Wireless Personal Communications (2022) 125:1827–1856
https://doi.org/10.1007/s11277-022-09636-8

Epidemic Models of Malicious-Code Propagation and Control in Wireless Sensor Networks: An Indepth Review

ChukwuNonso H. Nwokoye[1] · V. Madhusudanan[2]

Accepted: 7 February 2022 / Published online: 5 April 2022

Abstract

Besides anti-malware usage for the eradication of malicious attacks, researchers have developed epidemic models in order to gain more insights into the spread patterns of malware. For wireless sensor networks (WSN), these epidemic models, which are equation-based, have been seen to characterize both salient features of the network as well as the dynamics of malware distribution. In this study, an in-depth review aimed at generating the strengths and weaknesses of Susceptible-Infected (SI)-based compartmental models of malware spread in WSN was performed. Emphasis is placed on models resulting from the biological SI model developed by Kermack and Mckendrick, and its subsequent adaptation for malware spread in communication networks. Specifically, lessons and open areas were presented in accordance with the following factors: communication graph/topology, multi-group modeling, horizontal/vertical transmission (VT), communication range and density, patching, protocols, sensor mobility, energy consumption, optimal control/cost, stability, delay analysis, and numerical simulation. Amongst several findings, it was discovered that epidemic WSN models are yet to sufficiently represent medium access control, VT, alongside limited battery power, memory, authentication (using key schemes), survivability and availability etc. Additionally, only a few epidemic models have been developed to represent botnet propagation, concurrent multiple malware infection types, and sensor mobility in WSN.

Keywords Wireless sensor network · Mathematical models · Worm · Virus · Trojan · Botnet · Malware · Epidemic theory

✉ ChukwuNonso H. Nwokoye
chinonsonwokoye@gmail.com

V. Madhusudanan
mvms.maths@gmail.com

[1] Nigerian Correctional Service, Awka, Nigeria

[2] Department of Mathematics, S.A Engineering College, Chennai 600077, Tamilnadu, India

1 Introduction

Fundamentally, wireless sensor networks (WSN) are a network of sensor nodes that collectively monitor and perhaps control the sensor field, thus facilitating interactions between individuals or computer systems as well as the field of interest (FoI) [1]. Recently, WSN has generated plenty of research interest because of its crucial functions in several applications. The numerous WSN applications in defense, agro-industries, environmental surveillance, hazard reporting, and infrastructural performance monitoring are all examples of industries that need to be monitored [2]. In the military, it facilitates observing troops and armaments on the battlefield, reconnaissance, aiming, and combat damage assessment, while in the environment, it enhances insect monitoring, mapping of complexity, crop monitoring, and wildfire and flood inundation sensing and identification. Its uses include healthcare where it makes remote patient/doctor monitoring, and medication management possible. Advances in wireless communication have facilitated the production of these low-powered, low-cost infrastructure-less networks compared to the traditional WSN [3]. Sensors are deployed in and around the FoI and, by way of self-organization, the WSN is formed. More so, data packet communication to neighboring sensors is actualized through hopping. Collected data from monitoring may be managed by many nodes throughout transmission to arrive to the gateway node after hop-by-hop routing, and then to the control node via the world wide web or some network [4]. Indeed, with constrained battery power, activities such as sensing, processing, and transmission trigger a design method that unsurprisingly demands the combined contemplation of protocols for communication, processing of data, and signal distribution.

On WSN hardware, the architecture (Fig. 1) includes a sensor (the main part), a microcontroller, power management module and a transceiver (wireless). These parts, though miniaturized, play several roles, ranging from providing the power necessary for accumulating data to guaranteeing the strong transfer of signals. However, sensors can

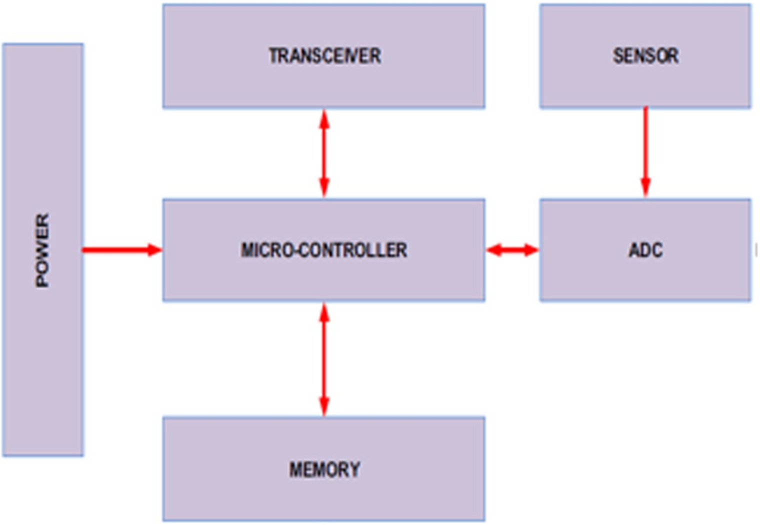


Fig. 1 Architecture of a node [1]

be furnished with an energy harvesting ability that is used to elongate work times. The trend is energy harvesting WSNs (EH-WSN), which can enable sensors by exploiting several sources (i.e. radiant, mechanical and thermal) of ambient energy [5]. While enumerating the following energy sources, which include solar, wind, vibration, thermal, ocean waves, nuclear reactions, acoustic noise, and radio frequency energy, Kanoun et al. [6] maintained that EH-WSNs are constrained, unsteady, unpredictable, and changeable in relation to the application and the environmental circumstances.

In defining the WSN multi-hop architecture, where nodes can both receive and transmit data packets, it is a routing concept in which data is transferred between two end points with the help of intervening nodes. Here, the source node sends data to a neighboring sensor, then this node transfers the collected data to a node within reach but in the direction of the gateway. This transmission procedure is continued until the packet reaches the gateway, which is its final destination. Additionally, the idea of multi-hop routing is achieved using several protocols categorized as either single-path or multipath [4]. Typically, WSN has challenges which are limited node energy and unstable transmission links. Through the self-organization method, networking of nodes provides the opportunity to improve robustness, and its outcome is an intelligent mesh network. Therefore, through this network type, sensors may possess several communication pathways in order to enhance network reliability. The interconnection technology used here is the 6LoWPAN low-power wireless, and this depends on the internet protocol version 6 (IPV6) addressing configuration, processing of data and signal distribution.

Note that the unsuitability of the contemporary approaches for employing high transmission rates is due to sensor node unreliability. This is as a result of the irregular/uneven environment, consumption of energy, and latency (stern real-time demands). Aside from sensors, a gateway is typically used in the WSN topology to connect to the internet. The deployment procedure and node organization follow some topology (linear, star, tree, mesh) or without any predetermined position [7]. Designed to depend on battery power, the sensors can transmit information over a distance of 800 to 100 m.

WSNs are designed bearing 'adaptation' in mind, i.e., they possess the ability to work irrespective of degradation problems caused by instability in transmission resulting from the rough sensor field. WSNs are more susceptible to interference and occlusion, resulting in failed transmission, when compared to conventional networks. The spread out nature of WSN queries the issue of privacy and security of sensor nodes. By implication, what is the possibility of guarding numerous data points against malicious attack by black hat hackers? Therefore, WSN demands remarkable conditions for trust, security, and privacy. Based on predetermined parameters, the network is split into numerous clusters. For each cluster, one sensor is chosen as the cluster head (CH), also known as the sub-network area head (SNH). The core operation, such as data gathering from member nodes, is handled by this SNH [8]. To tackle the issues, several clustering techniques have been widely utilized in WSN information exchange. In the light of WSN constraints, i.e. network performance, energy consumption, reliability, data aggregation, network coverage, and longevity [8], it is verily necessary that researchers in the field of network security expend efforts to remedy the instances of malware spread. One of such remedial approaches is the use of mathematical models (in the form of mathematical equations) to represent salient factors of malicious code propagation in WSNs, thus highlighting effective containment measures meant for educating network managers.

Since widespread Internet use has been severely harmed by data leaks and malware infection, it is acknowledged that the only strategy for strengthening general information security is to decontaminate cyberspace, optimize and standardize use groups and procedures. Mathematical models representing malicious objects' replication may aid in comprehending not just the dynamical behavior and spatial arrangement of malware, and also the relationships between the elements that influence malware propagation [9]. Therefore, the study is aimed at reviewing epidemic mathematical models originating from the susceptible–infected-removed (SIR) model developed by Kermack and Mckendrick [10] for biological networks but was further introduced for modeling communication networks due to similarities that exist between disease-causing agents and malwares. In the modelling of malware transmission in WSNs, this work analyzes numerous variables and associated phenomena. In addition, sensor designers, WSN authorities, scholars, and scientists will find this study useful since it provides a comprehensive description of epidemic research in each type of malware that exists in WSN.

The models reviewed herein are based on epidemic theory, which attempts to understand the infection outcomes of a given WSN population. Essentially, our study sought to expand a recent review [11] on WSN epidemic models, and to provide more insights on the journey of representing malware spread. The discoveries are discussed under the following subheadings; communication graph/topology, multigroup modeling, vertical/horizontal transmission, communication range and density, patching, protocols, sensor mobility, energy consumption, optimal control/cost, stability, delay analyses and numerical simulation.

The paper is organized as follows; Section II contains the taxonomy of malicious objects, while Section III presents the methodology of the review. Section VI discusses the findings and open areas, whereas Section V presents the conclusion of the study.

2 Taxonomy of Cyber Threats

This section presents taxonomical definitions for renowned threats (worm, virus, trojan and botnets) to cyber security. Malicious self-replicating and self-propagating programs are the major source of threats or attacks to cyber security. Generally, these are malicious objects whose purpose is to literally damage nodes, drain their energy, disrupt normal connections between them, or compromise the integrity of normal packets of data. The malware types in WSN to be reviewed are defined below.

2.1 Virus

This is a piece of computer code that attaches itself to a computer program, such as an executable file. Basically, virus propagation is activated when the infectious program is executed by a human. As it relates to networks, a virus is a collection of computer codes or scripts that may corrupt data or disable device operations and propagate across the Internet or wireless networks [12]. WSNs, by their complex nature, topology, and constraints in terms of limited energy, storage, and bandwidth [13], are susceptible to these kinds of malicious objects that can append themselves to a file, reproduce themselves, and spread to other files.

2.2 Worm

This is a stand-alone code process/thread running beneath the computer's operating system, and subsequently aiming to infect other connected systems. A worm is a hostile self-replicating software that could infect and propagate to uninfected computers without the need for human interaction [14]. On computers, they are independently replicating and autonomous infection agents capable of exploiting security or policy flaws in new host systems and infecting them via the network. It is a self-contained program designed to hop from machine to machine on its own, and while running in an infinite loop, it harms or bogs down a network by consuming its bandwidth [15]. According to Wang [16], sensor worm attacks over static WSNs are extremely destructive due to the large amount of generated scanning and communication traffic.

