Analysis of Epidemic Model for Performance Evaluation of Rechargeable Wireless Sensor Network

DOI : 10.36909/jer.ICCEMME.15847

Shashank Awasthi[1,3], Naresh Kumar[1], Pramod Kumar Srivastava[2*], Rudra Pratap Ojha[3]
[1]*Department of Computer Science & Engineering, Galgotias University Uttar Pradesh, India.*
[2]*Department of Mathematics, Rajkiya Engineering College, Azamgarh, Uttar Pradesh. India*
[3]*Department of Computer Science & Engineering, G.L.Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India*

* Corresponding Author: pramodksrivastava24042004@gmail.com

ABSTRACT

Wireless sensor network (WSN) is a decentralized network system which consists of sensor nodes, and these nodes are connected through wireless link. Due to decentralized network system and resource constraint WSN faces security threat. Malware (malicious signals, worm, Trajan horse, virus etc.) attacks on the sensor node of WSN and make them paralyze and steal information from the network. Malware attack also increases the energy consumption of Sensor nodes of WSN. It just begins to spread from an infected node, and spread across the entire WSN with the help of neighboring nodes. Therefore, security of WSN against attack of malware is an inescapable need. On the basis of earlier works and consideration of charging mechanism of sensor nodes, and considering the effect of coverage and connectivity, proposed a SILRD (Susceptible - Infectious – Low Energy – Recovered –Dead) model with vital dynamics. The propose model investigates the dynamics of malware propagation in WSN and also explain sensor node's energy consumption. The system's stability has analyzed in terms of local and global of malware-free and endemic equilibrium. For the investigation of system dynamics, the expression of basic reproduction number has computed, which is also utilized to analyze state of malware in WSN. The effect of charging, coverage and connectivity is explained in this paper.

The proposed model provides a better mechanism to prevent transmission of malware in WSN in comparison to existing models, which is validated through mathematical calculation as well as simulation results.

Keywords: Basic Reproduction Number, Coverage and Connectivity, Energy, Malware, Stability, Wireless Sensor Network.

INTRODUCTION

The use of WSN is increasing day-by-day with rapid development of new communication technologies. WSN encompasses a collection of sensor nodes, which are distributed either randomly or in a fixed manner (Guiyun et al.,2021). The sensor nodes can be installed anywhere as per the requirement for the purpose of monitoring and tracking. The unique characteristics possess by WSN so it becomes enable to play an important role in different area of applications such as smart home, smart grid, agriculture, military, health, intelligent transport system and industry, etc. (Liping et al., 2015). The primary objective of sensor nodes is to gather the environmental data from vicinities and transfer them to neighbouring sensor nodes, control centre/sink node. The control centre/sink node far away from the sensor nodes that may not be access directly, therefore to use multi-hop for delivering of the data at desired location. Due to constraint of resources WSN faces different types of challenges like energy, malware attack, coverage and connectivity, etc.

Limited energy is one the critical problem with WSN. Therefore, to mitigate the shortage of energy uses certain energy harvesting method, in which each sensor nodes are equipped with energy harvesters (Guiyun et al.,2020). Along with short lifespan of WSN, security is another typical issue associated with them. These are issues are need to address on priority basis. The topology of WSN provides a hotbed for the propagation of malware. The defense capabilities of WSN is weak, therefore malware exploit the vulnerability of sensor nodes and invade on them. Due to attack of malware paralyze the system and leads a huge economic loss. With increasing the applications of WSN in all walk of life its security also become an important issue among the researchers and industry. Therefore, to undertake the method of malware prevention in WSN, it is important to comprehend the dynamic characteristics of malwares propagation first. Malware propagation process in WSN is alike to the spreading of infectious disease in susceptible population. Thus, the epidemiology is useful to investigate the dynamic characteristics of malware in WSN. The numerous epidemic models have been developed on the basis SIR (Susceptible-Infected-Recovered) model which was first proposed in 1927 by Kermack and McKendrick (Kermack et al., 1927).

Like computer viruses, malwares also spread in WSN. WSN uses wireless communication for data transmission. Therefore, the vulnerability of WSN is more in comparison to computer network (Liang et al., 2017). The propagation of malware in WSN is affected by various factors for example sensor node's communication radius of, distribution of node density (Liping et al., 2015, Singh et al. 2018, Ojha et al., 2020), spatial correlation (Shakya et al., 2019), transmission delay (Upadhyay & Kumari, 2018), coupling degree (Qu, and Wang, 2017) and geospatial limitations (Haghighi et al. 2016).

