Jewel Journal of Scientific Research (JJSR) 7(2): 236–248, 2022
©Federal University of Kashere-Nigeria (Print ISSN: 2384 – 6267, Online ISSN 2756-651X)
jjsr.fukashere.edu.ng

Mitigation-Based Approach for Self-Propagating Worms in Wireless Sensor Network

***[1]Mohammed, Ibrahim**
[1]Department of Computer Science, Kaduna State University, PMB 2339, Tafawa Balewa, Way, Kaduna, Nigeria
***Corresponding Author**: mohammed.ibrahim@kasu.edu.ng; +2348076331586

Abstract
An attacker can copy malicious code from one memory location to another to spread a worm attack, resulting in malicious code stored in a contagious memory region. In the event of malware repeating the same process to the neighbouring sensor nodes, the memory efficiency of the infected node can affect the propagation dynamics of the worm attack. However, the existing worm propagation models do not consider the memory efficiency of the infected nodes while mitigating worm propagation. Consequently, this work proposed a Susceptible-Infectious-Abandon-Quarantine (SIAQ) model to mitigate worm propagation based on memory efficiency. To achieve this, the SIAQ model inspired by the epidemic model can mitigate the worm propagation by isolating infected memory-efficient nodes from the wireless sensor network (WSN). In this regard, the infected memory-efficient nodes are subjected to a sleeping mode. In a sleeping mode, the infected memory-efficient nodes cannot further interact with the other nodes in a WSN. Finally, the basic reproduction number is obtained to serve as a benchmark in determining the model's performance on the infection peak value. Based on the numerical simulation conducted, the result of the proposed SIAQ model outperforms the previous SIQR model at about 40% in mitigating worm propagation at the worm-endemic equilibrium state. Consequently, the proposed model can serve as a basis for assisting in planning, design, and defence of such networks from the investigator's point of view.

Keywords: Infection, Memory, Nodes, Susceptible, Worm

Received: 25th Sept., 2022 *Accepted:* 24th Dec, 2022 *Published Online:* 27th Dec., 2022

Introduction

Advancement in sensor technology has revolutionized traditional wired devices into a wireless sensor network (WSN). The emergence of WSNs exhibits promising potential in developing new technology such as smart homes, biological monitoring, battlefield surveillance, and target tracking (Wang *et al.*, 2010). WSNs, as shown in Figure 1, are made up of small-sized, cheap, low-energy and multi-functional devices commonly referred to as sensors that are deployed to extract data from an environment or monitor an incident (Akyildiz *et al.*,2002). In this regard, each wireless sensor node is equipped to sense, measure, and gather data from the surrounding environment. After that, the sensor data can be transmitted to the user (Khanh, 2016).

Although WSN exhibits promising applications in various fields, the weaknesses associated with the sensor nodes can result in an aggressive attack from perpetrators. As previously shown, the attacker can exploit different mechanisms of sensor nodes and spread malicious codes throughout the entire network without physical contact (Giannetsos *et al.*, 2009).

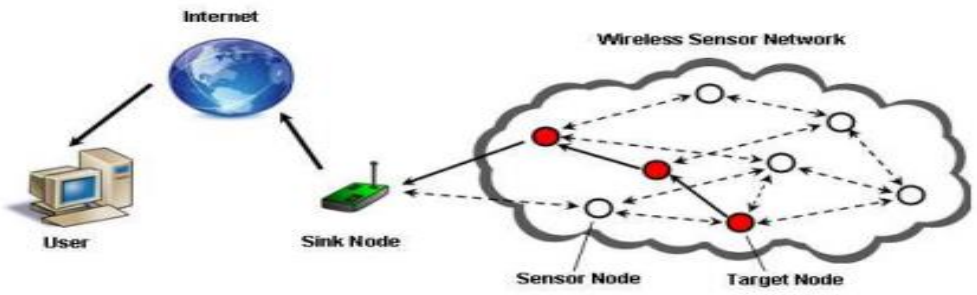

Figure 1. Sensor network communication structure (Khanh, 2016).

Consequently, this can lead to a worm attack that can be achieved by exploiting memory-related vulnerabilities. According to Giannetsos *et al*. (2009), the vulnerabilities of sensor nodes in which the same program images can be executed through various sensor nodes can lead to a self-propagating packet for injecting malicious code. As such, multi-worm spreading will become the main attack way in large-scale WSNs in the future (Wang et al., 2010).

Related Work

While highlighting factors that differentiate worm propagation in an Internet-based network from WSN, Wang *et al*. (2010) argued a need to develop a novel formal model. The formal model should describe the dynamic process of worm propagation that is distinguished from Internet worm propagation. Consequently, Wang *et al*., (2010) proposed an EiSIRS model that can precisely describe the process of worm propagation in WSN. Besides, a necessary condition for a worm to spread in a WSN was theoretically derived from incorporating working and sleeping states as influential factors. Based on these factors, various states were defined that include the Susceptible working node(S); in these states, nodes have not been infected by any nodes, Susceptible sleeping class (S') nodes in this class the nodes have not been infected and are sleeping with an assumption that worm will not try to infect them, the reason is that these nodes cannot communicate with their working neighbours. The next class is the Infectious working node (I); this class consists of nodes affected by worms and can infect some susceptible nodes. Another class is Infectious sleeping nodes(I'), which are infected but remain in sleep mode and cannot infect other nodes. The next class is the recovered working class(R), consisting of nodes that recover from the infection and currently working with the possibility of reinfections by neighbouring infected working nodes. And recover sleeping class(R') classes are recovered but remain in sleeping states and worms cannot try to affect them. Lastly is the Dead node class (D).