2.3 Trojan Horse

This is a type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the trojan, typically causing loss or theft of data and possibly system harm. Malicious programs are classified as Trojans if they do not attempt to inject themselves into other files (like a computer virus) or propagate themselves (like the computer worm). Describing a WSN trojan, Jalalitabar et al. [17] maintained that invasion of this malware type can change performance by interrupting communication or corrupting data.

2.4 Botnets

A malicious botnet is an interactive, self-replicating, self-propagating, and self-contained network programs that, when released, breaches the laws issued by a legislative body. It can be generally defined as an interactive, self-replicating, self-propagating, and self-contained network program. Note that, botnets vary from worms (regardless of the fact that they are occasionally propagated in a worm-like fashion) in that the botmaster's intentions rely on the survival of contaminated nodes [18]. More so, the inherent features of sensor networks as well as the conveniences of (internet of things) IoT devices have allowed the propagation of potential threats from botnets [19].

3 Methodology for the Review

A thorough literature review dealing with many aspects of malware outbreaks in WSN was conducted in this study. Many academics have worked hard to improve the functionality of WSNs and have authored multiple papers in the process. As a result, a lot of time and effort went into selecting the research articles for this evaluation. The Web of Science, SCI indexed, Scopus and Crossref databases were used to narrow down the selection of research papers that indicate a great level of research rigor. The review paper examines the content of 102 research publications published in various journals between 2005 and 2021 on the issue of malware distribution in WSNs. The stages of the review include:

- The gathering of research articles includes keyword searches, search string definitions, and access to a variety of academic resources. WSNs epidemic models were collected using a combination of the following terms: wireless sensor network, mathematical models, malware, worms, viruses, botnets, and epidemic models.

- Research articles are chosen based on their citations, publisher's databases such as Web of Science or Scopus (to guarantee a high degree of thoroughness), and the scholarly works that best fit epidemic models in WSNs.
- Descriptive analysis to first discover epidemic models in WSN and to classify the studies into their respective malware categories (virus, worm and trojan etc.) in the light of the paper strengths/achievements. Afterwards, the acronyms of both WSN features and malware dynamics are placed as column headings of the tables in the Result section. Once a particular feature/parameter is noted in a paper, the corresponding cell/field is checked with a tick symbol (ü). This implies that the author (s) considered those specific WSN characteristics or malicious objects' parameter within their article. Otherwise, the cell is empty and, by implication, that parameter has not been employed in the article.
- Reviewing articles, identifying research gaps, and suggesting open areas.

Specifically, most of these models are published in journals of applied mathematics and computation, journals of mathematical modeling, computer networks/Information security and journals of communication and networks (and/or their variants). A total of 71 experimental research papers out of the total 102 papers were used to generate the following tables in the section. The remaining 31 papers are cited in other parts of the review paper.

4 Results

In the 71 experimental research studies, authors represent epidemic theory, malware dynamics and some WSN features using SI-based epidemic compartmental models, which are basically mathematical equations. These 71 articles, with their publication dates, are depicted in Fig. 2. Therefore, full meanings of the models generated by the review are presented in Table 1. Table 2 presents 26 WSN epidemic models on worm propagation, while

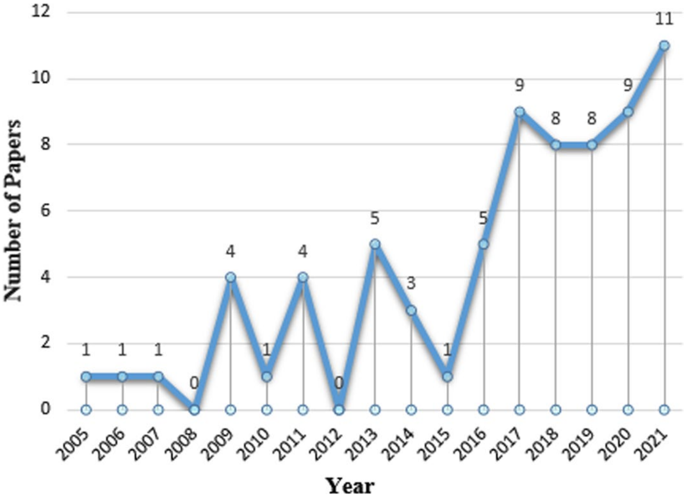


Fig. 2 Reviewed epidemic models and dates of publication

Table 1 Epidemic models and their meanings

Models	Meaning
SIS	Susceptible-Infected-Susceptible
SIR	Susceptible-Infectious-Recovered
SEIQR	Susceptible-Exposed-Infectious-Quarantined-Recovered
SIR-M	Susceptible-Infectious-Recovered-Maintenance
SEIRS-V	Susceptible-Exposed-Infectious-Recovered-Vaccinated
SEIQRS-V	Susceptible-Exposed-Infectious-Quarantined-Recovered-Vaccinated
SIQRV	Susceptible-Infectious-Quarantine-Recovered-Vaccinated
SIRD	Susceptible-Infected-Recovered-Dead
Q-SEIR	Quarantined-Susceptible-Exposed-Infectious-Recovered
Q-SEIRV	Quarantined-Susceptible-Exposed-Infectious-Recovered-Vaccinated
VLBT-I	Vulnerable-Latent-Breaking Out-Temporarily Immune-Inoculation
SILRD	Susceptible-Infected-Low-energy-Recovered-Dead
SI_1I_2LD	Susceptible-Infected-Mutant-Low-energy-Dead
SILSLID	Susceptible-Infected-Susceptible in Low-energy-Infected in Low-energy-Dysfunctional
SIKS	Susceptible-Infected-K reinfections-Susceptible
SIQRS	Susceptible-Infected-Quarantine Recovered
eVCjRI	Vulnerable-Contagious due to virus-Contagious due to worm-Contagious due to Trojan-Recovered-Inoculation
SEjIjR-V	Susceptible-Exposed (due to worm)-Exposed (due to virus)-Infectious (due to worm)-Infectious (due to virus)-Recovered-Susceptible-Vaccination
SE_1E_2IR	Susceptible, Infected class of short latent period-Infected class of long latent period-Infective-Recovered
IOT-SIS	Fraction of the Susceptible in the local network-Fraction of the Susceptible in the neighbour set-Fraction of Infected via random scanning-Fraction of Infected via local scanning-Fraction of Infected via peer to peer communication
IoT-SIEF	IoT- Susceptible, Infectious, Expose and Forensic
SSIIRRD	Susceptible-Susceptible while sleeping-Infected-Infected while sleeping-Recovered-Recovered while sleeping- Dead
SEIRD	Susceptible-Exposed-Infectious-Recovered-Dead
SNIRD	Susceptible-iNsidious-Infectious-Recovered-Dysfunctional
HSIRD	Heterogeneous Susceptible-Infectious-Removed-Dead
SITPS	Susceptible-Infected-Traced-Patched-Susceptible
SEIRS-F	Susceptible-Exposed-Infected-Recovered-Failed
SIALS	Susceptible–Infected–Anti-malware–Low-energy–Susceptible
SILS-P	Susceptible-Infected-Low-energy-Susceptible model under Pulse charging
SISIR	Susceptible cluster head-Infected cluster head-Susceptible common nodes-Infected common nodes-Recovered
SIR_1R_2	Susceptible-Infectious-Basically recovered-Completely recovered
$B_kBI_kBI_k$	Uncompromised devices- Bots, uninformed about control commands- Bots, informed about control commands

Table 3 presents 16 WSN epidemic models on virus propagation. Table 4 contains 3 WSN epidemic models on botnet propagation, whereas Table 5 contains 5 WSN epidemic models for multiple malware types. Table 6 presents WSN epidemic models with no particular malware type (MMPT). The percentage distribution for the reviewed models is depicted

Table 2 WSN epidemic models on worm propagation

Refs.	Model	CO	DA	EC	ES	HT	M	MP	ND	NQ	Ro	RIC	STE	TCR	V
[20]	SI					✓									
[21]	iSIR			✓		✓			✓					✓	
[22]	SIRD					✓			✓						
[23]	SEIRS-V				✓	✓				✓	✓		✓		✓
[7]	SEIQRS-V				✓	✓				✓	✓		✓		✓
[24]	SIQRS					✓			✓	✓			✓		
[25]	SIR					✓			✓		✓	✓	✓		
[26]	SEIRS-V				✓	✓			✓		✓	✓	✓		✓
[27]	SIQR					✓				✓	✓		✓		
[28]	SIDR			✓		✓					✓		✓	✓	
[29]	SIS					✓			✓					✓	
[30]	Q-SEIR + Q-SEIRV				✓	✓							✓		✓
[31]	SEIQRS-V				✓	✓			✓	✓	✓			✓	✓
[32]	VLBT-I					✓			✓		✓			✓	
[33]	SEIRS-V				✓	✓			✓		✓			✓	✓
[16]	SI	✓				✓	✓	✓							
[34]	SIQS					✓			✓	✓	✓	✓	✓		
[35]	Traditional &Agent SEIR-V				✓	✓							✓		✓
[36]	SEIQR				✓	✓			✓	✓	✓	✓			
[37]	SIQRV					✓			✓	✓	✓		✓	✓	✓
[38]	SEIRV				✓	✓			✓		✓	✓	✓		✓
[39]	SEIQRV				✓	✓				✓	✓	✓	✓		✓
[40]	SEIQRV				✓	✓			✓	✓	✓	✓	✓		✓
[41]	SILRD	✓		✓		✓		✓	✓					✓	
[42]	SEIRS-V		✓		✓	✓									✓
[43]	SEIRS-V		✓		✓	✓							✓		✓

in Fig. 3. From that figure, it is clear that epidemic WSN models on worm propagation are the largest followed by WSN models wherein the authors mentioned no particular malware type.

The following acronyms are used in the tables below:

BP: Battery power
C: Charging
CA: Cellular automation
CO: Cost/optimal strategies
DA: Delay analysis
DG: Differential Game
EC: Energy consumption
ES: Exposed stage
FA: Forensic Add-on
H: Heterogeneity
HT: Horizontal transmission
M: Mobility
MAC: Medium access control
ME: Memory efficiency
MP: Mobile patching
ND: Node density
NQ: Node quarantine
NR: Node recovery
P2PC: Peer to peer communication
Ro: Reproduction number
RIC: Radius of Infection/Communication
STE: Stability of equilibrium points in analysis
SW: Sleep and work rescheduling policy
TCR: Transmission/communication range
V: Vaccination

Considering the seeming ambiguities in the models, it is necessary to provide clarifications since there are no naming conventions. There are models where ‘S’ is placed at the end, for instance; SIS, SEIRS-V, SEIQRS-V and SIQRS. This implies that the recovered sensor nodes become susceptible to another infection. Furthermore, the difference between the SI and SIS models is that while the former does not consider reinfection, the latter does.

iSIR is equivalent to the SIR model; the ‘i’ is used to introduce some form of modification to the basic KM model. In addition, the VLBT-I model is also equivalent to the SEIRS-V model, because both models consider loss of temporary immunity. Here, synonyms were used, i.e., vulnerable/susceptible, latent/exposed, breaking out/infected, temporary immune/recovered, and inoculation/vaccination. Note that at the latent/exposed stage, the nodes are infected but not infectious, while at the breaking out/infected stage, the sensors are both infected and infectious. At the exposed stage, the speed of communication may be somewhat reduced. Interestingly, the difference between SEIR-V and SEjIjR-V is that in the latter, the exposed and the infected class are divided amongst the malware types involved in the study i.e. they have subclasses.