Many researchers have investigated the propagation dynamics of malware in order to provide a better protection mechanism against malware attack in WSN (Tang and Li ,2011, Liping et al., 2015, Singh et al. 2018, Ojha et al., 2020). Tang and Li (Tang and Li , 2011) analysed the spread of virus in WSN using traditional SI and modified SI model. The better security mechanism for WSN against virus attack is provided by modified SI model. Further, Tang et al. (Tang, et al.,2013) proposed a modified SIS model to analyse the process of virus spreading in the whole WSN. The mechanism of nodes recovery from infection is demonstrated. Liping et al. (Liping et al.,2015,) introduced a SIRS model to describe the dynamics of worm dissemination in WSN. They also explain the effect of coverage and connectivity on worm propagation.

Malware propagation leads to failure or paralyze WSN operations. Due to malware attacks information of the network may be leak and some economic losses also faced. Therefore, it is necessary to apply the corrective measures to ensure WSN security against malware attack. Liu et al. (Liu, et al. 2020) introduced the idea of low energy state and classify the sensor nodes of the network. They proposed an epidemic based SILRD model that explains the dynamics of malware propagation in WSN. For optimum use of energy and deterrence of malware infection spread in the sensor network they applied the method of game theory. Further, they extended the model (Liu, et al. 2020) with consideration of energy harvesting. They compare the proposed model with without energy harvesting epidemic models. They did not consider stability issues, WSN equilibrium and basic reproduction number, effects of coverage and connectivity of malware spread. The effects of communication radius on malware propagation speed are not analyzed. This is one of the critical design issues. Another point of discussion is distributed node density, which is also one of the important problems needs be to address.

This article explores the dynamics of malware propagation and tries to develop a model which is use to thwart the malware attacks in WSN. Furthermore, it configures the effects of charging, coverage and connectivity on propagation of malware and curtail the damaging impact in WSN which is caused due to attacks of malware. To analyze the propagation dynamics of malware in WSN, an epidemic model which contains five epidemic states namely Susceptible-Infectious- Low Energy -Recovered-Dead (SILRD) having different properties is proposed.

The key intent of the proposed model is to monitor the occurrence of malicious signals in the network and appropriately appertain counteractive procedures to prevent the attack in WSN. Summary of the contributions are as.

1. The proposed model is used to analyze the malware propagation dynamics in WSN, using the concept of epidemiology. The basic nature of malware propagation and communicable diseases spreading are similar, so the proposed model will provide the understanding of malware propagation dynamics and defend WSN against malware attacks.

2. Sensor nodes are energy-limiting devices; their energy is spent during operation, and they enter into a low-energy state. Due to attacks of malware consumption of sensor node’s energy increases. The coverage area or communication radius of sensor node also effect the energy consumption of sensor node. Therefore, it is required to develop a model which can prevent malware spread and minimize the consumption of sensor node’s energy. Thus, in this model the low energy state is considered and a mechanism of charging is applied to overcome the problem of energy consumption as well as security of WSN.

3. The method of next generation matrix is used to calculate the basic reproduction number,

which is used to analyze the system dynamics in different conditions.

4. The system stability and equilibrium points are also analyzed and studied the effects of various parameters of the system responsiveness.

5. The effects of low energy state and recovery state is investigated and analyze their effect on malware propagation and lifetime of WSN.

6. To validate the correctness and effectiveness of the proposed model analytical findings are verified by extensive simulation outcomes.

PROPOSED MODEL AND ASSUMPTIONS

The proposed model depicts the malware propagation dynamics in WSN. The impact of sensor nodes charging on malware dissemination and stability of the system is explained. The core aim of the proposed model is to protect WSN from malware attack, improve the stability of the network, and extend the lifespan of WSN. The proposed model is made up of five distinct epidemic states:

Susceptible State (S): a sensor node which is vulnerable to malware attack due to lack of protection. The consumption of node's energy is normal without malware attack.

Infectious State (I): a sensor node which has been compromised with malware and having the capacity to infect neighboring sensor nodes. The infected sensor node's energy consumption accelerates. Therefore, it is important to patched or charged these nodes on time otherwise they will die due to loss of node's energy.

Low-Energy State (L): sensor nodes are in low energy state; they are infected by malware and its energy consumption level is normal. These nodes are considered as low energy category which are not capable to perform normal network operations also such as data transmission to the neighboring nodes.

