Towards Modeling Malicious Agents in Decentralized Wireless Sensor Networks: A Case of Vertical Worm Transmissions and Containment

ChukwuNonso H. Nwokoye
Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria.
E-mail: explode2kg@yahoo.com

Virginia E. Ejiofor, Moses O. Onyesolu, Boniface Ekechukwu
Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria.
E-mail: virguche2004@yahoo.com, mo.onyesolu@unizik.edu.ng, boni_eke@yahoo.com

Abstract—Now, it is unarguable that cyber threats arising from malicious codes such as worms possesses the ability to cause losses, damages and disruptions to industries that utilize ICT infrastructure for meaningful daily work. More so for wireless sensor networks (WSN) which thrive on open air communications. As a result epidemic models are used to study propagation patterns of these malicious codes, although they favor horizontal transmissions. Specifically, the literature dealing with the analysis of worms that are both vertically and horizontally (transmitted) is not extensive. Therefore, we propose the Vulnerable–Latent–Breaking Out–Temporarily Immune–Inoculation (VLBTV-I) epidemic model to investigate both horizontal and vertical worm transmission in wireless sensor networks. We derived the solutions of the equilibriums as well as the epidemic threshold for two topological expressions (gleaned from literature). Furthermore, we employed the Runge-Kutta-Fehlberg order 4 and 5 method to solve, simulate and validate our proposed models. Critically, we analyzed the impact of both vertical and horizontal transmissions on the latent and breaking out compartments using several simulations experiments.

Index Terms—Epidemic model, Wireless sensor network, Worm, Vertical Transmission.

I. INTRODUCTION

The advent of Internet of Things (IoTs) has in recent times given rise to a different dimension to prevalent communication technologies, linking things such as mobile phones, web TVs/radios, sensors, the www and other cloud services. IoTs which are web-like structures of unique objects and their virtual representations can also include objects such as "large buildings, industrial plants, planes, cars, machines, any kind of goods, specific parts of a larger system to human beings, animals and plants and even specific body parts of them" [1].

However, Wireless sensor networks (WSNs) to an extent essentially underpin the IoTs paradigm or according to Yinibiao, Lee and Lancot [1], the idea of IoTs was developed in parallel to WSNs. Therefore, the flourishing research-based engrossment in IoT can be leveraged by its integration to low battery-power sensors, processors, smart wireless network and big data analytics. As Weiss and Yu puts it, the "…combination of (these) technologies enables a multitude of sensors to be put *anywhere*: not just where communications and power infrastructure exists, but anywhere valuable information is gleaned regarding the how, where, or what of a given *thing*" [2]. To buttress the above assertion, Zhan et al. [3] called WSN, "one of the key enablers of iThings". The idea of implanting several "things" such as machines, pipelines with `goal-oriented sensors which have sensing and computational capabilities is to provide both qualitative and quantitative information-oriented edge in various WSN applications found in industries.

The sensors are distributed in a geographical area where they collect data and route it back to the sink which is connected to the server and to the internet (of things) [4]. It is widely known that the industrial environment present an unfriendly deployment area for sensor activities which also strictly demands high integrity of data and information. This implies that, "any message received is confirmed to be exactly the message that was sent, without additions, deletions, or modifications of the content. Ensuring data integrity consequently enhances "efficiency, productivity and safety of industrial plants" [2].

Integrating WSN and other constituents of IoTs has the advantage of moving beyond remote access to commonly collecting and sharing heterogeneous data and information. Piyare and Lee [5] developed an

Towards Modeling Malicious Agents in Decentralized Wireless Sensor Networks:
A Case of Vertical Worm Transmissions and Containment

13

architecture based on Representational State Transfer (REST) web services for remote monitoring. Considering the unreliable nature of WSN, Ross and Watteyne [6] proposed the creation of IP-enabled sensors to makes low-power sensors accessible as web servers. They feel that with easy accessibility to sensors industries/businesses can achieve wide scale deployment and feeding of real-world information to IoTs.

On the other hand, this easy access gives way to security attacks. Securing data and information is essential to Industrial Wireless Sensor Networks (WSN). Primarily, WSN security goals include Confidentiality, Integrity and Authenticity (CIA), therefore "security is one of the most important research issues on WSNs for iThings" [3]. Attacks from malicious codes such as worms and viruses can distort the CIA measures of neighboring nodes thereby causing significant losses or damages. There is need to ensure that data and information survive the harsh terrains of the industrial operational environment without distortions (or attacks) from malicious codes such as worms. The emergence of the Cabir virus (that propagate over the air) and the Mabir worm (that employ scanning approaches for proximity attacks)[4], has kept the network community interested in developing better defense structures against malicious codes.

II. RELATED WORKS

This section presents an overview of the pertinent literature that underpins our study herein. Firstly, is epidemic theory and the rationale for its application to telecommunication networks such as WSN. Thereafter, we reviewed epidemic models of wireless sensor networks.

A. Epidemic Theory

The major objective of epidemic theory or epidemiology is to investigate the infective results of vulnerable population with respect to the disease; considering agent, host and the environment [7]. Of great interest are the interactions between these factors. Specifically, several variations exist between the host and the agent; and even more are the ways in which variations in the environment influence host-agent interactions.

The SIR model developed by Kermack and Mckendrick [8, 9, 10] initiated the journey to modeling epidemics in networks. In telecommunication networks, researchers have identified similarities between the spread of viral disease in biological networks and the propagation of malicious codes in telecommunication networks. This spurred the modification of the SIR model so as to cater for issues computer, peer-to-peer and other wireless network.

Motivated by epidemic theory, we study the vertical transmission of worms in WSN in the light of the topology of sensor distribution and the transmission range. It was discovered that the "literature dealing with the analysis of worms that are both vertically and horizontally (transmitted) is not extensive"[11]. Most epidemiological models focus on horizontal transmission where the infection is spread through contact between the susceptible and the infectious hosts[12]. Li, et al. [12] employed the parameters for vertical transmission for the global dynamical analysis of disease models and [11] extended it to computer networks where the worm infection is seen to pass from the main server to any node using the Susceptible-Exposed-Infectious-Recovered (SEIR) model. There exists other works that investigated the vertical transmission in computer networks using the Susceptible-Latent-Breaking Out-Susceptible (SLBS) [13] and the Susceptible-Latent-Breaking Out-Removed-Susceptible (SLBRS) [14]. To the best of our knowledge it has not been applied for the study of worm dynamics in WSNs.

