



A Review Article on Wireless Sensor Networks in View of E-epidemic Models

M. N. Srinivas¹ · V. Madhusudanan² · A. V. S. N. Murty¹ · B. R. Tapas Babu³

Accepted: 22 March 2021 / Published online: 5 April 2021

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract

Epidemic simulations have recently been used to model the dynamics of malicious codes in the network of wireless sensors. This is because of its open existence, which offers a simple target for malware attacks aimed at disrupting network operations or, worse, causing complete network failure. The Susceptible-Exposed-Infectious-Quarantined-Recovered–Susceptible with Vaccination compartments models like SIR-M, SEIRV, SEIQRV, SEIRS, SITR, SIR with delay are studied by various authors and some of such models that characterize worm dynamics in WSN. After a concise presentation of the wireless sensor network, some primary research consequences of e-pandemic models (of various researchers) are given and assessed. At that point the uses of wireless sensor network in the clinical wellbeing, agribusiness, and military, space and marine investigation are laid out. What's more, we break down the upside of wireless sensor network in these sectors. In this review article, we sum up the fundamental factors that influence the uses of wireless sensor networks in view of e-epidemic models and revived some epidemic models and also discussed some conceivable future works of different epidemic wireless sensor models.

Keywords Wireless sensor networks · Nodes · Susceptible · Infected · Recovered epidemic

✉ M. N. Srinivas
mnsrinivaselr@gmail.com

V. Madhusudanan
mvmsmaths@gmail.com

A. V. S. N. Murty
avsnmurthy2005@gmail.com

B. R. Tapas Babu
tapasbabu@saec.ac.in

¹ Department of Mathematics, School of Advanced Sciences, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India

² Department of Mathematics, S.A. Engineering College, Chennai, Tamil Nadu 600077, India

³ Department of Electronics and Communication Engineering, S. A. Engineering College, Chennai, Tamilnadu, India

1 Introduction

Wireless sensor network is countless static or portable sensors hubs which structure the remote system utilizing self-association and multi-bounce strategy, its motivation is to team up identification, handling and transmitting the item observing data in zones where the system inclusion. The sensor hub, sink hub, the client hub establish the three components of sensor systems. Sensor hub is the establishment of the entire system, they are liable for the view of information, handling information, store information and transmit information. The sensor notes are shared coordinated effort, note isn't straightforwardly transfer the first information, yet to utilize their own preparing limit with regards to legitimate activity and reconciliation, just forward the information that the lower-level note needs. The sensor hub can detect a lot of natural data, including temperature and dampness, pressure, light condition, vehicle development, mechanical weight quality, the speed of the wind stream course and different attributes. It is these attributes, sensor arrange in numerous viewpoints, for example, clinical wellbeing, condition and horticulture, clever home outfitting and building, military, space and marine investigation have been generally applied and show an important application prospect.

The fundamental highlights of remote sensor systems are self-association, multi-bounce course, dynamic system topology, hub assets restricted, information driven and security issue. The hubs of the remote sensor organize have the programmed organizing capacity and the hubs can speak with one another. In the utilization of remote sensor arrange, regularly the sensor hubs are put some place with no base system office. For example, a tremendous region of virgin woodland, or the threat region where individuals cannot come to, this requires the sensor hub has the self-association capacity to arrange and oversee consequently. At the point when a hub can't straightforwardly speak with the passage, it requires different hubs to transmit information, so the system information transmission is a multi-jump directing. In some unique applications, remote sensor organize is portable, sensor hubs may stop work on account of the vitality expended or other disappointment, these components will make the system topology changes. There are an enormous number of sensor hubs in wireless sensor network and regularly need to master minded in a particular observing zone. The equipment assets of sensor hub are restricted as a result of the size and cost requirements. So its registering power, stockpiling limit is generally feeble. Portable correspondence system or Ad hoc arrange for the most part thinks about how to improve the system transmission limit under current conditions, that is to give clients a data transfer capacity adequate, protected and solid transmission channel. Be that as it may, wireless sensor network is utilized to screen the different estimated information. In the system configuration process, we chiefly consider how to manage discernment information productively and transmit the got information to the client hub. Along these lines, one attribute of the remote sensor organize is information driven. As wireless sensor network system utilizes remote transmission, so the observing information is anything but difficult to be captured, or even befuddle clients in the wake of altering. After an enormous number of sensor hubs are caught, the foe may utilize them to decimate the current system. Thusly, in the structure of remote sensor systems, security issue is the focal point of the examination. The key advances of remote sensor systems are organize convention, time-synchronization, limitation, information conglomeration, power the board and security organization. In the remote sensor organize convention study, medium access control convention and directing convention is the key point. Wireless sensor network hubs are by and large battery-fueled; an organization of lifetime use, the battery charging and substitution is troublesome. In this

way, in the structure of wireless sensor network, we should work for the proficient utilization of vitality hub in the consummation of the prerequisites under the reason, beyond what many would consider possible to broaden the life of the whole system. In wireless sensor network, security organization is for the most part reflected in data security. Correspondence security for the most part thinks about the security hub, detached guard interruption assault and dynamic against intrusion. Furthermore, the data security for the most part thinks about the classification, honesty and viability of information.