Recovered State (R): sensor nodes those are immune to malware attacks and have recovered from an infectious condition. The recovered nodes not only having the immunity they also have high energy level.

Dead State (D): sensor nodes are fully dysfunctional. The nodes are likewise unable to function after charging. They are not able to communicate and infect with other nodes of the network due to complete loss of energy.

Initially, every sensor node of WSN is susceptible and which can be targeted by malware. The sensor node's transition state diagram is illustrated in the Fig. 1.

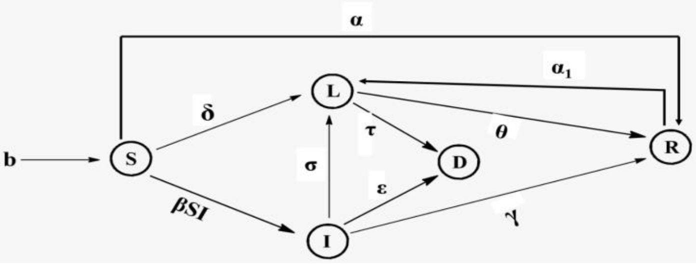

Figure 1: Transition State Diagram of SILRD Model

At any time $t \geq 0$, the aggregate count of nodes in WSN is N(t) and satisfies the condition N(t) = S(t) + I(t) + L(t)+ R(t) + D(t).

For the system analysis the following assumptions are made:

1. At the time of sensor node deployment each node of WSN is in state of susceptible and away from the malwares, but they are vulnerable to malwares. Sensor nodes are full of energy, malware can be implant artificially in WSN to destroy the node of WSN or steal the information. Sensor nodes loss its energy due to normal operation but rate of battery consumption increases when attacked by malware and move to low energy state at the rate of δ. Some of the susceptible sensor node come into contact with malware and become infected with probability β is βSI. By installing patches some of the susceptible sensor nodes achieve immunity against this kind of malware move to recovered state with rate of α.

2. The infection rate of malware affects the transition rate of susceptible number of nodes transfer into infected state. The energy consumption of infected sensor nodes increases with damaging degree of malware attacks and these nodes move at fast rate into dead state with probability of ε. Some of the sensor nodes of the network are infectious but not continuously attacked by the malware and they get immune by patch on time move into recovered state with the rate γ.

3. Recovered state nodes are immune as well as high energy state nodes. Recovered state nodes come from susceptible and infectious states and they are patched without charging. On the other hand, low energy state nodes required to patched and charged simultaneously to convert into recovered state with probability ɵ. The recovered state nodes exhaust their energy due to normal operation and move into low energy state at the rate α_1.

4. The low energy state nodes those are not immune exhaust their energy rapidly and move into dead state with the rate of τ and on the other hand immune nodes with low energy charged and move into recovered state. Dead state nodes cannot transmit the data and malware to other nodes of the network and they cannot be charged.

MATHEMATICAL FORMULATION AND ANALYSIS

At time t, the network contains $N(t)$ number of nodes and they are spread equally over the defined region. A sensor node's transmission area is πr^2 with communication radius r, and the susceptible node density in a unit area is $\rho(t) = \frac{S(t)}{L^2}$ and $S'(t) = \frac{\pi r^2 S(t)}{L^2}$ denotes the total number of adjoining nodes which are inside a susceptible sensor node's sensing region. The sensor nodes are scattered at random and have an equal chance of contacting one another. The charging of low-energy nodes is used to prevent malware spreading and to keep the network stable. An ordinary differential equation is used to explain malware propagation dynamics in WSN. A set of differential equations is developed to characterize the dynamics of malware.

$$\left.\begin{aligned}
&\dot{S} = b - \frac{\pi r^2}{L^2}\beta SI - \alpha S - \delta S,\\
&\dot{I} = \frac{\pi r^2}{L^2}\beta SI - (\gamma + \sigma + \varepsilon)I,\\
&\dot{L} = \sigma I + \alpha_1 R + \delta S - (\theta + \tau)L\\
&\dot{R} = \theta L + \alpha S + \gamma I - \alpha_1 R,\\
&\dot{D} = \tau L + \varepsilon I,
\end{aligned}\right\} \qquad (1)$$