In the D class, nodes have exhausted energy and cannot be infected by the worm. By associating these classes with various WSN parameters, the simulation results indicate that the dynamic characteristics of worm propagation are related to energy consumption, network topology, sleep, and the work interleaving schedule policy of large scale WSN. However, how to enhance the model to automatically adjust the communication range of nodes to control the worm propagation remains a challenge. To control and mitigate worm propagation in WSN, Kechen et al. (2012) studied the worm propagation dynamic of WSN with four distinct node deployment patterns and proposed a Select Immune Mechanism. The Select Immune Mechanism propagates anti-worm packets to suppress the worm propagation in WSN. The WSN is then classified into susceptible(S), Infected(I), Immune (E), and Dead nodes (D) sensor nodes. By conducting a simulation to check the mechanism effects on various nodes, it was found that worm propagation could be restrained by adding fewer efficient monitored nodes.

In similar trend, Mishra and Keshri., (2013) studied the attacking behaviour of possible

worms in WSN using a compartmental epidemic model. The model is proposed with Susceptible-Exposed-Infectious-Recovered-Susceptible and Vaccination compartments (SEIRS-V) to describe the dynamics of worm propagation with respect to time in WSN. The model was subjected to mathematical to determine the basic reproduction number R_0 to understand the propagation and fading of the worms in the wireless sensor network (WSN). Consequently, the outcome of the simulation reveals that proper vaccination of the sensor nodes will reduce the susceptibility of nodes towards the worm attack. Similarly, Mishra and Keshri., (2014) observed that worms in WSN can be contained more effectively by quarantining nodes in a group that has exhibited highly infectious behaviour.

Feng *et al*. (2015) proposed an improved Susceptible -infectious- recover- susceptible (SIRS), emphasising communication radius and distributed density of nodes and assuming a uniform distribution of nodes in a 2D space. Finally, the numerical simulations show that decreasing the value of communication radius or reducing the distributed density of nodes prevents worms from spreading WSNs effectively.

In the work of Khanh(2016), based on epidemic theory, a susceptible - infectious- quarantine - recovered (SIQR) model was proposed to describe the dynamics of worms propagation with quarantine in the wireless sensor network. Similarly, mathematical analysis shows that the dynamics of the spread of worms are determined by their threshold. If the worm-free equilibrium is globally asymptotically stable, the worm-endemic equilibrium is globally asymptotically unstable. A numerical investigation is carried out to confirm the analytical results. However, based on the results of parameter analysis, some effective strategies for eliminating worms are suggested that will decrease the contact and transformation parameters of the model can slow down the malware propagation. While investigating the effect of mobile actuators on worm propagation in WSN, Wang et al., (2017) proposed a microscopic mathematical model to describe the propagation dynamics of the sensor worm. The model follows the state transition scheme of a typical susceptible-infected (S-I) infection model but can microscopically compute the prior probability of each sensor being infected by the worm. The simulated results and comparison with the other models generated different results from various density values. Based on their findings, the involvement of infected mobile actuators reinforced worm propagation across a diverse number of tests.

Singh *et al*. (2018) studied the effect of worm propagation with various values of communication radius and node distributed density. While extending the SIRS model of Feng *et al.*, (2015), exposed and vaccination classes were added to the SIRS model. Hence, the authors developed a new model called the SEIRV model, and its stability was checked using the stability theory of differential equations. Numerical simulation of the SEIRV model was conducted with different communication radius and node density values while other parameters remain fixed. Comparing the simulation result with the existing model, the number of infectious sensor nodes responses to changes with the changes in communication radius and node density values in the proposed model. However, the number of infectious nodes remains unchanged in the existing model with the changes in communication radius. Also, it was found that the proposed scheme has a few numbers of infectious nodes for every communication range. With the previous models focusing on worm propagation, few exceptional models Acarali et al., (2019), Ji et al., (2019), Jerkins and Stupiansky, (2018) and Yin et al., (2019) have their work focusing on IoT WSN-based botnet propagation.

In any case, while previous models do consider various parameters of WSN in modelling worm propagation, the memory efficiency of the infected nodes has not been previously integrated in modelling worm propagation. As highlighted, the attacker exploits the memory of the infected node to run, execute, and store the malware packet for self-propagation to the neighbouring sensor nodes. Besides, a node's memory efficiency determines the free memory space that can speedily process malware packets and minimize packet loss

during worm propagation. However, the memory efficiency of sensor nodes varies in WSN, some nodes have higher memories than the others. Hence, there is need to analyze and mitigate worm propagation in the perspective of node's memory capability. Therefore, in this paper, we proposed a Susceptible-Infectious-Abandon-Quarantine (SIAQ) model to isolate infected nodes based on their memory efficiency to decrease the worm propagation in WSN.

