AN EPIDEMIC APPROACH FOR TRANSMISSION DYNAMICS OF MALWARE IN WIRELESS SENSOR NETWORKS

A Thesis Submitted

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY IN

Computer Science & Engineering

By

Shashank Awasthi

Admission No. –18SCSE3010016

Supervisor: Dr. Naresh Kumar,
Galgotias University, Greater Noida

Co Supervisor: Dr. Pramod Kumar Srivastava,

Rajkiya Engineering College Azamgarh

GALGOTIAS UNIVERSITY UTTAR PRADESH

June-2022

Galgotias University

Uttar Pradesh
School of Computing Science and Engineering

CERTIFICATE

This is to certify that Mr. Shashank Awasthi has presented her pre-submission seminar of the thesis entitled "**An Epidemic Approach for Transmission Dynamics of Malware in Wireless Sensor Networks**" before the committee and summary is approved and forwarded to School Research Committee of School of Computing Science and Engineering, in the Faculty of Engineering & Technology, Galgotias University, Uttar Pradesh.

Dr. Naresh Kumar
Supervisor & Professor,
Galgotias University, Uttar Pradesh

Dr.Pramod Kumar Srivastava
Co-Supervisor & Professor,
Rajkiya Engineering College
(Azamgarh)

Dean
School of Computing Science and Engineering
Galgotias University, Uttar Pradesh

Dean PG & PhD
Galgotias University
Uttar Pradesh

Date:

APPROVAL SHEET

This thesis entitled **"An Epidemic Approach for Transmission Dynamics of Malware in Wireless Sensor Networks"** by **Shashank Awasthi** is approved for the degree of DOCTOR OF PHILOSOPHY in Computer Science and Engineering.

Examiners

_____

_____

Supervisor (s)

_____

_____

_____

Chairman

_____

Date:

Place:

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis, entitled "**An Epidemic Approach for Transmission Dynamics of Malware in Wireless Sensor Networks**" in fulfilment of the requirements for the award of the degree of Doctor of Philosophy in Computer Science and Engineering, submitted in Galgotias University, Greater Noida is an authentic record of my own work carried out during a period from **September 2017 – December 2021** under the supervision of **Dr. Naresh Kumar** and co-supervision of **Dr. Pramod Kumar Srivastava**.

The matter embodied in this thesis has not been submitted by me for the award of any other degree of this or any other University/Institute.

Shashank Awasthi

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

Dr.Naresh Kumar
Supervisor
Galgotias University
Greater Noida

Dr.Pramod Kumar Srivastava
Co-Supervisor
Rajkiya Engineering College
Azamgarh

The Ph.D. Viva-Voice examination of Mr. Shashank Awasthi, Research Scholar, has been held on_____.

Sign. of Supervisor(s) Sign. of Co-Supervisor(s) Sign. of External Examiner

ACKNOWLEDGMENT

I express my deepest gratitude to the Almighty for bestowing his choicest blessings on me. It is with the invisible hand-holding of God that I have been able to complete this thesis. The completion of my thesis also involves the contribution of many people. I am thankful to all of them.

I express my heartfelt thanks to Dr.Preeti Bajaj, Vice Chancellor, Galgotias University, Greater Noida. She has been a guiding light in the successful completion of my work. Her constant support and positivity has been a source of motivation always.

I would also like to sincerely thank Prof. (Dr.) Avadesh Kumar, Pro Vice-Chancellor, Galgotias University, Greater Noida. He has been an ideal mentor who offered timely advice and encouragement unconditionally.

I am grateful to Dr.Munish Sabharwal, Professor & Dean (CSE)- Galgotias University, Greater Noida for giving valuable comments and suggestions regarding my work. It was because of him that I could reach this milestone.

I am extremely grateful to Dr. Sampath Kumar K, Professor, School of Computing Science and Engineering, Galgotias University, Greater Noida. His never ending support in accomplishing this task has made this journey enjoyable.

I extend my special thanks to Dr.Prashant Johri, Professor, Galgotias University, who has helped me in choosing the right tools in my research. Under his direction, this journey has been obstacle-free.

Finally, I would like to thank all my friends who have been a strong force in making me reach this height of success.

Shashank Awasthi

ABSTRACT

In recent decades, a lot of research has been done in the area of wireless sensor network (WSN). The field of WSN has attracted many researchers because of its progress in the capacity of sensors like more sensing power, effective communication and advanced computational abilities. Many applications are using the WSN nowadays. WSN is utilised in a variety of real-time applications to conduct tasks such as data collection, vehicle tracking, and activity monitoring. Malware attacks, communication range, reliability, and longevity of the nodes are just a few of the difficulties that WSN faces. Numerous researchers have proposed various models, techniques, and approaches to improve network performance. Whereas various factors were addressed in the construction of these development and evolution, a few key issues were overlooked. To address these flaws and to develop different models which are based on epidemiologic concept, this study looked into current research activity on malware (worms, viruses, and malicious codes) attacks.

WSN is a type of distributed network and due to short range of communication capability a method of multi-hop communication is used for data transmission. WSN is generally stationed in areas which are remote. There are various types of security threats associated with WSN due to weak defense capability. WSN is vulnerable to numerous security threats which can adversely affect performance. The security of WSN against malware attack is a serious challenging issue, so devising the methods to prevent security threats is of utmost importance. But the methods devised to prevent the attacks cannot guarantee that the attacks will not be launched and till now there has been no technique which can disable such attacks from WSN.

The different types of attacks are coming into picture on regular basis and are not known in advance. Presently, attack of malware in WSN is one of the prime concerns for security of information. The malwares attack is not limited to security only, they consume energy of sensor nodes quickly. So, the outcome of malware attack is network instability, that create the different types of operation problems in WSN. Therefore, stability of the network is important for smooth communication.

In this thesis, we studied the transmission dynamics of malware and security problems arising due to it and network stability in different conditions. The main objective of this thesis is to develop and analyse the epidemic based mathematical models for the study of dynamical behaviour of malware transmission in WSN. In this thesis, the three epidemiological models have been proposed in order to comprehend the situation in a better way. For the stability analysis of the proposed models, extensive mathematical analysis is performed. The proposed models' performance is assessed as well as their comparison to other models have been performed. The proposed models help in identification of potential factors that increase the transmission speed of malware and which can affect the performance of WSN. Such analysis helps the prevention of malware transmission and implementation of corrective measures in time to eradicate the malware from WSN.

In the beginning, we focussed on finding out where the malware attacks in WSN and which kinds of problems arise in the network. We proposed a SILRD (Susceptible-Infectious-Low Energy-Recovered- Dead) model, which is based on epidemiology. The model describes malware transmission dynamics in WSN. The developed model suggested a mechanism to control the transmission of malware and improvement of WSN lifetime. The effect of low-energy state and charging on transmission of malware in WSN is analysed. Moreover, this model is improved by including the idea of coverage and connectivity and their effects on transmission of malware is discussed. Further, the SILRD model extends by using the concept of early detection of malware presence in WSN. For early detection of malware presence in the sensor network used exposed (latent) state of epidemic modeling. This helps in control of malware transmission in WSN. The extended model is known as SEILRD (Susceptible-Exposed-Infectious-Low Energy-Recovered- Dead) model. The effect of exposed state on malware transmission in WSN is observed. The effects of other networks parameters such as communication radius, node density, rate of infection etc. are discussed.

This thesis has investigated the effects of simultaneous attack of multi-malware (two malware) on compromised transmission and proposed a modified SE_1E_2IR (Susceptible - Exposed category of 1 - Exposed category 2 – Infectious – Recovered). The proposed

model is used to prevent the malware transmission in WSN in case of multi-malware attack. The proposed model took into account two types of malware attack in WSN simultaneously. The stability analysis in case of multi-malware has been worked out through this analysis. The impacts of coverage and connectivity on transmission of malware is also discussed and the threshold value for smooth functioning of WSN is computed. The comparative study has been carried out.

For the study of the malware transmission dynamics in WSN, an important parameter needs to be obtained, and that parameter is known as basic reproduction number (R_0^{th}). This is borrowed from bio-mathematics and is an important parameter of epidemiology. To analyse the system stability in different conditions the value of R_0^{th} of all the propsed models has been obtained. The points of equilibria of malware-free and endemic of models have been examined and the conditions of malware eradication from the system has been analysed. All the proposed model has been investigated thoroughly, and their stability conditions have been determined using concept of modeling and theorems as well as proofs. The effectiveness of all the proposed model, as well as their comparison to existing models, in order to determine their feasibility has been analysed. To confirm the analytical findings, simulations of all the recommended models were executed. The simulation was carried out using the MATLAB (R2017a) software. To further explain the findings, a variety of graphs have been prepared. Some related discussions also took place.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF PUBLICATIONS

1. Awasthi, S., Kumar, N., Srivastava, P.K. (2020). A Study of Epidemic Approach for Worm Propagation in Wireless Sensor Network. In: Solanki, V., Hoang, M., Lu, Z., Pattnaik, P. (eds) Intelligent Computing in Engineering. Advances in Intelligent Systems and Computing, vol 1125. Springer, Singapore. https://doi.org/10.1007/978-981-15-2780-7_36

2. Shashank Awasthi, Naresh Kumar & Pramod Kumar Srivastava (2021) An epidemic model to analyze the dynamics of malware propagation in rechargeable wireless sensor network, Journal of Discrete Mathematical Sciences and Cryptography, 24:5, 1529-1543, DOI: 10.1080/09720529.2021.1951436 (Scopus/ESCI)

3. Shashank Awasthi1, Naresh Kumar, Pramod Kumar Srivastava, Rudra Pratap Ojha(2021). Analysis of Epidemic Model for Performance Evaluation of Rechargeable Wireless Sensor Network, Journal of Engineering Research (Kuwait), DOI : 10.36909/jer.ICCEMME.15847 (SCI/Scopus)

4. Shashank Awasthi1, Naresh Kumar, Pramod Kumar Srivastava (2022), "An Epidemic Model for the Investigation of Multi-Malware Attack in Wireless Sensor Network" Wireless Personal Communications", (Communicated)

ABBREVIATIONS

Abbreviation		Description
ADC	:	Analog to digital converter
EiSIRS	:	Extended improved Susceptible-Infectious-Recovered-Susceptible
iSIRS	:	improved Susceptible-Infectious-Recovered-Susceptible
SILRD	:	Susceptible-Infectious-Low Energy-Recovered-Dead
SI	:	Susceptible-Infectious
SIS	:	Susceptible-Infectious-Susceptible
SIR	:	Susceptible-Infectious-Recovered
SILRD	:	Susceptible-Infectious-Low-Energy-Recovered-Dead
SEIR	:	Susceptible-Exposed-Infectious-Recovered
SEIS	:	Susceptible-Exposed-Infected- Susceptible
SEILRD	:	Susceptible-Exposed-Infectious-Low-Energy-Recovered-Dead
SODE	:	System of Ordinary Differential Equations
TWPM	:	Topologically-Aware Worm Propagation Model
UWSN	:	Unattended Wireless Sensor Network
WSN	:	Wireless Sensor Network

Chapter 1: Introduction

1.1 Introduction to Wireless Sensor Network

Wireless sensor network (WSN) received tremendous attention from academia and industry due to different types of applications [1] from last decade. A WSN is a self-organizing wireless network which is comprised by the thousands or a greater number of spatially distributed tiny sensor nodes, they can communicate to each other and exchange data. Sensor node is mainly built-in order to observe the environmental conditions such as humidity, pressure, vibration, temperature, position, sound etc. Basically, WSN used for the purpose of data monitoring and collection [2].

In order to capture the real world's phenomenon from the environment WSN is used which is structurally distributed self-independent sensors, that collect information or data and transmits through sensor nodes to a special type of node having more ability which is known as Sink Node/Central Node/ Base Station (BS). The sink node stores the data for analysis purpose. Nowadays data is playing significant role in life of individuals and society. Decision making processes are using more data to make minimum error in implementation. Data collection, processing and transmission decides fate of systems in place. Data transmission is one of the challenging issue due to various environmental, hardware and software constraints. Numerous data transmission technology is being used and innovation is happening to provide faster, reliable and robust data transmission between devices. Information retrieval, collection and analysis is significantly important for decision making in different domains. In this regard WSN play an important role [3].

Sensor node is typically small, intelligent, low-cost, light-weighted, bearable, wearable and comparatively easy to deploy in resected to other methods of sensing. Sensor nodes can be distributed in structured or unstructured manner in the area of interest. In case of structured distribution location of each node are (sensor or sink node) known in advance. Then nodes can be controlled and programmed for data transmission and their maintenance work can be performed easily. In structured distribution with the help of smaller number of nodes better connectivity can be achieved and save cost. However, in case of unstructured distribution, the nodes are randomly located, and they are used only for monitoring the events [4].

WSN is made from hundreds to thousands of sensor nodes capable to connect each other's communication link. It is not necessary all sensor nodes connected to each other. Sensor nodes connection defines the wireless environment. A WSN is capable of gather data or information through sensor nodes and process using base station for real time application. The data or information flow can be performed in two-way direction from sensor nodes to base station and base station to sensor nodes. So WSN can also perform to broadcast messages to sensor nodes to pass specific data or instructions. These information collection and processing is done in wirelessly distributed environment. WSN proposes a wirelessly distributed information collecting and processing system which can be useful for number of applications. Fleet management system is important for battlefield operation and WSN plays important role in national defence operation. The role of defence innovation is a motivation behind development of WSN from defence to industries. Now WSN is being important part of day-to-day operation of industries from manufacturing to service industries such as health monitoring, weather monitoring, environment monitoring and more [2,5].

Limitations of WSN: The applications of WSN are increasing day-by-day. So, the different types of challenges are also surfacing due some limitations of sensor node. The limitations of sensor node are energy (battery), memory, transmission range, processing capability. Therefore, some challenging issues which are associated with WSN are energy consumption, nodes' deployment, area of coverage, security, data collection etc. Generally, WSN was used in specific field but with advancement in technology this has become more reliable and flexible in applications. So, WSN has become an integral part of new technologies such as Internet of Things (IoT), autonomous mobility, logistic operation, Industry 4.0, etc [6]. WSN is poised to change the world. This is amongst top ten technologies reviewed by MIT. WSN depends on sensor nodes and sensor nodes are completely dependent on their battery. The meaning thereby when the battery of sensor node will discharge, the working of sensor nodes will be automatically ceased. The shortcoming of this technology is its limited power resource, memory, bandwidth, latency, throughput and poor security mechanism etc. These are accountable for poor outcomes of the system. Sensor nodes replacement is not an easy task; hence, to optimize the utilization of energy is the solution in order to maintain overall system performance and to improve the lifetime of WSN. Therefore, due to prominent and numerous applications academicians and industries are focusing on research of WSN.

1.1.1 Sensor Node Architecture

Sensor node comprises of four components power unit responsible for energy supply, processing unit perform data processing, sensing unit provide interface for external environment and communication unit for data transmission. These are the four are the building blocks of sensor node. The sensor node's architecture is shown in figure 1.1 [2].

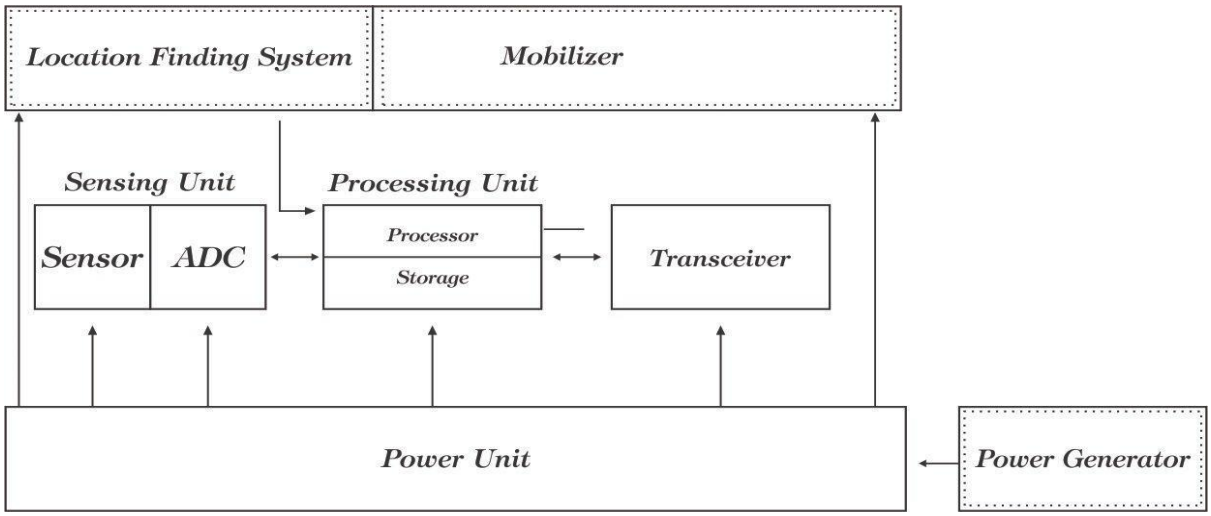

Figure 1.1: Sensor Node Architecture

Sensing Unit: Sensing unit comprises of analog to digital convertor (ADC) and various types of sensors. Sensor's sense events and produces analog signals. This unit works in a way to provide the interface with physical environment to virtual world. The inbuilt sensors collect data in analog format such as temperature, pressure, motion, etc. and pass it as digital signal for processing. The physical environment data collected in the analog form and that is converted into the digital signals. The analog signals are converted into digital signals by digital convertors. The digital signal feed to processing unit for further processing. According to the applications, the particular kinds of sensors can be selected.

Power Unit: The power unit is responsible for energy source of node and provides energy for data sensing, data processing and data transmission. The power supply can be provided directly from a power source or storage unit such as battery mainly. The sensor nodes embedded to any infrastructure have direct power supply but standalone sensor nodes depend on battery operated power sources. The sensor node uses their energy during the different operations in the network such as sensing of event, data processing and in communication. Data transmission phase uses more amount of energy compare to data collection and data processing.

Processing Unit: Processing unit is key component of sensor node which contains processor, operating system and memory. The task of the unit is to process data, execute instruction and store data. This unit determine the computational capability and use of sensor node's energy. Numerous categories of processors with specific properties are used in sensor nodes for example microcontrollers, digital signal processors, application-specific integrated circuits and field programmable gate arrays. The most commonly used process is microcontroller in sensor node.

Transceiver (or Communication) Unit: Data transmission and receiving task is performed by this unit. It makes the connection between different sub-components of the sensor node and processor. The other nodes of the network are also connected through this unit. The communication unit is an energy intensive unit in the sensor node and the use energy is control by transducer through switching amongst different modes such as sleep, active, idle. The transmitter is used to convert into optical form from the electrical signal at sender end as well as receiver end. For improvement of WSN performance, a sensor node may add the extra elements such as GPS (Global Positioning System), mobilizer, etc.

