Gyanshauryam, International Scientific Refereed Research Journal
© 2022 GISRRJ | Volume 5 | Issue 3 | ISSN : 2582-0095

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

MS Ojha, Assistant Professor, Govt. P.G. College Prayagraj, U.P., India
Prof. Manoj Kumar Srivastava, T.D.P.G. College, Jaunpur, U.P. , India

Artic Info

Publication Issue :
Volume 5, Issue 3
May-June-2022

Article History
Accepted : 01 May 2022
Published : 10 May 2022

Page Number : 127-141

ABSTRACT - Epidemic simulations have recently been used to model the dynamics of malicious codesin the network of wireless sensors. This is because of its open existence, which offers asim-ple 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 suchmodels that char-acterize worm dynamics in WSN. After a concise presentation of thewireless sensor net-work, some primary research consequences of e-pandemic models (of various researchers) are given and assessed. At that point the uses of wireless sensornetwork in the clinical wellbeing, agribusiness, and military, space and marineinvestigation are laid out. What's more, we break down the upside of wireless sensornetwork in these sectors. In this review article, we sum up the fundamental factors thatinfluence the uses of wireless sensor net-works in view of e-epidemic models and revivedsome epidemic models and also discussed some conceivable future works of different epidemic wireless sensor models.

Keywords : Wireless sensor networks, Nodes, Susceptible, Infected, Recovered epidemic

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

The fundamental highlights of remote sensor systems are self-association, multi-bouncecourse, dynamic system topology, hub assets restricted, information driven and securityissue. The hubs of the remote sensor organize have the programmed organizing capacityand the hubs can speak with one another. In the utilization of remote sensor arrange, regularlythe sensor hubs are put some place with no base system office. For example, a tremendousregion of virgin woodland, or the threat region where individuals cannot cometo, this requires the sensor hub has the self-association capacity to arrange and overseeconsequently. At the point when a hub can't straightforwardly speak with the passage, itrequires different hubs to transmit information, so the system information transmission is amulti-jump directing. In some unique applications, remote sensor organize is portable, sensorhubs may stop work on account of the vitality expended or other disappointment, thesecomponents will make the system topology changes. There are an enormous number ofsensor hubs in wireless sensor network and regularly need to master minded in a particularobserving zone. The equipment assets of sensor hub are restricted as a result of the size andcost requirements. So its registering power, stockpiling limit is generally feeble. Portablecorrespondence system or Ad hoc arrange for the most part thinks about how to improvethe system transmission limit under current conditions, that is to give clients a data transfercapacity adequate, protected and solid transmission channel. Be that as it may, wirelesssensor network is utilized to screen the different estimated information. In the system configurationprocess, we chiefly consider how to manage discernment information productivelyand transmit the got information to the client hub. Along these lines, one attributeof the remote sensor organize is information driven. As wireless sensor network systemutilizes remote transmission, so the observing information is anything but difficult to becaptured, or even befuddle clients in the wake of altering. After an enormous number ofsensor hubs are caught, the foe may utilize them to decimate the current system. Thusly, inthe 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 theremote sensor organize convention study, medium access control convention and directingconvention 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. Inthisway, in the structure of wireless sensor network, we should work for the proficient utilizationof vitality hub in the consummation of the prerequisites under the reason, beyond whatmany would consider possible to broaden the life of the whole system. In wireless sensornetwork, security organization is for the most part reflected in data security. Correspondencesecurity for the most part thinks about the security hub, detached guard interruptionassault and dynamic against intrusion. Furthermore, the data security for the most partthinks about the classification, honesty and viability of information.

