Evaluating Degrees of Differential Infections on Sensor Networks' Features Using the SEjIjR-V Epidemic Model

ChukwuNonso H. Nwokoye[1], Chikwue Umeugoji[2], Ikechukwu Umeh[3]

[1]Open Studies Unit, Nigeria Correctional Service, Awka, Nigeria.
[2,3]Computer Science Department, Nnamdi Azikiwe University, Awka, Nigeria.

chinonsonwokoye@gmail.com,chikwue@live.ca,ikumeh@gmail.com

Abstract

There are few models that discuss multi-group modeling for wireless sensor networks (WSNs), and this is because most studies have concentrated on computer networks epidemics. However, it has been discovered that this is a possible reality since epidemiological literature is cluttered with qualitative evidences of propagation of either worms or viruses in WSNs. Therefore, we propose Susceptible–Exposed (due to worm)–Exposed (due to virus)–Infectious (due to worm)– Infectious (due to virus)–Recovered–Susceptible model with Vaccination (SEjIjR-V) epidemic model using a simple mass action incidence. Summarily, the new model added sub-groups to the latent and infectious compartment. The solutions of the system of equations were derived for the equilibrium points and presented. These solutions aided the derivation of the reproduction number (Ro), which was obtained by finding the inverse of the susceptible compartment at the endemic equilibrium. This threshold parameter for secondary infections from one single case is the sum of the individual reproduction ratios of worms and viruses in the WSN. Finally, the study evaluated the impact of several parametric values for range and density after solving the system using a suitable numerical method. Specifically, it was discovered that increasing these spatial WSN features, increases the susceptibility to malware infection and lowers the impact of sensor vaccination. Put another way, more nodes exist in the exposed sub-classes, wherein the sensor nodes depict a reduced speed of transmission, thereby, causing even more nodes to become fully contagious at the Infected sub-classes of worms and viruses.

Keywords: *SEjIjR-V model, Worm, Virus, Communication range, Density, Wireless sensor networks*

1. Introduction

Communication through wired and wireless methods have become an essential component of daily living, not only for individuals but also for institutions that intend to increase effectiveness, efficiency, profit as well as to ensure leverage with information and communication technology (ICT). Transmission of data/information is possible through network types namely computer networks and wireless sensor networks (WSN). While the former consists of networked computers, the latter involves several sensors scattered in a field of interest in order to monitor temperature, humidity, movement and noise [1]. Adjacent sensors through multi-hop transmission aid information transfer to the base sink after data collection from neighboring sensor regions. At the sink node, the collected data undergoes more processing and analyses, and/or it is subsequently sent to the terminal recipient using a wired network [2]. This is because the sink is more complex and stronger, possessing more energy, communication and computing abilities. Several WSN applications are evident in the military (for battlefield surveillance), in agriculture (for precision farming) and in health (for

patient monitoring) [3]. To the list of WSN applications, Feng, et al. [4] added, "intrusion detection, perimeter monitoring, information gathering, and smart logistics support". These array of benefits has made WSN a contemporary research-worthy phenomena. However, even with the advantages of WSNs, that allows its deployment in inaccessible locations such as war zones, borders and unfriendly combative environments, it is constrained in terms of resources. Actually, sensors have little range of data sensing and transmission range for data communication. This has motivated the move to elongate sensor lifetime by several researchers who have dwelt on measures such as energy depletion, device deployment and topology. Other WSN challenges according to Shakya [1] are, "packet loss due to transmission errors, packet collisions, interference, node failures, and malicious attacks is common". Due to the fact that sensors possess fragile defense structures, they are soft targets to malware attack. Basically, the cyber threat attacks (or injects a malware) a vulnerable sensor node and through adjoining nodes, pervades the whole network causing failure. In order words, transmission done by infected sensor may imply replication of malware to neighboring nodes causing destruction, disruption of normal communication and damage of integrity for standard data packets.

To curb incessant cyber-attack on the ICT infrastructure, epidemic models have been used to understand the spread patterns of malwares. From the studies that clutter the extant network epidemiological literature, it is clear the models include Susceptibility, Latency, Infectiousness, Recovery, Quarantine, and Vaccination. Specifically, these analytical models involve vulnerable nodes while the exposed compartment represents a disease status wherein a node is infected but not infectious i.e. it has acquired the infection but it cannot be able transmit it yet. The import of the exposed state or compartment is found in its advantages in early worm detection and as Srivastava, Ojha, et al., [5] puts it, "(this) model is useful for the improvement of security and enhancing the lifetime of the wireless sensor network". Infectious nodes carry the malware infection whereas recovery is a state where is there is an absence of the infection. Vulnerable nodes can be inoculated to protect them against future malware attack. In this paper, we discuss the SEjIjR-V epidemic model, wherein the dynamics would consist of transmission range, density and the existence of more than one malicious-code (multi-group infections) in WSNs. This is to address the problem of simultaneous spread of multiple malware types such as worms and virus in a WSN. Note that this issue is yet to be addressed in WSN epidemiology.

The paper is organized as follows; Section 2 describes related works. Section 3 describes the methodology of the study. Section 4 introduces the SEjIjR-V model, its parameters and their meanings. Additionally, subsections of Section 4 describes the equilibrium points as well as the resulting reproduction number. Section 5 presents the numerical simulation and discussions while Section 6 presents the summary of the work and future directions.

2. Related Works

Under the review of pertinent literature, we would x-ray several mathematical models for WSN wherein phenomena such as susceptibility, node exposure, infectivity, recovery have been applied. In addition, we would also review the extent to which the multi-group concept has been applied in communication network epidemiology.