Proposed Model

A Susceptible-Infection-Abandon-Quarantine (SIAQ) model is proposed, a novel model that will consider the node's processing capabilities for worm propagation. The model assumes the existence of an infected node in a WSN environment. Then the model will measures the transient behaviour of the infection concerning the worm propagation. Our focus is particularly on memory availability that determines infected nodes abandon rate based on their memory capability to propagate the malware packet. To understand the propagation and mitigation of worm attacks, respectively, clear assumptions are stated as follows:

Dynamic network with mobility of nodes that is, nodes can be added/removed from the network. A random network deployment. Homogeneous sensor nodes with different memory statuses at a particular time.

SIAQ has similar emerges from the epidemic model with add-on classes A and Q to stand for the Abandon and Quarantine nodes, respectively. In this work, the Abandon nodes defined the number of infected nodes but not infectious due to memory incapability. The Quarantine nodes are infectious memory-efficient nodes that are isolated to avoid attack propagation. The Schematic diagram of the model is shown in Figure 2; given a population of nodes as N over a series of time interval t, a set of compartments representing possible node states will emerge.

The rate of nodes change from one state to another is dynamically represented using a system of differential equations.

The susceptible state is defined as a state in which nodes are not infected but vulnerable to infections at a given time. The susceptible nodes get infected and converted to infectious states by contacting the malware packets. The infected nodes are carrier nodes affected by the malware and capable of transmitting the infections to the susceptible nodes in contact using an infection parameter. Infected nodes with low memory space and cannot transmit the copy of the malware packet to the neighbouring can be transferred to an abandoned state based on the abandoned rate. However, infected memory-efficient nodes capable of transmitting malware packets can be transferred to the Quarantine state using the isolation parameter. Then the fractions of the susceptible, infectious, Abandoned nodes and Quarantine nodes make up the total number of nodes in the population. T can be expressed mathematically in equation (1).

$$N = S(t) + I(t) + A(t) + Q(t) = \frac{S(t)}{N} + \frac{I(t)}{N} + \frac{A(t)}{N} + \frac{Q(t)}{N} \quad (1)$$

Based on the flow diagram of the model as demonstrated in Figure 2, the model can be defined mathematically using a system of differential equations as can be expressed in equation (2).

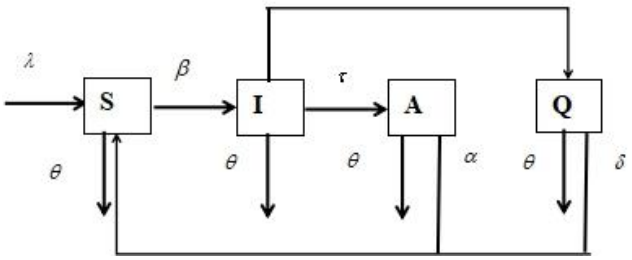

Figure 2. Flow Diagram of the proposed SIAQ model

$$\begin{aligned}\frac{dS}{dt} &= \lambda - \beta S(t)I(t) + \delta Q(t) + \alpha A(t) - \theta S(t)\\ \frac{dI}{dt} &= \beta S(t)I(t) - (\tau + \gamma + \theta)I(t)\\ \frac{dA}{dt} &= \tau I(t) - (\theta + \alpha)A(t)\\ \frac{dQ}{dt} &= \gamma I(t) - (\delta + \theta)Q(t)\end{aligned} \quad (2)$$

Where

$S(t)$ the total number of susceptible nodes in the network

$I(t)$ the total number of infectious nodes in the network

$A(t)$ the total number of abandoned infected nodes in the network

$Q(t)$ the total number of Quarantine nodes

λ number of new nodes added to the network system

β infection rate

τ Abandon rate of infected nodes

α rate of returning abandoned nodes to the susceptible class by removing the malware packet

γ rate of isolating infectious nodes.

δ Rate of transferring forensic nodes to the susceptible class due to data loss due to interaction with other nodes.

θ nodes leaving the system due to mobility or other activities.

Subsequently, the attacker will expand its attack surface to the susceptible sensor nodes by attacking a particular node and successfully getting infected. Nodes in the susceptible class S can be lost due to coming in contact with the malware packet. The infection of nodes can be achieved via random scanning of all the sensor nodes in the IoT network. Consequently, the susceptible nodes will transit to the infectious state I. Therefore, infected nodes can be identified from the I state and transits to the Quarantine state Q at a probability complement of the abandon rate $\gamma = (1-\tau)$. At the Quarantine state, nodes can similarly lose their data due to interaction with other nodes and return to the susceptible class S at the rate of δ . Finally, at every stage of the model, there is a probability θ of removing a node (s) due to mobility and other influential factors that affect WSN.