The SNIRD model [73] involves the N (iNsidious) and D (dysfunctional) compartments of the basic SIR model. N represents a different type of exposed stage where a sensor node is infected with malware, but the infection evades the installed intrusion detection system. D is a state where a node is defective as a result of a malware attack, exhaustion of battery power, or physical destruction. The D in the SNIRD model is different from the dead sensor nodes (D) of the SEIRD model [72]. Shen et al. [74] added heterogeneous (H) and dead (D) compartments to the basic SIR model to form the HSIRD model, which characterizes heterogeneity in the form of communication connectivity. The Traced (T) and Patched (P) compartments were conceived to form the SITPS model [75]; while the T node detects an infected node, the P node allows inoculation with a new patch, thus making the network free of the malware infection. The F in the SEIRS-F model signifies failed sensors. At this state, there is sensor death due to malevolent physical harm, subsystem malfunction, battery drain, or a fast depletion when contaminated by a malicious code.

In most malware epidemic studies, it was observed that one model could be used to represent different issues, matching the intentions of the authors. For instance, Mishra and Tyagi [7], and Nwokoye and Umeh [31] worked on the SEIQRS-V model, but the latter considered transmission range and density, i.e., WSN factors, which are absent in the former. Reference [40] used the same model, but employed the topology described by Feng et al. [25], while Nwokoye and Umeh [31] applied the topology described by Tang and Mark [46].

Figures 4 and 5 are Venn diagrams for relationships between the models reviewed in Tables 2, 3, 4 and 5. The diagrams are explained thus; at the intersection of all malware represented in Fig. 4 is the SI model by KM [71]—the acclaimed origin of all recent models, while the intersection of Fig. 5 is SI and SIS.

Virus ∩ Worm ∩ Botnet = SI
Virus ∩ Botnet = SIR
Worm ∩ Botnet = SIR
Virus ∩ Worm = SIS, SIR
MMT ∩ MMPT = SI, SIS

Figure 4 implies that the SIR model have been used to characterize the spread of virus, botnet and worm. Moreover, the SIS model has also been applied for the modeling of both virus and worms spread. The models that mentioned no particular malware type as well as multiple types of malware has SI and SIS models in common (Fig. 5). Figures 4 and 5 are clear indications that advancement in WSN infection modeling can be traced to the original compartmental (SI or SIR) models developed by Kermack and Mckendrick. In fact, new authors in this area of research build on top of these.

The above tables clearly highlight what has been done so far by employing WSN epidemic models, thus bringing to the fore several deficiencies and weaknesses, which include the absence of authentication, reliability, survivability, and availability. These factors are missing from these tables and the implication is that they have not been sufficiently investigated using epidemic models. More so, in Table 2, empty cells were abound for the

Table 3 WSN epidemic models on virus propagation

Refs.	Model	C	CO	DA	EC	H	MAC	ND	NR	Ro	RIC	STE	SW	TCR	V
[44]	SIR					✓		✓	✓		✓			✓	
[45]	SIR							✓	✓		✓			✓	
[46]	SIR-M							✓	✓		✓			✓	
[47]	SIR							✓	✓	✓	✓				
[48]	SIR							✓	✓		✓			✓	
[49]	SIKS								✓	✓				✓	
[50]	SI							✓					✓	✓	
[51]	SI							✓		✓	✓		✓	✓	
[52]	SI						✓	✓	✓		✓			✓	
[53]	SIS							✓	✓	✓	✓			✓	
[54]	SVEIR								✓	✓		✓			✓
[55]	SIR					✓	✓	✓	✓		✓		✓	✓	
[56]	Dual SIS					✓				✓		✓		✓	
[12]	SIR						✓			✓	✓	✓	✓	✓	
[57]	SISL	✓	✓	✓						✓		✓			
[58]	SIR	✓	✓						✓	✓		✓			

Table 4 WSN epidemic models on botnet propagation

Refs.	Model	BP	EC	ES	FA	MAC	ME	ND	P2PC	TCR
[18]	IOT-SIS	✓	✓					✓	✓	✓
[59]	$B_kBI_kBI_k$					✓		✓		✓
[60]	IoT-SIEF			✓	✓		✓			

following column headings: CO, DA, EC, M, MP and SW. Parameters for heterogeneity and charging of sensor batteries were not even represented using WSN epidemic models of worm propagation. While both charging and heterogeneity can be found in Table 3, plenty of empty cells can be observed for column headings such as CO, DA, EC, MAC, STE, and V. Energy consumption, mobility, node quarantine and mobile patching, etc., were not even part of the table because the virus models did not consider them. Tables 4 and 5 with their little content show that more work needs to be invested in the development of botnet propagation models and representations of concurrent multiple malware infection types. Additionally, in comparison to other tables, these two lack so many salient features and/or parameters. Table 6 has some empty cells for the following column headings; BP, C, CO, DG, EC, SW, and most especially, sensor mobility and vaccination. New studies can emerge by the addition of these absent factors.

5 Findings and Open Areas

The findings and open areas for research generated from the review are presented in this section in accordance to the following popular WSN-related factors; communication graph/topology, epidemic models, stability and simulation, multigroup modeling, vertical/horizontal transmission, communication range and density, patching and protocols.

5.1 Communication Graph/Topology

It was observed that fewer researchers considered communication graphs (CG) in the modeling of malware spread. This might be due to the complexity it introduces in the already complicated formulated mathematical models. Basically, CG include random, small world and scale-free networks. Random graphs were initiated by the pioneering work of

Table 5 WSN epidemic models for multiple malware types

Refs.	Model	Malware Types	CO	ES	ND	NR	Ro	M	STE	TCR	V
[61]	SIS	Virus, worm			✓		✓	✓			
[62]	e-VCjRI	Virus, worm, trojan			✓	✓	✓			✓	✓
[63]	SEjIjR-V	Virus, worm, trojan horse		✓	✓	✓	✓			✓	✓
[64]	SE_1E_2IR	Two worm types		✓		✓	✓		✓		
[65]	SI_1I_2LD	Virus and mutant virus	✓						✓		

Table 6 WSN epidemic models with no particular malware type (MMPT)

Refs.	Model	BP	C	CO	DG	EC	ES	H	M	ND	NR	STE	SW	Ro	TCR	RIC	V
[9]	SIRD								✓		✓				✓		
[66]	SIR, SIS, SIR-S					✓				✓	✓				✓	✓	
[67]	SSIIRRD	✓			✓	✓					✓		✓				
[68]	SIS				✓	✓				✓					✓		
[69]	SEIQRS-V						✓			✓	✓	✓				✓	✓
[70]	SIRD + Markov chains							✓			✓				✓		
[71]	Agent SEIRS-D					✓	✓				✓		✓				
[72]	SEIRD						✓			✓	✓			✓	✓		
[73]	SNIRD							✓			✓	✓		✓			
[74]	HSIRD							✓			✓	✓		✓			
[75]	SITPS		✓	✓						✓					✓	✓	
[76]	SILRD			✓	✓	✓					✓						
[77]	CA SIER						✓				✓	✓		✓		✓	
[78]	SIR			✓		✓			✓		✓	✓			✓		
[79]	Agent SEIRS-F	✓					✓				✓						
[80]	SILSLID		✓	✓	✓									✓			
[81]	SIALS		✓	✓	✓							✓		✓			
[82]	SID			✓	✓	✓									✓	✓	
[83]	SILS-P		✓	✓								✓		✓	✓		
[84]	SISIR				✓			✓		✓	✓	✓		✓	✓	✓	
[85]	SIR_1R_2										✓	✓		✓			

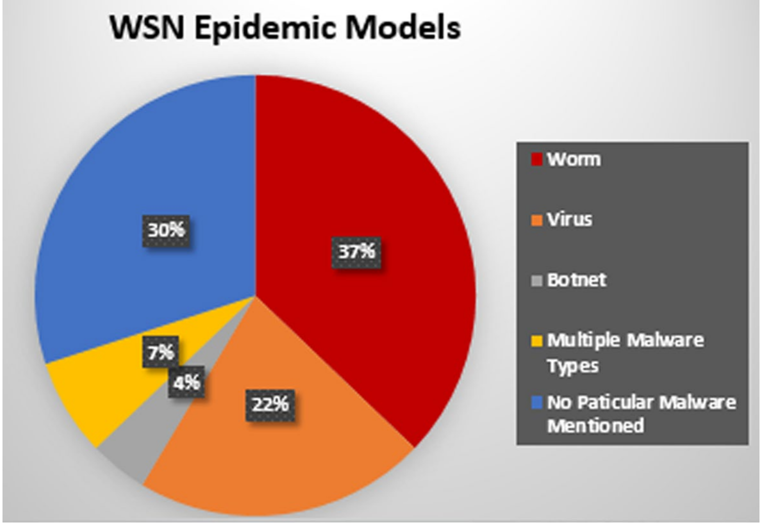


Fig. 3 Percentage distribution for the reviewed epidemic models

Erdős-Renyi (ER) [86] and was employed in the investigation of complex network behaviors. ER theory involves a scenario where n edges arbitrarily chosen are attached to N nodes in such a manner that an equally likely graphical structure emanates from the space, given that N is the network size. Table 7 shows the usage of CGs for WSN epidemic studies. Another concept of connectivity between nodes in the network were evident in some agent models and are shown in Table 8. The hybrid topology used in Ref. [44] is a combination of both star and mesh networks.

5.2 Multigroup Modeling

The convention is to represent one kind of malware spread across a network. However, studies have shown that multiple infection types can exist in a network. Also originating from public health and mathematical biosciences, there is a strong possibility that multiple diseases can concurrently exist in a biological network, and its representation using models is called multigroup modeling (MM). This is certainly so for communication networks such as computers and WSNs. MM has been performed for computer networks, though not exhaustive. Table 5 describes concurrent malware contagions alongside transmission range and density. While Nwokoye et al. [62] considered differential infectivity (DI), Ref. [63] considered both DI and differential exposure (DE). Specifically, DI implies more than one infected compartment whereas DE implies more than one exposed compartment in a given model. In the future, other issues such as node quarantine, mobility, and packet transmission rate can be represented with this concept.