With the progression of data innovation, there has been ascend in intolerable acts concerningremote systems. Such acts are security danger to an individual or a country. Aremote correspondence organize that guarantees security, dependability, proficiency wouldbe an incredible advantage for the cutting edge age individuals. Sensor hub in a remote systemis a smart, ease and little gadget. Remote Sensor Networks are utilized for occasionalinformation assortment to crucial sending. A few significant utilizations of WSNs aremilitary objective following, object observing agribusiness, calamity the executives, riskycondition investigation, ecological and contamination application, flood location, vehiclesfollowing, traffic checking, gas checking, water quality checking and seismic detecting,social insurance applications [1–3], and so forth. Nonetheless, sensor hubs are minimaleffort gadget that works cleverly. Also, they are asset limitation [4, 5]. In this way, becauseof constrained assets and decentralized design, remote correspondence alongside securityprovisioning between such systems is amazingly lumbering. Security dangers in remotesystem 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 inmulti-jump way [7]. An assailant focuses on a solitary hub of the system to dispatch theassault and this tainted hub spreads the worm in the whole system through neighbouringhubs [8]. Without a doubt, controlling worm engendering is urgent to guarantee sustenanceof the system. Along these lines, investigation of vindictive signs transmission and scientificdemonstrating turns into a fundamental instrument [9–20]. The exhibition of remotesensor networks is dissected by fluctuating different parameters, for example, hub thickness,standard deviation, correspondence go, and so on. By guaranteeing effective transmissionof 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 andto control malware transmission. To achieve this, another uncovered state (Q, R, V) is presentedthat helps in distinguishing the counterbalance of the malware from the get-go in theremote sensor networks. The hubs influencing the exhibition of system are considered asuncovered hubs. In such a circumstance, it goes basic to rapidly utilize restorative measuresto 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 attackerswhich are capable of attacking variety of mobile computing devices or nodes such assmart phones, laptops. These categories of malwares are capable of directly spreadingbetween the communicating devices through various wireless communication technologiessuch as Bluetooth, Wi-Fi etc. Since the propagation of worms among devices can be comparedwith the transmission of epidemic diseases such as Ebola and Corona virus amonghuman beings, the eco-epidemic models studied by the researchers can be incorporated tostudy and analyse the propagation dynamics of worms in wireless networks.Many researchers have published their work related to the epidemic model applicationsin the recent years. Inspiring on the aforementioned literature, we have formulatedthe SITR e-epidemic model and analysed the behaviour of worms spreading in the wirelessnetworks along with the major factors for this sort of propagation of worms which leads todraining 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 asclustering the nodes that is used for aggregating the data through which the consumption ofenergy can be minimized drastically.To examine the propagation of malwares and to control the infectious diseases, formulatingthe mathematical models according their behaviour play a major role. In recent literaturemany 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 authorsin 1927 to study the explosion of plague. Later the dynamic behaviour of such modelwas investigated by many researchers. The vaccine induced SIRS model was developedby the authors with inborn immunity. They analysed that the system underwent a reversebifurcation when the threshold is attained. The SIER model has an additional componentnamed Exposed apart from the susceptible, infected, recovered components which representsthat the infected people without symptoms may not spread the disease during thedormant 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 Sto study and analyse the global properties of the epidemic models. Later on variants of themodel was proposed by many researchers to represent infectious water body related diseaseslike bacterial infections.

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

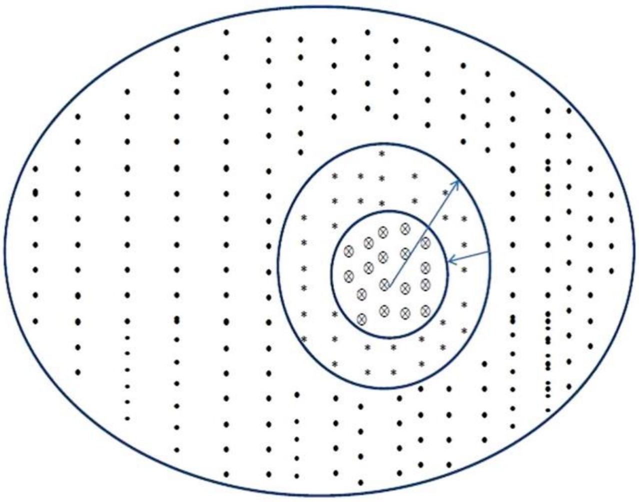

Fig. 1 Represents schematic diagram of the system proposed by [8]

