infected. This work studies the behavioral dynamics of the Vulnerable, infected and the recovered terminals on the mobile wireless network and the effectiveness of an antivirus security signature as countermeasure and the effect of lack of anti-virus update. Solving for stability, we found out that its Eigen values gives a negative value which means that the equilibrium point is in a stable state. We analyzed the differential equations using Homotopy Perturbation Method (HPM). The simulation to evaluate the consequence of different countermeasure options were carried on a mathematical-tool platform called maple. From our results we discovered that if security patches are fixed on our mobile devices and there is regular antivirus update on the devices, then financial fraud, privacy inversion and running of scam can be curtailed to a significant level.**

Keyword—Homotopy perturbation method; SIR model; malicious ware; stability; equillibrium introduction

I. INTRODUCTION

Network security threat is an apprehensive issue in cyber space owing to the rising cases of cybercrime, hacking and Nation state terrorism. How to manage and protect mobile devices within this space from horrendous activities of both virus and malicious software that has continue to undermine private and public security is not just a concern but an initiative of global imperative. Malware has been recognized to spread and propagates on network information topological via scanning [1]. Due to the disparaging nature of this propagation fueled by vulnerabilities within networked devices, the incidences of privacy inversion, identity theft, internet fraud, disruption and intrusion of mobile device, intellectual piracy and more recently dangerous radicalization and terrorism are no longer issue of if but when.

Reports from an internet security firm named M86 Security shows that a total of €675,000 has been stolen from a bank in Britain these is as a result of malware attacks. Reports from a Spanish newspaper named El Paisa stated that malware and mobile device viruses are responsible for the death of 154 people who were killed in the Spain air crash in Madrid some years ago [2]. Over the years, there has been explosive increase in malware attacks. Statistics has shown that the increase is about 600 percent yearly. Most system if not all have been a victim of at least one or more malware attack [3].

Looking at the recent numbers coming out from Digital Cyber Crime research Unit of Microsoft Corporation, malware attacks cost global economy an estimated 3 trillion US Dollars annually. This is more than the combined GDP estimate of Africa in 2015 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], [5], [6] & [7].

Every second, according to research report 12 devices get compromised with over 1 million daily worldwide [5]. This rate is above epidemiological threshold level and so requires investigation.

Sponsored by Tertiary Educational Trust Fund & supported by Federal University of Technology, Minna, Nigeria.

978-1-5090-6435-9/17/$31.00 ©2017 IEEE

It is against these backdrops that the need to continue to understand quantitatively the dynamics of its spread, the effectiveness of the existing control policy options and the pattern of feature outbreak remains an object of research and development.

This study is organized into nine sections. The first section covers introduction to the study including matters of public interest and concern. Two deals with accounts of development and issues on the subject matter by experts. Three look at model formulation and four define the model variables and parameters. While, the existence of equilibrium, Homotopy perturbation method of solution, results and discussion, conclusion and recommendation are captured in in Sections 5, 6, 7, and 8, respectively.

II. Related Works

The research and development need to fully understand the dynamics of the propagation of various malwares which has over the years lead to the formulation of varieties of models incorporating change and risk with which to compare and rank the outcome of alternative policy actions or strategy. The application of epidemiology in many of the models has been inspired by near mathematical structures which the spread of malware share with biological virus [8]. Mathematically, epidemiology has evolved so 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 subclasses in accordance to their epidemic status in addition to 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 concept SIS model was reconfigured to track the possibility of re-introduction of an existing computer virus or the introduction of a new virus. Few studies have considered spread of malware on other systems including the work of [18]. The investigation on whether or not a large-scale Bluetooth worm outbreak is viable in practice was conducted by a group of authors who used trace-driven simulations to examine the propagation dynamics of Bluetooth worms. They found that Bluetooth worms can infect a large population relatively quickly, in just a few days [19].

A combination of generic epidemiological models with substantial graph theory provide a close approximate and monitoring of the propagation of malware that target telephony networks, specifically, the Private Branch eXchanges (PBX) [18].

Formulating a model entails a procedural issue requiring the key assumptions upon which the model is predicated are clearly stated while relating these assumptions from the real life phenomena to the mathematical model [12]. Such model should enable the experimentation of changes and risks to provide basis for comparison and decision making going forward.

