Vol 8. No. 1 Issue 2 – May, 2015
African Journal of Computing & ICT

© 2015 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781
www.ajocict.net

Analyzing Time Delay and Sensor Distribution in Sensor Networks

C. H. Nwokoye & I. Umeh
Department of Computer Science,
Nnamdi Azikiwe University
Awka, Nigeria.
explode2kg@yahoo.com

M. Nwanze & B.F. Alao
Department of Computer Education,
Federal College of Education (Technical)
Asaba, Nigeria.

ABSTRACT

There has been a proliferation of malicious codes or softwares directed at the destruction of organizational ICT infrastructures. These malicious codes are also used in numerous cyber warfare by nation states to steal valuable information. To ensure security, researchers has used epidemic models for better understanding of worm proagation. In this paper we explored the impact of time delay and node distribution on the compartments that represent worm propagation dynamics in Wireless Sensor Networks (WSN). This is done using a modified SEIR epidemic model with a cyber mass action incidence rate. The sensor network is treated as a dynamical system, and its equilibrium points studied. We derived the reproduction number using the next generation matrix method, performed stability analysis and using real values we simulated the system.

Keywords: Epidemic theory; Malicious codes; Worms; Wireless Sensor Networks

African Journal of Computing & ICT Reference Format:
C. H. Nwokoye, I. Umeh, M. Nwanze & B.F. Alao (2015): Analyzing Time Delay and Sensor Distribution in Sensor Networks. Afr J. of Comp & ICTs. Vol 8, No. 1, Issue 1. Pp 159-164

1. INTRODUCTION

Wireless Sensor Networks (WSN) consists of sensor nodes which possess the ability to sense, process and communicate data and information [1]. These sensor nodes are densely deployed without any predetermined location. The applications of sensor networks are evident in the military (for monitoring forces/equipments, battlefield surveillance, reconnaissance, targeting, battle damage evaluation); the home and in the environment (for biocomplexity mapping, precision agriculture, fire and flood detection etc). Its use extends also to health applications (for telemonitoring of data, tracking/monitoring of doctors/patients and drug administration) and other commercial applications.

The sensor nodes collect and transmit data such as temperature, stress/noise levels, soil constituents etc. The sensor nodes are distributed in a sensor field and data moves from sensor to sensor back to the sink in a multihop fashion as depicted in Figure 1. The random distribution of sensor nodes is mostly done in unguarded and hostile environments. Due to its nature, WSN is open to several security challenges such as limited resources (energy/battery power, bandwidth, computational power, storage, and communication range); costly packets' authentication, and uncertainty (in mobility, topology control, density, sensing accuracy)[2].

These challenges can result to its vulnerability to several attacks in the cyberspace leading to the loss of confidentiality and integrity of neighboring nodes. Attacks in WSN arise from malicious codes i.e. worms, viruses, Trojan etc. Malicious code attacks cause substantial damage to organizations. In order to proffer defense measures to the insecurity that plagues sensor networks, network analysts have proposed several analytic (mathematical models) i.e. differential, discrete equations etc. This is to predict malicious code behavior in a network environment and to possibly contain its propagation.

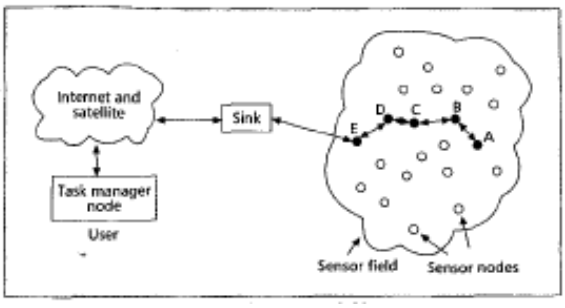

Figure 1. Sensor nodes scattered in a sensor field [4]

© 2015 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781

2. RELATED WORKS

Understanding the behavior of malicious codes in cyberspace can be traced to Epidemic theory or Epidemiology in public health. Epidemic theory investigates the contagion results of a susceptible population in view of the interaction between agent, host and environment [11]. The relationship between cyberspace and public health is due to the similarity in the spread of infection in the biological world and the propagation of malicious codes in the networked environment. Specifically, relating epidemiology to our discourse, the agent, host and environment equals the worm/virus, the sensor nodes and the wireless sensor network environment respectively. Malicious code modeling and analyses is necessary if network analysts are to elicit the factors that facilitate speedy spread.