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 susceptive, infective andrecuperated(recovered) hubs at time t, separately. Since the hubs are consistently haphazardlydisseminated with thickness σ, each contaminated hub can contact on the requestfor neighbour hubs. Be that as it may, reaching a neighbour doesn't really prompt anotherinfective hub. Review that there are three gatherings of hubs. Just a vulnerable neighbourof the contaminated hub can turn into another infective hub. Reaching a tainted neighbouror 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 consistentlyappropriated hub arrangement, the part of the tainted hub's neighbours that canget 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 aninfective and a helpless hub. Unmistakably β relies upon the infectivity of an infection andthe correspondence pace of a convention since the infection spreads itself by piggybackingon typical information through ordinary interchanges. Let γ indicates the recuperationlimit, which is the probabilistic rate at which an infective hub recoups and becomes insusceptiblewhen the infective hub is in the dynamic mode. Let $\_a$ and $\_m$ represent the rates atwhich a hub changes from the dynamic mode to the upkeep (rest) mode, and advances fromsupport to dynamic mode, separately. In the support mode, the framework upkeep programis consequently activated. The vulnerable and recuperation hubs will rapidly pass the checkand rest, while the infective hubs will set aside a more extended effort for treatment. Contingentupon the predefined timeframe of support (or rest), a small amount of the kept upinfective hubs, meant by p, will be restored and become recuperation hubs after continuingthe dynamic mode. The rest of the hubs will stay in the gathering of infective hubs. Weallude 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 improvethe system's enemy of infection ability and empower the system to adjust deftly to variouskinds of infections, without bringing about extra computational or flagging overhead. Theproposed model can catch both the spatial and transient elements of the infection spreadprocedure. We infer unequivocal investigative answers for the model and talk about somecommon sense uses of premium. Broad numerical outcomes are introduced to approve ourexamination. The proposed model (2.1, 2.2, 2.3) is relevant to the plan and investigation ofdata engendering instruments in correspondence systems.

Wireless sensor networks (WSNs) have gotten broad consideration because of theirextraordinary potential in common and military applications. The sensor hubs have constrainedforce 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—defencelesswith an immunization compartment (SEIRS-V) to depict the elements of worm engenderingas for time in WSN. The proposed model of [11] catches both the spatial and fleetingelements of worms spread procedure (Fig. 2).

The mathematical model for the proposed system is formulated as follows

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

$$E'(t) = \beta SI - (\mu + \alpha)E \qquad (2.5)$$

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

$$R'(t) = \gamma I - (\mu + \delta)R \qquad (2.7)$$

$$V'(t) = pS - (\mu + \eta)V \qquad (2.8)$$

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⁄ and 1⁄ are the periodsof immunity of the recovered & vaccinated susceptible nodes respectively, and A isthe inclusion of new sensor nodes to the population, is the crashing rate of the sensornodes due to hardware/software problem, is the crashing rate due to attack of worms, is the infectivity contact rate, is the rate of transmission from E-class to I-class, is the rate of recovery, is the rate of transfer from R-class to S-class, is the rate of transmissionfrom 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 offchance that generation number is short of what one, the contaminated portion of the sensorhubs vanishes and if the propagation number is more prominent than one, the tainted divisionendures and the doable locale is asymptotically steady area for the endemic balancestate. Numerical strategies are utilized to settle and recreate the frameworks of conditionscreated and furthermore to approve our model. A basic investigation of inoculation class

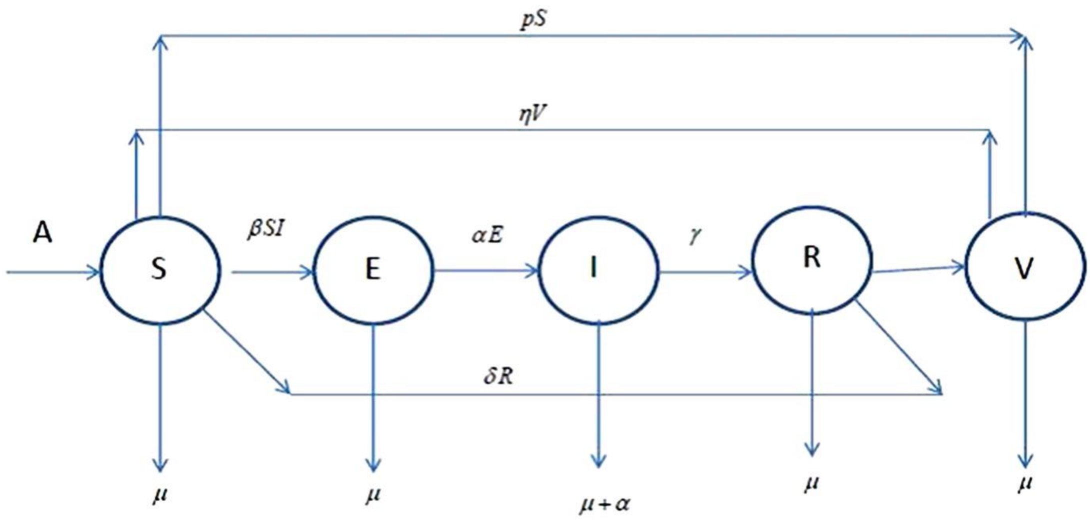

Fig. 2 Represents schematic diagram of the model proposed by [11]

concerningdefenceless 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.