2.1 Mathematical Models for WSN

Due to the lack of acceptable strategy for lengthening the sensor life span, Wang, et al. [2] developed the EiSIRS epidemic model that derived expressions for sleep and work arrangement. Like Shen, et al. [3], the vulnerable, infective and recovered sensor nodes can either be at sleep or working node.

Mishra and Keshri [6] proposed the Susceptible-Exposed-Infective-Recovered-Susceptible model with Vaccination (SEIR-V) epidemic model wherein there is an assumption of inoculation for vulnerable sensors in order to guard against subsequent infections. The exposed nodes has slow transmission speed as a result of acquiring the malicious-code infections. Furthermore, they generated the epidemic threshold for the ensuing infections due to the addition of a single infectious node into the vulnerable population. The possibilities of sensor mobility was explored by Wang, et al. [7], where the theory of reaction-diffusion equations was used to represent the activities involved in malware spread. The model presents a characterization of both temporal and spatial features of the sensors. More so, there is the application of strategic immunization procedures for rectifying infected nodes and ensuring a malware-free network. Evaluation was done for speed of mobility, communication range and packet transfer rate through simulation experiments.

Mishra and Tyagi [8] extended the work in Mishra and Keshri [6] by adding the quarantine compartment. Specifically, they proposed the Susceptible-Exposed–Infectious–Quarantine–Recovered with Vaccination (SEIQR-V) epidemic model to illustrate worm spread behavior in WSN. Similarly, the exposed nodes has a certain level of worm infection that causes a lowering of communication speed. Zhang and Si [9] presented an extension of the SEIR-V propagation model [6] by performing further analyses. As the analyses involved the latent node, they used delay as the bifurcation parameter so as to study the presence (or otherwise) of worms using the SEIR-V model. In their work, they evaluated the features of the Hopf bifurcation through the normal form method and the center manifold theorem and it showed an unacceptable WSN condition where worm spread moves from positive equilibrium to a limit cycle. Mishra, et al. [10] proposed the Susceptible-Infected-Quarantine-Recovered (SIQRS) model to illustrate the spread of worms in WSN. Aside the basic compartments, the model represented reinfection, generated the spectral radius and subsequently, performed numerical experiments.

Haldar, et al. [11] explored the effect of some attributes associated with epidemics in wireless networks. Specifically, they proposed a five-compartment epidemic model which represented trust, selfishness, collaboration and switching behavior, alongside the exposed (latent) and infected nodes using a bilinear incidence for effective contacts. The latent nodes here presented some form of difference with the usual i.e. it is divided between the malicious and the selfish nodes. Analyses was done for two equilibrium points namely, endemic and infection-free equilibrium, wherein the former was represented in existence conditions. The study generated the epidemic threshold and performed numerical solutions with several experimental frameworks. Feng, et al. [4] proposed a modification of the original Susceptible-Infected-Recovered (SIR) model by adding expressions for communication radius, energy consumption and node distribution density. Later, they generated the basic reproduction number and performed numerical simulations for the purposes of validation.

The challenge of assessing reliability required to maintain effectual and steady transfer of data between sources (sensors) to destination (sink) motivated Shen, et al. [3] to propose a model in the form of a game (based on continuous-time markov chain) that can forecast malicious-code infections. The model consists of two compartments each for susceptible,

infected and recovered sensors and one compartment for dead nodes. Finally, they calculated the mean time to failure of a sensor and validated their reliability.

Nwokoye, et al. [12] applied the uniform random distribution to the SEIR-V model. Their study described the quantitative investigation of the effect of transmission range and density in WSN context.The study also presented the corresponding reproduction ratios as well as numerical simulations. Nwokoye, et al. [13] proposed the Q-SEIR and Q-SEIRV models modifications of the SEIR and the SEIR-V epidemic models. They aimed at isolating and treating infected nodes (in the pre-quarantine compartment) before their addition into the population of susceptible nodes. The solution of the pre-quarantine compartment was generated from the convolution integral. These works [12, 13] possess the exposed compartment where there exists a certain level of malicious code infection.

Srivastava, et al. [5] explored the Susceptible-Exposed-Infected-Quarantined-Recovered (SEIQR) by adding a different perspective i.e. aside worm control, their model allows for early detection of infected sensor nodes through the exposed compartment. There work considered transmission range and coverage area of sensor deployment. Finally, they generated the reproduction ratios and performed numerical simulation experiments. Shakya [1] modified the original Susceptible-Infected (SI) model consisting of non-linear differential equations by incorporating several WSN attributes such as sensing and communication range, density, sleep and total sensor nodes. Due to network failure resulting from overwhelming sensors with malware, the model seeks to reduce subsequent infection by exploring the spatial correlation between sensor nodes. Nwokoye and Umeh [14] used multiagent systems to represent the SEIR-V epidemic model through building simulators with the NetLogo agent language.

2.2 Mathematical Multigroup Models of Networks

Since our study involves multiple malware types i.e. virus and worms, it is pertinent that we review several works of that nature. The following models are instances of multi-group infections for computer networks, however, we found none for WSNs. The challenge with most of the above-mentioned WSN epidemic models is that they only represent the spread/containment of one kind of malware infection at a time. This concept of representing multiple infection types is referred to as multi-group modelling, and was originally investigated in the field of Mathematical Biosciences, where a particular heterogeneous population is divided into several homogenous classes based on behavior.