Nodes Population and Scoping

WSN consists of small sensing devices with constricted bandwidth, power, and computational capabilities. In this regard, the sensing coverage per sensor node to determine the communication range based on the radius of the sensor. The nodes population is initially deployed in a small area with all the sensor nodes considered susceptible. We consider the infection to randomly scan all the susceptible nodes within the coverage of the infected node. We similarly assume that the population consists of a dynamic number of nodes with removing and addition of nodes back to the network.

Infection Rate

The worm self-propagation starts with the infection process, where the malware uses different scanning methods to capture large number of targets to be infected. In this regard, the infected nodes can propagate and execute the attack on the remaining susceptible nodes. Hence, the infection rate is the ratio of the number of infected nodes to the number of susceptible nodes multiplied by the contact rate at a given time. It can be expressed equation(3)

$$\beta = \frac{I(t)}{S(t)} \times contactrate \quad (3)$$

Abandon Rate

Hejazi and Ferrari (2018) denote ζm ∈ [0, 1] as the fraction of the remaining free memory in

sensor nodes during propagation of sensed data and its coefficient can thus be expressed in equation (4)

$$\zeta_m = \frac{r_m}{i_m} \quad (4)$$

Where r_m is the remaining free memory of each node and i_m is the initially available memory? Hence, the probability of abandoning an infected node τ depends on the attacker's size of the malware packet installed on the infected node and the fraction of the remaining free memory of the infected node during propagation. The processing of malware packet and the abandon probability rate can be mathematically expressed in equations (5) and (6), respectively:

$$\text{Malware}_{\text{process}} = \text{Size} \times \zeta_m \quad (5)$$

$$\text{Abandon rate } \tau = \frac{1}{Malware_{\text{Process}}} \quad (6)$$

Isolation Rate

The rate of isolating infectious memory-efficient nodes depends largely on the sensor's capability to process and propagate the malware packet. The malware packet can spread with the normal data to the neighboring nodes in a worm attack. Therefore, the expected infected memory-efficient nodes that propagate the malware due to their memory capabilities can be isolated to the Quarantine class. Therefore, the isolation γ is the probability complement of the abandon rate τ as adopted from Ibrahim (2021) and is given using the equation (7).

$$\text{Isolation rate } \gamma = 1 - \tau \quad (7)$$

The isolation rate subjects infected memory-efficient nodes to a sleep mode; they cannot transfer data or malware packets to the neighbouring nodes.

Data Loss Rate

Certain operations in WSN associating one node to another can result in data consumption among neighbouring nodes. Hence, nodes can be isolated in quarantine class but can lose their data and return to the susceptible class S. We defined the data loss rate δ using equation (8) due to their associated services.

δ = number of packet sent × Contact rate. (8)

Stability Analysis of the model

The analysis techniques utilized mostly in malware propagation works are based on stability analysis of the proposed model (Gardner et al., 2017). The concept generally is to understand the steady-state effects of different parameters in the models. To achieve this, the basic reproduction number R_0 which determines the number of secondarily infected nodes produced by a single (typical) infection in a completely susceptible population, can first be obtained. R_0 often serves as a threshold parameter that predicts whether an infection will spread in a WSN. To achieve this, we check the stability of the model based on worm-free and worm-endemic equilibrium states.

Basic Reproduction Number R_0

To generate R_0 from the mathematical equation model (2), we considered states consisting of the infectious parameter, including the following equations.

$$\frac{dI}{dt} = \beta S(t)I(t) - (\tau + \gamma + \theta)I(t)$$
$$\frac{dA}{dt} = \tau I(t) - (\theta + \alpha)A(t)$$

Next is to determine the infectious and transition parameters in matrix form. We denote F and V as matrices for the infectious and transition parameters, defined in equations (9) and (10), respectively.

$$F = \left[\beta SI\right] \quad (9)$$

$$v = \begin{bmatrix} (\tau+\gamma+\theta)I \\ -\tau I + (\theta+\alpha)A \end{bmatrix} \tag{10}$$

Taking derivatives of F and V for I and A, F and V can be respectively transformed in equations (11) and (12).

$$F = \begin{bmatrix} \beta S & 0 \\ 0 & 0 \end{bmatrix} \tag{11}$$

$$V = \begin{bmatrix} (\tau+\gamma+\theta) & 0 \\ -\tau & (\theta+\alpha) \end{bmatrix} \tag{12}$$

Obtaining V^{-1} as in equations (13) and (14)

$$V^{-1} = \frac{1}{(\theta+\alpha)(\tau+\gamma+\theta)} \begin{bmatrix} (\theta+\alpha) & 0 \\ \tau & (\tau+\gamma+\theta) \end{bmatrix} \tag{13}$$

$$V^{-1} = \begin{bmatrix} \frac{1}{(\tau+\gamma+\theta)} & 0 \\ \frac{\tau}{(\theta+\alpha)(\tau+\gamma+\theta)} & \frac{1}{(\theta+\gamma)} \end{bmatrix} \tag{14}$$