$$S'(t) = \lambda - \varsigma SI - \tau S - \rho S + \varphi R + \xi V \quad (2.9)$$

$$E'(t) = \varsigma SI - (\tau + \theta)E \quad (2.10)$$

$$I'(t) = \theta E - (\tau + \omega + v + \alpha)I \quad (2.11)$$

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

$$R'(t) = \eta Q + vI - (\tau + \varphi)R \quad (2.13)$$

$$V'(t) = \rho S - (\tau + \varepsilon)V \quad (2.14)$$

Here μdenotes the energy of nodes exhaust, probability to convert into dead node, d_1 representsmortality rate of nods due to the failure of software, ρdenotes that the rate of vaccinationfor susceptible sensor nodes, ϕrepresents the rate at which recovered nodes becomesusceptible to infection, εrepresents the rate of transmission from the vaccinated compartmentto the susceptible one, ςdenotes that the effective contact with an infected node for transfer

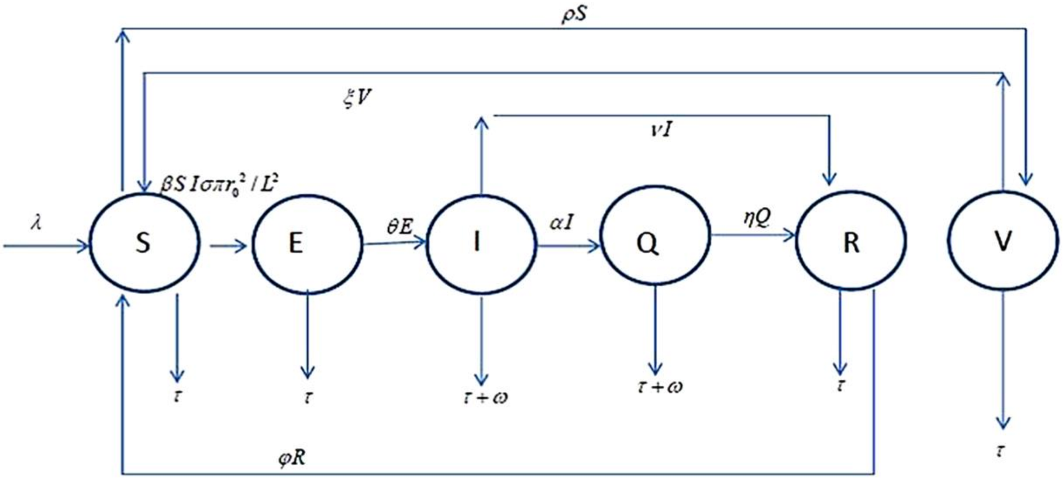

Fig. 3 Represents the schematic diagram of the system proposed by [16]

of infection, θrepresents the rate at which exposed nodes become infectious, d_2 representsthe crashing rate due to attack of malicious worms, μ_1 represents the rate of recovery, αrepresentsthe rate of transmission from the infectious compartment to the quarantined one, $\mu_2$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. Herewe take $\varsigma = \frac{\beta\pi\sigma r_0^2}{L^2}$ where βdenotes infectious contact rate. The representative arrangementsof the harmonies were inferred for two topological articulations separated from WSN writing.A reasonable numerical strategy was utilized to unravel, recreate and approve the alteredmodel. Recreation results show the impact of their alterations.