The system of equation (1) may be expressed as: $\phi = \frac{\pi r^2}{L^2}\beta$ for convenience

$$\left.\begin{aligned}
&\dot{S} = b - \phi SI - \alpha S - \delta S,\\
&\dot{I} = \phi SI - (\gamma + \sigma + \varepsilon)I,\\
&\dot{L} = \sigma I + \alpha_1 R + \delta S - (\theta + \tau)L\\
&\dot{R} = \theta L + \alpha S + \gamma I - \alpha_1 R,\\
&\dot{D} = \tau L + \varepsilon I,
\end{aligned}\right\} \tag{2}$$

The b is the probability of new nodes addition in WSN, transition probability of susceptible state to low energy state is δ. The rate of malware propagation from susceptible to infectious state is β, infectious nodes loss their energy and move into low energy state with probability σ. Infectious and low energy state nodes transit into dead state with probability ε and τ respectively, low energy nodes of the network patched and charged at rate move into recovered state with high energy state and α_1 is the rate at ө to transit into recovered state. Infectious nodes patched at rate γ to move into recovery state. The proposed system is defined in the domain $\Gamma = \{(S, I, L, R, D) \in \Re_+^5\}$. Subsequently, the model monitors distinct state of nodes, thus, each state variables continue to be non-negative for all $t \geq 0$.

EXISTENCE OF MALWARE-FREE EQUILIBRIUM

From equation (2) it is clear that nodes of class D does not appear in the first four equations of (2). It means that four equations are independent of the fifth equation, therefore for determining the equilibrium points of the system taking the first order derivatives of system of equation is equal to zero.

$$\left.\begin{aligned}
&0 = b - \phi SI - \alpha S - \delta S,\\
&0 = \phi SI - (\gamma + \sigma + \varepsilon)I,\\
&0 = \sigma I + \alpha_1 R + \delta S - (\theta + \tau)L\\
&0 = \theta L + \alpha S + \gamma I - \alpha_1 R,
\end{aligned}\right\} \tag{3}$$

Solving equation 3 yields the system's equilibrium points. The malware-free equilibrium (MFE) point is: $P_0^{MFE} = (S_0, I_0, L_0, R_0) = \left(\frac{b}{\alpha+\delta}, 0{,}0, \frac{\alpha b}{\alpha_1(\alpha+\delta)}\right)$

STABILITY ANALYSIS OF THE PROPOSED MODEL

Local and Global Stability Analysis of Malware Free Equilibrium

One of the most important issues is the system stability when malware enter in the system. Some theorems have been established to examine the stability of the proposed system, and the network's stability has been determined on the basis of following theorems:

Theorem 1: At Malware Free Equilibrium (MFE) P_0^{MFE} , if $R_0 < 1$ then the system represented in (2) is locally asymptotically stable otherwise unstable when $R_0 > 1$.

Proof. To determine the system's stability of point P_0, it is necessary to first form Jacobian matrix that helps in determination of eigenvalue values. The corresponding Jacobian matrix is

$$J(P_0^{MFE}) = \begin{pmatrix} -(\alpha+\delta) & -\phi S_0 & 0 & 0 \\ 0 & \phi S_0 - (\gamma+\sigma+\varepsilon) & 0 & 0 \\ \delta & \sigma & -(\theta+\tau) & \alpha_1 \\ \alpha & \gamma & \theta & -\alpha_1 \end{pmatrix} \qquad (4)$$

Two Eigenvalues of (4) are: $\kappa_1 = -(\alpha+\delta), \kappa_2 = \frac{1}{\varepsilon+\gamma+\sigma}(R_0 - 1)$ and other two eigen value is the roots of equation $b_0\kappa^2 + b_1\kappa + b_2 = 0$, where $b_0 = 1$, $b_1 = (\alpha_1 + \theta + \tau)$ and $b_2 = \alpha_1$. Since all coefficients $a_0, a_1$and a_2 are positive. Therefore, it is clear that all eigenvalues of the matrix are non-positive when $R_0 < 1$ and if $R_0 > 1, \kappa_2 > 0$. As a result, at malware-free equilibrium the system is locally asymptotically stable at $P_0$when $R_0 < 1$and otherwise unstable when $R_0 > 1$.

Theorem 2: The Malware Free Equilibrium (MFE) P_0^{MFE} is globally asymptotically stable if $R_0 \leq 1$.