Multiplying F and V^{-1} obtained equation (15)

$$FV^{-1} = \begin{bmatrix} \frac{\beta S}{(\tau+\gamma+\theta)} & 0 \\ 0 & 0 \end{bmatrix} \tag{15}$$

Then the basic reproduction number R_0 is the largest eigenvalue of equation (15) which can be expressed in equation (16).

$$R_0 = \frac{\beta S}{(\tau+\gamma+\theta)} \tag{16}$$

Considering the worm free equilibrium state when I(0)=0, A(0)=0, and Q(0)=0, then S(0) = $\frac{\lambda}{\theta}$, then the basic reproductive number is given in equation (17).

$$R_0 = \frac{\beta\lambda}{\theta(\tau+\gamma+\theta)} \tag{17}$$

If the value of $R_0 < 1$, the worm propagation will be eliminated within the WSN. The proposed model will stabilise at worm-free equilibrium. Otherwise, if $R_0 > 1$, the worm will propagate consistently within the WSN and the proposed model will stabilize at worm-endemic equilibrium.

Worm-free equilibrium stability state

To determine the system stability at a worm-free equilibrium state, we will assume $I(t) = 0$; that no worm attack exists on the network, meaning the entire network nodes are susceptible. And all other states $A(0) = 0$; and $Q(0) = 0$ are taking to be zero. Then, the system can be expressed as in equation (18).

$$\begin{bmatrix} -(\beta I+\theta) & -\beta S & \alpha & \delta \\ \beta I & \beta S-(\tau+\gamma+\theta)I & 0 & 0 \\ 0 & \tau & -(\theta+\alpha) & 0 \\ 0 & \gamma & 0 & -(\delta+\theta) \end{bmatrix} \quad (18)$$

Substituting $\left(\bar{S}\ \bar{I}\ \bar{A}\ \bar{Q}\right)=\left(\frac{\lambda}{\theta},0,0,0\right)$ into (18), we will have the matrix solution of equation (19).

$$\begin{bmatrix} -\theta & -\beta\frac{\lambda}{\theta} & \alpha & \delta \\ 0 & \beta\frac{\lambda}{\theta} & 0 & 0 \\ 0 & \tau & -(\theta+\alpha) & 0 \\ 0 & \gamma & 0 & -(\delta+\theta) \end{bmatrix} \quad (19)$$

Next is to determine the jacobian matrix of equation (19), and expressed in equation (20).

$$\det(J(\frac{\lambda}{\theta},0,0.0)-\eta I)=\begin{bmatrix} -\theta-\eta & -\beta\frac{\lambda}{\theta} & \alpha & \delta \\ 0 & \frac{\beta\lambda}{\theta}-\eta & 0 & 0 \\ 0 & \tau & -(\theta+\alpha)-\eta & 0 \\ 0 & \gamma & 0 & -(\delta+\theta)-\eta \end{bmatrix} \quad (20)$$

From equation (20), we have $\eta_1=-\theta, \eta_2=-(\theta+\alpha), \eta_3=-(\delta+\theta)$ and $\eta_4=\frac{\beta\lambda}{\theta}$. Hence for the eigenvalue, η_1, η_2, η_3 are all negative values indicate that the worm free-equilibrium is locally asymptotically stable $S(0)=\frac{\lambda}{\theta}$. However, η_4, the system can only be stable for the eigenvalue if otherwise $S(0)=\frac{\lambda}{\theta}$ remain unstable.

Worm-endemic equilibrium stability state

To assess the stability of the model at worm-endemic equilibrium state, it is assumed that $I(t)=I$, meaning infected nodes exist in the network. In this case

$$\left(\bar{S}\ \bar{I}\ \bar{A}\ \bar{Q}\right)=\left(0,\bar{I},0,0\right)$$

next is to substitute the values into equation (18) and determine the Jacobian of the matrix, which can be expressed in equation (21).

$$\det(J(0,\bar{I},0,0)-\eta I)=\begin{bmatrix} -(\beta\bar{I}+\theta)-\eta & 0 & \alpha & \delta \\ \beta\bar{I} & -(\tau+\gamma+\theta)I-\eta & 0 & 0 \\ 0 & \tau & -(\theta+\alpha)-\eta & 0 \\ 0 & \gamma & 0 & -(\delta+\theta)-\eta \end{bmatrix} \quad (21)$$

Similarly, from the matrix of equation (21), all the eigenvalues have negative values. It follows that the worm-endemic equilibrium is locally asymptotically stable for all the values I.

Numerical Simulation

To assess the proposed SIAQ model, a numerical simulation is used to analyse the dynamic changes in worm propagation by varying model parameter values. The simulation was first to ascertain the worm-endemic equilibrium state and then evaluate the proposed model in mitigating worm propagation at a worm-free equilibrium state.