Wireless sensor networks (WSNs) experience basic test of Network Security due to outrageousoperational requirements. The beginning of challenge starts with the passage of wormsin 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. Inthis paper, a numerical model is proposed dependent on scourge hypothesis. It is an improvementof SIRS and SEIS models. In 2019, Ozha R.P, et al. [18], proposed SEIRS model thatbeats 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. μrepresents the probability to convert into dead node as

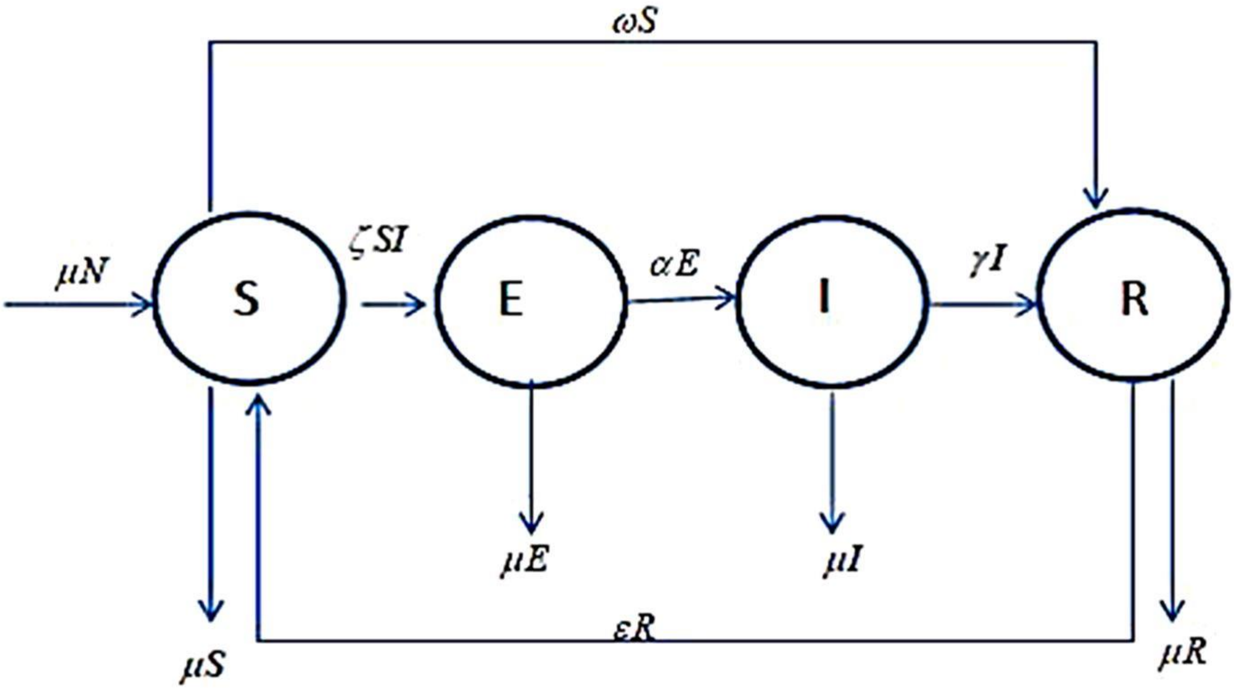

Fig. 4 Represents schematic diagram of the system proposed by [18]

the energy of nodes exhaust, $\zeta = (\pi r^2 \beta)/L2$ represents the total number of neighbouringnodes that are lying in the sensing area of a sensor node and where βdenotes infectiouscontact rate, the transmission area of a sensor node is $\pi r2$ with sensing range r , L^2 representsthe area in which the nodes are uniformly scattered, εrepresents the probability thatrecovered node may become susceptible again, ωrepresents the rate at which recovery isprovided to the susceptible node, αrepresents rate at which exposed node falls in the infectiousclass, γrepresents the rate of recovery is provided to the susceptible node. This proposed

enhanced model incorporates a limited correspondence sweep and the related hubthickness. The authors got essential generation number which decides the local and worldwideglobal proliferation elements of worm in

the WSNs. Similarly, the authors derivedarticulation for edge for hub thickness and correspondence range. They explored the controlinstrument against worm proliferation and also they contrast the proposed model anddifferent 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 proposedSEIRS model gives an improved strategy to restriction worms' transmission in correlationwith the current models.