With the progression of data innovation, there has been ascend in intolerable acts concerning remote systems. Such acts are security danger to an individual or a country. A remote correspondence organize that guarantees security, dependability, proficiency would be an incredible advantage for the cutting edge age individuals. Sensor hub in a remote system is a smart, ease and little gadget. Remote Sensor Networks are utilized for occasional information assortment to crucial sending. A few significant utilizations of WSNs are military objective following, object observing agribusiness, calamity the executives, risky condition investigation, ecological and contamination application, flood location, vehicles following, traffic checking, gas checking, water quality checking and seismic detecting, social insurance applications [1–3], and so forth. Nonetheless, sensor hubs are minimal effort gadget that works cleverly. Also, they are asset limitation [4, 5]. In this way, because of constrained assets and decentralized design, remote correspondence alongside security provisioning between such systems is amazingly lumbering. Security dangers in remote system are more in contrast with conventional systems since they are more defenceless [6]. Sensor hubs have low range correspondence limit and convey the gathered information in multi-jump way [7]. An assailant focuses on a solitary hub of the system to dispatch the assault and this tainted hub spreads the worm in the whole system through neighbouring hubs [8]. Without a doubt, controlling worm engendering is urgent to guarantee sustenance of the system. Along these lines, investigation of vindictive signs transmission and scientific demonstrating turns into a fundamental instrument [9–20]. The exhibition of remote sensor networks is dissected by fluctuating different parameters, for example, hub thickness, standard deviation, correspondence go, and so on. By guaranteeing effective transmission of information in the system, the unwavering quality of remote sensor networks [21] within the sight of malware spread under scourge hypothesis has been considered. The inspiration driving proposed model is to distinguish uncover hubs at the soonest and to control malware transmission. To achieve this, another uncovered state (Q, R, V) is presented that helps in distinguishing the counterbalance of the malware from the get-go in the remote sensor networks. The hubs influencing the exhibition of system are considered as uncovered hubs. In such a circumstance, it goes basic to rapidly utilize restorative measures to destroy the worm sources from the system or send them to rest mode.

In the recent years new categories of worms are being developed and spread by attackers which are capable of attacking variety of mobile computing devices or nodes such as smart phones, laptops. These categories of malwares are capable of directly spreading between the communicating devices through various wireless communication technologies such as Bluetooth, Wi-Fi etc. Since the propagation of worms among devices can be compared with the transmission of epidemic diseases such as Ebola and Corona virus among human beings, the eco-epidemic models studied by the researchers can be incorporated to study and analyse the propagation dynamics of worms in wireless networks.

Many researchers have published their work related to the epidemic model applications in the recent years. Inspiring on the aforementioned literature, we have formulated the SITR e-epidemic model and analysed the behaviour of worms spreading in the wireless networks along with the major factors for this sort of propagation of worms which leads to

draining the batter power of the nodes thereby leading to the reduced lifetime of the network. To accomplish the goal many techniques have been applied to the network such as clustering the nodes that is used for aggregating the data through which the consumption of energy can be minimized drastically.

To examine the propagation of malwares and to control the infectious diseases, formulating the mathematical models according their behaviour play a major role. In recent literature many researchers have formulated epidemic models such as SI, SIS, SIR, SIER, SIERS etc. Each model has its own style of strategies for controlling the spread of diseases. Initially SIR (susceptible-infected-recovered) model has been developed by the authors in 1927 to study the explosion of plague. Later the dynamic behaviour of such model was investigated by many researchers. The vaccine induced SIRS model was developed by the authors with inborn immunity. They analysed that the system underwent a reverse bifurcation when the threshold is attained. The SIER model has an additional component named Exposed apart from the susceptible, infected, recovered components which represents that the infected people without symptoms may not spread the disease during the dormant period. These models are capable of representing infectious diseases like dengue. The SIERS sort of model was developed by the authors with an additional component S to study and analyse the global properties of the epidemic models. Later on variants of the model was proposed by many researchers to represent infectious water body related diseases like bacterial infections.

2 Epidemic Models

In 2009, Shensheng Tang et.al [8] study the potential danger for infection spread in remote sensor systems (WSNs). Utilizing pestilence hypothesis, the authors [8] proposed the following mathematical model, called Susceptible-Infective-Recovered with Maintenance (SIR-M), to describe the elements of the infection spread procedure from a solitary hub to the whole system (Fig. 1).

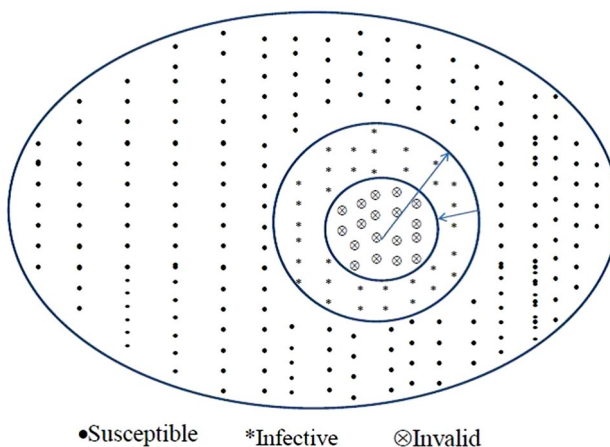


Fig. 1 Represents schematic diagram of the system proposed by [8]

The mathematical model for the proposed system is formulated as follows

$$S'(t) = -\beta I \frac{\sigma \pi r_0^2}{N} S + \lambda_a S - \lambda_m S \quad (2.1)$$

$$I'(t) = \beta I \frac{\sigma \pi r_0^2}{N} S - (1-p)I - \lambda_a I - \gamma I \quad (2.2)$$