B. WSN Epidemic Models

With emphasis on network topology, Khayam and Radha [15] developed a topologically-aware worm propagation model (TWPM), to help in defending against malicious worms and provide an effective vehicle to disseminate necessary information to secure the network considering physical, MAC, network, and transport layer parameters. By incorporating factors such as node density and the pairwise key scheme, De, Liu and Das [16] proposed an epidemiological model to investigate the probability of a infection breakout, the sizes of the affected components; and performed analysis on two specific types of node deployment scenarios, namely uniform random deployment and group based deployment of nodes. A general framework based on the principles of epidemic theory was proposed by De, Liu and Das [17] for vulnerability analysis of the propagation rate (speed) and the extent of spread (reachability) of a malware in current broadcast protocols in wireless sensor networks. Tang and Mark [7] modified the SIR model by introducing a maintenance mechanism (SIR-M) in the sleep nodes of the WSN, which can improve the network's anti-virus capability and enable the network to adapt flexibly to different types of viruses, without incurring additional computational or signaling overhead.

Wang, Li and Li [18] proposed a model for the sleep and work interleaving schedule policy for sensor nodes and describes the process of multi-worm propagation in WSNs. Considering the influence of the medium access control (MAC) mechanism on virus and using the mean-field theory, Wang and Yang [19] proposed an extended version of standard SI model to show that the MAC mechanism obviously reduces the density of infected nodes in the networks. In the light of worm emergence in networks, Mishra and Keshri [4] proposed a SEIRS-V model, Mishra, Mishra and Srivastava [20] proposed a SIQR model and Mishra and Tyagi [21] proposed the SEIQRS-V model to investigate the dynamics worm propagation with respect to time in WSN. Zhang and Si [22] modified the SEIRS- V by introducing the concept of delay which they used to study the existence of Hopf bifurcation and Feng et al. [23] modified the SIR model with the different expression (from the expression in [7, 19]) for distribution density

and transmission range. Nwokoye et al. [24] proposed the pre-quarantine concept using the SEIR-V epidemic model for computer and the wireless sensor networks.

Though some models mentioned above (with the exception of Mishra and Keshri [4], Mishra and Tyagi [21], Zhang and Si [22], Nwokoye et al. [24]) considered topology or sensor distribution none of the reviewed works considered the dynamics of vertical transmission in WSN.
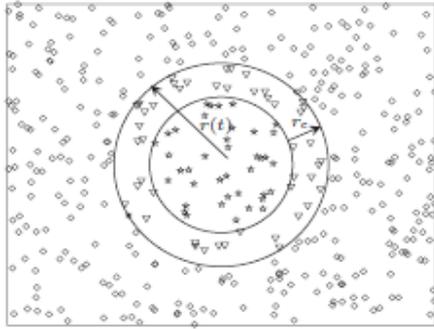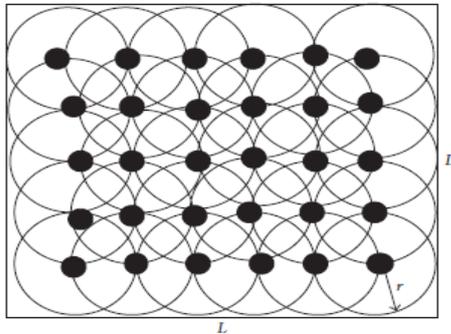

Fig.1. WSN Topology 1 [7,19]

Fig.2. WSN Topology 2 [23]

III. THE SEIR-V MODEL WITH VERTICAL TRANSMISSION

Here, we propose the Vulnerable–Latent–Breaking Out–Temporarily Immune–Vulnerable with an Inoculation compartment (*VLBTV-I*) epidemic model. Specifically, we apply the Tang and Mark[7]'s and Feng et al. [23]'s expression for uniform random distribution of sensor nodes as well as Mishra and Pandey [11]'s expression for vertical transmission. Essentially, Vulnerable (*V*) sensors are susceptible to new infections and has no immunity, Latent (*L*) sensors are exposed to worm infection, Breaking out (*B*) sensors are infected and infectious, Temporarily immune (*T*) sensors have recovered from a worm infection and Inoculated (*I*) sensors are vaccinated against worm infection. The model investigates both horizontal and vertical worm transmission in a wireless sensor networks. Let *V(t)*, *L(t)*, *B(t)*, *T(t)*, *I(t)* denote the numbers of sensors at time *t*.

Li et al. assumed, "that a fraction of the offsprings of infected hosts (both *L* and *B*) are infected at birth and, like adult infected hosts, will stay latent before becoming infectious, and hence the infected birth flux will enter the

L class". Consequently, Mishra and Pandey [11] assumes that, "the birth flux into the exposed class is given by $pbE + qbI$ and the birth flux into the susceptible class is given by $b - pbE - qbI$". This implies that a fraction p and a fraction q of the new nodes from the exposed and the infectious classes, respectively, are introduced into the exposed class. We adopt these assumptions too in the light of communication range and density; in our case herein the birth flux into the Latent (exposed) compartment is $p\lambda L + q\lambda B$ and the birth flux into the Vulnerable compartment is $\lambda - p\lambda L - q\lambda$. Table 1 presents the meanings and names of several parameters employed for our WSN model formulation.

Table 1. WSN Parameters and Their Meaning

| Parameters	Name	Meaning
p	p	Fraction of new nodes from the latent compartment
q	q	Fraction of new nodes from the breaking out compartment
$\lambda - p\lambda L - q\lambda B$	-	Birth flux in the Vulnerable compartment
$p\lambda L + q\lambda B$	-	Birth flux in the Exposed compartment
λ	lambda	Recruitment rate of vulnerable nodes to the sensor network
σ	sigma	Distribution density
r_0^2	r	Transmission range
L^2	-	Length of side
σr_0^2	-	Effective contact with an infected node for transfer of infection (Topology 1)
$\sigma \pi r_0{}^2 / L^2$	-	Effective contact with an infected node for transfer of infection (Topology 2)
β	beta	Infectivity contact rate
τ	tau	Death rate of nodes due to hardware or software failure
ω	omega	Crashing rate due to attack of malicious codes (in this case worm)
θ	theta	Rate at which latent nodes enter the breaking out compartment
ν	nu	Rate at which infected nodes become temporarily immune
φ	phi	Rate at which temporarily immune nodes become vulnerable
ρ	rho	Rate of inoculation for vulnerable sensor nodes
ξ	zeta	Rate of transmission from the inoculation compartment to the vulnerable compartment

