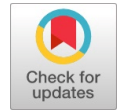


# Analyze The Effects of Quarantine And Vaccination on Malware Propagation in Wireless Sensor Network



Satya Ranjan Biswal, Santosh Kumar Swain

**Abstract:** Malware (worm, virus, malicious signals, etc.) propagation in Wireless Sensor Network (WSN) is one of the important concern. The WSN becomes unstable due to presence of malicious signals. Vulnerability of WSN is very high because of the structural constraint of sensor nodes. The attackers target a sensor node of WSN for malware attack. A single infected node starts to spread the malware in the entire network through neighbouring nodes. Therefore, for controlling of malware propagation in WSN a mathematical model is developed. The developed model is based on epidemic theory. The developed model consist of five states such as Susceptible-Infectious-Quarantine-Vaccination-Dead (SIQVD). The quarantine is a method through which to cease the infection spread in WSN. And through vaccination eliminate the malware from the network. The combination of quarantine and vaccination technique improves the network stability. This technique prevents malware propagation in WSN. The basic reproduction number ( $R_0$ ) of the model is deduced. The stability of the network depends on the value of basic reproduction number. It is found that if the value of  $R_0$  is less than one the network system exist in malware-free state, otherwise in endemic state. The equilibrium points of the system is obtained. The effects of quarantine and vaccination has been analyzed on system performance. The theoretical findings are verified by simulation results. Attack Epidemic model Equilibrium point Malware propagation Security Wireless Sensor Network

## I INTRODUCTION

Wireless Sensor Network (WSN) is a group of smart, intelligent sensor nodes. Sensor node a low-power device which is consist of an array of sensors, memory unit, processor unit, radio unit and power unit. The sensor nodes are used to sense, compute, and collect information from the physical environment. Due to confined transmission power of sensor node, the information transmit to the sink node in multi-hop manner. The sensor node is a resource constraint device. Therefore, information security is important during transmission in the network. In reality, the security of information due to malwrae attack is one of the crucial subject. The a lot of applications of WSN such as vehicle tracking, battlefield, environmental monitoring, disaster management etc. [1]. The sensor nodes are vulnerable towards malware attack [2, 3].

Manuscript published on 30 August 2019.

\*Correspondence Author(s)

Satya Ranjan Biswal, Associate Professor in Department of Computer Science & Engineering, Trident Academy of Technology, Bhubaneswar, Odisha.

Santosh Kumar Swain, Professor in department of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, Odisha

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

The security of WSN due to malware attacks is one the critical field of research. The presence of malware in WSN affects network stability, increase congestion, slow-down the operation of network, etc.[3]

The propagation characteristics of biological worms are similar to software created worm [4]. The malwres can by easily make a target of sensor nodes due its structural limitations and lack of strong defense techniques. The attackers victimize a node of WSN, then start to spread in the entire network with the help of adjacent nodes. And disturb the smooth network operation. Therefore, this is necessary to identify infected nodes of WSN and accordingly apply corrective techniques for removal of malware from WSN. Numerous authors [2, 5, 6, 7, 8, 9] have presented the security issues in WSN due to malware attacks. They have investigated the propagation process of malware in the network on the basis of epidemic modeling. The main focus of this paper is to explain the malware propagation process and its dynamics in WSN. And developed a model that can prevent malware propagation in WSN. The developed model analyzes the effect of various states on malware propagation in WSN. The model is used the basic concept of epidemic modeling. The developed model consists of five states. The states are Susceptible-Infectious-Quarantine-Vaccination-Dead (SIQVD). The developed mechanism prevent WSN against the various types of attacks. The contributions of developed model is:

- Developed a mathematical model to analyze the malware dynamics in WSN and invent technique for its elimination.
- Utilize the concept of Quarantine state to restraint the malware propagation and optimize energy depletion of sensor node.
- To analyze the system responsiveness and investigate the effect of vaccination on network stability.
- To develop the mechanism for removal of malware from WSN and improve network stability under different conditions. The rest section of the paper is structured as: related work in Section 2; Section 3 described the formulation of the SIQVD model. Equilibrium points of the system computed in Section 4 and stability analysis of the system in Section 5. Discussion of simulation results in Section 6 and finally in Section 7 conclusions along with future study.