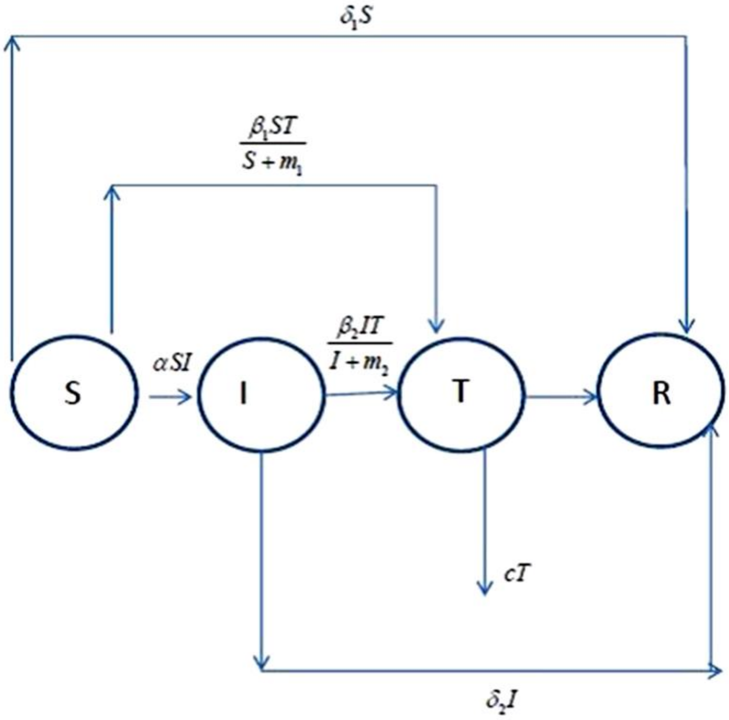

Fig. 5 Represents schematic diagram of the system proposed by [23]

An endeavour has been made to comprehend the transmission elements of malevolent signalsin 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.

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

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

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

$$R'(t) = \delta_1 S + \delta_2 I \tag{2.22}$$

where$S(t)$, $I(t)$, $T(t)$ and $R(t)$ denote the number of susceptible, infectious, terminallyinfected and recovery nodes at time t respectively. r_1 and r_2 represents intrinsic growth ratesof susceptible and infected nodes respectively, k and l represents carrying capacities ofsusceptible and infectious nodes respectively, $\alpha$and α_1 represents transmission rates, $\beta_1$representsinter-nodes interference coefficient of class T for susceptible node, β_2 representsinter-nodes interference coefficient of class T for infectious nodes, m_1 and m_2 representshandling time of susceptible and infected nodes respectively, δ_1 and δ_2 represents recoveryrates for susceptible and infectious nodes respectively, c represents crashing rate of the terminallyinfected node. Steadiness investigation is performed for all the equilibrium focuses,whose trademark conditions include the time delay. Global stability and Hopf bifurcationexaminations 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 ofthe subsequent intermittent arrangements. Numerical investigation displays twofold Hopfbifurcation dynamics and it causes steadiness exchanging i.e., shakiness to strength andback to precariousness or the opposite progress of the arrangement of the thought aboutframework. At long last, numerical recreations give helpful perceptions to various postponementsand they show an intriguing bifurcation situation. The effect of the controlparameters β and τ on the framework elements has been examined. The outcomes of proposeddelayed model that the information parcel delay and discrete deferral are responsiblefor the dependability exchanging and the event of confused elements separately. The nearnessof disorganized elements demonstrates delicate security arrangement of the system.By looking into the re-enactment results, the authors found that the best control measuresto control the proliferation of pernicious signs.In 2018, authors Abhishek Kumar and Nilam [24], presented a mathematical study ofa deterministic model for the transmission and control of epidemics. They proved that theincidence rate of susceptible being infected is very crucial in the spread of disease andalso the delay in the incidence rate is fatal. The authors proposed an SIR mathematicalmodel with the delay in the infected population by considering nonlinear incidence rate forepidemics along with Holling type II treatment rate for understanding the dynamics of theepidemics as follows (Fig. 6).