Topology 1
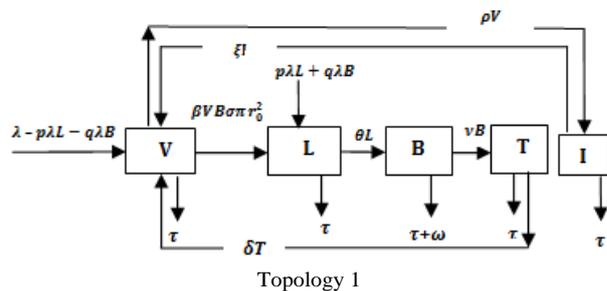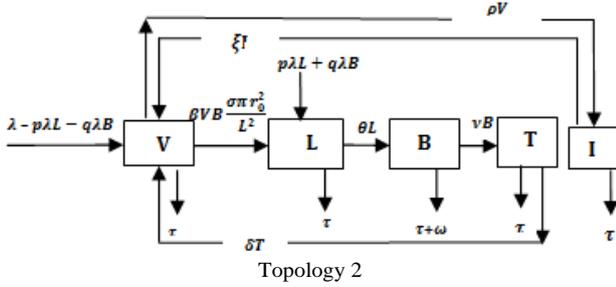
Topology 2

Fig.3. Schematic diagram of Topologies ((1) and (2)) for Wireless Sensor Networks

The schematic diagram for the dynamical vertical and horizontal transmission of worms in a WSN given our assumption is depicted as Fig. 1. The system of differential equation (1) is adapted from Mishra and Keshri [4] but modified to capture distribution density, transmission range and vertical transmission.

The VLBTV-I Model 1 for topology 1 is represented using the following system of differential equations;

$$
\begin{aligned}
\dot{V} &= \lambda - \beta VB\sigma\pi r_0{}^2 - p\lambda L - q\lambda B - (\tau + \rho)V + \delta T + \xi I \\
\dot{L} &= \beta VB\sigma\pi r_0{}^2 + p\lambda L + q\lambda B - (\tau + \theta)L \\
\dot{B} &= \theta L - (\tau + \omega + \nu)B \\
\dot{T} &= \nu B - (\tau + \delta)T \\
\dot{I} &= \rho V - (\tau + \xi)I
\end{aligned}
\tag{1}
$$

The VLBTV-I Model 2 for topology 2 is represented using the following system of differential equations;

$$
\begin{aligned}
\dot{V} &= \lambda - \frac{\beta VB\sigma\pi r_0{}^2}{L^2} - p\lambda L - q\lambda B - (\tau + \rho)V + \delta T + \xi I \\
\dot{L} &= \beta VB\sigma\pi r_0{}^2 / L^2 + p\lambda L + q\lambda B - (\tau + \theta)L \\
\dot{B} &= \theta L - (\tau + \omega + \nu)B \\
\dot{T} &= \nu B - (\tau + \delta)T \\
\dot{I} &= \rho V - (\tau + \xi)I
\end{aligned}
\tag{2}
$$

A. Solutions of Equilibrium Points

We equate the modified system of differential equations (1) to zero to obtain two solutions which are the Worm-free equilibrium and the Endemic equilibrium points i.e. $\dot{V} = 0$; $\dot{L} = 0$; $\dot{B} = 0$; $\dot{T} = 0$; $\dot{I} = 0$. The Worm-free equilibrium describes the absence of worms while the Endemic equilibrium describes the presence of worms in the Wireless Sensor Network using formulated mathematical model.

For both topologies (i.e. Model 1 and Model 2); the solutions of Worm-free equilibrium $W_0^F = (V_0^*, L_0^*, B_0^*, T_0^*, I_0^*)$ i.e.

$$
V_0^* = \frac{\lambda(\xi+\tau)}{\tau(\xi+\rho+\tau)}, \; L_0^* = 0; \; B_0^* = 0; T_0^* = 0, I_0^* = \frac{\lambda\rho}{\tau(\xi+\rho+\tau)}
\tag{3}
$$

Topology 1: Endemic equilibrium $E_1^E = (V_1^*, L_1^*, B_1^*, T_1^*, I_1^*)$ i.e.

$$
V_1^* = \frac{((\theta-p\lambda+\tau)(\nu+\tau+\omega)-q\theta\lambda)}{\beta\theta\sigma\pi r_0^2}
$$

$$
L_1^* = \frac{(\delta+\tau)(\nu+\tau+\omega)(\lambda - V_1^*\frac{\tau(\xi+\rho+\tau)}{(\xi+\tau)})}{\delta\tau(\theta+\nu+\tau)+\delta(\theta+\tau)\omega+\tau(\theta+\tau)(\nu+\tau+\omega)}
$$

$$
B_1^* = \frac{(\delta+\tau)(\theta\lambda - \frac{\tau(\xi+\rho+\tau)((\theta-p\lambda+\tau)(\nu+\tau+\omega)-q\theta\lambda)}{\beta(\xi+\tau)\sigma\pi r_0^2})}{\delta\tau(\theta+\nu+\tau)+\delta(\theta+\tau)\omega+\tau(\theta+\tau)(\nu+\tau+\omega)}
\tag{4}
$$

$$
T_1^* = \frac{\nu(\theta\lambda - \frac{\tau(\xi+\rho+\tau)((\theta-p\lambda+\tau)(\nu+\tau+\omega)-q\theta\lambda)}{\beta(\xi+\tau)\sigma\pi r_0^2})}{\delta\tau(\theta+\nu+\tau)+\delta(\theta+\tau)\omega+\tau(\theta+\tau)(\nu+\tau+\omega)}
$$

$$
I_1^* = \frac{\rho((\theta-p\lambda+\tau)(\nu+\tau+\omega)-q\theta\lambda)}{\beta\theta(\xi+\tau)\sigma\pi r_0^2}
$$

Topology 2: Endemic equilibrium $E_1^E = (V_1^*, L_1^*, B_1^*, T_1^*, I_1^*)$ i.e.

