Applied Mathematical Modelling 37 (2013) 4103–4111

Contents lists available at SciVerse ScienceDirect

Applied Mathematical Modelling

journal homepage: www.elsevier.com/locate/apm

Mathematical model on the transmission of worms in wireless sensor network

Bimal Kumar Mishra *, Neha Keshri

Department of Applied Mathematics, Birla Institute of Technology Mesra, Ranchi 835 215, India

ARTICLE INFO

Article history:
Received 19 January 2012
Received in revised form 27 July 2012
Accepted 10 September 2012
Available online 25 September 2012

Keywords:
Global stability
Epidemic model
Worms
Antivirus treatment
Wireless sensor network

ABSTRACT

Wireless sensor networks (WSNs) have received extensive attention due to their great potential in civil and military applications. The sensor nodes have limited power and radio communication capabilities. As sensor nodes are resource constrained, they generally have weak defense capabilities and are attractive targets for software attacks. Cyber attack by worm presents one of the most dangerous threats to the security and integrity of the computer and WSN. In this paper, we study the attacking behavior of possible worms in WSN. Using compartmental epidemic model, we propose susceptible – exposed – infectious – recovered – susceptible with a vaccination compartment (SEIRS-V) to describe the dynamics of worm propagation with respect to time in WSN. The proposed model captures both the spatial and temporal dynamics of worms spread process. Reproduction number, equilibria, and their stability are also found. If reproduction number is less than one, the infected fraction of the sensor nodes disappears and if the reproduction number is greater than one, the infected fraction persists and the feasible region is asymptotically stable region for the endemic equilibrium state. Numerical methods are employed to solve and simulate the systems of equations developed and also to validate our model. A critical analysis of vaccination class with respect to susceptible class and infectious class has been made for a positive impact of increasing security measures on worm propagation in WSN.
© 2012 Elsevier Inc. All rights reserved.

1. Introduction

A sensor network is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or predetermined. This allows random deployment in inaccessible terrains or disaster relief operations. Wireless sensor networks (WSNs) have received extensive attention due to their great potential in civil and military applications [1]. The sensor nodes are usually scattered in a sensor field as depicted in Fig. 1. Each of these scattered sensor nodes have the capabilities to collect data and route data back to the sink. Data are routed back to the sink by a multihop infrastructureless architecture through the sink. In Fig. 1, red dots represent the transmission of data from one node to another and data transmission obstruction is due to the attack of worm in sensor network. The sensor nodes have limited power and radio communication capabilities. Thus due to the limited transmission range, data generated from sensors that are far away from the sink, a source node sends its data to its neighbor nodes, which in turn sends the data to their respective neighbors.

As wireless sensor networks are unfolding their vast potential in a plethora of application environment, security still remains one of the most critical challenges yet to be fully addressed [2]. Because sensor nodes are resource constrained, they

* Corresponding author. Tel.: +91 9430764860; fax: +91 651 2275401.
E-mail addresses: drbimalmishra@gmail.com (B.K. Mishra), keshri.neha7@gmail.com (N. Keshri).

0307-904X/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.apm.2012.09.025

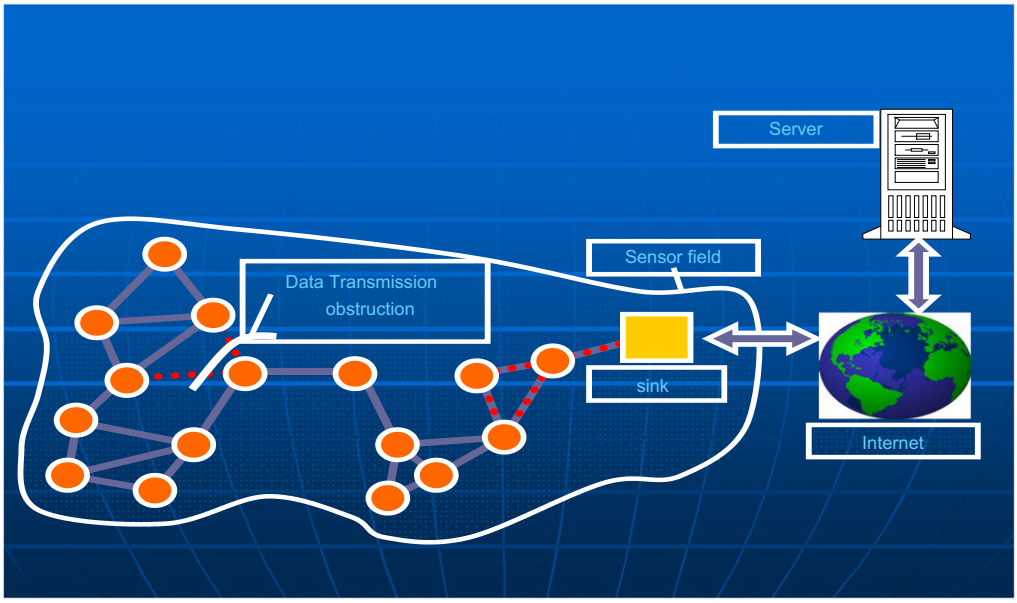

Fig. 1. Sensor network communication structure.

generally have weak defense capabilities and are attractive targets for software attacks (like virus or worm attacks on the Internet). Worms are self-replicating computer viruses which can propagate through computer networks without any human intervention [3–5]. Cyber attack by worm presents one of the most dangerous threats to the security and integrity of the computer and telecommunications networks. The last few years have seen the emergence of a new type of worms specifically targets portable computing devices, such as smart phones and laptops. The novel feature of these worms is that they do not necessarily require internet connectivity for their propagation. They can spread directly from device to device using wireless communication technology, such as Wi-Fi or Bluetooth [6–8]. Actually, malicious codes targeting wireless devices have already started to emerge. Recently surfaced virus Cabir that can spread over the air interface has unveiled a disastrous threat for wireless sensor networks. Inescapably, viruses targeting wireless sensor networks will emerge. The Mabir worm [9] uses similar scanning techniques to launch proximity attack. Thus, security mechanism that can defend sensor nodes against software attacks is of great interest to the wireless sensor network community.