A model by Ojha et al. [64] exhibited the DE concept with one infected class possessing two latent periods (short and long). This work is interesting as it considers a particular malware variant i.e. two types of worms (Cabir and Mabir) with different exposed stages, wherein the incubation time to full infectiousness (I class) are not the same. Therein, (0.476, 0.479 and 0.51) and (0.0026, 0.0028 and 0.003) are the rates

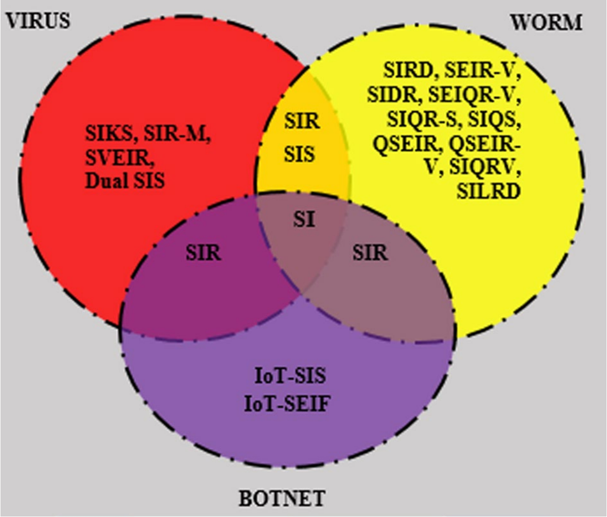

VIRUS
WORM
SIKS, SIR-M, SVEIR, Dual SIS
SIR
SIS
SIRD, SEIR-V, SIDR, SEIQR-V, SIQR-S, SIQS, QSEIR, QSEIR-V, SIQRV, SILRD
SI
SIR
SIR
IoT-SIS
IoT-SEIF
BOTNET

Fig. 4 Venn diagram showing relationships for models I

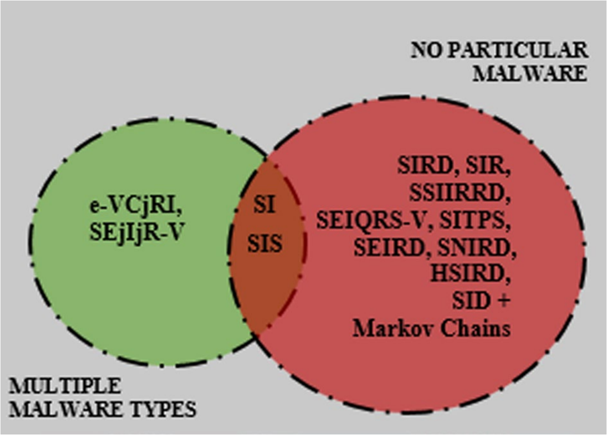

NO PARTICULAR MALWARE
e-VCjRI, SEjIjR-V
SI
SIS
SIRD, SIR, SSIIRRD, SEIQRS-V, SITPS, SEIRD, SNIRD, HSIRD, SID + Markov Chains
MULTIPLE MALWARE TYPES

Fig. 5 Venn diagram showing relationships for models II

for the transition from the E compartments to the I compartment. Additionally, Liu et al. [65] considered mutation of virus, wherein the new mutant is different from the original malware. In a biological network, for instance, the influenza virus undergoes gene-related changes causing antigens to ’drift,’ resulting in a modified virus with a different appearance from the parent viral agent. Vaccines targeting old virus strains and protection from prior influenza virus attacks are no longer effective against the drifted variant as a result of this drifting.

In telecommunication, mutation may imply that the mutant may possess the ability to evade the current immune system or network defense structure of the network. Epidemically, this mutation (a kind of DI) is represented using two sub-compartments; one for the original virus and the other for the mutant.

5.3 Vertical/Horizontal Transmission

Most epidemic models study propagation strategies through horizontal transmissions. In the light of the fact that studies that dealt with both vertical and horizontal worm transmissions are few, however, the model (VLBT-I) in Nwokoye et al. [32] was the only study in this direction. Note that vertical transmission (VT) occurs when a portion of contaminated hosts' offspring (both L and B) are sick at birth and like mature infected hosts, will remain latent before becoming contagious, resulting in the infected birth flux entering the exposed compartment [87]. Put another way, VT can be described as "the birth flux into the exposed class given as pbE + qbL and the birth flux into the susceptible class given as $b - pbE + qbL$" [88].

5.4 Communication Range and Density

While communication range is the range over which a sensor can contact other sensors, density is the measurement of the total population of sensors per unit area. The diagrammatic description of sensor fields (WSN deployment areas) whose expressions aided model analysis is presented in Figs. 6 and 7. Zhang et al. [69] applied the topological expression of range proposed by Feng et al. [25] which is $\pi r^2/L^2$. Other studies that included range in their analyses used the topology proposed by Tang and Mark [46], which is πr^2. Note that density was included as σ, which together with βSI forms either $\beta SI\sigma\pi r^2$ or $\beta SI\sigma\pi r^2/L^2$. This expression is the effective contact rate for successful transmission of the malware infection. The density in WSN was also described by some authors [18] as the total number of nodes divided by the deployment area. However, to generate the number of neighbors, they posited that it is the product of the density and transmission range.

In the light of these topologies, wherein Tang [50] assumed that a sensor node has equal chances per time for effective contact, Wang et al. [16] argued that models developed with these circular or rectangular network boundary, presents unrealistic assumptions and may possess poor scalability. Additionally, with the sensing range—a spatial parameter, Shakya [55] added a spatial correlation between sensor nodes which is the portion of overlapping sensing area of rs-radius disc nodes centered at their own location. With the works arising from [26, 30–33, 39, 40] etc., it is commendable to represent WSN infection scenarios without density and range, as seen in works by Prof. Bimal Mishra [7, 23].

Reference [3] asserted that the sensor node's communication range is constrained, both technically and due to the need to save energy. The exact range a particular transmission signal strength may reach is determined by a variety of environmental changes like weather and topography. This assertion about environmental factors was not included in expressions of range in WSN. Additionally, Priyadarshi et al. [1] distinguished between communication and sensing range (Fig. 8) and the latter means the largest distance between a node and a location within a specified FoI at which a sensor node may detect any event that occurs. Most reviewed models dealt with the former, therefore, an interesting work might arise from x-raying the impact of the sensing range or both range types (as it was done in Shakya [55]) alongside other WSN features or epidemic scenarios.

On the other hand, by analyzing the patterns of communication/transmission described in the reviewed models, one can easily decipher that the authors significantly assume that multi-hop network types correctly and always transmit received information. Interestingly, Wang et al. [9] considered packet transmission rate, thus confirming this assertion. This is not entirely true because there exists a tool named Sympathy, which identifies failures

Table 7 Usage of CGs in WSN epidemic studies

Refs.	Scale-free	Random	Small-world	Spatial	2D Lattice
[20]		✓			✓
[44]		✓		✓	
[46]		✓			
[47, 48]		✓		✓	
[49]	✓		✓		✓
[52]		✓			
[70]	✓				
[71]	✓		✓		
[73, 74]	✓				
[75]				✓	
[79]		✓			

Table 8 Usage of network topologies in WSN

Refs.	Star	Mesh	Hybrid
[20]	✓		
[44]	✓	✓	✓

found in the node itself, the path of communication or in the base station failure. Failures in the reviewed models, on the other hand, are denoted as death due to software or hardware failure [7, 23, 30–33, 35, 39], leaving the last two, path and sink failure, unattended. While path failure may not easily be incorporated into SI-based models, sink failure was represented in studies [56, 70] that involved some form of heterogeneity, i.e., modeling normal sensors, base stations, and CH [44, 84]. WSN description in these terms are depicted as Fig. 9 [90]. While Ref. [56] involved two sensor types, normal sensors and the base station, Ref. [71] implemented three by including CH/routers. From the reviewed models, other instances of heterogeneity observed were for communication connectivity [73, 74].

5.5 Patching

Patching or eliminating the malicious codes using anti-malware is the most common method of recovery, which is depicted in Tables 2, 3 and 5 as NR. Generally, this results in a situation referred to as "multi-epidemical decay"-a condition in which infections are unable to overwhelm the entire network and, as a result, die out. The sustained survivability of a network (whether it be a traditional computer network or a WSN) depends on how fast hosts (sensor nodes) recover from any malware attack or infection. Conversely, if a network is not quickly remediated, then it may suffer downtime, which may amount to losses, damage, and disruptions. In WSN, actuators have proven to possess the ability of improving the performance of the network, aiding collection of data and supplementing the limited sensor battery power [16]. However, it was discovered that even with the immense benefits of an actuator in a WSN, experiments have shown that a malicious attacker can successfully exploit it, making it a mobile worm carrier, thereby, speeding up the worm spread process.

From the reviewed papers, mobile actuators were only implemented in this study [16], while a novel concept of worm elimination was conceived by Ref. [29]. Therein, whenever an infection begins to propagate, it is discovered that after a specific length of time, a virtual patch is created. This patch is then inserted into the network, much like an updated firmware, and replicates like a worm, albeit at a slower rate.

Ensuring a malware-free network may also include immunisation (random or targeted) [9], vaccination/inoculation [7, 23, 26, 30, 31, 33, 35, 37–40, 54] and/or quarantine (i.e. the isolation of infected hosts for later treatment). Pre-quarantine [30]/Network Access Control [33] and pre-vaccination [37] have also been contemplated; while the former implies nodes passing through a pre-screening process, where infectious immigrant nodes are isolated, treated, and sent to the remediated compartment, the latter depicts the pre-inoculation of nodes in order to extremely reduce their vulnerability to worm attack. Vaccination was considered in a different light using the SIR_1R_2 model [85], where there are two recovered compartments. While the first one is for sensors' basic recovery, the second is for the sensor's complete recovery. The implication is that at first, sensors are cleansed of malicious objects, and they acquire the fundamental capacity to resist malware, but there is still the possibility of being infected again. At the second R compartment, the sensors become more resistant to malware following contamination and complete recovery.

UAV [76] was used to distribute virtual vaccines to infected nodes. This is referred to as mobile patching [16, 41]. Another way of ensuring a virus-free WSN using a maintenance mechanism was conceived by the SIR-M model [46]. Here, the proposed model can flexibly adapt to any viral variant with less computational burden on hardware.

The recovered class of the IoT-SEIF model for botnets were modified to a Forensic compartment, which may reduce the amount of secondary bots created during infectious peak value and peak period of botnet dissemination [60]. More explanation was provided by the authors and it goes thus; nodes having enough memory to spread an assault are prioritized by the control command, whereas nodes with limited memory capacities are abandoned. However, in order to prevent botnet growth, nodes of significant interest to the botmaster's command structure will be recognized as forensic items and transferred to the forensic compartment. As a result, the rate of spread may be decreased, which could also reduce botnet development. Memory issues have also been ignored in epidemiological WSN studies; this should not be so because it is also a crucial part of the sensor node architecture, which holds both instruction set and sensed data.