$$
V_1^* = \frac{L^2((\theta-p\lambda+\tau)(\nu+\tau+\omega)-q\theta\lambda)}{\beta\theta\sigma\pi r_0^2}
$$

$$
L_1^* = \frac{(\delta+\tau)(\nu+\tau+\omega)(\lambda - V_1^*\frac{\tau(\xi+\rho+\tau)}{(\xi+\tau)})}{\tau(\theta+\tau)(\nu+\tau+\omega)-\delta(\theta(\tau+\omega)+\tau(\nu+\tau+\omega))}
$$

$$
B_1^* = \frac{\theta(-\delta-\tau)(-\nu-\tau-\omega)(\lambda - V_1^*\frac{\tau(\xi+\rho+\tau)}{(\xi+\tau)})}{(\nu+\tau+\omega)(\delta\tau(\theta+\nu+\tau)+\delta(\theta+\tau)\omega+\tau(\theta+\tau)(\nu+\tau+\omega))}
\tag{5}
$$

$$
T_1^* = \frac{\nu(L^2\tau(\xi+\rho+\tau)(-q\theta\lambda+(\theta-p\lambda+\tau)(\nu+\tau+\omega))-\beta\theta\lambda(\xi+\tau)\sigma\pi r_0^2)}{\beta(\xi+\tau)(\delta\tau(\theta+\nu+\tau)+\delta(\theta+\tau)\omega+\tau(\theta+\tau)(\nu+\tau+\omega))\sigma\pi r_0^2}
$$

$$
I_1^* = \frac{L^2\rho((\theta-p\lambda+\tau)(\nu+\tau+\omega)-q\theta\lambda)}{\beta\theta(\xi+\tau)\sigma\pi r_0^2}
$$

B. Epidemic Threshold

The epidemic threshold can also be referred to as the Reproduction number denoted as R_O. The reproduction number is defined as "the expected number of secondary cases produced in a completely susceptible population, by a typical infective individual"[25]. Using the method that was used in Mishra and Pandey, [11], which regarded the Reproduction number as the inverse of the susceptible nodes (S_1^*) at the endemic equilibrium; our Reproduction numbers here are;

Topology 1: $R_O = \frac{\beta\theta\sigma\pi r_0^2}{((\theta-p\lambda+\tau)(\nu+\tau+\omega)-q\theta\lambda)}$

Topology 2: $R_O = \frac{\beta\theta\sigma\pi r_0^2}{L^2((\theta-p\lambda+\tau)(\nu+\tau+\omega)-q\theta\lambda)}$

In Mishra and Pandey [11], the reproduction number depends on the rate of the transmission from the exposed (latent) to the infectious (breaking out) class, the rate of the transmission from the infectious to the recovered class, the deaths as a result of the worm infections and other causes, the fraction of the exposed and infectious introduced into the exposed class. So is our reproduction number, but with the addition of the parameters for communication range and density. Note that the reproduction number of topology 2 involves L which denotes the length of side.

C. Stability of the Worm-free Equilibrium Point

We show the proof of local asymptotic stability at the Worm-free Equilibrium using the jacobian method. This is done by showing that "the eigen-values of the jacobian matrix all have negative real parts" [4] or that the "characteristic equation of the jacobian matrix" derived from the system of equations has negative roots [26].

Theorem 1: The worm-free equilibrium (for topology 1)

is locally asymptotically stable if $R_O < 1$ and unstable if $R_O > 1$.

The Jacobian matrix at worm free equilibrium point W_0^F for topology 1 is;

$$J = \begin{pmatrix} -\beta B\sigma\pi r_0{}^2 - (\tau+\rho) & -p\lambda & -\beta V\sigma\pi r_0{}^2 - q\lambda & \delta & \xi \\ \beta B\sigma\pi r_0{}^2 & -(\tau+\theta)+p\lambda & \beta V\sigma\pi r_0{}^2 + q\lambda & 0 & 0 \\ 0 & \theta & -(\tau+w+\nu) & 0 & 0 \\ 0 & 0 & \nu & -(\tau+\delta) & 0 \\ \rho & 0 & 0 & 0 & -(\tau+\xi) \end{pmatrix} \quad (6)$$

$$J(W_0^F) = \begin{pmatrix} -(\tau+\rho) & -p\lambda & \frac{-\beta\sigma\pi r_0{}^2\lambda(\xi+\tau)}{\tau(\xi+\tau)} - q\lambda & \delta & \xi \\ 0 & -(\tau+\theta)+p\lambda & \frac{\beta\sigma\pi r_0{}^2\lambda(\xi+\tau)}{\tau(\xi+\tau)} + q\lambda & 0 & 0 \\ 0 & \theta & -(\tau+w+\nu) & 0 & 0 \\ 0 & 0 & \nu & -(\tau+\delta) & 0 \\ \rho & 0 & 0 & 0 & -(\tau+\xi) \end{pmatrix} \quad (7)$$

Theorem 2: The worm-free equilibrium (for topology 1) is locally asymptotically stable if $R_O < 1$ and unstable if $R_O > 1$. The Jacobian matrix at worm free equilibrium point W_0^F for topology 2 is

$$J = \begin{pmatrix} -\beta B\sigma\pi r_0{}^2 - (\tau+\rho) & -p\lambda & -\beta V\sigma\pi r_0{}^2/L^2 - q\lambda & \delta & \xi \\ \beta B\sigma\pi r_0{}^2 & -(\tau+\theta)+p\lambda & \beta V\sigma\pi r_0{}^2/L^2 + q\lambda & 0 & 0 \\ 0 & \theta & -(\tau+w+\nu) & 0 & 0 \\ 0 & 0 & \nu & -(\tau+\delta) & 0 \\ \rho & 0 & 0 & 0 & -(\tau+\xi) \end{pmatrix} \quad (8)$$

$$J(W_0^F) = \begin{pmatrix} -(\tau+\rho) & -p\lambda & \frac{-\beta\sigma\pi r_0{}^2\lambda(\xi+\tau)}{L^2\tau(\xi+\tau)} - q\lambda & \delta & \xi \\ 0 & -(\tau+\theta)+p\lambda & \frac{\beta\sigma\pi r_0{}^2\lambda(\xi+\tau)}{L^2\tau(\xi+\tau)} + q\lambda & 0 & 0 \\ 0 & \theta & -(\tau+w+\nu) & 0 & 0 \\ 0 & 0 & \nu & -(\tau+\delta) & 0 \\ \rho & 0 & 0 & 0 & -(\tau+\xi) \end{pmatrix} \quad (9)$$

Eigenvalues of (7) and (9) for both topologies are: $-(\tau+\rho), -(\tau+\theta)+p\lambda, -(\tau+w+\nu),$ $-(\tau+\delta),$ $-(\tau+\xi)$ which all are negative; hence the system is locally asymptotically stable at worm free equilibrium point W_0^F.

lambda=1.2; tau=0.2; beta=1.3; phi=0.8; theta=0.4; nu=0.6; omega=0.3; delta=0.8; p=0.1; q=0.1; rho=0.1; xi = 0.1; adapted and modified from [11].

