***I.J. Wireless and Microwave Technologies*, 2017, 6, 33-45**
Published Online November 2017 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2017.06.04

***Available online at* http://www.mecs-press.net/ijwmt**

The Impact of Sensor Area on Worm Propagation Using SEIR and SEIR-V Models: A Preliminary Investigation

ChukwuNonso H. Nwokoye[a], Njideka N. Mbeledogu[b], Ihekeremma A. Ejimofor[c]

[a,b]Department of Computer Science, Nnamdi Azikiwe University, Nigeria.
[c]Department of Computer Engineering, Madonna University, Enugu, Nigeria

Received: 26 May 2017; Accepted: 16 June 2017; Published: 08 November 2017

Abstract

Cyber security is of topical concern in the computing industry and in organizations that require ICT infrastructure for business-related activities. Theft or disrupting the flow of data and information can cause devastating damage to an institution's reputation and this may lead to huge financial losses. More mayhem can be perpetrated by malicious codes such as worms to organizations that use wireless sensor networks for collecting and transmitting data and information. To tackle the issue of malicious code propagation, researchers have used epidemiological models (such as SEIR and SEIR-V) to gain insights into spread patterns. However, topological concerns and its impact on worm propagation haven't been thoroughly studied. Here, we modify older models by applying a different expression for sensor deployment area; we intend to highlight the spatial parameters that may allow for the extinction of worms in wireless sensor networks amidst countermeasures deployed by network managers.

Index Terms: Epidemic theory, Epidemic model, Worms, Sensor Area

1. Introduction

Security of both stationary/moving data and information has occupied the interest of researchers in cyberspace in recent times. This is to preserve the confidentiality, integrity and availability (CIA) parameters of nodes/terminals in organizations that employ information and communication technologies and its infrastructures for meaningful work and business. These ICT infrastructures in organizations often involve large networks such as computer networks, peer-to-peer (P2P) and wireless sensor networks (WSN). Our interest is in ensuring security of data and information in organization that use WSNs in Africa.

Sensor networks are composed of large number of sensor nodes that are densely deployed without an

* Corresponding author.Tel.: +2347033858720, +2348036686032, +2348145582830
E-mail address: explode2kg@yahoo.com , njidembeledogu@yahoo.com, iaejims2@yahoo.com

engineered or predetermined location for the nodes [11][18]. According to [20], a Wireless Sensor Network (WSN) is a self-configuring network of small sensor nodes (so-called motes) communicating among them using radio signals, and deployed in quantity to sense the physical world. Due to the miniaturized sizes of the sensor nodes resources such as battery capability, memory and processing power are limited, nevertheless Wireless sensor network (WSN) is a developing technology, which promises modification of the method of information collection, processing and distribution [6]. Military applications of sensor networks are mainly for monitoring forces/equipments, battlefield surveillance, reconnaissance, targeting, battle damage evaluation; while environment applications are evident in biocomplexity mapping, precision agriculture, fire and flood detection etc. Advanced health industries also apply sensors for telemonitoring of data, tracking/monitoring of doctors/patients and drug administration [2]. Also WSN has been applied, “for coalescing the diverse possibilities of controlling applications that may relate to disaster prevention, prediction, intrusion detection, safety and other critical concerns” [22].

Envisaging the tremendous roles of wireless sensor networks in developing countries, researchers have advocated its use in the expedition of novel solutions that help curb development problems and the facilitation of research activities in environmental monitoring, physics of complex systems and energy management [21]. Zennaro’s work focused on Africa; therein they highlighted a plethora of sensor network applications in the continent. Other works found during our literature search availed the use of sensor network for early fire detection and monitoring fire outbreaks in Uganda [10]. The authors employed these sensors so as to curb the “over 70% of the fires [that] occur in Kampala metropolitan area”; statistics has it that the open markets are most vulnerable to these incessant fire outbreaks. Their aim in the paper was to eliminate the delays that plague the existing firefighting method. In Nigeria, WSN used precision farming was aimed at increasing agricultural productivity[1]. Therein, the sensors sense several parameters of the environment and transmit the collected data to the base station. The parameters can be the physical changes of, for instance air, humidity, wind, temperature, soil, pressure etc [23]. At the base station the collected data are analyzed and its results impact decision making for matters such as irrigation scheduling, fertilization scheduling etc.

The sensor networks by their distributed nature are prone to numerous challenges; they include faster bandwidth utilization, computational power depletion, low storage, and communication range; costly packets’ authentication, and uncertainty (in mobility, topology control, density, sensing accuracy) [16], [3]. These challenges culminate to weak defense capabilities for the sensor nodes. It also makes them appealing targets for malicious code attacks. Malicious codes in cyberspace include worms, viruses, trojans etc; their aim can be to deplete the already limited power of the tiny sensor node. As noted in [5] though researchers have developed several strategies for elongating the life time of sensors, injecting malwares into nodes (through *worm* attacks) has become an enormous threatening possibility in the WSN industry. This is due to the emergence of malicious codes (such as the cabir and mabir worms) that attack wireless devices. These wireless malwares employ the Bluetooth or the WiFi technology for its dissemination. As Mishra *et al.* [11] puts it, “cyber attack by worm presents one of the most dangerous threats to the security and integrity of the computer and telecommunications networks” such as wireless sensor networks. The interesting feature of these worms is that they do not require internet connectivity or human intervention for its spread. This makes the need to ensure a worm-free cyberspace through research activities an expedient one.