Simulation at worm-endemic equilibrium State

To simulate the dynamic worm propagation at worm-endemic equilibrium state, we chose a parameter values in such a way that R_0 >1. Therefore, our parameter values are set λ =7, β =0.106, δ =0.075, α =0.06, τ =0.1 γ =1- τ and θ =0.295, contact rate=0.07/hr with malware packet size=50mb, average sensor nodes remaining memory rm = 20mb and corresponding initial memory size= 100mb. Then the value of our R_0=1.8324>1. With the initial condition given as (S(0)=2.5, I(0)=3.75, A(0)=0.025, Q(t)=4.0)(Khanh, 2016).

Simulation at worm-free equilibrium State

In this section, the simulation evaluates the proposed SIAQ model and compares the performance with the SIQR model (Khanh,2016) in mitigating worm propagation. As such, we set our parameters λ =3, β =0.106, δ =0.075, α =0.06, τ =0.1, γ =1- τ and θ =0.301 with malware packet size=50MB, average remaining memory size rm=20MB and corresponding initial memory space of the sensor nodes ri=100MB. Then the value of our R_0=0.8133<1 at a contact rate =0.0578/hr , close to that of SIQR model R_0=0.8138<1 (Khanh, 2016) with the initial condition (S(0)=1.5, I(0)=2.75, A(0)=1.15, Q(t)= 0.01).

Results

Based on the simulations conducted, the results of the simulations will be categorized into worm-endemic equilibrium and worm-free equilibrium states.

Result at worm-endemic equilibrium state

The result of the simulation conducted at the worm-endemic equilibrium state is shown in Figure 3.

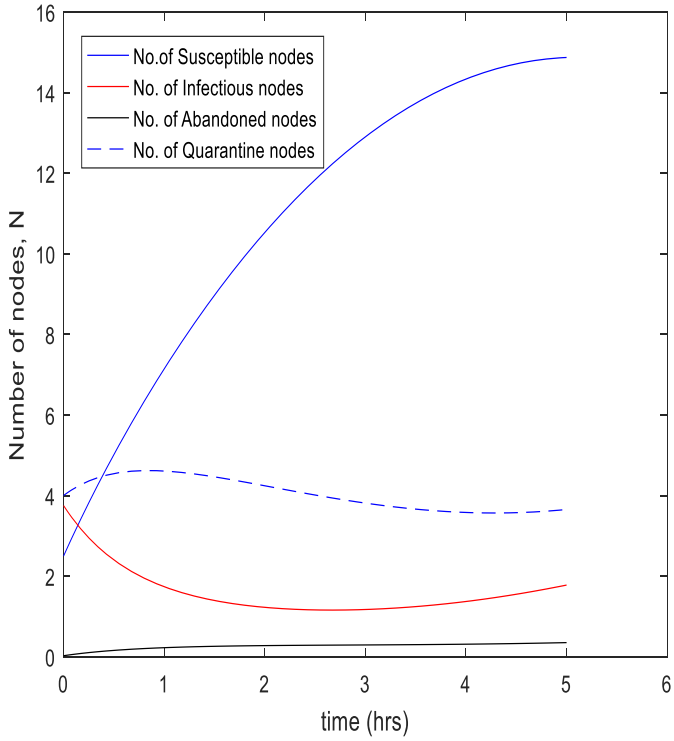

Figure 3. SIAQ model: Dynamic propagation at worm-endemic equilibrium state.

The result shows that the SIAQ model has suppressed the number of infectious nodes I(t) (red line) from the initial 3.75 nodes to 1.5 nodes. This is due to isolating some of the infectious nodes to quarantine class Q(t)(dotted blue line). Also, while suppressing the propagation over time, the number of susceptible nodes increases S(t) (blue line). This is due to the increase in nodes interaction while abandoning a few noninfectious nodes A(t) (black line) due to the attack's inability to transmit. However, as can be seen, the number of infectious nodes raises again for the remaining hours. The result justified our analytical findings with the basic reproduction number R_0=1.8324>1, the worm will spread persistently in a WSN.

Result at worm-free equilibrium state

The simulation results show that the worm infectious dies out from the WSN for both the proposed SIAQ and SIQR models (Khanh,2016), as indicated in Figures 4 and 5, respectively. As can be observed, the infectious nodes I(t) (red line) approaches zero as $t \to \infty$. This shows that the worm attack will not persist in WSN, which justifies our analytical finding that the worm attack will be eliminated with the basic reproduction number R_0<1. Therefore, both the proposed SIAQ model and SIQR model satisfied the condition for stability.