The sensors are normally categories as physical, biological and chemical, which are smart to supervise a broad range of ambient sites. WSN uses for data collection on periodic basis in applications of mission critical [2,5-8]. Numerous vital applications are discussed in the literature, military target tracking and surveillance [9-10] Health-care applications [11-12], object monitoring [13, 14], flood detection [15], vehicles tracking [16], Gas monitoring [17], traffic monitoring [18], Water quality monitoring [19], seismic sensing [20], agriculture [21-22] and disaster [23], dangerous environment exploration, environmental and pollution application [24-25], etc.

The sensor nodes are equipped with microchip controller, integrated circuits, and communication antenna and battery source. Sensor size can vary from millimetre to meters depending on the requirement and involved technologies. Smaller sensor size in microns is also feasible as per the need and technology involvement. The technology involved, transmission rate, memory, energy requirement and size of sensor defines the cost of sensor nodes. The higher efficient sensor nodes incur the higher cost. These nodes are designed to collect the data from different sources in different networking environment and passed to base station for further processing.

1.2 WSN Communication Structure

Afterward gaining the acquaintance of sensor node architecture, it is imperative to know the WSN communication structure. WSN' communication structure is different from the traditional communication structure such as computer network. Sensor nodes are normally installed in hostile environments and have the capability to sense the data from different geographical areas [26]. Sensor nodes collect the data from nearby coverage area and collected data deliver to sink node or base station (BS) with the help of neighbouring nodes. A Sink node is more equipped and is powerful in terms of computation, communication range and energy in comparison to sensor node. Sink node acts as a gateway node (GWN) between the end users and WSN. The key aim of sensor nodes deployment is to cover the optimum possible area, to implement effective, reliable and secure communication. Sensor nodes communicate data to base station through intermediate nodes. This communication is referred as multi hop communication. Multi-hop communication is very reliable way to transmit data. It provides hop to hop communication which is robust in nature and effective in critical environment. Multi-hop communication is better than end to end communication which require dedicated path from both end and not suitable for critical infrastructure more prone to data loss [27]. A structure of WSN is shown in figure 1.2.

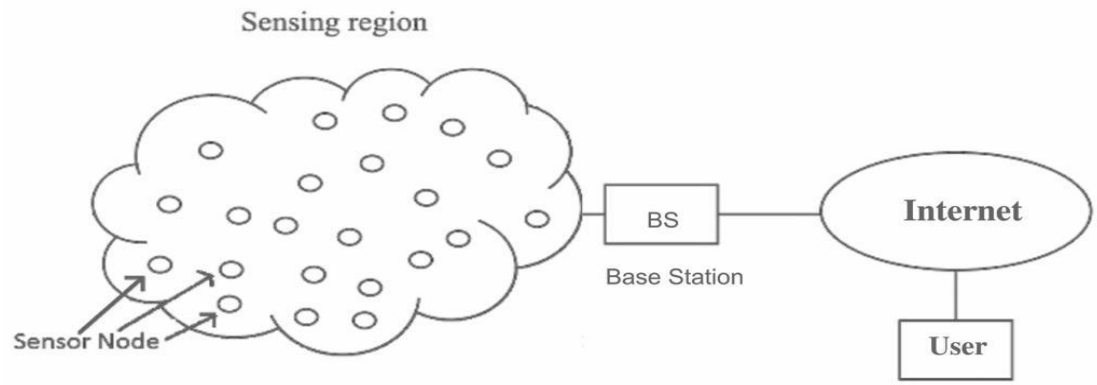

Figure 1.2: WSN Communication Structure

1.3 Features of Wireless Sensor Network

WSN can be deploy in normal to critical situation. It requires minimum to high infrastructure availability as per requirement, energy deficiency to energy surplus supply, small to large network, normal geographical to critical geographical location that can be used. WSN can be

useful in normal applications to critical applications. It is ready to be deployed with minimum to no infrastructure as per the application requirement in minimum time. Some application requires temporary network to be deployed on demand and WSN is best case fulfilling all requirements. These advantages or features have made WSN having edge over other computer network. These networking features energy consumption, fault tolerant, node mobility, processing capability, communication capability, distributed networking, dynamic topology and ready to be deployed are important characteristics of WSN [28,29].

Energy Efficient: Sensor nodes are micro electronic devices have limited power resources. A nodes life depends on power source availability and energy require to data gathering and data transmission. A sensor performs role of data creator and data transmitter. If a path is broken with what so reasons, then it requires to finding new path, reroute data and repair broken path. This frequent change in network topology and energy constraints put down challenges for proper power management [3, 4]. Sensor node require energy for multiple task data collection, processing, transmission and internal components. A sensor node is become inactive after exhausted of energy source and abandoned by network. Inactive node or dead node perform no task and replaced by other active nodes. Data transmission phase require high energy for data transmission. So WSN lifetime depends on how the limited energy source is utilized. An energy efficient mechanism is required for WSN to increase lifespan of sensor nodes.

Self-Organized Network: WSN is a collaborative and self-organized network system. Sensor nodes of WSN have ability to build a network when installed in any unidentified manner and establish the communication between the nodes. Sensor nodes coordinate to each other and form the network automatically. They work in self-adjustable and cooperative manner to constitute a network.

Quality of Services: Sensor nodes are equipped with low power for data processing and transmission. Network is designed to provide efficient services with quality. It is primary aim of any network which is offering services to users. Quality of service demands high processing and consume high energy and bandwidth. WSN suffers from energy constraints as well bandwidth limitation, so use different methods to offer quality of services. This can be achieved due flexible and adaptive nature of WSN. A highlife time can be trade off with quality, lower throughput and high transmission delay.

Computing Capacity: WSN has limited computing capacity due to its resource constraints. The sensor node equipped with a processor with low capability. Energy constraint as well as processor's low capability reduce the WSN from high end processing. Computing process require high energy which is not favourable for sensor nodes having limited energy storage. In

WSN, high end computing is performed on base station or centralized system. It saves sensor node's energy from high energy required process. Sensor nodes can perform data collection, minimum processing and data transmission without wasting energy on high processing [5]. Sensor nodes are equipped with on board processing which is used to carry out data sensing, collection and transmission. Sometimes sensor nodes perform data computation and transmit the necessary information to central system.

Wireless Communication: Wireless communication technique uses by WSN, it uses mainly radio frequency for data transmission between the sensor nodes. They use radio frequency to communicate with base station also. Sensor nodes are having low coverage area and WSN covers short communication range. It reduces capability of data transmission for WSN. To increase overage of network, more sensor nodes are required in operation. WSN can perform data transmission in large distance with efficient energy and data transmission mechanism. Wireless communication can be performed in unidirectional, bidirectional and omnidirectional direction basis on application requirements. Sensor nodes are equipped with unidirectional and omnidirectional antenna to perform directional or broadcast data communication. Wireless communication comes with its advantage of wireless data transmission with ease and adoptability but having its own demerits. Wireless transmission suffers from outside environment, nature, terrain, manmade structures and natural disaster. It all effects performance of WSN in hostile environment.

Dynamic Topology: WSN follows dynamic network topology which depends on application requirements. Sensor nodes having limited energy source so its energy can be exhaust due to operation and become inactive or dead. So, it is required to replace inactive or dead nodes from the network. It causes network topology to change in runtime. WSN supports network topology required for application suitable for hostile environment. Sensor nodes failure leads to frequent broken path and data loss. WSN topology maintenance is high resource incentive task which becomes more challenging with a greater number of sensors. Topologies should be carefully selected for sensor network and maintenance strategy should be depends on node's density. Nodes are capable with self-organizing and self-sustainable topologies. Dynamic topology should support nodes scalability with minimized incur associated cost. Sensor nodes deployed in mobility environment should support dynamic topology with movement. Frequent movement results into broken paths and high maintenance for organizing alternative routes to destination.

Security and Privacy: WSN is prone to security breach and attacks. Wireless networks use wireless medium for communication which can be easily penetrated against vulnerability and malware insertion. WSN is a kind of wireless network so it's also vulnerable for security breach and attacks. To enhance security of WSN, advanced security technique is required. It also needs to be updated from time to time. WSN works for critical application in hostile environment, so its security is upmost challenges [2, 8].

Multi-hop Communication: Sensor nodes are designed for short range communication. They have limited resources and energy which is not suitable for large range communication. Larger wireless range require powerful antenna and more energy to operate. WSN uses multi-hop communication to expand its coverage area. WSN can be deployed for distanced data transmission using node to node communication. In multi-hop communication, each nodes established a connection to nearby nodes within their range and so on. A node is responsible for only data transmission to nearby nodes. Source node transmit data to nearby node and this process is performed until the sink node received the data. Multi-hop communication increases the range of WSN network [4]. Sensor networks are designed for variety of applications. These applications are mostly requiring sensor nodes in closed proximity. Sensor nodes creates a dense communication topology in large numbers. Mostly sensor networks use large number of sensors in dense environment. These dense population is favourable to multi-hop communication and require less energy to operate. Point to point or single hop communication consumes more energy in comparison to multi-hop communication in dense population. Sensor nodes uses less power to transmit the data to nearby nodes.

Fault tolerant: Fault tolerant networks are designed for more robust performance in hostile conditioned. The networks are designed for critical conditioned environment or resource inefficient network. Wireless networks are less efficient to wired network due to wireless transmission medium. Wireless transmission suffers from data loss, nodes failure, natural causes and etc. WSN have these advantage with energy constrained. WSN network are designed to work in dynamic environment so they must incorporate fault tolerant, self-organization and self-repairing mechanism in order to handle transmission loss in case of nodes becomes inactive.

Deploy Ability: WSN is ready to deploy in any environment. WSN can be deployed for small scale to large scale data transmission. As per demand, WSN can be deployed in any location with no to minimum infrastructure requirement. Sensor nodes can be small to large as per the need of application. Smaller sensor nodes require less energy and resources and easy to be deploy to established network. Sensor nodes cost decides the cost of WSN, so it should be

minimum to build and operate. Sensor nodes deployment strategy can differ based on scenario. Sensors collect data from the environment with full of noise. Sometimes these sensors are established far away from locations. Large sensors are deployed to collect data by the use of complex techniques for example space exploration and environment studies. Times series data play significant role in designing time critical applications for example high speed mobility. In this deployment strategy, communications topology has utmost importance which need to be carefully chosen. Autonomous mobility faces challenge in communicating topology where information is collected from mobility and passed to centralized system for processing.

Scalability: Applications are designed to support users demand for quality contents or services. With time the number of users, demands, upgraded services need to be updated which require a scalable network. WSN are capable to scale as per demand. Sensor nodes can be added from tens to thousands in existing network to cater application demands. Node density varies with applications. Some applications require high number of sensors as per demand on some specific time.

Data Transmission: Data transmission is carried out through wireless medium in wireless network. These wireless mediums are comprised of radio wave, infrared, microwave and optics. Medium can be used as per availability and locations. Sometimes terrain affect selection of medium. Not all medium is suitable everywhere for data transmission. WSN can be established by using any medium for data transmission as per availability and suitability. Sensor nodes transceiver should be small in size, minimum environment inference, cost effective, adopt unregulated frequency and operate on low power. These constrains limit the options for hardware capacity, antenna efficiency and power usage. So, while choosing the transmission medium considering these constrains will improve WSN performance. Radio frequency (RF) is widely adopted in sensor networks due to their low power requirement and efficiency in low range data transmission. Infrared communication is also adopted in smart devices for in sight communication. It is easier to develop, low cost, offer robust communication and license free solutions for smaller devices. Only drawback with infrared is line of sight communication. Smart dust mode is a sensing technology uses optical fibre communication medium for data exchange.

Small Physical Size: Normally, sensor nodes size is small and they have limited range of communication, memory, energy, and processing speed.

Low Cost: The larger number of sensor nodes are required to deploy in field for measurement of anticipated physical environment. The price of sensor nodes should be the lowest possible to minimize the complete cost of whole WSN. Sensor network are designed for applications

catering individuals, society and business. Health care application require low cost and effective sensor nodes to support users from underprivileged backgrounds. Cost effective sensor nodes are in demand. Cost of sensor nodes are getting minimum with time. WSN made from number of sensor nodes if they are costly then it results into high cost of sensor networks. Producing sensor nodes with minimum cost is challenging topics and gain attention from research and manufacturing community. A continuous effort is carried out by researchers and developers to minimize sensor nodes cost and improve operability and features [3, 4, 10].

Responsiveness: The sensor nodes are self-organizing device so; they are independent and work in any circumstances and show responsiveness. If sensor nodes exhibit responsiveness traits without explicit user or administrator action, WSN functions more effectively. A much more flexible network produces more throughput, which in turn boosts the network's efficiency.

1.4 Wireless Sensor Network Applications

Sensor node are small in size, incur low cost, inbuilt energy storage and workable in hostile environment. Sensor nodes are of different types such as Temperature Sensor, light sensor, pressure sensor, biological sensor, proximity sensor, infrared sensor and chemical sensor. These vast majority of sensor types open a possibility of different types of WSN uses in different domain. They are easy to deploy, support critical application and can work in any environment.

Sensor nodes are well equipped to perform sensing, detection of event and controlling outcomes. Applications are mainly to collect the sense data to identification of events and control their actuators to provide desire outcomes. These phenomenon makes sensor nodes useful in commercial applications, defence applications, health applications, environment and many more. WSN infiltration is growing in new area of applications with time. Applications may range from multiple domains as per domain specific needs and resource availability. Here outline some important applications on WSN but not limited to [28,30].

Defense Applications: Defense is a core issue for any nation and world as whole. Every nation has right to be live in peace and can take any steps to improve their security. People are living in a world of uncertainty where they are under continuous threat from border as well as inside. Security requires ready to deploy and on demand solutions such as battle field network, fleet management etc. These applications require a wireless network having support to any kind of

devices which is possible through WSN. Data collected from sensor nodes are feed to surveillance system for tracking movement, targeting enemy and decision planning. These data are important for parties. Faster and accurate data results into better chances of winning the battle and WSN can provide a way to transmit the data into such harsh environment. Critical operation carry inside the nation also uses WSN to collect significantly important data for better resource utilization and mission planning.

Healthcare Applications: Healthcare sector is significantly important for individuals and nation as whole. Healthy person is important asset for nation and government responsible to provide affordable and available health services to each individual. Healthcare sector uses a large number of devices to collect patient data and analyse to provide effective medical assistant. It is a known facts that medical practitioner and services are relatively less to requirement. Data analysis play an important role to provide faster and affordable solutions to patients and WSN can be well used to collect these data through sensors node embedded into devices. It reduces the cost of medical services drastically and provide affordable services to far reachable locations not facilitated by government. A patient data can be collected via medical devices and directly send to centralized system. Data analysis is carried out by processing system with the help of medical practitioner and required solutions is revert back to the patient using well organized WSN. For the purpose of status tracking and monitoring of patients in hospital rooms, in Intensive Care Units (ICUs) and emergency situations WSN play an important role.

Agriculture Sector Applications: Agriculture is an important component for country economy specially developing countries. In last century, population has increased exponentially which creates demands of agriculture commodity. Devices equipped with sensors is used in agriculture to improve productivity. WSN can be established in a agriculture field to monitor real time data from fields in which crops are sowed. These networks can work in any conditioned irrespective of weather scenario. A decision support system can be integrated with these networks to support agriculture development activity. Agriculture is promising field and faces new challenges such as air quality, soil quality, humidity, etc with the time. These problems can have better solutions by analysing the data provided by deployed WSN.

Disaster Management Applications: Natural disaster is unpredicted and can damage any communication support which is nightmare for affected individuals. Earthquake, forest fire, flood and etc. can create havoc and need of instant support. WSN can be effectively provide solutions for data collection and analysis for better decision system. Natural disaster

management system personal require instant networking solution for transmitting critical information.

Environment Monitoring Applications: Environment is unpredicted and can cause unprecedented changes in life of human. Human population growth and natural resources consumption have increased so much it has damaged the whole ecosystem. Famous cities are losing the favourable conditioned for living standard for human being. Forest is under constant threats from unpredicted events or human activity. Sensors can be deployed on critical points to monitor real time pollution, rainfall detection, wind speed and temperature. Environmental crisis is long term phenomenon and follow series of events to reach final outcome. This requires continuous monitoring and sensing events with accuracy. It can help some time to take necessary actions to prevent environmental crisis and avoid heavy losses to human losses and resources. Every year, world suffers from loss of resources and human lives which can be minimized or avoided by using effectively sensor nodes deployment at critical points.

Industrial Applications: WSN is heavily deployed in industrial application. Industries require real time data monitoring for effective productive activity. Real time data monitoring can handle problems, maintain quality and provide better solutions. Industrial applications smart homes, manufacturing, automotive mobility, energy sector etc. are using WSN to improve day to day activity.

Hazardous Detection Applications: Chemical and biological material usage has tremendous growth in last decades. They are being used in health sector, manufacturing sector, environment and mass destruction weapons. WSN is used to provide detection, monitoring and controlling of events in chemical and biological induced operations. These chemical and biological agents require continuous and remote based tracking which require highly accurate and faster data transmission medium. Sensor network are best candidate to provide sensed data with accuracy in real time.

Home Automation and Smart Environment Applications: Home automation or smart homes are new popular terminology in last decades. Smart homes are equipped with smart appliances capable to communicate to each other over internet. These devices have inbuilt smart sensor nodes with on-board data sensing, processing and transmission capability. Home automation and smart devices are gaining investment and research. This research mainly focuses on communication technology in WSN. Human oriented and technology oriented are two approaches for developing smart environment. Human oriented smart environment focuses on technologies adaptation as per user needs while technology-oriented solutions adopt need of devices.

Commercial Applications: Services and production industries uses sensors heavily in monitoring and controlling events. When they produce in large scale then sensor network deemed to be efficient in real time. A product or service depends on high number of sensor data from initial phases to final outcomes. These sensors networks can be deployed in normal to critical environment. WSN has significantly important role in commercial applications which requires high end sensors to maintain quality of product and services.

1.5 Research Subjects in Wireless Sensor Network

Sensors are important for applications but this is a device with resource constraints. Sensor nodes are suffering from different types of problems such as coverage, energy, security, connectivity etc. due to limited resources. And WSN is a collection of sensor nodes. Therefore, WSN also suffers from network coverage, lifetime of WSN, connectivity and security against malware attack etc. problems. Hence, for larger distance data transmission in WSN the multi-hop communication is used. The sensor nodes are vulnerable to attacks and security issues. In the following subsections some important issues of WSN are discussed.