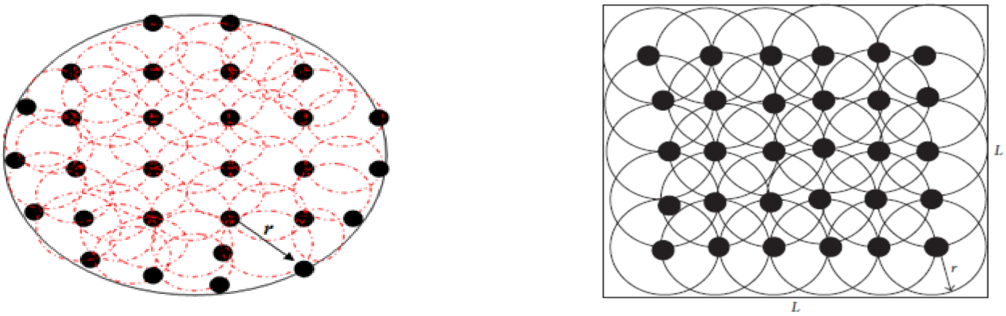
2. Related Works

Epidemiological models have been used to study the destructive activities of malicious codes in technological networks. This approach can be traced to public health wherein they are used for modelling infectious diseases in biological networks[11], [16], [17]. This area of research highlights the similarity between spread of biological disease-causing agents such virus and the spread of virtual malicious codes such as worms. In network epidemiology (evident in public health), analysts conceptually assume the compartmentalization of nodes based on their health status; further dividing the population of nodes into susceptible, infectious, recovered, dead etc. These epidemic models help provide better understanding of malicious code prevalence/spread and the factors that enhance it. In order to curb intrusions of worms, we feel epidemic models are very necessary if we are to get a better insight into the WSN dynamics.

In the light of the existing literatures which portray the use of epidemic models in studying worm spread features[11]; improvements, extensions and modifications have been based on the Kermack- Mckendrick SIR model [8], [7] and [9]. In modelling wireless sensor networks, popular countermeasures in public health such as quarantine [15] and vaccination[11] have constituted model improvements over the years. So is time delay [16] and topological considerations [17] etc.

Tang and Mark [18] formulated expressions for uniform random distribution of nodes and applied it on the (Susceptible-Infectious-Recovered-Maintenance) SIR-M model for WSN. Specifically, their work characterized the effects of communication range and density in order to enhance the antivirus capability of the network without “additional computational or signalling overhead”. Wang and Tang [19] used the Susceptible-Infectious (SI) model to study the impact of medium access control (MAC) on virus propagation in wireless sensor networks. Like [18], they analyzed the density and communication radius. Mishra *et al.* [11] used the Susceptible-Exposed-Infectious-Recovered-Vaccinated (SEIR-V) model to characterize the dynamics of worm propagation in WSN. Therein, they derived the reproduction number, the equilibria and its stability. With differential dynamical theories [5] represented worm propagation in WSN considering communication radius, distributed density and node energy exhaustion.

Nwokoye *et al.* [16] extended the model in [13,14] by applying the expression of distribution density and communication range observed in [19] and [18]. Nwokoye *et al.* [17] extended the model in [11] by applying the expression for uniform random distribution of sensor nodes. Both works highlighted the increase of the Exposed and Infectious nodes with corresponding increase in both the communication range and the density. Note that while communication range means “*the range over which a sensor can contact other sensor(s)*”, density “*implies the measurement of the total population of sensors per unit area*”. Other epidemiological models of malicious code propagation in WSN not discussed here can be seen in the above-mentioned works.



(1) (2)

Fig.1. WSN Topology 1 [18] , Fig. 2: WSN Topology 2 [5]

2.1. Objectives of the Study

Apparently, the analysis performed in [16] and [17] for VEIR and SEIR-V models respectively, involving the expression of distribution density and transmission range assume a topological structure described in Fig 1. We feel their work assume a circular sensor field for the WSN, this is because the expression (πr_0^2) for range and density as observed in [16], [17], [18] and [19] is close to the expression for the area of a circle. Therefore, in this study;

i. We apply a slightly different topological expression (as observed in Feng *et al.* [5] – Fig. 2) on the SEIR and SEIR-V models of worm propagation in WSNs; in order to highlight its impact on the Exposed and Vaccinated compartments. This analysis is absent in Feng *et al.* [5].
ii. We derive the reproduction numbers for secondary infections from a single infective node assuming the deployment area mimics a different WSN topology. This is necessary since the reproduction numbers in [16] and [17] assume a different expression for uniform random distribution.