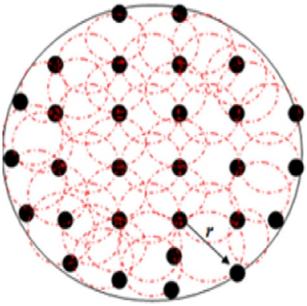
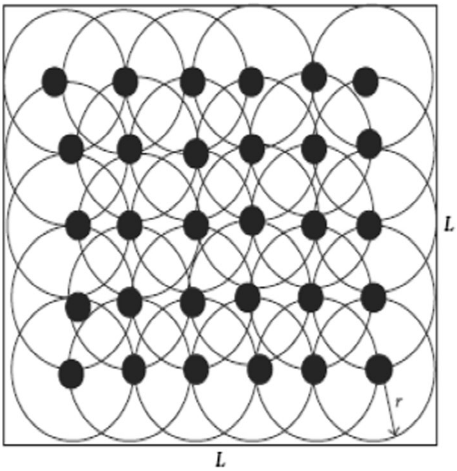


Fig. 6 WSN topology I [46]

Fig. 7 WSN topology II [25]



5.6 Protocols

The WSN protocol stack layers are physical, data link, network, transport, and application [5]. Several studies [20, 45] have treated protocol layers (physical, data link, and network) and multi-hop broadcast protocols (MBPs) such as Trickle, Deluge, and MNP [45]. De et al. [48] added Firecracker to the list of MBPs. On information dissemination strategies, Anagnostopoulos et al. [49] implemented their model for uniform gossip and flooding schemes. Most WSN models have ignored protocols and information transmission schemes in their analyses. Note that the former is missing parameters for transport and application layers. Using the SEIRS-D agent model [71], the following common WSN protocols were implemented: self-organizing and energy efficient clustering and routing protocols.

There are other important protocols whose parameters are yet to be sufficiently investigated using WSN epidemic models. For instance, the key management protocols and secure routing protocols. Reference [91] described some classifications of coverage protocols (CP), i.e. coverage aware deployment, sleep scheduling for flat networks, and cluster-based

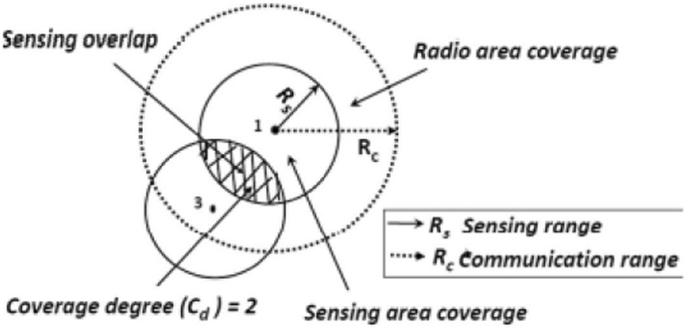


Fig. 8 Sensing and communication range of node [89]

sleep scheduling, while security protocols involve decentralized key-exchange [44, 92] and location-aware key (LKE) establishment [93]. References [47, 48] modeled the pairwise key scheme (PKS), which is the fourth phase of the LKE establishment protocol. Here, two sensor nodes share a common key dependent on their location details. Therefore, communication is possible with this key. The first three phases include pre-distribution, node self-configuration, and the polynomial share-distribution phase. It is worth noting that PKS was last seen in WSN epidemic modeling in 2009 in the works cited above.

5.7 Sensor Mobility

Valler et al. [61] represented several periodic mobility models, namely: random walk, levy flight, and random waypoint. Reference [9] also involved node mobility in their model. Contrary to these approaches, Kumari and Upadhyay [78] implemented sensor mobility using reaction–diffusion modeling. Aside from these studies, no other model involved mobility. The change in position of sensor nodes may be as a result of the objective of the WSN. Actually, node mobility improves the network performance with a degree of flexibility, which allows FoI monitoring at different times, thereby, increasing quality of service [1]. The aforementioned studies can be extended by conceiving FoI obstacles in the expressions of the mobility models, tackling the issue of path planning and factors such as wind disturbances etc.

5.8 Power/Energy

Since battery is the major source of power, its consumption is a very vital factor when forming a WSN, and care is taken to reduce its depletion per node. If energy is conserved efficiently, the amount of wasted bandwidth may ultimately be reduced [66]. WSN activities such as sensor action, receiving, transmitting, and processing data are the main sources of energy reduction. Put differently, dissipated energy is for transducers, for communication among sensor nodes and for microprocessor computation. In order to conserve energy and prolong the network lifetime, several researchers have considered sleep/work scheduling modes for sensors in WSN using the following epidemic models; SIRD [22], SIR-M [46], SI [50] and SSIIRRD [67]. Note that due to the intervals of sleep and work, only a neighboring working sensor can be infected by malicious code on another working sensor,

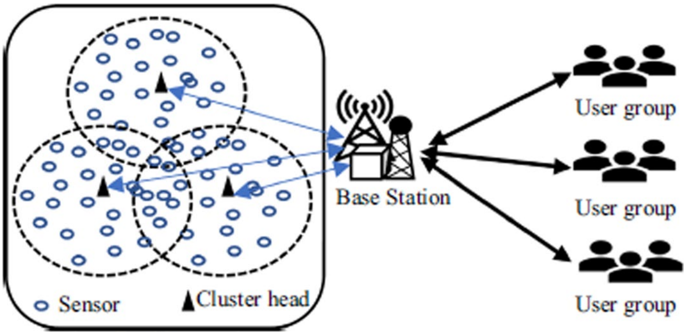


Fig. 9 Wireless sensor network [90]

while a sleeping node in the transmission range remains uninfected. In these works [12, 55, 71], this sleep/work interleaving policy was referred to as the duty cycle, which has two modes (active and inactive): time the node collects environmental data or sends data, and time the node falls asleep or awakens.

The sensor life time was elongated using batteries in the agent model developed by Xu [79], while the battery power was calibrated as low, medium and high. Additionally, at the continual exhaustion of node energy, more sensors disappear, i.e. become dead and do not participate in malware propagation. From the tables, the following models represented energy consumption; SIS [68], SSIIRRD [67] and SILRD [41, 76]. The last three studies employed the differential game (DG) approach, which is known for its benefits in modeling dynamical and complex problems. It has been applied to WSN studies [67, 76, 80, 81]. Basically, DG is played by several individuals in a continuous time system, which allows them to optimize their respective objectives in order to attain the most favorable and advantageous time-related game plan/policy.

Realistically, the depletion of power is a concept that requires a continual charging process aimed at elongating the WSN lifetime. Although most epidemic WSN models ignore this important factor, recently, rechargeable WSNs (WRSNs) have started to appear in the literature. In WRSN, energy exhaustion has been classified as a special attack, i.e., denial of charge (DOC), which has necessitated the inclusion of a compartment known as "low energy" (L). Considering the basic SIR model, the charging process essentially means the transition from the L class to the S class for conceptions where only one L compartment exists [57]. Some authors have discussed the possibility of separate L compartments for S, I, and R classes, but during charging, the low-energy infected nodes (LI) [58] are ignored so as to ensure more effective malicious-code containment in the WSN. Sensors of L status can be charged using mobile chargers (MC) as considered by Guiyun et al. [41] to elongate sensor battery life. On the other hand, high energy nodes are those that transition from vulnerable and diseased states to recovered states and do not require mobile charging. Beyond having just low and high energy sensor nodes, EC was implemented for an additional energy state (medium) in Xu [79] and 3 additional energy states (very low, medium and very high) in Batista et al. [71]. Several charging approaches (pulse, continuous and-charging) were compared by Liu et al. [83]. In order to enhance significant energy savings, many MAC protocols have been created and explored [94] using these two epidemic models [52, 55].

EH-WSN concepts, which involve incorporating energy collectors into a sensor node to reduce the effect of a power outage on the WSN's lifetime, have also been conceptualized using epidemic models. Specifically, the SILRD model [76] was developed with solar energy in mind. In a single day, there are 2 time periods without sunshine. The first period is from 0 to 5 a.m., and the second is from 8 p.m. to 12 a.m. Solar energy collectors turn off during these two times, and sensors may become unresponsive as a result of the loss of electric power. Aside from this epidemic study on solar power, other energy sources such as wind, vibration, thermal, ocean waves, nuclear reaction, etc., are yet to be represented and used for analysis. More so, judging from a recent survey on energy management [95], WSN modelers are yet to exhaust schemes (Fig. 10) therein. However, it is obvious that the aforementioned models in this subsection have not considered the latent period/exposed stage for sensors. Therefore, the constrained battery power of other listed models above can be considered by researchers in future studies, alongside latent period and factors such as protocol layers, packet transmission rate etc.

5.9 Optimal Control/Cost

The cost of a given strategy has been investigated using the optimal control approach, which identifies the control law for a complex dynamical system. Therein, the Pontryagin Minimum Principle (PMP) was used to attain a low infection degree at a low cost [75]. PMP was applied using the game approach in Guiyin et al. [41], wherein it was discovered that charging can be a defense approach that hinders malicious-code spread, thus reducing cost. Evaluating cost is absolutely necessary because by disrupting the transmission framework between nodes, contaminated nodes waste a lot of their own energy and incur a given cost. Furthermore, eavesdropping on WSNs through such sensors results in unanticipated losses. Specifically, several types of costs can be evaluated:

- Refs. [41, 53]: costs in terms of any extra hardware effort, as well as any added computing or signaling expense. Note that the optimal control or cost analysis for computing/signaling burden was not considered in this study.
- Ref. [75]: aggregate cost of tracking malware, generating new patches and upgrades, and forwarding the fixes to sensor nodes.
- Refs. [65, 78]: the costs of virus elimination and charging L sensor nodes.
- Ref. [76]: total costs for running network anti-malicious program, sensor deployment (manufacturing and human), patch distribution to the S and I classes, energy collection, conversion, and recharging.
- Refs. [84]: total cost of an infected node's cyberattack, of fixing an infected node, and of vulnerable nodes' security detection on incoming data packets.

5.10 Stability, Delay Analysis and Simulation

It was discovered that most of the models pursued the derivation of the reproduction ratio (Ro)/epidemic threshold and the stability analyses at both the endemic (EE) and malware free equilibrium (MFE) points. The epidemic threshold is defined as the expected number of secondary infections produced by one infected computer node in completely susceptible nodes and can be derived using the next generation matrix (NGM) method [54, 73, 74, 80, 81, 85]. The NGM approach, alongside the Floquet theorem, was used to evaluate the stability of periodic solutions [83].

There is the general assumption that the ability to build resilient networks is aided by the presence of stability conditions. The stability study of equilibrium points helps forecast whether malware spread on the network will disappear or continue over time. As a result, the entire network can be protected against malware assaults by understanding the notion of stability. Analyses are mostly performed to ascertain both the local and global asymptotic stability (GAS) for EE and MFE. Using a linearization technique that involves construction of a Jacobian matrix (JM) [54] and deriving the characteristic equation aids the local asymptotic stability, whereas the Lyapunov theorem [80, 81] alongside LaSalle's invariance principle are used for checking GAS [54]. The Routh-Hurwitz (RH) criterion has been used to assess the stability of EE [78]. In a particular study [77], only one equilibrium point was checked for stability using the JM method, and the LAS and GAS of equilibria were proven with the use of a technique involving the RH and Bendixson-Dulac criteria [81]. From Table 4, one can observe that stability analysis has not been performed for epidemic models on botnet propagation; this may interest mathematics enthusiasts. Table 9 presents the type of stability analyses performed in the reviewed epidemic models in the study.