Node Deployment and : Deployment of sensor nodes in the field, where perform the monitoring and control task is a crucial issue in WSN. The sensor nodes deployment is a basic of WSN applications [31]. Monitoring is important to save the life of people, animals etc in the universe and for monitoring purpose WSN is very useful. Traditional monitoring techniques are not able to detect unforeseen circumstances such as hazards in the environment they used only for remedial measures after unforeseen circumstances [32]. For improvement of quality of services and fearless life of people, animals and others require strong monitoring mechanism which can measure the different parameters of the environment. On the basis of environmental parameters forecast the unforeseen situation and minimize the possibility of any kinds of disaster. That can ensure the safety, security, satisfaction of customers, minimize losses etc. For this purpose, WSN is suitable due to intelligent device, flexible and adaptable nature as well as use of wireless communications technology in operations. WSN overcomes the drawback of traditional technology and growing its use for monitoring is day-by-day.

Algorithm of node optimization was proposed by Hou Y et al. [33] with concept of problem of computational geometry. This algorithm reduces the cost and improve the connectivity. Utilize the concepts of cellular grid Fan Zhigang [34] suggested an algorithm for sensor node deployment in the area of monitoring. The suggested method reduced the problem of redundant sensor nodes and attain the maximum coverage. The idea of Voronoi elements was used by

Alam et al. [35] for sensor nodes deployment. The proposed system divides the deployment field into number of polyhedrons and then compute the farthest separation in the polyhedron between two of any points in a manner that sensors can ensure communication of each other and transmit the data to the sink node. The proposed method of sensor nodes deployment was verified with good connectivity results. Priyadarshi et al [36] presented a survey in which to discussed the different node deployment methods that can minimize the cost and improve the connectivity of the network.

WSN Coverage and Connectivity: The connectivity of sensor network and coverage of sensor nodes are limited due to certain constraint. It is important points in WSN research and research are continuous pouring out to find the effective solutions to increase effective coverage and connectivity of sensor nodes. Signal attenuation level is changing with the position of sensor nodes. It can vary significantly which can cause poor network coverage and connectivity. Sensor nodes capability of sensing communication channel varies due to various factors. It causes a variable sensing model to be adopted to calculate the network coverage. Node failure is common phenomenon for wireless network [37,38]. WSN suffer from node failure due to limited power availability which can be last longer. One node failure affect the node connectivity in neighbourhood and multiple node failure affect the overall network. Research work explain the node failure affect on overall network connectivity.

Liu et al. [39] discussed the shadow effect on the coverage and connectivity of the network by use of shadow-fading model. Ou et al. [40] explained the connectivity of the sensor network when the sensing radius of sensor node is varied. The effect of radius on connectivity and coverage is discussed by them in details. Kumar et al. [41] discussed the effects of shadowing fading and multi-path on connectivity and coverage of WSN. Kaiwartya et al. [42] analysed the effect of sensor nodes deployment on WSN connectivity. They developed seven metrics for measurement of quality of connectivity and coverage of WSN. Also, they extended their own work [43] and explain network formation cost and energy consumption along with connectivity and coverage.

Limited life of WSN: WSN nodes are limited with power supply and depends on battery power source. The limited power source exhaust after some time and nodes becomes inactive [44]. These nodes are declared as dead nodes and needed a replacement. Dead nodes are replaced by more active nodes but this a difficult task. Numerous research is carried out to improve the life of sensor nodes and improve their efficiency. Jurdek we al. [45] proposed comprehensive node

energy model to increase the life of sensor nodes. An adaptive method was developed to optimized sleep time of a sensor nodes. Sleep time is duration when node is not active and have no communication. After sleep time, node will become active and wait for its communication. Authors have uses MAC protocol to save nodes energy by forcing node to sleep mode while no communication is going on. As soon as the data communication becomes available then nodes are also active and start receiving and sending the data. Yadav and Yadav [46] presented detailed review of various design issue for energy consumption. Several factors such as data size, aggregation process, routing path, internal processing and etc. consume energy differently. These factors have varying energy requirement and depends on internal or external factors. Piyare et. al. [47] suggested a wake-up system for finding transmission and letting main receiver offline and thus improving power utilization effectively. Dynamic topology management approach uses adaptive energy approach for residual energy in sensor nodes. Energy is balanced among the nodes and lower energy nodes are given less task to perform in order to increase lifetime of WSN. For lifetime improvement of WSN some other mechanism with different concepts was suggested. LoBello et al. [48] suggested a method of dynamic topology management through which balance energy using adaptive approach. Another method for saving energy in WSN was proposed by Luo et al. [49]. They subjugated the idea of opportunistic routing idea for enhancement of WSN lifetime.

Security threats and Malware Attack on WSN: WSN is vulnerable to many security threats and malware attacks [50, 51]. Sensor nodes are exploited due to their nature, energy constraint, limited processing capability and operational restrictions. WSN is developed to collect and process important data mostly in hostile environment such as battlefield, medical industries and logistic mobility. These data transmission is under continuous threats from illegitimate parties. Security and privacy have become important research issues and a large number of research work has been proposed to provide solutions. These attacks are under continuous evolution but some common threats for sensor nodes such as malware attacks, congestion, and denial of service are still big challenge. Sensor nodes has limited network coverage so WSN uses multi-hop communication [52] in order to increase transmission capability. Remote location connectivity makes it prone to security threats. WSN are useful for applications and services require critical data collection using limited resources so security threats further burden the system and reduces the performance of WSN.

Security and privacy are challenging topics and finding a fruitful solution is always an effort demanding task. WSN is struggling with novice security threats and each time new threats are having edge to old attacks and existing security solutions. No solutions are permanent and nothing can guarantee for full system protection. So, continuous research is needed in field of WSN to tackle the demand of secure solutions. Some security threats are new in nature and have no clue from past attacks. They demand completely new strategies based on new approaches. In this thesis three epidemic models have been proposed taking in account of various WSN aspects. The proposed models analyse the transmission dynamics of malware in WSN. In this thesis, we are proposing three mathematical model as solutions for different kind of security threats in WSN which can deal with changing pattern of security threats.

1.6 Network Security Threats and Malware Transmission in WSN

WSN is significantly incorporated in applications related to individuals and society. It is used to provide ready to use, efficient, reliable and secure communication medium for military application, agriculture applications, and natural disaster relief operations. WSN applications are finding its way to a wide range of applications addressing individuals, society and nations. WSN is a cost-effective solution for data transmission but its limited resource constrained has made it vulnerable to security. Security threats in WSN is a challenging area of research. Traditional wireless network is different from WSN in resources management, distributed architecture and limited communication. These factors make it security in WSN more challenging. Security analysts continuously provides solutions for different types of threats [53]. Still attackers find the loophole into the network and exploit it to infect the sensor nodes. The sensor nodes are affected from software bugs vulnerability. These software bugs exposed sensor nodes to security threats and possible door to worm intrusion.

The various types of security threats face by WSN due to attack of malware. Therefore, efficient security mechanisms are required to secure WSN due to attack of malware. The applications of WSN are increasing day-by-day so, security [53-58] of WSN has become an essential need. The foremost goal of WSN security is to realize confidentiality, authenticity, integrity and availability of the various forms of information [59-60]. For the purpose of data collection WSN can be deploy anywhere due to its flexible and adaptive nature as well cost effective. Whereas data protection in WSN is one of the tedious jobs in comparison to wired communication. WSN suffers from jamming and various kinds of Denial of Service (DoS)

attacks [61]. The traditional protection methods for WSN malware attack are not sufficient due deployment in hostile and unattended environments. Security of WSN is more challenging compare to their counterparts. Network security solutions developed for traditional network is not effective for WSN due to its openness and working in hostile environment.

Malware Transmission in WSN: Malware attacks is one of the most common attacks on WSN in which the malicious code is injected to sensor nodes [62]. It is one of the reasons for numerous types of attacks and malware can differ in their structure. So, effective solutions need to be updated regularly to cope with the malware. Network resources is unnecessary utilized and processing capability exploited which result into degradation of network performance quality. WSN comes with limited resources and malware attack can degrade performance drastically. Wireless network constraints make it vulnerable and easy target of malware attack [63]. Network security provides authentic access of messages or resources, reliable data transmission, and confidentiality. Malware attack breach authenticity and data transmission reliability. Sensor nodes can be easily targeted by intruders through virus, worms or malicious codes [64-65]. WSN can be deployed in any physical environment as cost effective data transmission. Applications of WSN increasing day-by-day and scope of attack is also increasing.

Malware nodes can disrupt the communication losing data packets and diverting them to illegitimate location. Multi-hop communication can increase the phenomenon due to their communication behaviours [66]. An infected node can affect the nearby nodes and infection can be progressed throughout the network [67, 68]. An infected network cannot be trusted to data transmission and critical applications cannot be deployed on infected WSN. Malware identifies vulnerability in sensor nodes and exploit it to get access into the network. If malware inserted into one node, then it can transmit to entire network. So, entry point node vulnerability overcome is very important to secure to stop malware from inserting into network. It is difficult to detect infected nodes in large network and identification of nodes is tedious task. Study of malware and its transmission into network require study the malware types, behaviour and network properties. Security of WSN is challenging due to nodes mobility, nodes distribution, nodes coverage and connectivity. And it has become more challenging due to variation in malware attacks.

The packets of data may be loss in transmission between the sensor nodes or between sensor nodes and sink node due to malware attacks [69]. A sensor node of WSN is infected by malware after that infected node starts to transmit the malware in the complete network through neighbouring sensor nodes. The confidentiality and stability of WSN get affected due malware attacks [70]. The transmission control of malware in WSN is one of the tough tasks. Therefore, research on malware transmission in WSN is considered to be one of the essential keys to comprehend WSN security. The attack of malwares in WSN is perilous for confidentiality, authenticity information integrity and availability [71-72]. The consumption of energy is also one the problem in WSN and consumption of sensor nodes' energy increases with attack of malware [73-74].

Malware transmission is affected by the various factors [68,75]. So, identification of factors that affect the malware transmission is essential and accordingly provide solutions to prevent transmission of malware in WSN is important research areas. The attacker targets the sensor nodes and install malware to capture network information, exploit network resources. This is a question how to provide sustainability of network against these kinds of attacks. The nature of malware transmission in WSN is similar to the virus transmission in population. Therefore, apply the approach of epidemic modeling to provide the solutions of addressed issues in the thesis. Epidemic modeling is a part of mathematical modeling. Mathematical modeling plays an important role in development of the solutions against dynamic transmission behaviour of malware in WSN [76].

1.7 Mathematical Modeling

The "modeling" word is derived from a Latin word "modellus". Mathematical modelling describes real world problems in mathematical forms for better analysis and effective solution generation. Real world problem is identified, converted into the mathematical problems, generating real world solutions under certain conditioned. Mathematical tools are effective to understand facts, perform analyse and justify facts the technical problem in mathematical domain with scientific investigation. Mathematical modelling is used to solve complex problems which is not feasible for existing model due to their expensive solutions. It can provide cost effective solutions with minimum resource requirement. In mathematical modelling, real world problems are stated as variables and these variables can be represented

as parameters. Mathematical models are used in various application areas of engineering, science and technology. In figure1.3 [77] the steps of mathematical modeling are represented.

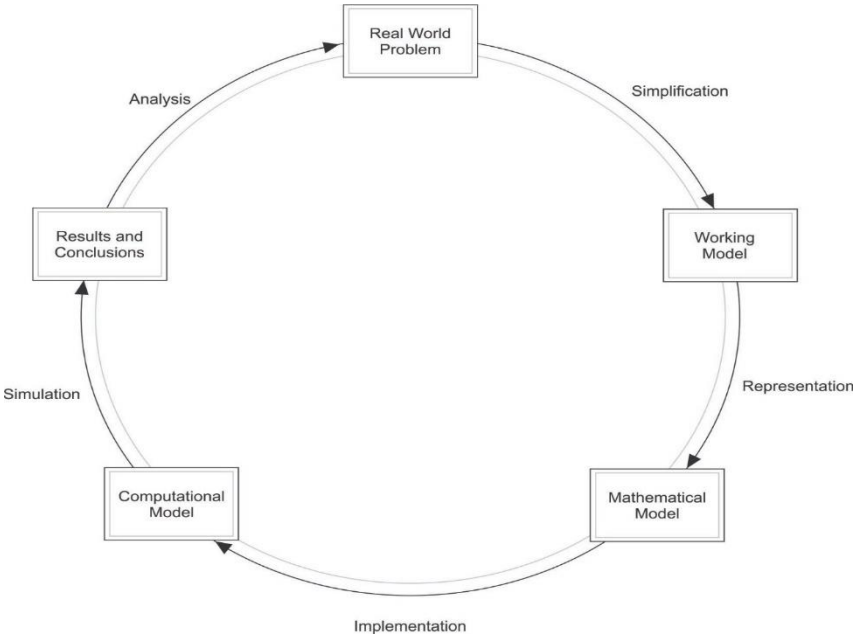

Figure 1.3: Formulation steps of real-world problem

In recent decades, computation capability has grown tremendously which favoured high end computing techniques. Mathematical modelling involves computation techniques to solve complex and lengthy real-world problems. Network behaviour is analysed using mathematical model such as nodes mobility, data transmission, data traffic, routing protocol, energy consumption, network deployment and transmission delay etc [78-83]. Mathematical model parameters are verified in simulated environment. Simulation environment is useful for comparing different models. Existing models have their discrepancy and vulnerable to network attacks. On the basis of this study, some new models can be developed to overcome the problems of existing models such as malwares attack, energy consumption, network connectivity and network coverages, bandwidth utilization, node deployment etc. In this thesis **three** mathematical models based of **epidemiology** have been developed, and investigated the transmission dynamics of malware in WSN under different conditions. Mathematical Modeling is useful for the analysis of real-world problems under the given constraints and provide solutions according to conditions. The model helps in the analysis of the system behaviour.

1.7.1 Epidemic models and its applications

The dynamics of communicable disease spread in the demography of population is described with the help of epidemic theory. Using the concept of epidemic theory, developed mathematical models that explains how a communicable disease spreads in the entire population. The models developed which is based this theory investigate the risk level of the communicable disease spread. The risk is connected to susceptibility for a disease by an entity in population. Infection rate, exposure and frequency of occurrence are primary factors that contribute to epidemic behaviour.

The concept of epidemic modeling is used in WSN to investigate the transmission dynamics of malware. It describes propagation of event in demography of sensor networks and these events pertains risk behaviour in part or entire wireless networks. Risk level analysis is important in order to assess how much particular events is decimated. The risk level of nodes depends on various factors like rate of infection, exposure to external factors, workload and etc. these factors can increase vulnerability of nodes and risk factors of network is very high.

The basic epidemic model can be represented as susceptible-infectious, susceptible-infectious-susceptible, and susceptible-infectious-recovered. In susceptible-infectious mode (SI), nodes are categorized as susceptible or infectious nodes. Infectious nodes are not contacted by malware but susceptible nodes get infected after comes in contact by malware and remains infectious lifetime.

Another epidemic model is susceptible-infectious model (SIS), susceptible nodes state becomes infectious states upon malware attack and they can revert back to susceptible state by processing with antimalware. In susceptible- infectious-recovered model (SIR), nodes state can be into susceptible state, infectious state and recovered state. A nodes state change from susceptible state to infectious state upon contacting infected nodes. An infected nodes can be recovered into recovered state which is not possible previous mentioned models. It is difficult to permanently immunize all nodes from being get infected. In wireless network, numerous models have been used to study the propagation and behaviour dynamics of malware propagation. An infectious disease transmission into populations has challenges. Its ability to invade population has been topic of research and continuously adopted in different disease

identification and controlling strategies. Disease free equilibrium (DFE) is a state defined for disease absence in population in epidemiological models. Basic reproduction number value is used to define stability of the system. If Basic reproduction number value exceeds certain threshold, then system will be unstable with more infection possibility [84].

Malware propagate epidemically in the network. So epidemic modeling is adopted to study malware propagation in social networking [85-86], computer networking [87-88], IoT [89-90] and WSN [67,68,73,74]. Efficient mechanisms are required to prevent malware propagation from infected nodes in WSN. Malware propagation follows epidemic nature in propagation so epidemic model are important to find the traits of malware transmission. Numerous research works has used epidemic models as solutions to limit the impact of malware propagation in WSN. Malware has irregular and complex propagation behaviour so it is required to research new approaches to handle newer way of malware propagation and disinfection of infectious nodes.

Sensor nodes are vulnerable to malware attack due to its vulnerability, so when nodes contact any malware attack it becomes hotpot to spread the malware throughout the network. Malware attack exploits the software vulnerabilities of sensor nodes to fetch confidential information by avoiding the existing security techniques. Mathematical modeling is being used to describe analysis of malware transmission in WSN. A number of mathematical models has been proposed and developed using epidemic theory. These models presented their view about s malware transmission in WSN and presented solutions for controlling the malware transmission.

1.8 Motivation

Security of WSN due to malware attack is one of the important concerns. The malware targets a sensor node of WSN after that begin to transmit in the entire network. The nodes of WSN loss its energy and becomes dead due to malware attacks. In this condition WSN will not execute the task effectively. Hence, in this case WSN fails and stop communication between the nodes. Due to network failure some problems occur such as data collection, decision-making, accuracy of information and loss of money in some cases. There are various applications such as smart city, smart operation of machine in industry, in medical science, transportation, offices, medical health care, safety of public, management of infrastructure,

agriculture and environmental monitoring etc. of WSN; hence it is important to prevent malware transmission in WSN.

The emerging technologies such as Internet of Things (IoT), Industrial IoT (IIoT), industry 4.0 etc. are using WSN. WSN is an intelligent network, which has ability to identify, observe and understand the phenomenon of real world. Now sensor node has become an integral part of technology and world is moving around the technology. And people are relying on technology. Therefore, security of WSN from attacks of malware is an indispensable requirement. Hence, it is important task to understand the transmission dynamics of malware in WSN. The transmission dynamics of malwares in WSN is very intricate, thus it is not an easy task to understand. The mathematical modeling is an important tool to understand the behaviour of malware transmission dynamics. The traditional security mechanisms for WSN protect due to malware attack is not efficient, because they possess the following limitations.

- Sensor node is a resource limited device having restricted capacity for example computation capability, energy, communication range and memory.
- WSN is a wireless network which is different from traditional types of wired network. WSN is deploy in unidentified or hostile field. Therefore, the sensor nodes of WSN experiences extra physical risk.
- WSN deploys in open media environment, hence the security challenges of WSN are increased.
- Consumption of sensor nodes' battery is a crucial issue in WSN. This problem stops the communication in WSN.

The previous security methods are insufficient in regards to the issues discussed, therefore the new and innovative models are required to ensure smooth operation of the sensor network. Therefore, the mechanisms are needed to prevent the transmission of malware in WSN. The proposed models improve the WSN security against malware attack and analyse the transmission dynamics of malware. The proposed model also suggests the mechanism of charging through which supress the transmission of malware and increase the lifetime of WSN. The model also deals with multi-malware attacks.