3. Methodology

The methodology employed here is basically analysis, modeling and simulation. This method is mostly seen in studies of network epidemics (biological, technological etc); herein the networks are handled like a dynamical system with equilibrium positions that can be investigated for local/global asymptotic stability/instability. The methodology as [17] puts it starts with; model formulation (and optionally drawing the schematic diagram); finding the equilibrium states (for the worm-free and the endemic states); and deriving the reproduction number. Subsequent stages include; proof of stability and simulations experiments using software such as MatLab, Maple etc. At the model formulation stage, the modeler's intention is to abstract the real life phenomena (i.e. malicious code spread in WSN) using mathematical models. The modeler may decide to present a diagrammatic representation of the dynamical temporal transmissions between compartments. Thereafter, he/she obtains the equilibrium points by equating the equation-based model (differential equations) to zero. The reproduction ratio is derived from the model; this is necessary in determining the number of secondary infections that can arise from an infectious node. On the stability analyses, the jacobian method and the lyapunov's theorem are used to show the local and global analyses at the established equilibriums. Model perturbations are performed by varying the values for model parameters; this can be likened to simulations experiments. These experiments highlight the dynamical behavior of the compartments and their responses/results can be used to make decisions or to draw conclusions. However, one should note that the steps of network epidemics (presented above) are not hard and fast i.e. a modeler can decide to ignore the presentation of the symbolic solutions of different compartments. But from experience, model formulation and simulation experiments are always part of the study.

4. The VEIR-V Model

Since the modification done to the model in [16] applies the expression for the WSN topology in Fig. 2, some of the conditions therein persists here. In [16] the Vulnerable-Exposed-Infectious-Recovered-Vulnerable (VEIR-V) model represents temporal WSN dynamics. The sensors are stationary, similar and distributed and collected data are transferred to neighboring nodes (within their transmission range) using their antennas. The nodes may die due to worm infection or other hardware/software failure. The sensors are all vulnerable to attack and compromised nodes can collapse the whole network if unchecked. Before the infectious class, nodes exist in the exposed class; here we assume the nodes cannot transmit the infection. Compromised node recovery is possible through countermeasures deployed by network managers but the acquired immunity is temporary because recovered nodes become susceptible to worm infection again.

The sensor population in divided into the Vulnerable(V), Exposed(E), Infectious(I) and Recovered(R). Therefore, $N(t) = V(t) + E(t) + I(t) + R(t)$. The sensor nodes are stationary after its deployment in a uniformly random fashion with a density of σ, communication range of r_0^2 and the length of side L. Other parameters include ζ which is the inclusion rate of nodes into the sensor network population, β is the infectivity contact rate, μ is the mortality or the death rate of nodes due to hardware or software failure, ϖ is the crashing rate due to worm attack, ϑ is the rate at which exposed nodes become infectious, α is the recovery rate, ϱ is the rate at which recovered nodes become susceptible to infection due to temporal immunity.

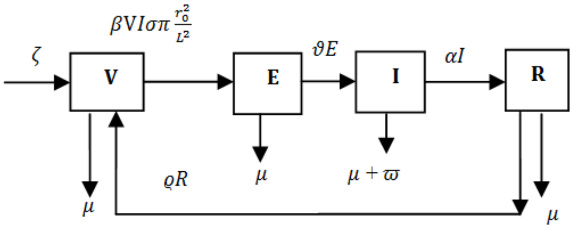


Fig.3. Flow of worms in WSN

$$\begin{aligned}
&\dot{\boldsymbol{V}} = \boldsymbol{\zeta} - \boldsymbol{\beta VI\sigma}\frac{\boldsymbol{\pi r_0^2}}{\boldsymbol{L^2}} - \boldsymbol{\mu V} + \boldsymbol{\varrho R}\\
&\dot{\boldsymbol{E}} = \boldsymbol{\beta VI\sigma}\frac{\boldsymbol{\pi r_0^2}}{\boldsymbol{L^2}} - (\boldsymbol{\mu} + \boldsymbol{\vartheta})\boldsymbol{E}\\
&\dot{\boldsymbol{I}} = \boldsymbol{\vartheta E} - (\boldsymbol{\alpha} + \boldsymbol{\mu} + \boldsymbol{\varpi})\boldsymbol{I}\\
&\dot{R} = \alpha I - (\mu + \varrho)R
\end{aligned} \tag{1}$$

In the light of our assumptions, Fig. 3 depicts the spatial and temporal dynamics of WSN and the system of differential equation (1) is the model.

4.1 Symbolic Solutions of Equilibrium Points

The system of differential equations (1) is equated to zero to obtain solutions of the Worm-free equilibrium and the Endemic equilibrium points. The Worm-free equilibrium (W_0^F) signifies the absence of worms and the Endemic Equilibrium (E_1^E) signifies the presence of worms in the network. The solutions of equilibrium points are Worm-free equilibrium $W_0^F = (V_0^*, E_0^*, I_0^*, R_0^*)$ i.e.

$$V_0^* = \frac{\zeta}{\mu};\ E_0^* = 0;\ I_0^* = 0; R_0^* = 0 \tag{2}$$

Endemic equilibrium E_1^E = (V_1^*, E_1^*,I_1^*, R_1^*,) i.e.