A. Numerical Simulation Results for Topology 1

IV. NUMERICAL RESULTS AND DISCUSSION

The systems of differential equation ((1) and (2)) was solved using a numerical method i.e. Runge-Kutta Fehlberg method of order 4 and 5. This numerical method was used because it has been found suitable for a wide variety of initial value problems in practical applications. Subsequently we performed simulation experiments using the following initial values for the Wireless Sensor network: V=100; L=3; B=1; T=0; I=0. For the simulation experiments, we performed model alignment i.e. our model was docked to match (and compare our results with) the WSN model results in [4] and [27]. Summarily, Vulnerable, Latent, Breaking out, Temporarily immune, Inoculated in our model imply Susceptible, Exposed, Infectious, Recovered and Vaccinated respectively in [4,27]. Other simulation values include sigma=0.3; r=1;

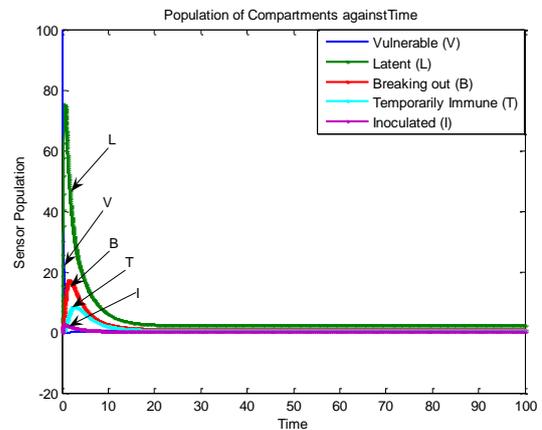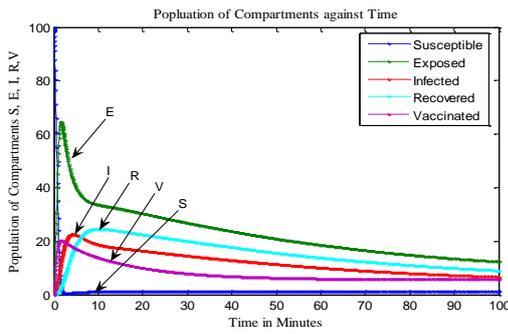Fig.4. Sensor Population against Time at p= q=0.1
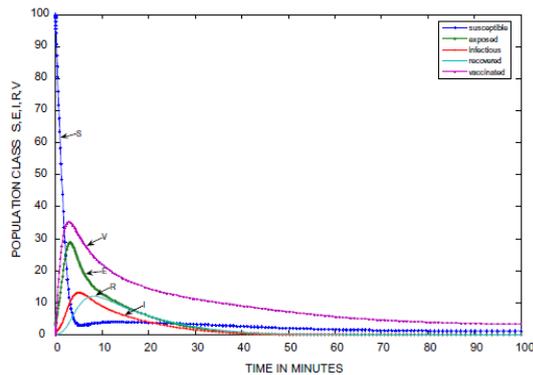
Fig.5. Sensor Population against Time [16]

Fig.6. Sensor Population against Time [12]

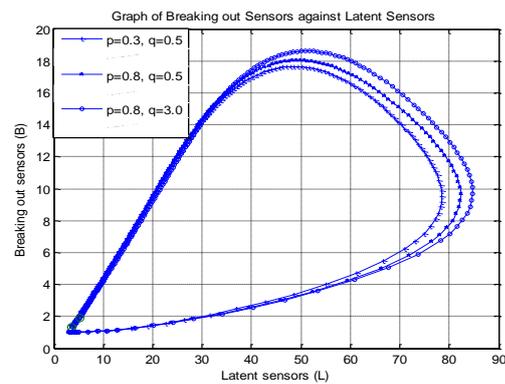Fig7. Breaking out vs Latent at $\lambda = 1.2$

Fig. 4, Fig. 5 and Fig. 6 are the time histories for our model herein and the WSN models in [27] and [4], respectively. A cursory look at the figures shows several differences. They include the almost disappearance of vulnerable nodes in our model. Then, the increase in the number of latent (exposed) sensor nodes in our model compared to responses from other models. Note that the increase in density and range increased the exposed nodes in both our study and in [27]; since the model in [4] doesn't entirely depict a wireless sensor network.

Keeping p constant (at 0.8) and keeping q constant (at 0.5) depicts the effect of vertical worm transmission in Fig. 7. This figure shows that increasing the fraction of latent nodes (p) and the fraction of breaking out nodes (q) introduced into the breaking out compartment (B) increased both B and latent (L) compartments. Note that λ

(which is the recruitment rate of susceptible nodes to the sensor network) was kept constant at 1.2, all through the simulation in Fig. 7. Additionally, the infectivity contact rate or the effective contact rate (which results in horizontal worm transmission) was kept constant was also constant throughout the simulation in Fig. 7.

In Fig. 8 we kept p and q constant so as to elicit the actual effect of new sensor nodes added to the sensor network. This is because the relation (i.e. $p\lambda L + q\lambda B$) that represents vertical worm transmission involves sensor node inclusion into the network. The inoculated (I) compartment in our model decreased greatly; however, Fig. 9 was plotted in a three dimensional form to show the effects of vertical worm transmission on the breaking out and the inoculated nodes.
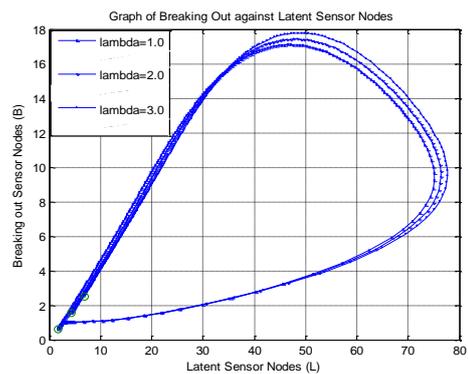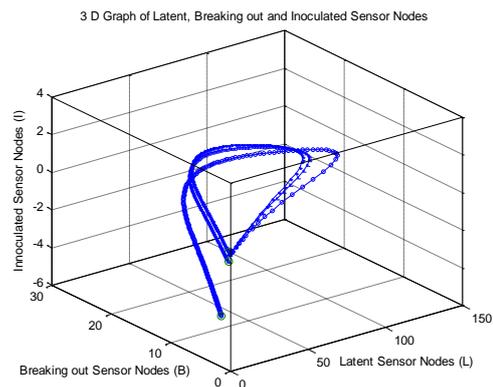