1.9 Objective of Proposed Research Work

Now-a-days, wireless network has become an integral part of digital world. Data collection, data transmission as well as data processing have become faster and easy with development

of newer technologies. Earlier, theses task were expensive and time-consuming affairs due to the different types of intricacies associated with traditional networks. Nevertheless, these complications have been optimized with the advent of wireless communication but they experience different types of complications. Therefore, there is a need to design and develop the models which can overcome the problems in existing models and provide the improved solutions.

The followings are the objectives of proposed work:

1. The mathematical models based on epidemic models are developed which will analyse the transmission dynamics of malware in WSN. The models considered the different parameters and study their effects on the transmission of malware. Malware transmission modeling considers the real-world perspective and analyse them. This research incorporates new ideas into engineering and technology of modeling network as well as presents a potential insight for antivirus developer and network designer.
2. The concept of low-energy state and mechanism of charging have used to supress the transmission of malware in WSN and also enhance the network stability. The existence of positive equilibrium points as well as malware-free and endemic states has been obtained.
3. To identified malware presence at early stage in WSN and consequently employ the methods to thwart malware transmission. The objective is also to investigate the existence of positive equilibrium points, stability of the system under different conditions.
4. Investigate the system stability in case of muti-malware (two types of malwares) attacks. The objective of the study the multi-malware transmission dynamics in WSN and analyse the stability of the network in case of muti-malware attack.
5. The proposed models have been validated mathematically as well as with extensive simulation results. The objective is to analyze the effects of various parameters which are used in the development of mathematical models to provide protection of WSN against attack of malware and also improve the lifetime of WSN.
6. The comparative study has been carried out between the proposed and existing models.

1.10 Organization of the Thesis

This thesis work is organized into six chapters. Chapter 1 discusses the detail introduction of WSN, architecture of sensor node, communication structure of WSN, features and applications of WSN, research problems in WSN, security threats in the network and malware transmission, mathematical modelings, epidemic modeling and its applications etc. This chapter also includes motivation of the research, objectives and contributions of the thesis. Finally, the summary of chapter is presented.

Chapter 2 includes the literature reviews in the fields of WSN and epidemic models, malware transmission models in WSN, the different epidemic models and their analysis is presented, concept of low-energy state and charging method is discussed. Literature review gives the basic understanding of the modeling and their applications. The study assisted in development of the new models of this work. The literature review has been drawn the information security issues in WSN against malware attacks. Its idea has been utilized for the research work.

Chapter 3 titled 'An Epidemic Model to Analyse the dynamics of Malware Propagation in Rechargeable Wireless Sensor Network' presents an epidemic model that describe the dynamics of malware transmission in WSN. The proposed model introduced the concept of low-energy state with other epidemic states. This model also considers the method of charging that supress the transmission of malware in WSN and improve the lifetime of WSN. Stability analysis of the system has been discussed. The existence positive equilibrium points of malware-free and endemic equilibrium points of the system are obtained. The value of basic reproduction number is computed. This is one of the vital parameters that is used to analyse the system stability and malware effect in WSN. The threshold value of communication radius and node density has been discussed. Theoretical findings are proved with the help of simulation results. The developed model in this work is used for improvement of WSN stability and its lifetime. The effects of different parameters are analysed. The comparative analysis has been carried out between the proposed model and existing model.

Chapter 4 titled 'Chapter 4: Study of Malware Propagation in Rechargeable Wireless Sensor Networks: A Modified SILRD Epidemic Model'. This is an extension of the model presented in chapter 3. The proposed model includes the exposed state with low-energy state. This model helps in identification of malware presence in WSN at early time. Stability study points of equilibria of the system is obtained. Effect of charging and exposed state has discussed. Performance evaluation of the proposed model is carried out. Theoretical findings are verified with the help of simulation results. The effects of different parameters have been discussed. The comparative study has been performed between the proposed model and existing model.

Chapter 5, titled `Investigation of Multi-Malware Attack in Wireless Sensor Networks using Epidemic Model ' investigates the effects of multi-malware attacks on WSN. In this model two malwares attack in the network simultaneously is discussed, explain the prevention method through which control the transmission of malware in WSN. The impacts of different parameters on the wireless network system are discussed. Performance analysis of the proposed models has been done by the variation of parameters. The proposed models ensure effective protection against malwares attack in WSN.

Chapter 6 titled 'Conclusions and Future Scope' summarizes findings of the research presented in this thesis and future work.

1.11 Summary of the chapter

This chapter has furnished an overview of WSN and discussed the related topics which are more relevant to this thesis. Sensor node components and features of WSN are discussed. Various applications and utilities of WSNs are described. Different issues such as deployment, localization, energy consumption along with security are discussed. Concept of mathematical modeling and epidemic modeling are explained. Epidemic modeling and its applications in WSN have been discussed. The formulations of real-life problems into mathematical models are described. Motivation of present study, the research efforts made in it and the structure of thesis are briefly explained.

Chapter 2: Literature Survey

A detailed discussion on the research work presented in the form of literature survey of WSN which was much similar to the proposed approach shown in the thesis. Initially the review was done on the modelling and its utility in the design of security mechanism against the malware attacks. After this we showcase the existing models which are related to networks especially WSN and represents the various characteristics of the malware transmission and the challenges of network security.

2.1 Literature Review on WSN and Epidemic Models

During the 1980s the first practical utility of WSN was done in the field of military applications. WSN do consist of spatially distributed networks of nodes that consist of micro sensors without any fixed positions and specific design. When combined in all is known as sensor nodes or motes. Basic relevance of sensor node is that they itself are self-organizing and its purpose is to keep an eye on the events that are happening around the area. The utility of sensor is to record the humidity, movement, pressure, temperature etc., further the data is recorded by other nodes of WSN. The motes can be placed in any position. In the current trend the computing environment uses motes because of its well deserving capabilities and properties of sensor nodes. Its further utilities have been discussed in chapter 1.

Mathematical approach was performed to investigate the infectious diseases that is progressing the different peoples and it was named as **Epidemic modeling** [91-92]. This is the vital tool for having an overview over the epidemic spread, pattern of the disease, and overall study of control techniques. Over the last twenty years the economics has been involved with epidemic modelling, social science, big data technology etc. The major concept behind this modelling is the mathematical concepts. Those are utilized for observe the nature of epidemic spread and have an idea to create some policies for the control of the disease. Overall, the mathematical model focuses on the macroscopic behaviour of the spread [93].

A model was suggested by Bernoulli to investigate the effect of vaccination in view of the small pox attack [94]. In the year 1920, authors named Reed and Frost showed a model which states the disease that disburses among the population. Kermack and Mckendrick [95] suggested a mathematical approach that predicts the disease transmission among the population which later was named as Susceptible-Infected-Recovered (SIR) compartment representation. The

differentiation in this model was done on three different sets named as Susceptible, Infected and Recovered states. The Susceptible persons will be infected when come in contact with biological elements. The infected hosts transfers to the recovery state when the attached pathogens are removed from them. The three ordinary differential equations have been stated for better knowledge of the system dynamics. The various coefficients of the equations used are considered as transmission and recovery rate. The term threshold value was firstly introduced in the year 1927 which was evidently related to epidemiology. The term was also related to the basic reproduction number (R_0^{th}) first by Macdonald [96] and its necessity was showcased after the literature was published in Nature in the year 1979 by Anderson and May [97]. The basic reproduction number (R_0^{th}) is the fundamental element of epidemic theory. The R_0^{th} defined as the average number of secondary cases generated due to a single infectious host during its infectious period. The system dynamics is investigated with the help of R_0^{th}. The system stability along with worm free equilibrium and endemic equilibrium can be determined with the help of R_0^{th} [84]. The expression for R_0^{th} was derived from the system of differential equations. It was found that if $R_0^{th} < 1$, then the worm will be died out from the system, and the system becomes stable at worm-free state. On the contrary, if $R_0^{th} > 1$ then the worm will present perennially in the system, and the system becomes stabilize at endemic state. Heesterbeek [98] had done a study over the demographic idea to epidemiology. R_0^{th} was first ever used to conduct an investigation over contagious syndrome. It depicts the mathematical and philosophical views on epidemic concepts. This was also utilized for the modelling of population epidemic behavior. Kermack and Mckendrick have suggested the global SIR (Susceptible-Infected-Recovered) model that has the homogeneous distribution of population and is being randomly mixed over the fact that the chance of contacting each other is very low and equal. This study was used for the basics of compartmental models hence was important in epidemiology. For investigating global models, the concept of mathematical modelling using the differential equations were used that describes all the three compartments which shows the overall study for epidemic. This concept can be used as an alternative that focus on particular characteristic of individual population. Not only local interactions were considered but they also explain the relations with malware propagation and find different transmission and recovery rate of individuals.

The suggested models depict the different topology as each node has multiple number of neighbors as each sensor has different neighbors. The discrete mathematical tools are utilized by these models for example agent-based model, cellular automata, etc. They represent the global as well as individual behavior. But in some cases, it becomes very tuff to investigate the model dynamics in respect to qualitative properties, empirical simulation provides sufficient data for analysis of behavior pattern of the system. The topological feature can be recorded by global models that has considerations of various categories of respective individual and their contact structure. The malware propagation and topological structure helps in studying the system dynamics where the population is categories in different compartments and formulate the system based on compartmental models. For example, when one neighbor come in contact with infections then it would come under the category one-degree infectious individuals, likewise when K neighbors come in contact they are termed as K degree infectious and express as P(K) that shall determine the network types like scale free network model, random network models etc. These examples help us in predicting the mathematical models for widespread of infectious signals in different environment [99-100]. Overall, many models are existing in epidemic theory and illustrates the spreading nature such as SI(Susceptible-Infectious) model, SIS (Susceptible-Infective-Susceptible) and SIR (Susceptible-Infective-Recovered) model. Several authors have referred the epidemic theory to study domains like complex network, ICT, IOT, social and behavior science, data analytics and WSN.

2.2 Literature Review on Malware Transmission Models in WSN

The Chapter 1 deals with the significance of mathematical modeling which is helpful in analyzing the functioning of the system dynamics along with its design. In order to have a proper knowledge of the behavioral patterns of the system, it is important to find out its influencing criteria and the mathematical model is successful in doing so. This model can be used in any areas of research. This chapter mainly focusses on a crucial security matter in WSN which is the worm attacks and tries to explain the different models which deal in security issues and the methods of worm spread. The biggest danger to the network in WSN is the worm attacks [77, 101]. Also maintaining the security of the network is an issue to be dealt with. The network may be either wired or wireless. In a wireless network such as the WSN, the entire application faces trouble if the network gets disturbed. Research shows that the WSN is easily prone to worm attacks and that the worm spread is proportional to the usage

of energy. The manner in which the worm propagates in a WSN is different in comparison to those of the other networks. The approach made by the researchers for studying and categorizing the method in which the worm spreads is mentioned further [102]. The mathematical models define the ways in which the worm spreads and its behavior in WSN using SODE (system of ordinary differential equations) [67,68,73,74, 103-104].

There are other models which use delayed ODE [105]. In these models the nodes are of similar types. We need to study the nature and mannerisms of the worm spread before we can develop defensive methods for protection against worm attacks. At first, the researchers found out the features of the worm spread and by using the mathematical modeling and later based on that study they developed methods to prevent the spread. When we study the method of worm spread, it gives us an insight into how the worm can spread more in future and then it becomes easy to develop methods to stop them. Some researchers generally hover around their proposed work or at the most venture into the location of the malware. Some others may also go to the extent of finding out the cause of the malware so that a barrier against worm spread could be developed. These models can help us assess the important features of worm spread. Till date many models have found out the methods in which the worm spreads and the instruments which spread them and also how this spread can be stopped. But the engendering of the worms is yet a matter of research. A detailed study of how a worm spread is caused should be attempted. We should also try to reduce the effect of the worm attacks. It is imperative to also study the major restrictions of the propagation models which can help in knowing the spreading behavior and habit of the worms so that a proper protection method can be devised.

Many surveys [106–108] have been put forth by the researchers where the worm spread and how to detect and stop the spread is discussed. Though a comprehensive comparison and classification of the models has not been attempted. One of the survey papers on worm spread in WSN and modeling made a comparison between the various propagation models based on two different ways of worm spread. For studying the spreading behavior of the worms in the network, various topologies have been used. The researchers found various models which could study the malware spread behavior and they studied the result of each model.

A crucial topic for research has been the Malware spreading in WSN and many researchers have given various findings on safety [109-110] of the WSN against malware attacks. The security of WSN is crucial as the data gathered by the sensor nodes can be very important and sensitive. When a network is attacked by the worms, it is a matter of great concern. There are

many attackers who want to destroy the security of the network and so they deploy malefic signals in the network. The main reason behind these malware attacks is that the attackers want an access to the system or they want to financially cripple the system. The example of such an attack is the first worm transplanted into the network which was named Morris and which could invade the entire computer system and spread in the entire network. The feature of the worms is to make a duplicate of its own or to multiply and then propagate on its own. As it can multiply and spread without the user's intervention, it is considered to be highly dangerous. This it becomes all the more important to know the spreading mannerism of the malware. A huge number of hosts fall under the category of Red Code and Slammer attacks and a lot of financial loss is borne by them as a result of these attacks. There is a method to protect the sensor node through the tamper proof hardware but this a costly affair. Actually in a wireless network, the malware attack affects the entire protocol stack and so the safety against malware attacks is inevitable. Once the sensor nodes are attacked by the malware, the malicious signals can in no way be protected by key management or cryptographic methods [27]. As these methods require a lot of computation, a lot of node energy is depleted. Despite this, the usage of WSN is widely increasing in many fields like human health monitoring, infrastructure, etc., In such areas, the malware attack or due to malefic codes financial as well as loss of life can occur. Hence the need for protection of WSN becomes important.

In WSN, the data is sent through sensor nodes to the target area in a multi-hop method. Once the malware attack occurs, the data packets are lost [69]. Therefore, during a malware attack [56] the reliability of the network has to be thoroughly checked before sending the data packets from the sink node to the source node. The injected malicious codes block the normal functioning of the sensor nodes and the network is affected. The energy used by the sensor nodes is depleted fast [27, 111]. By using the buffer flow sensitivity, the malefic codes are injected in sensor nodes of WSN. They also enlighten hop by hop self-renewal of malware dispersion in whole wireless sensor network. Diverse method was employed by the attackers to contaminate sensor nodes with help of self-propagation [112] of malware packets in wireless sensor networks by employing the memory pertaining susceptibility and disseminate mal-packet using current application codes without disruption of sensor's operations. For testing purpose, the 27-bit Mica2 sensor is utilized and with help of simulation it is observed that malware quickly spread in the whole networks or rest on the traffic prerequisites.

Epidemic theory always plays a significant role for displaying of malware spread in network. Over the last few years, epidemic modeling develops an alternative adaptable, scalable and robust techniques for recognizing of malware spread in network (computer network, ad-hoc network, wireless sensor network etc.) A substantial amount of attention was earned from researchers [113–116] due to their efficacy in study of malware conduct. Precisely, for designing of wireless network procedure. Biological models are used such as cellular signalling systems [114-118] and immune system [119-120]. The spread nature of biological worms is simlar to the computer worms [77,116, 121-123]. The malignant signals communicate with data among the nodes. There are basically two ways to know about a node. The node is recognized as "infected" once it found malignant signals with data otherwise it is supposed as "vulnerable" node. The spread of malignant signals is epidemic in nature and contamination begins to disseminate in the network in the form of chain reaction. The genuine performance of network protocol based on epidemic model realizes with help of modification in wireless networks which is presented by authors [124-125]. Venkatramanan et al. [124] while studying the time-threshold policy for a combined development model. Fluid limit was derived by them for a model and acquired relay node prime policy to deliver the imitated substance at preferred endpoint. The outcome of numerous constraints through simulation was studied by them. Chen et al. [125] established a model for controlling information spread and analytically submissive. They utilized the concept of dynamic programming for reducing the network cost of signal distribution time with SIR epidemic model.

2.3 Literature Review on Epidemic Models for WSN and their Analysis

Khayam and Radha [126] were of the view that the virus spread in WSN needs to be thoroughly examined. They also assumed that the Susceptible or Infected states of the nodes could be possible. They termed this model as the topologically-aware worm propagation model (TWPM). The susceptible nodes when in contact with the infectious node contract the infection. They also felt that the node which gets the worm payload is said to be infected and such receptions by these nodes are generally without any intention. Once infected, the nodes immediately start propagating the worms. Such a model is termed as SI model and it is widely established on epidemic diseases. If we want to find out the total number of odes in WSN, then we need to add both the infected nodes as well as the susceptible nodes. The verification of the exactness of the closed-form expression by them has been done through simulation.

The position of the channel in WSN through SI Model and the result it produces in the rate of worm propagation has been analyzed in detail. In the beginning stages, the worm propagation is very quick and this causes a sort of clogging at the routers due to the traffic created by the worms. Through this TWPM, we can get an exact worm spread model for WSN though we cannot get recover the nodes which are already infected. The method of malware propagation has been proved through differential equations and more precisely through graph theoretical model. The authors [127] went further and used a method of signal processing so that they could know about the spatiotemporal limits and also about the dynamics of the worm spread in WSN. This proposed model of worm propagation along with the physical characteristics of the data, combined to network protocol and transport, helps in knowing the spreading of the unknown malware attacks. This proposed model of TWPM clearly shows the method of calculation of the infection through the closed form result. But this model does not mention about the existing effects of recovering the infected nodes. Based on the results of the simulation, it can be clearly said that TWPM model is very effective in terms of knowing the worm spread in WSNs.

De et al. [128] specified in their research that how one infected node propagates the worms slowly in the complete sensor network. They were of the view that the nodes, which are evenly distributed or sometimes distributed in a random manner at a specified place, have a safe communication amongst each other. Before the transmission begins, the secret key is propagated to all the nodes in a random way. It is these keys that the attacker manages to get from any sensor that is targeted. He then sets up a secure communication with the neighboring nodes using those keys and also uses them towards the targeted nodes. As the communication is set up with the neighboring nodes, the susceptible nodes manage to read the malignant code and the malefic code is transferred to them. In this way the susceptible nodes are infected and the secret keys of the other nodes which are susceptible can now be got. By this method, the malefic code is spread in the complete WSN and the nodes are compromised.

The authors have given a compromised propagation model where the rate of infection and the time period of each infected node decides the worm spread. The authors took up two situations for examining the result of compromise worm spread. One was where the infected nodes could be recovered and the next was where the infected nodes could not be recovered. They felt that in a compromised situation, the infected nodes may be recovered in the network. Many methods are available to know the node recovery. One of the ways is to withdraw the earlier keys which were propagated and to make available a new set of secret keys to the nodes. By

this method of removing the compromised keys, the network can be safe. Such a method is known as Key Management Scheme. The other way of recovering the nodes is to totally remove the compromised node either by blocking them or reloading programs for node. Through this analysis, the recovery time of the infected nodes from the network was found out. This will be helpful in acting as a prevention against any epidemic which would spread. In a huge network, these verifications through simulations can be very effective. Authors have also analyzed temporal dynamic propagation.