III. Model Variables and Parameters

- β = rate at which vulnerable mobile devices are recruited on the network
- μ = rate at which systems terminates from the network (not due to infection) but due to battery extortion
- γ = Recovery rate of infected systems due to the use of antivirus or windows defender as counter measures in preventing the device from an attack
- α = contact rate of vulnerable and infected mobile devices
- δ = rate at which the device terminates due to malware infection
- ω = rate at which the anti-virus loses its effectiveness due to new variant of a particular malware
- S = vulnerable mobile devices on network
- I = infected mobile devices on network
- R = recovered mobile devices on network
- t = time taken for every mobile 6devices on network to be vulnerable, infected and recovered
- N = total population size of the vulnerable, infected and recovered devices

IV. Model Formulation

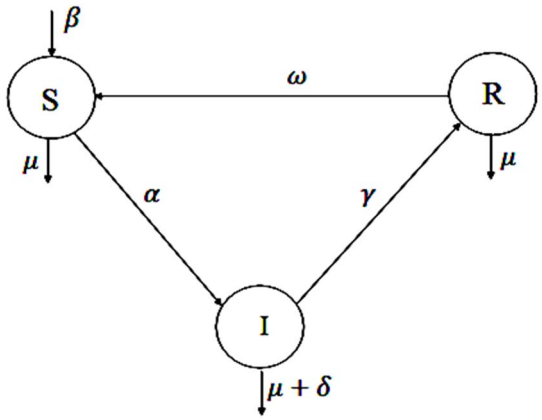

Fig. 1. Schematic diagram of the model.

The model is made up of three compartments, namely: Vulnerable nodes (S); infected nodes (I); Recovered nodes

978-1-5090-6435-9/17/$31.00 ©2017 IEEE

(R) (see Fig. 1). The network gets expanded at a constant rate β and we assume that all the recruited nodes are Vulnerable. The communication or interaction between the Vulnerable and the Infected mobile devices due to sharing of data such as (Hotspot, Mails, etc.) is at a constant rate α, γ is the rate at which the anti-virus is being installed on the infected devices, also the anti-virus lose effectiveness at the rate ω overtime due to lack of update. μ is the rate at which the vulnerable mobile devices terminate either due to battery extortion or increase in media access rate and δ is the rate of failure of mobile devices due to digital systemic attack.

Translating our assumptions into mathematical relationship, we have the following set of equations:

$$\frac{dS}{dt} = \beta S - \mu S - \alpha SI + \omega R \tag{1}$$

$$\frac{dI}{dt} = \alpha SI - (\gamma + \mu + \delta)I \tag{2}$$

$$\frac{dR}{dt} = \gamma I - (\mu + \omega)R \tag{3}$$

$$N=S+I+R \tag{4}$$

V. Existence of Equilibrium

Given any arbitrary equilibrium, the rate of change of change of each variable is constant at zero, i.e.

$$\frac{dS}{dt} = \frac{dI}{dt} = \frac{dR}{dt} = 0 \tag{5}$$

We let,

$$(S, I, R) = (S^*, I^*, R^*) \tag{6}$$

At any arbitrary equilibrium, so that 2.1 to 2.4 becomes,

$$\beta S^* - \mu S^* - \alpha S^* I^* + \omega R^* = 0 \tag{7}$$

$$\alpha S^* I^* - (\gamma + \mu + \delta)I^* = 0 \tag{8}$$

$$\gamma I^* - (\mu + \omega)R^* = 0 \tag{9}$$

From 2.8,

$$(\alpha S^* - (\gamma + \mu + \delta))I^* = 0 \tag{10}$$

This implies that,

$$I^* = 0 \tag{11}$$

Or

$$(\alpha S^* - (\gamma + \mu + \delta)) = 0 \tag{12}$$

A. Disease Free Equilibrium

Lemma1: We have a disease free equilibrium (DFE) at the points,

$$E^0 = (S^0, I^0, R^0) = (0, 0, 0) \tag{13}$$

Proof:

From (11),

$$I^0 = 0 \tag{14}$$

Substituting into (9),

$$R^0 = 0 \tag{15}$$

Furthermore, putting (14) and (15) into (7),

$$S^0 = 0 \tag{16}$$

As required.