Since Kermack and McKendrick [5–7] developed their Susceptible-Infectious-Recovered (SIR) model, several models have been proposed to cater for numerous issues of the networked environment. Modifications of the SIR, include the Susceptible-Infectious-Susceptible (SIS) without recovery and the SIR-S where there is recovery and subsequent re-infection due to temporal immunity. Other modifications include SEIR with delay and SEIV with delay and vaccination.

Here, we extend the work of [12] by adding time delay represented by the Exposed and Recovered compartment to form the Vulnerable-Exposed-Infectious-Recovered-Vulnerable (VEIR-V). Wang et al.'s analysis was absent the Exposed and the Recovered compartments. This extension is also necessary for the model in [11]; therein their analysis didn't account for time delay and the temporary immunity in cyberspace. However, a model similar to our (VEIR-V) i.e. SEIR model was proposed by [9,10] for a computer network; but we extend the work to WSN by adding parameters for distribution density and communication range. Density (σ) is the measurement of the sensor population per unit area while communication range (r) is the range over which a sensor can contact other sensors [8].

3. RESEARCH METHODOLOGY

Fundamentally, we perform modeling and simulation in this study. We would employ the extensively used procedure for studying epidemics in networked environments. This method has been used to study social, biological and communication systems/networks. Specifically, the network is handled like a dynamical system and the points of no change (Equilibriums) are investigated. The steps of this methodology include formulation of the model (i.e. the system of equations); deriving solutions for the equilibrium points; finding the Reproduction ratio; performing the proof of stability and finally running simulation experiments (i.e. perturbing the model with real values).

3.1 The VEIR-V Model

To represent the dynamics of wireless sensor network with respect to time we employ the Vulnerable-Exposed-Infectious-Recovered-Vulnerable (VEIR-V) model. Generally, we assume that the sensors are stationary, similar and distributed in an area. With the help of their antennas they sense and transfer gathered information to neighboring nodes (within their communication range). In this model we assume that nodes are added to the network and nodes crash out due to malicious code infection (i.e. worm) or due to hardware/software failure. The total population of sensors is prone to attack from worms due to its nature and can acquire the worm infection with time (constituting the sensors in the Infectious class). Nodes which are compromised by worm attack spread alongside the gathered data through protocols to their neighbors causing a major collapse of the network with time.

Prior to the full infectious stage the worm(s) in the network may experience a time delay (i.e. the exposed class). Sensor nodes may have a sleep capability wherein their (installed) antiviral softwares perform maintenance functions (i.e. infection check) [11]. Nodes can recover as a result of these countermeasures deployed by the network managers but due to temporal immunity (acquired at the recovery stage) sensor nodes may become vulnerable again to worm infection.

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 randomly fashion with a density of σ and communication range of r. 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.

When there is no worm attack, the sensor population approaches the carrying capacity ζ/μ, therefore $dN/dt = \zeta - \mu N - \varpi I$.

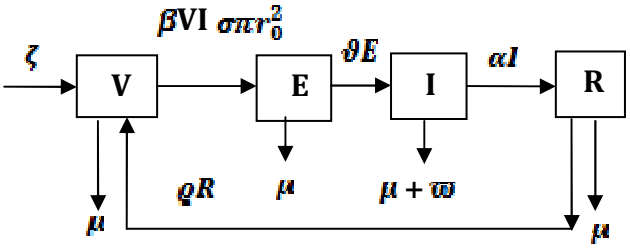

Figure 2. Flow of worms in WSN

© 2015 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781

Figure 2 depicts the dynamics of worm transmission in a wireless sensor network in view of our asssumtion. The system of ordinary differential equation (1) captures time delay, density and the communication range. The modified SEIR-S model is represented using the following system of differential equations;

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

3.2 Symbolic Solutions of Equilibrium Points

Equating the modified system of differential equations (1) to zero i.e. $\dot{V} = 0; \dot{E} = 0; \dot{I} = 0; \dot{R} = 0;$ we obtain two solutions which are the Worm-free equilibrium and the Endemic equilibrium points. While the Worm-free equilibrium (W_0^E) signifies when there is no worm in the network, the Endemic Equilibrium (E_1^E) signifies the presence of worms.