The action of malicious objects throughout a network can be studied by using epidemiological models for disease propagation [10–19]. Based on the Kermark and Mc Kendrick, SIR classical epidemic model [20–22], dynamical models for malicious objects propagation were proposed, providing estimation for temporal evolutions of infected nodes depending on network parameters considering topological aspects of the network [23–27,10–12]. The kind of approach was applied to e-mail propagation schemes [28] and modification of SIR models generated guides for infections prevention by using the concept of epidemiological threshold [10–12,29]. The model SEIR proposed by the authors [30] assumes that recovery hosts have a permanent immunization period with a certain probability, which is not consistent with real situation. In order overcome limitation, Mishra and Saini [10] presents a SEIRS model with latent and immune periods, which can reveal common worm propagation. Recently, more research attention has been paid to the combination of virus propagation models antivirus countermeasures to study the prevalence of virus, for example, virus immunization [12,31–35] and quarantine [36–38].

Since there is a basic similarity between the software virus spread among wireless devices and the transmission of epidemic disease in a population, the epidemiological models extensively used by social researchers [39–43] can be applied to study the spread of viruses in wireless networks. Some of related applications of epidemic models in wireless environments have been discussed in the recent literature [44–48].

In this paper, we study the attacking behavior of possible worms in wireless sensor network. Using compartmental epidemic model, we propose susceptible – exposed – infectious – recovered – susceptible with a vaccination compartment (SEIRS-V) to describe the dynamics of worm propagation with respect to time in wireless sensor network. We assume inclusion of new sensor nodes and crashing of the nodes due to the attack of worms and also due to hardware/software problem in the sensor field. We do assume all the sensor nodes in the sensor field to be susceptible towards the possible worms attack. Worms as per their spreading nature infect any one sensor node which in due course of time infects the other neighboring sensor nodes making a infectious class of nodes. Before the sensor nodes become fully infectious it shows the symptoms of attack, i.e., the usual speed of transmission of data become slow etc. We put these classes of nodes in exposed compartment. By introducing a maintenance mechanism in the sleep nodes of wireless sensor network, our SEIRS-V model can improve the network's anti-virus capability and enable the network to adapt flexibility to different type of worms. As there is no permanent immunization in the cyber world, the nodes are temporarily immune and there after again become

susceptible towards the possible attack of worms. Some possible application of real life is also discussed in this paper. The developed model and its analytical method will be applicable to design and analyze the information (including attacking behavior of worms) for communication network.

2. e-Epidemic model of worm spread in wireless sensor network

Let $S(t)$, $E(t)$, $I(t)$, $R(t)$ and $V(t)$ denote the number of susceptible, exposed, infectious, recovered, vaccinated nodes at time t, respectively.

Assume $N(t) = S(t) + E(t) + I(t) + R(t) + V(t)$ for all t.

The system of differential equations that describes the rate of change of different classes and as per our assumptions, which is depicted in Fig. 2, is given as:

$$\begin{aligned}
\frac{dS}{dt} &= A - \beta SI - \mu S - pS + \delta R + \eta V \\
\frac{dE}{dt} &= \beta SI - (\mu + \alpha)E \\
\frac{dI}{dt} &= \alpha E - (\mu + \varepsilon + \gamma)I \\
\frac{dR}{dt} &= \gamma I - (\mu + \delta)R \\
\frac{dV}{dt} &= pS - (\mu + \eta)V
\end{aligned} \tag{1}$$

where,$\frac{1}{\delta}$ and $\frac{1}{\eta}$ are the periods of immunity of the recovered & vaccinated susceptible nodes respectively, and A is the inclusion of new sensor nodes to the population, μ is the crashing rate of the sensor nodes due to hardware/software problem, ε is the crashing rate due to attack of worms, β is the infectivity contact rate, α is the rate of transmission from E-class to I-class, γ is the rate of recovery, δ is the rate of transfer from R-class to S-class, η is the rate of transmission from V-class to S-class, p is the vaccinating rate coefficient for the susceptible nodes.

Now, $\frac{dN}{dt} = A - \mu N - \varepsilon I$.

In the absence of attack, the population size of the node approaches the carrying capacity A/μ. The differential equation for N implies that solution of (1) starting in the positive orthan R_5^+ approach, enter or remain in the epidemiologically meaningful subset.

$$D = \{(S, E, I, R, V)/S \geqslant 0, E \geqslant 0, I \geqslant 0, R \geqslant 0, V \geqslant 0, S + E + I + R + V \leqslant A/\mu\}$$

Thus, it suffices to consider solutions in region D. Solution of the initial value problem starting in D and defined by (1) exist and are unique on maximal interval [49,50]. Since solution remain bounded in the positively invariant region D, the maximal interval is $(0, \infty)$. Thus, initial value problem is well posed both mathematically and epidemiologically.