B. Endemic Equilibrium

Lemma 2: We have an endemic equilibrium at points $E^1 = (S^1, I^1, R^1) = (\frac{\gamma + \mu + \delta}{\alpha}, \frac{\beta - \mu}{\alpha}, \gamma(\frac{\beta - \mu}{\alpha(\mu + \omega)})$

From (10),

$$S^1 = \frac{(\gamma + \delta + \mu)}{\alpha} \tag{17}$$

Substituting (17) into (7),

$$I^1 = \frac{\beta - \mu}{\alpha} \tag{18}$$

Further substitution of (17) and (18) into (9) gives,

$$R^1 = \gamma(\frac{\beta - \mu}{\alpha(\mu + \omega)}) \tag{19}$$

Q.E.D.

C. Stability Analysis

Malwares can be controlled effectively on mobile devices, under certain condition in finite time, if the DFE is stable under the same condition. We can evaluate the stability of the disease free equilibrium based on the signs of the Eigen values of the Jacobean matrix. If all the real parts of the characteristic values are negative then the equilibrium is locally stable.

Theorem 1

The disease free equilibrium is (LAS)

Proof:

Using the Jacobean stability matrix, we have,

978-1-5090-6435-9/17/$31.00 ©2017 IEEE

$$J=\begin{bmatrix} \frac{df_1}{dS} & \frac{df_1}{dI} & \frac{df_1}{dR} \\ \frac{df_2}{dS} & \frac{df_2}{dI} & \frac{df_2}{dR} \\ \frac{df_3}{dS} & \frac{df_3}{dI} & \frac{df_3}{dR} \end{bmatrix} \quad (20)$$

So that,

$$J^0=\begin{bmatrix} (\beta-\mu) & 0 & \omega \\ 0 & -(\gamma+\delta+\mu) & 0 \\ 0 & \gamma & -(\mu+\omega) \end{bmatrix} \quad (21)$$

Reducing to upper triangular matrix gives,

$$J^0=\begin{bmatrix} \beta-\mu & 0 & \omega \\ 0 & -\gamma-\mu-\delta & 0 \\ 0 & 0 & -\mu-\omega \end{bmatrix} \quad (22)$$

The Eigen values is evaluated using,

$$\left|J^0-\lambda I\right|=0 \quad (23)$$

Suppose,

$$k_1=-(\gamma+\mu+\delta) \quad (24)$$

$$k_2=-(\mu+\omega) \quad (25)$$

So that (22) becomes,

$$\begin{bmatrix} (\beta-\mu) & 0 & 0 \\ 0 & k_1 & 0 \\ 0 & 0 & k_2 \end{bmatrix}-\begin{bmatrix} \lambda_3 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_1 \end{bmatrix}=0 \quad (26)$$

Equating (26) to zero, we have,

$$\lambda_2-k_1=0, \quad (27)$$

$$\lambda_1-k_2=0 \quad (28)$$

And,

$$\lambda_3-(\beta-\mu)=0, \quad (29)$$

Hence,

$$\lambda_3<1 \quad (30)$$

If and only if

$$R_c<1 \quad (31)$$

Hence, we have proved the theorem.

Thus, the system is locally asymptotically stable.

VI. Homotopy Perturbation Method of Solution

The Homotopy perturbation method (HPM) was proposed by [20]. In this method, the solution is considered as the summation of an infinite series, which usually converges rapidly to the exact solution. This method is employed to solve the Susceptible, Infected, Recovered (SIR) model proposed by Kermack and McKendrick in (1927). The HPM method is based on the use of a power series, which transforms the original non-linear differential equation into a series of linear differential equations. Two continuous functions from one topological space to another are called homotopic, if one can be "continuously deformed" into the other, such a deformation is called a homotopy between the two functions. The Homotopy Perturbation Method (HPM), which provides analytical approximate solution, is applied to various linear and non-linear equations [12].