Mishra and Ansari [15] proposed an electronic differential Susceptible-Infectious-Removed- Susceptible (e-SIRS) for viral and worm propagation in a computer network. The model investigated periods of latency, immunity and time of self-multiplication. The reproduction number was derived and the solutions of the system was generated by the help of a numerical method. Mishra and Singh [16] developed the Susceptible, Infectious due to worm, Infectious due to virus, Infectious due to Trojan Horse, Recovered and Susceptible ($SI_1I_2I_3RS$) model with mass action incidence so as to provide protection to the cyber world. Their study discussed the threshold parameter, stability analyses of equilibrium points and solved the system of differential equations. Mishra and Prajapati [17] proposed the Susceptible class-1 for virus (S_1) - susceptible class-2 for worms (S_2) -susceptible class-3 for Trojan horse (S_3) – Infectious (I) – Recovered (R)) for malicious code transfer in a computer networks. Mishra [18] proposed the Susceptible, Infectious due to worm, Infectious due to virus, Recovered and Susceptible (SI_1I_2RS) epidemic model to restrain the effect and transfer of these malicious codes. The Liapunov function was employed for the stability analysis at stated equilibrium points and using numerical methods were used to simulate the model for

validation. While the infectious population of [15, 16 and 18] is divided into homogenous groups based on behaviors of malwares (virus, worm etc.), the susceptible population in [17] was divided for these same malicious codes.

From the reviewed works, it is clear that although the SEIR-V model has been used to represent the propagation of one malicious object, no study has evaluated the spread of multiple malwares in WSNs, and this has motivated this study. Our model herein involves differential infectivity of both the exposed and infected nodes – a phenomena that hasn't been addressed even for multi-group computer network models.

3. Research Methodology

We adopt a renowned methodology in network epidemiology called the Modeling and Analysis of Dynamical Systems. The methodology commences with; 1. Formulation of the model and the schematic diagram. In this case, the SEjIjR-V epidemic model would be formulated (Section 4) with parameters that depict a functional WSN. 2. Finding the equilibrium points (for the malicious code-free and the endemic). These solutions are gotten by equating the system of differential equations to zero. 3. Generating the epidemic threshold or reproduction number (Ro). Ro is necessary if we network managers are to understand the rate at which secondary infections would occur.4. Performing sensitivity analysis or numerical simulations using parametric values and highlighting the import of observed responses and behaviors of compartments. Although, there exists plenty software used for simulation purposes, we would employ MATLAB.

4. SEjIjR-V Epidemic Model with Differential Exposure, Infectivity, Communication Range

In order to represent the dynamics of multiple malicious code spread in a WSN, we present the Susceptible (S)–Exposed due to worm (E_1)–Exposed due to virus (E_2)–Infectious due to worm (I_1)–Infectious due to virus (I_2)–Recovered (R)–Susceptible (S) model with Vaccination (V) ($SE_1E_2I_1I_2R$-V) epidemic model (Figure 1). Several assumptions considered for the study include; the sensors are of same size and make, they are stationary and scattered in sensor field, thus, they collect and transmit data to neighbor nodes using antennas. For the transmission range and distribution density, we adopt the expression proposed by Tang and Mark [19], which is slightly different to the expression by Feng et al. [4]. Nodes are added to the network as susceptible sensors and death is a result of worm/virus attack and/or software/hardware failure. Nodes carrying the infection (from virus or worms) can recover with a transient immunity which can be lost making it possible for node reinfection. The schematic diagram for the dynamical transfer of malicious codes in a WSN given our assumptions is depicted as Figure 1. The actual parameters for the model are; λ is the recruitment of susceptible nodes in the WSN, μ is the death rate due to the software or hardware failure, σ is the distribution density for the sensor nodes, r^2 is the communication range, β_1 is the infectivity rate due to virus, β_2 is the infectivity rate due to worm, ω_1 is the death rate of the sensor node as a result of virus attack, ω_2 is the death rate of the sensor node as a result of worm attack, α_1 is the rate of recovery from virus infection, α_2 is the ate of recovery from worm infection, φ is the rate of loss of temporary immunity and entrance into the susceptible compartment, θ_1 is the rate of transfer to from the exposed to the virus infectious compartment, θ_2 is the rate of transfer to from the exposed to the worm infectious compartment, ρ is the rate of transmission from the vaccination class to the susceptible

compartment and ξ is the rate of vaccination for vulnerable sensor nodes. The total sensor nodes in the WSN at any time t is

$$N(t) = S(t) + E_1(t) + E_2(t) + I_1(t) + I_2(t) + R(t) + V(t) \quad (1)$$

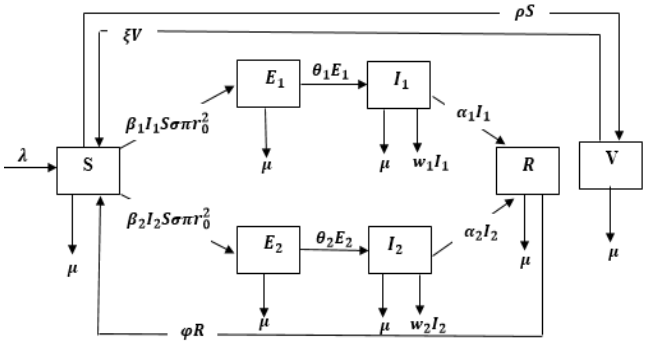


Figure 1. Schematic Diagram for the flow of Malware in a WSN

Our proposed modifications was done on the SEIR-V model [6**]** by adding sub groups for the exposed and the infectious compartments alongside distribution density and transmission range. This resulted to the SEjIjR-V Epidemic Model, which is characterized using the following system of differential equations;

$$\dot{S} = \lambda - \mu S - \sum_{j=1}^{2} \beta j I j S \sigma \pi r^2 + \varphi R - \rho S + \xi V$$