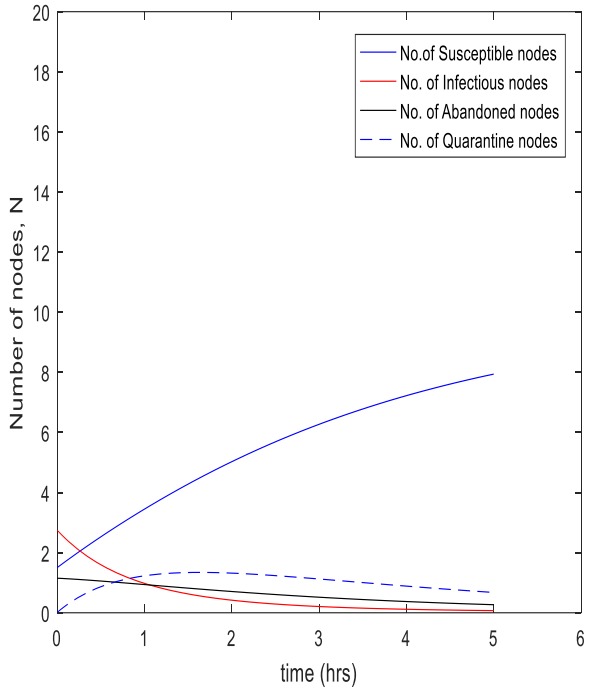

Figure 4. Proposed SIAQ Model: Dynamic propagation at worm-free equilibrium state

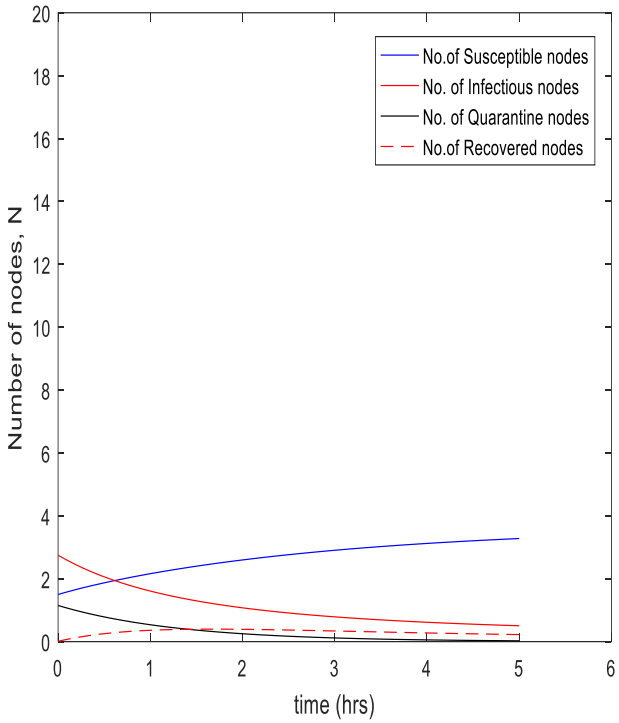

Figure 5. SIQR Model: Dynamic propagation at worm-free equilibrium state

For evaluation purposes, we perform the simulation on many susceptible nodes S(t) in WSN. For an increasing number of susceptible nodes from 1.5 to 20 nodes, other parameters remain constant. That is with initial condition (S(0)=20, I(0)=2.75, A(0)=1.15, Q(t) = 0.01) at contact rate =0.77/hr, the proposed SIAQ model outperforms previous SIQR model in mitigating worm propagation as shown in Figure 6.

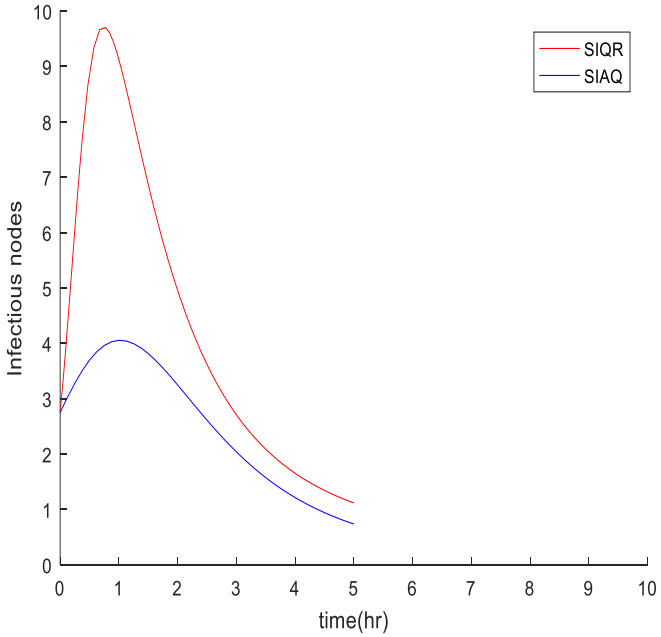

Figure 6. Evaluation of the proposed SIAQ model with SIQR

The result shows that the proposed SIAQ model (blue line) suppressed the worm secondary infectious nodes to limit at 4.0 nodes at peak. Contrary to the previous SIQR model (red line) that suppressed the worm secondary infectious nodes to 10 nodes at peak. In this regard, the proposed SIAQ model limit the infectious nodes to 4 nodes while SIQR model limit the infectious nodes to 10 nodes. Hence, the performance of the proposed SIAQ model against SIQR is calculated below.

percentage = ((10-6)/10)*100= 40%

However, in both the proposed SIAQ and SIQR models, the infectious nodes are eliminated from the network after reaching the peak values.