We applied Homotopy Perturbation Method (HPM) to our equation, as follows:

Applying HPM we have

Let,

$$S=(x_0+px_1+p^2x_2+\ldots) \quad (32)$$

$$I=(y_0+py_1+p^2y_2+\ldots) \quad (33)$$

$$R=(z_0+pz_1+p^2z_2+\ldots) \quad (34)$$

$$(1-p)\frac{dS}{dt}+p(\frac{dS}{dt}+\alpha SI+\mu S-\omega R-\beta)=0$$

$$\begin{aligned} &[(\dot{x_0}+p\dot{x_0}+p^2\dot{x_2}-p\dot{x_0}-p^2\dot{x_1}-p^3\dot{x_2}) \\ &(p\dot{x_0}+p^2\dot{x_1}+p^3\dot{x_2}+\alpha p^2x_0y_1+\alpha p^3x_0y_2+ \\ &\alpha p^2x_1y_0+\alpha p^3x_1y_1+\alpha p^4x_1y_2+\alpha p^3x_2y_0+ \\ &\alpha p^4x_2y_1+\alpha p^5x_2y_2+\mu px_0+\mu p^2x_1+ \\ &\mu p^3x_2-\omega pz_0-\omega p^2z_1-\omega p^3z_2)-\beta p]=0 \end{aligned} \quad (35)$$

$$p^0:\dot{x}_{1=0} \quad (36)$$

$$p^1:\dot{x}_1+\alpha x_0y_0+\mu x_0-\omega z_0-\beta=0 \quad (37)$$

$$p^2:\dot{x}_0+\alpha(x_0y_1+x_1y_0)+\mu x_1-\omega z_1=0 \quad (38)$$

$$(1-p)\frac{dI}{dt}+p[\frac{dI}{dt}+\alpha SI+(\gamma+\mu+\delta)I]=0$$

978-1-5090-6435-9/17/$31.00 ©2017 IEEE

$$(y_0 + p\,y_1 + p^2\,y_2 + \ldots) + p\{y_0 + p\,y_1 + p^2\,y_2 + \ldots + \alpha(x_0 + px_1 + p^2x_2 + \ldots)(y_0 + py_1 + p^2y_2 + \ldots) + (\gamma + \mu + \delta)(y_0 + py_1 + p^2y_2 + \ldots) = 0 \quad (39)$$

$$p^0 : y_{0=0} \quad (40)$$

$$p^1 : y_1 + \alpha x_0 y_0 + (\gamma + \mu + \delta)y_0 = 0 \quad (41)$$

$$p^2 : y_2 + \alpha(x_0 y_1 + x_1 y_0) + (\gamma + \mu + \delta)y_1 = 0 \quad (42)$$

$$(z_0 + p\,z_1 + p^2\,z_2 - pz_0 - p^2\,z_1 - p^3\,z_2) + p[z_0 + p\,z_1 + p^2\,z_2 + (\omega + \mu)(z_0 + pz_1 + p^2z_2 + \ldots) - \gamma(y_0 + py_1 + p^2y_2 + \ldots)] = 0 \quad (43)$$

$$p^0 : z_{0=0} \quad (44)$$

$$p^1 : z_1 + (\mu + \omega)z_0 + \gamma y_0 = 0 \quad (45)$$

$$p^2 : z_2 + (\mu + \omega)z_{1-}\gamma y_1 = 0 \quad (46)$$

$$x(t) = \lim_{p \to 1} x_0(t) + px_1(t) + p^2x_2(t) + \ldots$$

$$S(t) = s_0 + (\beta - \alpha s_0 i_0 - \mu s_0 + \omega r_0)t - \alpha s_0 i_0[\alpha s_0 - (\gamma + \mu + \delta) + (\beta - \alpha s_0 i_0 - \mu s_0 + \omega r_0)(\alpha i_0 + \mu - \omega)]\frac{t^2}{2} \quad (47)$$

$$y(t) = \lim_{p \to 1} y_0(t) + py_1(t) + p^2y_2(t) + \ldots \quad (48)$$

$$I(t) = i_0 + (\alpha s_0 - [(\gamma + \mu + \delta)i_0 t + i_0(\alpha s_0 - (\gamma + \mu + \delta))^2 + \alpha i_0(\beta - \alpha s_0 i_0 - \mu s_0 + \omega r_0)]\frac{t^2}{2} \quad (49)$$

$$z(t) = \lim_{p \to 1} z_0(t) + pz_1(t) + p^2z_2(t) + \ldots \quad (50)$$

$$R(t) = r_0 + [(\gamma i_0 - \mu r_0)t + \gamma i_0(\alpha s_0 - (\gamma + \mu + \delta) - \mu(\gamma i_0 - (\omega + \mu)r_0]\frac{t^2}{2} \quad (51)$$

VII. RESULTS

A. Variable Values Estimation

The variable values of this work have been gotten based on the raw data from previous attacks of malware and we carry out our simulation with mathematical tool (maple software). We fixed in the Table 1 some of the referenced and hypothetical values.