The choice of the extent of stability analyses to be performed in a particular paper is not defined, although it seems to be dependent on the mathematical knowledge of the authors. Researchers from the mathematics field seemingly perform more mathematical analysis than their counterparts in other related disciplines. Beyond stability analyses, some go as far as performing delay analyses so as to determine bifurcation (Hopf) and persistence [83] for the proposed model. Hopf bifurcation [43, 58, 69, 78, 82] was explored by applying the normal form theory and the center manifold theorem. In addition, it can be inferred from the surveyed articles that the proposed system of differential equations are solved using the Runge–Kutta-Fehlberg order 4 and 5 method [7, 23, 26, 30, 32 etc.]. Numerical simulation experiments gotten from solving the system of equations are used to assess efficacy and to provide awareness of the effect of malicious objects' propagation under various conditions.

5.11 Other Issues

On node deployment scenarios, De et al. [47, 48] considered two types of scenarios, namely uniform and group-based. Most models reviewed above refer to sensor deployment using the following nomenclatures; node addition, node inclusion or recruitment of new nodes. For instance, the parameter for deployment of sensors has been denoted as A [16, 27, 37], b [40] or μ [39] etc. Senouci and Mellouk [96] noted that the deterministic or random deployment of nodes depends on the sensor type, application and the environment of operation. Most epidemic models assume a uniform random distribution format without considering deployment constraints, which include coverage, cost, energy, data fidelity, fault tolerance, network connectivity, and lifetime.

Some have argued that incorporating an authentication scheme can hugely reduce worm attack capabilities. It guarantees that connectivity and exchange of information between nodes is authentic, thereby ensuring that a hostile node cannot impersonate a trustworthy network node. As Gautam and Kumar [90] put it, authentication strategies provide benefits for WSNs. They include reduced load for work and data,

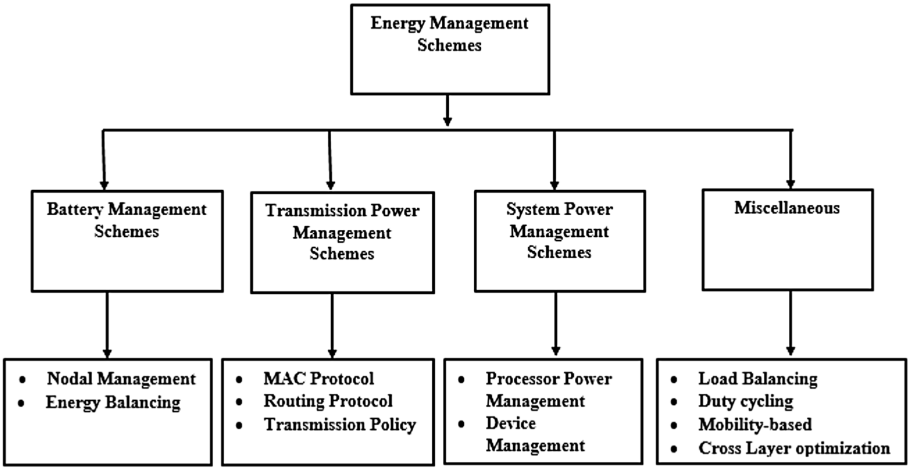

Energy Management Schemes
Battery Management Schemes
Transmission Power Management Schemes
System Power Management Schemes
Miscellaneous
• Nodal Management
• Energy Balancing
• MAC Protocol
• Routing Protocol
• Transmission Policy
• Processor Power Management
• Device Management
• Load Balancing
• Duty cycling
• Mobility-based
• Cross Layer optimization

Fig. 10 Energy management schemes [95]

reduced energy/power dissipation, robust security, and effective utilization of resources like memory and bandwidth. Interestingly, these authors [16] employed Subha's authentication mechanism, which consists of three algorithms: key generation algorithm, signature algorithm, and verification. With the exception of this work, reviewed models are yet to sufficiently represent authentication using SI-based epidemic models.

The force of infection, which is the rate at which vulnerable nodes in a WSN population contract a malware infection measured in units of time, is significantly of interest during modeling. This is also called the incidence rate. In fact, various WSN epidemic studies have been conducted by some researchers using incidence rates such as mass action/bilinear (βSI) [42, 43, 52, 57, 64, 65, 69, 82], standard incidence (βSI/N) [45, 48, 50, 51, 58, 84], and nonlinear incidence [βSI/f (I)] [54, 78]. The Holling type II function [54] is a form of non-linear incidence rate. Note that Ref. [27] utilized the point to group infection mode in WSNs in their work.

On theoretical analysis/experimental results, it was discovered that most of the models favor theoretical analyses instead of real world experiments with actual WSN data. Tang et al. [16] compared theoretical results with datasets from the actual WSN environment, while these authors [59] used actual Mirai botnet data for their studies. This is uncommon in most reviewed models since they are filled with theoretical analyses and numerical simulations. However, abstractions and model representations should be experimented on with prominent WSN standards such as IEEE 802.15.4, ZigBee, WirelessHART, ISA100.11, IETF 6LoWPAN, IEEE 802.15.3 and Wibree using testbeds (Open access research testbed for next-generation wireless networks, MoteLab and Emulab).

The concept of reliability is of great concern in WSNs, but it hasn't been sufficiently or thoroughly studied alongside the impact of malware propagation. Although Shen et al. [67] investigated reliability using an SI-based game model, considering Fig. 11, it is obvious that more studies should be performed in this direction. Reliability denotes the likelihood that sensors would continue to execute activities like data imaging, transfer, and integration for a given length of time within specified scenarios and it was evaluated using two measures, which are standard methods for assessing the dependability of devices as well as other technological innovations. These measures are Mean Time to Failure (MTTF) and Mean Time between Failures (MTBF); while MTTF represents the amount of time that a gadget is anticipated to work for, MTBF implies the average duration between a gadget's operational failures.

Cyber threats always aim at disrupting the afore-mentioned security services and the reviewed models are yet to entirely address them. More attempts are required in this regard. Of course, to some extent, this highlights the limitations of the SI-based differential equation model. Therefore, agent-based models (ABM) [35, 71] and cellular automata (CA) [77] have been proposed as ways of adding more heterogonous and spatial factors.

For instance, although Batista et al. [71]'s agent model may seem deficient when considered against some of the parameters of traditional SI epidemic, it represented several phenomena including computing capability, security level, data gathering methods, and human behaviors are all factors to consider. These issues are not easily represented using the conventional SI model. Propagation techniques (self-replication, exploitation, and user involvement) and target categories (malware dissemination and data exfiltration were also considered in Batista et al. [71]. To this list, Xu [79] added reliability (in terms of gathering, communication, and computing), maintenance and target types that involved software functions, hardware subsystems, and battery power. Of course, mathematical analyses such as stability at equilibrium points are not totally significant in agent modeling, as it is clear

Table 9 Stability analyses in reviewed models

Refs.	LAS for MFE	LAS for EE	GAS for MFE	GAS for EE
[54, 57, 65, 78, 81, 84, 85]	✓	✓	✓	✓
[69]		✓		
[56, 83]	✓		✓	
[58, 64]	✓	✓		

that agent models do not include such exercises. ABM alongside CA models constitute the individual-based modeling paradigm, which allows for more complex representations of heterogeneity, stochasticity and availability for WSN as well as attendant critical epidemic scenarios. Agent development toolkits used for implementation are Netlogo [35, 79], which runs on Java virtual machine, and the Mesa framework [71], which runs on an Apache2 server. Additionally, numerical simulations in the SID model [82] were performed with CA in Netlogo.

Beside terrestrial WSN wherein most mathematical models have dwelt for a long time, other WSN types include underground [98], underwater [99], and multi-media [100] WSNs. In light of this, most of the models reviewed above represent terrestrial WSNs. However, models representing the remaining types are yet to be conceived. For instance, contemplating underground WSN, where sensors are buried beneath the ground, in mines/caves; malware propagation using SI-based models would present an interesting dimension if one considers obstructions that may arise due to the soil, rocks, water, mineral contents and the profound difficulty attendant to charging or replacing a battery. For underwater WSN [99], SI-based representations may include limited bandwidth, long propagation delay, signal fading issues, and the harsh ocean environment while considering WSN security requirements: availability, authorization, authentication, confidentiality, integrity, nonrepudiation, freshness, self-organization, time synchronization, secure localization, accountability, and survivability [90]. Finally, although it seems like mathematical modeling of WSN may be the answer to understanding epidemics in WSN, it is advised that the modeler should thoroughly understand a significant phenomenon before employing it.

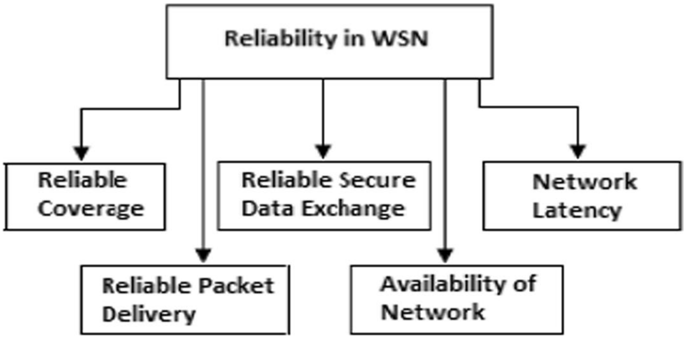


Fig. 11 Categories of reliability in WSN [97]

6 Conclusion

In this study, SI-based models developed for epidemics in WSNs were reviewed. This is immensely essential, if one considers the uses of WSN in agriculture (for precision farming), battlefield monitoring and in the health industry. This review is very necessary because it provides requisite information for newbies and graduate researchers, who are interested in WSN epidemiology. Unlike the study in [11], our paper provided lessons and elicited open areas based on the following; communication graph/topology, epidemic models, stability and simulation, multigroup modeling, vertical/horizontal transmission, communication range and density, patching and protocols. Others include sensor mobility, authentication mechanism, power/energy, theoretical analysis/experimental results and WSN types. Furthermore, work is currently ongoing in order to generate a review of epidemic models on computer networks and peer to peer networks. In the future, WSN alongside deep learning approaches [101] for epidemic predictions will be x-rayed. It is noteworthy that epidemic models have yet to be used for modeling some WSN attacks reviewed by Rehman et al. [102]; representing them will also be done in the future.

Author Contributions CHN had the idea for the article. CHN and VM performed the literature search and data analysis. CHN and VM drafted the work. CHN and VM critically revised the work.

Funding The authors did not receive support from any organization for the submitted work.

Data Availability Not Applicable.