$$\begin{aligned}
&V_1^* = \frac{L^2(\vartheta+\mu)(\alpha+\mu+\varpi)}{\beta\vartheta\sigma\pi r_0^2}\\
&E_1^* = \frac{(\alpha+\mu+\varpi)(\mu+\varrho)(L^2\mu(\vartheta+\mu)(\alpha+\mu+\varpi)-\beta\zeta\vartheta\sigma\pi r_0^2)}{\beta\vartheta((\vartheta+\mu)(\mu+\varpi)(\mu+\varrho)+\alpha\mu(\vartheta+\mu+\varrho))\sigma\pi r_0^2}\\
&I_1^* = \frac{(\mu+\varrho)(L^2\mu(\vartheta+\mu)(\alpha+\mu+\varpi)-\beta\zeta\vartheta\sigma\pi r_0^2)}{\beta((\vartheta+\mu)(\mu+\varpi)(\mu+\varrho)+\alpha\mu(\vartheta+\mu+\varrho))\sigma\pi r_0^2}\\
&R_1^* = \frac{\alpha(L^2\mu(\vartheta+\mu)(\alpha+\mu+\varpi)-\beta\zeta\vartheta\sigma\pi r_0^2)}{\beta((\vartheta+\mu)(\mu+\varpi)(\mu+\varrho)+\alpha\mu(\vartheta+\mu+\varrho))\sigma\pi r_0^2}
\end{aligned} \tag{3}$$

4.2 Reproduction Ratio

The reproduction ratio is defined as “the expected number of secondary cases produced in a completely susceptible population, by a typical infective individual”[4]. Our reproduction ratio is the inverse of the susceptible at the endemic equilibrium [12] i.e. $\frac{\beta\vartheta\sigma\pi r_0^2}{L^2(\vartheta+\mu)(\alpha+\mu+\varpi)}$. This reproduction ratio is significantly different from $\frac{\beta\vartheta\sigma\pi r_0^2}{(\vartheta+\mu)(\alpha+\mu+\varpi)}$ derived in [16].

4.3 Stability of the Worm-free Equilibrium point

Here we show the proof of stability using the Jacobian approach. This approach is necessary if we are to show that the jacobian matrix have negative real parts. However, at asymptotic stability ($R_O < 1$) the worm disappears otherwise ($R_O > 1$) the network approaches the endemic state. Linearizing the model around the equilibrium positions by deriving the corresponding Jacobian matrix we have;

$$J\,(W_0^F) = \begin{bmatrix} -\mu & 0 & -\beta\frac{\zeta}{\mu}\sigma\frac{\pi r_0^2}{L^2} & \varrho \\ 0 & -(\mu+\vartheta) & \beta\frac{\zeta}{\mu}\sigma\frac{\pi r_0^2}{L^2} & 0 \\ 0 & \vartheta & -(\alpha+\mu+\varpi) & 0 \\ 0 & 0 & \alpha & -(\mu+\varrho) \end{bmatrix} \qquad (4)$$

With the exception of the values at (1,3) and (2,3), the jacobian matrix obtained here is almost the same as the jacobian matrix in [16]. This similarity is depicted in the diagonals of the Jacobian matrix ($-\mu, -(\mu+\vartheta), -(\alpha+\mu+\varpi), -(\mu+\varrho)$). They all have negative real parts; hence the system is asymptotically stable at worm-free equilibrium.

5. The Modified SEIRS-V Model

For the model in [17], the total population N (t) represents the nodes in the wireless sensor network which is subdivided into Susceptible, Exposed (latent), Infectious (contagious), Recovered (temporarily immune), Vaccinated (immunized) denoted by S(t), E(t), I(t), R(t) and V(t). This implies that S(t) + E(t) + I(t) + R(t) + V(t) = N(t).

Our analysis is done using the assumptions of below. The sensor nodes are uniformly and randomly deployed with a distribution density of σ and a transmission range of r_0^2 , this implies that the effective contact with an infected node for transfer of infection is in the order of σ (〖π r〗 _0^2)⁄L^2 . Other parameters include λ which is the inclusion rate of nodes into the sensor network population, β is the Infectivity contact rate, τ is the mortality or the death rate of nodes due to hardware or software failure, ω is the crashing rate due to attack of malicious objects (in this case worm), θ is the rate at which exposed nodes become infectious, ν is the recovery rate, φ is the rate at which recovered nodes become susceptible to infection, ρ is the rate of vaccination for susceptible sensor nodes and ξ is the rate of transmission from the vaccinated compartment to the susceptible compartment.

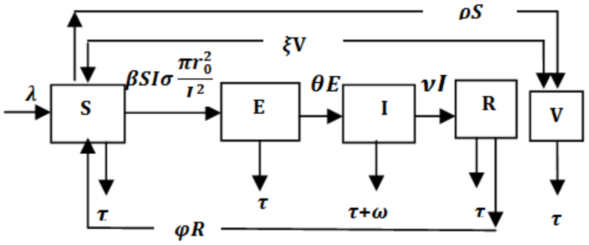


Fig.4. Flow of worms in WSN

$$\begin{aligned}
\dot{S} &= \lambda N - \beta S I \sigma \frac{\pi r_0^2}{L^2} - \tau S - \rho S + \varphi R + \xi V \\
\dot{E} &= \beta S I \sigma \frac{\pi r_0^2}{L^2} - (\tau + \theta) E \\
\dot{I} &= \theta E - (\tau + \omega + \nu) I \\
\dot{R} &= \nu I - (\tau + \varphi) R \\
\dot{V} &= \rho S - (\tau + \xi) V
\end{aligned} \tag{5}$$

In the light of our assumptions, Fig. 4 depicts the spatial and temporal dynamics of WSN and the system of differential equation (5) is the model.