3. Existence and stability of equilibrium

For equilibrium points, we have

$$\frac{dS}{dt} = 0; \quad \frac{dE}{dt} = 0; \quad \frac{dI}{dt} = 0; \quad \frac{dR}{dt} = 0; \quad \frac{dV}{dt} = 0$$

and on simple calculation, we get, equilibrium points as:

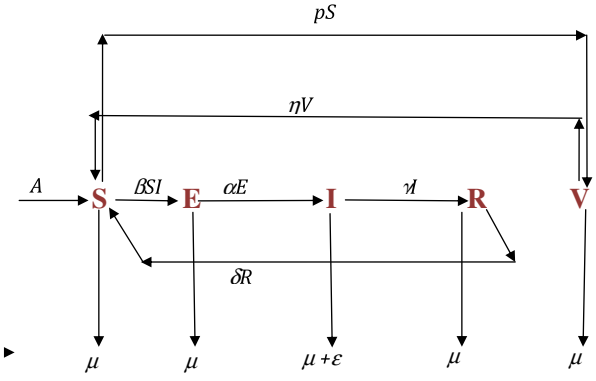

Fig. 2. Schematic diagram for the flow of worms in sensor network.

$P = \left(\frac{A(\mu+\eta)}{\mu(\mu+\eta+p)}, 0, 0, 0, \frac{pA}{\{(\mu+\delta)(\mu+p)-p\eta\}}\right)$ for worm-free state and $(S^*, E^*, I^*, R^*, V^*)$ for endemic state,

where, $S^* = \frac{(\mu+\alpha)\theta}{\alpha\beta}$

$$E^* = \frac{\theta(\mu+\delta)}{\{\gamma\alpha\delta-(\mu+\delta)(\mu+\alpha)\theta\}\alpha}\left[\frac{(\mu+\alpha)\theta}{\beta} * \frac{(\mu+p)(\mu+\eta)-\eta p}{(\mu+\eta)} - \alpha A\right]$$

$$I^* = \frac{(\mu+\delta)}{\gamma\alpha\delta-(\mu+\delta)(\mu+\alpha)\theta}\left[\frac{(\mu+\alpha)\theta}{\beta} * \frac{(\mu+p)(\mu+\eta)-\eta p}{(\mu+\eta)} - \alpha A\right]$$

$$R^* = \frac{\gamma}{\gamma\alpha\delta-(\mu+\delta)(\mu+\alpha)\theta}\left[\frac{(\mu+\alpha)\theta}{\beta} * \frac{(\mu+p)(\mu+\eta)-\eta p}{(\mu+\eta)} - \alpha A\right]$$

$$V^* = \frac{p(\mu+\alpha)\theta}{(\mu+\eta)\alpha\beta}$$

where, $\theta = (\mu + \varepsilon + \gamma)$

3.1. The basic reproduction number (R_0)

The basic reproduction number can be obtained by calculating V and F, where V and F are given as

$$V = \begin{bmatrix} \mu+\alpha & 0 \\ -\alpha & \mu+\varepsilon+\gamma \end{bmatrix}, \quad F = \begin{bmatrix} 0 & \beta \\ 0 & 0 \end{bmatrix}$$

The basic reproduction number is defined as the dominant Eigen value of FV^{-1}.

that is, $R_0 = \frac{\alpha\beta}{(\mu+\alpha)(\mu+\varepsilon+\gamma)}$.

3.2. Stability of the worm-free equilibrium stage

At worm free equilibrium point P, the Jacobian matrix is

$$J(P) = \begin{pmatrix} -(\mu+p) & 0 & -\beta A(\mu+\eta) & \delta & \eta \\ 0 & -(\mu+\alpha) & \beta A(\mu+\eta) & 0 & 0 \\ 0 & \alpha & -(\mu+\varepsilon+\gamma) & 0 & 0 \\ 0 & 0 & \gamma & -(\mu+\delta) & 0 \\ p & 0 & 0 & 0 & -(\mu+\eta) \end{pmatrix} \tag{2}$$

Eigen values of (2) are: $-(\mu + p)$, $-(\mu + \alpha)$, $-(\mu + \varepsilon + \gamma)$, $-(\mu + \delta)$, $-(\mu + \eta)$ which all are negative; hence the system is locally asymptotically stable at worm free equilibrium point P.

Lemma 1. *If $R_0 < 1$, the worm-free equilibrium P is locally asymptotically stable. If $R_0 = 1$, P is stable; $R_0 > 1$, P is unstable. Let, $f_\infty = \lim_{t\to\infty} \inf_{\theta\geqslant t} f(\theta)$, $f^\infty = \lim_{t\to\infty} \sup_{\theta\geqslant t} f(\theta)$*

Lemma 2. *Assume that a bounded real valued function $f:[0,\infty) \to R$ be twice differentiable with bounded second derivative. Let $k \to \infty$ and $f(t_k)$ converges to f^∞ or f_∞ then,*

$$\lim_{t\to\infty} f'(t_k) = 0$$

Theorem 1. *If $R_0 < 1$, then the worm-free equilibrium P is globally asymptotically stable.*

Proof. From system (1), we have,

$$\frac{dS}{dt} \leqslant A - \frac{\mu(\mu+\eta+p)}{(\mu+\eta)}S$$

A solution of the equation $\frac{dX}{dt} \leqslant A - \frac{\mu(\mu+\eta+p)}{(\mu+\eta)}X$ is super solution of S (t)

Since $X \to \frac{(\mu+\eta)A}{(\mu+\eta+p)\mu}$ as $t \to \infty$, then for a given $\varepsilon_1 > 0$, there exists t_0 such that

$$S(t) \leqslant X(t) \leqslant \frac{(\mu+\eta)A}{(\mu+\eta+p)\mu} + \varepsilon_1 \text{ for all } t \geqslant t_0$$

Thus $S^\infty \leqslant X(t) \leqslant \frac{(\mu+\eta)A}{(\mu+\eta+p)\mu} + \varepsilon_1$

Let $\varepsilon_1 \to 0$ then $S^\infty \leqslant \frac{(\mu+\eta)A}{(\mu+\eta+p)\mu}$.