The solutions of equilibrium points are Worm-free equilibrium

$W_0^E = (V_0^*, E_0^*, I_0^*, R_0^*)$ i.e. $V_0^* = \frac{\xi}{\mu}$;

$$E_0^* = 0;\ I_0^* = 0; R_0^* = 0, \quad (2)$$

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

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

3.3 The Basic Reproduction Number

Using the next generation matrix method we would derive the Reproduction number commonly denoted as R_0. The Reproduction number is the spectral radius or the "dominant eigenvalue of the matrix G = $\mathbf{FV^{-1}}$"[3]; where F is the rate of appearance of new infections in the Infectious compartment and V is the rate of transfer of terminals into and out of the Infectious compartment.

The Reproduction number is given as;

$$F = \begin{bmatrix} 0 & \beta\sigma\pi r_0^2 \\ 0 & 0 \end{bmatrix}, V = \begin{bmatrix} \mu+\vartheta & 0 \\ \vartheta & \alpha+\mu+\varpi \end{bmatrix}$$

$$R_0 = \frac{\beta\vartheta\sigma\pi r_0^2}{(\vartheta+\mu)(\alpha+\mu+\varpi)} \quad (4)$$

3.4 Stability of the Worm-free Equilibrium point

The Jacobian method is use to show the proof of stability at the worm-free equilibrium point. We would specifically show that the eigenvalues of the jacobian matrix have negative real parts.

The stability of the equilibrium positions determines the possible worm replication in the sensor network represented by our VEIR-V model. In essence, when asymptotically stable the worm infection cease to exist otherwise an epidemic occurs. Using the Reproduction number notations, the worm-free equilibrium is locally asymptotically stable if $R_0 < 1$ and unstable if $R_0 > 1$.

We linearize the model around the equilibrium positions by deriving the corresponding Jacobian matrix given as

$$J=\begin{bmatrix} -\mu & 0 & -\beta V I \sigma\pi r_0^2 & \varrho \\ 0 & -(\mu+\vartheta) & \beta V I \sigma\pi r_0^2 & 0 \\ 0 & \vartheta & -(\alpha+\mu+\varpi) & 0 \\ 0 & 0 & \alpha & -(\mu+\varrho) \end{bmatrix} \quad (5)$$

$$J=\begin{bmatrix} -\mu & 0 & -\beta\frac{\xi}{\mu}\sigma\pi r_0^2 & \varrho \\ 0 & -(\mu+\vartheta) & \beta\frac{\xi}{\mu}\sigma\pi r_0^2 & 0 \\ 0 & \vartheta & -(\alpha+\mu+\varpi) & 0 \\ 0 & 0 & \alpha & -(\mu+\varrho) \end{bmatrix} \quad (6)$$

Substituting the values of the worm-free equilibrium in the Jacobian matrix (5) gives (6). The diagonals of the Jacobian matrix are; $-\mu, -(\mu+\vartheta), -(\alpha+\mu+\varpi), -(\mu+\varrho)$ i.e. they all have negative real parts; hence the system is asymptotically stable at worm-free equilibrium.

© 2015 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781
www.ajocict.net

4. NUMERICAL RESULTS

The system of differential equation was solved using a numerical method called the Runge-Kutta-Fehlberg order 4 and 5 method.

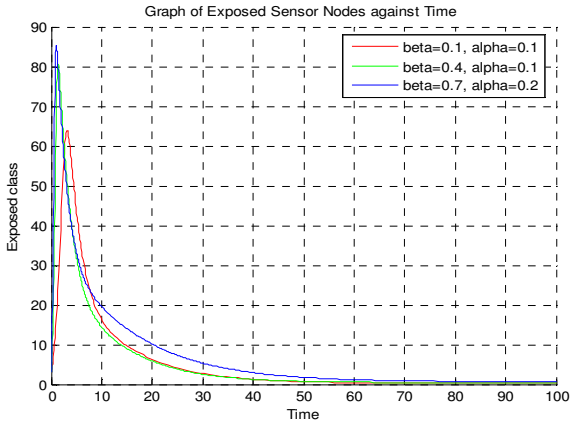

Figure 3. Behavior of Exposed Compartment versus Time w.r.t. to β and α

Figure 3 presents the transient response of the population of Exposed sensor nodes *E(t)* as function of different parameter. Gradually with the passage of time *E(t)* increases to its peak point (at 63, 76 and 85 for the three responses) and slowly decreases to zero. The Exposed sensor nodes signify the time delay before sensor nodes becomes fully infectious.