Fig.8. Breaking out vs Latent at p=0.1 and q=0.1

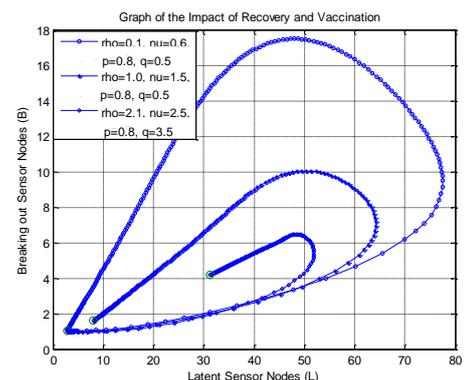Fig.9. 3D Phase Plane showing *L*, B and *I* sensor nodes

Fig.10. Breaking out vs Latent Sensor Nodes

Fig. 10 depicts the impact of increasing both the rate at which nodes become temporarily immune to worm infection and the rate of inoculation. From the diagram, it is evident that the rate of infectiveness (or break out) for both the latent/breaking out sensor nodes reduced to 62/7 from a high value of 75/18. Correspondingly, the rate of sensor inoculation was increased (in Fig. 11) from below 10 to almost 40 as a result.
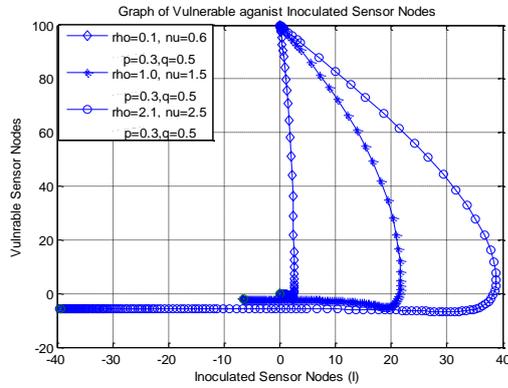

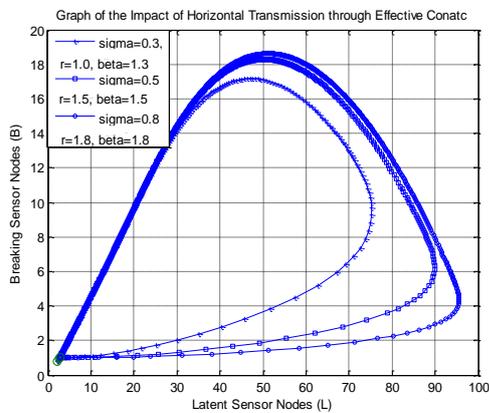Fig.11. Vulnerable vs Inoculated Sensor Nodes
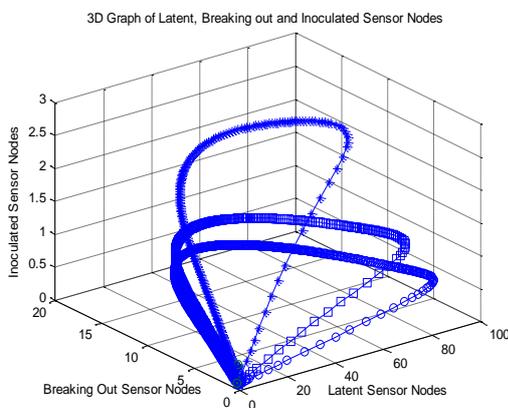

Fig.12. Breaking out vs Latent Sensor Nodes

Fig.13. 3D Phase Plane showing *L, B* and *I* Sensor Nodes

Fig. 12 and Fig. 13 were used to depict the impact of horizontal transmission (by increasing the parameters that form the effective contact rate i.e. $\sigma \pi r_0^2$) in Model 1.

While Fig. 12 shows the relationship between latent and the breaking out sensor nodes using a two dimensional graph, Fig. 13 shows the relationship between latent, breaking out and the inoculated sensor nodes using a three dimensional phase plane. Summarily, the two plots showed how horizontal worm transmission in Model 1 increases infectiousness.

B. Numerical Simulation Results for Topology 2

The two proposed models herein are mostly the same, if not for the addition of length of side (L^2) in the topological expression in [23]. There is the implicit (and accurate) assumption that the above simulation results of Model 1 would be "*almost*" the same with the results of Model 2, if simulated with the same values. Therefore, we perform simulation experiments in order to elicit the impact/effect of the length of side, existent in Model 2.
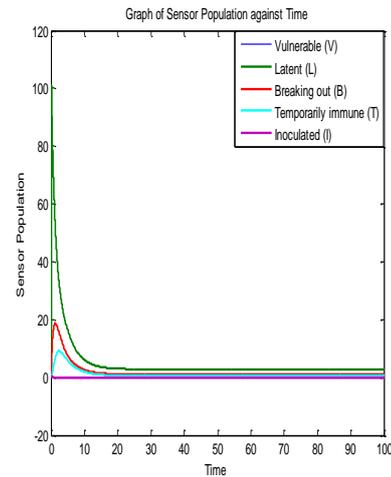

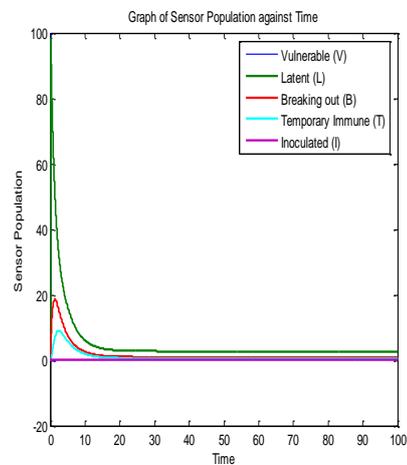Fig.14. Sensor Population against Time at *L*=0.1