# Analyze The Effects Of Quarantine And Vaccination On Malware Propagation In Wireless Sensor Network

## II RELATED WORK

Different types of epidemic models has been used to explain the propagation of malware in WSN. These models used the concept of epidemic theory. The epidemic theory was used for the study of biological disease spread in people [11]. But, now epidemic theory concept has become important in different area of research such as Internet of Things(IoT), social network [13], computer network [12], and Wireless Sensor Network [5, 14, 15, 16]etc. A survey paper presented by Yu et al.[30], in which they discussed the different types of mathematical models related to malware propagation. Rey and Peinado [31] discussed various mathematical models related to malware propagation in WSN. They suggested some methods for design of good mathematical model for malware propagation in WSN. The SIR (Susceptible - Infected - Recovered) model proposed De et al.[5] in which they describe the effects of worm attack on WSN. They verified the proposed model with the help of simulation outcomes. A different type of SIR-M epidemic model used by Tang and Mark [15]. They investigated the spreading behaviour of virus in WSN. The concept of sleep mode and working mode used by them for maintenance of infected sensor nodes. The removal operation of virus from infected sensor nodes can be easily perform during its sleep mode. The maintenance model useful for improvement of WSN lifetime along with security. The model assumptions were verified by simulation results. Wang and Yang [16] presented a SI (Susceptible-Infected) model with MAC mechanism to control the virus spread in WSN. The various aspects of security was discussed in this model and suggested techniques for virus spreading control. Tang [19] introduced a modified SI model for the study of virus spread in WSN. The author suggested a mechanism for prevention of virus spread in WSN. This model provides an idea for improvement of antivirus capability against virus attack. The proposed concept was justified by exhaustive simulation results. Subsequently, Tang and Li [20] proposed an adaptive SI model to control virus spread in WSN. They compare the traditional SI model with modified model. They utilized the sleep mode of sensor node for system maintenance and improved antivirus capability along with WSN lifetime. The two adaptive methods for virus spread control have been discussed. These methods are TNP technique and PNP technique. They also obtained the operational conditions of the WSN in presence of virus in the system. The effects of various parameters have been discussed. Tang et al.[21] proposed a different modified SIS model for investigation of virus spread in WSN. They explained that the virus spreads in WSN through normal data communication or piggybacking. They assumed that all nodes are equipped with antivirus and activate periodically for checking the status of sensor nodes. The adjustable virus control technique was proposed by them. This technique helps to avoid the WSN failure due to virus attack. The analysis was conformed through simulation results. An improved SIRS (iSIRS) model proposed by Wang and Li [17] in which to consider the dead node along with susceptible, infectious and recovered nodes in the model. They discussed energy consumption of sensor nodes and propagation of malicious in WSN. There was drawback associated with this model like working state of sensor nodes. In this model sensor nodes were always in active mode. They proposed an another model expanded iSIRS

(EiSIRS) [18] model. This model conquered the shortcomings of existing iSIRS model. This model described the multi-worm propagation in large scale sensor networks. In this model they used the concept of active and sleep mode of sensor node. The method has been discussed in this paper for improvement of WSN lifetime against worm attack. The simulation has been performed for validation of model. The malware prevention method has been discussed by Zaobo et al.[32]. They focused on malware prevention methods. The concept of spatial-temporal has been used along with different parameters. The dead node was also considered in the method of malware dynamics study. The above models did not discussed some important issues such as equilibrium points existence, stability of the system, basic reproduction number ( $R_0$ ), etc. The basic reproduction number ( $R_0$ ) used for the analysis of system dynamics. This term has been borrowed from bio-mathematics. De et al.[6] proposed an epidemic model for the study of virus spread in WSN. They described the various aspects of virus attack on WSN. The recovery method of infectious sensor nodes has been explained. They also obtained a controlling factor of the system. This factor was known as basic reproduction number( $R_0$ ). They also explained the cardinal property of basic reproduction number( $R_0$ ). The effects of vaccination on WSN has been demonstrated by Mishra and Keshri [2] using SEIR-V epidemic model. They described the temporal and spatial worm propagation dynamics in WSN. They derived the expression of basic reproduction number. The analysis of stability of the system under various conditions has been performed and compute the equilibrium points for worm-free state as well as endemic state. They also described the effects of different epidemic states and parameters. Furthermore, Mishra et al.[33] investigated a the effect of quarantine on infected WSN. The quarantine scheme was used to isolate the infectious nodes from the network and stop further worm propagation. They also compute the basic reproduction number for SIQRS model and equilibrium points for worm-free and endemic state. Some numerical examples was illustrated and perform the simulation for verification of the proposed model. The one different SIQR model proposed by Khanh [33] in which to include the quarantine state of sensor node. This model described the dynamics behaviour of worm dissemination in WSN. Author discussed the local and global stability of the system. For these analysis used Jacobin matrix and method of Lyapunov function. Further, Ojha et al.[34] proposed a modified SIQR model and analyze the performance of WSN against worm attack. The stability study of the system has been investigated. And the role of basic reproduction number has also discussed. An another SIRS epidemic model proposed by Liping et al. [22] for the analysis of worm spreading effects on WSN. The stability conditions of the system has been obtained in different states such as worm-free and endemic. The basic reproduction number of the model and equilibrium points of the system was calculated. For the verification of theoretical findings they performed simulation. These models did not included the dead state of nodes in the analysis.

A SIDR model was presented by Srivastava et al.[23] for the study of worm propagation. They considered dead state and analyze its importance. They obtained the value of basic reproduction number and discussed system stability.

