Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

Epidemiological Model for Stability Analysis of Wireless Sensor Network under Malware Attack

Chakradhar Verma*

*Corresponding author, Research Scholar, Rajasthan Technical University, Kota ,Rajasthan-324010, India, E-mail: chakradharverma@gmail.com

C. P. Gupta

Professor, Department of Computer Science and Engineering, Rajasthan Technical University, Kota Rajasthan -324010, India, E-mail: guptacp2@rediffmail.com

Abstract

Malware attack is growing day by day in cyberspace. And Wireless Sensor Network (WSN) is also facing a hazardous type of situation due to attack of malware (malicious code, virus, worm etc.). Malwares target sensor nodes easily because, nodes are equipped with limited resources. Hence, security of WSN against malware attack is one of the imperative requisite. Malware spreads in the entire network wirelessly, which initiates from single infectious node and spread in the whole WSN. In this way the complete network comes under the security threat. Therefore, it is mandatory to apply the security technique through which to secure WSN against malware attacks. To secure WSN due to malware attacks a quarantine based model has been proposed. The proposed model consists of various epidemic states namely: Susceptible Carrier - Infectious - Quarantine - Recovered - Susceptible (SCIQRS). The model explained the propagation dynamics of malware in WSN and proposed a technique to prevent its propagation. The technique of quarantine along with recovery is to much effective in prevailing of malware propagation in WSN. For the determination of WSN stability and equilibrium points the expression of basic reproduction number has been obtained. Malware propagation is affected by different network parameters, which has been also discussed. The comparative investigation of proposed model has been carried out with existing model. The proposed model has been substantiated by simulation outcomes.

Keywords: Basic Reproduction Number; Malware Security; Stability; Wireless Sensor Network;

DOI: 10.22059/jitm.2022.86484 Manuscript Type: Research Paper University of Tehran, Faculty of Management

Received January 07, 2021 Accepted March 25, 2021

Introduction

The world is coming closer day by day due to development of Internet technology. At the next stage of Internet technology emerging a new paradigm Internet of Things (IoT). That means everything connected through Internet. In this technology everywhere and every time people and object are connected. Sensor nodes are used in IoT technology (Singh, 2016) for collection of data. And large number of sensor nodes forms the Wireless Sensor Network (WSN). The security of WSN due to malware is one the crucial issue (Srivastava, 2016, Alaba, 2017, Ojha, 2020, Liu, 2021). WSN security due to malware attack becomes an important area of research because its applications growing rapidly day by day. The spreading pattern of malware in WSN is similar to spreading pattern of communicable disease in individuals. To analyze the study of malware spread in WSN need to address the concept of epidemic modeling.

For the study of communicable disease transmission among the people the concept of epidemic modeling is used. The epidemic modeling is a useful tool for study the behaviour infectious diseases spread, to predict outbreak of infectious diseases in future and accordingly help in the preparation of strategies to curb an epidemic (Tang Modified SIS). Generally, in case of epidemic modeling the total individuals is divided into three different groups namely: susceptible (S), infectious (I) and recovered (R). The fact is that every people in this world is in susceptible state (S) and they become infectious (I) when come into contact with virus (such as COVID-19, mumps or measles, chickenpox etc.). The group of people is in infectious state (I) get immune or recovered come into recovered state (R) after treatment. And recovered group of people may be further infected by same or a different kind of virus in future. A model consists of these three groups is said to be an SIR model. Other than older virus, recent day virus COVID-19 (Luo, 2020) also belongs to this category of model because till date no vaccine is available for this disease.

Considering the concept of epidemic modeling in communication network, such as Internet, Internet of Things (IoT), computer network, WSN, and it is realized that devices (nodes) of the network also infected by the software viruses and these can be recovered with the help of some techniques such as antivirus, but these recovered nodes again targeted by new type or the same virus in future. The pattern of malware propagation in communication network is similar to the biological worms (Mishra,2013).

The operation of WSN can be interrupted by malware attack and confidential data can be easily stolen (Bahi.,2014) by attacker. The basic characteristics of the biological agents (virus, bacteria, etc.), are similar to software created malwares. And the spreading nature of malware in WSN follows the epidemic characteristics. Malware spreads in WSN in epidemic manner and disturb the network stability. The epidemic models are used for the investigation of worm spreading in WSN. In these models, the sensor nodes of the network is divided into different states viz. susceptible, exposed, infectious, recovered states etc.(Mishra,2013,De.,P.2009). The worm-free nodes (or healthy nodes) come under the category of susceptible nodes. Susceptible nodes cab be attacked by the malicious codes and

converted into infectious state. The single infectious node communicated with neighbour nodes through data transmission and infects its neighbouring nodes. Similarly, in this manner all neighbour nodes come into contact with infectious node. Malware may be with data or wirelessely spread in the entire network.

Sensor nodes are vulnerable (De, 2009, Ojha,2018) due to limitations of resources. Therefore, malware can be easily makes victim of sensor nodes. Keep in the view of these limitations of sensor nodes, keeping in the view of these limitations of sensor nodes, a security mechanism is essential to prevent the malware. The hacker targets a node of the network and inject the malware into them after that the targeted node becomes infectious and start to spread the mal-ware through neighbour nodes in the complete WSN. Due to malware attacks nodes of WSN exhaust its energy, increase traffic flow in the network, etc. The malware attack can also steal or delete personal data, damage the devices and may cause of the economical crisis. The various models have been proposed by the different researchers to analyze the propagation of malware in WSN. And accordingly, they have proposed protection mechanisms for WSN against malware attack utilizing the concept of epidemic theory (Mishra,2013.De, 2009, Feng, 2015,Ojha,2018).

To secure WSN against malware attack the mechanism of malware detection and its elimination can be applied. Generally, the spreading dynamics of malware in WSN is investigated by mathematical model. And investigation model is formulated by the set of di-erential equations. The prime aim of the proposed model is to find out the appearance of malware in WSN and accordingly apply a suitable security measure to protect WSN. To prevent malware attacks on WSN, it is necessary to design a method for malware detection and its elimination. In a sensor network other than sensor nodes some carrier devices are also needed, these devices can be also targeted by malware. Guillen and Rey (Hernandez Guillen,2017) modelled and studied the carrier compartment effect of propagation of malware in the network. They discussed the various factors that impact the malware propagation in the network. The value of basic reproductive has been obtained and analyze explained how this is an important factor in developing of countermeasure of the malware attack on the network. Considering the characteristics of WSN. Rey et al. (Rey,2016) proposed a Susceptible-Carrier-Infectious-Recovered-Susceptible (SCIRS) model, in which included the carrier devices. And They studied the malware spreading in WSN. Further Guillen and Rey (Hernandez Guillen,2019) proposed an improved model over the earlier model and proposed a technique for controlling of malware spreading in WSN.