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

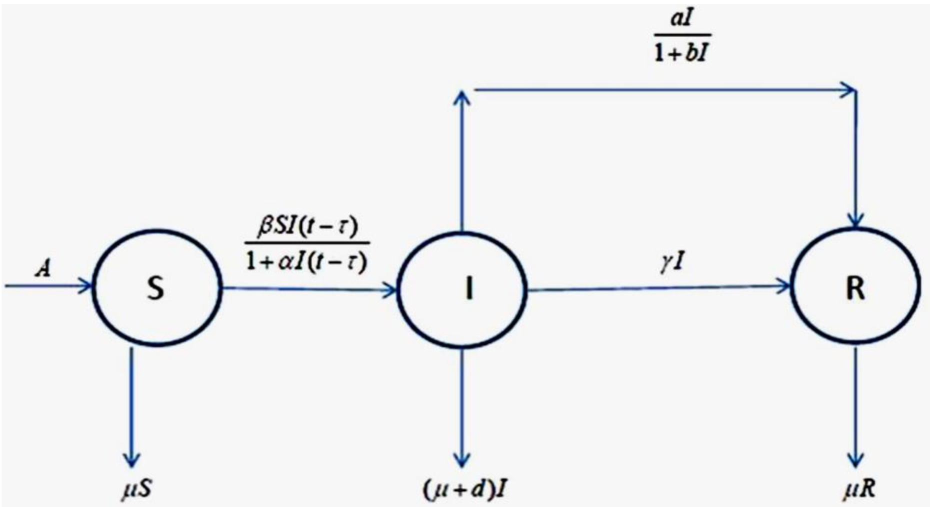

Fig. 6 Represents schematic diagram of the system proposed by [24]

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

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

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

The authors analyzed the stability by considering the basic reproduction number R_0in terms of locally asymptotically stable for disease-free equilibrium when the basicreproduction number R_0 is less than one and investigated the stability of the model fordisease-free equilibrium at R_0 equals to one using center manifold theory. They alsoexamined 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 tosusceptible individuals via contacts. As time passes, infected individuals lose infectivityand move to recover compartment by auto recovery due to autoimmune response of thebody or by treatment. Also, Holling type II treatment rate is considered for the recoveryof the infected population. Where A represents recruitment rate per day, α representsmeasure of inhibition, β represents effective contact rate, μ represents natural mortalityrate, d represents disease induced mortality rate and γ represents recovery rate, a ispositive constant and b is a constant taking into account as resource limitation $\tau > 0$ isa fixed time during which the infectious agents develop in the vector and it is only afterthat time that the infected vector can infect a susceptible individual. Additionally, mathematicalsimulations are offered to epitomize the investigative studies.

The weakness that exists in the computer network by the disease of infection whenthe assets are uncovered requires the investigation of the idea of proliferation of infectioninto the network. In 2020, the authors V. Madhusudanan and R. Geetha [25] haveassumed a novel pandemic Susceptible-Infected-Recovered model by assuming thateach node is denoted as one computer and the state of it can be healthy computer butare 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 whichcannot get disease or transmit and that manages the contaminated hubs in the organizationregarding the turn of events of insusceptibility accomplished after recuperation asfollows (Fig. 7).

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

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

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

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

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 examinedby Routh–Hurwitz criteria without delay. The time arrangement examination withrespect to nature of the defenceless, contaminated and recuperated hubs in the organizationhas been performed utilizing genuine control parameter oriented boundaries. The authorsadditionally dissected that time deferral may play critical part on the strength of the proposedmodel since at whatever point delay surpasses the basic esteem the framework loses its steadiness and a Hopf bifurcation happens. The mathematical reproduction results legitimizethat the proposed model is approved against the scientific investigations of infectionproliferation and subsequently inspecting the hypothetical outcomes. Where b is new numberof the computers, p is the immune rate of the computers, $\beta$is the infection rate of theinfected computers, d is the death rate of computers, $\delta$is loss rate of immunity of the recoveredcomputers, d is death rate due to virus, $\alpha$is the recovered rate of the infected computers,$\gamma$is the saturation factor that measures the inhibitory effect. Finally authors observedthat the time delay may play significant role on the stability of the proposed model, since

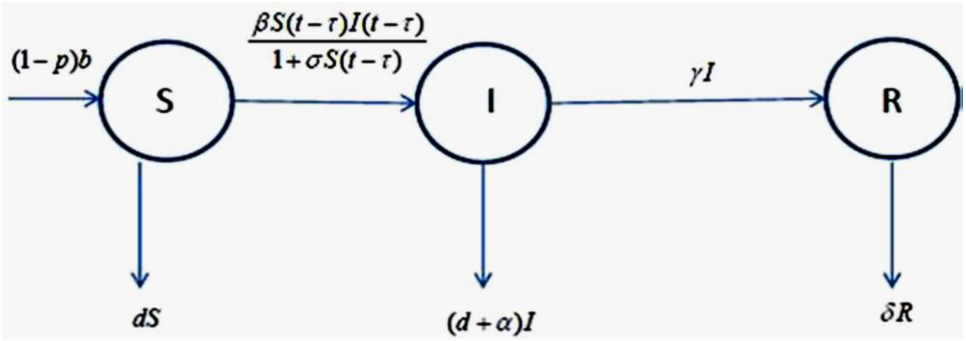

Fig. 7 Represents schematic diagram of the system proposed by [26]