Additionally, De et al. [129-130] recommended a common framework to examine the worm spread. Broadcast protocol such as MNP, Deluge and Trickle were applied to investigate susceptibility of broadcast in epidemic model. To understand the vulnerability of policies and to develop guard techniques against augmented virus attacks. This is vital to discover the dispersion method of these proprieties as far as their speed and accessibility is concerned. During this process, a common mathematical model was also set up, which helped investigating the malware propagation procedure cantered on epidemic theory over numerous broadcast protocols. In a static network situation, this model is fixed by the two neighboring spatial connection and the chronological circulation of dispersal procedure. They considered two conditions and consequently penned their set of disparity equations as well as elucidated the dynamics of malware spreading in WSN. First model contains two states Vulnerable and Infected and case of no retrieval. Explaining these calculations, they established that how infection spread in the network and resulting expression for rate of malware communication. Under various condition of network connectivity, this model is analyzed the information propagation. Three states such as Vulnerable, Infected and Improved state of the sensor node were measured by the second model. Resolving the equations, they derived expression for retrieval at any time *t*. The outcome of node density on the network with consideration of physical effect was studied and was found that in case of high node density more number of packets are misplaced due to crash and concealed terminal problem become very noticeable predominantly in case of Deluge protocol. However, problem like concealed terminal was not efficiently dealt by this model. This is established that when degree of network upsurges, the rate of malware propagation upsurges as well because more vulnerable nodes come under the contaminated node. On the contrary to this it is being discovered that when degree of node density is very high number of packet crash increases and dispersal rate of malware decreases. It was presumed by the authors that sensor nodes are every time in working mode and it was not considered by them that node status as sleep (maintenance) mode and working mode.

The idea was inked by Tang and Mark [131] of working and sleep of mode of sensor node and suggested a model on the basis of epidemic theory known as modified SIR with maintenance (SIR-M) and elucidated the malware dispersion in WSN. Dispersion dynamics of virus in respect of space and time was examined by the SIR-M model. Firstly, all the nodes of WSN goes to susceptible class of nodes, virus infects one node of WSN, and then infected node spreads the virus in the complete network via neighbor nodes. The spreading conduct is gentle towards the energy drop and network topology. Infected node spreads the malevolent signals to those susceptible nodes which lies in the range of its spread. Malware attacks on nodes consumed energy and decrease lifetime of sensor networks. The maintenance mechanism concept is presented for wireless sensor networks using SIR-M model that boosts the anti-virus ability against virus attacks and diminishes the infected number of nodes. This study contemplates the transition working-sleep (maintenance) and sleep- working state. For preservation of power, the sensor node transfers into sleep mode for some time depending on WSN design. The maintenance tasks are executed during the sleep mode because node is inactive for data transmission during this period. The system maintenance programs routinely initiated during maintenance mode and check the status of nodes, those nodes which are in vulnerable or recovery state rapidly move to sleep, although infectious nodes needed more time for treatment. The portion of infectious nodes will be preserved during maintenance (depends on predefined maintenance period) mode and grew into improved nodes, and become accessible for data transmission. The anti-virus ability of network's can be significantly improved without further computational calculation, signaling overhead or information exchange and battle different types of viruses. The presented model is suitable to more broad situations, for instance, representing either information flow or a malware attacks over the several kinds of network.

The energy of single node is exhausted during information transmission between each other and become no longer alive. Wang et al. [132] presented the conception of dead node state in WSN. The proposed model is an improvement over the SIR model. An upgraded feedback variance system of non-linear dynamics has been suggested while working on the model. The model is being called improved SIRS (iSIRS) which is centered on epidemic modeling and instituted by numerous differential equations. The nodes which are considered in this model belong to one of the states among four states at a time. It being considered by them that states of nodes are as: Vulnerable, Transmittable, Recovered and Dead. Infectious node, recovered node and vulnerable node could become a dead node due to energy exhaustion of nodes. The

malware propagation process is not proficiently described by iSIRS model, particularly in enormous scale WSN. To increase lifespan of WSN, the nodes used two operational modes as sleep and active mode. Usually, they applied the concept of sleep and active interleaving scheduling method to upsurge the lifetime of WSN. But the iSIRS model did not elaborate about equilibrium points, network stability, etc. Srivastava et al. [133], emphasized these issues and figured the basic reproduction number (R_0^{th}) value for presented model. To study the system dynamics this value can be utilized. The worm available in the network or not can be figured out by the R_0^{th} . To assess the constancy of the system in both conditions endemic and worm-free equilibrium was analyzed by them while carrying out the process. The simulations outcomes authenticate the analytical study.

There are various advantage of sleep mode which were not targeted by the iSIRS model. Therefore, Wang et al established a model to conquer the disadvantages of iSIRS model by an EiSIRS (expanded iSIRS) [134] model. They exactly elucidated the spread process of malware in WSN. This model was also based on epidemic theory and for that model, they established a set of distinction equations. The obligatory situations for virus spreading in the sensor network has been theoretically attained. The EiSIRS model delivers an improved structure for designing of a secure WSN. The model was authenticated by the simulation consequences.

After a little while another SI model which was on the basis of maintenance was proposed by Tang [135-136] which had the same features as that of the SIR-M-model. In the beginning the author studied the SI model without any anti-virus and realized that the entire network stopped functioning when the malware attacks and all this starts with only one compromised node. This node which is compromised now propagates the worm in the entire network with the help of communication with its neighboring nodes. To overcome this weakness of the SI model, the author made a better SI model which could maintain the system by stimulating the not so active part of the node. This idea helped in improving the capacity of the antivirus and no further hardware modification or overhead signals were required in this method. This model gave a very exclusive solution to stop the worm spread in WSN. The author also made a study of the for the new SI model which had space and time related worm spread in WSN. The author has also made an attempt to stop the possibility of network failure if the malware attacks. The proposed model has been clearly examined through many simulations and has also proved to be of use in many types of networks like WSN, Social network and computer network. The study has also been done on the manner in which the worm spreads in WSN.

By using the maintenance method, the number of nodes which have been infected can be controlled.

Tang and Li [67] went a bit deep in their earlier work and devised a method to protect the network which was adaptive. In order to know the status of the network, the authors found out the minimal value of the nodes which were infected. The malware attack has to be prevented as they can cause a network failure. So a security against such attacks is required. The suggestion made by them was that the power of transmission to the node should be reduced and the rate of transition should be increased. The network starts failing when the value of the infected nodes is more than the threshold value. The authors suggested two adaptive ways to protect the network. The first one was that the time of operation will vary when the transition rate is altered. This method of operating is controlled by the sink nodes and the rate of infection of the virus is the base here. Such a method is termed time based network protection (TNP). The second method is based on the transmission of power to the nodes. This method is called PNP (Power based network protection). On the basis of study of both these methods, a protection against the malware attacks was developed and verified through simulations.

The projected prototype did not take into consideration the role of MAC technique opposed to malware attacks. The connection between MAC technique and malware outspread was suggested by Wang and Yuan [137]. They explained the consequence of MAC technique over malware outspread in WSN. The suggested SI prototype was applied to avert malware outspreading in WSN by application of primary features of MAC technique. In case of MAC technique, when a contaminated node transfers or expresses the information to another node, persisting nodes, those are in the transmission radius of this node, must remain inactive. Thus, amount of contamination can be decreased. They also analysis the consequence of communication radius and allocated node density.

To break the worm circulation in WSN, it is inevitable to spot the infected nodes first. Then put on precautionary instrument to break worm spread. Yang et al. [138] well-thought-out the conventional SI with varied software approach to advance the sensor network safety against worm outbreaks. The elementary notion of its process is to barrier the network into a cluster of grid cell and each cell allocated with divergent type of flash program in the way that two nearby cells do not share the flash program of similar type. A worm contaminates one cell by using the susceptibility of flash program but tough to contaminate the nearby cells as they

have divergent type of flash program. In this method, it is supposed that each type has susceptibilities but all are dissimilar to one another. This plan [139] was expanded to analyze the situations where numerous generations of software have been applied in a sensor. This scheme offers safety to the sensor networks in contrast to traditional method. But this method does not reflect how to slab the dispersion nature of worm to an excessive amount focusing on resistant nodes by selection technique.

A dissimilar *SIS* model came into sight in which to contemplate the re-contamination of improved nodes by similar kind of worm another time. This one is not appropriate to shield the nodes against worm attack. Henceforward, an improved SIS model [140] was proposed to analyze the bug dispersal behavior in the network, which was also grounded on the impression of toxicology. The viruses' outbreak on sensor nodes, and some nodes get infested then virus transmission itself to nearby nodes by transportation of normal data over conventional communication and outbreak in the whole networks in the similar way via adjacent nodes. In the projected structure every node should have antivirus software and triggered in interlude for scrutinizing and may eliminate the virus from contagious node and gets improved from contagious state to vulnerable.

The SIRD model [133] did not focus on detection of worm presence in WSN at earlier stage. The issue is considered by Biswal et al. [141] and proposed SEIRD model. The value of R_0^{th} is obtained and investigate the propagation dynamics of worm in the network. The effect of exposed state on worm propagation is discussed by them. The comparative study has been performed between SIDR model [133] and in SEIRD model, SEIRD model shows the better results. The lesser count of nodes gets infected in SEIRD.

Shen et al. [142] articulated a model which was amalgamation of game-theory method and epidemic philosophy. The advanced method described the circulation kinematics of worm in WSN. They analyzed the kinematics of the method through the collection of different calculations and involved the theory of inactive node as well as dead mode of the sensor node. The theory of different calculations was used to increase the safety of WSN under worm outbreak and protect sensor nodes energy. For scrimmaging with worm generation and strengthening of WSN accomplishment apply an approach of effective control.

De et al. [143] extend its work [128] and used instead of one kind of sensor nodes positioning theory it used two theories. It used the positioning theories both in casually and homogeneously. The uniform random distribution theory was applied in previous [128]

prototype but in stretched prototype, it measured the both positioning theories for more genuine study of worm circulation. The influence of node retrieval was examined on compromised method. The various methods were used to retrieve the compromise nodes of the method like protection or key rejection. They also accomplished the comparable study between both deployment methods and detected that team-based deployment is not as much of accessible in comparability to uniform random deployment to infestation circulation. Network accessibility also influences the contamination unfold procedure. The limited accessed range gets limited influenced in contrast to the greatly accessed range. They also introduced the idea of (R_0^{th}) in epidemic method, its reputation has talked over in chapter 1 by now. The R_0^{th} depends on the various network variables. The expression of R_0^{th} is obtained in terms of infectivity and which relies on two things; the infective duration and the infection frequency. The minimum required value of elementary duplication number is one, when its rate is more than one widespread eruption happens. The outcome based on arbitrary graph confirmed the accuracy of suggested model in respect to the minimum required value of R_0^{th} and make sure for stable communication in WSN, and apprehend the extensive outbreak of worm contamination. But writer did not observe the kinetics and the intelligence of the encroached in simulating the assail.

Pietro and Verde [144] talked over the evidence sustainability in existence of worm outbreaks in Unattended Wireless Sensor Network (UWSN) using the notion of widespread pattern. They suggested the model of two invaders and defined the sensor network actions. The conditions are formed for data sustainability in the existence of invaders. Authors also described about the enhanced application of energy and bandwidth of sensor nodes. The complication of geometric limitations (deployment area shape and communication radius) is emphasized by them and suggested effective results. They observed three diverse widespread models to analyze the data sustainability in WSN and calculated R_0^{th} for all suggested models. One of the salient queries is that how to enhance the sensor network sustainability under worms' outbreak. Aliberti et al. [145] observed *SIS* model and applied the idea of [144] and enhanced the data sustainability even in the existence of worm outbreak. They described the barter amongst three characteristics resources utilization, accumulating time and information sustainability. For advancement of WSN lifespan, the prearranged master-plan of on/off was applied. Various devices have been utilized to secure WSN in oppositions to the different kinds of outbreaks. Some devices are as node restrain, outbreak-flexible data aggregation

[146], contradicting in opposition to routing protocols, MAC layers' outbreaks, channel blocking etc.

A SIRS prototype with some advancement was given by Feng et al. [147] for the analysis of incremental outspreading nature of malware in WSN. In this analysis, they reviewed three aspects which can influence the transmission nature of malware in WSN. These aspects are (i) communication range (ii) node concentration and (iii) power application. The vulnerable node is out broken by malware and transformed into transmissible node with period. The transmissible node begins to contaminate nearby nodes which comes under the radius of communication range of transmissible node. They advanced an approach to pinpoint malware presence in WSN by connecting sensing tool with sensor nodes. The contaminated nodes get signal from malware and transform into improved kind of nodes. The persistent protection is not feasible in the cybernetic world. Some improved nodes transfer into vulnerable condition again as a consequence of losing protection or maybe any other kind of worm impression in the network. The expression of R_0^{th} is gained that assists in study of spreading pattern of worm in WSN. The value of R_0^{th} is subject to the network's constraints. It is noticed that if the value of $R_0^{th} < 1$ the malware can be eradicated from the network and if value of $R_0^{th} > 1$ the malware will remain in the network frequently. The consequences of node concentration as well as communication range has been observed by them. They noticed that if these rates increase the malware multiplication value also increases. The minimum required value of these specifications had also gained. They noticed the state of malware-less equilibrium, indigenous equilibrium and steadiness of the network. This prototype was unsuccessful to sense the malware existence in the system at primary phase.

This issue was talked by Lopez et al and SEIS [148] model was suggested which describes the casual blocking outcomes in WSN due to worm circulation. The model concentrated on casual blocking appear at substantial or MAC layer and impart a system to foretell the outbreak of worm outbreak and advanced probable preventive. The R_0^{th} of model was achieved which supported in the scheming of safety device. The advanced procedure defends WSN from worm outbreak. The procedure like impairing specific nodes or put on active rout to reduce the outbreak. Ojha et al. [149] by introducing the idea of exposed state by developing SEIRS. This prototype also describes the dynamic nature of reproduction. They collated the suggested prototype with SIRS [147] and SEIS [148] and noticed that SEIRS prototype

performed one step ahead in terms of malware reproduction control. The outcome of communication range and node density has also been studied with open state. The value of R_0 of the SEIRS prototype was gained and also analyzed the threshold value of node density and communication radius. These constraints are decisive for system design. The equilibrium points were assessed. They have also verified it with the substantial simulation out comes.

Liu et al. [150] considered the case of malware mutation and proposed SEIRS model. They computed the value of R_0^{th} and obtained and invetigate the stabilities are local and global both. Optimla control mechnism kis proposed by them. Muthukrishnan et al. [151] proposed a SITPS model to reduce the spreading of malware through optimal control strategy. The mechanism suggested that the count of infection nodes can minimized. The cost of operation can also be minimized. Basically, the models are emphasis on network reliability and propagation of malware but ignore the failure of security of cascading between the information domain and physical domain as well robustness. Theses issues are addressed by Xu et al. [152] and proposed a SEIRS-F model. They analysed the connectivity of the network and system robustness when malware attack in the system. The effect of connectivity on malware propagation is studied. The robustness of the system is also analysed in the different conditions. The simulation results have been obtained to validate the study.

Mishra and Keshri [153] introduced a dissimilar outbreak model for analysis of reproduction nature of expected malwares in WSN. They studied the nature dynamics with respect to various periods and enhanced immunization state with SEIRS-V model. They supposed that in first instance all sensor nodes are unprotected against the malware outbreak. This model analysis the consequence of immunization on the WSN. The model used sleep mode for preservation of sensor nodes and enhances the antivirus capacity of WSN against various kinds of worm out breaks. Eventually it is necessary to remove the malware from the node where the immunized node may get contaminated again have interim protection limited period. The mathematical study and numerical simulation have been executed, and described the temporal and contagious process of spreading nature in wireless sensor network. The value of R_0^{th} has found and verified that if $R_0^{th} < 1$ the globally asymptotically steady malware-less equilibrium is attained and malware is estranged from the network. When $R_0^{th} > 1$, network will asymptotically steady at endemic equilibrium, and fragment of malware will exist

frequently in the network. The consequences of immunization against contagious or vulnerable class have been executed and found that safety of WSN enhanced against malware outbreak. WSN increased against worm attacks. Some shortcomings related to this model such as distribution of node density, communication radius, and energy consumption were found. Akansha et al. [103] overcame this weakness. With the help of the same (SEIRS-V) model, the network parameters like distribution of node, the range of communication, and usage of nodes' energy were included. In WSN they studied the results of these network parameters on the working of worm transmission. The value of R_0^{th} is calculated by using the set of differential equations. One of the benefits of R_0^{th} is that it aids in calculating the limit value of these parameters. The solidity of this model under different situations was researched. When a comparison of this model was done with [153] model, it was seen that this model had a better method of controlling the virus.

The concept of low energy state is introduced by Liu et al. [73] and included this sate with other epidemic state and proposed a (Susceptible-Infected-Low (energy)-Recovered-Dead) SILRD model. This model discussed the effect of charging on malicious programs. They use the concept of game theory and proposed the mechanism for controlling of malicious signal spread in WSN. Further, they extend the model and proposed ΛSILRD [154] with solar energy harvesters. The optimal strategies applied for the controlling of malicious programs spread in WSN. The strategies of different charging are applied and found that most efficient is the solar charging. The impact of various parameters is also investigated. But these models are not discussed about the basic reproduction number, stability of the network, points of equilibrium etc. Some other models which are considering the low-energy state with other state. Liu et al. [155] proposed a SIALS model and analyzed the stabilities like local and global stability of the model. The model explains the propagation dynamics of malware in WSN. They taking into account the process of charging, process of program of anti-malware activation, and the process launching malicious attack. The model discussed the effect of anti-malware state on the recovery process. They computed the value of $R_0{}^{th}$ and conclude that from analysis if $R_0{}^{th} < 1$, quickly malware extinct whereas if $R_0{}^{th} > 1$, malware exist in the system. Liu et al. [156] use SIRS traditional model with addition of low-energy state to analyse the propagation of virus in WSN. The charging delay is used investigate the

bifurcation. The local stability is studied under certain conditions. The SIIRL model proposed by Liu et al. [157] for controlling of malware propagation in WSN. The equilibrium points and base reproductive number and stability of the system in the different conditions is studied by them. A SILS model is proposed by Liu et al. [74] with consideration of charging along with process of reinfection in rechargeable WSN. The stabilities of the model are studies and equilibrium points are investigated and obtained R_0^{th}. The effect of charging on R_0^{th} is analysed. The results are validated with the help of simulation results.