$$R'(t) = \gamma I + p\lambda_m I + \lambda_a R - \lambda_m R \quad (2.3)$$

where $S(t)$, $I(t)$ and $R(t)$ mean the quantity of susceptible, infective and recuperated(recovered) hubs at time t , separately. Since the hubs are consistently haphazardly disseminated with thickness σ , each contaminated hub can contact on the request for neighbour hubs. Be that as it may, reaching a neighbour doesn't really prompt another infective hub. Review that there are three gatherings of hubs. Just a vulnerable neighbour of the contaminated hub can turn into another infective hub. Reaching a tainted neighbour or a recuperated neighbour doesn't change the condition of the framework, since such a hub is either effectively contaminated or is safe to disease. Because of the presumption of consistently appropriated hub arrangement, the part of the tainted hub's neighbours that can get contaminated at time t can be approximated as $S(t)/N$. Let β indicate the disease limit, which speaks to the probabilistic pace of getting contaminated in a contact between an infective and a helpless hub. Unmistakably β relies upon the infectivity of an infection and the correspondence pace of a convention since the infection spreads itself by piggybacking on typical information through ordinary interchanges. Let γ indicates the recuperation limit, which is the probabilistic rate at which an infective hub recoups and becomes insusceptible when the infective hub is in the dynamic mode. Let λ_a and λ_m represent the rates at which a hub changes from the dynamic mode to the upkeep (rest) mode, and advances from support to dynamic mode, separately. In the support mode, the framework upkeep program is consequently activated. The vulnerable and recuperation hubs will rapidly pass the check and rest, while the infective hubs will set aside a more extended effort for treatment. Contingent upon the predefined timeframe of support (or rest), a small amount of the kept up infective hubs, meant by p , will be restored and become recuperation hubs after continuing the dynamic mode. The rest of the hubs will stay in the gathering of infective hubs. We allude to this changed SIR model as the SIR-M model, where, M represents maintenance. By presenting a support system in the rest method of WSNs, the SIR-M model can improve the system's enemy of infection ability and empower the system to adjust deftly to various kinds of infections, without bringing about extra computational or flagging overhead. The proposed model can catch both the spatial and transient elements of the infection spread procedure. We infer unequivocal investigative answers for the model and talk about some common sense uses of premium. Broad numerical outcomes are introduced to approve our examination. The proposed model (2.1, 2.2, 2.3) is relevant to the plan and investigation of data engendering instruments in correspondence systems.

Wireless sensor networks (WSNs) have gotten broad consideration because of their extraordinary potential in common and military applications. The sensor hubs have constrained force and radio correspondence capacities. As sensor hubs are asset obliged, they for the most part have frail guard abilities and are alluring focuses for programming assaults. Digital assault by worm presents one of the most risky dangers to the security and uprightness of the PC furthermore, WSN. In 2013, Bimal Kumar Mishra et.al. [11],

analysed the assaulting conduct of potential worms in WSN. Utilizing compartmental plague model, we propose helpless—uncovered—irresistible—recuperated—defenceless with an immunization compartment (SEIRS-V) to depict the elements of worm engendering as for time in WSN. The proposed model of [11] catches both the spatial and fleeting elements of worms spread procedure (Fig. 2).

The mathematical model for the proposed system is formulated as follows

$$S'(t) = A - \beta SI - \mu S - pS + \delta R + \eta V \tag{2.4}$$

$$E'(t) = \beta SI - (\mu + \alpha)E \tag{2.5}$$

$$I'(t) = \alpha E - (\mu + \varepsilon + \gamma)I \tag{2.6}$$

$$R'(t) = \gamma I - (\mu + \delta)R \tag{2.7}$$

$$V'(t) = pS - (\mu + \eta)V \tag{2.8}$$

where $S(t)$, $E(t)$, $I(t)$, $R(t)$ and $V(t)$ denote the number of susceptible, exposed, infectious, recovered, vaccinated nodes at time t respectively. where, $1/\delta$ and $1/\eta$ are the periods of immunity of the recovered & vaccinated susceptible nodes respectively, and A is the inclusion of new sensor nodes to the population, μ is the crashing rate of the sensor nodes due to hardware/software problem, ε is the crashing rate due to attack of worms, β is the infectivity contact rate, α is the rate of transmission from E -class to I -class, γ is the rate of recovery, δ is the rate of transfer from R -class to S -class, η is the rate of transmission from V -class to S -class, p is the vaccinating rate coefficient for the susceptible nodes. Generation number, equilibriums, and their solidness are additionally found. On the off chance that generation number is short of what one, the contaminated portion of the sensor hubs vanishes and if the propagation number is more prominent than one, the tainted division endures and the doable locale is asymptotically steady area for the endemic balance state. Numerical strategies are utilized to settle and recreate the frameworks of conditions created and furthermore to approve our model. A basic investigation of inoculation class

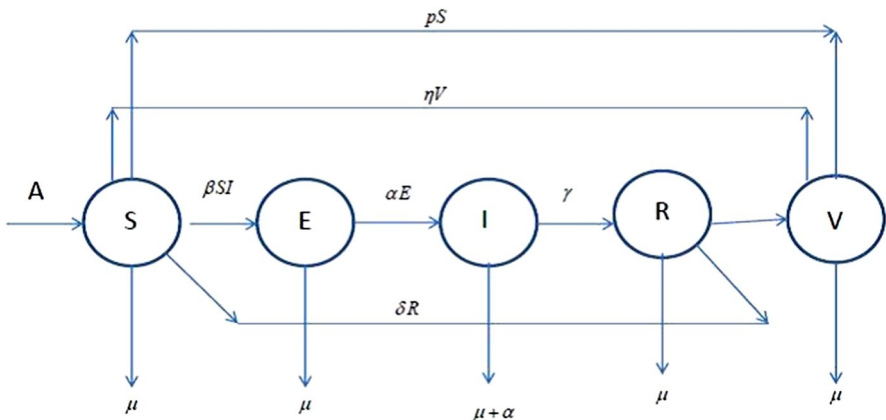


Fig. 2 Represents schematic diagram of the model proposed by [11]

concerning defenceless class and irresistible class has been had for a beneficial outcome of expanding safety efforts on worm proliferation in WSN.