Second equation of (1) reduces to

$$\frac{dE}{dt} = \beta \mathrm{I} \frac{(\mu+\eta)A}{(\mu+\eta+p)\mu} - (\boldsymbol{\mu}+\alpha)E \tag{3}$$

Now taking third equation of (1) with (3)

$$\begin{bmatrix} \dot{E} \\ \dot{I} \end{bmatrix} \leqslant Z \begin{bmatrix} E \\ I \end{bmatrix} \tag{4}$$

where, $Z = \begin{bmatrix} -(\mu+\alpha) & 0 \\ \alpha & -(\mu+\varepsilon+\gamma) \end{bmatrix}$

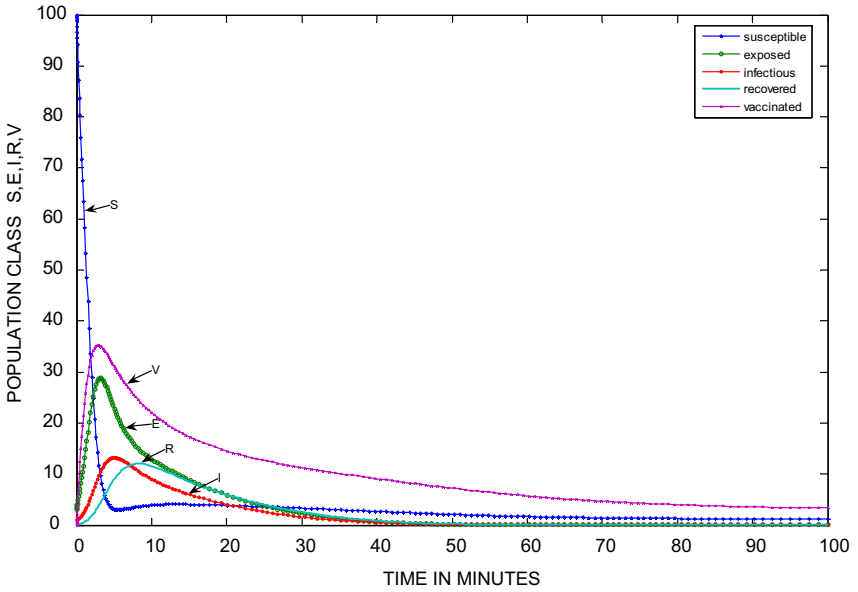

Fig. 3. Dynamical behavior of the system for different classes when $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.3$; $\eta = 0.06$; $\alpha = 0.25$; $\varepsilon = 0.07$; $\gamma = 0.4$, With initial values: $S(0) = 100$; $E(0) = 3$; $I(0) = 1$; $R(0) = 0$; $V(0) = 0$.

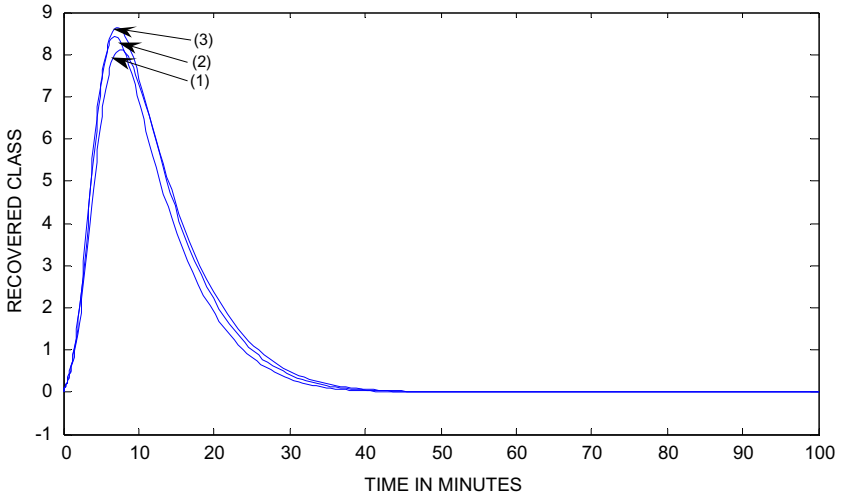

Fig. 4. Dynamical behavior of recovered class with respect to time for: (1) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; p = 0.3; $\delta = 0.3$; $\eta = 0.06$; $\alpha = 0.25$; $\varepsilon = 0.07$; $\gamma = 0.4$ (2) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.33$; $\eta = 0.06$; $\alpha = 0.28$; $\varepsilon = 0.07$; $\gamma = 0.43$ (3) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p9 = 0.3$; $\delta = 0.39$; $\eta = 0.06$; $\alpha = 0.31$; $\varepsilon = 0.07$; $\gamma = 0.46$. With initial values: $S(0) = 100$; $E(0) = 3$; $I(0) = 1$; $R(0) = 0$; $V(0) = 0$.

