International Journal of Control and Automation
Vol. 11, No. 3 (2018), pp.129-142
http//dx.doi.org/10.14257/ijca.2018.11.3.12

Modeling Multigroup Malicious Code Infections in Sensor Networks

Chukwu Nonso H. Nwokoye and Moses O. Onyesolu

Nnamdi Azikiwe University, Awka, Nigeria
explode2kg@yahoo.com, mo.onyesolu@unizik.edu.ng

Abstract

Older epidemic models of wireless sensor network (WSN) mostly cater for one type of malicious code infection. Inspired by the modeling of heterogeneous populations of diseases in the Biosciences, we propose the Susceptible, Infectious due to virus, Infectious due to worm, Infectious due to a virus/worm variant, Recovered and Susceptible with Vaccination (SI_jRS-V) epidemic model, to characterize the dynamics of propagation of more than one malicious code infection in a WSN. Aside possessing differential infectivity, the proposed model has transmission range and density – characteristic features of a WSN. We discovered that the actual reproduction number (R_o) involves the infective and death rates of virus, worm and a virus/worm variant as well as the communication range and density. In other words, the actual R_o is the sum of the 'reproduction numbers' for each group. A numerical method was used to solve the system of equations. The impact of transmission range and distribution density on the different types of malicious codes was investigated using simulation experiments.

Keywords: *SIjRS-V epidemic model; Virus; Worm; Virus/Worm variant; Communication range; Distribution Density*

1. Introduction

The advent of the cyber world has brought tremendous changes in today's society, allowing quick access to data and information just by a button click. Of course, underlying the cyber world is the Internet. Its increasing use presents numerous potentials, resources, solutions and conveniences. Consequent upon these developments is the threatening possibilities of malicious attacks to information and communication technology (ICT) infrastructures/networks of organizations/institutions that employ the internet connectivity for daily work and business. Misuses of computers in these organizations also contribute to network intrusion by malicious objects/codes. In fact, these malicious objects are threatening the existence and the utility of the cyber world [1]. Attacks in networks ranges from virus, worms, Trojans and root kits *etc.* Popular worms include Confiker, Nimda, Code Red while popular viruses include Melissa, Love letter *etc.* On the other hand, while viruses may require human intervention in the form of sharing disks, opening an email *etc*, worms may self replicate from one machine to another.

As Nwokoye *et al.* [2] puts it, "WSN consists of sensor nodes which are distributed in a sensor field where they are connected to the sink, to track, record and send ambient territorial parameters to a data collector (or base station) through multihop infrastructureless transmission between neighboring sensor nodes". Figure 1 depicts the structural representation of a typical WSN. Research has shown that WSN are vulnerable to attacks from worms. This may be due to its open nature of communication. The malicious attacks "can be of a lesser intrusive nature (such as

Received (December 28, 2017), Review Result (February 5, 2018), Accepted (February 16, 2018)

ISSN: 2005-4297 IJCA

violations of confidentiality or privacy, as in traffic analysis and eavesdropping) as well as of higher intrusive nature (such as disruption of the normal functions of the sensor nodes or altering the network traffic and hence destroying the integrity of the information)"[2]. Due to the ubiquity of WSN attacks such as Sinkhole, Sybil *etc.*, it becomes overly expedient to devise effective countermeasures against malware hazards. Recent developments in sensor networks indicate that a malevolent attacker can utilize several challenges (*i.e.* finite bandwidth, computational power, storage, and communication range; uncertainty (in mobility, topology control, density, sensing accuracy) of sensor nodes to outspread malicious codes all through the network without physical contact or human intervention [2]. Network security enthusiasts employ epidemic models to understand the propagation patterns of these malicious objects.

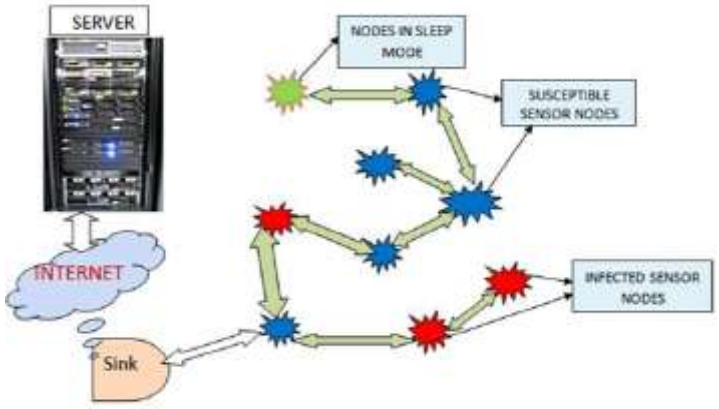

Figure 1. Structural Representation of WSN [3]

2. Related Works

In recent times epidemiological researchers of network security have highlighted the sameness in connectivity realities between biological viruses and malware equivalents. This has resulted to the use of epidemic models for the understanding of malware spread in networks (computer networks [4], peer-to-peer (P2P) [5], wireless sensor networks [6] and the WWW [7] or the internet [8]). These epidemic models compartmentalize the hosts according to their disease/infection status. Popular compartments include susceptible, infectious and recovered hosts and they mean hosts prone to infection, hosts that have acquired the infection and hosts that have recovered from the infection, respectively.