$$\dot{E} = \sum_{j=1}^{2} \beta j I j S \sigma \pi r^2 - (\theta j + \mu) E j$$

$$\dot{I} = \sum_{j=1}^{2} \theta j E j - (\mu + wj + \alpha j) I j; \text{ j = 1, 2.} \quad (2)$$

$$\dot{R} = \sum_{j=1}^{2} \alpha j I j - (\mu + \varphi) R$$

$$\dot{V} = \rho S - (\mu + \varepsilon) V$$

From the system of differential equations, transient immunity periods for the recovered and the vaccinated nodes are $1/\varphi$ and $1/\xi$ respectively. In the absence of either virus or worm attack, the population size of the sensor nodes approaches the carrying capacity λ/μ. System of differential equations (2) is decomposed to give the following;

$$\dot{S} = \lambda - \mu S - S \sigma \pi r^2 (\beta_1 I_1 + \beta_2 I_2) + \varphi R$$

$$\dot{E}_1 = \beta_1 I_1 S \sigma \pi r^2 - (\mu + \theta_1) E_1$$

$$\dot{E}_2 = \beta_2 I_2 S \sigma \pi r^2 - (\mu + \theta_2) E_2$$

$$\dot{I}_1 = \theta_1 E_1 - (\mu + w_1 + \alpha_1) I_1 \quad (3)$$

$$\dot{I}_2 = \theta_2 E_2 - (\mu + w_2 + \alpha_2) I_2$$

$$\dot{R} = \alpha_1 I_1 + \alpha_2 I_2 - (\mu + \varphi) R$$

$$\dot{V} = \rho S - (\mu + \varepsilon) V$$

4.1 Existence of Equilibrium

We obtain the solutions of the system of equations (3) by equating it to zero. Specifically, this will result to a two possible equilibrium points; the malicious code-free equilibrium (MFE) and the endemic equilibrium (EE).

$$\frac{dS}{dt} = 0, \frac{dE_1}{dt} = 0, \frac{dE_2}{dt} = 0, \frac{dI_1}{dt} = 0, \frac{dI_2}{dt} = 0, \frac{dR}{dt} = 0, \frac{dV}{dt} = 0.$$

By simple calculation, the MFE has the following solutions;

$$S^0 = \frac{(\lambda\mu+\lambda\xi)}{(\mu(\mu+\xi+\rho))}, E_1^0 = 0, E_2^0 = 0, I_1^0 = 0, \ I_2^0 = 0, R^0 = 0, V^0 = \frac{\lambda\rho}{\mu(\mu+\xi+\rho)}$$

While the endemic equilibrium has the following solutions;

$$S^* = \sum_{j=1}^{2} \frac{(\mu+\theta_j)(\mu+\alpha_j+\omega_j)}{\sigma\pi r^2\beta_j\theta_j}$$

$$E^* = \sum_{j=1}^{2} \frac{(\mu+\varphi)(\mu+\alpha_j+\omega_j)(\lambda - \frac{\mu(\mu+\xi+\rho)(\mu+\theta_j)(\mu+\alpha_j+\omega_j)}{(\mu+\xi)\sigma\pi r^2\beta_j\theta_j})}{\mu\alpha_j(\mu+\varphi+\theta_j)+(\mu+\varphi)(\mu+\theta_j)(\mu+\omega_j)}$$

$$I^* = \sum_{j=1}^{2} \frac{(\mu+\varphi)(\lambda\theta_j - \frac{\mu(\mu+\xi+\rho)(\mu+\theta_j)(\mu+\alpha_j+\omega_j)}{(\mu+\xi)\sigma\pi r^2\beta_j})}{\mu\alpha_j(\mu+\varphi+\theta_j)+(\mu+\varphi)(\mu+\theta_j)(\mu+\omega_j)}$$

$$R^* = \sum_{j=1}^{2} \frac{\alpha_j(\lambda\theta_j - \frac{\mu(\mu+\xi+\rho)(\mu+\theta_j)(\mu+\alpha_j+\omega_j)}{(\mu+\xi)\sigma\pi r^2\beta_j})}{\mu\alpha_j(\mu+\varphi+\theta_j)+(\mu+\varphi)(\mu+\theta_j)(\mu+\omega_j)}$$

$$V^* = \sum_{j=1}^{2} \frac{(\rho(\mu+\theta_j)(\mu+\alpha_j+\omega_j))}{((\mu+\xi)\sigma\pi r^2\beta_j\theta_j)}$$

At the MFE, it is evident that the exposed and infectious sub-compartments equals zero, and the implication is that there is no infection at this equilibrium point. Since there is no infection in the network, none of the nodes recover, thereby, making the recovered compartment to be equal to zero. This is consistent with the real world. On the other hand, at EE, our results shows the solutions for all the compartments. Note that each solution (at EE) is for both virus and worms in the WSN, thus, the reason for using the summation sign (Σ).

4.2 Reproduction Number (R_0)

As Diekmann, et al. [20] puts it, "reproduction number is the expected number of secondary cases produced in a completely susceptible population, by a typical infective individual (or node)". However, aside using the next generation matrix method, R_0 can also be determined by simply finding the inverse of the susceptible compartment at endemic equilibrium. In that case, the R_0 for the SEjIjR-V model is given as follows;

$$R_0 = \sum_{j=1}^{2} \frac{\sigma \pi r^2 \beta_j \theta_j}{(\mu + \theta_j)(\mu + \alpha_j + \omega_j)}$$

The actual R_0 for secondary cases generated through one single infection is the sum of individual R_0s for both worm and virus infections. This is consistent with the study by Driessche and Watmough [21] on compartmental epidemic models. Specifically, in this study, the reproduction number depends on the infectivity contact rates due to virus and worm, order of effective contact with an infected node for transfer of infection, which consists of WSN features such as communication range and distribution density. Other parameters that contribute to the Ro are death rates as a result of malicious objects and hardware/software failure, rates of transfer from exposed to infectious compartments and rates of recovery from the multiple infections.