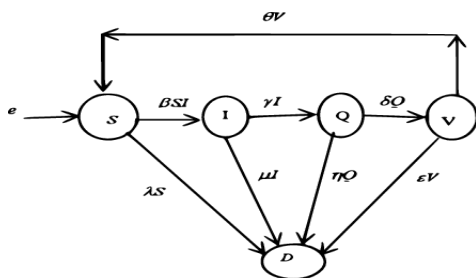
The effects of worm attack has been analyzed under different conditions of provide a mechanism for reduction of worm spread. The theoretical studies were verify by simulation results and discussion.

Ojha et al.[24] investigated a SEIRS model for the study of worm propagation in WSN. They investigated the conditions of system stability in worm-free and endemic equilibrium state. They also calculated the value of basic reproduction number and effect of various parameters. The proposed model was compared with SIRS [22]. For justification of the study perform simulation with the help of MATLAB.The proposed model considered the dead state of sensor node along with vaccination and quarantine state. The model focused on the infected isolation and immunization of infested nodes. This model improves the security aspect of and lifetime of WSN.

**A Formulation of the SIQVD model**

We formulated a model based on epidemic theory in context of malware attack in WSN. The SIQVD model is proposed for the study of malware dynamics propagation in WSN. This is a newer type of model which can be used for combating malware from WSN. We obtained the mathematical conditions for the existence of WSN under malwre attack. For designing of energy efficient system, we considered the sensor nodes working in working and sleep mode. These modes of sensor nodes considered for investigation of attacking behaviour of malware propagation in WSN. In this model there are different five states. Let the total number of nodes in the network at any time  $t$  is  $N$ . The node states are as Susceptible state ( $S$ ), Infectious state ( $I$ ), Quarantine state ( $Q$ ), Vaccination state ( $V$ ) and Dead state ( $D$ ). The different states of the proposed model are:

- Susceptible nodes ( $S$ ): sensor nodes are not infected by malware yet but these are unprotected in WSN against attacks.
- Infectious nodes( $I$ ): these sensor nodes have been attacked by malarware in WSN and these nodes have capability to spread infection in susceptible nodes.
- Quarantine nodes ( $Q$ ): these are the isolated nodes of WSN, which can not communicate with other nodes of the network.
- Vaccinated nodes ( $V$ ): these are the immunized nodes of the system.
- Dead nodes ( $D$ ): sensor nodes which energy have been exhausted, they can not communicate with other nodes. These nodes have not ability to propagate malware in WSN.



**Figure 1: Flow Diagram Of Malware Propagation In WSN**

Figure 1 represent the flow diagram of malware propagation in WSN. In a network the total number of nodes

is  $N(t)$  at any time  $t$ . The nodes of the WSN of five sub-class such as Susceptible  $S(t)$ , Infectious  $I(t)$ , Quarantine  $Q(t)$ , Vaccinated  $V(t)$  and Dead( $D$ ).

$N(t) = S(t) + I(t) + Q(t) + V(t) + D(t)$ , fulfill this condition at any time  $t \geq 0$ .

Some assumptions have been made for the formulation of model. In the beginning, each sensor nodes of WSN are in susceptible state. Once malware comes into WSN, the state of sensor node may change according to the following assumptions:

- When infectious nodes of the system in working state, they interact with susceptible nodes and transmit the infection. The susceptible nodes moves into infectious node as a function  $\beta SI$ . Some of the susceptible nodes become dead due to exhaust of node’s energy or software/hardware failure with probability  $\lambda$ .
- When infectious nodes of the system get identified then move into quarantine state with rate  $\gamma$ . Some node’s energy get exhausted or failure of software/hardware become dead with probability  $\mu$ .
- The quarantine nodes of the system do not communicate with other nodes of the network. These nodes are immunized with rate  $\delta$ . Those nodes can not immunize, they become dead with rate  $\eta$ .
- Vaccinated nodes of the system moves into susceptible state with probability  $\theta$ . Some nodes may lost their energy or software/hardware failure may become dead with probability  $\epsilon$ .
- When quarantine and vaccinated nodes of the system are in sleep mode then susceptible nodes and infectious nodes of the system are communicating with each others and infectious node sends malware with data packets. The malwares spread into WSN when an infected data or worm is transmitted from an infectious node to the susceptible types of nodes.

The transition state of the nodes for SIQVD model govern by the set of differential equations as:-

$$\left. \begin{aligned} \frac{dS}{dt} &= e - \beta SI - \lambda S + \theta V, \\ \frac{dI}{dt} &= \beta SI - I(\mu + \gamma), \\ \frac{dQ}{dt} &= \gamma I - Q(\delta + \eta), \\ \frac{dV}{dt} &= Q\delta - V(\theta + \epsilon), \\ \frac{dD}{dt} &= S\lambda + \mu I + \eta Q + \epsilon V. \end{aligned} \right\} (1)$$

Where  $S(t) + I(t) + Q(t) + V(t) + D(t) = N(t)$ . Meaning of the used parameters are listed in Table 1. The SIQVD model system dynamics is expressed in the domain  $\Gamma = \{(S, I, Q, V, D)\} \in R_5^+$  and all state variable will be positive for all  $t \geq 0$ .