Let $M \in R^+$, such that $M \geqslant max((\mu+\alpha),(\mu+\varepsilon+\gamma))$

Thus $Z + M\ I_{2\times 2}$ is a strictly positive matrix, if ω_1 and ω_2 are the eigen values of Z then $\omega_1 + M$, $\omega_2 + M$ are eigenvalue of $Z + M\ I_{2\times 2}$. Thus form the Perron–Frobenius theorem [51], $Z + M\ I_{2\times 2}$ has a simple positive eigenvalue equal to dominant eigenvalue and corresponding eigenvector $e > 0$, which implies that ω_1 and ω_2 are real. If $\omega_1 + M$ is the dominant eigenvalue of $Z + M\ I_{2\times 2}$, then $\omega_1 > \omega_2$ and $eZ = e^{\omega_1}$. Obviously ω_1, ω_2 are the roots of the equation

$$\lambda^2 + (2\mu + \alpha + \varepsilon + \gamma)\lambda + (\mu+\alpha)(\mu+\varepsilon+\gamma) = 0 \tag{5}$$

Since $R_0 < 1$ for $\varepsilon_1 > 0$, sufficiently small, we have,

$$(\mu+\alpha)(\mu+\varepsilon+\gamma) > 0$$

Therefore, the coefficients of the quadratic equation (5) are positive

Thus ω_1, ω_2 all are negative, from Eq. (5), for $t \geqslant t_0$

$$\frac{d}{dt}(e[E(t), I(t)]) \leqslant \omega_1 . e[E(t), I(t)]$$

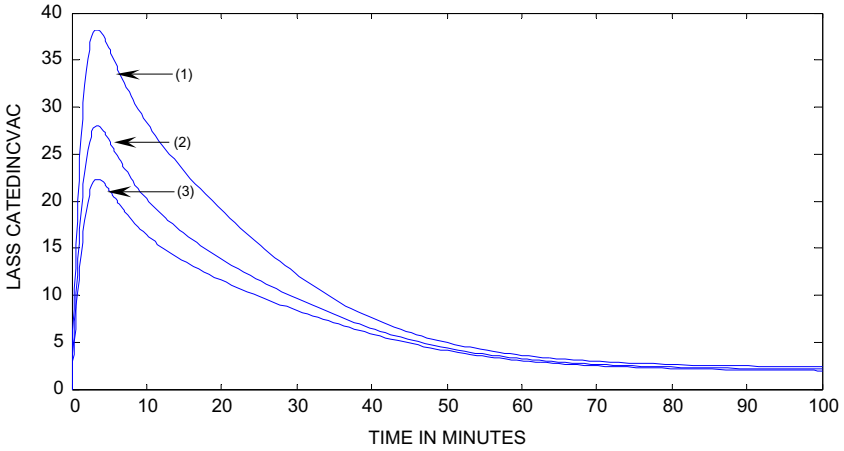

Fig. 5. Dynamical behavior of vaccinated class with respect to time for: (1) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.3$; $\eta = 0.06$; $\alpha = 0.25$; $\varepsilon = 0.07$; $\gamma = 0.4$ (2) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.2$; $\delta = 0.3$; $\eta = 0.009$; $\alpha = 0.25$; $\varepsilon = 0.07$; $\gamma = 0.4$ (3) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.15$; $\delta = 0.3$; $\eta = 0.004$; $\alpha = 0.25$; $\varepsilon = 0.07$; $\gamma = 0.4$. With initial values: $S(0) = 100$; $E(0) = 3$; $I(0) = 1$; $R(0) = 0$; $V(0) = 0$.

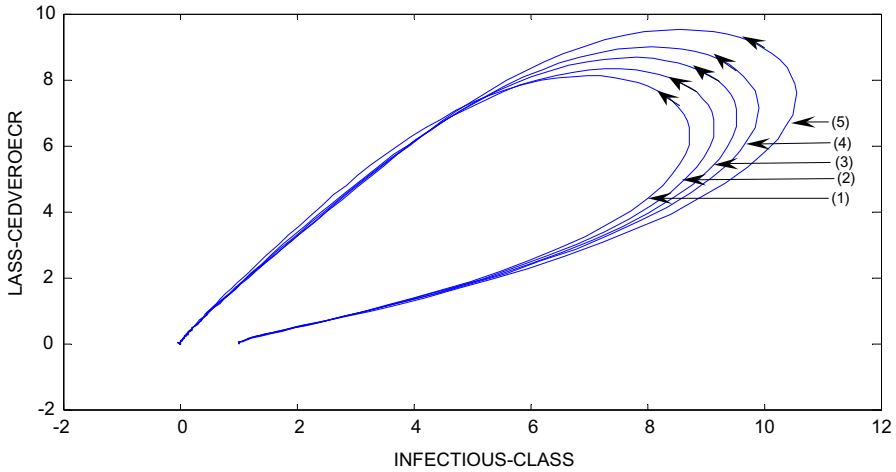

Fig. 6. Dynamical behavior of recovered class versus infectious class when (1) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.3$; $\eta = 0.06$; $\alpha = 0.25$; $\varepsilon = 0.07$; $\gamma = 0.4$ (2) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.33$; $\eta = 0.06$; $\alpha = 0.27$; $\varepsilon = 0.07$; $\gamma = 0.42$ (3) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.35$; $\eta = 0.06$; $\alpha = 0.29$; $\varepsilon = 0.07$; $\gamma = 0.44$ (4) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.37$; $\eta = 0.06$; $\alpha = 0.31$; $\varepsilon = 0.07$; $\gamma = 0.46$ (5) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.39$; $\eta = 0.06$; $\alpha = 0.34$; $\varepsilon = 0.07$; $\gamma = 0.48$. With initial values: $S(0) = 100$; $E(0) = 3$; I $(0) = 1$; $R(0) = 0$; $V(0) = 0$.