5. Numerical Simulation and Discussion

To solve the proposed system of differential equations (3), we employed a numerical method i.e. theRunge-Kutta order 4 and 5 in MATLAB. The software allowed the simulation of the model using parametric values. The network is assumed to have the following initial values: S=100, E_1=3, E_2=5, I_1=1, I_2=2, R=0, V=0. The other values used for the numerical simulations are as follows; $\lambda = 0.33$, $\mu = 0.003$, $\sigma = 0.1$, r =1; $\beta_1 = 0.2$, $\beta_2 = 0.3$, $\varphi = 0.3$; $\theta_1 = 0.30$; $\theta_2 = 0.40$, $\alpha_1 = 0.40$, $\alpha_2 = 0.25$, $\omega_1 = 0.27$, $\omega_2 = 0.09$, $\rho = 0.3$, $\xi = 0.06$.

The following figures shows the complex dynamics of propagation and containment when multiple infections are considered in a WSN. Figure 2 shows the time histories of the WSN considering E_1, E_2, I_1, I_2 nodes at 3,5,1, 2 (left) and 5, 3, 2, 1(right) respectively. Note that the range and density was kept constant at 1 and 0.3 respectively. From both figures it is clear that the exposed class increased, signifying the increase of sensors whose transmission speed lowered as a result of malware infection.

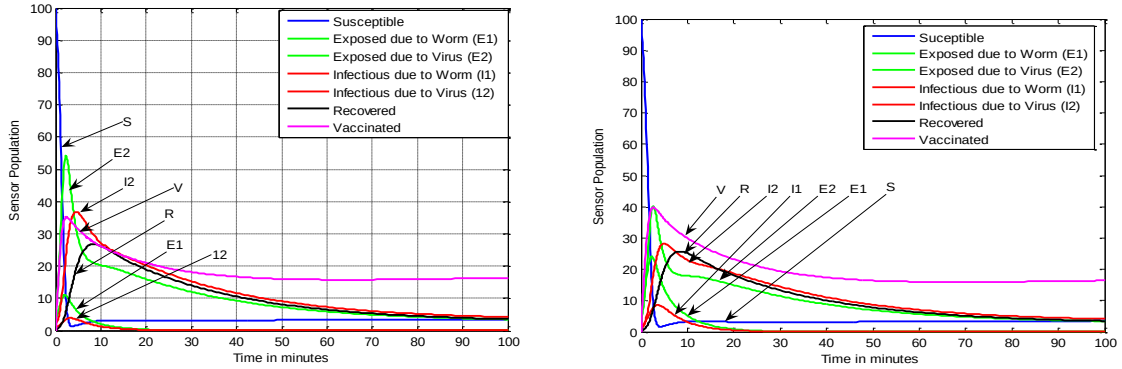
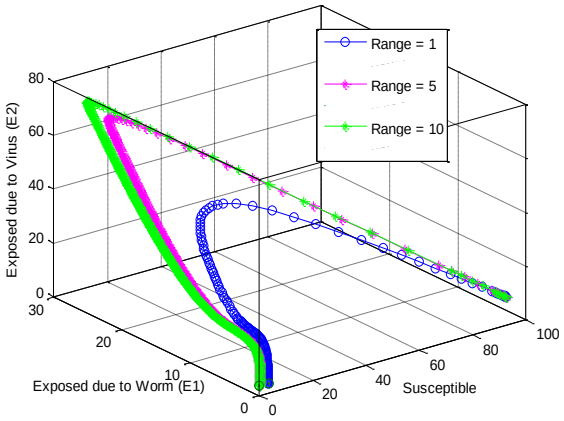


Figure 2. Time histories of the Sensor Population

Subsequent diagrams are basically three dimensional (3D) phase representations of the subgroups of exposed and infectious compartment alongside other compartments (Susceptible, Recovered and Vaccinated). On the left (L) are simulation results for varying communication ranges (1, 5, 10) when density is kept constant at 0.1, while on the right (R) are simulation results for changing density (0.1, 0.3, 0.6) when range is kept constant at 1. Figure 3 shows the 3D phase plot for range (L) and density (R) versus susceptible and the exposed compartments. Figure 4 is the 3D phase plot for range (L) and density (R) versus exposed sub-compartments and recovery. Figure 5 is the 3D phase plot for range (L) and density (R) versus exposed sub-compartments and vaccinated. Figure 6 depicts the 3D phase

plot for range (L) and density (R) versus infectious sub-compartments and susceptible. Figure 7 illustrates the 3D phase plot for varying range (L) and density (R) versus infectious sub-compartments and recovered. Figure 8 shows the 3D phase plot for varying range (L) and density (R) versus infectious sub-compartments and vaccinated.