2.4 Summary of the chapter

The Literature survey was propounded on related work of WSN, which is quite appropriate to the thesis. A discussion has been conducted on comprehensive applications of WSN. Mathematical modeling, specifically epidemic based models was analyzed. The main and central idea of this thesis is the epidemic modeling which has been successfully applied in WSN.This model can be applied not only to WSN but other networks as well. A detailed discussion on low- energy state and charging method and its result on malware spread has been done in this chapter. A unique exploration of how to check and control the worm spread combining the methods of epidemic modeling and charging was made. Epidemic modeling and its ideologies have also been propounded in this chapter. The chapters to follow slowly build upon the mathematical models. These models are based on the theory of Epidemics and definite models have been framed with the required solutions for the network.

Chapter 3: An Epidemic Model to Analyse the Dynamics of Malware Propagation in Rechargeable Wireless Sensor Network

3.1 INTRODUCTION

Many sensor nodes constitute Wireless Sensor Network (WSN) and the exchange of data occurs through these nodes. These nodes which are distributed in a fixed way or in a random way gather information from the environment and deliver it to the destination node. Since the sensor nodes have a limited capacity, area, memory and energy sources, the problems like energy depletion and many other issues like malware attacks and energy constraint crop up in the sensor network. Hence, preventive measures to stop the transmission of the malwares like, virus, worm, Trajan horse, etc. which attack the sensor nodes of WSN are to be taken. The sensor nodes have a weak defense mechanism and thus it is easily prone to such malware attacks. We have thereby addressed, in this chapter, the issue of energy depletion of the sensor nodes, and have come up with the proposition of a model that gives a detailed account of the malware transmission dynamics as well as energy depletion of the sensor nodes. The security issues along with consumption of sensor node's energy is a prime concern. As the malware cannot be implanted in the sensor nodes by a human, it becomes challenging to prevent the malware attack which transmits in the entire network on its own.

The malware attacks like "beauty Killer "and "Chernobyl" [158] which paralyzed the functioning of the internet services and stopped the functioning of the computer system respectively Since the application of WSN is widely used by the Internet of Things (IoT) and Internet of Vehicles (IoV) in various fields like Transportation, agriculture, Medicine, etc., the prevention of the malware attacks which can freeze the normal functioning of the WSN becomes all the more important.

Malware transmission dynamics in WSN is a contemporary research area, and is fundamentally based on the epidemic theory. Security issues and malware transmission in WSN have previously been discussed in preceding chapters. An epidemic model has been proposed now which will analyze the transmission dynamics of malware in WSN.

Security along with lifetime of WSN is one of the crucial concerns. Initially, a sensor node of

WSN is attacked by malware and then begin to transmit in the whole network through adjoining sensor nodes. Due to attack of malware malfunction start in WSN. The consequences of malware attack are, increase the consumption rate of sensor node's energy, increasing the network traffic and destabilize the network etc. Due to close similarity between biological worms and the software generated malwares [159]. The epidemic modeling is useful for investigation of malware transmission in WSN, computer network, etc.

Tang [135-136] studied the dynamics of virus spreading in WSN using modified SI (susceptible-infective) model. The comparative study has been performed between SI model and modified SI model. The anti-virus capability improved by modified SI model. Therefore, modified SI model has ability to prevent the spreading of virus in WSN. For the modified SI the explicit analytical solutions are derived. The validity of the model is verified by extensive numerical outcomes. Another SIR-M model is presented by Tang and Mark [131]. The process of virus spreading dynamics in WSN with respect to time is described by them. They studied the potential threat in WSN due to virus attack. The mechanism of maintenance has been introduced by them during the sleep mode of WSN. The model is used to prevent virus spreading in WSN. This model also considers temporal (e.g., transient responses of R(t), I(t) and S(t)) and spatial (e.g., transmission range and node density) dynamics spreading process of virus. The explicit solutions have been derived for the count of sensor nodes in different class in respect to time. They presented an extensive numerical result for validation of theoretical analysis.

Each sensor node losses their energy due to data transmission in the network and they become dead. The concept of dead state combined with epidemic theory has introduced by Wang and Li [132] for study of virus spreading dynamics in WSN. This model is an improvement over the SIR model. This model is called improved SIRS (iSIRS) model, which analyses the worm propagation dynamics with energy consumption of sensor nodes in WSN. The proposed model tried to explain the influence of energy consumption of sensor nodes on process of worm propagation in WSN. The discussed the effect of energy consumption and the network topology on worm propagation in WSN. The effect of various parameters such as communication range of sensor node, deployment area of sensor nodes and infection rate etc. on worm propagation in WSN is discussed.

However, the iSIRS model cannot effectually explain the worm propagation process in WSN with consideration of the active and sleep interleaving scheduling policy of sensor nodes in WSN. This scheduling policy is typically use to schedule the sensor nodes to lengthen the lifespan of a WSN, particularly a large size WNS.

To conquer the drawback of the iSIRS model, the concept of sleep state and active state of sensor nodes to expand the iSIRS model and the expanded iSIRS model is called EiSIRS [134]. This model appropriately describes the worm propagation process in WSN with respect to iSIRS model. The necessary conditions which decide the worm spreading conditions in WSN has been derived theoretically by them. The simulation results verify the theoretical findings. They also considered the condition of multi-worm attack in WSN and suggested that for controlling of worm propagation communication range of nodes can be adjust.

All these models are describing the process of virus spreading in WSN and for the analysis of virus propagation dynamics used differential equations. These models did not consider the method charging of sensor node. The sensor nodes cannot move into dead state directly, they move into the low-energy state before dead state. Therefore, the method of charging can be applied to improve the WSN lifetime. For charging of the sensor nodes of WSN Lei Mo et al. [160] introduced an idea of mobile charger. The scheduling technique is used to charge the sensor nodes of the network.

Liu et al. [73] proposed a noble model which is based of epidemic modeling. They introduced the concept of low-energy state and improved the basic epidemic model. The energy storage of WSN is considered. They proposed a SLLRD model to deal with dynamics of malicious program spreading in WSN and method of charging is applied to supplement the energy and suppress the spreading of malicious program in WSN. They consider the rechargeable factor to maintain the normal operation of the network. For recharging of sensor nodes use MCs (Moving Chargers) Or UAVs (Unmanned Aerial Vehicles). The game theory is applied to find the optimal control strategy to prevent the spreading of malicious program and optimize total cost. To maintain the smooth operation of WSN under different conditions some issues are not addresses by them [73] such as vital dynamics case of epidemiology, basic reproduction number which is a crucial parameter for the analysis of system stability, system equilibria, stability of the system in different conditions, effect of communication radius on malware transmission, effect of sensor nodes deployment i.e., distributed nodes density on malware transmission.

To improved description, the features of malware transmission dynamics in WSN, in this chapter, we investigate the attacking behaviour of probable malwares in WSN by proposing a SILRD (Susceptible - Infectious – Low Energy – Recovered –Dead) epidemic model with vital dynamics. In this model, the following factors are considered: (i) compute the value of basic reproduction number (ii) system equilibria (iii) stability of the system in different conditions (iv) impact of communication radius on malware transmission; and (v) impact of distributed nodes density on malware transmission. In this chapter these critical issues are discussed.

Organization of the chapter. The remainder section of this chapter is structure in the following order: Section 3.2 describes the proposed SILRD model and their assumptions. In section 3.3, discuss the existence of different types of equilibrium points and the system stability under different conditions in Section 3.4. Evaluation of theoretical findings with Simulation Results in section 3.5. An improved SILRD is discussed in section 3.6. The equilibrium points and stability study of the improved model is carried out. The impact of communication radius, node density and area of deployment on malware propagation in WSN is also investigated. In section 3.7, analysed the performance of the model with variation of different parameters. Simulation outcomes and comparative analysis between existing and proposed model is carried out in section 3.8. In Section 3.9 summary of the work is presented.

3.2 Proposed Model

To investigate the malware transmission dynamics in WSN a SILRD (Susceptible - Infectious – Low Energy – Recovered –Dead) model with vital dynamics is proposed. The model classifies the sensor nodes state are of five types. On the basis of energy level sensor nodes can be divided into two types high energy and low energy nodes. Through this model studied the malware transmission dynamics in WSN and analyzed the effects of charging on transmission of malware in WSN.

The important factors of the proposed model are:

1. The energy of sensor nodes starts to consume due to operations in WSN and they come into low-energy state from high energy. In the meantime, as some malware attacks would manifest themselves in a faster energy consumption, the introduction of a low-energy state can partially indicate the severity of the attack.
2. WSN's rechargeable factor has been taken into consideration. For maintaining the normal function of WSN the factor of rechargeable is introduced because one of the main shortcomings of WSN is limited energy, which constrained the lifetime of WSN. The sensor nodes of WSN can consume quick energy when get infected by malicious program.

Therefore, to suppress the influence of malicious programs the method of charging can be apply. For charging of sensor nodes deployment of UAVs (Unmanned Aerial Vehicles) is required. As the count of low-energy nodes decreases the operational cost of WSN increases due to deployment of UAVs.

The key contribution of the chapter is:

- Formulated a model which is based on theory of epidemics for study of transmission dynamics of malware in WSN and further suggest a mechanism for controlling of malware transmission in WSN.
- Investigate the effects of charging on transmission of malware in WSN. The method of charging and patching use to control the transmission of malware as well enhance the lifetime of WSN.
- Study the system's responsiveness and steady state, and provides the understanding of system recovery from infected state.
- Obtain the points of equilibria and investigate the proposed model's performance in different conditions.
- The stability of the system is analysed in different circumstances and validate the theoretical findings through simulation results.

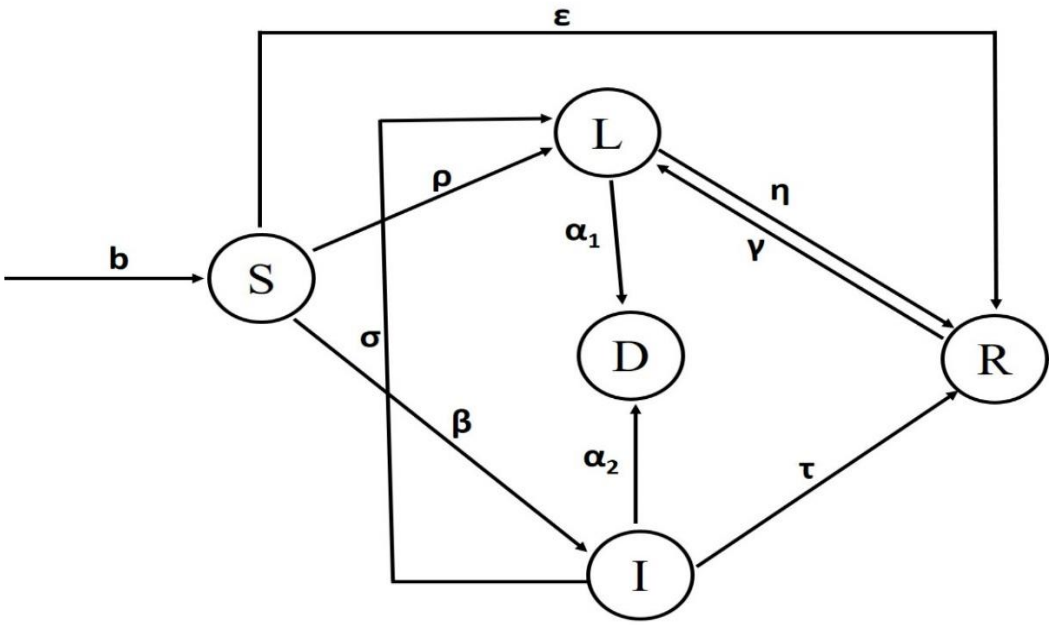

Figure 3.1: Phase change of SILRD Model

The model consists by following states:

Susceptible State (S): Sensor nodes which are uninfected from any type of malware and having high-energy level. They can execute the assigned task in the normal way but due to lack of defense mechanism they are extremely vulnerable against attack of malware.

Infectious State (I): Sensor nodes are attacked by the malware and get infected, and are capable of spreading the infection to the nearby nodes. The infected sensor nodes loss their energy at rapid rate. Therefore, charging or patching is required on time to save the sensor nodes to dead.

Low-Energy State (L): Sensor nodes when lose its energy due to operation or attack of malware. They have not sufficient energy to work in proper manner and cannot transmit data or infection to other sensor nodes.

Recovered State (R): Sensor nodes have high energy level and immune to malware attack as they have recovered from the state of infection or low-energy state or susceptible state are considered as recovered state nodes. The patching and charging take place simultaneously. These sensor nodes are immune to the relevant type of malware attack but they may not by secure against irrelevant type of malware attacks.

Dead State (D): Sensor nodes have lost their functionality completely and are incapable of transmitting the data in spite of being charged. They have not capability to infect nearby sensor nodes also.

The important reason for development of the model is to control the malware transmission as well as to enhance WSN's lifetime. The model elucidates the process of malware transmission of dynamics in WSN, the key contributions of proposed model is:

1. The proposed model investigates the process of malware transmission dynamics in WSN and helps in the understanding of transmission behaviour of malware.
2. The concept of low-energy state combined with epidemic modelling to analyse the transmission of malware dynamics in WSN.
3. To supress the malware transmission and consumption of sensor node's energy in WSN by applying the mechanism of charging and patching.
4. To study the response of system in case of malware attack and appertain the process of speedy recovery of infectious and low-energy state nodes in WSN.
5. To analyse the effects of spatial and temporal parameter on transmission of malware in WSN.

6. To analyse the system stability in different situations and substantiate analytical findings through extensive simulation outcomes.

For formulation of the model some assumptions are made. The homogeneous type of sensor nodes is scattered in an area to collect the information from the surroundings and deliverer at designated destination in single hop or multi-hop. It is supposed that initially, all sensor nodes are of Susceptible (S) state and free from malicious signals. The attacker installs a malware by targeting a sensor node of WSN. When malware installs successfully in the network then start to communicate with other nodes of the network then state of sensor nodes changes due to malware attack. The state transition diagram is shown in figure 3.1.

3.2.1 Model Description and Assumptions made in its Analysis

The sensor nodes distributed in a field in random or fix manner and their objective is to gather the data from environment. The coverage area of WSN is greater than the maximum coverage area of each sensor node. Therefore, in multi-hop transmission is needed to delivered the data at desired destination (sink/control centre/terminal computer). And distributed structure of WSN provides hotbed for transmission of malware. Moreover, due to weak defesnse capabilities sensor nodes vulnerable against malware attack. Therefore, it is essential to develop a countermeasures mechanism that can protect WSN against malware attack. Along with protection of WSN, energy consumption of sensor node is also an important issue. To keep these issues in mind proposed the model which is based on epidemiology. The proposed model consists of five states.

Below given are the assumptions made for a clear analysis of the system:

1. In the beginning, the nodes of WSN are in a state of high energy and completely free from malware attack. They are in a Susceptible state but they always stand a chance of being attacked by the malware. The attackers take advantage of these susceptible nodes and launch the malware attack here. Once attacked by the malware, these nodes use up a lot of energy and go in a state of low energy with rate of ρ. Out of these, some of the infected nodes move into a recovered state at the rate ε. The infection rate of malware is β, so the WSN's susceptible sensor nodes infected by malware is βSI.

2. The nodes which have been infected lose their energy and turn into a state of low energy (L) at the rate σ. Due to this energy draining, some nodes become Dead nodes at the rate α_2. The infected nodes move is recovered state at the rate τ. Some of these

recovered nodes may also be attacked again by malware and the energy is further depleted in these nodes moving them into a low energy state at rate γ.

3. The low energy nodes are charged and are moved into a recovered state with high energy of rate η whereas some of the nodes which cannot be charged turn into a state of dead at the rate of α_1.

4. The nodes which have been recovered are now high energy nodes and are immuned to malware attacks but not forever.

S.No.	Parameter	Meaning of the used Parameter
1.	b	Addition rate of susceptible nodes in the network
2.	α_1	Low-Energy node enter into dead node
3.	α_2	Rate at which infectious nodes destroy by malware attack and drain the energy completely move into dead state
4.	σ	Probability of infectious state nodes enter into low-energy node
5.	η	Rate of conversion of low-energy state nodes into recovered nodes
6.	ε	Probability of installation of anti-malware in susceptible nodes
7.	ρ	Probability of conversion of high-energy level susceptible nodes into low-energy level
8.	β	Probability of conversion of susceptible node to exposed node due attack of malware (rate of infection)
9.	τ	Rate of repairing of infectious nodes at high-energy level i.e. recovery rate of infectious nodes
10.	γ	Probability to turn recovered (high energy) to low energy

Table 3.1: Used parameters and their Meanings

In this model at any time t, sensor nodes in the system are divided into five states. The states are Susceptible State S(t), Low-Energy State L(t), Infectious State I(t) Recovered State R(t) and Dead State D(t).

At any time $t \geq 0$, N(t) is the summation of sensor nodes in WSN, and satisfies the conditions

$$N(t) = D(t)+R(t)+L(t)+I(t)+S(t)$$

The transmission of malware in WSN is depicted by figure 3.1, the movement of malware transmission dynamics is described below using differential equations.

$$\left.\begin{aligned}
&\dot{S} = b - \rho S - \varepsilon S - \beta SI,\\
&\dot{I} = \beta SI - (\sigma + \tau + \alpha_2)I,\\
&\dot{L} = \sigma I + \gamma R + \rho S - (\alpha_1 + \eta)L\\
&\dot{R} = \tau I - \gamma R + \varepsilon S + \eta L,\\
&\dot{D} = \alpha_1 L + \alpha_2 I,
\end{aligned}\right\} \qquad (3.1)$$

The system is defined in the domain $\Gamma = \left\{(S, I, L, R, D) \in \Re_+^5\right\}$. For the cases when $t \geq 0$ the distint parametes remain in the positive value. Durimg this phase the model observes the different sates of sensor nodes. The meaning of the used symbiol s in equation (3.1) is given in table 3.1.