Integrating the above in equation, we have,

$$0 \leqslant e.[E(t), I(t)] \leqslant e.[E(t_1), i(t_1)]e^{\omega_1(t-t_1)} \quad \text{for } t \geqslant t_1 \geqslant t_0$$

Since $\omega_1 < 0$, $e.[E(t),I(t)] \to 0$ *as* $t \to \infty$

Using $e > 0$, *we have* $E(t),I(t) \to (0,0)$ *as* $t \to \infty$

By Lemma 2, we choose a sequence $t_n \to \infty$, $S_n \to \infty (n \to \infty)$ such that $S(S_n) \to S^{\infty}$

$$S(t_n) \to S_{\infty}, \quad \dot{S}(S_n) \to 0, \quad \dot{S}(t_n) \to 0$$

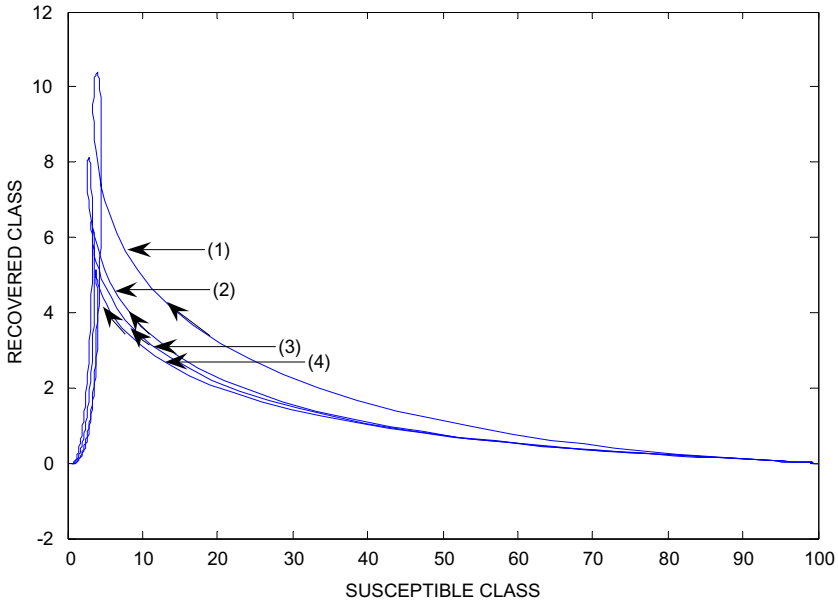

Fig. 7. Dynamical behavior of susceptible class versus recovered class when (1) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.3$; $\eta = 0.06$; $\alpha = 0.25$; $\varepsilon = 0.07$; $\gamma = 0.4$ (2) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.5$; $\eta = 0.06$; $\alpha = 0.27$; $\varepsilon = 0.07$; $\gamma = 0.42$ (3) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.8$; $\eta = 0.06$; $\alpha = 0.30$; $\varepsilon = 0.07$; $\gamma = 0.45$ (4) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.3$; $\delta = 0.8$; $\eta = 0.06$; $\alpha = 0.7$; $\varepsilon = 0.07$; $\gamma = 0.47$. With initial values: $S(0) = 100$; $E(0) = 3$; $I(0) = 1$; $R(0) = 0$; $V(0) = 0$.

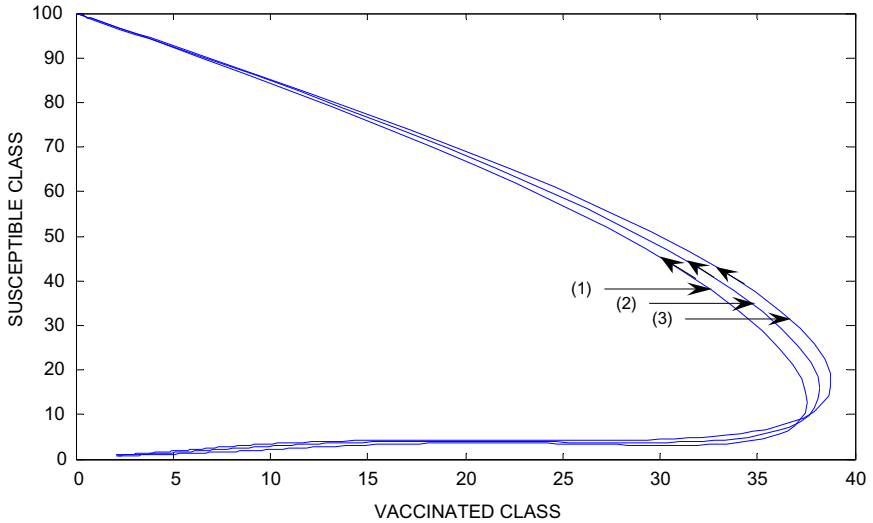

Fig. 8. Dynamical behavior of vaccinated class versus susceptible class when (1) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.32$; $\delta = 0.3$; $\eta = 0.06$; $\alpha = 0.25$; $\varepsilon = 0.07$; $\gamma = 0.4$ (2) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.35$; $\delta = 0.3$; $\eta = 0.09$; $\alpha = 0.25$; $\varepsilon = 0.07$; $\gamma = 0.4$ (3) $A = 0.33$; $\beta = 0.1$; $\mu = 0.003$; $p = 0.38$; $\delta = 0.3$; $\eta = 0.12$; $\alpha = 0.25$; $\varepsilon = 0.07$; $\gamma = 0.4$. With initial values: $S(0) = 100$; $E(0) = 3$; $I(0) = 1$; $R(0) = 0$; $V(0) = 0$.

Since $E(t) \to 0$, $I(t) \to 0$ *for* $t \to \infty$, thus from the first equation of (1), we have,

$$\lim_{n\to\infty} S(t) = \frac{(\mu+\eta)A}{(\mu+\eta+p)\mu}$$

Hence, by incorporating lemma1, the worm-free equilibrium P is globally asymptotically stable, if $R_0 < 1$.