Here, we review epidemic models used to model worm/virus infection propagation and containment in WSN. The layer protocols and the topological consequences of many sensors placed in a grid was modeled by Khayam and Radha [9] using the topology-aware worm propagation model (TWPM). In a later publication, Khayam and Radha [10] modeled infection spread using the TWPM; the work considered protocols and signal processing strategy. While De *et al.* [11] proposed an epidemic model that employs the random graphs structured in relation to real network parameters; De *et al.* [12] investigated the susceptibility of multihop protocols (*i.e.* Trickle, Deluge and MNP) in terms of speed and reachability. De *et al.* [13] characterized two sensor node deployment strategies *i.e.* uniform random and group-based deployment. To cater for automatic triggering of effective antivirus software for treatment of infected sensor nodes, Tang and Mark [14] proposed the addition of a maintenance mechanism to the SIR model. Wang and Li [15]

formulated the nonlinear iSIR model to represent malicious code patterns in sensor networks. In a bid to add the sleep and work interleaving policy of WSN, Wang *et al.* [16] proposed the EiSIRS model as modification to the iSIR model that assumes that sensors work all the time. In order to check hardware and signaling overhead cost, Tang [17] proposed the addition of maintenance functionality to the basic SI epidemic model. Mishra and Keshri [6] proposed the Susceptible-Exposed-Infective-Recovered-Vaccination (SEIRS-V) model with mass action incidence rate and assumed that sensor nodes can be immunized against future infection. The model also assumed temporary immunity/re-infection and a latent phase where sensor nodes display slow transmission of data. Like Tang and Mark [14], Wang and Yang [18] investigated the effect of medium access control (MAC) and topology/uniform random distribution of sensor nodes on virus spread in a WSN using the Susceptible-Infected (SI) epidemic model. To describe worm dynamics in WSN, Mishra *et al.* [19] proposed the Susceptible–Infected–Quarantine–Recovered – Susceptible (SIQRS) model, Mishra and Tyagi, [20] proposed the Susceptible-Exposed–Infectious–Quarantine–Recovered with Vaccination (SEIQR-V) epidemic model. Aside the addition of the quarantine compartment in both models, the former did not consider the latent stage and the vaccination of sensor nodes in a wireless sensor network. Zhang and Si [21] studied the properties of the existent Hopf bifurcation in the SEIR-V epidemic model using the normal form method and the center manifold theorem. Keshri and Mishra [3] proposed security mechanisms using three epidemic models; they include the Susceptible–Infectious–Recovered–Crashed (SIRC) model, the Susceptible–Infectious–Quarantined–Recovered–Crashed (SIQRC) model and the Susceptible–Infectious–Recovered–Vaccination–Crashed (SIRVC) model. Using the expression for uniform random distribution proposed by Wang and Li [15], Feng *et al.*, [22] investigated the effect of communication radius, energy and density.

The issue with the above WSN epidemic models is the fact that they model one type of malicious code infection at a time; however, in our study herein we intend to model more than one type of infection at a time – this is referred to as multigroup modeling. As Driessche and Watmough [23] puts it, "'multigroup' usually refers to the division of a heterogeneous population into several homogeneous groups based on individual behaviour…(where)…each group is then subdivided into epidemiological compartments". Epidemic literature on technological networks availed instances of multi-group models that represent more than one type of infection, but they model the computer network and not the wireless sensor network. Examples of these multigroup models include the SI_jRS (Susceptible, Infectious due to worm, Infectious due to virus, Infectious due to trojan horse, Recovered and Susceptible) epidemic model to represent malicious transmissions with simple mass action incidence developed by Mishra and Singh [1]. Mishra and Ansari [24] formulated the eSIRS epidemic model (with standard incidence) wherein the susceptible and infected populations are divided into different groups and the nodes are vulnerable to virus and worms. Mishra and Singh [1] and Mishra and Ansari [24] are not suitable to characterize WSN because they lack parameters such as transmission range and distribution density. As it is evident in these works; [14], [15], [18] *etc*, these two parameters (range and density) have been added for epidemic modeling in WSN.

The needfulness of performing multi-group modeling for WSN is drawn from two reasons which include; (a) the fact that epidemic models have been used to model the propagation of virus [14, 18] and that of worms [3, 5 and 20], and (b) the strong possibility that both worm and virus might exist at the same time [1, 24].

3. The SI_jRS-V Epidemic Model with Differential Infectivity, Transmission Range and Density

To characterize the dynamics of propagation for more than one malicious code infection in a WSN, we propose the Susceptible, Infectious due to virus, Infectious due to worm, Infectious due to a virus/worm variant, Recovered and Susceptible with Vaccination (SI_jRS-V) model (Figure 2). We assume the sensors are similar, stationary and distributed in a sensor field. They also collect ambient data, which are sent to neighboring nodes within their signal transmission range using omnidirectional antennas. New nodes are recruited into the sensor network as susceptible nodes and death can be due to attacks from worm, virus or due to hardware failure. Infectious nodes (due to worms/viruses) may infect neighboring nodes; the population of infectious nodes is divided into three groups. Infectious nodes can recover with a certain temporal immunity. With the possible existence of virus/worm variants, recovered nodes quickly lose their immunity to become susceptible to infection again. Table 1 presents the actual WSN parameters and their meanings.