Code Availability Not Applicable.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Priyadarshi, R., Gupta, B., & Anurag, A. (2020). Deployment techniques in wireless sensor networks: A survey, classification, challenges, and future research issues. *The Journal of Supercomputing*. https://doi.org/10.1007/s11227-020-03166-5
2. Rashid, B., & Rehmani, M. H. (2016). Applications of wireless sensor networks for urban areas: A survey. *The Journal of Network and Computer Applications, 60*, 192–219.
3. Mishra, A., Shukla, S., Singh, A. K., & Gupta, A. (2020). DTSS and clustering for energy conservation in wireless sensor network. *Advances in Intelligent systems and computing*, *1125*, 43-50. https://doi.org/10.1007/978-981-15-2780-7_6
4. Lopez-Ardao, J. C., Rodríguez-Rubio, R. F., Suárez-González, A., Rodríguez-Pérez, M., & Sousa-Vieira, M. E. (2021). Current trends on green wireless sensor networks. *Sensors, 21*(4281), 1–34.
5. Adu-Manu, K. S., Adam, N., Tapparello, C., Ayatollahi, H., & Heinzelman, W. (2018). Energy-harvesting wireless sensor networks (EH-WSNs): A review. *ACM Transactions on Sensor Networks, 14*(2), 1–50.
6. Kanoun, O., Bradai, S., Khriji, S., Bouattour, G., El Houssaini, D., Ben Ammar, M., Naifar, S., Bouhamed, A., Derbel, F., & Viehweger, C. (2021). Energy-aware system design for autonomous wireless sensor nodes: A comprehensive review. *Sensors, 21*(548), 1–25.

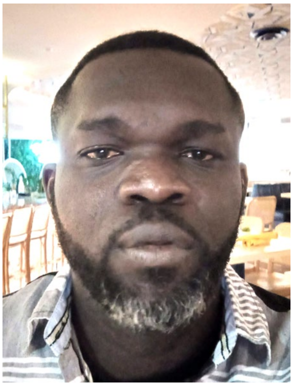
7. Mishra, B. K., & Tyagi, I. (2014). “Defending against malicious threats in wireless sensor network: A mathematical model. *International Joural of Information Technology and Computer Science, 3*(4), 12–19.
8. Rajaram, V., & Kumaratharan, N. (2021). Multi-hop optimized routing algorithm and load balanced fuzzy clustering in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing, 12*, 4281–4289.
9. Wang, X., He, Z., Zhao, X., Lin, C., Pan, Y., & Cai, Z. (2013). Reaction-diffusion modeling of malware propagation in mobile wireless sensor networks. *Science China Information Sciences, 56*, 2013.
10. Avram, F., Adenane, R., & Ketcheson, D. I. (2021). A review of matrix SIR arino epidemic models. *Mathematics, 9*(1513), 1–14.
11. Srinivas, M. N., Madhusudanan, V., Murty, A. V. S., & Bapu, B. R. T. (2021). A review article on wireless sensor networks in view of e-epidemic models. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-021-08436-w
12. Jiang, L., Xu, Q., Pan, H., Dai, Y., & Tong, J. (2020). Virus propagation in wireless sensor networks with media access control mechanism. *Security and Communication Networks, 6513920*, 1–11.
13. Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2017). A framework for cyber-topology attacks: Line-switching and new attack scenarios. *IEEE Transactions on Smart Grid, 10*(2), 1704–1712.
14. Goel, D., & Jain, A. K. (2017). Mobile phishing attacks and defense mechanisms: State of art and open research challenges. *Computers & Security, 73*, 519–544.
15. Kak, A. (2021). *Malware: Viruses and worms, lecture notes on computer and network security*. Purdue University.
16. Wang, T., Wu, Q., Wen, S., Cai, Y., Tian, H., Chen, Y., & Wang, B. (2017). Propagation modeling and defending of a mobile sensor worm in wireless sensor and actuator networks. *Sensors*. https://doi.org/10.3390/s17010139
17. Jalalitabar, M., Valero, M., & Bourgeois, A. G. (2015). Demonstrating the threat of hardware Trojans in wireless sensor networks. In 24th international conference on computer communication and networks, pp. 1-8. https://doi.org/10.1109/ICCCN.2015.7288392
18. Acarali, D., Rajarajan, M., Komninos, N., & Zarpelão, B. B. (2019). Modelling the spread of botnet malware in IoT-based wireless sensor networks. *Security and Communication Networks*. https://doi.org/10.1155/2019/3745619
19. Trend Micro Incorporated. (2019). Into the battlefield: A security guide to IoT Botnets. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/into-the-battlefield-a-security-guide-to-iot-botnets
20. Khayam, S. A., & Radha, H. (2005). A topologically-aware worm propagation model for wireless sensor networks. In *2nd Int’l workshop on security in distributed computing systems*, USA.
21. Xiaoming, W., & Yingshu, L. (2009). An improved SIR model for analyzing the dynamics of worm propagation in wireless sensor networks. *Chinese Journal of Electronics, 18*(1), 8–12.
22. Wang, X., Li, Q., & Li, Y. (2010). EiSIRS: A formal model to analyze the dynamics of worm propagation in wireless sensor networks. *Journal of Combinatorial Optimization, 20*, 47–62.
23. Mishra, B. K., & Keshri, N. (2013). Mathematical model on the transmission of worms in wireless sensor network. *Applied Mathematical Modeling, 37*, 4103–4111.
24. Mishra, B. K., Srivastava, S. K., & Mishra, B. K. (2014). A quarantine model on the spreading behavior of worms in wireless sensor network. *Transaction on IoT and Cloud Computing, 2*, 1–12.
25. Feng, L., Song, L., Zhao, Q., & Wang, H. (2015). H, “Modeling and stability analysis of worm propagation in wireless sensor network.” *Mathematical Problems in Engineering, 129*, 1–8.
26. Nwokoye, C. H., Ejiofor, V. E., Orji, R., & Umeh, I. (2016). Investigating the effect of uniform random distribution of nodes in wireless sensor networks using an epidemic worm model. In Proceedings of the CORI’16, Ibadan, Nigeria, pp. 58–63. http://ceur-ws.org/Vol-1755/
27. Khanh, N. H. (2016). Dynamics of a worm propagation model with quarantine in wireless sensor networks. *Applied Mathematics & Information Sciences, 10*, 1739–1746.
28. Srivastava, A. P., Awasthi, S., Ojha, R. P., Srivastava, P. K., & Katiyar, S. (2016). Stability analysis of SIDR model for worm propagation in wireless sensor network. *Indian Journal of Science and Technology, 9*, 1–5.
29. 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 Information Forensics and Security, 11*, 2854–2865.

30. Nwokoye, C. H., Ejiofor, V. E., & Ozoegwu, C. G. (2017). Pre-Quarantine approach for defense against propagation of malicious objects in networks. *International Journal of Computer Network and Information Security, 9*, 43–52.
31. Nwokoye, C. H., & Umeh, I. (2017). The SEIQR–V model: On a more accurate analytical characterization of malicious threat defense. *International Journal of Information Technology and Computer Science, 12*, 28–37.
32. Nwokoye, C. H., Ejiofor, V. E., Onyesolu, M., & Ekechukwu, B. (2017). Towards modeling malicious agents in decentralized wireless sensor networks: A case of vertical worm transmissions and containment. *International Journal of Computer Networks and Information Security, 9*, 12–21.
33. Nwokoye, C. H., Mbeledogu, N., Umeh, I. I., & Ejimofor, A. (2017). Modeling the effect of network access control and sensor random distribution on worm propagation. *International Journal of Modern Education and Computer Science, 11*, 49–57.
34. Ojha, R. P., Sanyal, G., Srivastava, P. K., & Sharma, K. (2017). Design and analysis of modified SIQRS model for performance study of wireless sensor network. *Scalable Computing, 18*, 229–241.
35. Nwokoye, C. H., & Umeh, I. (2018). Analytic-agent cyber dynamical systems analysis and design methodology for modeling temporal/spatial factors of malware propagation in wireless sensor networks. *Methodx*. https://doi.org/10.1016/j.mex.2018.10.005
36. Srivastava, P. K., Ojha, R. P., Sharma, K., Awasthi, S., & Sanyal, G. (2018). Effect of quarantine and recovery on infectious nodes in wireless sensor network. *International Journal of Sensors, Wireless Communications and Control, 8*, 26–36.
37. Srivastava, P. K., Ojha, R. P., & Sanyal, G. (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, 9*, 1–23.
38. 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*, 2535–2551.
39. Ojha, R. P., Sharma, K., Srivastava, P. K., & Sanyal, G. (2019). An epidemic model for security and performance of wireless sensor networks. *International Journal of Advanced Intelligence Paradigms*. https://doi.org/10.1504/IJAIP.2019.099947
40. Ojha, R. P., Srivastava, P. K., Sanyal, G., & Gupta, N. (2020). Improved model for the stability analysis of wireless sensor network against malware attacks. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-020-07809-x
41. Guiyun, L., Baihao, P., Xiaojing, Z., & Xuejing, L. (2020). Differential games of rechargeable wireless sensor networks against malicious programs based on SILRD propagation model. *Complexity*. https://doi.org/10.1155/2020/5686413
42. Zhang, Z., & Si, F. (2014). Dynamics of a delayed SEIRS-V model on the transmission of worms in a wireless sensor network. *Advances in Difference Equations*. https://doi.org/10.1186/1687-1847-2014-295
43. Zhang, Z., & Wang, Y. (2017). Bifurcation analysis for an SEIRS-V model with delays on the transmission of worms in a wireless sensor network. *Mathematical Problems in Engineering*. https://doi.org/10.1155/2017/9898726
44. De, P., Liu, Y., & Das, S. K. (2006). Modeling node compromise spread in wireless sensor networks using epidemic theory. In International symposium on a world of wireless, mobile and multimedia networks, USA, pp. 237–243. https://doi.org/10.1109/WOWMOM.2006.74
45. De, P., Liu, Y., & Das, S. K. (2007). An epidemic theoretic framework for evaluating broadcast protocols in wireless sensor networks. In *Conference on mobile adhoc and sensor systems*, Pisa, Italy.
46. Tang, S., & Mark, B. L. (2009) Analysis of virus spread in wireless sensor networks: An epidemic model. In *7th international workshop on the design of reliable communication networks, Washington, USA*.
47. De, P., Liu, Y., & Das, S. K. (2009). Deployment aware modeling of node compromise spread in wireless sensor networks. *IEEE Transaction in Sensor Network, 5*, 23–35.
48. De, P., Liu, Y., & Das, S. K. (2009). An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks. *IEEE Transactions in Mobile Computing, 6*, 413–425.
49. Anagnostopoulos, C., Hadjiefthymiades, S., & Zervas, E. (2011). An analytical model for multi-epidemic information dissemination. *Journal of Parallel and Distributed Computing, 71*, 87–104.
50. Tang, S. S. (2011). A modified SI epidemic model for combating virus spread in wireless sensor networks. *International Journal of Wireless Information Networks, 18*, 319–338.
51. Tang, S., & Li, W. (2011). An epidemic model with adaptive virus spread control for wireless sensor networks. *International Journal of Security and Networks, 6*, 201–210.