**Table 1: Details Of Parameters Used**

S.No	Parameter	Meaning of Parameter
1	$e$	New sensor nodes addition in the WSN
2	$\mu$	Infectious sensor nodes become dead with probability $\mu$ , may be due to exhaust of node’s energy or failure of software/hardware
3	$\beta$	Probability of malware transmission WSN



# Analyze The Effects Of Quarantine And Vaccination On Malware Propagation In Wireless Sensor Network

4	$\lambda$	Susceptible sensor nodes become dead with probability $\lambda$ , may be due to exhaust of node's energy or failure of software/hardware
5	$\gamma$	Rate of moving the infectious nodes into quarantine nodes
6	$\delta$	Rate of immunization of quarantined nodes
7	$\varepsilon$	Vaccinated sensor nodes become dead with probability $\varepsilon$ , may be due to exhaust of node's energy or failure of software/hardware
8	$\eta$	Quarantine sensor nodes become dead with probability $\eta$ , may be due to exhaust of node's energy or failure of software/hardware
9	$\theta$	Probability of converting vaccinated nodes into susceptible nodes

### III EQUILIBRIUM POINTS OF THE SYSTEM

We will investigate the two types of equilibrium points of the system. In one condition, when the malware infection exits in WSN, i.e.  $I \neq 0$  and in the other condition when the malware infection dies out, i.e.  $I = 0$ . In case of malware-free equilibrium, i.e.  $I = 0$ . Therefore, the system of equation (1) will be given as

$$\left. \begin{aligned} \frac{dS}{dt} &= e - \beta SI - \lambda S + \theta V = 0 \\ \frac{dI}{dt} &= \beta SI - I(\mu + \gamma) = 0 \\ \frac{dQ}{dt} &= I\gamma - Q(\delta + \eta) = 0 \\ \frac{dV}{dt} &= Q\delta - V(\theta + \varepsilon) = 0 \\ \frac{dD}{dt} &= S\lambda + \mu I + \eta Q + \varepsilon V = 0 \end{aligned} \right\} (2)$$

After solving the system of equation (2), we found malware-free equilibrium points. The malware-free points of the system at  $P_0 = (S_0, I_0, Q_0, V_0) = (\frac{e}{\lambda}, 0, 0, 0)$ . In case of endemic equilibrium  $I \neq 0$ . The endemic equilibrium points are given as  $P^* = (S^*, I^*, Q^*, V^*)$  as

$$S^* = \frac{(\mu + \gamma)}{\beta}, I^* = \frac{e(\theta + \varepsilon)(\delta + \eta)}{L^*} \left\{ 1 - \frac{1}{R_0} \right\},$$

$$Q^* = \frac{e\gamma(\theta + \varepsilon)}{L^*} \left\{ 1 - \frac{1}{R_0} \right\}, V^* = \frac{e\gamma\delta}{L^*} \left\{ 1 - \frac{1}{R_0} \right\}$$

where  $L^* = (\gamma + \mu)(\theta + \varepsilon)(\delta + \eta) - \theta\gamma\delta$  and  $R_0 = \frac{e\beta}{\lambda(\gamma + \mu)}$ , where  $R_0$  [28] is the basic reproduction number. It is explicit that  $P^*$  will be exist uniquely if  $R_0 > 1$ .

### IV STABILITY ANALYSIS OF THE SYSTEM

The malware-free equilibrium  $P_0$  of system given by a set of equations (1) is locally asymptotically stable(LAS)in  $\Gamma$  if its all eigenvalues are less than zero.

*Proof.* For the stability of the system (1) at point  $P_0$ , the Jacobian matrix can be considered as

$$J(P_0) = \begin{bmatrix} -\lambda & -\beta \frac{e}{\lambda} & 0 & \theta \\ 0 & \beta \frac{e}{\lambda} - (\gamma + \mu) & 0 & 0 \\ 0 & \gamma & -(\delta + \eta) & 0 \\ 0 & 0 & \delta & -(\theta + \varepsilon) \end{bmatrix} (3)$$

The eigenvalues of equation (3) are :  $\omega_1 = -\lambda, \omega_2 = -(\delta + \eta), \omega_3 = -(\theta + \varepsilon)$  and  $\omega_4 = (R_0 - 1)(\gamma + \mu)$  The value of all four eigenvalues  $\omega_1, \omega_2, \omega_3$  and  $\omega_4$  are

negative, when  $R_0 < 1$ . Hence, the system will be locally asymptotically stable(LAS)in  $\Gamma$ . On other hand, we found from  $\omega_4$  if  $R_0 > 1$ , the system becomes unstable.

Worm endemic state (WES) is locally asymptotically stable, if  $R_0 > 1$ .