5.1 Symbolic Solutions of Equilibrium Points

The solutions of equilibrium points are Worm-free equilibrium $E_0^F = (S_0^*, E_0^*, I_0^*, R_0^*, V_0^*)$ i.e

$$S_0^* = \frac{\lambda(\xi+\tau)}{\tau(\xi+\rho+\tau)}\,;\ E_0^* = 0;\ I_0^* = 0; R_0^* = 0, V_0^* = \frac{\lambda\rho}{\tau(\xi+\rho+\tau)} \tag{6}$$

Endemic equilibrium E_1^E = (S_1^*, E_1^*,I_1^*, R_1^*, V_1^*) i.e.

$$\begin{aligned}
S_1^* &= \frac{L^2(\theta+\tau)(\nu+\tau+\omega)}{\beta\theta\sigma\pi r_0^2} \\
E_1^* &= \frac{(\tau+\varphi)(\nu+\tau+\omega)(\lambda - S_1^* \frac{\tau(\xi+\rho+\tau)}{(\xi+\tau)})}{\theta\tau(\nu+\tau+\varphi)+\theta(\tau+\varphi)\omega+\tau(\tau+\varphi)(\nu+\tau+\omega)} \\
I_1^* &= \frac{(\tau+\varphi)(\theta\lambda - \frac{L^2\tau(\theta+\tau)(\xi+\rho+\tau)(\nu+\tau+\omega)}{\beta(\xi+\tau)\sigma\pi r_0^2})}{\theta\tau(\nu+\tau+\varphi)+\theta(\tau+\varphi)\omega+\tau(\tau+\varphi)(\nu+\tau+\omega)} \\
R_1^* &= \frac{\nu(\theta\lambda - \frac{L^2\tau(\theta+\tau)(\xi+\rho+\tau)(\nu+\tau+\omega)}{\beta(\xi+\tau)\sigma\pi r_0^2})}{\theta\tau(\nu+\tau+\varphi)+\theta(\tau+\varphi)\omega+\tau(\tau+\varphi)(\nu+\tau+\omega)} \\
V_1^* &= \frac{L^2\rho(\theta+\tau)(\nu+\tau+\omega)}{\beta\theta(\xi+\tau)\sigma\pi r_0^2}
\end{aligned} \tag{7}$$

The inverse of the susceptible at the endemic equilibrium for this model matches the reproduction ratio derived in section 4.2.

5.2 Stability of the Worm-free Equilibrium point

Using the jacobian approach we show that the "characteristic equation of the jacobian matrix" derived from the system of equations has negative roots"[17]. The corresponding Jacobian matrix derived from the system of equations is given as;

$$\det \begin{vmatrix}
-(\tau+\rho)-x & 0 & \frac{-\beta\sigma\pi {r_0}^2\lambda(\xi+\tau)}{L^2\tau(\xi+\tau)} & \varphi & \xi \\
0 & -(\tau+\theta)-x & \frac{\beta\sigma\pi {r_0}^2\lambda(\xi+\tau)}{L^2\tau(\xi+\tau)} & 0 & 0 \\
0 & \theta & -(\tau+w+)-x & 0 & 0 \\
0 & 0 & \nu & -(\tau+\varphi)-x & 0 \\
\rho & 0 & 0 & 0 & -(\tau+\xi)-x
\end{vmatrix} = 0 \tag{8}$$

Which equates to;

$$-(x+\tau)(x+\xi+\rho+\tau)(x+\tau+\varphi)\big((x+\theta+\tau)(x+\nu+\tau+\omega)-S_0^*\theta\beta\,\sigma\pi r_0^2/L^2\big)=0 \qquad (9)$$

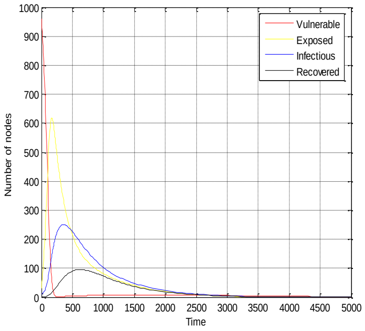
The roots of the characteristic equation all have negative real parts i.e. $-\tau,\ \ -\xi-\rho-\tau\,,\ -\tau-\varphi\,,\ \frac{1}{2}\Big(-\theta-\nu-2\tau-\omega-\sqrt{(-\theta+\nu+\omega)^2+4S_0^*\theta\beta\,\sigma\pi r_0^2/L^2}\Big),\ \frac{1}{2}(-\theta-\nu-2\tau-\omega+\sqrt{(-\theta+\nu+\omega)^2+4S_0^*\theta\beta\,\sigma\pi r_0^2/L^2})$; therefore the worm free equilibrium is locally asymptotically stable.

6. Numerical Results

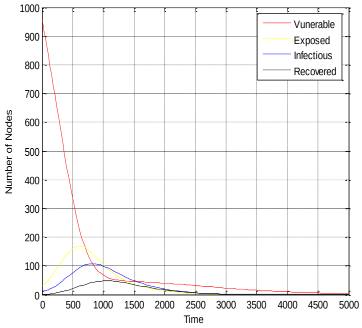
The systems of differential equations (1) and (5) were solved using a numerical method i.e. Runge-Kutta Fehlberg method of order 4 and 5. This is a suitable numerical method for initial value problems such as described in this study.