TABLE I. SHOWING THE BASELINE VALUES FOR VARIABLES OF MALWARE ON MOBILE DEVICE MODEL.

S/No	Variables	Values	Source
1	S	293	Bimal (2013)
2	I	25	Assumed
3	R	10	Assumed

B. Parameter Values Estimation

Also based on the previous records of malware attacks on mobile devices, we fixed in the Table 2 the referenced and the hypothetical values. The rate at which the anti-virus is applied as the countermeasures, are also shown in our graphs.

TABLE II. SHOWING THE BASELINE VALUES FOR PARAMETERS OF THE MALWARE ON MOBILE DEVICE MODEL

S/No.	Parameters	Values	Source
1	α	0.10	Assumed
2	β	0.10	Bimal (2013)
3	μ	0.01	Bimal (2013)
4	γ	Varies	Assumed
5	δ	0.09	Bimal (2013)
6	ω	Varies	Assumed

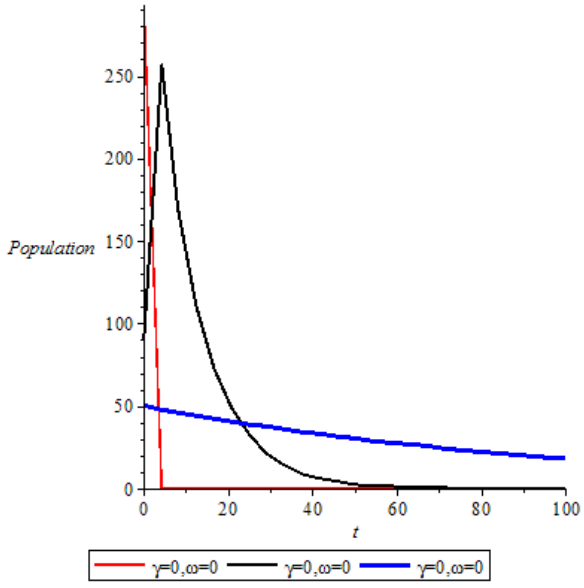

Fig. 2. Graph of Network population Against time ($\gamma = 0, \omega = 0$).

Fig. 2 is the graph that displays the pictorial representation of the behaviors of the table above where the blue line in the graph symbolizes the behavior of the population of the recovered nodes which declined due to the lack of the use of

978-1-5090-6435-9/17/$31.00 ©2017 IEEE

anti-virus on our mobile devices. The black line symbolizes that infected nodes increases instantaneously due to lack of anti-virus on the mobile devices and later drops exponentially due to battery extortion or crashed mobile device and the red colored line symbolizes the population of mobile devices that are vulnerable to attacks by malwares this population drops exponentially in less than 10 days due to battery extortion or crashed mobile devices becomes asymptotically stable.

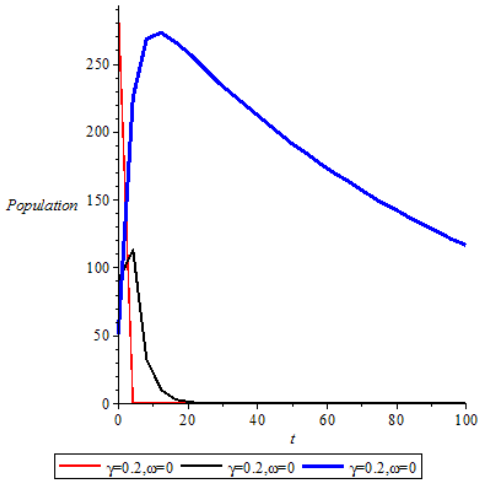

Fig. 3. Graph of Network population Against time ($\gamma = 0.2, \omega = 0$).