Fig.15. Sensor Population against Time at *L*=0.2

Fig. 4 and Fig. 14 are almost the same; only that the inoculated nodes became zero and the vulnerable nodes disappeared in the latter; so is Fig. 15. The three figures were simulated with the same values except for the addition of L^2=0.1 in Fig. 14 and L^2=0.2 in Fig. 15. Fig. 16 depicts a three dimensional plot of the dynamical

relationship/behavior of latent, breaking out and inoculated sensor nodes. It also shows the corresponding decrease in the inoculated nodes. The effect of the length of side (L^2) is clear if one compares the 3D phase plane of Model 1 (Fig. 13) and that of Model 2 (Fig. 16). Recall that L^2 is part of the parameters that constitute the effective contact rate in Table 1. The effect of increasing the factors of vertical transmission and L^2 is evident if one compares Fig. 16 and Fig. 17.
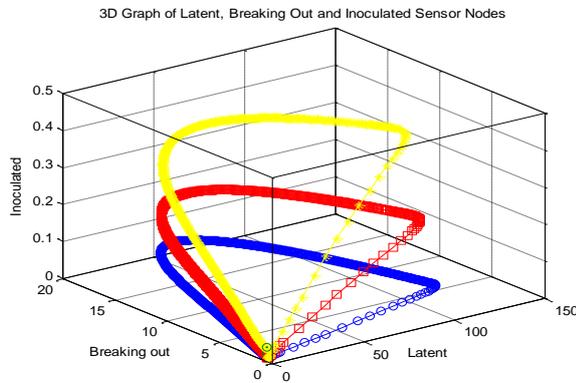

Fig.16. 3D Phase Plane showing *L, B* and *I* sensor nodes at L^2=0.1, 0.2, 0.3; p=0.1 and q=0.1
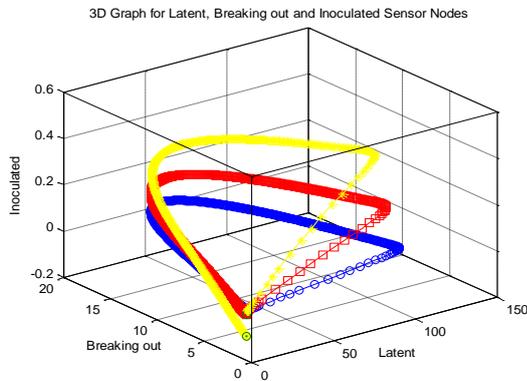

Fig.17. 3D Phase Plane showing *L, B* and *I* sensor nodes at L^2=0.1, 0.2, 0.3; *p*=0.3, 0.8, 0.8 and *q*=0.5, 0.5, 3.5

C. Analysis Using the Epidemic Threshold

Here, we present the actual values for the epidemic threshold (reproduction ratios) derived at Section III using the time histories of Model 1 (Fig. 4), Model in [27] (Fig. 5), Model in [4] (Fig. 6) and Model 2 (Fig. 15). Table 2 presents the reproduction numbers for the time histories of the study herein. This would further display the impact of vertical worm transmissions in the wireless sensor network.

Going by the fact that at $R_O < 1$ the infection is contained and at $R_O \geq 1$ the infection spreads and there is an epidemic; Table 2 displays interesting results. Note that the rationale for comparing our study herein and the models in [4] and [27] is because they all involved the SEIR-V epidemic model. Table 2 shows that Fig. 6 of [4] has the lowest reproduction number; this is because it is unlike Fig. 4 and Fig. 15

that involved range, density and vertical transmission. The impact of characterizing range and density without vertical transmission is expressly shown in the difference between Fig. 4 and Fig. 5 or the difference between Fig. 5 and Fig. 15. The table also shows that vertical transmission for both topologies made R_O to rise above 1. Furthermore, the reproduction number for topology 2 i.e. Fig. 15 significantly rose beyond 1 to 25.529. To prevent epidemic, network managers should strive to keep the reproduction numbers below 1.

Table 2. Time Histories and their Reproduction Numbers

Figures	Parameters Considered	Reproduction numbers
Fig. 4.	Vertical transmission, Range and Density (topology 1)	1.021
Fig. 5. [27]	Range and Density (topology 1)	0.788
Fig. 6. [4]	---	0.209
Fig. 15.	Vertical transmission, Range and Density (topology 2)	25.529

V. CONCLUSION AND FUTURE DIRECTIONS

In this study, we characterized and investigated both vertical and horizontal transmission of worms using two epidemic WSN models. These two epidemic models represented the topological expressions for uniform random sensor distribution, and are culled from [7, 19] and [23]. Vertical and horizontal worm transmissions are studied alongside these expressions. Thereafter, a suitable numerical method for an initial value problem was chosen to solve, simulate and validate these proposed models.

WSN characterization using two topologies culled from literature was necessary because it aided the derivation of novel reproduction numbers. Note that the WSN models that underpin this study presented reproduction numbers that characterize only horizontal worm transmission. However, the reproduction numbers (of our study), which differ from (those in) underpinning works depicts the resulting secondary infections when vertical transmission, communication range and distribution density are put into consideration.

Vertical worm transmissions increased the latent and the breaking out sensor nodes by the introduction of new births, so was horizontal worm transmissions. However, the negative impact of these worm transmissions was significantly reduced by increasing correspondingly the rate of temporary immunity and the rate of sensor inoculation. Noteworthy is the fact that temporary immunity achieved by increasing v (nu) quickly becomes of no effect due to the existence of another worm variant or another malicious code type.

In furtherance, we would check the effect of vertical transmission on other network countermeasures such as quarantine, network access control etc. Additionally, we would explore the possibilities of using a different

modeling approach such as agent modeling (ABM) in order to represent and analyze the import of other instances of stochasticity and heterogeneity in wireless sensor networks.

REFERENCES

[1]   P. Yinbiao, S. Lee and K. Lanctot, "*Internet of Things : Wireless Sensor Networks,"* 2014.

[2]   R. Weiss and J Yu, "*Electronic design: Wireless sensor networking for the industrial IOT*", 2015. doi.org/http://electronicdesign.com/print/iot/wireless-sensor-networking-industrial.

[3]   Y. Zhan, L. Liu, L. Wang, and Y. Shen. 2013. Wireless Sensor Networks for the Internet of Things. *International Journal of Distributed Sensor Networks* 2013: pp. 2-11, 2013. doi.org/http://dx.doi.org/10.1155/2013/717125

[4]   B. K. Mishra and N. Keshri, "Mathematical model on the transmission of worms in wireless sensor network," *Applied Mathematical Modelling* 37, 6: 4103–4111. doi.org/10.1016/j.apm.2012.09.025

[5]   R. Piyare and S. R. Lee, "Towards internet of things (IoTs): integration of wireless sensor network to cloud services for data collection and sharing," *International Journal of Computer Networks & Communication (IJCNC)* vol. 5, pp. 59–72. doi.org/DOI : 10.5121/ijcnc.2013.5505

[6]   Y. Ross and T. Watteyne, "*Reliable , Low Power Wireless Sensor Networks for the Internet of Things : Making Wireless Sensors as Accessible as Web Servers,"*`pp.1-4, 2013.