3.3 Existence of Positive Equilibrium

In order to determine various equilibrium points system, we consider the first derivatives o for the complete model which is equal to zero for the value of equations (3.1).

$$\left.\begin{aligned}
&0 = b - \rho S - \varepsilon S - \beta SI,\\
&0 = \beta SI - (\sigma + \tau + \alpha_2)I,\\
&0 = \sigma I + \gamma R + \rho S - (\alpha_1 + \eta)L\\
&0 = \tau I - \gamma R + \varepsilon S + \eta L,\\
&0 = \alpha_1 L + \alpha_2 I,
\end{aligned}\right\} \qquad (3.2)$$

On evaluating the equations (3.2) we can obtain the various equilibrium points and the malware- free equilibrium (MFE) point is stated by:

$$P_0 = (S, I, L, R) = \left(\frac{b}{\alpha + \delta}, 0, 0, \frac{\alpha b}{\alpha_1(\alpha + \delta)}\right)$$

and point of endemic equilibrium is denoted as $P^* = (S^*, I^*, L^*, R^*)$, where

$$S^* = \frac{b}{(\varepsilon + \rho){R_0}^{th}}, \quad I^* = \left[\frac{b({R_0}^{th} - 1)}{(\tau + \sigma + \alpha_2){R_0}^{th}}\right], L^* = \frac{1}{\alpha_1}\left[(\sigma + \tau)I^* + (\varepsilon + \rho)S^*\right]$$

$$R^* = \frac{1}{\gamma}\left[\tau I^* + \sigma S^* + \eta L^*\right]$$

$${R_0}^{th} = \frac{b\beta}{(\tau + \sigma + \alpha_2)(\varepsilon + \rho)}$$

On solving it is clearly noticed that positive endemic equilibrium point exists when R_0^{th} value is greater than 1, and the R_0^{th} notifies the basic reporduction number[161].

3.4 Analysis of System Stability

One of the major concerns is the stability of WSN which is disturbed due to the malware attacks. In order to have a correct analysis of the stability of the proposed model. The existing theorems have been modified in order to have a perfect analysis of the stability of the system. The theorems and their proof are given for the investigation of system stability.

Theorem 3.1: The system described by the set of equation (3.1) is asymptotically stable at malware-free equilibrium (MFE) P_0, if all of its eigenvalues are negative.

Proof. Stability of point P_0 of the system is obtained by using the Jacobian matrix which helps to obtain the eigen values. The Jacobian matrix can be represented as depicted below.

$$J(P_0)=\begin{pmatrix} -(\varepsilon+\rho) & -\beta S_0 & 0 & 0 \\ 0 & \beta S_0 -(\tau+\sigma+\alpha_2) & 0 & 0 \\ \rho & \sigma & -(\eta+\alpha_1) & \gamma \\ \varepsilon & \upsilon & \eta & -\gamma \end{pmatrix} \tag{3.3}$$

Two eigenvalues of (3.3) are: $\varsigma_1=-(\varepsilon+\rho), \varsigma_2=\frac{1}{\alpha_2+\tau+\sigma}\left(R_0-1\right)$ and other two eigenvalues obtained from the roots of equation $a_0\varsigma^2+a_1\varsigma+a_2=0$, where, $a_0=1$, $a_1=(\gamma+\eta+\alpha_1)$ and $a_2=\gamma$ Since all coefficients a_0, a_1 and a_2 are positive. Therefore, it is clear that all eigenvalues obtained from the matrix are negative when $R_0^{th}<1$. So, the system is locally asymptotically stable at malware-free equilibrium (MFE).

Theorem 3.2: If $R_0^{th}\le 1$, the Malware-Free Equilibrium (MFE) point is globally asymptotically stable.

Proof. Consider the Lyapunov function L

$$L(t): R^4 \to R^+ \text{ defined by } L(t)=\omega I \tag{3.4}$$

By Differentiating the Lyapunov function L w.r.t time, and assuming ω, we obtained

$\dot{L} = \omega \dot{I} = \omega(\beta SI - (\tau + \sigma + \alpha_2)I) \leq (R_0^{th} - 1)I$, where $\omega = \frac{1}{(\tau + \sigma + \alpha_2)}$. If $R_0^{th} \leq 1$ then $\dot{L} \leq 0$ holds.

Moreover $\dot{L} \leq 0$ if and only if $I = 0$. Thus, the largest invariant set in $\left\{(S, I, L, R, D) \in \Gamma : \dot{L} \leq 0\right\}$ is the singleton set P_0. Hence the global stability of P_0 when $R_0^{th} \leq 1$ according to LaSalle's [162] invariance principle.

Theorem 3.3: The endemic equilibrium (EE) P^* is of the system will be locally asymptotically stable if $R_0^{th} > 1$.

Proof. In order to obtain the Jacobian Matrix for determining the endemic equilibrium of the system stability at the point P^*, and the said matrix is represented as

$$J(P^*) == \begin{pmatrix} -\beta I^* - (\varepsilon + \rho) & -\beta S^* & 0 & 0 \\ \beta I^* & \beta S^* - (\tau + \sigma + \alpha_2) & 0 & 0 \\ \rho & \sigma & (\eta + \alpha_1) & \gamma \\ \varepsilon & \upsilon & \eta & -\gamma \end{pmatrix} \tag{3.5}$$

Eigenvalues of (5) are the roots of the equations: $\varsigma^4 + a_1\varsigma^3 + a_2\varsigma^2 + a_3\varsigma + a_4 = 0$ (3.6)

where,

$$a_1 = (L_1 + M_1), a_2 = (L_2 + M_2 + L_1M_1), a_3 = (L_1M_2 + L_2M_1), a_4 = L_2M_2$$

$$\left.\begin{aligned} L_1 &= \eta + \alpha_1 + \gamma, \\ L_2 &= \gamma\alpha_1, \\ M_1 &= (\varepsilon + \rho + \tau + \sigma + \alpha_2) + \frac{\beta b}{R_0^{th}}\left[\frac{(R_0^{th} - 1)(\varepsilon + \rho) - (\tau + \sigma + \alpha_2)}{(\tau + \sigma + \alpha_2)(\varepsilon + \rho)}\right], \\ M_2 &= (\varepsilon + \rho)(\tau + \sigma + \alpha_2) + \frac{\beta b}{R_0^{th}}\left[(R_0^{th} - 1)\right]. \end{aligned}\right\} \tag{3.7}$$

It is clear that all a_1, a_2, a_3, a_4 are non-negative if $R_0{}^{th} > 1$, by a mathematical computation $G_1 = a_1 > 0, \quad G_2 = a_1 a_2 - a_3 > 0, \quad G_3 = a_3 G_2 - a_1^2 a_4 > 0,$ and $G_4 = a_4 G_3 > 0$. Thus, as per the rules of Routh Hurwitz, equation (3.7) will generate the value of all the roots with non-positive real parts. Thus, when $R_0{}^{th} > 1$, the locally asymptotically stable endemic equilibrium (EE) P^*.

3.5 Evaluation of theoretical findings with Simulation Results

In this section, the theoretical findings have been verified by simulation results. For the same, MATLAB (R2018a) software has been used. For mathematical analysis the value of different parameters are: $b = 0.35, \beta = 0.0001, \alpha_1 = 0.0001; \alpha_2 = 0.002, \rho = 0.007, \gamma = 0.002, \tau = 0.009,$ $\eta = 0.003, \sigma = 0.008, \varepsilon = 0.0004.$ Assume that the count of sensor nodes in the various state at time t=0 is S (0), I (0), L (0), R (0) and D (0) be 999, 1, 0, 0 and 0 respectively. The movement of malware dissemination in WSN has been brought out in the figures 3.2 and 3.3. When the nodes move from one state to the other, changes occur and these changes in respect to time (t) are shown clearly in the figures 3.2 and 3.3.

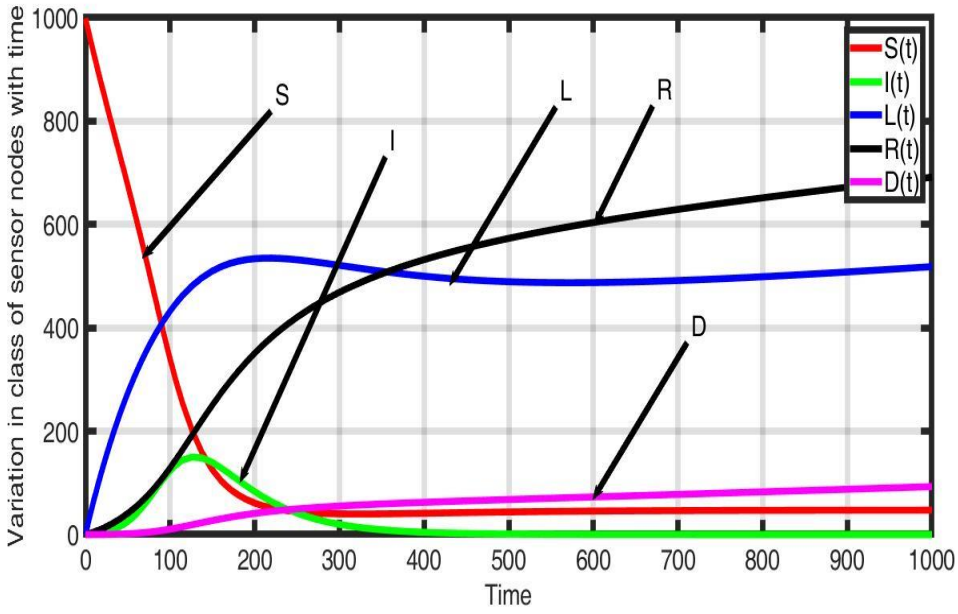

Figure 3.2: Transmission dynamics of malware when $R_0{}^{th} < 1$

Figure 3.2 shows in the variation of sensor nodes count with respect to time when $R_0^{th} < 1$ ($R_0^{th} = 0.2489$). The count of sensor nodes is increasing in all classes but deceasing in susceptible class of sensor nodes in the beginning. Subsequently infected count of sensor node starts to decrease and become zero after some time. In this situation the malware is no more present in the system as it is dead. In this condition model may show oscillations in the count of recovered, low-energy and susceptible nodes specially in the initial stage of attack, it succeeds to steady swiftly. Hence the condition of theorem 3.1 and theorem 3.2 are fulfilled. However, the counting of dead sensor nodes is linearly increasing because exhaust of node's energy or letdown of hardware/software.

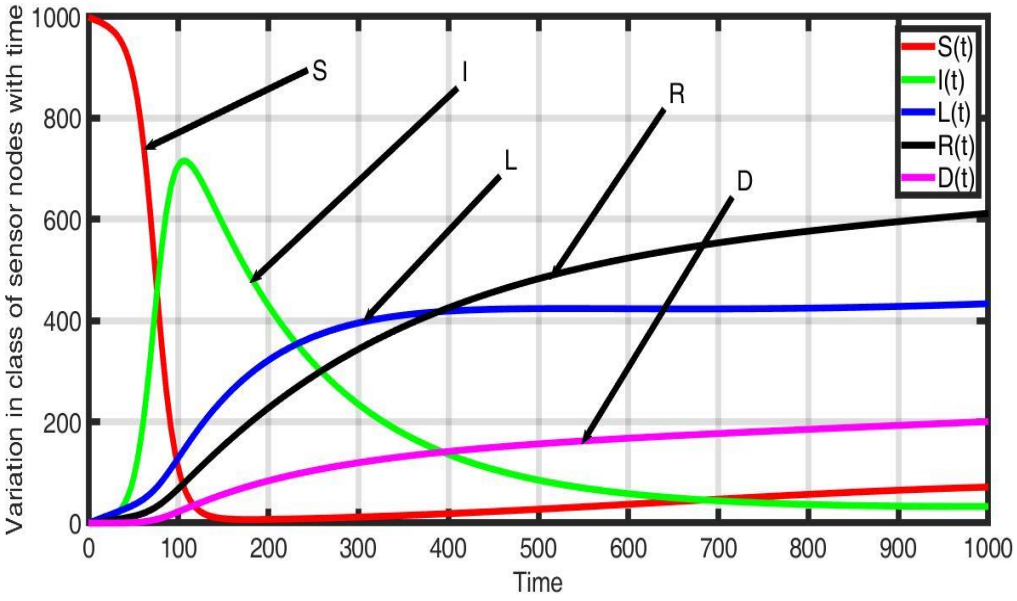

Figure 3.3: Transmission dynamics of malware when $R_0^{th} > 1$

The value of some parameter changes which are $\sigma = 0.004, \varepsilon = 0.0002$, $\alpha_2 = 0.001, \tau = 0.002$. From Figure 3.3, it is clear that the count of infected nodes first rises rapidly and then after reaching the zenith, it starts to decline and then stabilizes with time when $R_0^{th} > 1$ ($R_0^{th} = 5.55$) greater than 1. This endemic state is also proved in the theorem 3.3. According to this theorem, the malware be present in the system continuously.

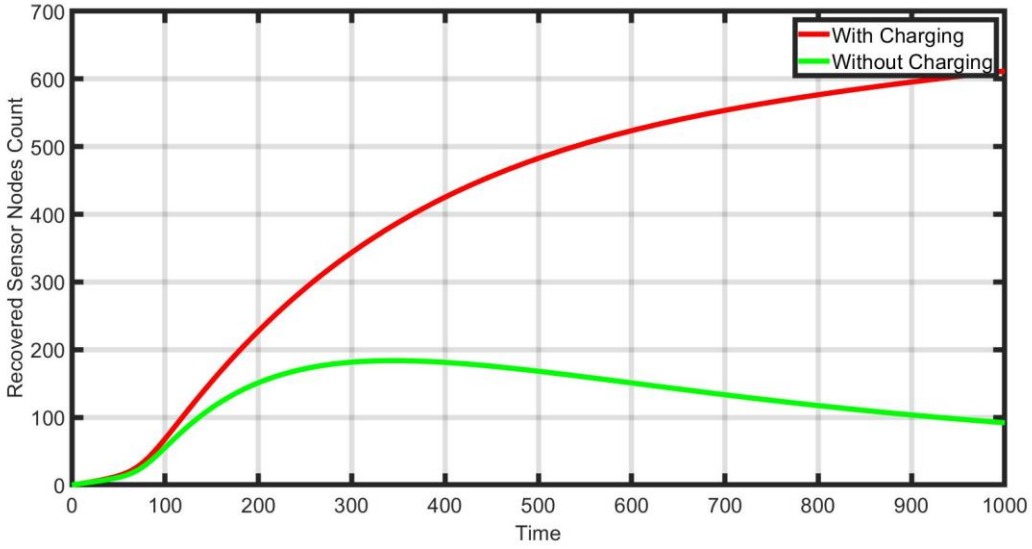

Figure 3.4: Comparison between charging and without charging

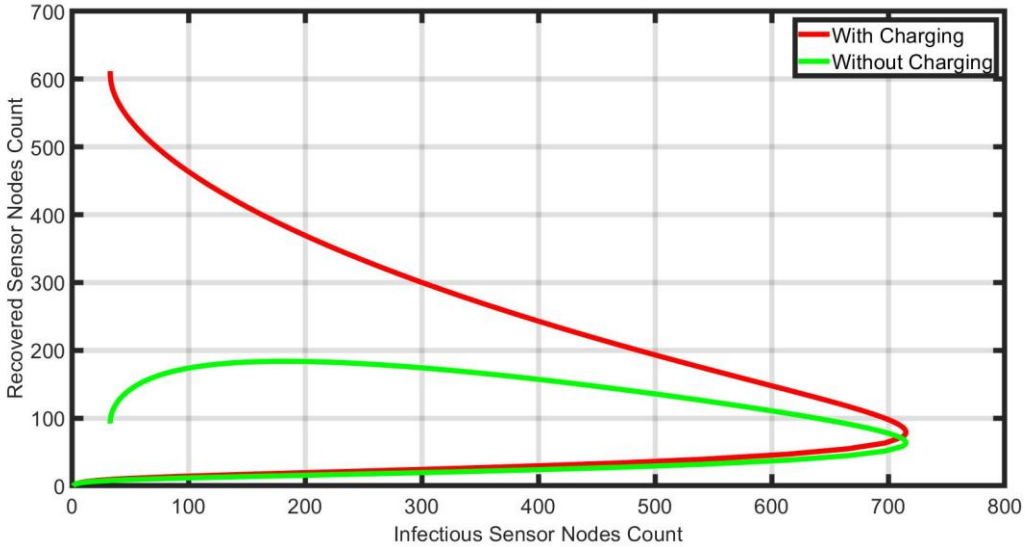

Figure 3.5: Comparison between charging and without charging

Figure 3.4 and 3.5 depict the effects of charging on malware transmission. It is noticed that when the nodes are charging many nodes recovered when compared to the nodes when not charged in similar conditions. In case of charging infected count of nodes decrease in respect to without charging which is shown in figure 3.5. This clearly demonstrates that charging the sensor nodes is an effective method to supress the malware transmission in WSN.

3.6 Improved SILRD Model

The mechanism of malware escalation in WSN is represented in the above-recommended model. Stability of this model and the effect of charging on malware transmission has been also analyzed. The prime objective of the recommended solution / model is to restrain malware

from the network, sustain network stability and enhancement lifespan of WSN. But the model did not discuss about coverage and connectivity of network and their impact of transmission dynamics of malware in WSN. Therefore, to analyze the impact of coverage and connectivity on malware transmission in WSN proposed an improved SILRD model.

The sensor nodes are identical and scattered uniformly a space of two-dimensional having the length l. Therefore, the total area $A = l^2$, in which the sensor nodes are installed. Assume that the total number of sensor nodes are N and installed in the area of A, then the average distributed node density $d = \frac{N}{A}$. Each sensor node having the communication radius r, which is installed in the area of A. Thus, the area covered by each sensor node is πr^2. The area covered by a sensor node specifies that a sensor node can connect to all those nodes which are within their coverage area. The sensor nodes sense the event in their nearby area and gather the event data first and then communicate to the destination node (sink node) in single hop or multi-hop. To begin with, suppose that all nodes are susceptible and possibly could be attacked by malware.

In this study, it is assumed that at any time t, total count of sensor nodes are $N(t)$ which are scattered in the area of A, and susceptible count of sensor nodes are $S(t)$. A sensor node having the communication radius of r and its coverage area is πr^2.