The total sensor population in the network at any time t is

$$N(t) = S(t) + I_1(t) + I_2(t) + I_3(t) + R(t) + V(t) \quad (1)$$

$$\frac{dN}{dt} = \eta k - \eta N - \sum_{j=1}^{3} e_j I_j \quad (2)$$

When the model involves a certain probability (P) of infectious nodes from the susceptible class

$$\frac{dN}{dt} = \eta k - \eta N - Pj \sum_{j=1}^{3} e_j I_j \quad (3)$$

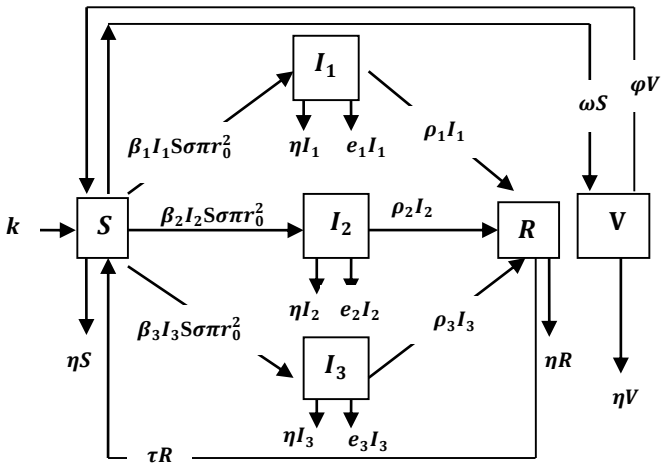

Figure 2. Schematic Diagram for the Flow of Malicious Codes in a WSN

Table 1. WSN Parameters and Their Meaning

Parameters	Meaning
k	The recruitment of susceptible nodes in the wireless sensor network
η	Death rate due to the reason other than the attack of malicious objects
σ	Distribution density
r_0^2	Transmission range
β_1	Infectivity contact rate for virus
β_2	Infectivity contact rate for worm
β_3	Infectivity contact rate for a virus/worm variant
$\sigma\pi r_0^2$	The order of effective contact with an infected node for transfer of infection
e_1	Mortality rate of the sensor nodes due to the attack of virus
e_2	Mortality rate of the sensor nodes due to the attack of worm
e_3	Mortality rate of the sensor nodes due to the attack of virus/worm variant
ρ_1	Rate of recovery from virus
ρ_2	Rate of recovery from worm
ρ_3	Rate of recovery from another virus/worm variant
τ	Rate of transfer to the susceptible class when temporal immunity wears off
φ	Rate of transmission from the vaccination class to the susceptible class
ω	Rate of inoculation for susceptible sensor nodes

The schematic diagram for the dynamical transmission of malicious codes in a WSN given our assumption is depicted as Figure 2. The system of differential equation (4) is adapted from Mishra and Singh [1] but modified to capture distribution density, transmission range and sensor vaccination. The SI_jRS-V Epidemic Model is represented using the following system of differential equations;

$$\begin{aligned}
\frac{dS}{dt} &= k - \eta S - \omega S - \sum_{j=1}^{3} \beta_j I_j S\sigma\pi r_0^2 + \tau R + \varphi V \\
\frac{dI}{dt} &= \sum_{j=1}^{3} \beta_j I_j S\sigma\pi r_0^2 - (\eta + e_j + \rho_j) I_j;\ j = 1, 2, 3. \\
\frac{dR}{dt} &= \sum_{j=1}^{3} \rho_j I_j S\sigma\pi r_0^2 - (\eta + \tau) R \\
\frac{dV}{dt} &= \omega S - (\eta + \varphi) V
\end{aligned} \tag{4}$$

The system of differential equation (4) is decomposed to give the following:

$$\begin{aligned}
\frac{dS}{dt} &= k - S(\eta + \omega) - S\sigma\pi r_0^2 (\beta_1 I_1 + \beta_2 I_2 + \beta_3 I_3) + \tau R + \varphi V \\
\frac{dI_1}{dt} &= \beta_1 I_1 S\sigma\pi r_0^2 - (\eta + e_1 + \rho_1) I_1 \\
\frac{dI_2}{dt} &= \beta_2 I_2 S\sigma\pi r_0^2 - (\eta + e_2 + \rho_2) I_2 \\
\frac{dI_3}{dt} &= \beta_3 I_3 S\sigma\pi r_0^2 - (\eta + e_3 + \rho_3) I_3 \\
\frac{dR}{dt} &= \rho_1 I_1 + \rho_2 I_2 + \rho_3 I_3 - (\eta + \tau) R \\
\frac{dV}{dt} &= \omega S - (\eta + \varphi) V
\end{aligned} \tag{5}$$

3.1. Existence of Equilibrium

The equilibrium points of system of equations (5) are the solution of the system of ordinary differential equation. Therefore, we have;

$$\frac{dS}{dt} = 0; \frac{dI_1}{dt} = 0; \frac{dI_2}{dt} = 0; \frac{dI_3}{dt} = 0; \frac{dR}{dt} = 0; \frac{dV}{dt} = 0.$$

The system of equations has two possible equilibriums; the infection free equilibrium (IFE) and the endemic equilibrium (EE). On simple calculations the infection-free equilibrium has the following solutions;

$$S^0 = \frac{k(\eta+\varphi)}{\eta(\eta+\varphi+\omega)}, I_1^0 = 0,\ I_2^0 = 0,\ I_3^0 = 0, R^0 = 0, V^0 = \frac{k\omega}{\eta(\eta+\varphi+\omega)} \tag{6}$$

While the endemic equilibrium is as follows;

$$S_j^* = \sum_{j=1}^{3} \frac{\eta + e_j + p_j}{\beta_j \sigma \pi r_0^2}$$

$$I_j^* = \sum_{j=1}^{3} \frac{(\eta+\tau)(-\eta(\eta+\varphi+\omega)(\eta+e_j+p_j) + k(\eta+\varphi)\beta_j\sigma\pi r_0^2)}{(\eta+\varphi)((\eta+\tau)(\eta+e_j)+\eta p_j)\beta_j\sigma\pi r_0^2} \tag{7}$$

$$= \sum_{j=1}^{3} \frac{p_1(-\eta(\eta+\varphi+\omega)(\eta+e_j+p_j) + k(\eta+\varphi)\beta_j\sigma\pi r_0^2)}{(\eta+\varphi)((\eta+\tau)(\eta+e_j)+\eta p_j)\beta_j\sigma\pi r_0^2}$$

$$R_j^*$$

$$V_j^* = \sum_{j=1}^{3} \frac{\omega(\eta+e_j+p_j)}{(\eta+\varphi)\beta_j\sigma\pi r_0^2}$$

If we assume a distinct transmission range and distribution density for each group of infection then the resulting solutions at the endemic equilibrium includes the following list of parameters; $\sigma_1, r_1^2, \sigma_2, r_2^2, \sigma_3, r_3^2$. These parameters are described in Table 2.