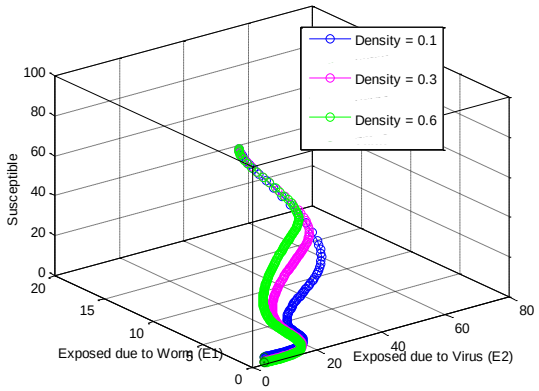
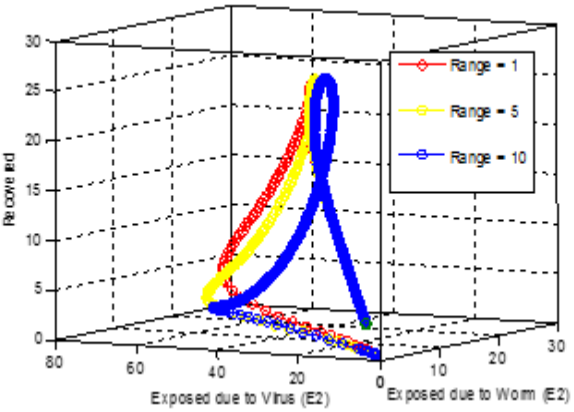


Figure 3. 3D Phase Plot of Range (L) and Density (R) for Susceptible and the Exposed Compartment



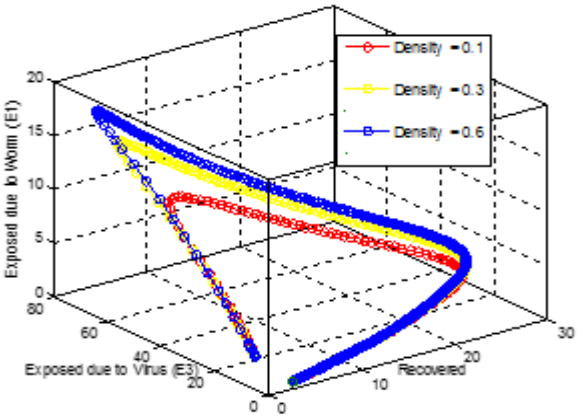
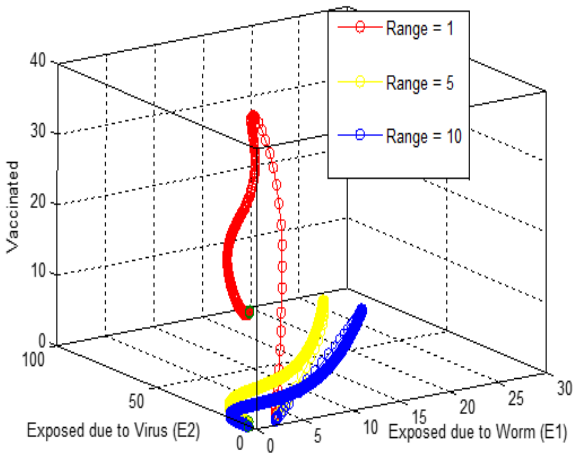


Figure 4. 3D Phase Plot of Varying Values of Range (L) and Density (R) for Exposed compartments and Recovery



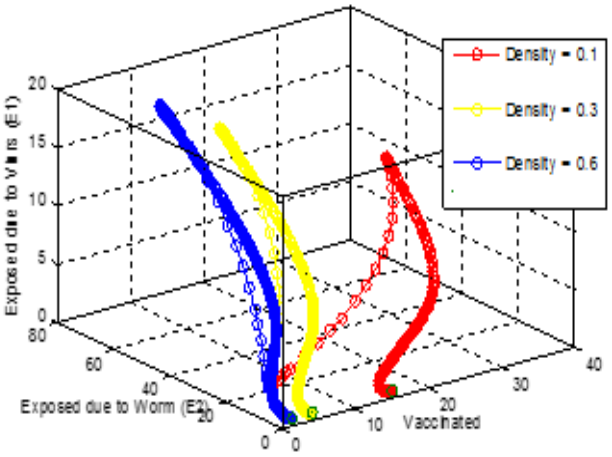


Figure 5. 3D Phase Plot of Varying Values of Range (L) and Density (R) for Exposed compartments and Vaccinated

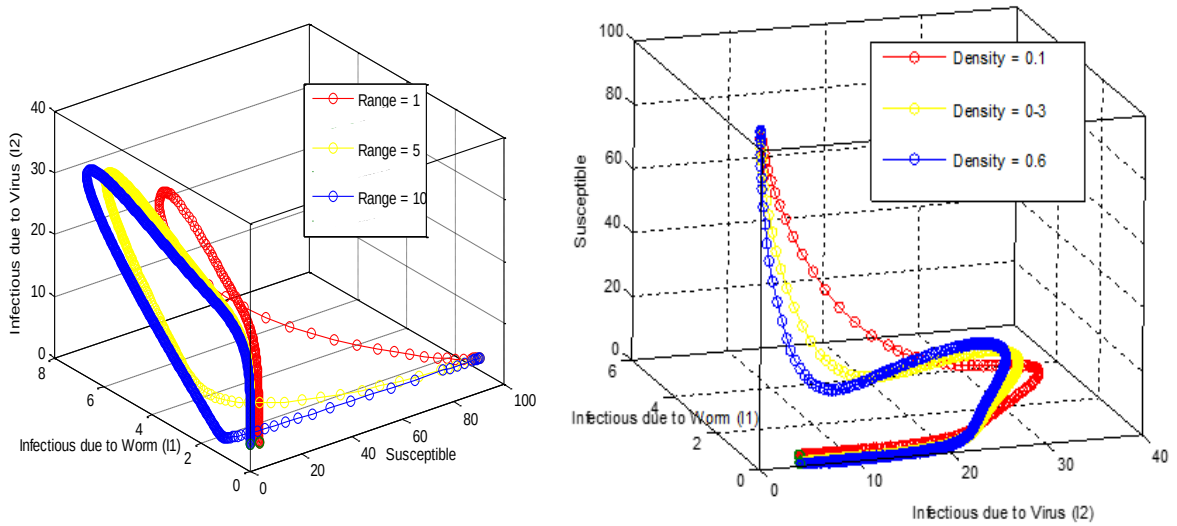


Figure 6. 3D Phase Plot of Varying Values of Range (L) and Density (R) for Infectious compartments and Susceptible