4. Application of wireless sensor network

Wireless sensor networks can be used by the military for a number of purposes such as monitoring militant activity in remote areas and force protection. Being equipped with appropriate sensors, these networks can enable detection of enemy movement, identification of enemy force and analysis of their movement and progress. Driven by the confluence between the need to collect data about people's physical, physiological, psychological, cognitive, and behavioral processes in spaces ranging from personal to urban and the recent availability of the technologies that enable this data collection, wireless sensor networks for healthcare have emerged in the recent years. Advances in wireless sensor networking have opened up new opportunities in healthcare systems. The future will see the integration of the abundance of existing specialized medical technology with pervasive, wireless networks. They will co-exist with the installed infrastructure, augmenting data collection and real-time response. Examples of areas in which future medical systems can benefit the most from wireless sensor networks are in-home assistance, smart nursing homes, and clinical trial and research augmentation.

5. Conclusion

Inspired by the compartmental biological epidemic model, we propose an e-SEIRS-V model for the attacking behavior of worms in sensor nodes. Reproduction number is obtained to understand the spreading and fading of the worms in the sensor field. We establish that the worm-free equilibrium is globally asymptotically stable, if reproduction number is less than one. Runge–Kutta–Fehlberg method of order 4 and 5 is used to solve and simulate the system of equations developed. With the help of MATLAB, an extensive simulation is performed to validate the developed model. Fig. 3 represents the dynamical behavior of the system under different parametric values. A powerful impact of vaccination provided to the sensor nodes is clearly observed over exposed and infectious class in Fig. 3. Analysis of recovered and vaccinated class with respect to time is depicted in Figs. 4 and 5, respectively. If the parameters of Figs. 4 and 5 are well taken into the account, the recovery of the sensor nodes from worm attack after having proper treatment by anti-virus software will be very high and also the impact of vaccination will be strong respectively. Fig. 6 represents the dynamical behavior of infectious class versus recovery class. When suitable parameters are taken into account, we observe from the figure that the recovery is very high. The transfer of recovered class of nodes to susceptible class of nodes is depicted in Fig. 7, whereas, the dynamical behavior of vaccinated class of nodes versus susceptible class of nodes is depicted in Fig. 8. If we have a proper vaccination given to the sensor nodes, the susceptibility towards the attack of worms will be very low. The study will help the software organization in developing highly efficient antivirus software to minimize the attack of malicious signals in the sensor nodes. Also the study will give an idea to the end users for proper vaccination and regular use of antivirus software to the sensor nodes in the sensor field for making the defense mechanism strong and to minimize the attacks.

References

[1] S. Tang, W. Li, Qos supporting and optimal energy allocation for a cluster-based wireless sensor network, Comput. Commun. 29 (2006) 2569–2577.
[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on networks, IEEE Commun. Mag. 40 (8) (2002).
[3] S.Stantiford, V. Paxton, Weaver, in: Proc. Of the 11th USENIX Security Symposium (Security '02), 2000.
[4] T.M. Chen, J-M Robert, IEEE Comput. (2004) 48–53.
[5] R. Pastor-Satorras, A. Vespignani, Evolution and Structure of the Internet: A Statistical Physics Approach, Cambridge University Press, Cambridge, UK, 2004.
[6] P. Szor, The Art of Computer Virus Research and Defense, Symantec Press, 2006.
[7] N. Levitt, IEEE Comput. 38 (4) (2005) 20–23.
[8] D. Dagon, T. Starnear, IEEE Pervas. Comput. 3 (2004) 11–15.
[9] E. Chien, Security response: symbos.mabir, Tech. Rep., Symantec Corporation, 2005.
[10] Bimal Kumar Mishra, Dinesh Kumar Saini, SEIRS epidemic model with delay for transmission of malicious objects in computer network, Appl. Math. Comput. 188 (2) (2007) 1476–1482.
[11] Bimal Kumar Mishra, Dinesh K Saini, Mathematical models on computer virus, Appl. Math. Comput. 187 (2) (2007) 929–936.
[12] Bimal Kumar Mishra, Navnit Jha, Fixed period of temporary immunity after run of anti-malicious software on computer nodes, Appl. Math. Comput. 190 (2) (2007) 1207–1212.
[13] E. Gelenbe, Dealing with software viruses: a biological paradigm, Inform. Security Tech. Rep. 12 (4) (2007) 242–250.
[14] Erol Gelenbe, Dealing with software viuses under control, in: 20th International Symposium on Computer and Information Sciences – ISCIS 2005, Lecture Notes in Computer Science, vol. 3733, Springer, 2005.
[15] Erol Gelenbe, Varol Kaptan, Yu Wang, Biological metaphor for agent behavior, in: 19th International Symposium on Computer and Information Science-ISCIS 2004, Lecture Notes in Computer Science, vol. 3280, Springer-Verlag, 2004, pp. 667–675.
[16] J.R.C. Piqueira, F.B. Cesar, Dynamical models for computer virus propagation, Math. Prob. Eng. dio: 101155/2008/940526.
[17] J.R.C. Piqueira, B.F. Navarro, L.H.A. Monteiro, Epidemiological model applied to virus in computer networks, J. Comput. Sci. 1 (1) (2005) 31–34.
[18] S. Forest, S. Hofmeyr, A. Somayaji, T. Longastaff, Self-nonself discrimination in a computer, in: Proceeding of IEEE Symposium on Computer Security and Privacy, 1994, pp. 202–212.