Endemic models have been utilized as of late to display the elements of noxious codes in wireless sensor network (WSN). This is because of its open nature which gives an obvious objective to malware assaults planned for upsetting the exercises of the system or at more awful, causing absolute disappointment of the system. The SEIQR-V model by Mishra and Tyagi [22] is one of such models that portray worm elements in WSN. In any case, a basic examination of this model and WSN plague writing shows that it is missing fundamental factors, for example, correspondence range and appropriation thickness. In this way, the authors (2017) Nwokoye, C. H., et al. [16] adjust the SEIQR-V model to incorporate these elements and to produce better proliferation proportions for the presentation of an irresistible sensor into a defenceless sensor populace as follows in the form of flow chart (Fig. 3).

The mathematical model for the proposed system is formulated as follows.

$$S'(t) = \lambda - \zeta SI - \tau S - \rho S + \phi R + \xi V \tag{2.9}$$

$$E'(t) = \zeta SI - (\tau + \theta)E \tag{2.10}$$

$$I'(t) = \theta E - (\tau + \omega + \nu + \alpha)I \tag{2.11}$$

$$Q'(t) = \alpha I - (\tau + \omega + \eta)Q \tag{2.12}$$

$$R'(t) = \eta Q + \nu I - (\tau + \phi)R \tag{2.13}$$

$$V'(t) = \rho S - (\tau + \epsilon)V \tag{2.14}$$

Here μ denotes the energy of nodes exhaust, probability to convert into dead node, d_1 represents mortality rate of nodes due to the failure of software, ρ denotes that the rate of vaccination for susceptible sensor nodes, ϕ represents the rate at which recovered nodes become susceptible to infection, ϵ represents the rate of transmission from the vaccinated compartment to the susceptible one, ζ denotes that the effective contact with an infected node for transfer

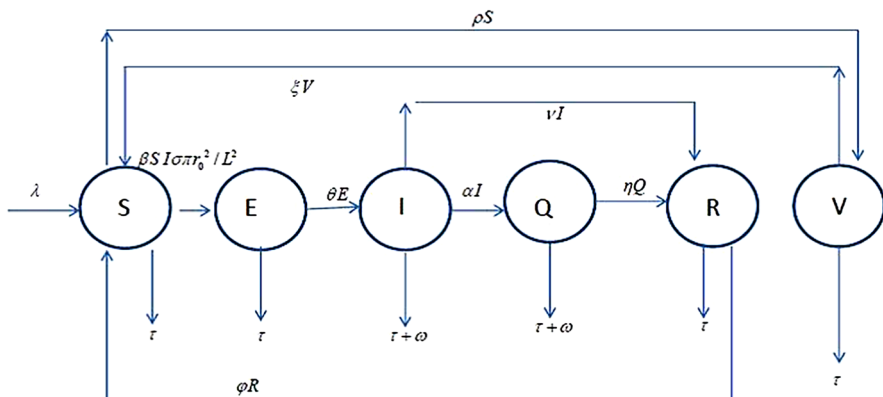


Fig. 3 Represents the schematic diagram of the system proposed by [16]

of infection, θ represents the rate at which exposed nodes become infectious, d_2 represents the crashing rate due to attack of malicious worms, η_1 represents the rate of recovery, α represents the rate of transmission from the infectious compartment to the quarantined one, η_2 represents the rate of transmission from the quarantined to the recovered compartment and $N = S + E + I + Q + R + V$. Let $L \times L$ is the area in which nodes are distributed. Here we take $\zeta = \frac{\beta \pi \sigma r_0^2}{L^2}$ where β denotes infectious contact rate. The representative arrangements of the harmonies were inferred for two topological articulations separated from WSN writing. A reasonable numerical strategy was utilized to unravel, recreate and approve the altered model. Recreation results show the impact of their alterations.

Wireless sensor networks (WSNs) experience basic test of Network Security due to outrageous operational requirements. The beginning of challenge starts with the passage of worms in the remote system. Only one tainted hub is sufficient to spread the worms over the whole system. The tainted hub quickly contaminates the neighbouring hubs in an unstoppable way. In this paper, a numerical model is proposed dependent on scourge hypothesis. It is an improvement of SIRS and SEIS models. In 2019, Ozha R.P, et al. [18], proposed SEIRS model that beats the downsides of existing models as follows (Fig. 4).

The mathematical model for the proposed system is formulated as follows.

$$S'(t) = \mu N - \zeta SI + \varepsilon R - (\mu + \omega)S \tag{2.15}$$

$$E'(t) = \zeta SI - (\mu + \alpha)E \tag{2.16}$$

$$I'(t) = \alpha E - (\mu + \gamma)I \tag{2.17}$$

$$R'(t) = \gamma I + \omega S - (\mu + \varepsilon)R \tag{2.18}$$

where $S(t), E(t), I(t), R(t)$ denote the number of susceptible, exposed, infectious, recovered, nodes at time t respectively. μ represents the probability to convert into dead node as

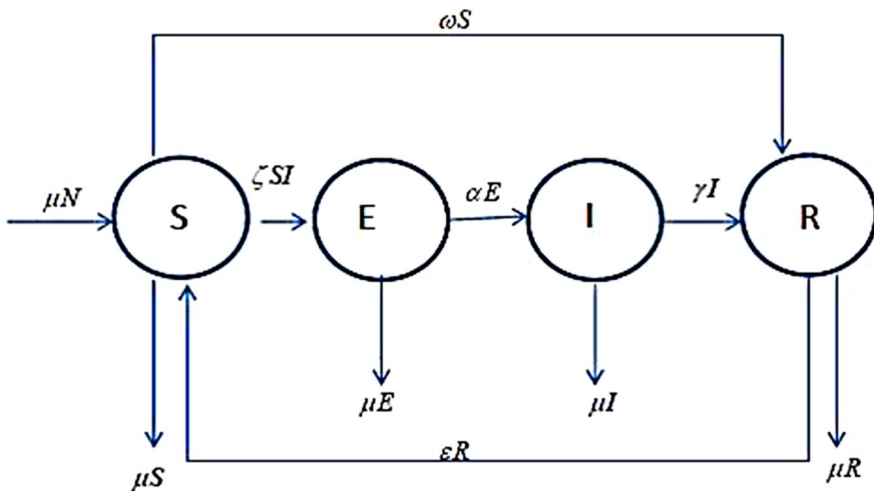


Fig. 4 Represents schematic diagram of the system proposed by [18]