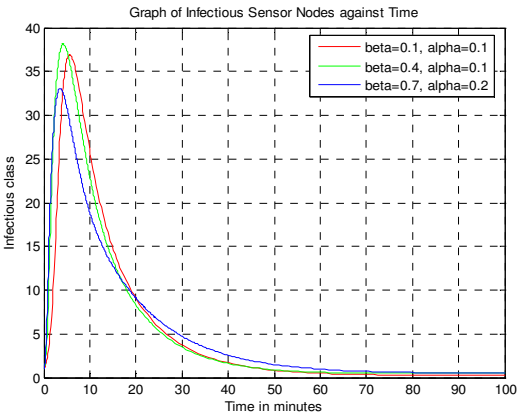

Figure 4. Behavior of Infectious Compartment versus Time w.r.t. to β and α

Figure 4 presents the transient response of the population of Infectious sensor nodes *I(t)* as function of different parameters of the model. Over time *I(t)* increases up to its peak point and then decreases to zero. More nodes get infected as the rate of infectivity contact was increased (from 0.1 to 0.7) and rate of recovery kept constant at α=0.1; for the first and the second responses.

But slightly increasing the rate of recovery slows down the spread of the worm i.e. instead of a noticeable increase above the second response, the third response (depicted with blue) reduced to 30 Infectious nodes due to the increase in the rate of recovery. This is because containment approaches deployed by network managers are targeted at infectious nodes.

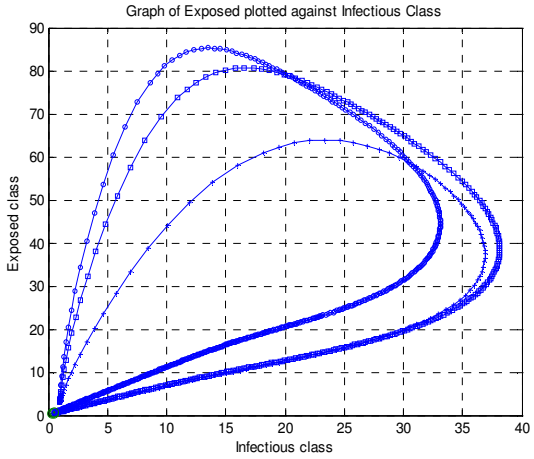

Figure 5. Behavior of Exposed Compartment Infectious Compartment w.r.t. to β and α

Figure 5 depicts clearly the relationship between the Exposed and the Infectious class. Here, it is clear that increasing the rate of infectivity contact (β) and the rate of recovery (α) increases the both the Exposed and the Infectious class.

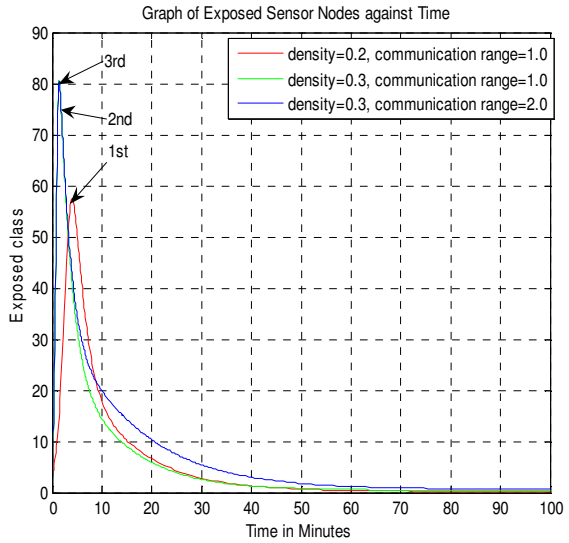

Figure 6. Dynamical behavior of Exposed Compartment versus Time w.r.t. to σ and r

© 2015 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781
www.ajocict.net

In Figure 6 it is evident that increasing the distribution density and the communication range increased the sensor nodes in the Exposed class when the infectivity contact rate and recovery rate are constant. The second (green) and third (blue) responses are not too distinct (at their peak points) because their distribution density is the same (i.e. 0.3). The increase in communication range from 1 to 2 also increased the sensor nodes from above 50 nodes to 80 nodes.