[19] Y. Wang, C.X. Wang, Modeling the effect of timing parameters on virus propagation, in: 2003 ACM Workshop on Rapid Malcode, ACM, October 2003, pp. 61–66.
[20] W.O. Kermack, A.G. Mckendrick, Contributions of mathematical theory to epidemics, Proc. R. Soc. Lond. – Ser. A 115 (1927) 700–721.
[21] W.O. Kermack, A.G. Mckendrick, Contributions of mathematical theory to epidemics, Proc. R. Soc. Lond. – Ser. A 138 (1932) 55–83.
[22] W.O. Kermack, A.G. Mckendrick, Contributions of mathematical theory to epidemics, Proc. R. Soc. Lond. – Ser. A 141 (1933) 94–122.
[23] Bimal Kumar Mishra, Samir Pandey, Dynamic model of worms with vertical transmission in computer network, Appl. Math. Comput. 217 (2011) 8438–8446.
[24] C.C. Zou, W.B. Gong, D. Towsley, L.X. Gao, The monitoring and early detection of internet worms, IEEE/ACM Trans. Network 13 (5) (2005) 961–974.
[25] J.O. Kephart, S.R. White, D.M. Chess, Computers and epidemiology, IEEE Spectrum (1993) 20–26.
[26] M.J. Keeling, K.T.D. Eames, Networks and epidemic models, J. R. Soc. Interf. 2 (4) (2005) 295–307.
[27] Ma. M. Williamson, J. Leill, An epidemiological model of virus spread and cleanup, 2003, <http://www.hpl.hp.com/techreports/>.
[28] M.E.J. Newman, S. Forrest, J. Balthrop, Email networks and spread of computer virus, Phys. Rev. E 66 (2002). 035101-1-035101-4.
[29] M. Draief, A. Ganesh, L. Massouili, Thresholds for virus spread on networks, Ann. Appl. Prob. 18 (2) (2008) 359–378.
[30] Ping Yan, Shengqiang Liu, SEIR epidemic model with delay, J. Aust. Math. Soc. Ser. B – Appl. Math. 48 (1) (2006) 119–134.
[31] J.O. Kephart, A biologically inspired immune system for computers, in: Proceedings of International Joint Conference on Artificial Intelligence, 1995.
[32] N. Madar, T. Kalisky, R. Cohen, D. Ben Avraham, S. Havlin, Immunization and epidemic dynamic in complex networks, Eur. Phys. J.B 38 (2004) 269–276.
[33] R. Pastor-Satorras, A. Vespignani, Epidemics and Immunization in Scale-Free Networks, Handbook of Graphs and Networks: From the Genome to the Internet, Wiley-VHC, Berlin, 2002.
[34] R.M. May, A.L. Lloyd, Infection dynamics on scale – free networks, Phys. Rev. (E) 64 (066112) (2001) 1–3.
[35] S. Datta, H. Wang, The effectiveness of vaccination on the spread of email – borne computer virus, in: IEEE CCECE/CCGEI, IEE, May 2005, pp. 219 – 223.
[36] C.C. Zou, W. Gong, D. Towsley, Worm propagation modeling and analysis under dynamic quarantine defense, in: Proceedings of the ACM CCS Workshop on Rapid Malcode, ACM, 2003, pp. 51–60.
[37] D. Moore, C. Shannon, G.M. Voelker, S. Savage, Internet quarantine: requirements for containing self – propagating code, in: Proceedings of IEEE INFOCOM 2003, IEEE, 2003.
[38] T. Chen, N. Jamil, Effectiveness of quarantine in worm epidemics, in: IEEE International Conference on Communications 2006, IEEE, 2006, pp. 2142–2147.
[39] J.-L. Sanders, Quantitative guidelines for communicable disease control programs, Biometric 27 (1971) 883–893.
[40] H.W. Hethcote, An immunization model for a heterogeneous population, Theor. Popul. Biol. 14 (1978) 338–349.
[41] R. Pastor–Satorras, A. Vespignani, Epidemic spreading in scale-free networks, Phys. Rev. Lett. 86 (2001) 3200–3203.
[42] M.E.J. Newman, Spread of epidemic disease on networks, Phys. Rev. E 66 (2002) 1–11.
[43] Y. Moreno, M. Nekovee, A. Vespignani, Efficiency and reliability of epidemic data dissemination in complex networks, Phys. Rev. E 69 (2004) 1–4.
[44] A. Khelil, C. Becker, J. Tian, K. Rothermel, Directed-graph epidemiological models of computer viruses, in: Proc. Fivth ACM Int. Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, 2002, pp. 54–60.
[45] S.A. Khayam, H. Radha, A topologically-aware worm propagation model for wireless sensor networks, in: Proc. Second Int. workshop on Security in Distributed Computing Systems, 2005, pp. 210–216.
[46] H. Zheng, D. Li, Z. Gao, An epidemic model of mobile phone virus, in: First Int. Symposium on Pervasive Computing and Applications, 2006, pp. 1–5.
[47] P. De, Y. Liu, S.K. Das, Modeling node compromise spreading in wireless sensor networks using epidemic theory, in: Proc. IEEE WoWMoM 2006, (Niagara-Falls, NY), June 2006.
[48] P. De, Y. Liu, S.K. Das, An epidemic theoretic framework for evaluating broadcast protocols in wireless sensor networks, in: Proc. IEEE (Int'l Conf. on Mobile Adhoc and sensor systems (MASS), (Pisa, Italy), Oct. 2007.
[49] J.K. Hale, Ordinary Differential Equations, second ed., Krieger, Basel, 1980.
[50] Bimal Kumar Mishra, Prasant Kumar Nayak, Navnit Jha, Effect of quarantine nodes in SEQIAmS model for the transmission of malicious objects in computer network, Int. J. Math. Model. Simul. Appl. 2 (1) (2009) 102–113.
[51] R.S. Varga, Matrix Iterative Analysis, Prentice-Hall Inc., Englewood cliffs, N.J, 1962.