6.1. Numerical Results for VEIR

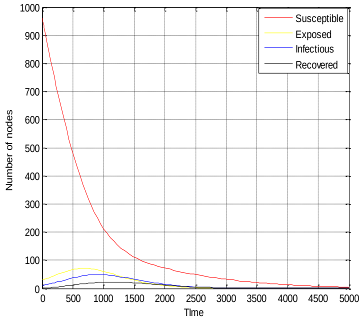
The simulation experiments for the VEIR model were done using these initial values for the Wireless Sensor network: V=960; E=30; I=10; R=0. Other values used for the simulation include; $\zeta = 0.001$; $\beta = 0.0003$; $\mu = 0.001$; $\varrho = 0.0003$; $\vartheta = 0.0001$; $\varpi = 0.001$; $\alpha = 0.002$; adapted from the time history of [5].



(5)

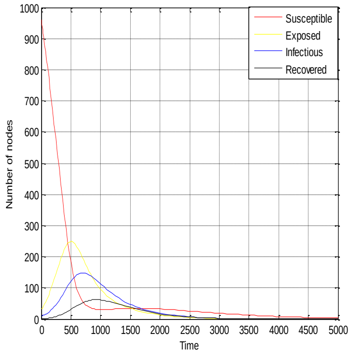


(6)

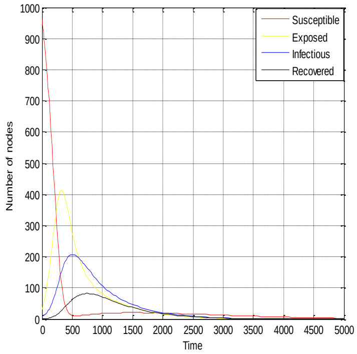


(7)

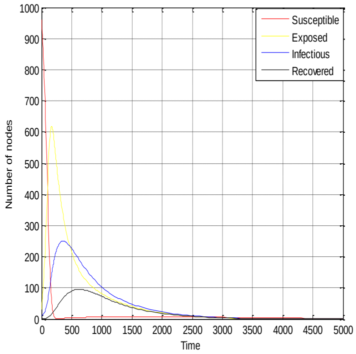
Fig.5. σ=0.3, r=1, L=1; Fig 6. σ=0.3, r=1, L=3; Fig 7. σ=0.3, r=0.5, L=2



(8)



(9)

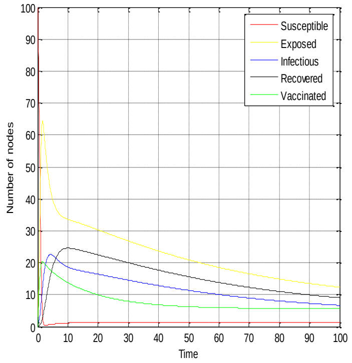


(10)

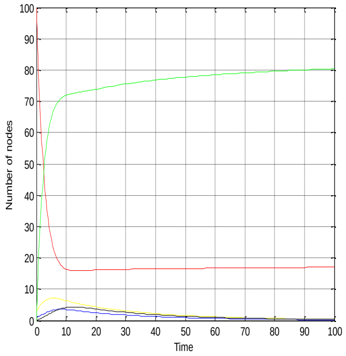
Fig.8. σ=0.3, *r*=0.8, *L*=2; Fig. 9. σ=0.1, *r*=0.1, *L*=0.1; Fig. 10. σ=0.3, *r*=0.1, *L*=0.1

6.2. Numerical Results for SEIR-V

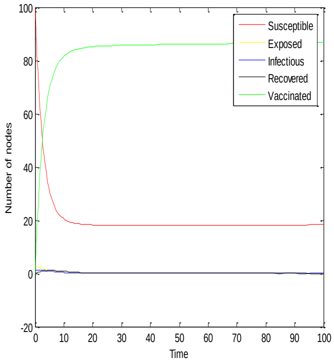
The simulation experiments for the SEIR-V model were done using these following initial values for the Wireless Sensor network S=100; E=3; I=1; R=0; V=0. Other values used for the simulation include λ=0.33; $\beta = 0.1$; τ=0.003; ω=0.07; θ=0.25; ν=0.4; φ=0.3; ρ=0.3; ξ =0.06; adapted from the time history of [11].



(11)

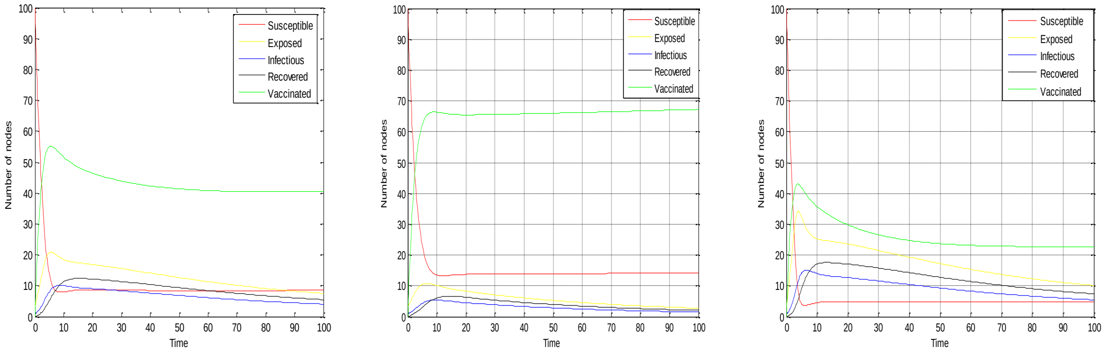


(12)