There are various area of research in WSN such as energy consumption, node deployment, security, transmission delay, etc., among of these in this pa-per, we are focusing on security as well as energy consumption of sensor nodes. It is observed that when malware attacks on WSN start flooding of data due to which energy consumption of sensor nodes increases. It is observed that when malware attacks on WSN start flooding of data due to which energy consumption of sensor nodes increases. Therefore, our objective is that to proposed a strong security method and investigate the effect of quarantine state (Q) against malware attack in WSN. This method prevents the malware attack in WSN and control its

spreading. In this paper, we proposed a SCIQRS model which is improvement over the SCIRS model. We will verify from experimental and analytical findings the proposed model works well.

The key goals of the proposed model is to undertake a method of quarantine of compromised nodes in WSN and remove malware from them. The contributions are listed as:

1. Develop a mathematical model based on epidemic modeling to investigate the spreading dynamics of malware in WSN and develop a method that can prevent the malware spreading in WSN.

2. Utilized the idea of quarantine class of epidemic model to stop further malware spread and save the energy of sensor nodes.

3. To investigate responsiveness of the system when malware attack and study steady state of the system.

4. To develop the mechanism for recovery of infected sensor nodes of WSN.

5. To investigate the equilibrium points and stability of the proposed system under the said conditions.

6. To verify the correctness of analytical findings of the proposed model through extensive simulation.

Remaining section of the paper is organized in the following order: the related work is presented in section 2. Details of the proposed model is presented in section 3. Equilibrium points Existence is discussed in Section 4; in section 5 system stability has been discussed with relevant theorems and their proof. In section 6 simulation results along with comparative analysis between existing model the proposed model is presented and finally in section 7 discussed conclusion and future work.

Background

In the beginning the application of WSN was for military (Yick,J.2008). It was used for monitoring and surveillance of enemies. WSN is an ad-hoc network system in which sensor nodes are distributed spatially. The applications of WSN is increasing rapidly due to integration of the different types of network such as IoT. With increasing of applications challenges are also appearing in the operations of WSN. Among the various challenges one of the challenge is malware attack, which has been discussed in introduction section.

For the study of malware spreading in WSN, the different types of models based on epidemic modeling has been presented by the number of researchers. First time Kermack and Mckendrick (kermack,1927) introduced the concept of epidemic modeling for the prediction of infection due to infectious disease in the population over time. Later on, for different purposes this concept is applying in diverse area of study, for example social network for the analysis of rumor spread (He,Z.,2015.,He,Z.2015.,2017) for malware spreading behaviour in computer network (Upadhyay,2017), mobile ad-hoc network, and WSN,

etc.(hayel,Y.2017.Wang,T.2017).

The classical SI (Susceptible - Infected) model was proposed by Khayam and Radha [28] for worm propagation study in the sensor network. They explained the effect of worm propagation in WSN and also described how it begins from a sensor node and disseminate in the whole network. Further, they (Khayam,S.A.,2006) applied a method of signal processing and suggested an another model which was based on epidemic theory for the analysis of propagation dynamics of worm in WSN over different broadcast protocols. For providing the protection of sensor network due to malware attack Peiyan and Ping (Peiyan Yuan, Ping Liu,2015) suggested a model in which they combined the concept of epidemic modeling with mean delivery delay and utilization of sensor nodes' energy.

Wang and Yang (Wang Ya-Qi ,yang,2013) presented an epidemic based SI model which is used to restrain the virus spreading in WSN. To achieve the better prevention mechanism of virus spread in WSN they combined epidemic model with MAC mechanism. They also explained the effect of different network parameters on virus spreading in the sensor network. The one maintenance based SIR-M model was developed by Tang and Mark (Tang,S.,Mark,B.L.2009) to secure WSN due to virus attack. In this model method of recovery has been used. The infected nodes of WSN cleaned during sleep mode of sensor nodes. This technique is known as maintenance technique because signaling overhead does not occur in sleep mode of sensor node. An improved SIR(iSIRS) model was presented by Wang et al.(Wang,2009) in which they explained the non-linear dynamics of virus spreading in the sensor network. The energy exhaustion of sensor nodes due to virus attack on WSN has been analyzed in consideration of different parameters. This model posses some problem related to network size and others. The extended iSIRS (EiSIRS)(Wang,2010) model conquered these problems, which was also based on epidemic modeling. This model is useful for large size network and utilized the sleep and awake mode of sensor node to optimize energy consumption of sensor nodes. They also suggested a strong security mechanism for WSN, which is used to prevent virus attack on the network.

An another maintenance mechanism based SI model has been presented by Tang (S.,Tang,2011). They compared the two cases in one case consider antivirus imposed on infected nodes and another case there is not applied antivirus on infected nodes. The spreading of virus dynamics in sensor network has been explained with the help of this model. Further, Tang and Li (Tang,Shensheng,2011)proposed an enhance method for protection of sensor network due to virus attack. This is an enhancement over the earlier model(S.,Tang,2011). The concept of adaptive network protection technique was adopted to provide protection of WSN due to attack of virus. The model was verified by simulation results.

Feng et al.(Feng.,2015) proposed a SIRS model for the analysis of worm propagation dynamics in the sensor network. They also explained the effect of coverage and connectivity on propagation of worm in WSN. The value of basic reproduction number (R_0) of the proposed model has obtained, this value is one of the important parameter in epidemic theory.

This parameter helps in the determination of network status. On the basis of this value it can be determine that network will be stable or unstable when work attack on WSN. They also obtained the equilibrium points of the system. But this model was not able to detect the appearance of worm in WSN at earlier period. Thus, to surmount this problem Ojha et. al.(Ojha,2019) suggested a SEIRS model, basically this model is an extension of SIRS model (Feng,2015). In SEIRS model introduced the idea of exposed class for earlier detecting of worm appearance in WSN. They also obtained the value of basic reproduction number (R_0) for study of worm propagation behaviour in WSN. The worm propagation dynamics discussed by them also compare this model with SIRS model [11] and SEIS model (Miguel,2016) under the similar conditions.

But these models did not included the concept of carrier devices. First time the concept of carrier devices were introduced by Rey et al.(Rey Martin,2016) and pro-posed a SCIRS model for restraining of malware spread in WSN. The basic reproductive number has also been obtained for the analysis of network dynamics.They determined the equilibrium points of the suggested system and discussed when the system will be in disease-free steady state. And the endemic steady state of the system has been also discussed by them. Further, the shortcomings of this model improved by Guillen and Rey (Hernandez,2019). They modified the earlier model and developed a technique for controlling of malware spreading in WSN. The global and local stability of the system is analyzed by them under various conditions. They obtained the value of R_0 and discussed efficient security countermeasures for WSN. Numerical proves are presented in this paper along with simulation results. But they also did not apply the technique of quarantine to improve WSN security due malware attack.