Proof. Assume the Lyapunov function as follows:

$L(t): \mathbb{R}^4 \to \mathbb{R}^+$ defined by $L(t) = \omega I$ (5)

Differentiate equation (5), we get $\overset{\bullet}{L} = \omega \overset{\bullet}{I} = \omega(\phi S I - (\gamma + \sigma + \varepsilon)I) \leq (R_0 - 1)I$, where $\omega = \frac{1}{(\gamma+\sigma+\varepsilon)}$. If $R_0 \leq 1$ then $\overset{\bullet}{L} \leq 0$ holds. Moreover $\overset{\bullet}{L} \leq 0$, if and only if $I = 0$. Thus, the largest invariant set in $\left\{(S, I, L, R, D) \in \Gamma: \dot{L} \leq 0\right\}$ is the singleton set P_0. Thus the global stability of P_0^{MFE} when $R_0 \leq 1$, according to LaSalle's (LaSalle, J.P.,1976) invariance principle.

Malware Endemic Equilibrium: Existence & Uniqueness

In this section, we investigate the existence and uniqueness of the endemic equilibrium.

For malware endemic equilibrium (MEE) point,

$$\left.\begin{aligned}
&0 = b - \phi S^{*} I^{*} - \alpha S^{*} - \delta S^{*},\\
&0 = \phi S^{*} I^{*} - (\gamma + \sigma + \varepsilon) I^{*},\\
&0 = \sigma I^{*} + \alpha_1 R^{*} + \delta S^{*} - (\theta + \tau) L^{*}\\
&0 = \theta L^{*} + \alpha S^{*} + \gamma I^{*} - \alpha_1 R^{*},
\end{aligned}\right\} \qquad (6)$$

By straight-forward calculation malware -endemic equilibrium (MEE) P^{*MEE}point is given by

$$S^{*} = \frac{b}{(\alpha+\delta)R_0},\ I^{*} = \left[\frac{b(R_0-1)}{(\gamma+\sigma+\varepsilon)R_0}\right], L^{*} = \frac{1}{\psi}\left[(\sigma+\gamma)I^{*} + (\alpha+\delta)S^{*}\right], R^{*} = \frac{1}{\alpha_1}\left[\gamma I^{*} + \alpha S^{*} + \theta L^{*}\right]$$

where $R_0 = \frac{\phi b}{(\gamma+\sigma+\varepsilon)(\alpha+\delta)}$is the basic reproduction number (Diekmann, et al.1990). It is clear that malware endemic equilibrium (MEE) point exists & unique when $R_0 > 1$.

Local Stability Analysis of Malware Endemic Equilibrium

In this section, the local stability analysis of malware endemic equilibrium point $P^{*MEE} = (S^{*}, I^{*}, L^{*}, R^{*})$ is given. The Jacobian matrix is

$$J(P^{*MEE}) = \begin{pmatrix} -(\phi I^{*} + \alpha + \delta) & -\phi S^{*} & 0 & 0 \\ \phi I^{*} & \phi S^{*} - (\gamma + \sigma + \varepsilon) & 0 & 0 \\ \delta & \sigma & -(\theta + \tau) & \alpha_1 \\ \alpha & \gamma & \theta & -\alpha_1 \end{pmatrix} \qquad (7)$$

Theorem.3. At Malware Endemic Equilibrium (MEE) P_0^{MEE} , if $R_0 > 1$ then the system represented in (2) is locally asymptotically stable.

Proof. To determine the system's stability at the point P^{*MEE}, compute the eigen values of matrix (7). Eigen values of the Jacobian matrix are the roots of the equation

$$a_0\kappa^4 + a_1\kappa^3 + a_2\kappa^2 + a_3\kappa + a_4 = 0 \qquad (8)$$

where, $a_0 = 1, a_1 = (L_1 + M_1), a_2 = (L_2 + L_1M_1 + M_2), a_3 = (L_1M_2 + L_2M_1), a_4 = L_2M_2$ and

$$L_1 = (\theta + \tau + \alpha_1), L_2 = \tau\alpha_1, M_1 = \alpha + \delta + \gamma + \sigma + \varepsilon + \frac{\phi b}{R_0}\left[\frac{(R_0 - 1)(\alpha+\delta) - (\gamma+\sigma+\varepsilon)}{(\alpha+\delta)(\gamma+\sigma+\varepsilon)}\right], M_2 = (\alpha+\delta)(\gamma+\sigma+\varepsilon) + \frac{\phi b}{R_0}[R_0 - 1]$$

The coefficients of equation (8) are satisfied the Routh-Hurwitz criteria for the fourth-degree polynomial if $R_0 > 1$; which implies that all eigen values have a negative real part and therefore the system is locally asymptotically stable at malware endemic equilibrium point P^{*MEE}.