the energy of nodes exhaust, $\zeta = (\pi r^2 \beta) / L^2$ represents the total number of neighbouring nodes that are lying in the sensing area of a sensor node and where β denotes infectious contact rate, the transmission area of a sensor node is πr^2 with sensing range r , L^2 represents the area in which the nodes are uniformly scattered, ε represents the probability that recovered node may become susceptible again, ω represents the rate at which recovery is provided to the susceptible node, α represents rate at which exposed node falls in the infectious class, γ represents the rate of recovery is provided to the susceptible node. This proposed enhanced model incorporates a limited correspondence sweep and the related hub thickness. The authors got essential generation number which decides the local and worldwide global proliferation elements of worm in the WSNs. Similarly, the authors derived articulation for edge for hub thickness and correspondence range. They explored the control instrument against worm proliferation and also they contrast the proposed model and different existing models and assess its presentation based on different execution measurements. The investigation affirms correction in the imperative perspectives like security; organize dependability, transmission proficiency, vitality effectiveness for WSNs. The proposed SEIRS model gives an improved strategy to restriction worms' transmission in correlation with the current models.

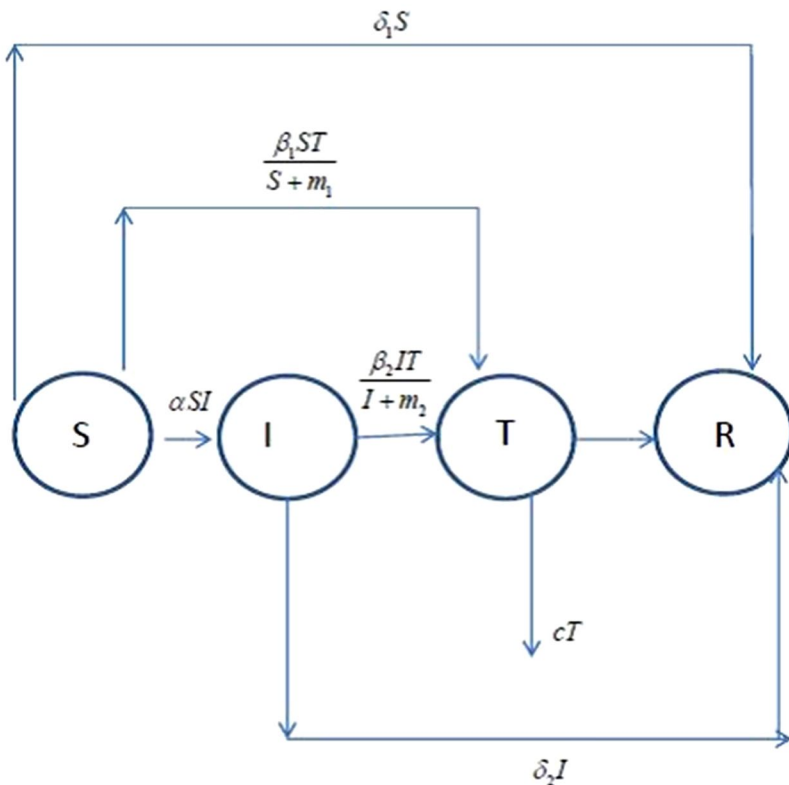


Fig. 5 Represents schematic diagram of the system proposed by [23]

An endeavour has been made to comprehend the transmission elements of malevolent signals in wireless sensor network. In 2019, Upadhyay, R. K et al. [23] proposed vitality proficient e-pestilence model with information parcel trans-mission delay as follows (Fig. 5).

The mathematical model for the proposed system is formulated as follows.

$$S'(t) = r_1 S \left(1 - \frac{S}{k}\right) - \alpha SI - \frac{\beta_1 ST}{S + m_1} - \delta_1 S \quad (2.19)$$

$$I'(t) = r_2 I \left(1 - \frac{I}{l}\right) + \alpha_1 SI - \frac{\beta_2 IT}{I + m_2} - \delta_2 I \quad (2.20)$$

$$T'(t) = \frac{\gamma_1 \beta_1 ST}{S + m_1} + \frac{\gamma_2 \beta_2 IT}{I + m_2} - cT \quad (2.21)$$

$$R'(t) = \delta_1 S + \delta_2 I \quad (2.22)$$

where $S(t)$, $I(t)$, $T(t)$ and $R(t)$ denote the number of susceptible, infectious, terminally infected and recovery nodes at time t respectively. r_1 and r_2 represents intrinsic growth rates of susceptible and infected nodes respectively, k and l represents carrying capacities of susceptible and infectious nodes respectively, α and α_1 represents transmission rates, β_1 represents inter-nodes interference coefficient of class T for susceptible node, β_2 represents inter-nodes interference coefficient of class T for infectious nodes, m_1 and m_2 represents handling time of susceptible and infected nodes respectively, δ_1 and δ_2 represents recovery rates for susceptible and infectious nodes respectively, c represents crashing rate of the terminally infected node. Steadiness investigation is performed for all the equilibrium focuses, whose trademark conditions include the time delay. Global stability and Hopf bifurcation examinations are completed for the endemic steady state purpose of the postpone framework. Consideration has been paid to the bearing of Hopf bifurcation and the security of the subsequent intermittent arrangements. Numerical investigation displays twofold Hopf bifurcation dynamics and it causes steadiness exchanging i.e., shakiness to strength and back to precariousness or the opposite progress of the arrangement of the thought about framework. At long last, numerical recreations give helpful perceptions to various postponements and they show an intriguing bifurcation situation. The effect of the control parameters β and τ on the framework elements has been examined. The outcomes of proposed delayed model that the information parcel delay and discrete deferral are responsible for the dependability exchanging and the event of confused elements separately. The nearness of disorganized elements demonstrates delicate security arrangement of the system. By looking into the re-enactment results, the authors found that the best control measures to control the proliferation of pernicious signs.