Fig. 3 is the graph that displays the pictorial representation of the behaviors of the Table 1 where the blue line in the graph symbolizes the behavior of the population of the recovered nodes which increases due to the use of anti-virus at 20% on our mobile devices, but the population later dropped uniformly since the rate at which the countermeasure was administered is not too efficient. The black line symbolizes that infected nodes increases 100 thousand to about 110 thousand and later drop due to use of anti-virus on the mobile devices and the red colored line symbolizes the population of mobile devices that are vulnerable to attacks by malwares this population drops drastically in less than 10 days due to battery extortion or crashed mobile devices and also the use of antivirus as countermeasure.

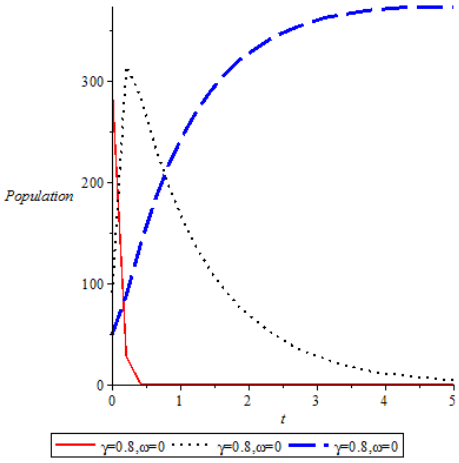

Fig. 4. Graph of Network population Against time ($\gamma = 0.8, \omega = 0$).

Fig. 4 is the graph that displays the pictorial representation of the behaviors of the Table 1 where the blue line in the graph symbolizes the behavior of the population of the recovered nodes which increases due to the use of anti-virus at 80% on the mobile devices and later becomes stable at a population of about 400 thousand since the rate at which the counter measure was administered is efficient. The black line symbolizes that infected nodes increases 100 thousand to about 110 thousand and later drop due to use of anti-virus on the mobile devices and the red colored line symbolizes the population of mobile devices that are vulnerable to attacks by malwares this population drops drastically in less than 10 days due to battery extortion or crashed mobile devices and also the use of antivirus as countermeasure.

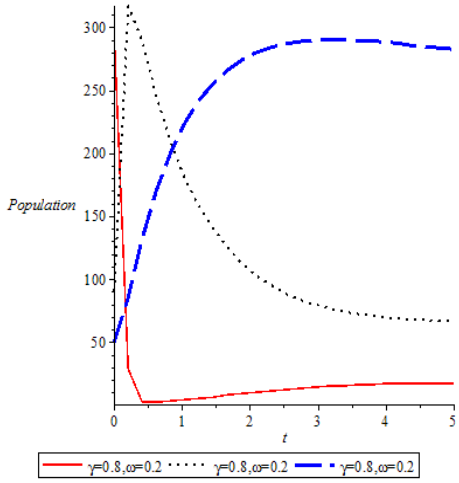

Fig. 5. Graph of Network population Against time ($\gamma = 0.8, \omega = 0.2$).

Fig. 5 is the graph that displays the pictorial representation of the behaviors of the Table 1 where the blue line in the graph symbolizes the behavior of the population of the recovered nodes which increases due to the use of anti-virus at 80% on the mobile devices and later becomes stable at a population of about 400 thousand since the rate at which the counter measure was administered is efficient, later this recovered devices which becomes vulnerable due to lack of anti-virus update since the anti-virus loses effectiveness at 20%. The black line symbolizes that infected nodes increases from 100 thousands to over 300 thousands and later drop due to use of anti-virus on the mobile devices but the anti-virus was not updated over time therefore the malware was not controlled completely and the red colored line symbolizes the population of mobile devices that are vulnerable to attacks by malwares this population drops drastically in less than 10 days due to battery extortion or crashed mobile devices and also the use of antivirus as countermeasure, but later the vulnerable devices started increasing again due to lack of update.

Fig. 6 is the graph that displays the pictorial representation of the behaviors of the Table 1 where the blue line in the graph symbolizes the behavior of the population of the recovered nodes which increases due to the use of anti-virus at 80% on the mobile devices and later becomes stable at a population less than 250 thousand since the rate at which the counter measure was administered is efficient. Later this

978-1-5090-6435-9/17/$31.00 ©2017 IEEE

recovered devices become vulnerable due to lack of anti-virus update since the anti-virus loses effectiveness at 50%.