MALWARE PROPAGATION THRESHOLD ANALYSIS AND SIMULATION RESULTS

Compute the basic reproduction number (R_0) to analyze system dynamics in different conditions. To obtain the threshold value of R_0, R_0 equates to one. If the value of $R_0 < 1$, malwares in WSN can be exterminated, and system (2) will stabilize at malware free equilibrium. Whereas, if $R_0 > 1$malwares will persist continuously in WSN, and system (2) will stabilize at the endemic equilibrium. To validate the correctness of theoretical study, the analytical simulation has performed.

Node Communication Radius

We know that, $R_0 = \frac{\phi b}{(\gamma+\sigma+\varepsilon)(\alpha+\delta)}$ (9)

For finding threshold value, replace $R_0 = 1$in equation (9), we get

$$r_{th} = L\left(\frac{(\gamma+\sigma+\varepsilon)(\alpha+\delta)}{\pi\beta b}\right)^{1/2} \qquad (10)$$

Taking the values of different parameters are as: $b = 0.37, \beta = 0.002,\ \alpha = 0.0006, \delta = 0.0008, \gamma = 0.007, \sigma = 0.006,$ ɵ $= 0.004, \tau = 0.003, \alpha_1 = 0.003, r = 0.9, L = 12, \varepsilon = 0.0015$ and the value of $R_0 = 0.644.$ Change only the value of $r = 2.2$ and others values remain same the value of $R_0 = 3.847.$ The threshold value of communication radius $r_{th} = 1.122.$ When $r \le r_{th}, r \le r_{th}$, ($R_0 = 0.644$), with the assistance of theorem 2, it proves that eradicate malware from the system and WSN will become stable at malware free equilibrium P^{*MFE}, which is shown by Fig.2 (a). According to theorem 3, when $r > r_{th}$, $R_0 > 1$ ($R_0 = 3.847$). As a result, malware will always exist in the system, and WSN will become stable at endemic equilibrium P^{*MEE},which is shown in Fig. 2 (b).

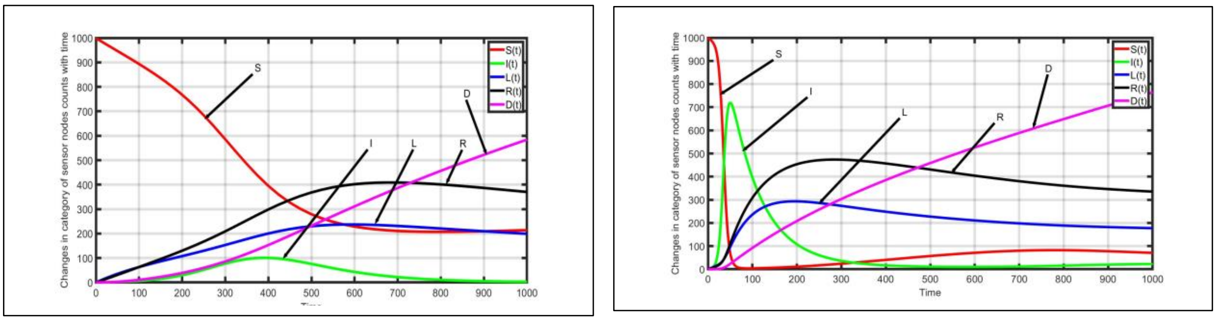

Figure 2: System dynamics when (a) r = 0.9 and (b) 2.2

from Fig. 2 (a) and 2(b) that when the value of r increases the connectivity will improve. But on the other hand, the value of R_0 also increases with increase in r. Since R_0 is proportional to r^2, the system acquires endemic status as the value of r increase. So, for designing of WSN threshold value of communication radius is important.