Table 2. Other WSN Parameters and Their Meaning

Parameters	Meaning
σ_1	Distribution density for virus propagation
r_1^2	Transmission range for virus propagation
σ_2	Distribution density for worm propagation
r_0^2	Transmission range for worm propagation
β_1	Infectivity contact rate for virus
β_2	Infectivity contact rate for worm

In the light of this addition, the endemic equilibrium is;

$$S^* = \frac{\eta+e_1+p_1}{\beta_1\sigma_1\pi r_1^2} + \frac{\eta+e_2+p_2}{\beta_2\sigma_2\pi r_2^2} + \frac{\eta+e_3+p_3}{\beta_3\sigma_3\pi r_3^2}$$

$$I_j^* = \sum_{j=1}^{3} \frac{(\eta+\tau)\left(-\eta(\eta+\varphi+\omega)(\eta+e_j+p_j) + k(\eta+\varphi)\beta_j\sigma_j\pi r_j^2\right)}{(\eta+\varphi)\left((\eta+\tau)(\eta+e_j)+\eta p_j\right)\beta_j\sigma_j\pi r_j^2} +$$

$$\frac{(\eta+\tau)(-\eta(\eta+\varphi+\omega)(\eta+e_2+p_2) + k(\eta+\varphi)\beta_2\sigma_2\pi r_2^2)}{(\eta+\varphi)\left((\eta+\tau)(\eta+e_2)+\eta p_2\right)\beta_2\sigma_2\pi r_2^2} +$$

$$R^* = \frac{(\eta+\tau)(-\eta(\eta+\varphi+\omega)(\eta+e_3+p_3)+k(\eta+\varphi)\beta_3\sigma_3\pi r_3^2)}{(\eta+\varphi)\big((\eta+\tau)(\eta+e_3)+\eta p_3\big)\beta_3\sigma_3\pi r_3^2} \quad (8)$$

$$= \frac{p_1(-\eta(\eta+\varphi+\omega)(\eta+e_1+p_1)+k(\eta+\varphi)\beta_1\sigma_1\pi r_1^2)}{(\eta+\varphi)\big((\eta+\tau)(\eta+e_1)+\eta p_1\big)\beta_1\sigma_1\pi r_1^2} + \frac{p_2(-\eta(\eta+\varphi+\omega)(\eta+e_2+p_2)+k(\eta+\varphi)\beta_2\sigma_2\pi r_2^2)}{(\eta+\varphi)\big((\eta+\tau)(\eta+e_2)+\eta p_2\big)\beta_2\sigma_2\pi r_2^2} + \frac{p_3(-\eta(\eta+\varphi+\omega)(\eta+e_3+p_3)+k(\eta+\varphi)\beta_3\sigma_3\pi r_3^2)}{(\eta+\varphi)\big((\eta+\tau)(\eta+e_3)+\eta p_3\big)\beta_3\sigma_3\pi r_3^2}$$

$$V^* = \frac{\omega(\eta+e_j+p_j)}{(\eta+\varphi)\beta_1\sigma_1\pi r_1^2} + \frac{\omega(\eta+e_j+p_j)}{(\eta+\varphi)\beta_2\sigma_2\pi r_2^2} + \frac{\omega(\eta+e_j+p_j)}{(\eta+\varphi)\beta_3\sigma_3\pi r_3^2}$$

3.2. Reproduction Number

Recall that the reproduction number is a threshold quantity that depicts "the expected number of secondary cases produced in a completely susceptible population, by a typical infective individual (or node)"[25]. The Reproduction number for the SI_jRS-V model is given as follows:

$$R_o = \sum_{j=1}^{3} \frac{\beta_j \sigma \pi r_0^2}{\eta+e_j+p_j} = (\sigma\pi r_0^2)\frac{\beta_1}{\eta+e_1+p_1} + \frac{\beta_2}{\eta+e_2+p_2} + \frac{\beta_3}{\eta+e_3+p_3} \quad (9)$$

If we assume a distinct transmission range and distribution density for each group of infection then the reproduction number is given as follows;

$$R_o = \sum_{j=1}^{3} \frac{\beta_j \sigma_j \pi r_j^2}{\eta+e_j+p_j} = \frac{\beta_1\sigma_1\pi r_1^2}{\eta+e_1+p_1} + \frac{\beta_2\sigma_2\pi r_2^2}{\eta+e_2+p_2} + \frac{\beta_3\sigma_3\pi r_3^2}{\eta+e_3+p_3} \quad (10)$$

In this study, the reproduction number depends on the infectivity contact rate due to virus, infectivity contact rate due to worm, infectivity contact rate due to virus/worm variant, communication range, distribution density, mortality rate due to virus, mortality rate due to worm, mortality rate due to virus/worm variant and mortality rate due to the reason other than the attack of malicious objects. The reproduction number also depends on the transmission range and the density. From the expressions above, it is evident that the actual reproduction ratio/number for the multigroup model is the sum of the 'reproduction numbers' for each group.

4. Numerical Simulation and Discussion

The Runge-Kutta-Fehlberg order 4 and 5 is employed to solve the system of differential equation (2) under different real parametric values and the graphs are plotted in MATLAB. The network is assumed to have initial values: S=95; I_1=25; I_2=20; I_3=30; R=0; V=0. Other parametric values used for the simulation experiments are listed in Table 3 below.