Some quarantine based models have been presented by different authors to protect WSN due to malware attack. A quarantined based SIQR model is presented by Khanh (Nguyen,2016). This model explained the dynamic behaviour of worm attack in WSN. The stability of the WSN system has been analyzed with the help of this model in case of worm attack. The impacts of quarantine technique has been analyzed and nd that this is useful in protection of WSN against worm attack. Further, Ojha et al. (Ojha,2019) suggested a modified SIQR model for protection of WSN caused by worm attack. They surmounted the problem of SIQR(Nguyen,2016) and address the issue of coverage and connectivity in WSN. The effect in coverage and connectivity on worm propagation has been also analyzed by them. The value of R_0 has been also obtained by them for the investigation of network stability under worm-free conditions. The relationship with R_0 and coverage/connectivity has been explained and their impacts of worm spreading is discussed. The model has been validated with the help of mathematical proof as well as simulation results. These models also did not taken into account the carrier devices. In this paper proposed an epidemic based model in which to apply the method of quarantine and taken into consideration of carrier devices.

Proposed Model: The Improved SCIQRS Model

The modification of SIRS model is proposed with consideration of quarantine state. This model focuses on the analysis of dynamics of malware spreading in WSN. The proposed model is an advancement over the existing SCIRS model(Hernandez,2019). In the analysis of malware spreading in WSN normally carrier de-vices are ignored. In this model consider the two cases, in one case carrier devices can be damage, and in another case carrier devices will not be dam- age. The key objective of the proposed model is to secure WSN due malware attacks, improve network stability, and improve the lifespan of WSN. There are different models have been suggested by a number of authors to secure WSN against the malware attacks, but we found a distinguishable improvement in the proposed model.

The different states of the proposed model which are as follows:

(i)Susceptible nodes (S): The nodes which are not in contact with malwares, but these nodes are vulnerable and may be attack by malwares.

(ii)Carrier nodes (C): These nodes are serve as the transmission vector or carrier of the mal-ware.

(iii)Infectious nodes (I):The nodes which got infected by malware and can infect neighbour-ing nodes.

(iv)Recovered nodes (R): These nodes affected by malware have been detected and eliminat-ed from them.

(v) Quarantined Nodes (Q): These nodes keep in isolation and are not be able to communicate with others nodes of the network.

1. Description and Assumptions of the Proposed Model

The proposed model is a deterministic model. Assume that N number of sensor nodes distributed in the field for the purpose of data collection. These nodes are grouped into the di-fferent classes of nodes, namely: Susceptible class (S), Carrier class (C), Infectious class (I), Quarantine class (Q) and Recovered class (R). A complete transition diagram of the SCIQRS model is illustrated in Fig. 1. This model consist of five different states. At any time $t \geq 0$, $N(t) = S(t) + C(t) + I(t) + Q(t) + R(t)$ satisfy this condition.

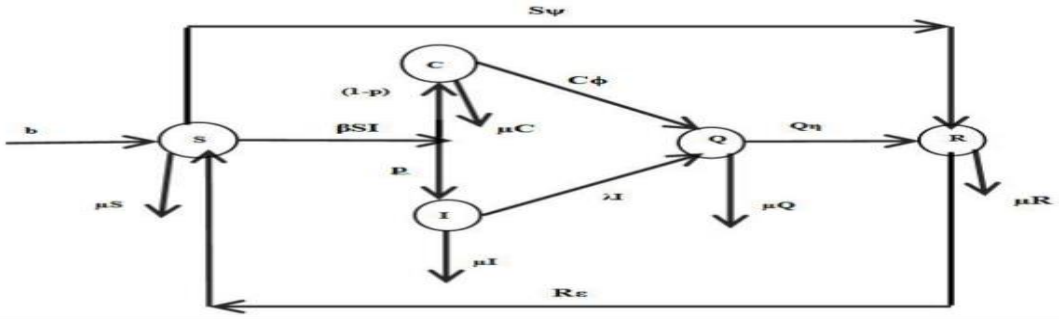

Figure 1. Transition states of the SCIQRS model

For the analysis the following assumptions have been made:

(i)All the nodes of WSN belong susceptible state in the beginning, these nodes can be attacked by malware. At time t, if malware attacks on the susceptible nodes they may become infectious with rate p SI. On the other hand the chances is that the susceptible devices may turn into carrier devices with probability (1 p) SI. Where p is the part of susceptible nodes attacked by malware.

(ii)The infectious node spread the malware to the neighbouring nodes of WSN, therefore to prevent the further infection in WSN infectious nodes send into quarantine state with probability I. Some of the infectious nodes can be crashed due to drain of sensor nodes battery or malfunction of hardware/software.

(iii)The carrier devices carry the malware and can infect the other nodes of the network, so to overcome this problem these devices can be also quarantine with probability C. Some of the carrier devices can be crashed due to malfunction of hardware/software.

(iv)In quarantine state the antivirus will be executed on quarantined nodes for elimination of malware from them with the rate of Q. During the quarantine state of nodes the antivirus works efficiently and eliminate malware from the nodes, and quarantined nodes move into the types of recovered nodes. After the recovery they are ready for communication. Some of the quarantine nodes can be crashed due to drain of sensor nodes battery or malfunction of hardware/software.

(v)The recovery cannot ensure that the recovered nodes cannot be infected again by the same or new type of malwares. The recovered nodes may loss its immunity and becomes susceptible at the rate of R". Some of the recovered nodes can be crashed due to drain of sensor nodes battery or malfunction of hardware/software.

(vi)Some of the susceptible nodes immunized by antivirus at the time of deployment and they achieve temporary immunity against the malware attack. The immunization rate of susceptible nodes is taken as S.

In this model, it is assumed that different types of nodes are randomly present in the network, hence the possibility to make the contact with others nodes is same. In the proposed model the quarantine mechanism is considered because the secondary case in infection will to cease in the network. Along with quarantine mechanism recovery operation is been also performed to eliminate the malware from sensor nodes. In this work, the meaning of quarantine is that the ability of infectious nodes to infect others other nodes of the network has been disappeared. The proposed model governed by the set of differential equations that describes the network dynamics in case of malicious actions.

$$\left.\begin{aligned}
\frac{dS}{dt} &= b - \beta SI - (\mu + \psi)S + \varepsilon R \\
\frac{dC}{dt} &= (1-p)\beta SI - (\mu + \phi)C \\
\frac{dI}{dt} &= p\beta SI - (\mu + \lambda)I \\
\frac{dQ}{dt} &= \lambda I + \phi C - (\mu + \eta)Q \\
\frac{dR}{dt} &= \eta Q + \psi S - (\mu + \varepsilon)R
\end{aligned}\right\} \quad (1)$$

where the meaning of symbols is given in table 1.