In 2018, authors Abhishek Kumar and Nilam [24], presented a mathematical study of a deterministic model for the transmission and control of epidemics. They proved that the incidence rate of susceptible being infected is very crucial in the spread of disease and also the delay in the incidence rate is fatal. The authors proposed an SIR mathematical model with the delay in the infected population by considering nonlinear incidence rate for epidemics along with Holling type II treatment rate for understanding the dynamics of the epidemics as follows (Fig. 6).

The mathematical model for the proposed system is formulated as follows.

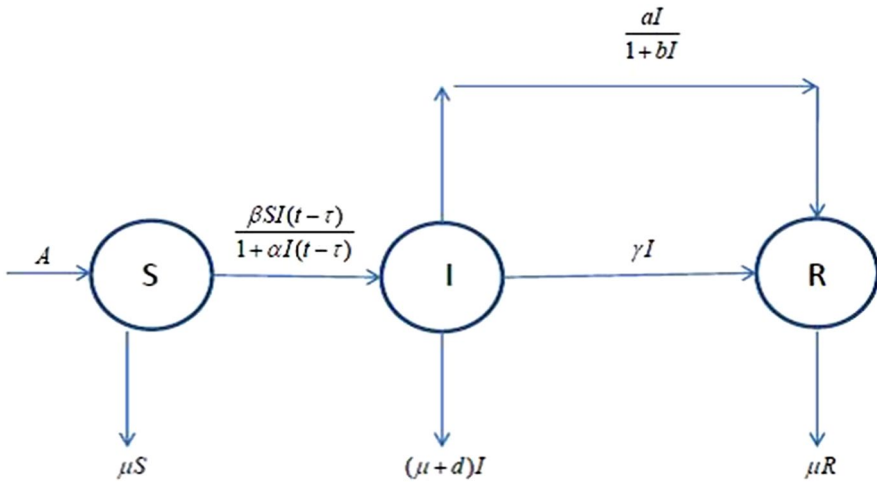


Fig. 6 Represents schematic diagram of the system proposed by [24]

$$S'(t) = A - \mu S - \frac{\beta SI(t - \tau)}{1 + \alpha I(t - \tau)} \tag{2.23}$$

$$I'(t) = \frac{\beta SI(t - \tau)}{1 + \alpha I(t - \tau)} - (\mu + d + \gamma)I - \frac{aI}{1 + bI} \tag{2.24}$$

$$R'(t) = \frac{aI}{1 + bI} + \gamma I - \mu R \tag{2.25}$$

The authors analyzed the stability by considering the basic reproduction number R_0 in terms of locally asymptotically stable for disease-free equilibrium when the basic reproduction number R_0 is less than one and investigated the stability of the model for disease-free equilibrium at R_0 equals to one using center manifold theory. They also examined the stability for endemic equilibrium point and assumed that the total population N is divided into three compartments: susceptible individuals compartment $S(t)$, infected individuals compartment $I(t)$ and recovered individuals compartment $R(t)$. Susceptible individuals are those who can get a disease under appropriate conditions. Infected individuals are the one who has got a disease and can spread the disease to susceptible individuals via contacts. As time passes, infected individuals lose infectivity and move to recover compartment by auto recovery due to autoimmune response of the body or by treatment. Also, Holling type II treatment rate is considered for the recovery of the infected population. Where A represents recruitment rate per day, α represents measure of inhibition, β represents effective contact rate, μ represents natural mortality rate, d represents disease induced mortality rate and γ represents recovery rate, a is positive constant and b is a constant taking into account as resource limitation $\tau > 0$ is a fixed time during which the infectious agents develop in the vector and it is only after that time that the infected vector can infect a susceptible individual. Additionally, mathematical simulations are offered to epitomize the investigative studies.

The weakness that exists in the computer network by the disease of infection when the assets are uncovered requires the investigation of the idea of proliferation of infection into the network. In 2020, the authors V. Madhusudanan and R. Geetha [25] have assumed a novel pandemic Susceptible-Infected-Recovered model by assuming that each node is denoted as one computer and the state of it can be healthy computer but are susceptible (S) to infection by the computers that already infected some computers (I) which can transmit the disease to the healthy ones or the recovered (R) one which cannot get disease or transmit and that manages the contaminated hubs in the organization regarding the turn of events of insusceptibility accomplished after recuperation as follows (Fig. 7).

The mathematical model for the proposed system is formulated as follows.

$$S'(t) = (1 - p)b - \frac{\beta S(t - \tau)I(t - \tau)}{1 + \sigma S(t - \tau)} - dS + \delta R \tag{2.26}$$

$$I'(t) = \frac{\beta S(t - \tau)I(t - \tau)}{1 + \sigma S(t - \tau)} - (d + \alpha + \gamma)I \tag{2.27}$$

$$R'(t) = \gamma I + pb - (d + \delta)R \tag{2.28}$$

The authors have been checked positivity and bounded ness of the proposed model (2.26, 2.27, 2.28). Neighbourhood security investigation of the proposed model is examined by Routh–Hurwitz criteria without delay. The time arrangement examination with respect to nature of the defenceless, contaminated and recuperated hubs in the organization has been performed utilizing genuine control parameter oriented boundaries. The authors additionally dissected that time deferral may play critical part on the strength of the proposed model since at whatever point delay surpasses the basic esteem the framework loses its steadiness and a Hopf bifurcation happens. The mathematical reproduction results legitimize that the proposed model is approved against the scientific investigations of infection proliferation and subsequently inspecting the hypothetical outcomes. Where b is new number of the computers, p is the immune rate of the computers, β is the infection rate of the infected computers, d is the death rate of computers, δ is loss rate of immunity of the recovered computers, d is death rate due to virus, α is the recovered rate of the infected computers, γ is the saturation factor that measures the inhibitory effect. Finally authors observed that the time delay may play significant role on the stability of the proposed model, since