Table 3. WSN Parameters and their Values

Parameters	Value
k	0.090
η	0.005
σ	0.500
r_0^2	1.000
β_1	0.080

β_2	0.060
β_3	0.040
e_1	0.992
e_2	0.992
e_3	0.992
ρ_1	0.008
ρ_2	0.007
ρ_3	0.006
τ	0.005
φ	0.050
ω	0.090
P_1	0.260
P_2	0.270
P_3	0.470

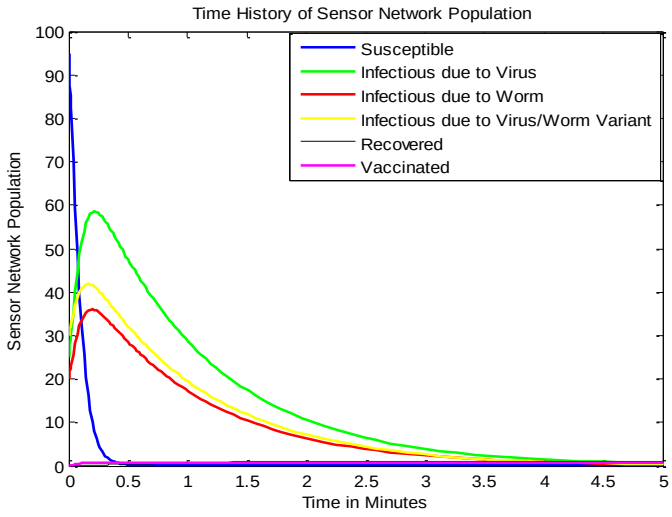

Figure 3. Dynamical Behaviour of the Classes (Without Probability of Infectious Nodes)

From Table 2 it is clear that we assume the same value for the mortality of sensor nodes as a result of attack from virus, worm and virus/worm variant. Figure 3 shows the dynamical behaviour of the classes (without probability of infectious nodes).

The model in Mishra and Singh [1] involved a certain probability of infective nodes (q*j*) which enter into the group I*j* from the susceptible class. Our system of equation (3) is absent this parameter. Below we present the probability of infective nodes alongside its resultant reproduction number.

The probability (P) of infectious nodes from the susceptible class =

$$Pj \sum_{j=1}^{3} \beta_j I_j S \sigma \pi r_0^2 \tag{11}$$

While the resultant reproduction number (R_o) in a WSN case =

$$\sum_{j=1}^{3} \frac{\beta_j P_j \sigma \pi r_0^2}{\eta + e_j + p_j} \tag{12}$$

For a distinct transmission range and distribution density for each subgroup, we present the probability of infective nodes alongside its resultant reproduction number.

The probability (P) of infectious nodes from the susceptible class =

$$Pj \sum_{j=1}^{3} \beta_j I_j S \sigma \pi r_0^2 \quad (13)$$

While the resultant reproduction number (R_o) in a WSN case =

$$\sum_{j=1}^{3} \frac{\beta_j P_j \sigma_j \pi r_j^2}{\eta + e_j + p_j} \quad (14)$$

The numerical simulation to observe the impact of adding the probability of infectious nodes from the susceptible class is presented as Figure 4, and the parametric values used were adapted from Mishra and Singh [1]. Though Figure 4 is the time history of the SI_jRS-V epidemic model (like Figure 3), the differences between the two figures are clearly evident.

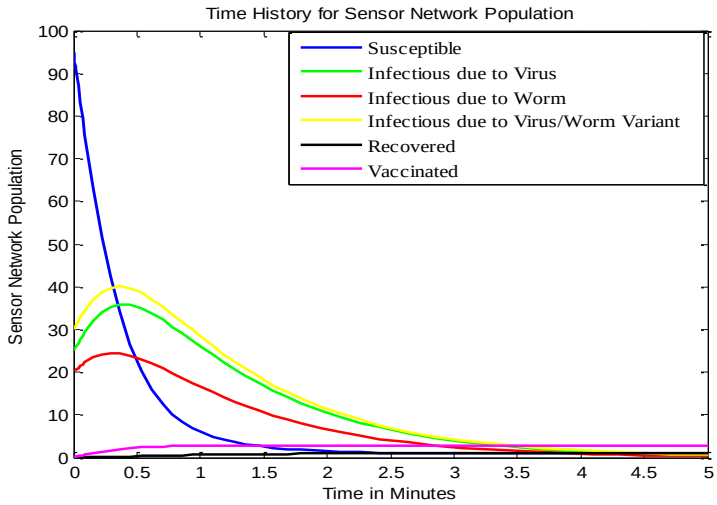

Figure 4. Dynamical Behaviour of the Classes (With Probability of Infectious Nodes)

Figure 5 depicts the impact of transmission range on the subgroups of the Infectious class while Figure 6 depicts the impact of transmission range on the susceptible, the recovered and the vaccinated sensor nodes. During the simulation of the two figures density was kept constant at 0.3, while the range was varied for 1, 3 and 10. From the two figures, it is evident that the increase in range increased infection and reduced the sensor inoculation in the network.