(13)

Fig.11. σ=0.3, *r*=1, *L*=0.5; Fig. 12. σ=0.3, *r*=1, *L*=2; Fig. 13. σ=0.3, *r*=0.3, *L*=2



(14) (15) (16)

Fig.14. σ=0.3, r=0.8, L=2; Fig. 15. σ=0.1, r=0.1, L=0.1; Fig. 16. σ=0.3, r=0.1, L=0.14

6.3. Discussion of Results

For both the VEIR and SEIR-V model, it is evident in section 6 that keeping the range r constant and increasing L, reduced the nodes in the exposed and the infected compartments i.e. Fig. 5. and Fig. 6 (for VEIR) and Fig. 11. and Fig. 12. (for SEIR-V). On the other hand keeping L constant and increasing r, increased the exposed and the infectious nodes i.e. Fig. 7. and Fig. 8. (for VEIR) and Fig. 13. and Fig. 14. (for SEIR-V). This is consistent with Feng *et al.* [5], at least for infectious sensor nodes.

The simulation results for both models show that keeping both r and L constant and increasing the density (σ) correspondingly increased the number of both the exposed and infectious nodes. The increase in density also reduced the number of vaccinated sensor nodes as evident in Fig. 9 and Fig. 10 (for VEIR); and Fig. 13 and Fig. 16 (for SEIR-V). Note that although the results here are gotten with a different expression for WSN topology, the results are consistent with Nwokoye *et al.* [16-17] (for exposed and the infectious nodes) and with [18] and [19] (for infectious sensor nodes). The implication is that increase in density generally increases the rate of worm infection (and correspondingly reduces the impact of vaccination) in wireless sensor networks at least for the two WSN topologies presented above.

7. Industrial Significance and Eventual Benefits

It is no news that Wireless Sensor Networks can aid energy management and the functionalities of complex systems. It can also enhance forces/equipments monitoring, battlefield surveillance, reconnaissance, targeting, battle damage evaluation. In the light of the detailed benefits of a wireless sensor network in Africa listed in [20], there is need to invest research efforts into WSNs' security, because malicious code propagation will constitute several losses/disruptions for organizations that use them.

The significance of our analyses herein is that it elicited the topological factors that increase the number of exposed nodes and reduce/increase the impact of vaccination. Considering the models of our analyses and the topological expression of WSN used, our study is of topical importance. This is because in network epidemiology, the exposed class contains nodes that are infected but not fully infectious. Some researchers allude to a lower (or no) infectivity rate at this (*exposed*) stage compared to the nodes in the infectious class. According Mishra et al. [11], common symptom for sensor nodes in this latent stage is slow data transmission speed. Additionally, vaccination (or inoculation) is a known countermeasure in network epidemiology. It is aimed at strengthening a fraction of the sensor population before to the outset of an epidemic. Our study is immensely necessary, since the work of Feng *et al.* [5] that employed similar topological expression didn't account for the latent phase of worms (Exposed compartment). Correspondingly, nodes of WSN can be exposed to worm infection and the network administrators of organizations that use sensor networks can employ vaccination schemes to harden their networks.

Insights generated as a result of analyses of distribution density and transmission range can help these organizations in sensor deployment activities/decisions. In other words it will positively impact this "*randomness*" of sensor distribution/location in the sensor field. They would now understand the factors that might expose a sensor node or weaken any countermeasure mustered by network managers. The generalized version of our analytical model can be integrated into the cyber-defense structure of organization(s) that use Wireless Sensor Networks in order to creatively protect the interchange of stationary and moving data and information.

8. Conclusions

Our study herein exemplifies theoretical explorations on the dynamics of worm propagation in wireless sensor networks. Specifically, we employed the expression that closely mimics the WSN topology depicted in Fig. 2, in order to generate better understanding of worm propagation in the presence of density and range using the SEIR (VEIR) and SEIR-V models. The analyses highlighted several differences when compared to the results of older models that mimicked the WSN topology of Fig. 1. Aside generating interesting solutions for endemic equilibrium, our study derived the reproduction ratio for finding the secondary infections that may arise from the introduction of a single infective sensor node. The reproduction number for both models herein is the same; this is because the addition of the vaccinated compartment in SEIR-V didn't affect the compartments that determine worm infection or otherwise.

The consistency of our study is depicted in the fact that although we used different input values adapted from different sensor epidemic studies the results follow the same pattern for both models. Specifically, the values for the simulation experiment in Feng *et al.* [5] were adapted for our VEIR model while the input data of Mishra *et al.* [11] was used for our SEIR-V.

In the furtherance of this study, we would include the media access control (MAC) mechanism as applied in [19] and other communication protocols using our models herein. Therein, we would check the effects of the protocols on the compartments and the WSN topology. We would also modify quarantine models observed in literature by applying the expressions of WSN topology used in this study. Since we provided the solutions of the endemic equilibrium, we would also pursue other extended objectives such as performing global stability analyses using for example the geometrical approach. This is to highlight how it differs from global stability analyses of similar models in literature.

References

[1] Adebayo S, Akinwunmi AO, Aworinde HO. Increasing agricultural productivity in Nigeria using wireless sensor network (WSN). IEEE African Journal of Computing & ICT 2015; 3: 121–128.