*Proof.* For the stability of the system (1) at point  $P_0^*$ , the Jacobian matrix can be considered as

$$J(P_0^*) = \begin{bmatrix} -\beta I^* - S - \omega & -\beta S & 0 & \theta \\ 0 & \beta I^* \beta S - (\gamma + \mu) - \omega & 0 & 0 \\ 0 & \gamma & -(\delta + \eta) - \omega & 0 \\ 0 & 0 & \delta & -(\theta + \varepsilon) - \omega \end{bmatrix} (4)$$

The two eigenvalues of matrix (4) are  $\omega_1 = (-\eta + \delta), \omega_2 = -(\theta + \varepsilon)$  and other two eigenvalues of the quadratic equation (5) are

$$a_0 \omega^2 + a_1 \omega + a_2 = 0 (5)$$

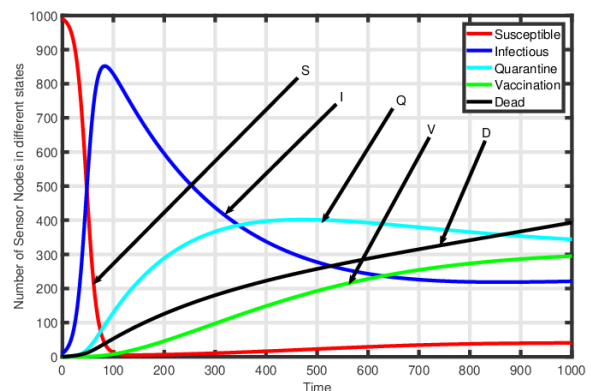
where  $a_0 = 1, a_1 = \frac{e\beta(\theta + \varepsilon)(\delta + \eta)}{L^*} \left\{ 1 - \frac{1}{R_0} \right\} + \frac{(\gamma + \mu)}{\beta}$

$$a_2 = \frac{e\beta(\theta + \varepsilon)(\delta + \eta)}{L^*} \left\{ 1 - \frac{1}{R_0} \right\} \gamma - \frac{e(\gamma + \mu)}{\lambda R_0}$$

It is clear that all coefficients of equation (5)  $a_0, a_1, a_2$  are positive when  $R_0 > 1$ , thus, from Routh-Hurwitz criteria, roots of equation (5) are real and negative. Therefore, the endemic equilibrium at  $P^*$  is locally asymptotically stable if  $R_0 > 1$ .

### V ANALYSIS OF SIMULATION RESULTS

For the verification of theoretical findings, we performed simulations on MATLAB. The effects of various parameters on malware propagation in WSN is analyzed. Taking the values of different parameters for simulations are  $e = 0.31, \theta = 0.002, \beta = 0.0001, \eta = 0.0001, \lambda = 0.0001, \mu = 0.001, \gamma = 0.0029, \varepsilon = 0.0001$  and  $\delta = 0.002$ . Assume that at time  $t = 0$  the values of  $S(0), I(0), Q(0), V(0)$  and  $D(0)$  be 990, 10, 0, 0, and 0 respectively. The value of basic reproduction number  $R_0 = 79.4872$ , which is greater than one.



**Figure 2: Malware Propagation dynamics with time when  $R_0 > 1$**

Figure 2 shows the effects of malware propagation in WSN, this represent the values of different states of sensor nodes with respect to time in condition of ( $R_0 = 79.4872$ )  $R_0 > 1$ . It is found from Fig. 2 that the number of infectious, quarantine, vaccinated and dead nodes increases and at the same time number of susceptible nodes decreases.



The infectious number of nodes attain the maximum value in a small time then start to decrease and become stable. From Fig. 2, it is also observed the value of  $I \neq 0$ . This is the case of endemic equilibrium. In this condition the malware persist in WSN continuously. This is also verify theorem 2.

For the different set of simulation taking the values of parameters  $e = 0.22$ ,  $\theta = 0.002$ ,  $\beta = 0.00001$ ,  $\eta = 0.0001$ ,  $\lambda = 0.0002$ ,  $\mu = 0.007$ ,  $\gamma = 0.008$ ,  $\varepsilon = 0.0001$  and  $\delta = 0.002$ .

After computation found the value of basic reproduction number  $R_0 = 0.73$ , which is less than one.

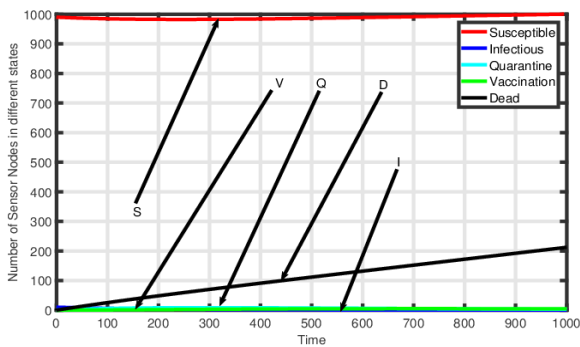


Figure 3: Malware Propagation dynamics with time when  $R_0 < 1$

Figure 3 shows the effects of malware attack in WSN when value of  $R_0 = 0.73$  is less than one. It is concluded from Fig. 3 that the malware dies out from WSN. We observed from Fig. 3 that the number of dead nodes increases linearly with time. This indicated that even if the system is in malware-free state, the sensor nodes die out due to exhaust of nodes' energy or may be failure of hardware/software. The theorem 1 is satisfied and obtained malware-free state.