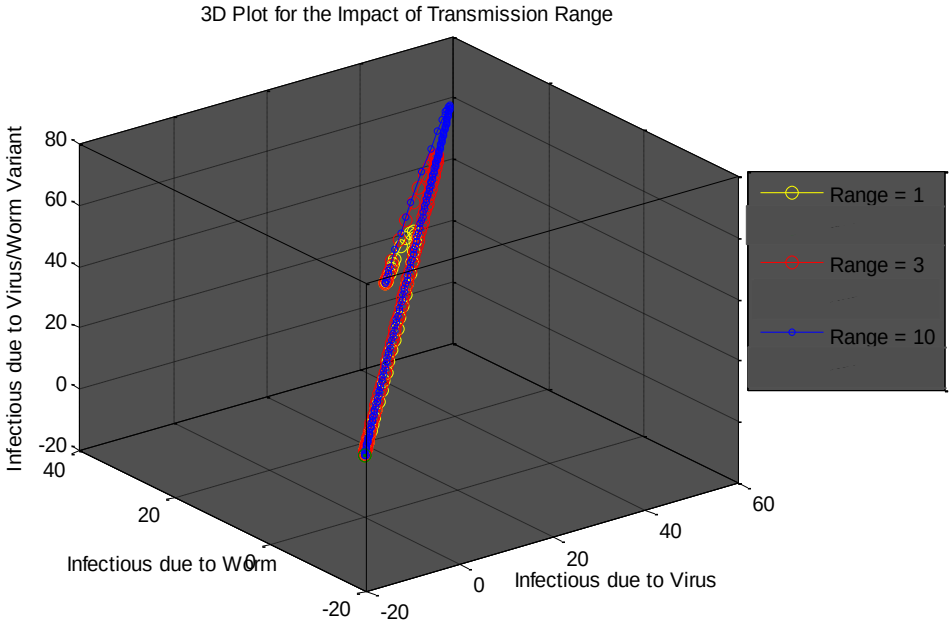

Figure 5. Dynamical Behaviour of the Infectious Class for showing the Impact of Transmission Range

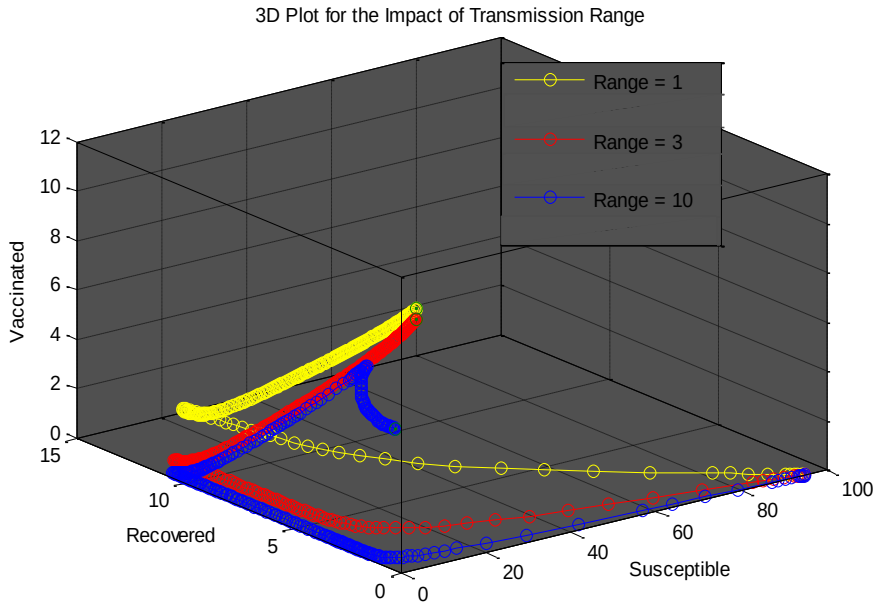

Figure 6. Dynamical Behaviour of the Susceptible, Recovered and Vaccinated for Transmission Ranges

We show the impact of distribution density on firstly, the subgroups of the infectious class (using Figure 7) and secondly, the susceptible, recovered and vaccinated sensor nodes (using Figure 8). During the simulation of the two figures, range was kept constant at 2, while the density was varied for 0.3, 0.8 and 1.3. The two figures displayed sensitivity to the increase in distribution density in the WSN when the subgroups of infections are considered as well as when other compartments are considered *i.e.* the increase in distribution density increased

infection and reduced the sensor vaccination in the network. Figure 9 depicts the dynamical behaviour of the Infectious due to virus, the Infectious due to worm and the Recovered class. The rates of recovery for the attack from the infectious class improved as we varied values of p1, p2 and p3.

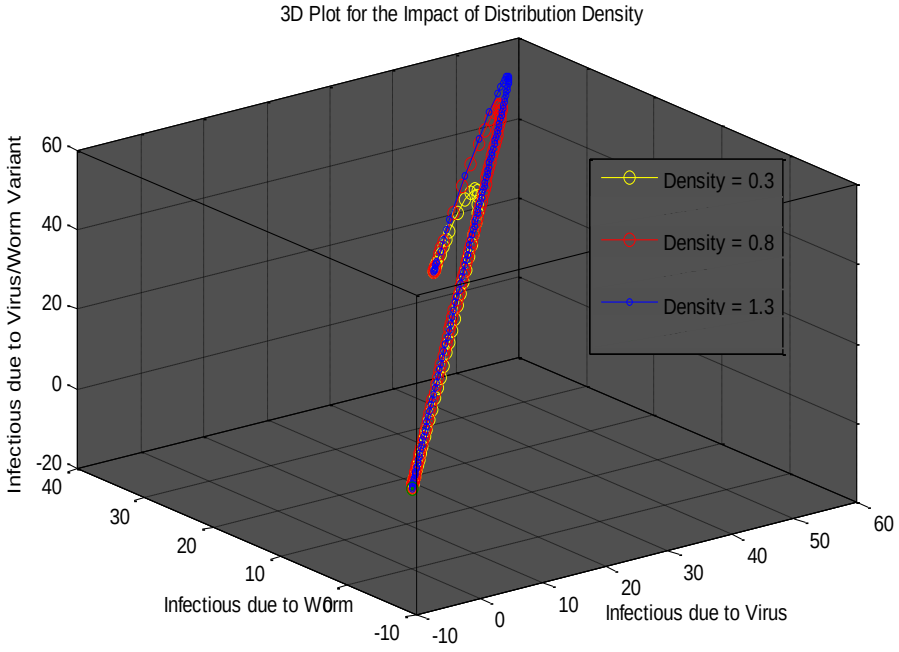

Figure 7. Dynamical Behaviour of the Infectious Class for showing the Impact of Distribution Density