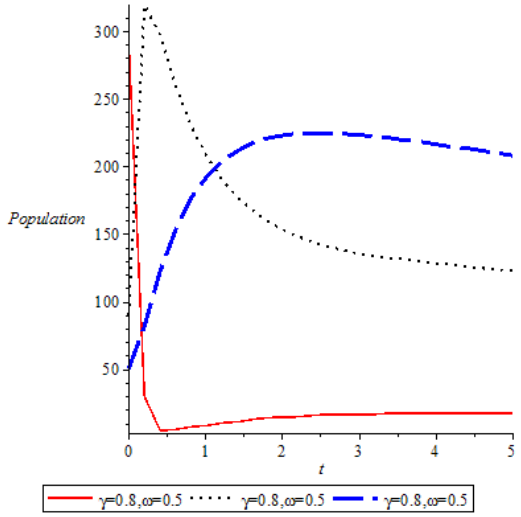

Fig. 6. Graph of Network population against time ($\gamma = 0.8, \omega = 0.5$).

The recovered nodes here are not as much as the population when the anti-virus only loss effectiveness at 20%. The black line symbolizes that infected nodes increases 100 thousand to over 300 thousand and later drop due to use of anti-virus on the mobile devices but the anti-virus was not updated/absence of security patches over time therefore the malware was not controlled completely and the red colored line symbolizes the population of mobile devices that are vulnerable to attacks by malwares this population drops drastically in less than 10 days due to battery extortion or crashed mobile devices and also the use of antivirus/application of security patch as countermeasure, but later the vulnerable devices started increasing again due to lack of update

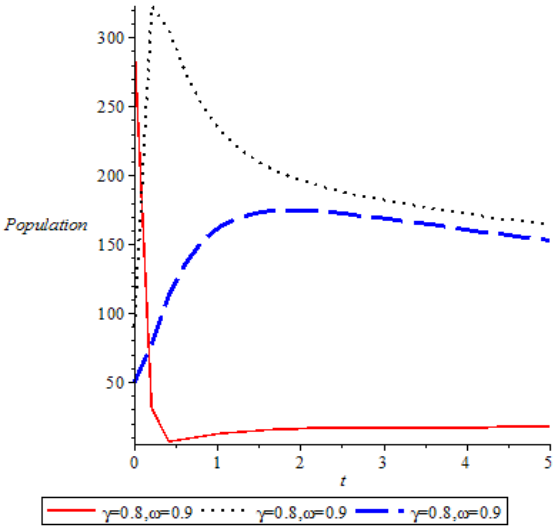

Fig. 7. Graph of Network population against time ($\gamma = 0.8, \omega = 0.9$).

Fig. 7 is the graph that displays the pictorial representation of the behaviors of the Table 1 where the blue line in the graph symbolizes the behavior of the population of the recovered nodes which increases due to the use of anti-virus at 80% on the mobile devices and later becomes stable at a population less than 200 thousand since the rate at which the counter measure was administered is efficient, later this recovered devices becomes vulnerable due to lack of anti-virus update since the anti-virus loses effectiveness at 90% the recovered nodes here are not as much as the population when the anti-virus only loss effectiveness at 50%. The black line symbolizes that infected nodes increases 100 thousand to over 30 thousand and later drop (the dropping is not as significant as when the lack of antivirus update was just 50%) due to use of anti-virus on the mobile devices but the anti-virus was not updated over time therefore the malware was not controlled completely and the red colored line symbolizes the population of mobile devices that are vulnerable to attacks by malwares this population drops drastically in less than 10 days due to battery extortion or crashed mobile devices and also the use of antivirus as countermeasure, but later the vulnerable devices started increasing again due to lack of update.