52. Wang, Y. Q., & Yang, X. Y. (2013). Virus spreading in wireless sensor networks with a medium access control mechanism. *Chinese Physics B, 22*, 1–5.
53. Tang, S., Myers, D., & Yuan, J. (2013). Modified SIS epidemic model for analysis of virus spread in wireless sensor networks. *International Journal of Wireless and Mobile Computing, 6*(2), 34–45.
54. Upadhyay, R. K., Kumari, S., & Misra, A. K. (2017). Modeling the virus dynamics in computer network with SVEIR model and nonlinear incident rate. *Journal of Applied Mathematics and Computing, 54*, 485–509.
55. Shakya, R. K. (2018) Modified SI epidemic model for combating virus spread in spatially correlated wireless sensor networks, pp. 1–12. arXiv:1801.04744
56. Tang, S., & Tang, C. (2018). A dual SIS epidemic model for virus spread analysis in cluster-based wireless sensor networks. *Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering*, *251*, 652–662. https://doi.org/10.1007/978-3-030-00557-3_65
57. Liu, G., Li, J., Liang, Z., & Peng, Z. (2021). Analysis of time-delay epidemic model in rechargeable wireless sensor networks. *Mathematics, 9*, 1–19.
58. Liu, G., Li, J., Liang, Z., & Peng, Z. (2021). Dynamical behavior analysis of a time-delay SIRS-L model in rechargeable wireless sensor networks. *Mathematics, 9*, 1–21.
59. Ji, Y., Yao, L., Liu, S., Yao, H., Ye, Q., & Wang, R. (2018). The study on the botnet and its prevention policies in the internet of things. In *Proceedings of the IEEE 22nd international conference on computer supported cooperative work in design* (pp. 837–842). IEEE.
60. Ibrahim, M., Abdullah, M. T., Abdullah, A., & Perumal, T. (2019). Modelling and mitigation strategy of IoT botnet propagation. *Preprints*. https://doi.org/10.20944/preprints201912.0097.v1
61. Nicholas, C., Prakash, B. A., Tong, H. H., & Faloutsos, M. (2011). Epidemic spread in mobile ad hoc networks: Determining the tipping point. In 10th international IFIP TC 6 networking conference, Spain, 6640, 266-280. https://doi.org/10.1007/978-3-642-20757-0_21
62. Nwokoye, C. H., Umeh, I., & Ositanwosu, O. (2021). Characterization of heterogeneous malware contagions in wireless sensor networks: A case of uniform random distribution. In *Lecture notes on networks and systems: ICT analysis and applications.* (Vol. 2).
63. Nwokoye, C. H., Umeugoji, C., & Umeh, I. (2020). Evaluating degrees of differential infections on sensor networks' features using the SEjIjR-V epidemic model. *Egyptian Computer Science Journal, 44*, 86–97.
64. Ojha, R. P., Srivastava, P. K., & Sanya, G. (2018). Mathematical model for wireless sensor network with two latent periods. *Next-generation networks, advances in intelligent systems and computing*, *638*, 497–504. https://doi.org/10.1007/978-981-10-6005-2_50
65. Liu, G., Peng, Z., Liang, Z., Li, J., & Cheng, L. (2021). Dynamics analysis of a wireless rechargeable sensor network for virus mutation spreading. *Entropy, 23*, 572.
66. Di Pietro, R., & Verde, N. V. (2013). Epidemic theory and data survivability in unattended wireless sensor networks: Models and gaps. *Pervasive and Mobile Computing, 9*, 588–597.
67. Shen, S., Huang, L., Liu, J., Champion, A. C., Yu, S., & Cao, Q. (2016). Reliability evaluation for clustered wsns under malware propagation. *Sensors*. https://doi.org/10.3390/s16060855
68. Aliberti, G., Di-Pietro, R., & Guarino, S. (2017). Epidemic data survivability in unattended wireless sensor networks: New models and results. *Journal of Network and Computer Applications, 99*, 146–165.
69. Zhang, Z., Kundu, S., & Wei, R. (2019). A delayed epidemic model for propagation of malicious codes in wireless sensor network. *Mathematics, 7*(396), 1–17.
70. Wu, X., Cao, Q., Jin, J., Li, Y., & Zhang, H. (2019). Nodes availability analysis of nb-iot based heterogeneous wireless sensor networks under malware infection. *Wireless Communications and Mobile Computing*. https://doi.org/10.1155/2019/4392839
71. Batista, F. K., Martín del Rey, A., & Queiruga-Dios, A. (2020). A new individual-based model to simulate malware propagation in wireless sensor networks. *Mathematics, 8*, 1–23.
72. Biswal, S. R., & Swain, S. K. (2019). Model for study of malware propagation dynamics in wireless sensor network. In *3rd international conference on trends in electronics and informatics*, 647-653. https://doi.org/10.1109/ICOEI.2019.8862736.
73. Shen, S., Zhou, H., Feng, S., Liu, J., & Cao, Q. (2019). SNIRD: Disclosing rules of malware spread in heterogeneous wireless sensor networks. *IEEE Access, 7*, 92881–92892.
74. Shen, S., Zhou, H., Feng, S., Huang, L., Liu, J., Yu, S., & Cao, Q. (2019). HSIRD: A model for characterizing dynamics of malware diffusion in heterogeneous WSNs. *Journal of Network and Computer Applications, 146*, 1–14.

75. Muthukrishnan, S., Muthukumar, S., & Chinnadurai, V. (2020). Optimal control of malware spreading model with tracing and patching in wireless sensor networks. *Wireless Personal Communication*. https://doi.org/10.1007/s11277-020-07959-y
76. Liu, G., Peng, B., Zhong, X., Cheng, L., & Li, Z. (2020). Attack-defense game between malicious programs and energy-harvesting wireless sensor networks based on epidemic modeling. *Complexity*. https://doi.org/10.1155/2020/3680518
77. Zhang, H., Shen, S., Cao, Q., Wu, X., & Liu, S. (2020). Modeling and analyzing malware diffusion in wireless sensor networks based on cellular automaton. *International Journal of Distributed Sensor Networks, 16*(11), 1–9.
78. Kumari, S., & Upadhyay, R. K. (2021). Exploring the behavior of malware propagation on mobile wireless sensor networks: Stability and control analysis. *Mathematics and Computers in Simulation, 190*, 246–269.
79. Xu, B., Lu, M., Zhang, H., & Pan, C. (2021). A novel multi-agent model for robustness with component failure and malware propagation in wireless sensor networks. *Sensors, 21*, 1–25.
80. Liu, G., Peng, B., & Zhong, X. (2021). A novel epidemic model for wireless rechargeable sensor network security. *Sensors, 21*, 123.
81. Liu, G., Peng, B., & Zhong, X. (2021). Epidemic analysis of wireless rechargeable sensor networks based on an attack-defense game model. *Sensors, 21*, 594.
82. Zhou, H., Shen, S., & Liu, J. (2020). Malware propagation model in wireless sensor networks under attack–defense confrontation. *Computer Communications*. https://doi.org/10.1016/j.comcom.2020.08.009
83. Liu, G., Huang, Z., Wu, X., Liang, Z., Hong, F., & Su, X. (2021). Modelling and analysis of the epidemic model under pulse charging in wireless rechargeable sensor networks. *Entropy*. https://doi.org/10.3390/e23080927
84. Zhu, X., & Huang, J. (2021). Malware propagation model for cluster-based wireless sensor networks using epidemiological theory. *PeerJ Computer Science*. https://doi.org/10.7717/peerj-cs.728
85. Ye, X., Xie, S., & Shen, S. (2021). SIR1R2: Characterizing malware propagation in WSNs with second immunization. *IEEE Access, 9*, 82083–82093.
86. Serena, L., Ferretti, S., & D'Angelo, G. (2021). Cryptocurrencies activity as a complex network: Analysis of transactions graphs. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-021-01220-4
87. Wang, X., Wang, C., & Wang, K. (2020). Global dynamics of a novel deterministic and stochastic SIR epidemic model with vertical transmission and media coverage. *Advances in Difference Equations*. https://doi.org/10.1186/s13662-020-03145-3
88. Mishra, B. K., & Pandey, S. K. (2011). Dynamic model of worms with vertical transmission in computer network. *Applied Mathematics and Computation, 217*, 8438–8446.
89. More, A., & Raisinghani, V. (2017). A survey on energy efficient coverage protocols in wireless sensor networks. *Journal of King Saud University - Computer and Information Sciences, 29*(4), 428–448.
90. Gautam, A. K., & Kumar, R. (2021). A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. *SN Applied Sciences, 3*, 50.
91. Elhabyan, R., Shi, W., & St-Hilaire, M. (2019). Coverage protocols for wireless sensor networks: Review and future directions. *Journal of Communications and Networks, 21*(1), 45–60.
92. Al Hayajneh, A., Bhuiyan, M. Z. A., & McAndrew, I. (2020). A novel security protocol for wireless sensor networks with cooperative communication. *Computers*. https://doi.org/10.3390/computers9010004
93. Abdallah, W., & Boudriga, N. (2016). A location-aware authentication and key management scheme for wireless sensor networks. In *2016 22nd Asia-Pacific conference on communications*, pp. 488–495.
94. Bouazzi, I., Zaidi, M., Usman, M., & Shamim, M. Z. M. (2021). A new medium access control mechanism for energy optimization in WSN: Traffic control and data priority scheme. *Journal on Wireless Communications and Networking, 42*, 1–23.
95. Singh, J., Kaur, R., & Singh, D. (2020). A survey and taxonomy on energy management schemes in wireless sensor networks. *Journal of Systems Architecture, 111*, 1–22.

96. Senouci, M. R., & Mellouk, A. (2016). Wireless sensor networks. *Deploying wireless sensor networks* (pp. 1–19). Elsevier.
97. Gupta, S., Verma, S., & Abrol, R. K. (2015). Towards achieving reliability in wireless sensor networks—a survey. *International Journal of Control and Automation, 8*, 417–440.
98. Zhao, D., Zhou, Z., Wang, S., Liu, B., & Gaaloul, W. (2020). Reinforcement learning–enabled efficient data gathering in underground wireless sensor networks. *Personal and Ubiquitous Computing*. https://doi.org/10.1007/s00779-020-01443-x
99. Awan, K. M., Shah, P. A., Iqbal, K., Gillani, S., Ahmad, W., & Nam, Y. (2019). Underwater wireless sensor networks: A review of recent issues and challenges. *Wireless Communications and Mobile Computing*. https://doi.org/10.1155/2019/6470359
100. Genta, A., Lobiyal, D. K., & Abawajy, J. H. (2019). Energy efficient multipath routing algorithm for wireless multimedia sensor network. *Sensors (Basel), 19*(17), 1–21. https://doi.org/10.3390/s19173642
101. Wuke, Li., Guangluan, Y., & Xiaoxiao, C. (2020). Applications of deep extreme learning machine in network intrusion detection systems. *IAENG International Journal of Computer Science, 47*(2), 136–143.
102. Rehman, A., Rehman, S. U., & Raheem, H. (2018). Sinkhole attacks in wireless sensor networks: A survey. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-018-6040-7



ChukwuNonso H. Nwokoye obtained a BSc and PhD degrees in Computer Science. He is a two-time ACM SIGCHI Gary Marsden Student Award recipient. His interests include simulation and modeling of complex systems, agent-based modeling, wireless sensor networks and network security, social computing and computer supported cooperative work (CSCW). He is currently working on modeling and analysis of the propagation of malicious objects in network environments using analytical and agent-based modeling approaches.

V. Madhusudanan 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 areas of research are Mathematical modeling, Computational Intelligence and Control Systems. He has published many papers in various reputed national and international journals.