Analyze the effect of quarantine state by changing the values of quarantine rate.

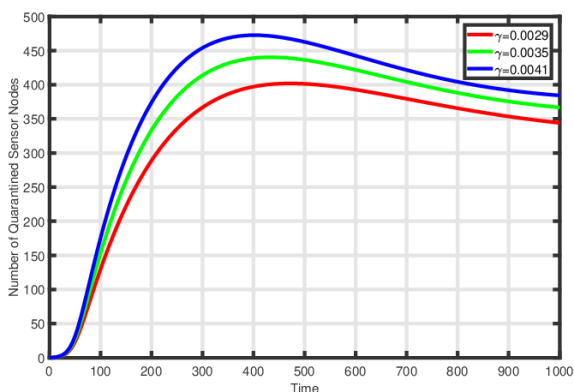


Figure 4: Effect of quarantine state on malware propagation

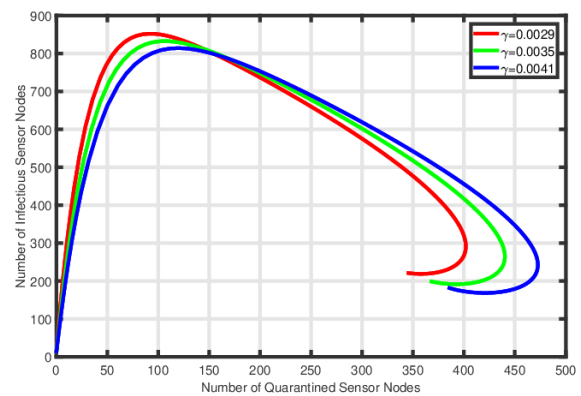


Figure 5: Effect of quarantine rate on infectious nodes

Figure 4 and 5, illustrate the effects of quarantine state on malware propagation in WSN. we observed from Fig.4, when value of quarantine rate  $\gamma$  increases then the number of isolated nodes also increases. This technique is useful for highly infectious network, because quarantine nodes can not interact with other nodes of the network. Therefore, malware propagation becomes stopped. Figure 5 shows that when the value of quarantine rate increases the number of infectious nodes decreases. From Fig. 4 and 5, we establish that malware propagation can be terminated or minimize using this method. Investigate the effect of vaccination state by changing the values of vaccination rate.

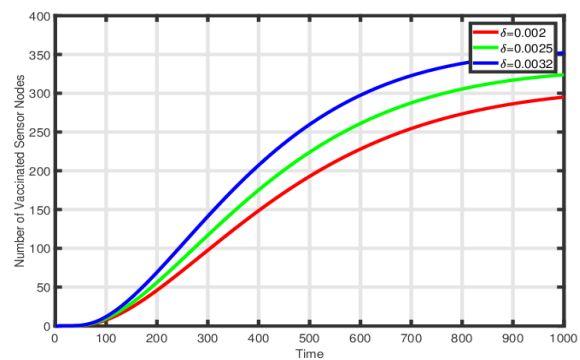


Figure 6: Effect of vaccination state on malware propagation

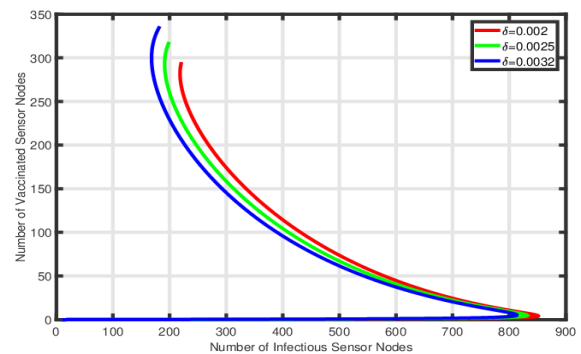


Figure 7: Effect of vaccination rate on infectious nodes

# Analyze The Effects Of Quarantine And Vaccination On Malware Propagation In Wireless Sensor Network

Figure 6 and 7, illustrate the effects of vaccination state on malware propagation in WSN. we observed from Fig.6, when value of vaccination rate  $\gamma$  increases then the number of vaccinated nodes also increases. This is a method of immunization of sensor nodes. This technique is used for removal of malware from WSN. Execute the antivirus by leveraging the sleep mode of sensor node. This technique improve the resistance capability of sensor nodes and combat malware propagation in the network. Figure 7 demonstrates that when the value of vaccination rate increases the number of infectious nodes decreases. From Fig. 6 and 7, we establish that stability of the system can be against malware attack by the method of immunization. We conclude from above analysis combined effect of isolation and immunization increase the network stability and life time of WSN.