VIII. Conclusion

With more than 1 million devices' victims of malware attack, every day around the globe costing the world an estimated 3.5 trillion dollars annually. This figures 30 times the external reserve of United State which is bigger than the combined external reserve of the whole Europe. It is against this background that a clear understanding of the dynamics of spread and countermeasure of malware attack would not only put people back in control of their devices but is of business, industrial, Government and defense imperative. Based on the existence of isomorphism that exists between the mathematical structures of epidemic disease (compartmental models, an SIR (i=1,2,3)) and malware phenomenon. The initial parameters rates (Table 2) were hypothetical. The Homotopy Perturbation Method (HPM) were used to solve and analyze the model equations, we run the simulation using mathematical package (maple) and our results were presented graphically. The study confirms a link between malware attack and effectiveness of countermeasure (i.e. application of antivirus-virus signature defense or security patches) (see Fig. 1 to 7) with spread within short time of outbreak. Malware attack is severe and persistent when the countermeasure coverage rate is limited (i.e. poorly effectively). Hence, an effective countermeasure (at least 80%) would mitigate the impact of malware intrusion and disruption on the mobile wireless devices network (see Fig. 4 to 7). The study also found that the recovery rate of compromised mobile devices do well with an effective implementation antivirus signature defense (done early enough) though temporarily once a new malware variant emerges (see Fig. 4 to 7). Again, since regular updates of antivirus signature defense and application of security parches remain the most effective countermeasure policy option (at 80%) as seen in our investigation then it follows that intelligent farming and sharing on the mobile wireless network an anchored on big data technology is the way to go.

978-1-5090-6435-9/17/$31.00 ©2017 IEEE

IX. RECOMMENDATIONS

Combating malwares on mobile wireless network whether it is virus or worm including ransom-ware is long drawn battle because of the complexity of human behavior and new variants of malware being generated on a daily basis. Hence the study recommends the following:

1) The sustenance of existing good practices of Installation and frequent update of countermeasures (anti-malware packages or security patches on vulnerable) on vulnerable mobiles devices to deal with new variants of malware not yet blacklisted.

2) Access points between mobile wireless networks should be protected by VPN (private virtual network).

3) The suspicious level of malicious websites, mail and mobile applications at the checkpoints should be raised.

4) Due to the surge in the use of mobile wireless devices globally even among minors the level of public sensitization (include intelligent sharing) on what the hackers and cyber criminals are capable of doing (such as hijacking of mobile devices and strategic files, bullying, radicalization, terrorism, privacy inversion, identity theft, financial swindling, technical support scam) should be step up.

Finally, in view of the positive possibilities that the combine effect of integrating the existing countermeasures with big data technology, legal framework and forensic science holds on the curtailing of malware assault on the mobile wireless networked devices: Future research should evaluate these possibilities.

REFERENCES

[1] L.Abboth, N.Davis,Park J.,James,"Modelling,Demography Analysis,Network Stealth Worms", Network Security, 2006, pp.-149-156.

[2] A, Hansson & T. Vikström, "Successful Crisis Management in the Airline Industry: A Quest for Legitimacy through Communication", Uppsala Universitet, 2011, pp.-17-26.

[3] D. John, "Murderd by Malware". Retrieved from blogs: http://blogs.computer.com/16801/murdered_by_malware_can_omputer_viruses_kill.html, 16th August, 2014.

[4] Adeyinka A. Falaye, Oluwafemi Osho, Maxwell I. Emehian, & Seun Ale 'Dynamics of SCADA System Malware: Impacts on Smart Grid Electricity Networksand Countermeasures' International Conference on Information and Communication Technology and Its Applications (ICTA 2016)Federal University of Technology, Minna, Nigeria,November 28 – 30,2016.

[5] Microsoft, "Digital Crimes Unit Fact Sheet." 2016.

[6] 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].

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

[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.I & II. The Problem of Endemicity," Proc. Roy. Soc. Lond. Series- A, vol. 11, pp. 700– 721, 1927 & *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] J. Su, K. Chan, A. Miklas, A. A. K. Po, S. Saroiu, E. Lara, and A. Goel, "A preliminary investigation of worm infections in a bluetooth environment," in Proc. 4th ACM Workshop on Recurring Malcode (WORM 2006), Fairfax, VA, USA, November 2006, pp. 9–16.

[20] J. Ji-Huan, "Homotopy Pertubation Technique", Computer Methods in Applied Mechanics and Engineering, vol. 178 (2), 1999, pp.-257-262.

978-1-5090-6435-9/17/$31.00 ©2017 IEEE