[7]   S. Tang and B. L. Mark, "Analysis of virus spread in wireless sensor networks: An epidemic model", *Proceedings of the 2009 7th International Workshop on the Design of Reliable Communication Networks, DRCN 2009*:   pp.   86–91. http://doi.org/10.1109/DRCN.2009.5340022

[8]   W. O. Kermack and A. G. McKendrick, A contribution to the mathematical theory of epidemics. *Proceedings of the Royal Society A*, vol. 115, pp. 700–721, August 1927. doi.org/10.1098/rspa.1927.0118

[9]   W. O. Kermack and A. G. McKendrick, Contributions of mathematical theory to epidemics, III–Further studies of the   problem of endemicity. *Proceedings of the Royal Society of London, Series A*, vol. 138. pp. 55-83, 1932.

[10]   W. O. Kermack and A. G. McKendrick, "Contributions of mathematical theory to epidemics, II–The problem of endemicity," *Proceedings of the Royal Society of London, Series A*, vol. 141, pp. 94-122, 1933.

[11]   B. K. Mishra and S. K. Pandey, "Dynamic model of worms with vertical transmission in computer network. *Applied Mathematics and Computation*", vol. 217, pp. 8438–8446, 2011. doi.org/10.1016/j.amc.2011.03.041

[12]   M. Y. Li., H. L. Smith, and L. Wang, "Global dynamics of an SEIR epidemic model with vertical Transmission," *SIAM J. Appl. Math.,* vol. 62, pp. 58–69, 2001.

[13]   C. Zeng and Y. Liu. 2016. Global stability of a computer virus model with cure and vertical transmission. *International Journal of Research Studies in Computer Science and Engineering* vol. 3, pp. 16–24, 2016.

[14]   M. Yang, Z. Zhang, Q. Li, and G. Zhang, "An SLBRS model with vertical transmission of computer virus over the internet," *Discrete Dynamics in Nature and Society*, vol.   925648,   pp.   1-17,   2012. doi.org/10.1155/2012/925648

[15]   S. A. Khayam and H. Radha, "A topologically-aware worm propagation model for wireless sensor networks. *Proc. 2nd Int'l workshop on Security in Distributed Computing Systems*, pp. 210–216, 2005.

[16]   P. De, Y. Liu, and S. K .Das, "An epidemic theoretic framework for evaluating broadcast protocols in wireless sensor networks. *2007 IEEE International Conference on Mobile Adhoc and Sensor Systems*, IEEE, 1–9, 2007.

[17]   P. De, Y. Liu, and S. K .Das, "An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks. *IEEE Transactions on Mobile Computing*, vol. 8, pp. 413–425, 2009.

[18]   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, pp. 47–62, 2010. doi.org/10.1007/s10878-008-9190-9

[19]   Y. Wang and X. Yang, "Virus spreading in wireless sensor networks with a medium access control mechanism", *Chinese Physics B* vol. 22, 40206. doi.org/10.1088/1674-1056/22/4/040206

[20]   B. K. Mishra, B. K. Mishra and S. K. Srivastava, "A quarantine model on the spreading behavior of worms in wireless sensor network," *Applied Mathematical Modelling,* vol. 2, pp. 1–12, 2014. doi.org/10.1016/j.apm.2012.09.025

[21]   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, 12–19, 2014. doi.org/10.5815/ijitcs.2014.03.02

[22]   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*: pp. 1–15, 2014. doi.org/http://www.advancesindifferenceequations.com/content/2014/1/295

[23]   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.

[24]   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 (IJCNIS),* vol. 9, pp. 43-52, 2017. doi:10.5815/ijcnis.2017.02.06

[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,   pp.   365–382,   1990. http://doi.org/10.1007/BF00178324

[26]   B. Mishra and A. Singh, "Global stability of worms in computer   network," *Applications   and   Applied Mathematics An International Journal*, vol. 5, pp. 1511–1528, 2010.

[27]   C. H. Nwokoye, V. E. Ejiofor, R. Orji, I. Umeh, and N. Mbeledogu, "Investigating the effect of uniform random distribution of nodes in wireless sensor networks using an epidemic worm model", *Proceedings of the 2nd International Conference on Computing Research and Innovations   (CoRI'16),*   pp.   58–63,   2016. doi.org/urn:nbn:de:0074-1755-8

Authors' Profiles

ChukwuNonso Henry Nwokoye is currently completing his Doctoral research in the Department of Computer Science, Nnamdi Azikiwe University Awka. He obtained a BSc degree in Computer Science and an MSc degree in Information Technology. 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 and network security, social computing and computer supported cooperative work (CSCW). His PhD research is on modeling and analysis of the propagation of malicious objects in network environments using analytical and agent-based modeling approaches.

Virginia Ebere Ejiofor holds BSc, MSc, and PhD all in Computer Science. She has been teaching Computer Science since 1997 and had published in a variety of local and international journals. Dr Ejiofor is a member of many professional bodies such as Computer Professionals (Registration Council) of Nigeria (CPN), Nigeria Computer Society (NCS), British Computer Society (BCS), Computer Forensics Institute, Nigeria (CFIN), Free and Open Source Software for Africa (FOSSFA), Open Source Foundation of Nigeria (OSFON), Association of Computing Machinery (ACM). She became a Fellow of BCS in 2010 and a Fellow of Institute of Corporate Administration of Nigeria in 2012. She served as a council member of CPN from 2009 to 2013 and is presently a council member of NCS. She was the past Editor-in-Chief of the Journal of Computer Science and its Applications. From 2011 to 2014 she was the Head of the Computer Science Department, Nnamdi Azikiwe University, Awka. Her interests include Distributed Database, Information Systems, Complex Networks, Modeling of Dynamical systems and Human Computer Interaction.

Moses O. Onyesolu: 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).

Boniface Ekechukwu holds BSc, MSc, and PhD, all in Computer Science. He has been teaching Computer Science for over twenty years and had published in a variety of local and international journals. He is a Reader; and also the incumbent head of Computer Science department, Nnamdi Azikiwe Unviersity, Awka, Nigeria. His research interests include software engineering, remote sensing, GIS, modeling and simulation of complex systems.