Node Distributed Density

Taking the value of $R_0 = 1$, to find the threshold value of node density $\rho_{th} = N/L^2$

$$1 = \rho_{th}\frac{\pi r^2 b\beta}{N(\gamma+\sigma+\varepsilon)(\alpha+\delta)} \Rightarrow \rho_{th} = \frac{N(\gamma+\sigma+\varepsilon)(\alpha+\delta)}{\pi r^2 b\beta} \qquad (11)$$

All the parametric values in case of communication radius are same and some other values are as: $r = 1.0, 0.37,\ N = 1000$, the threshold value of node density $\rho_{th} = 8.736$. Taking the value of $L = 12$ then $\rho = 6.94$ and $R_0 = 0.79$. Changing only the value of $L = 5$ and others values remain same the value of $\rho = 40$ and $R_0 = 4.578$. When $\rho \le \rho_{th}$, $R_0 \le 1$ ($R_0 = 0.79$), with the assistance of theorem 2, it proves that eradicate malware from the system and WSN will become stable at malware free equilibrium P^{*MFE}, which is shown by Fig.3(a). Malware propagation will be controlled. According to theorem 3, when $\rho > \rho_{th}$ and $R_0 > 1$ ($R_0 = 4.578$). In this situation, malware will always be existed in the system, and WSN will become stable at endemic equilibrium P^{*MEE}, which is shown in Fig.3(b).

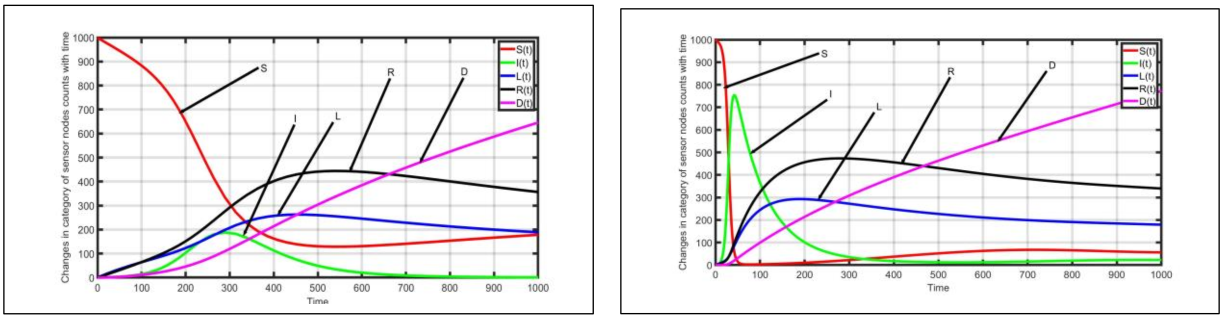

Figure 3: System dynamics when (a) ρ = 6.94 and (b) ρ =40

From Fig. 3(a) and 3(b), we found that as the value of node density is increasing the value of R_0 also increasing. Therefore, it is necessary to understand the requirement of node deployment in the designated area. When spacing between nodes are very close connectivity will be strong but malware propagation will be also fast. So, keep these parameters at the time of develop a WSN.

Comparison with Previous Model

The proposed model compares with the SIRS model (Liping et al., 2015) under the similar condition by varying the value of communication radius.

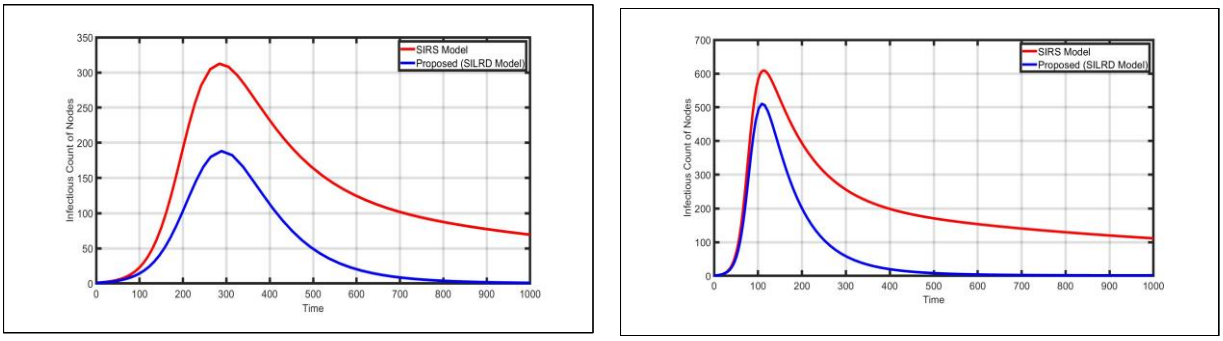

Figure 4: Comparison with previous SIRS model (a) r = 1.0 and (b) 1.5

Fig. 4 (a) and 4(b) show the comparative analysis between previous SIRS model and proposed SILRD model. It is found from analysis the lesser count of susceptible sensor nodes attacked by the malware in proposed model with respect to the previous model. So, proposed model's performance is better in controlling and preventing malware propagation in WSN.