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 Keshr i, 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
RudraPratapOjha, Pramod Kumar Srivastava and GoutamSanyal [19]	SEIRS	Considering exposed and recovered and recover y rate is provided to the susceptible	Detection of worms in the system at an early stage, t he 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 existenceof periodic oscillations that leads to the cause of a Hopf bifurcation. With the help ofthe 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 sensorin a systematic way. The authors considered various mathematical models and investigatedthe stability about the equilibrium points. They also studied the delayed WSN modelswhich are most useful for analysis of epidemiology, agribusiness, military, space andmarine investigation.

Following the same symbolization, we can incorporate diffusive terms in almost all themodels which are quoted in the above to study the dynamics of the WSNs with respect totime and space variables. The effect of dispersal and spatial heterogeneity is more importantin the epidemiology, as it plays major role on the stability of the WSN's. The diffusiveanalysis may produce interesting results that the effect of diffusion coefficients in changingthe unstable behaviour to stable one. It is also very important to analyse the dynamicalfeatures of the various models and to get an insight on the switch of stability in the presenceof cross diffusion. Similarly, we can develop all above mentioned models in viewof stochasticity i.e. impact of noise on the above models and it is necessary to computethe population intensities of fluctuations (variances) around the positive equilibrium due towhite noise. We can also improve the above mentioned models (Sect. 2) to find the steadystates 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 onbiomedical 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 wirelesssensor 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 reputationmodels in wireless sensor networks. International Journal of Electronics, 103(3), 530–540.
6. Haghighi, 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 InformationForensics and Security, 11(12), 2854–2865.
7. Kumar, V., Dhok, B. S., Tripathi, R., &Tiwari, S. (2016). Cluster size optimization with TunableElfessensing model for single and multi-hop wireless sensor networks. International Journal of Electronics,104(2), 312–327.A Review Article on Wireless Sensor Networks in View of E-epidemic…
8. Tang, S., & Mark, B. L. (2009). Analysis of virus spread in wireless sensor networks: An epidemicmodel. Proceedings of the 2009 7th International Workshop on the Design of Reliable CommunicationNetworks, DRCN 2009, 86–91. 2009, Washington, DC, USA.
9. De, P., Liu, Y., & Das, S. K. (2009). An epidemic theoretic framework for vulnerability analysis ofbroadcast 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 propagationin 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 wirelesssensor network. Applied Mathematical Modelling, 37(6), 4103–4111.
12. Ojha, R. P., Sanyal, G., &Srivastava, P. K. (2018). Pre-vaccination and quarantine approach fordefense against worms propagation of malicious objects in wireless sensor networks. InternationalJournal 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 propagationin 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 andControl, 12(4), 479–494.

16. Nwokoye, C. H., &Umeh, I. I. (2017). The SEIQR–V model: On a more accurate analytical characterizationof malicious threat defense. International Journal of Information Technology and ComputerScience, 9(12), 28–37.

17. Singh, A., Awasthi, A. K., Singh, K., &Srivastava, P. K. (2018). Modeling and analysis of wormpropagation 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 performancethrough 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 maliciouscodes in wireless sensor network. Mathematics, 7(5), 396.

20. Awasthi, S., Kumar, N., &Srivastava, P. K. (2020). A study of epidemic approach for worm propagationin wireless sensor network. In V. Solanki, M. Hoang, Z. Lu, & P. Pattnaik (Eds.), Intelligentcomputing 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 evaluationfor 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 wirelesssensor 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 nonlinearincidence rate and Holling type-II treatment rate. International Journal of Computational Methods,15(6), 1850055. https:// doi. org/ 10. 1142/ S0219 87621 85005 5X.

25. MadhuSudanan, V., &Geetha, R. (2020). Dynamics of epidemic computer virus spreading modelwith delays. Wireless Personal Communications, 115(3), 2047–2061.

26. Geetha, R., Madhusudanan, V., &Srinivas, M. N. (2021). Influence of clamor on the transmissionof worms in remote sensor network. Wireless Personal Communications. https:// doi. org/ 10. 1007/s11277- 020- 08024-4.