Table 1. Description of used symbols

S.No.	Symbol	Meaning of Symbol
1	b	Inclusion of sensor node / carrier nodes in WSN
2	μ	Crashing rate of sensor nodes/ carrier nodes due to malfunction of software/hardware or exhaust of sensor node battery
3	β	malware transmission rate in WSN
4	λ	Quarantine rate of infectious sensor nodes
5	ϕ	Quarantine rate of infectious carrier nodes
6	ψ	Rate of immunization of susceptible nodes
7	ε	Recovered nodes converted into susceptible nodes
8	η	Rate of quarantine nodes to recovered nodes transmission

Analysis of Equilibrium and Basic Reproduction Number

For finding the equilibrium points of the system taking the first derivative of the set of equations 1 is equal to zero, i.e.

$$\frac{dS}{dt} = 0, \frac{dC}{dt} = 0, \frac{dI}{dt} = 0, \frac{dQ}{dt} = 0, \text{ and } \frac{dR}{dt} = 0.$$

$$\left.\begin{aligned}
0 &= b - \beta SI - (\mu + \psi)S + \varepsilon R \\
0 &= (1-p)\beta SI - (\mu + \phi)C \\
0 &= p\beta SI - (\mu + \lambda)I \\
0 &= \lambda I + \phi C - (\mu + \eta)Q \\
0 &= \eta Q + \psi S - (\mu + \varepsilon)R
\end{aligned}\right\} \quad (2)$$

Sovling the equation 2 simultaneously and obtained the equilibrium points for malware free state is $E_0 = (S_0, C_0, I_0, Q_0, R_0) = (\frac{b(\varepsilon+\mu)}{(\mu+\psi+\varepsilon)}, 0, 0, 0, \frac{b\psi}{(\mu+\psi+\varepsilon)})$.

On the other hand if $I^* > 0$,then the endemic equilibrium point $E^* = (S^*, C^*, I^*, Q^*, R^*)$of the system is given as $S^* = \frac{(\lambda+\mu)}{p\beta}, C^* = [\frac{(1-p)(\lambda+\mu)}{p(\phi+\mu)}]I^*,$

$$I^* = \frac{\frac{b}{R_0\mu(\psi+\varepsilon+\mu)}\{\frac{(\psi+\mu)(\varepsilon+\mu)}{p\beta} - \varepsilon\psi - R_0\mu(\psi+\varepsilon+\mu)\}}{L^*}, Q^* = [\frac{(1-p)\phi\mu + \lambda(p\mu+\phi)}{p(\phi+\mu)(\eta+\mu)}]I^*,$$

$R^* = \frac{\psi S^* + \eta Q^*}{(\varepsilon + \mu)}$, where $L^* = \frac{\varepsilon\eta}{\varepsilon+\mu}[\frac{(1-p)\phi\mu + \lambda(p\mu+\phi)}{p(\phi+\mu)(\eta+\mu)}] - \frac{(\lambda+\mu)}{p}$

And Ro[41]is the basic reproduction number which is expressed as

$R_0 = \frac{p\beta}{(\lambda+\mu)}[\frac{b(\varepsilon+\mu)}{\mu(\varepsilon+\mu+\psi)}]$. and the endemic equilibrium E^* will uniquely exist ,only when $R_0 > 1$

System Stability and its Analysis

The stability analysis of the system is important when malware attacks. For the analysis of the system stability different theorems have been established and one the basis of these theorems determine the network stability. The existing theorems are modified for the stability analysis. The modifications are based on the idea of proposed model.

Theorem 1: The malware-free equilibrium (MFE) of the system is given by the set of equations (1) is locally asymptotically stable if $R_0 < 1$ otherwise unstable if $R_0 > 1$.

Proof To found the local stability of P_0, the Jacobian matrix is obtained by linearizing the model of equation 1. And Jacobian matrix is as:

$$J(P_0) = \begin{bmatrix} -(\psi+\mu+\omega) & 0 & -\beta S_0 & 0 & \varepsilon \\ 0 & -(\phi+\mu+\omega) & (1-p)\beta S_0 & 0 & 0 \\ 0 & 0 & -p\beta S_0 - (\lambda+\mu+\omega) & 0 & 0 \\ 0 & \phi & \lambda & -(\eta+\mu+\omega) & 0 \\ \psi & 0 & 0 & \eta & -(\varepsilon+\mu+\omega) \end{bmatrix} \quad (3)$$

The eigenvalues of the above Jacobean matrix are: $\omega_1 = -\mu, \omega_2 = -(\eta+\mu)$, $\omega_3 = -(\phi+\mu), \omega_4 = -(\varepsilon+\mu+\psi)$, and $\omega_5 = \frac{(R_0-1)}{(\lambda+\mu)}$.

The values of first four eigenvalues $(\omega_1, \omega_2, \omega_3, \omega_4)$ are negative. But the value of eigenvalues (ω_5) will be negative only when value of R_0 is less than one. Hence, the system is locally asymptotically stable if $R_0 < 1$. Whereas when value of $R_0 > 1$ then (ω_5) becomes positive. Then in this case system comes into unstable state.

Theorem 2: The malware-free equilibrium (MFE) of the system is given by the set of equations (1) is globally asymptotically stable, if $R_{0\leq} 1$.

Proof Consider the suitable Lyapunov function L(t): $R^5 \longrightarrow R^+$, defined by $L(t) = \omega I(t)$.

By taking the first derivative of L(t) with respect to time t, we get

$$\frac{dL(t)}{dt} = \omega\dot{I}(t) \implies \frac{dL(t)}{dt} = \omega(p\beta SI) - (\lambda+\mu)I$$

After suitable assumption of $\omega = \frac{1}{(\lambda+\mu)}$,we get $\frac{dL}{dt} = [\frac{p\beta S\psi}{(\lambda+\mu)} - 1]I \leq R_0 - 1$

It is obvious from the above expression, $\frac{dL}{dt}$ only when I=0.Therefore the maximum invariant set $\{\Gamma = (S, C, I, Q, R) \in R_5^+\}$ the singleton set $\{E_0\}$. If $R_0 \leq 1$, then, as per Lasalle's invariance principle (La salle,1976) malware-free equilibrium P_0 is globally asymptotically stable.

Results

Malware attack in WSN is one of the important threat.To prevent the malware attack on WSN, it is necessary to predict and understand the propagation behaviour of malware. On the basis of understanding and prediction of the malware propagation behaviour the preventive action against malware attack should be applied in WSN. For verification of the correctness of theoretical studies of the proposed model has compared with the results achieved through simulation. The MATLAB has been used for simulation. The effects of various parameters on malware spread in WSN has been analyzed. Taking the initial parametric values at time t = 0 in case one is as: S(0) = 100; C(0) = 0; I(0) = 1; Q(0) = 0; R(0) = 0; b = 1; μ= 0:01; β= 0:00002; φ= 0:004;λ= 0:06;
ψ = 0:04; ε = 0:006; p = 0:9 and η = 0:01. And calculate the value of basic reproduction number R_0 = 0:857.