[2] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey. computer networks 2002, 4: 393–422.

[3] De P, Liu Y, Das SK. Modeling node compromise spread in wireless sensor networks using epidemic theory. International Symposium on a World of Wireless, Mobile and Multimedia Networks 2006: 237–243.

[4] Diekmann O, Heesterbeek JAP, Metz JAJ. On the definition and the computation of the basic reproduction ratio R0 in models for infectious diseases in heterogeneous populations. Journal of Mathematical Biology 1990, 4: 365–382.

[5] Feng L, Song L, Zhao Q, Wang H. Modeling and stability analysis of worm propagation in wireless sensor network. Mathematical Problems in Engineering 2015.

[6] Yaeghoobi BK, Soni MK, Tyagi SS. Dynamic and real-time sleep schedule protocols for energy efficiency in WSNs. I. J. Computer Network and Information Security 2016, 1: 9–17.

[7] Kermack WO, McKendrick AG. Contributions to the mathematical theory of epidemics. ii. the problem of endemicity. Proceedings of the Royal Society of London, Series A 1832; v138i834: 55– 83.

[8] Kermack WO, McKendrick AG.. A contribution to the mathematical theory of epidemics. Proceedings of the Royal Society of London A: mathematical, physical and engineering sciences, The Royal Society 1927;, 700–721.

[9] Kermack WO, McKendrick AG. Contributions to the mathematical theory of epidemics. III. Further studies of the problem of endemicity. Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character 1933; 843: 94–122.

[10] Lule E, Bulega TE. A scalable Wireless Sensor Network (WSN) based architecture for fire disaster monitoring in the developing world. I. J. Computer Network and Information Security 2015; 2: 40–49.

[11] Mishra BK, Keshri N. Mathematical model on the transmission of worms in wireless sensor network. Applied Mathematical Modelling 2013, 6: 4103–4111.

[12] Mishra BK, Pandey SK. Dynamic model of worms with vertical transmission in computer network. Applied Mathematics and Computation 2011, 21: 8438–8446.

[13] Mishra BK, Saini D. Mathematical models on computer viruses. Applied Mathematics and Computation 2007; 2: 929–936.

[14] Mishra BK, Saini D. SEIRS epidemic model with delay for transmission of malicious objects in computer network. Applied Mathematics and Computation 2007; 2: 1476–1482.

[15] Mishra BK, Tyagi I. 2014. Defending against malicious threats in wireless sensor network: A mathematical model. International Journal of Information Technology and Computer Science 2014; 3: 12–19.

[16] Nwokoye CH, Umeh I, Nwanze M, Alao BF. Analyzing time delay and sensor distribution in sensor networks. IEEE African Journal of Computing & ICT 2015, 1: 159–164.

[17] Nwokoye CH, Ejiofor VE, Orji, R, Umeh I. 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 2016, 58–63.

[18] Tang S, Mark BL. Analysis of virus spread in wireless sensor networks: An epidemic model. 7th International Workshop on the Design of Reliable Communication Networks, DRCN 2009: 86–91.

[19] Wang Y, Yang X. Virus spreading in wireless sensor networks with a medium access control mechanism. Chinese Physics B 2013, 4: 40206.

[20] Zennaro M, Pehrson B, Bagula A. Wireless sensor networks: A great opportunity for researchers in developing countries. 2nd IFIP Intl Symp. on Wireless Communications and Information Technology in Developing (Countries, South Africa) 2008.

[21] Zennaro M, Pehrson B, Bagula A. Wireless Sensor Networks : A great opportunity for researchers in Developing Countries.

[22] Singh A, Snigdh I. Modelling failure conditions in zigbee based wireless sensor networks. International Journal of Wireless and Microwave Technologies (IJWMT), 2017; 2: 25-34, 2017.

[23] Palani S. Providing useful data reliably to mobile cloud users from random wireless sensor network. International Journal of Wireless and Microwave Technologies (IJWMT) 2017; 1: 49-62.

Acknowledgements

We thank the anonymous reviewers that read our manuscript and their keen efforts directed at ensuring accuracy of our work.

Authors' Profiles

ChukwuNonso Henry Nwokoye 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 and 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.

Njideka N Mbeledogu is a lecturer at the Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria. She holds Bachelor of Science (BSc), Master of Science (MSc) and PhD degrees in Computer Science. She is a member of the Computer Professional of Nigeria (CPN) and the Nigerian Computer Society (NCS). Her interests include Network Security, Neural Networks and Fuzzy logic.

Ihekeremma Amara Ejimofor is a lecturer at the Department of Computer Engineering, Faculty of Engineering, Madonna University, Enugu, Nigeria. She holds a Bachelor of Engineering degree in Computer Engineering and a Master of Science degree in Computer Science. She is currently pursuing her PhD degree in Computer Science in Nnamdi Azikiwe University, Awka, Nigeria. Her interests include networks security, experts systems and big data analytics.

How to cite this paper: ChukwuNonso H. Nwokoye, Njideka, N. Mbeledogu, Ihekeremma A. Ejimofor," The Impact of Sensor Area on Worm Propagation Using SEIR and SEIR-V Models: A Preliminary Investigation", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.7, No.6, pp. 33-45, 2017.DOI: 10.5815/ijwmt.2017.06.04