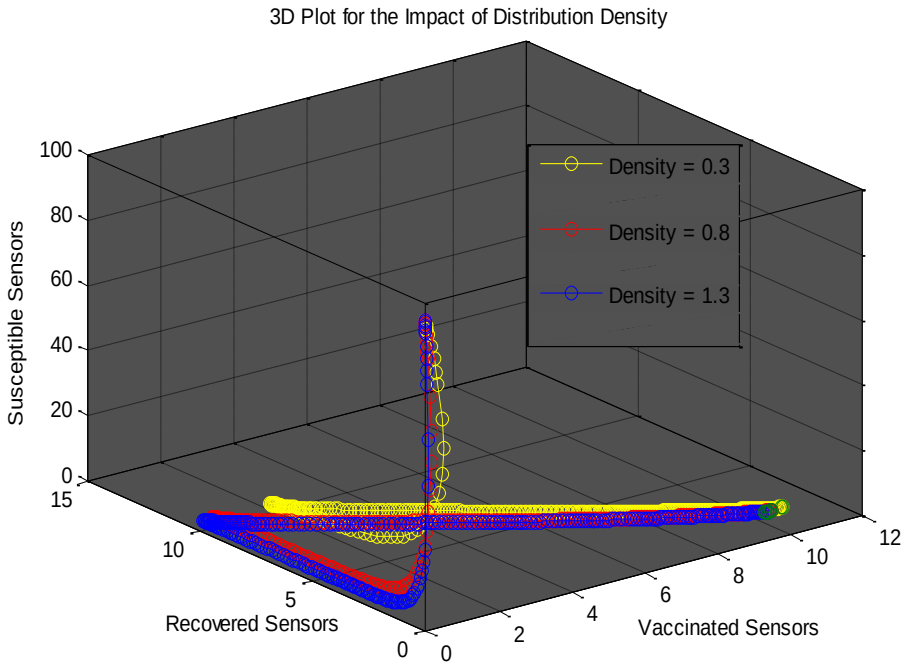

Figure 8. Dynamical Behaviour of the Susceptible, Recovered and Vaccinated for Various Distribution Densities

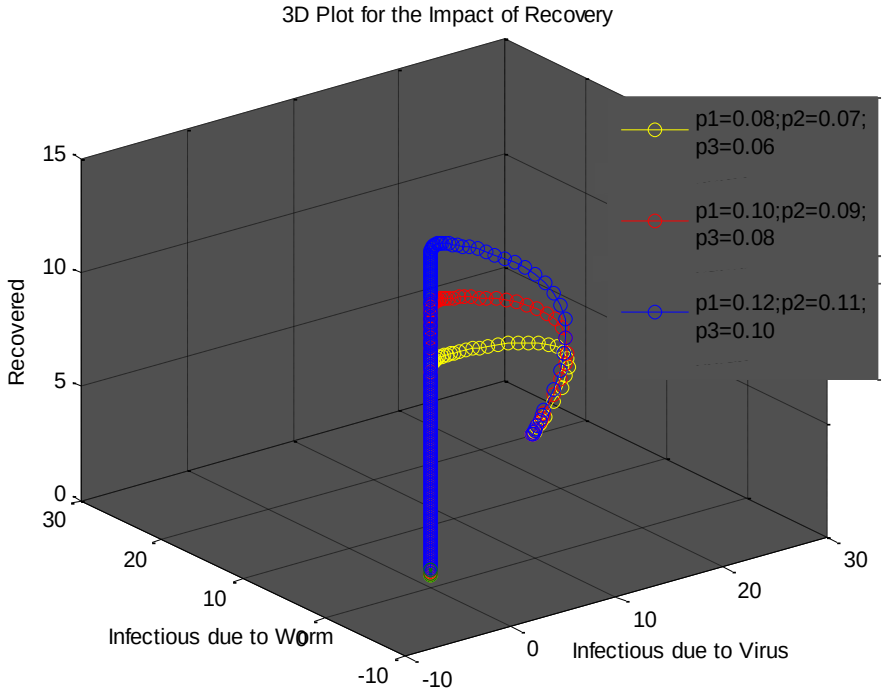

Figure 9. Dynamical Behaviour of the Infectious class and the Recovered Class

5. Conclusion and Future Directions

Motivated by multi-group modeling and analyses of diseases such as HIV and Gonorrhea in the Mathematical Biosciences as well as the strong possibility that both virus and worm attacks may plaque sensor networks (at a time), we developed the Susceptible, Infectious due to virus, Infectious due to worm, Infectious due to a virus/worm variant, Recovered and Susceptible with Vaccination (SI_jRS-V) model. This study is necessary since older epidemic models of wireless sensor network (WSN) mostly cater for one type of malicious code infection at a time. Aside generating solutions of the existent equilibriums, we derived the expression for the probability (P) of infectious nodes from the susceptible class and the resultant reproduction number (R_o) in a WSN case, when distinct transmission range and distribution density for each infection subgroup are considered in the multigroup model and when they are not. For each case, the actual R_o is the sum of the 'reproduction numbers' for each subgroup. The SI_jRS-V model was solved using the Runge-Kutta-Felhberg order 4 and 5 method – a suitable numerical method for initial value problems. Using simulation experiments where density was kept constant at 0.3 while range was varied for 1, 3, 10 and where range was kept constant at 2 while density was varied for 0.3, 0.8 and 1.3; we elicited the effects on the classes (susceptible, infectious (due to virus, worm, virus/worm variant), recovered and vaccination) involved in our study. Future work would address the addition of latency (exposed phase) and quarantining of sensor nodes using the multigroup models. In addition, we would investigate the division of the susceptible class into subgroups. Or the division of recovered of nodes into subgroups, this is to cater for the differential recovery of sensors.