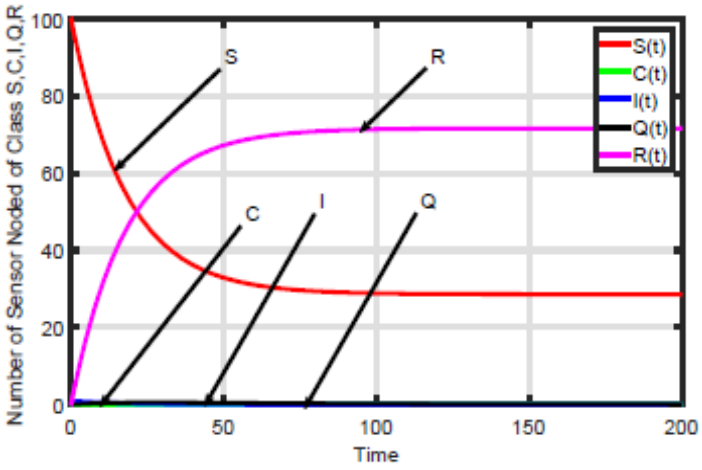

Fig. 2. Dynamics of malware propagation when $R_0 < 1$

Figure 2 illustrates the dynamic spreading behaviour of malware in WSN. The number of infectious nodes are diminishing with time in this figure. This indicates that malware is not existing in the network or eliminate from the network. The basic reproduction number (R_0) is an important parameter which plays a role in determination of network stability. In this case the value of R_0 = 0:857 which is less than one. Hence the network will exist in the malware-free state. Consider the another case and changing the some values of the network parameters are β= 0:002; and λ= 0:04 other parameters remain same. In this condition the value of basic reproduction number R_0 = 128:57.

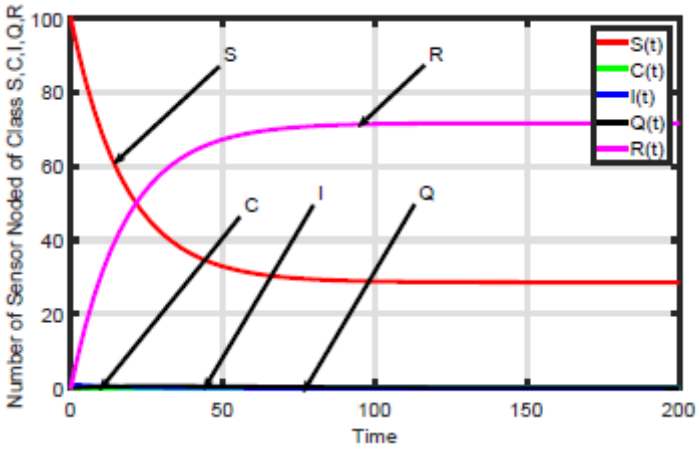

Fig. 3. Dynamics of malware propagation when $R_0 > 1$

Figure 3 shows the dynamics of malware propagation when $R_0 > 1$, in this figure in the starting susceptible number of nodes decreases and other class of nodes increases with time. The infectious number of nodes begin to decline but not completely eliminates from the network. The infectious nodes persist in the network continuously as results that malware outbreak attains endemic state. In this case network never becomes malware-free.

Considering the case when number of susceptible increases the variation in the other states of nodes is also observed with time. The variation in different states of nodes with time in case of large number of nodes is shown in figure 4.

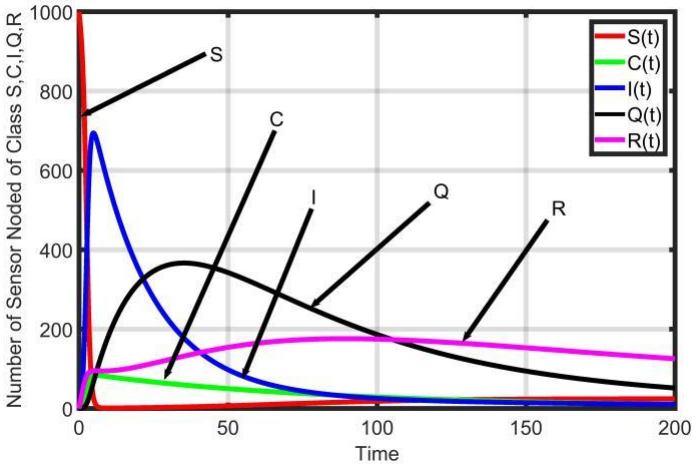

Fig. 4. Dynamics of malware propagation when $R_0 > 1$

The effect of malware transmission rate (β) on malware propagation in WSN is analyzed, here changing the values of (β = 0.002, 0.004, 0.007) and remaining parameters in all conditions are similar b = 1; μ= 0:01; φ= 0:004;

λ= 0:04; ψ = 0:04; € = 0:006; p = 0:9 and η = 0:01.

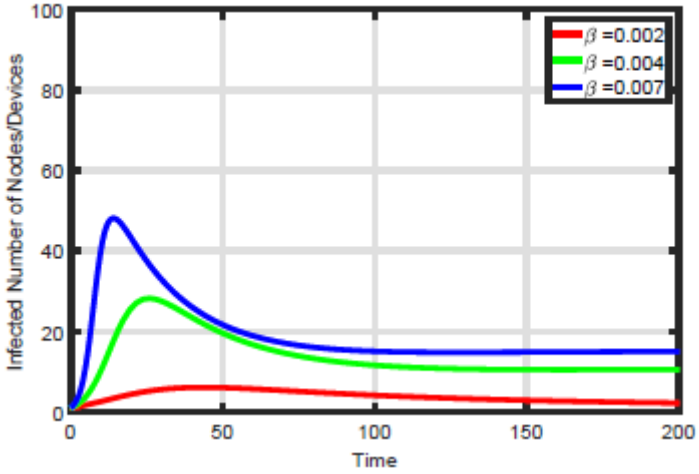

Fig. 5. Effect of malware transmission rate (β) on WSN

The effect of malware transmission rate (β) on WSN is explained with the help of figure 5. From figure 5, we found that as the value of malware transmission rate increases the number of infected nodes/devices increases. And when the value of is β larger then more number of nodes/devices gets infected in the similar condition. Therefore, it can be realize that if malware transmission rate is high it will outbreak in the network in quickly manner.

The effect of quarantine on malware spreading rate in WSN is analyzed. In this model basically two types of infectious class one is carrier class and second is infectious class. Both are spreading the malware in the network. The malware disseminates in the network may be wirelessely or with data. But one the important issue in the network is that communication can not be stop completely. Hence, a dynamic quarantine mechanism is required.The dynamic quarantine mechanism prevent the malware spreading in the network and communication keep continued in the network.