## VI CONCLUSION

The main purpose of proposed model is to combat the malware propagation from the network and elongate the life time of WSN. For that purposed an epidemic based SIQVD model. We analyzed the dynamic behaviour of malware propagation in WSN. The two types of equilibrium points of the system has been obtained. One is malware-free and other is endemic. The basic reproduction number ( $R_0$ ) of the proposed model has been computed, and analyzed its effect in the analysis of system dynamics. We observed from analysis, if  $R_0 < 1$  the system will be stabilize and free from malware, and when  $R_0 > 1$  then malware survives in the system at endemic state. The effects of quarantine state and vaccinated state have been discussed in this paper. We also found that if the rate of quarantine or vaccination increases the number of infectious nodes decreases. The combined technique of quarantine and vaccination improved the network stability along with life time of WSN. Hence, for design and development of secure WSN the combined technique is magnificent. In future communication radius, spatial correlation, heterogeneous nodes and nodes density can be included.



## REFERENCES

1. Akyildiz, I.F., Su, Weilian, Sankarasubramaniam, Y., and Cayirci, E., "Wireless sensor networks: a survey", Computer Networks, Elsevier Science B.V., vol.38(4), pp.393-422(2000).
2. Mishra, B.K., and Keshri, N., "Mathematical model on the transmission of worms in Wireless Sensor Network", Applied Mathematical Modelling, vol.37(6), pp.4103 - 4111 (2013).
3. López, M., Peinado, A., & Ortiz, A., "A SEIS Model for Propagation of Random Jamming Attacks in Wireless Sensor Networks", International Joint Conference SOCO'16-CISIS'16-ICEUTE'16 Advances in Intelligent Systems and Computing, pp. 668-677, (2016), León, Spain.
4. Jacques, M. B., Christophe G., Mourad, H., and Abdallah, Makhoul: Epidemiological approach for data survivability in unattended wireless sensor networks., Journal of Network and Computer Applications, 46, 374 - 383 (2014)
5. De, Pradip., Liu, Yonghe., and Das, S. K., "An Epidemic Theoretic Framework for Vulnerability Analysis of Broadcast Protocols in Wireless Sensor Networks", IEEE Transactions on mobile Computing, vol.8(3), pp.413-425(2009).
6. 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).
7. Ojha, R.P., Sanyal, G., 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 18(3), 229-241(2017).
8. Haghghi, 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, vol.11(12), pp.2854-2865 (2016).
9. Upadhyay, R.K., and Kumari, S., "Bifurcation analysis of an e-epidemic model in wireless sensor network", International Journal of Computer Mathematics, vol.95(9), pp.1775-1805, (2017).
10. Lin, C.Y., Tseng, Y.C., and Lai, T. H., "Exploiting Spatial Correlation at the Link Layer for Event-driven Sensor Networks", Int. J. of Sensor Networks, Vol. 1(3/4), pp.197-212, (2012).
11. Kermack, W.O., and McKendrick, A. G., "A contribution to the mathematical theory of epidemics", The Royal Society, vol.115 (772), pp.700-721 (1927).
12. Upadhyay, R., Kumari, S., and Misra, A., K., "Modeling the virus dynamics in computer network with SVEIR model and nonlinear incident rate", Journal of Applied Mathematics and Computing, vol.54(1), pp.485-509, (2017).
13. He, Z., Cai, Z., Yu, J., Wang, X., Sun, Y., and Li, Y., "Cost-Efficient Strategies for Restraining Rumor Spreading in Mobile Social Networks", IEEE Transactions on Vehicular Technology, vol.66(3), pp.2789-2800, (2017).
14. Song, Y., and Jiang, G. P., "Model and Dynamic Behavior of Malware Propagation over Wireless Sensor Networks", In: Zhou J. (eds) Complex Sciences. Complex 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 4., pp. 487-502 (2009) Springer, Berlin, Heidelberg.
15. Tang, S., and Mark, B. L., "Analysis of Virus Spread in Wireless Sensor Networks: An Epidemic Model", Proceedings of the 2009 7th International Workshop on the Design of Reliable Communication Networks, DRCN 2009, pp. 86-91. November 2009, Washington, DC, USA.
16. Wang, Y.Q., and Yang, X., Y., "Virus spreading in wireless sensor networks with a medium access control mechanism", Chin.Phys.B, vol.22pp.(4:040206), (2013).
17. Wang, X., M., and Li, Y., "An improved SIR model for analyzing the dynamics of worm propagation in wireless sensor networks", Chinese Journal of Electronics, vol.18(1), pp.8-12, (2009).
18. Wang, X., Li, Q., & Li, Y., "EiSIRS: A formal model to analyze the dynamics of worm propagation in wireless sensor networks", Journal of Combinatorial Optimization, vol.20(1), pp.47-62, (2010).
19. Tang, S.: A Modified SI Epidemic Model for Combating Virus Spread in Wireless Sensor Networks., Int. J Wireless Inf Networks, 18: 319-326 (2011). : 10.1007/s10776-011-0147-z
20. Tang, S., and Li, W., "An epidemic model with adaptive virus spread control for Wireless Sensor Networks", International Journal of Security and Networks, vol.6(4), pp. 201-210, (2011).
21. Tang, S., Myers, D., and Yuan, J., "Modified SIS epidemic model for of virus spread in wireless sensor networks", Int. J. Wireless and Mobile Computing, vol.6(2), pp. 99-108, (2013).
22. Feng, L., Song, L., Zhao, Q., and Wang, H., "Modeling and Stability Analysis of Worm Propagation in Wireless Sensor Network", Mathematical Problems in Engineering, 2015, 2015, 129598.
23. Srivastava, A.P., Awasthi, S., Ojha, R.P., Srivastava, P.K., and Katiyar, S., "Stability Analysis of SIDR Model for Worm Propagation in Wireless Sensor Network", Indian Journal Of Science and Technology, Vol. 9(31), pp.1-5, August 2016.
24. Ojha, R.P., Srivastava, P.K., and Sanyal, G., "Improving wireless sensor networks performance through epidemic model", International Journal of Electronics, Vol. 106, issue 6, pp.862-879, 2019.
25. Shakya R.K., Singh Y.N., and Verma N.K., "A Correlation Model for MAC protocols in Event-driven Wireless Sensor Networks", Proceedings IEEE Region 10 conference TENCON 2012, Cebu City, Philippines, (2012).
26. Shakya R.K., Singh Y.N., and Verma N.K., "A Novel Spatial Correlation Model for Wireless Sensor Network Applications", Proceedings IEEE WOCN 2012, pp. 1-6. Indore City (MP), India, (2012).
27. Shakya R.K., Singh Y.N., and Verma N.K., "Generic Correlation Model for Wireless Sensor Network Applications", Journal of IET Wireless Sensor Systems, vol.3(4), pp.266-276, (2013).
28. Driessche, P.V., and Watmough, J., Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission, Mathematical Biosciences, 180(1), 29-48, https://doi.org/10.1016/S0025-5564(02)00108-6.