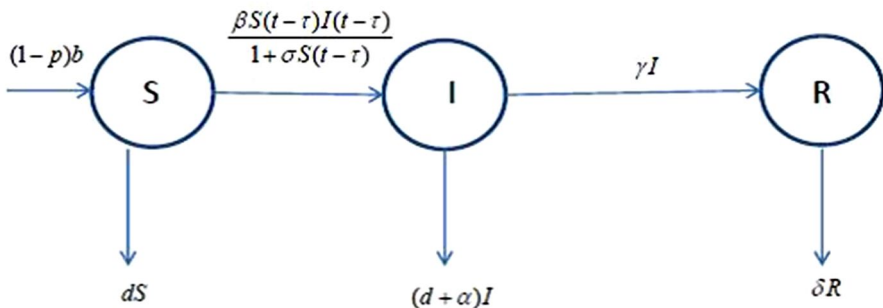


Fig. 7 Represents schematic diagram of the system proposed by [26]

Table 1 Researches on stability of epidemic model in Wireless sensor networks (WSNs)

Authors	Model	Characteristics	Study
Tang, S., and Mark, B. L. [8]	SIR-M	Considering maintenance mechanism	Potential threat of virus spread in WSN
Mishra,B.K., and Keshri, N. [11]	SEIRV	SEIRS with vaccination compartment	Attacking behaviour of possible worms and the dynamics of worm propagation w.r.to time in WSN
Nwokoye, C. H., and Umeh, I. I. [17]	SEIQRV	SEIQRV model with uniform random distribution	The impact of vertical transmission, media access control and oscillations
Rudra Pratap Ojha, Pramod Kumar Srivastava and GoutamSanyal [19]	SEIRS	Considering exposed and recovered and recovery rate is provided to the susceptible	Detection of worms in the system at an early stage, the technique for worm removal from WSNs
Upadhyay, R. K., and Kumari, S [21]	SITR	Considering sleep mode concept of WSN	Stability and direction of Hopf bifurcation for endemic equilibrium point of worm propagation of WSN
Abhishek Kumar and Nilam [25]	SIR	Considering the delay in the infected population by considering nonlinear incidence rate for epidemics along with Holling type II treatment rate	Stability analysis for disease free and endemic steady states
Madhusudanan, V., Geetha, R., [23]	SIR	Considered the delay in the interaction term of susceptible and infectious nodes	Stability analysis, delay analysis, Hopf-bifurcation
Geetha, R., Madhusudanan, V. and Srinivas, M.N [26]	SEIR	SEIR model with additive white noise	Stochastic stability, influence of noise on SEIR model

the increase in the delay value leads to the loss of stability of the model as well as existence of periodic oscillations that leads to the cause of a Hopf bifurcation. With the help of the performance of computer simulations, the authors validate the analytical studies. Also, recently, the authors [26] recently investigated the effect of noise on SEIR model (Table 1).

3 Conclusions and Future Works

We reviewed various research articles in the area of epidemic models of wireless sensor in a systematic way. The authors considered various mathematical models and investigated the stability about the equilibrium points. They also studied the delayed WSN models which are most useful for analysis of epidemiology, agribusiness, military, space and marine investigation.

Following the same symbolization, we can incorporate diffusive terms in almost all the models which are quoted in the above to study the dynamics of the WSNs with respect to time and space variables. The effect of dispersal and spatial heterogeneity is more important in the epidemiology, as it plays major role on the stability of the WSN's. The diffusive analysis may produce interesting results that the effect of diffusion coefficients in changing the unstable behaviour to stable one. It is also very important to analyse the dynamical features of the various models and to get an insight on the switch of stability in the presence of cross diffusion. Similarly, we can develop all above mentioned models in view of stochasticity i.e. impact of noise on the above models and it is necessary to compute the population intensities of fluctuations (variances) around the positive equilibrium due to white noise. We can also improve the above mentioned models (Sect. 2) to find the steady states by using various algorithms and numerical methods.

References

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks*, 38(4), 393–422.
2. Hu, F., Li, S., Xue, T., & Li, G. (2011). Design and analysis of low-power body area networks based on biomedical signals. *International Journal of Electronics*, 99(6), 811–822.
3. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks*, 51(12), 2292–2330.
4. Azad, P., & Sharma, V. (2015). Pareto-optimal clusters scheme using data aggregation for wireless sensor networks. *International Journal of Electronics*, 102(7), 1165–1176.
5. Verma, V. K., Singh, S., & Pathak, N. (2016). Impact of malicious servers over trust and reputation models in wireless sensor networks. *International Journal of Electronics*, 103(3), 530–540.
6. Haghghi, M. S., Wen, S., Xiang, Y., Quinn, B., & Zhou, W. (2016). On the race of worms and patches: Modeling the spread of information in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, 11(12), 2854–2865.
7. Kumar, V., Dhok, B. S., Tripathi, R., & Tiwari, S. (2016). Cluster size optimization with TunableElves sensing model for single and multi-hop wireless sensor networks. *International Journal of Electronics*, 104(2), 312–327.