Discussion

Previous work emphasized WSN characteristics to model the dynamic propagation of worm attacks. This work considers WSN characteristics and the constraint nature of the sensor device itself. With the constraint nature of the energy and memory capability of the sensor nodes, it is paramount to consider both the energy and memory efficiency of the sensor nodes in dealing with worm attacks. Consequently, with the proposed SIAQ model that focuses on the isolation of infectious memory-efficient nodes, it was demonstrated that the model could dynamically model the propagation of worm attacks at both the worm-endemic and worm-free equilibrium state. Also, from our findings, the proposed SIAQ model outperforms the SIQR model in mitigating worm propagation at large-scale WSN deployment.

Conclusion

Worm and its propagation within WSN remain a challenging issue in a security domain. Previous approaches engaged various parameters to dynamically model the process and mitigate the propagation of worms in WSN. However, the constrained nature of sensor nodes has not given due to consideration in mitigating the menace. Consequently, in this work, a novel SIAQ model was proposed to isolate infectious memory-efficient nodes to mitigate worm propagation. The SIAQ model has effectively decreased the infectious peak value while mitigating worm propagation. At a worm-free equilibrium state, the proposed SIAQ model outperforms the previous SIQR model to suppress the number of secondary worm infections in a large-scale WSN deployment. Consequently, the proposed model can serve as a basis for assisting the planning, design, and defence of such networks from the investigator's point of view. To effectively enhance the efficiency of the proposed model, it should further incorporate energy and other sensor parameters as a basis for isolating the infectious nodes.

References

Acarali D., Rajarajan, M., Komninos N., and Zarpelão, B. B. (2019) Modelling the Spread of Botnet Malware in IoT-Based Wireless sensor networks. *Security and Communication Networks*, 2019: 1-13.

Akyildiz, I., Su, F.W., Y. Sankarasubramaniam and E, Cayirci (2002). Wireless sensor networks: A survey. *Computer Networks*, 38(4): 393-422.

Feng L, Song L., Zhao, Q. and Wang, H (2015) Modelling and stability analysis of worm propagation in the wireless sensor network. *Mathematical Problems in Engineering*, 2015: 1-8.

Gardner M.T., Beard, C. and Medhi D. (2017). Using SEIRS epidemic models for IoT botnets attacks, Proceeding of 13th International Conference on Design of Reliable Communication Networks, Munich, Germany, March 08-10, pp.62-69.

Giannetsos, T., Dimitriou, T., and Prasad, N. R (2009). Self-propagating worms in wireless sensor networks, International student workshop on Emerging networking experiments and technologies, Rome, Italy, 1st December, pp31-32.

Hejazi,P. and Ferrari G. (2018). Energy and Memory Efficient Data Loss Prevention in Wireless Sensor Network. *Prepreints doi:10.20944/preprints201807.0206.v1*,pp.1-18.

Jerkins,J. A., and Stupiansky, J.(2018). Mitigating IoT insecurity with inoculation epidemics, *ACMSE Southeast Conference*, Richmond, KY, USA, 29-31 March, 2018, pp-1-6.

Ji,Y., Yao, L., Liu, S., Yao, H., Ye, Q. and Wang, R.(2018). The Study on the Botnet and its Prevention Policies in the Internet of Things. International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanjing, China, May, 2018, pp 837-842.

Kechen, Z., Hong, Z., and Kun, Z. (2012). Simulation-based analysis of worm propagation in wireless sensor networks, Fourth International Conference on Multimedia Information Networking and Security, Nanjing, China, 2-4 November.

Keshri, N., and Mishra, B. K. (2014). Two time-delay dynamic models on the transmission of malicious signals in wireless sensor networks, *Chaos, Solitons & Fractals*, 68: 151-158

Khanh N.H. (2016). Dynamics of a Worm Propagation Model with Quarantine in Wireless Sensor Networks. *Appl. Math* 10(5): 1739-1746.

Ibrahim M.(2021). Epidemic Based Modelling For the Mitigation of IoT Botnet Propagation at Equilibrium Point. *Kasu journal of Mathematical sciences.* 2(2):74-83

Mishra, B. K. and Keshri, N. (2013). Mathematical model on the transmission of worms in the wireless sensor network. *Applied Mathematical Modelling*, 37(6): 4103-4111.

Singh A., Awasthi, A. K., Singh, K. and Srivastava, P. K. (2018). Modelling and analysis of worm propagation in wireless sensor networks. *Wireless Personal Communications*, 98(3): 2535-2551.

Wang, T., Wu, Q., Wen, S., Cai, Y., Tian, H., Chen, Y., and Wang, B.(2017). Propagation modelling and defending of a mobile sensor worm in wireless sensor and actuator networks. *Sensors*, 2017(17): 1-17.

Wang, X., Li Q., and Li, Y. (2010). EiSIRS: a formal model to analyse the dynamics of worm propagation in wireless sensor networks. *Journal of Combinatorial Optimization*, 20(1): 47-62.

Yin, M., Chen, X., Wang Q., Wang W., and Wang, Y. (2019). Dynamics on Hybrid Complex Network: Botnet Modeling and Analysis of Medical IoT. *Security and Communication Networks*, 2019: 1-4