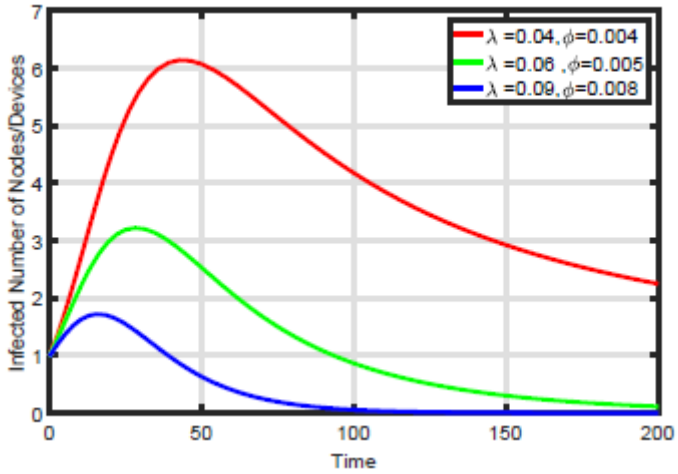

Fig. 6. Effect of quarantine on spread of malware in WSN

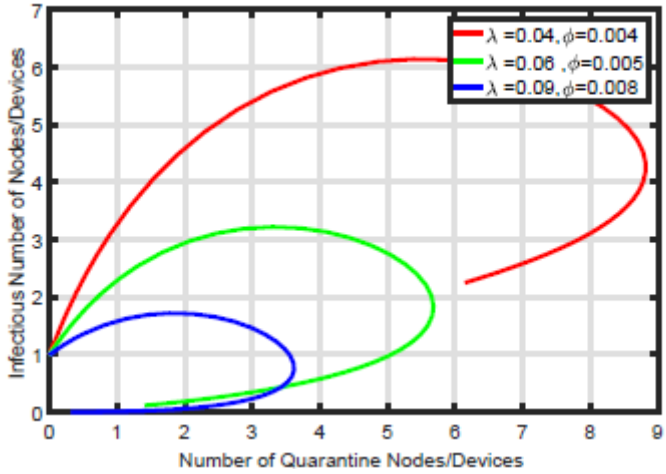

Fig. 7. Effect of quarantine on spread of malware in WSN

Figure 6 and 7 illustrate the effect of quarantine mechanism on spread of malware in WSN. We observed from figures as the quarantine rate increasing the number of infectious nodes decreasing in the network.It is observed that due to this mechanism the spreading speed of malware is declined in the network. The malware spreading also impact the battery consumption of sensor nodes of WSN. If the spreading speed of malware will decrease network becomes stable and battery consumption of sensor nodes also decreases.

The effect of rate of infection (β) and rate of quarantine (λ)is studied. The values of these parameters (β and λ) varies.

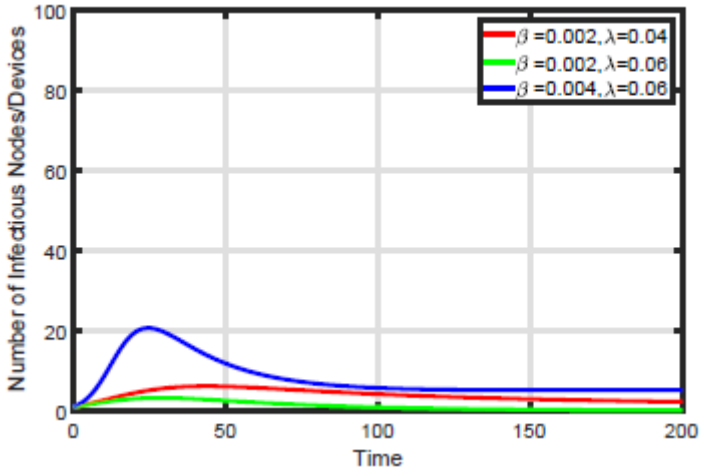

Fig. 8. Effect of β and λ on spread of malware in WSN

In figure 8 taking the two cases in one case fixed the value of β and increased the value of λ then the count of infectious nodes decrees and count of quarantine nodes increases. So, the prevention of malware spread can be minimize. In the another case when the value of is fixed and increase the value of the count of infectious nodes increases. The figure 8 portray that the controlling technique of malware spread in WSN.

The mechanism of recovery with quarantine for controlling of malware spreading in WSN is studied. Recovery is a mechanism through which to remove the malware from

nodes/devices by the use of antivirus. This mechanism impoves the network stability by elimination of malware and increase the life-time of WSN.

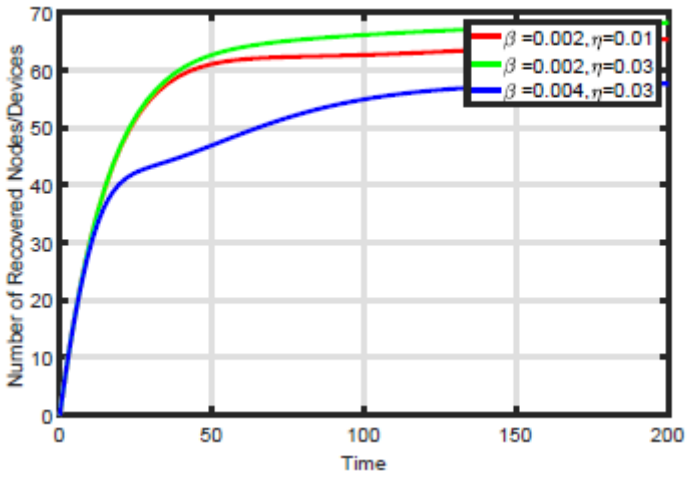

Fig. 9. Effect of recovery on spread of malware in WSN

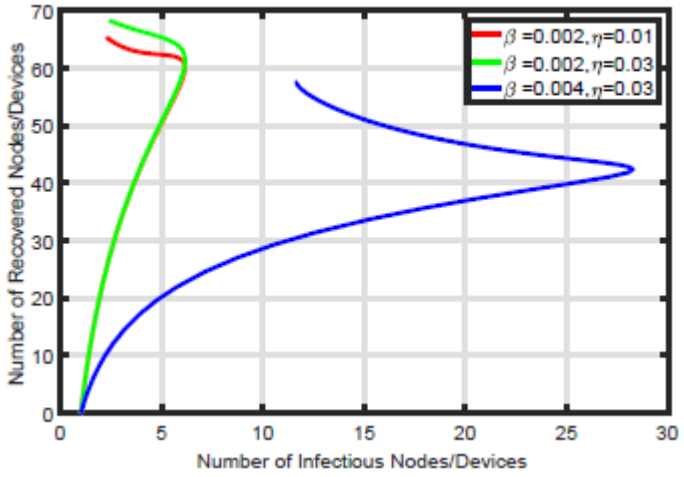

Fig. 10. Effect of recovery on spread of malware in WSN

Figure 9 and 10 show the impact of recovery on infectious nodes. We found from figure 9 that when rate of infection is constant and rate of recovery increases then the number of immune nodes increases. One the other case when rate of recovery is constant and transmission rate of malware increases then number of recovered nodes declined. This is also satisfied by figure 10 in which it found that as transmission rate of malware is constant and recovery rate increases then less number of nodes present in infectious state and in another case when transmission rate of malware increases and recovery rate is constant then more number of nodes are present in infectious state.