8. Tang, S., & Mark, B. L. (2009). 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, 86–91. 2009, Washington, DC, USA.
9. De, P., Liu, Y., & Das, S. K. (2009). An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks. *IEEE Transactions on mobile Computing*, 8(3), 413–425.
10. Feng, L., Song, L., Zhao, Q., & Wang, H. (2015). Modeling and stability analysis of worm propagation in wireless sensor network. *Mathematical Problems in Engineering*, 2015, 1–8.
11. Mishra, B. K., & Keshri, N. (2013). Mathematical model on the transmission of worms in wireless sensor network. *Applied Mathematical Modelling*, 37(6), 4103–4111.
12. Ojha, R. P., Sanyal, G., & Srivastava, P. K. (2018). Pre-vaccination and quarantine approach for defense against worms propagation of malicious objects in wireless sensor networks. *International Journal of Information System Modeling and Design (IJISMD)*, 9(1), 01–20.
13. Wang, X. M., & Li, Y. S. (2009). An improved SIR model for analyzing the dynamics of worm propagation in wireless sensor networks. *Chinese Journal of Electronics*, 18(1), 8–12.
14. Wang, Y., Wen, S., Xiang, Y., & Zhou, W. (2014). Modeling the propagation of worms in networks: A survey. *IEEE Communications Surveys and Tutorials*, 16(2), 942–960. <https://doi.org/10.1109/surv.2013.100913.00195>.
15. Dubey, B. (2007). A prey-predator model with a reserved area. *Nonlinear Analysis Modelling and Control*, 12(4), 479–494.
16. Nwokoye, C. H., & Umeh, I. I. (2017). The SEIQR–V model: On a more accurate analytical characterization of malicious threat defense. *International Journal of Information Technology and Computer Science*, 9(12), 28–37.
17. Singh, A., Awasthi, A. K., Singh, K., & Srivastava, P. K. (2018). Modeling and analysis of worm propagation in wireless sensor networks. *Wireless Personal Communications*, 98(3), 2535–2551.
18. Ojha, R. P., Srivastava, P. K., & Sanyal, G. (2019). Improving wireless sensor networks performance through epidemic model. *International Journal of Electronics*, 106(6), 862–879.
19. Zhang, Z., Kundu, S., & Wei, R. (2019). A delayed epidemic model for propagation of malicious codes in wireless sensor network. *Mathematics*, 7(5), 396.
20. Awasthi, S., Kumar, N., & Srivastava, P. K. (2020). A study of epidemic approach for worm propagation in wireless sensor network. In V. Solanki, M. Hoang, Z. Lu, & P. Pattnaik (Eds.), *Intelligent computing in engineering. Advances in intelligent systems and computing* (Vol. 1125, pp. 315–326). Springer, Singapore. https://doi.org/10.1007/978-981-15-2780-7_36.
21. Shen, S., Huang, L., Liu, J., Champion, A. C., Yu, S., & Cao, Q. (2016). Reliability evaluation for clustered WSNs under malware propagation. *Sensors*, 16(6), 855. <https://doi.org/10.3390/s16060855>.
22. Mishra, B. K., & Tyagi, I. (2014). Defending against malicious threats in wireless sensor network: A mathematical model. *International Journal of Information Technology and Computer Science*, 6(3), 12–19.
23. Upadhyay, R. K., & Kumari, S. (2018). Bifurcation analysis of an e-epidemic model in wireless sensor network. *International Journal of Computer Mathematics*, 95(9), 1775–1805.
24. Kumar, A., & Nilam. (2018). Stability of a time delayed SIR epidemic model along with nonlinear incidence rate and Holling type-II treatment rate. *International Journal of Computational Methods*, 15(6), 1850055. <https://doi.org/10.1142/S021987621850055X>.
25. MadhuSudanan, V., & Geetha, R. (2020). Dynamics of epidemic computer virus spreading model with delays. *Wireless Personal Communications*, 115(3), 2047–2061.
26. Geetha, R., Madhusudanan, V., & Srinivas, M. N. (2021). Influence of clamor on the transmission of worms in remote sensor network. *Wireless Personal Communications*. <https://doi.org/10.1007/s11277-020-08024-4>.



M. N. Srinivas received his Ph.D. degree from JNTUK, Kakinada, Andhra Pradesh, India. He is currently working as a faculty at VIT University, Vellore, India. He has about 18 years of experience in academics and has published a number of research articles in various national and international journals. His major research interest is in Mathematical Biology and Ecology modeling, stability analysis.



V. Madhusudan received his PhD from Annamalai University; Chidambaram in 2017. He is working as Associate Professor in the department of Mathematics, S.A. Engineering College. He has a vast teaching and research experience in the field of Mathematics and Computer Science. His area of research is Mathematical modeling, Computational Intelligence and Control Systems. He has published many papers in various reputed national and international journals.



A. V. S. N. Murty is working as Associate professor in Mathematics at VIT, Vellore, Tamilnadu, India. He received PhD from Andhra University in March 2007. He has 17 years of Teaching experience and more than 10 years of Research experience. He published Research papers in reputed National and International Journals.



B. R. Tapas Babu obtained his Ph.D. in Electronics and Communication Engineering department from St. Peters University Chennai -54. He is currently working as Professor, Faculty of Electronics and Communication Engineering, S. A. Engineering College, Chennai -77. He has a total teaching experience of 20.6 years in engineering colleges alone. He has published 17 plus international journals which includes 3 papers in Web of Science and 5 in Scopus indexing. He is reviewers for few international journals in Springer and Inderscience publications. His area of research is Wireless Sensor Networks, Network Security and Image Processing. He is also interested in Digital Electronics, Microprocessor and Microcontroller, Analog and Digital Communication, Linear Integrated Circuits, and Control Systems. Completed B.E. (ECE) in the year 1997 from National Engineering College, Kovilpatti, Tamilnadu, India. Affiliated to Manonmaniam Sundaranar University. Completed M.E (Applied Electronics) in the year 2004 from Hindustan College of Engineering, Chennai. Affiliated to Anna University, Chennai.