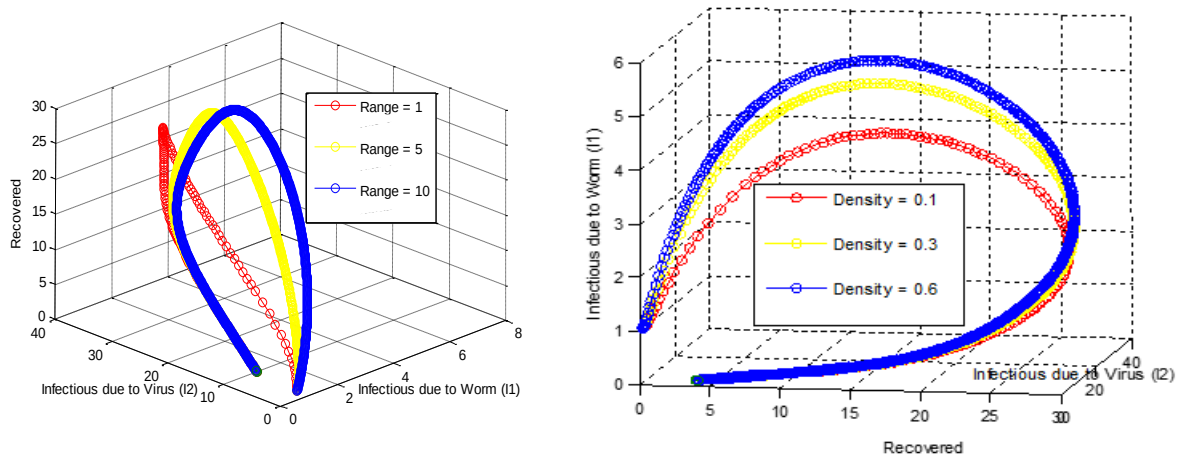


Figure 7. 3D Phase Plot of Varying Values of Range (L) and Density (R) for Infectious Sub-compartments and Recovered

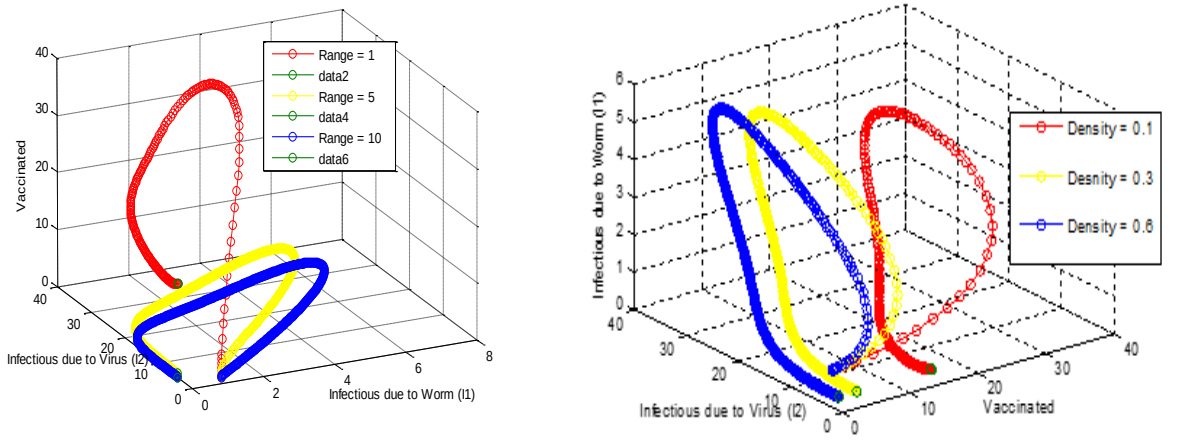


Figure 8. 3D Phase Plot of Varying Values of Range (L) and Density (R) for Infectious Sub-compartments and Vaccinated

Through the responses of Figure 3, increase in range and density visibly increases the susceptibility to malware infection. Also, Figure 6 at range = 1, 5 and 10, shows that increase in range and density visibly increases the susceptibility to malware infection. If the number of exposed nodes increase, then more sensor nodes approach full infectiousness and consequently, there is a higher tendency for network inundation by these hazardous varieties of malicious codes. Increasing these spatial WSN features also reduces the impact of sensor vaccination, if one considers Figure 8. This is consistent with older studies [12, 19] that model a single kind of malicious object using epidemic models. Some insights for network security management can be obtained through our analyses and simulations; since we now understand the impact of WSN features in a multi-group context. The implication is that institutions using WSNs for daily work should work on increasing the rate of sensor recovery and inoculation as worthy countermeasures. They should also aim to treat the infections at the exposed stage, whenever they notice that the speed of sensor transmission starts lower.