Comparison with earlier model and Proposed Model

In this section compare the proposed model with earlier model which was proposed by Guillen and Rey [19]. For comparative study taking the parameters as follows: S(0) = 100; C(0) = 0; I(0) = 1; Q(0) = 0; R(0) = 0; b = 1;μ = 0:01;β= 0:004; φ= 0:004; λ= 0:06; = 0:04; ψ = 0:006; p = 0.9 and η = 0:01. Consider the similar condition for both the models.

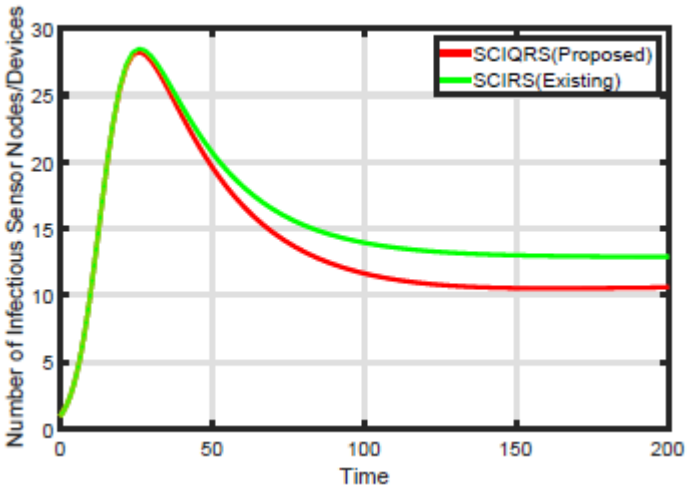

Fig. 11. Comparison between SCIQRS and SCIRS model

Draw the graph between time and infectious number of nodes/devices. From figure 11 it is obvious that the less number of nodes/devices gets infectious in the proposed model with respect to the earlier model. The quarantine mechanism reduces the speed of infection in proposed model. Hence, it can conclude that the mechanism of quarantine is useful for controlling and prevention of malware spread in WSN.

Conclusion

In this paper a SCIQRS model is proposed, which is an improvement over the SCIQRS model. The mechanism of quarantine and recovery is taken into account for prevention and controlling of malware spread in WSN. For the determination of network stability and dynamics of malware analysis calculated the value of basic reproduction number (R_0). The R_0 is one the most crucial parameter in epidemiology. The value of R_0 determined that the network will be malware-free if its value is less than one, and if its value is greater than one then in this condition malware continuously persist in the network. The malware-free and endemic equilibrium points of the system has been calculated. The stability of the system has analyzed in different conditions and provide the proof of theorems in the support of stability.

The effect of different states of the model has been discussed and found that if quarantine rate is more then speed of infection will be low. The dynamic mechanism of quarantine mechanism has been explained. The effect of recovery is also analyzed and observed that recovery mechanism reduces the infectious number of nodes/devices in the network. The comparative study is also conducted with earlier model and found that proposed mechanism is providing the better mechanism for prevention and control malware spread in WSN. In the similar condition less number of nodes/devices gets infected in proposed model. In future, to achieve a ameliorate network security scheme, coverage, connectivity and spatial correlation can be consider.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article

References

Alaba, A., Othman, M., Hashem, T., and Alotaibi, F., Internet of Thing security: A survey. J Netw Comput Appl, Volume 88, pages 10-28, 2017.

Bahi, J. M., Guyeux, C., Hakem, M., and Makhoul, A., Epidemiological approach for data survivability in unattended wireless sensor networks, Journal of Network and Computer Applications, Volume 46,pages 374-383, 2014.

De, P., Liu, Y., and Das, S. K., An Epidemic Theoretic Framework for Vulnerability Anal-ysis of Broadcast Protocols in Wireless Sensor Networks, IEEE Transactions on Mobile Computing, Volume 8,Number 3, pages413-425,2009.

De,P.,Liu, Y.,and Das, S. K.,Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory, ACM Transactions on Sensor Networks, vol.5(3),pp.1-33.(2009).

Feng, Liping and Song, Lipeng and Zhao, Qingshan and Wang, Hongbin, Modeling and Stability Analysis of Worm Propagation in Wireless Sensor Network, Mathematical Problems in Engineering, volume 2015, number Article ID 129598, pages 1-8,2015.

Haghighi.,S., M., Wen, S.,Xiang,Y.,Quin, B., and Zhou, W.\On the Race of Worms and Patches: Modeling the Spread of Information in Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, Volume 11, Number12,Pages 2854-2865, 2016.

Hayel, Y., and Zhu, Q.,Epidemic Protection Over Heterogeneous Networks Using Evolutionary Pois son Games IEEE Transactions on Information Forensics and Security, Vol-ume12, Number 8, pages1786-1800,2017.

He,Z., Cai, Z., and Wang, X., Modeling Propagation Dynamics and Developing Op-timized Counter measures for Rumor Spreading in Online Social Networks, IEEE 35th International Conference on Distributed Computing Systems, Pages 205-214 Columbus, OH, 2015.

He,Z., Cai,Z., Yu, J., Wang, X., Sun, Y., and Li,Y. Cost-E cient Strategies for Re-straining Rumor Spreading in Mobile Social Networks,IEEE Transactions on Vehicular Technology, Volume66, Number3, pages2789-2800,2017.

Hernandez Guillen, J.,D., and Rey Mart n A., del., A mathematical model for malware spread on WSNs with population dynamics, Physica A, Pages 1-23, 2019.

Hernandez Guillen, J.,D., and Rey Mart n A., del.,Modeling malware propagation using a carrier compartment, Communications in Nonlinear Science and Numerical Simulation, Pages 1-22, 2017.

Jacques, M. B.,Christophe G.,Mourad, H.,and Abdallah, Makhoul: Epidemiological ap-proach for data survivability in unattended wireless sensor networks., Journal of Network and Computer Applications,46,374 -383 (2014)

Kermack, W. O., and McKendrick, A. G., A contribution to the mathematical theory of epidemics, Volume 115, Number 772, pages 700-721. The Royal Society, 1927.

Khan, Tayyab, Karan Singh, Mohamed Abdel-Basset, Hoang Viet Long, Satya P. Singh, and Manisha Manjul. "A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks." IEEE Access 7 (2019): 58221-58240.

Khayam, S. A., and Radha, H., Using signal processing techniques to model worm propagation over wireless sensor networks, IEEE Signal Processing Magazine, Volume 23, Number 2, pages164-169,2006

Khayam, S., A., and Radha, H., A topologically-aware worm propagation model for wireless sensor networks, 25th IEEE International Conference on Distributed Computing Systems Workshops, pages 210-216. IEEE, Columbus, OH, USA, 2005.