References

[1] 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, no. 3, **(2012)**, pp. 357-362.
[2] C. H. Nwokoye, N. Mbeledogu, I. I. Umeh and I. A. Ejimofor, "Modeling the effect of Network Access Control and Sensor Random Distribution on Worm Propagation", International Journal of Modern Education and Computer Science., vol.9, no.11, **(2017)**, pp. 49-57.
[3] N. Keshri and B. K. Mishra, "Optimal Control Model for Attack of Worms in Wireless Sensor Network," International Journal of Grid Distribution Computing, vol 7, no. 3, **(2014)**, pp. 251-272.
[4] B. K. Mishra and D. K. Saini, "Mathematical Models on Computer Viruses", Applied Mathematics and Computation, vol. 187, **(2007)**, pp. 929–936.
[5] T. Richard and C. Mark, "Epidemiological Modelling of Peer-To-Peer Viruses and Pollution", Proceedings - IEEE INFOCOM, **(2006)**.
[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] L. Chunbo and J. Chunfu, "Modeling Passive Propagation of Malwares on the WWW", Physics Procedia, vol. 33, **(2012)**, pp. 271–278.
[8] Y. Yao, L. Guo, H. Guo, G. Yu, F. X. Gao and X. J. Tong, "Pulse Quarantine Strategy of Internet Worm Propagation: Modeling and Analysis", Computers and Electrical Engineering, vol. 38, **(2012)**, pp. 1047–1061.
[9] S. A. Khayam and H. Radha, "A Topologically-aware Worm Propagation Model for Wireless Sensor Networks", 25th IEEE International Conference on Distributed Computing Systems Workshops, **(2005)**, pp. 210–216.
[10] S. A. Khayam and H. Radha, "Using Signal Processing Techniques to Model Worm Propagation over Wireless Sensor Networks," IEEE Signal Processing Magazine, **(2006)**, pp. 164–169.
[11] P. De, Y. Liu and S. K. Das, "Modeling node compromise spread in wireless sensor networks using epidemic theory," International Symposium on on World of Wireless, Mobile and Multimedia Networks, **(2006)**, pp. 237–243.
[12] P. De, Y. Liu and S. K. Das, "An epidemic theoretic framework for evaluating broadcast protocols in wireless sensor networks", IEEE International Conference on Mobile Adhoc and Sensor Systems, **(2007)**, pp. 1–9.
[13] P. De, Y. Liu and S. K. Das, "2009 Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory", ACM Transactions on Sensor Networks (TOSN), vol. 5, **(2009)**, pp. 3-23.
[14] 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.
[15] X. Wang and Y, Li, "An Improved Sir Model for Analyzing the Dynamics of Worm Propagation in Wireless Sensor Networks," Chinese Journal of Electronics, vol. 18, **(2009)**.
[16] 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.
[17] S. Tang, "A Modified SI Epidemic Model for Combating Virus Spread in Wireless Sensor Networks", International Journal of Wireless Information Networks, vol. 18, **(2011)**, pp. 319–326.
[18] Y. Wang and X. Yang, "Virus Spreading in Wireless Sensor Networks with a Medium Access Control Mechanism", Chinese Physics B, vol. 22, **(2013)**, pp. 40200-40206.
[19] B. K. Mishra, S. K. Srivastava and 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.
[20] 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.
[21] 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, **(2014),** pp. 1–15.
[22] L. Feng, L. Song, Q. Zhao and H. Wang, "Modeling and stability analysis of worm propagation in wireless sensor network", Mathematical Problems in Engineering, **(2015)**.
[23] P. Driessche and J. Watmough, "Reproduction Numbers and Sub-Threshold Endemic Equilibria for Compartmental Models of Disease Transmission", Mathematical Biosciences, no. 180 **(2002)**, pp. 29–48.
[24] B. K. Mishra and G. M. Ansari, "Differential Epidemic Model of Virus and Worms in Computer Network", International Journal of Network Security, vol.14, no.3, **(2012)**, pp. 149-155.
[25] 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, no. 4, **(1990)**, pp. 365–382.

Authors

ChukwuNonso H. Nwokoye, he obtained a BSc degree in Computer Science. He is an ACM SIGCHI Gary Marsden Student Award recipient. His interests include simulation and modeling of complex systems, agent-based modeling, wireless sensor networks, network security, social computing and computer supported cooperative work (CSCW). He is currently on modeling and analysis of the propagation of malicious objects in network environments using analytical and agent-based modeling approaches.

Moses O. Onyesolu, he has Ph.D. (Virtual Reality), M.Sc. B.Sc. (Computer Science) from Nnamdi Azikiwe University, Nigeria where he works as a lecturer and researcher. His research interests are mainly in computer modeling and simulation, e-learning/virtual reality technologies, queuing system/theory and its applications. He has published widely in those areas. He is a member of the following learned societies: Nigerian Computer Society (NCS), Computer Professionals (Registration Council of Nigeria) (CPN), and International Association of Engineers (IAENG), International Association of Computer Science and Information Technology (IACSIT) and European Association for Programming Languages and Systems (EAPLS).