6. Conclusion and Future Directions

In this study, a differential $SE_1E_2I_1I_2R$-V epidemic model using a simple mass action incidence was developed. Therein, the exposed and infectious compartments are split into two groups consisting of firstly, nodes exposed/infected as a result of virus attack and secondly, nodes infected as a result of worm attack. Subsequently, we solved the system of differential equations by first equating it to zero to derive solutions at both the MFE and EE points. Typically, MFE possessed no infections at the exposed, infected and recovered compartments, and some symbolic solutions at the susceptible and the vaccinated compartments due to the inoculation of vulnerable sensor nodes. On the hand, the EE displayed amazing results, though complex. The summation sign was replaced at EE because the solutions are a sum of malware types (as well as other parameters) in the network. Furthermore, we derived and presented the attributes of the reproduction ratio, which is also the inverse of the susceptible compartment at EE. More so, we used the Runge-Kutta-Fehlberg fourth fifth order method to solve and simulate the proposed system of equations. Two dimensional and 3D phase plots were generated to be able to highlight the internal dynamical behavior of WSN in a multi-group context. In the future, we would evaluate the impact of other factors such as interleaving sleep and work modes, mobility, sensing range using a modified form of the proposed epidemic model. Furthermore, we would x-ray the impact of susceptibility for the subgroups of both exposed and the infections with differential reinfection. Our study herein is necessary because in the future, there will be possible incorporation of pervasive and wireless devices (and networks) with for instance, the extant plentiful dedicated medical and military technology.

References

[1]. R. K. Shakya, “Modified SI epidemic model for combating virus spread in spatially correlated wireless sensor networks, 2018, pp. 1-12,

[2]. X. Wang, Q. Li, and Y. Li, "EiSIRS: A formal model to analyze the dynamics of worm propagation in wireless sensor networks," Journal of Combinatorial Optimization, vol. 20, 2010, pp. 47–62.

[3]. S. Shen, L. Huang, J. Liu, A. C. Champion, S. Yu and Q. Cao. Reliability evaluation for clustered WSNs under malware propagation, Sensors, vol. 16, 2016, pp. 855.

[4]. L. Feng, L. Song, Q. Zhao, and H. Wang. Modeling and Stability Analysis of Worm Propagation in Wireless Sensor Network. Mathematical Problems in Engineering, vol. 2015, pp. 1-10.

[5]. P. K. Srivastava, R. P. Ojha, K. Sharma, S. Awsthi and G. Sanyal, "Effect of quarantine and recovery on infectious nodes in wireless sensor network", International Journal of Sensors, Wireless Communications and Control, vol. 8, 2018, pp. 26-36.

[6]. B. K. Mishra and N. Keshri, "Mathematical model on the transmission of worms in wireless sensor network," Applied Mathematical Modelling, vol. 37, 2013, pp. 4103–4111.

[7]. X. Wang, Z. He, X-Q. Zhao, C. Lin, Y. Pan and Z. Cai, "Reaction-diffusion modeling of malware propagation in mobile wireless sensor networks," Sci China Inf Sci, vol. 56, 2013.

[8]. B. K. Mishra and I. Tyagi, "Defending against malicious threats in wireless sensor network: A mathematical model", International Journal of Information Technology and Computer Science, vol. 6, 2014, pp. 12–19.

[9]. Z. Zhang and F. Si, "Dynamics of a delayed SEIRS-V model on the transmission of worms in a wireless sensor network," Advances in Difference Equations, vol. 2014, pp. 1–15.

[10]. B. K. Mishra, S. K. Srivastava, B. K. Mishra. A quarantine model on the spreading behavior of worms in wireless sensor network. Transaction on IoT and Cloud Computing, vol. 2, 2014, pp. 1-12.

[11]. K. Haldar, N. Narayan and B. K. Mishra, "A mathematical model on selfishness and malicious behavior in trust based cooperative wireless networks," I. J. Computer Network and Information Security, vol. 10, 2015, pp. 15-22.

[12]. C. H. Nwokoye, V. E. Ejiofor, R. Orji, I. Umeh, and N. N. Mbeledogu, "Investigating the effect of uniform random distribution of nodes in wireless sensor networks using an epidemic worm model", CORI'16, 2016, pp. 58-63.

[13]. C. H. Nwokoye, V. E. Ejiofor and C. G. Ozoegwu, "Pre-Quarantine approach for defense against propagation of malicious objects in networks," International Journal of Computer Network and Information Security, vol. 9, 2017, pp. 43-52.

[14]. C. Nwokoye and I. Umeh. Analytic-agent cyber dynamical systems analysis and design method for modeling spatio-temporal factors of malware propagation in wireless sensor networks. MethodsX, vol. 5, 2018, pp. 1373–1398.

[15]. B. K. Mishra and G. M. Ansari, "Differential epidemic model of virus and worms in computer network", International Journal of Network Security, vol.14, 2012, pp. 149-155.

[16]. B. K. Mishra and A. K. Singh, "SIjRS E-epidemic model with multiple groups of infection in computer network", International Journal of Nonlinear Science, vol.13, 2012, pp. 357-362.

[17]. B. K. Mishra and A. Prajapati. Mathematical model on attack by malicious objects leading to cyber war. International Journal of Nonlinear Science, vol.17, 2014, pp. 145-153

[18]. B. K. Mishra, "Mathematical model on attack of worm and virus in computer network, "International Journal of Future Generation Communication and Networking, vol. 9, 2016, pp. 245-254.

[19]. S. Tang and B. L. Mark, "Analysis of virus spread in wireless sensor networks: An epidemic model," Proceedings of the 7th International Workshop on the Design of Reliable Communication Networks, 2009, pp. 86–91.

[20]. O. Diekmann, J. A. P. Heesterbeek and J. A. J. Metz, "On the definition and the computation of the basic reproduction ratio R0 in models for infectious diseases in heterogeneous populations", Journal of Mathematical Biology, vol. 28, 1990, pp. 365–382.

[21]. P. Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission", Mathematical Biosciences, vol. 180, 2002, pp. 29–48.