RESULT AND DISCUSSION

The proposed model based on epidemic modeling is developed which describes propagation dynamics of malware in WSN. The concept of low energy node along with communication radius and distributed node density is introduced in this paper. The effect of charging is also discussed. The equilibrium points of the malware free and endemic is also obtained. The expression for reproduction number R_0 is obtained and found from analysis if $R_0 < 1$ then the malware-free equilibrium is globally asymptotically stable and malware will be disappeared from the network. Otherwise, if $R_0 > 1$ malware will survive in the network. The effects of communication radius on propagation of malware are discussed and compute its threshold value which help in designing of WSN. The role of distributed node density is also discussed. The coverage and connectivity of network and its effect on malware propagation is described. Comparative study between previous model and proposed model is also discussed and proposed model provides better malware control mechanism in comparison to previous model. In future discussion include the quarantine and vaccination state.

REFERENCES

Liu, G., Peng, B., & Zhong, X. 2021. Epidemic Analysis of Wireless Rechargeable Sensor Networks Based on an Attack–Defense Game Model. Sensors, 21(2), 594.

Liping, F., Song, L., Zhao, Q., & Wang, H. 2015. Modeling and stability analysis of worm propagation in wireless sensor network, Mathematical Problems in Engineering, 2015, 1–8.

Liu, G.Y., Peng, B.H., Zhong, X.J., Cheng, L.F., & Li, Z.F. 2020. Attack-Defense Game between Malicious Programs and Energy-Harvesting Wireless Sensor Networks Based on Epidemic Modeling. Complexity 2020, 2020, 3680518.

Kermack, W. O., and McKendrick, A. G. 1927. A contribution to the mathematical theory of epidemics, vol.115, no. 772, 700-721. The Royal Society.

Liang, G., Weller, S. R., Zhao, J., Luo, F. & Dong, **Z. Y. 2017.** A framework for cyber topology attacks: line-switching and new attack scenarios, IEEE Transactions on Smart Grid, vol. 10, no. 2: 1704–1712.

Singh ,A., Awasthi, A., Singh K., & Srivastava P. K. 2018. Modeling and analysis of worm propagation in wireless sensor networks Wirel. Pers. Commun., vol. 98, no. 3: 2535–2551.

Ojha, R.P., Srivastava, P.K., Sanyal, G., & Gupta, N. 2020. Improved Model for the Stability Analysis of Wireless Sensor Network Against Malware Attacks. Wirel. Pers. Commun., doi:10.1007/s11277-020-07809-x.

Shakya, R. K., Rana, K., Gaurav, A., Mamoria, P., & Srivastava, P. K. 2019. Stability analysis of epidemic modeling based on spatial correlation for wireless sensor networks, Wireless Pers. Commun., vol. 108, no. 3: 1363–1377.

Upadhyay, R. K., & Kumari,S. 2018. Bifurcation analysis of an e-epidemic model in wireless sensor network, Int. J. Comput. Math., vol. 95, no. 9, pp. 1775–1805.

Qu, B. & Wang, H., 2017. SIS epidemic spreading with correlated heterogeneous infection rates, *Physica A: Statistical Mechanics and Its Applications*, vol. 472:13–24.

Haghighi, M. S., Wen, S., Xiang, Y., Quinn, B., & Zhou, W. L. 2016. On the race of worm and patches: modeling the spread of information in wireless sensor networks, IEEE Transct. on Information Forensics and Security, vol. 11, no. 12: 2854–2865.

Tang, S. &Wei Li. 2011. A modified SI epidemic model for combating virus spread in wireless sensor networks, Int. Journal of Wireless Information Networks, 18(4): 319–326.

Tang, S., David, M., & Jason, Y. 2013. Modified SIS epidemic model for analysis of virus spread in wireless sensor networks. Int. Journal of Wireless and Mobile Com., 6(2): 99–108.

Liu, G.Y., Peng,B. H., Zhong, X. J. & Lan, X. J. 2020. Differential games of rechargeable wireless sensor networks against malicious programs based on SILRD propagation model, Complexity, vol. 2020, Article ID 5686413, 13.

LaSalle, J.P. 1976. The stability of dynamical system, (SIAM, Philadelphia).

Diekmann, O. et al. 1990, On the definition and the computation of the basic reproduction ratio R_0 in models for infectious diseases in heterogeneous populations, Journals of Mathematical Biology 28(4):365-382