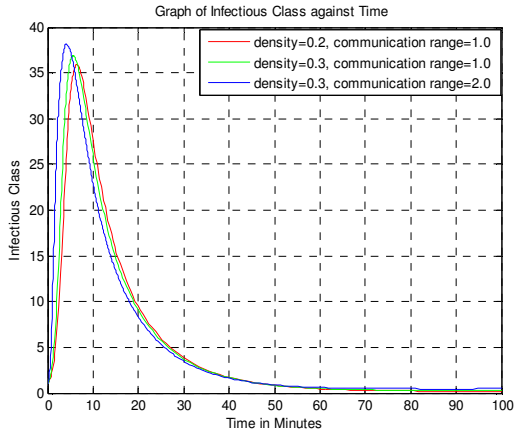

Figure 7. Dynamical behavior of Infectious Compartment versus Time w.r.t. to σ and r

Figure 7 shows the dynamical behavior of the Infectious sensor nodes with varied parameters of the distribution and the communication range. Aside the noticed gradual increase and then decrease of the Infectious class, it is clear that keeping the range constant (at 1.0) and increasing the density from 0.2 to 0.3 consequently increased the Infectious class. Additionally, keeping the density constant (at 0.3) and increasing the range from 1.0 to 2.0 consequently increased the Infectious class.

5. CONCLUSION

With the presence of the parameters for density and communication range, slowing down the rate at which the worm pervades the sensor network depends on the rate of recovery, the density and the communication range. Analysis using the SEIR-S (our VEIR-V) model involves this time delay as well as the density and range. Recovery of Infectious sensor nodes was obtained due to increase in the rate of recovery. The increase in the Infectious sensor nodes observed in our study is consistent with the SIR model in [11] and the SI model in [12]. It is also expedient to highlight that the expression (πr_0^2) used for the range is same with the area of circle; and this implies that the area for sensor deployment considered in our study is a circular strip.

This study assumed that the sensor nodes are stationary therefore an extension of the work can involve sensor node mobility or a combination of both. Furthermore, we would extend our analysis to include the Media Access Control (MAC) mechanism as applied in [12] and other communication protocols using our model. Therein, we would check the effects of the communication protocols on the compartments of our study.

© 2015 Afr J Comp & ICT – All Rights Reserved - ISSN 2006-1781

REFERENCES

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. 2002. Wireless sensor networks: a survey. *Computer Networks* 38, 4: 393–422. http://doi.org/10.1016/S1389-1286(01)00302-4

[2] De, P., Liu, Y and Das, S. K. 2006. Modeling node compromise spread in wireless sensor networks using epidemic theory. *Proceedings - WoWMoM 2006: 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks* 2006: 237–243. http://doi.org/10.1109/WOWMOM.2006.74

[3] Driessche, P. V. and Watmough, J. 2002. Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission. *Mathematical Biosciences* 180: 29–48. http://doi.org/10.1016/S0025-5564(02)00108-6

[4] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E. 2002. A Survey On Sensor Networks. *IEEE communication Magazine*, 102–114.

[5] Kermack, W. O. and McKendrick, A. G. 1932. Contributions to the mathematical theory of epidemics. ii. the problem of endemicity. *Proceedings of the Royal Society of London. Series A. v138 i834*: 55–83.

[6] Kermack, W. O. and McKendrick, A. G.. 1927. A contribution to the mathematical theory of epidemics. *Proceedings of the Royal Society of London A: mathematical, physical and engineering sciences*, The Royal Society, 700–721.

[7] Kermack, W. O. and McKendrick, A. G. 1933. 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* 141, 843: 94–122.

[8] Martin, K. M. and Paterson, M. 2008. An Application-Oriented Framework for Wireless Sensor Network Key Establishment. *Electronic Notes in Theoretical Computer Science* 192, 2: 31–41. http://doi.org/10.1016/j.entcs.2008.05.004

[9] Mishra, B. K. and Saini, D. 2007. Mathematical models on computer viruses. *Applied Mathematics and Computation* 187, 2: 929–936. http://doi.org/10.1016/j.amc.2006.09.062

[10] Mishra, B. K. and Saini, D. K. 2007. SEIRS epidemic model with delay for transmission of malicious objects in computer network. *Applied Mathematics and Computation* 188, 2: 1476–1482. http://doi.org/10.1016/j.amc.2006.11.012

[11] Tang, S and Mark, B. L. 2009. 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*: 86–91. http://doi.org/10.1109/DRCN.2009.5340022

[12] Wang, Y. and Yang, X. 2013. Virus spreading in wireless sensor networks with a medium access control mechanism. *Chinese Physics B* 22, 4: 40206. http://doi.org/10.1088/1674-1056/22/4/040206