29. LaSalle, J.: The stability of dynamical systems, CBMS-NSF Regional Conference Series in Applied Mathematics, pp 96-106, (1976) <https://doi.org/10.1137/1.9781611970432>.
30. Yu, S.; Wang, G.; Zhou, W. Modeling malicious activities in cyber space. IEEE Netw. 2015, 29, 83-87.
31. del Rey A.M., Peinado A. (2018) Mathematical Models for Malware Propagation in Wireless Sensor Networks: An Analysis. In: Daimi K. (eds) Computer and Network Security Essentials. Springer, Cham
32. He Z., Lin Y., Liang Y., Wang X., Vera Venkata Sai A.M., Cai Z. (2019) Modeling Malware Propagation Dynamics and Developing Prevention Methods in Wireless Sensor Networks. In: Du DZ., Pardalos P., Zhang Z. (eds) Nonlinear Combinatorial Optimization. Springer Optimization and Its Applications, vol 147. Springer, Cham
33. Khanh, N.H.: Dynamics of a worm propagation model with quarantine in wireless sensor networks, Appl. Math. Inf. Sci., 2016, 10, (5), pp. 1739-1746.
34. Ojha, R. P., Sanyal, G., 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, vol. 18, no. 3, pp. 229-241, 2017.

### AUTHORS PROFILE

	<p><b>Satya Ranjan Biswal</b> is working as Associate Professor in Department of Computer Science &amp; Engineering, Trident Academy of Technology, Bhubaneswar, Odisha. He has completed M.Tech. in CSE from Utkal University, Bhubaneswar, Odisha and continuing Ph.D. scholar in Department of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, Odisha. He has twelve years of academic experience and three years of industry experience. He has published five international journal research papers and three international conference papers. His areas of interest are Computer Security, Software Engineering, IoT and Computer Architecture and Computer Networks. He is a life time Member of Indian Society of Technical Education (ISTE) and Computer Society of India (CSI).</p>
	<p><b>Santosh Kumar Swain</b> is a Professor in department of Computer Engineering, KIIT Deemed to be University, Bhubaneswar, Odisha. He has completed Ph.D. degree in Computer Science and Engineering from KIIT Deemed to be University, Bhubaneswar. He has twenty-eight years of academic experience and one year of industry experience. His areas of interest are Software Engineering, Computer Security, Compiler Design, and Data Mining &amp; machine Learning. He has written three books in the area of Computer Science. He has published around twenty international and national journal research papers and also ten international conference papers. He is a regular visiting faculty member of many Universities and educational institutions of national repute. Under his guidance, three Ph.D. research scholars have been awarded. He is a Life Time Member of Indian Society of Technical Education (ISTE) and also of Indian Science Congress (ISC).</p>