La Salle, J., The Stability of Dynamical Systems,Society for Industrial and Applied Mathematics,1976.

Liu G, Peng B, Zhong X. A Novel Epidemic Model for Wireless Rechargeable Sensor Network Security. Sensors. 2021; 21(1):123.

Luo, J., When Will COVID-19 End ? Data-Driven Prediction, Data-Driven Innovation Lab (http://ddi.sutd.edu.sg), Singapore University of Technology and Desig (http://www.sutd.edu.sg).

Miguel, L., Alberto, P., and Andres. O., A SEIS Model for Propagation of Random Jamming Attacks in Wireless Sensor Networks, In: Gra~na M., Lopez-Guede J., Etxaniz O., Herrero A., Quintian H.,Corchado E. (eds) International Joint Conference SOCO'16-CISIS'16-ICEUTE'16. SOCO 2016, ISIS 2016, ICEUTE 2016. Advances in Intelligent Systems and Computing, Volume 527, pages 668-677. Springer, Cham.

Mishra, B. K., and Keshri, N., Mathematical model on the transmission of worms in wireless sensor network, Applied Mathematical Modelling, Volume37, Number 6, pages 4103-4111,2013.

Nguyen Huu, Khanh, Dynamics of a Worm Propagation Model with Quarantine in Wireless Sensor Networks,Applied Mathematics & Information Sciences volume 10,2016.

Ojha, R., P. and Srivastava, P., K. and Sanyal, G., Pre-Vaccination and Quarantine Approach for Defense Against Worms Propagation of Malicious Objects in Wireless Sensor Networks, volume9 ,number1,pages1-20,2018.

Ojha, R., P., and Sanyal, G. and Srivastava, P., K. and Sharma, K. Design and Analysis of Modified SIQRS Model for Performance Study of Wireless Sensor Network, Scalable Computing: Practice and Experience, volume18,pages229-242,2017.

Ojha, R., P., and Srivastava, P., K., and Sanyal, Goutam, Improving wireless sensor net-works performance through epidemic model, International Journal of Electronics, volume 106,number 6, pages 862-879, 2019.

Ojha, R.P., Srivastava, P.K., Sanyal, G. *et al*. Improved Model for the Stability Analysis of Wireless Sensor Network Against Malware Attacks. *Wireless Pers Commun* (2020).

P. van den Driessche and James Watmough, Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission,Mathematical Bio-sciences, volume 180,number ,pages 29 - 48,2002.

Peiyan Yuan and Ping Liu, Data fusion prolongs the lifetime of mobile sensing networks, Journal of Network and Computer Applications,volume49, pages51 - 59,2015.

Rey Mart n A., del., Hernandez Guillen, J.,D., and Sanchez Gerardo Rodr guez, A SCIRS Model for Malware Propagation in Wireless Networks, International Joint Conference SOCO'16-CISIS'16-ICEUTE'16 Advances in Intelligent Systems and Computing,Volume-527, Pages 638-647, (2016),Leon, Spain.

S. Yu and G. Gu and A. Barnawi and S. Guo and I. Stojmenovic, Malware Propaga-tion in Large-Scale Networks,IEEE Transactions on Knowledge and Data Engineering, volume27, number1, pages

S., Tang, A Modi ed Epidemic Model for Virus Spread Control in Wireless Sensor Networks, 2011 IEEE Global Telecommunications Conference- GLOBECOM 2011, pages 1-5,2011.

Singh, A., Awasthi, A. K., Singh, K., and Srivastava, P. K., Modeling and Analysis of Worm Propagation in Wireless Sensor Networks, Wireless Personal Communications, Volume 98, Number 3, Pages 2535-2551, 2018.

Singh, S., Sharma, P.,K., Moon, S.,Y., Moon, D., and Park, J.,H., A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. The Journal of Supercomputing, pages 1-32, 2016.

Srivastava, A.P.; Awasthi, S.; Ojha, R.P.; Srivastava, P.K.; Katiyar, S. Stability analysis of SIDR model for worm propagation in wireless sensor network. Indian J. Sci. Technol. 2016, 9, 1–5.

Tang, S., A Modi ed SI Epidemic Model for Combating Virus Spread in Wireless Sensor Networks, International Journal of Wireless Information Networks, Volume 18, Number 4, pages 319-326, 2011.

Tang, S., and Mark, B. L., Analysis of virus spread in wireless sensor networks:An epidemic model, 2009 7th International Workshop on Design of Reliable Communication Networks, pages 86-91.IEEE,Washington DC, 2009.

Tang, Shensheng and Li, Wei, An Epidemic Model with Adaptive Virus Spread Control for Wireless Sensor Networks, Int. J. Secur. Netw.,volume 6,number4,pages201-210,2011.

Tianrui, Z., Lu-Xing, Y., Xiaofan, Y., Yingbo, W., and Yuan Yan T., Dynamic malware containment under an epidemic model with alert, Physica A: Statistical Mechanics and its Applications, Volume 470, pages249-260,2017.

Upadhyay, R. K., Kumari, S., and Misra, A. K., Modeling the virus dynamics in com-puter network with SVEIR model and nonlinear incident rate, Journal of Applied Math-ematics and Computing, Volume 54, Number1, pages485-509,2017.

Wang Xiaoming and LI Yingshu, An Improved SIR Model for Analyzing the Dynamics of Worm Propagation in Wireless Sensor Networks, Chinese Journal of Electronics vume18, number1, pages 8-12,2009

Wang, T., Wu, Q., Wen, S., Cai, Y., Tian, H., Chen, Y., and Wang, B., Propagation Modeling and De fending of a Mobile Sensor Worm in Wireless Sensor and Actuator Net-works, Sensors, Volume17,Number12, pages1-17,2017.

Wang, Xiaoming and Li, Qiaoliang and Li, Yingshu, EiSIRS: a formal model to analyze the dynamics of worm propagation in wireless sensor networks,Journal of Combinatorial Optimization, volume20,number1,pages47-62,2010.

Winkler, I., and Treu, G., A., Advanced Persistent Security. A cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection and Reaction Strategies. Cam-bridge, MA: Singress, Else vier Inc; 2017.

Y. Wang, S. Wen, Y. Xiang and W. Zhou, Modeling the Propagation of Worms in Net-works: A Survey,IEEE Communications Surveys Tutorials, Vol.16, Number2,pages942-960,2014.

Yick, J., Mukherjee, B., and Ghosal, D., Wireless sensor network survey,Computer Net-works, Vol ume 52,Number 12, pages 2292-2330, 2008.

Bibliographic information of this paper for citing:

Verma, Chakradhar, & Gupta, c.p. (2022). Epidemiological Model for Stability Analysis of Wireless Sensor Network under Malware Attack. *Journal of Information Technology Management*, Special Issue, 69-88.