Therefore, in per unit area density of susceptible nodes

$$d(t) = \frac{S(t)}{A} \tag{3.8}$$

Area of a sensor node communication

$$A_r = \pi r^2 \tag{3.9}$$

Total number of sensor nodes which are withing communication area of a susceptible sensor node

$$S'(t) = A_r d(t) \tag{3.10}$$

From equations (3.8) and (3.9) substitute the value of $d(t)$ and A_r in equation (3.10), we get

$$S'(t) = \pi r^2 \frac{S(t)}{l^2} \tag{3.11}$$

To have better understanding, the sensor node's transition phases are shown in the figure (3.1) by considering all nodes are homogenous. The differential equation may be used to describe

malware transmission dynamics in WSN. So, as per relationship of state transition in figure 3.1, malware transmission in WSN can be derivative as follows:

$$\left.\begin{aligned}
&\dot{S} = b - \frac{\pi r^2}{l^2}\beta SI - \varepsilon S - \rho S,\\
&\dot{I} = \frac{\pi r^2}{l^2}\beta SI - (\tau + \sigma + \alpha_2)I,\\
&\dot{L} = \sigma I + \gamma R + \rho S - (\alpha_1 + \eta)L\\
&\dot{R} = \tau I + \varepsilon S + \eta L - \gamma R,\\
&\dot{D} = \alpha_2 I + \alpha_1 L,
\end{aligned}\right\} \qquad (3.12)$$

Substitute $\xi = \frac{\pi r^2}{l^2}\beta$ for convenience in the system of equation (3.12) then the system of equation may be written as:

$$\left.\begin{aligned}
&\dot{S} = b - \xi SI - \varepsilon S - \rho S,\\
&\dot{I} = \xi SI - (\tau + \sigma + \alpha_2)I,\\
&\dot{L} = \sigma I + \gamma R + \rho S - (\alpha_1 + \eta)L,\\
&\dot{R} = \tau I + \varepsilon S + \eta L - \gamma R,\\
&\dot{D} = \alpha_2 I + \alpha_1 L,
\end{aligned}\right\} \qquad (3.13)$$

3.6.1 Existence of Positive Equilibrium

In the system of equation (3.13) the first four equations do not contain the D state. It shows that the first four equations do not dependent on the fifth equation. Hence, to determine the points of system's equilibria equate the derivatives of first order of equations of the system to zero.

$$\left.\begin{aligned} 0 &= b - \xi SI - \rho S - \varepsilon S, \\ 0 &= \xi SI - (\alpha_2 + \tau + \sigma) I, \\ 0 &= \sigma I + \gamma R + \rho S - (\alpha_1 + \eta) L, \\ 0 &= \tau I + \varepsilon S + \eta L - \gamma R, \end{aligned}\right\} \qquad (3.14)$$

To obtaining the points of system's equilibria solve the equation (3.14) and computed malware-free equilibrium (MFE) point is: $P_0^{MFE} = (S_0, I_0, L_0, R_0) = \left(\frac{b}{\varepsilon + \rho}, 0, 0, \frac{\varepsilon b}{\gamma(\varepsilon + \rho)} \right)$

3.6.2 Malware Endemic Equilibrium: Existence and Uniqueness

The uniqueness and existence of the endemic equilibrium (MEE) point is determined through the equation (3.15) .

$$\left.\begin{aligned} 0 &= b - \xi S^* I^* - \varepsilon S^* - \rho S^*, \\ 0 &= \xi S^* I^* - (\tau + \sigma + \alpha_2) I^*, \\ 0 &= \sigma I^* + \gamma R^* + \rho S^* - (\alpha_1 + \eta) L^*, \\ 0 &= \tau I^* + \varepsilon S^* + \eta L^* - \gamma R^*, \end{aligned}\right\} \qquad (3.15)$$

Point of malware endemic equilibrium (MEE) P^{*MEE} is obtained by straight-forward computation

$$S^* = \frac{b}{(\varepsilon + \rho) R_0{}^{th}},$$

$$I^* = \left[\frac{b(R_0{}^{th} - 1)}{(\tau + \sigma + \alpha_2) R_0{}^{th}} \right],$$

$$L^* = \frac{1}{\alpha_1} \left[(\rho + \varepsilon) S^* + (\sigma + \tau) I^* \right]$$

$$R^* = \frac{1}{\gamma} \left[\varepsilon S^* + \tau I^* + \eta L^* \right]$$

where $R_0{}^{th} = \frac{\xi b}{(\tau + \sigma + \alpha_2)(\varepsilon + \rho)}$ is the basic reproduction number [161]. If $R_0^{th} > 1$, then the malware endemic equilibrium (MEE) point P^{*MEE} will exists and unique.

3.6.3 Evaluation of theoretical findings with Simulation Results

To study the transmission dynamics of malware in WSN, it is necessary to compute the value of R_0^{th}. The theoretical study of R_0^{th} has already been done. On the basis of R_0^{th} value

analyses that the status of malware in the system. From theoretical study, it is found that if the value of $R_0^{th} < 1$, malware vanishes from the system and infectious nodes will not exist in the system; whereas if $R_0^{th} > 1$, malware persist in the system and infectious nodes will be present in the system. The theoretical findings verified through simulation results. In case of malware-free condition the value of R_0^{th} ($R_0^{th} = 0.644.$) which is less than 1. This satisfies the condition of theorem 3.1 and theorem 3.2. In case of endemic equilibrium, the value of R_0^{th} ($R_0^{th} = 3.847$) which is greater than 1. In this case, malware persists in the network and system exists in endemic equilibrium, which fulfils the conditions of theorem 3.3, on analyzing the transmission dynamics of malware in WSN by taking into account of different parameters simultaneously. Simulation has been performed to study the impacts of different parameters. Outcomes of all these findings are discussed in in following sections.

3.6.3.1 Impacts of Communication Radius of Node (r) on Performance of the System

The communication radius is associated with $R_0{}^{th}$ and its value is given as

$$R_0{}^{th} = \frac{\pi r^2 b\beta}{(\tau + \sigma + \alpha_2)(\varepsilon + \rho)l^2} \tag{3.16}$$

To obtained the threshold value of communication radius (r_{th}), puts the value of $R_0{}^{th} = 1$ in equation (3.16), we get

$$r_{th} = l\left(\frac{(\tau + \sigma + \alpha_2)(\varepsilon + \rho)}{\pi\beta b}\right)^{1/2} \tag{3.17}$$

The different parametric values are taking into account as : $\varepsilon = 0.0006,\ l = 12, \alpha_2 = 0.0015,$ $r = 0.9,\ \rho = 0.0008, \tau = 0.007, \gamma = 0.003, \sigma = 0.006,\ b = 0.37, \beta = 0.002$ $\eta = 0.004, \alpha_1 = 0.003$ putting these values in equation (3.16) the computed value of $R_0{}^{th} = 0.644.$ and obtained the threshold value of communication radius $r_{th} = 1.122$ from equation (3.17). The value of $R_0{}^{th}$ is changing with change in the value of r, initially at

time $t = 0$, assume the count of different class of nodes are S (0), I (0), L (0), R (0) and D (0) be 999, 1, 0, 0 and 0 respectively. The simulation results are illustrated in the figures 3.6 (a-d).

Case 1: If $r \le r_{th}$ then $R_0^{th} \le 1$ [103,147], the malware-free equilibrium of the system can be obtained and system becomes stable. And if malware occurs in the system that will be removed quickly. This condition is supported by theorem 3.1 and 3.2.

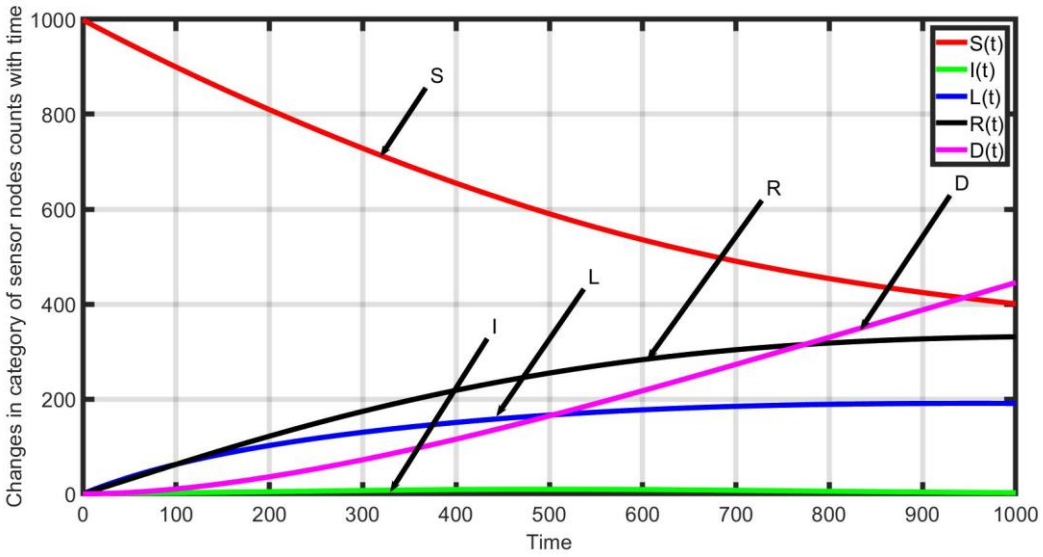

Figure 3.6(a): Malware transmission dynamics in WSN ($r = 0.75$)

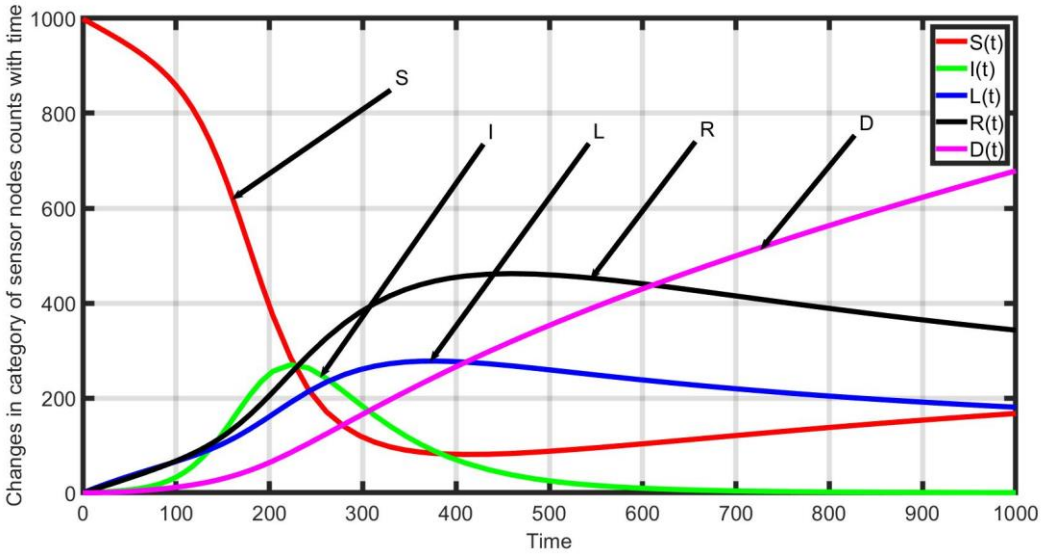

Figure 3.6(b): Malware transmission dynamics in WSN ($r = 1.1$)

Figures 3.6 (a-b) show malware transmission in WSN in case of $r \le r_{th}$ and $R_0^{th} \le 1$ or state of malware free state. When $r = 0.75$ then $R_0^{th} = 0.447121$ which is demonstrated by figure 3.6 (a), and figure 4.3 (b) for the value of $r = 1.1$ then $R_0^{th} = 0.961808$. From figures 3.6 (a-b) observed that finally the count of infectious sensor nodes reaches to zero, this satisfies the condition of malware free equilibrium and in this situation, system moves into the stable state. The outcomes of the simulation verify the theoretical finding. Figures 3.6 (a-b) also support the theoretical findings and the condition of malware free equilibrium as well as condition of theorem 3.1 and 3.2. The count of dead nodes linearly increasing in the system due to exhaust of sensor nodes energy or failure of software/ hardware.

Case 2: If $r > r_{th}$ then $R_0^{th} > 1$ [103,147], in this case the endemic equilibrium will be locally asymptotically stable and system continue with malware. This is supported by theorem 3.3.

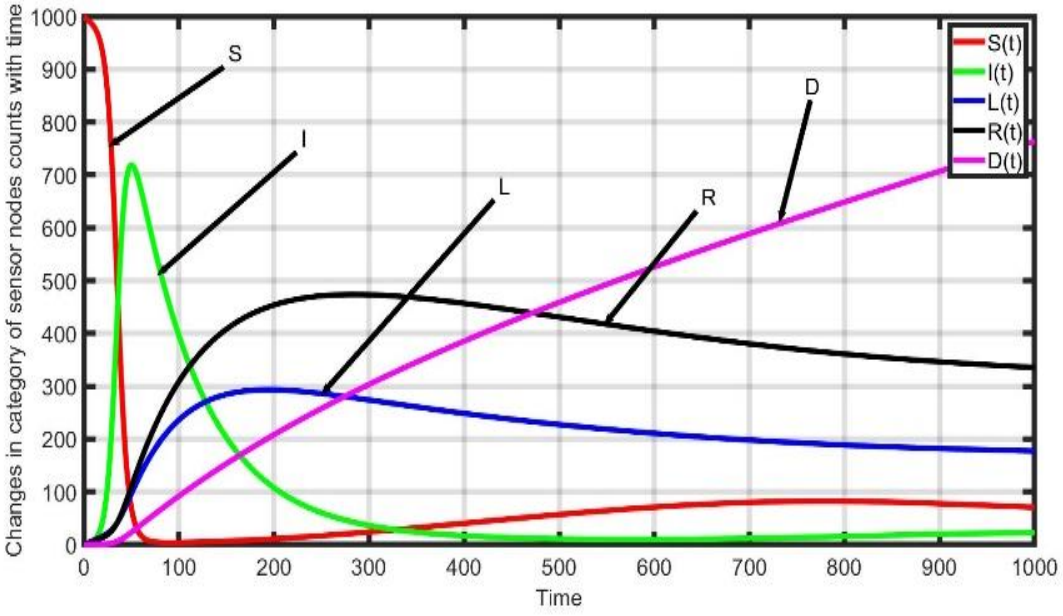

Figure 3.6 (c): Malware transmission dynamics in WSN ($r = 2.2$)

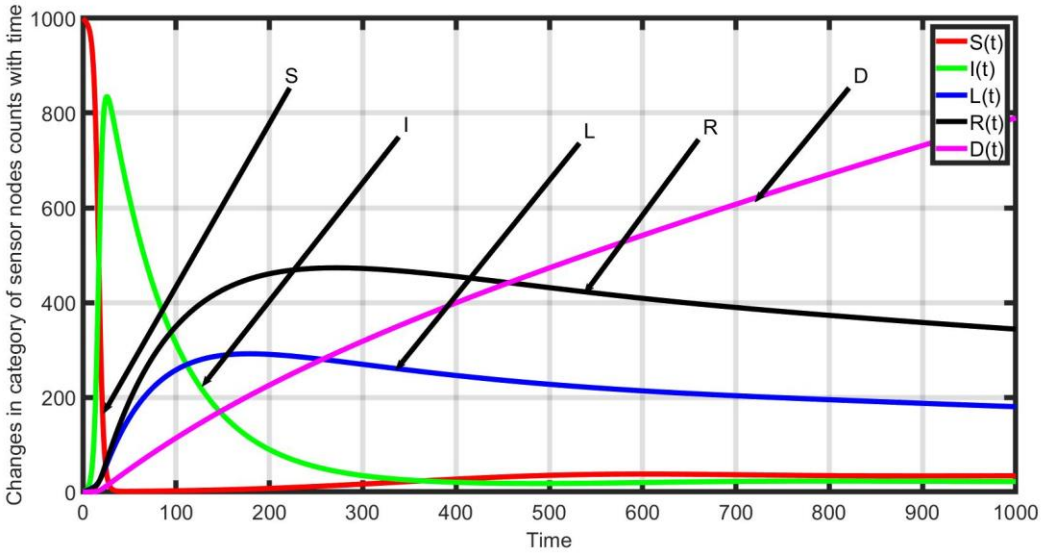

Figure 3.6 (d): Malware transmission dynamics in WSN ($r = 2.8$)

Figures 3.6 (c-d) show the endemic state system stability when $r > r_{th}$ and $R_0^{th} > 1$. When $r = 2.2$ then $R_0^{th} = 3.847$ and result of this condition is demonstrated in figure 3.6 (c), and when $r = 3.1$ then $R_0^{th} = 7.638819$ and outcome of the result is shown in figure 3.6 (d). From figures 3.6 (c-d), it is noticed that in the initial stage susceptible number of nodes are decreasing and others are increasing. The number of infectious nodes reaches to the maximum value after that start to decrease and attain the steady state and on the other hand then the susceptible number node starts to increase. This demonstrates that malware exist continuously in the system and fulfil the condition of endemic equilibrium. The outcomes of simulation verify the theoretical findings. Figures 3.6 (c-d) also support the theoretical findings and the condition of endemic equilibrium as well condition of theorem 3.3. The count of dead nodes linearly increasing in the system due to exhaust of sensor nodes energy or failure of software/ hardware.

Communication radius (r) is a vital factor for overall connectivity of the network when it comes to forming a connection among various sensor nodes. As a result, connectivity is a function of r.

On the basis of analytical and simulation study in connection with communication radius has been observed. The following are some key findings in relation to r:

1. To enhance the connectivity of the network it is required increase the radius (r) of sensor nodes. As the value of r increases, the value of R_0^{th} increases as well. The network will be stable in malware free state when $r < r_{th}$. This is discussed in case 1with detail descriptions.

2. The impacts of r on malware transmission is obseerved and how it influences on the performance of the system is explained in case 1 and case 2. The counts of infectious sensor nodes increase as the value of r increase. The reason to increase in count of infectious sensor nodes with increase in communication radius is that an infectious sensor node of the network can communicate with more number of susceptible at a time as well infect them also. Because that can cover large area of the network due large r. With an increase in R_0^{th}, the network becomes more vulnerable, possibly leading to network failure.
3. The threshold value of r is an important parameter which help in malware transmission controlling, malware extermination, and improvement in lifetime of WSN. That value can be optimized as per the requirement of the network design.
4. Basic reproduction number (R_0^{th}) is directly proportional to r from equation (3.16), so this shows the effect of r on system stability.

3.6.3.2 Impacts of Node Density (d) on Performance of the System

Taking the value of $R_0^{th} = 1$, the threshold value of node density d_{th} is determined as follows:

$$1 = d_{th} \frac{\pi r^2 b\beta}{N(\tau+\sigma+\alpha_2)(\varepsilon+\rho)}$$

$$\Rightarrow d_{th} = \frac{N(\tau+\sigma+\alpha_2)(\varepsilon+\rho)}{\pi r^2 b\beta} \qquad (3.18)$$

The following parametric value are taking into account: $\varepsilon = 0.0006$, $\alpha_2 = 0.0015$, $r = 1.0$, $\rho = 0.0008, \tau = 0.007, \gamma = 0.003, \sigma = 0.006$, $b = 0.37, \beta = 0.002$, $\eta = 0.004, \alpha_1 = 0.003$. To compute the threshold value of distributed node density puts these values in equation (3.18) then computed value of $d_{th} = 8.736$. The sensor nodes deployment in area of l^2 with length l. The value of R_0^{th} is changing with change in the value of d, initially at time $t = 0$, assume the count of different class of nodes are S (0), I (0), L (0), R (0) and D (0) be 999, 1, 0, 0 and 0 respectively. The simulation results are illustrated in the figures 3.7 (a-d).

Case 1: If $d \le d_{th}$ then $R_0^{th} \le 1$ [103,147], the malware-free equilibrium of the system can be obtained and system becomes stable. And if malware occurs in the system that will be exterminate swiftly. This condition is supported by theorem 3.1 and 3.2.

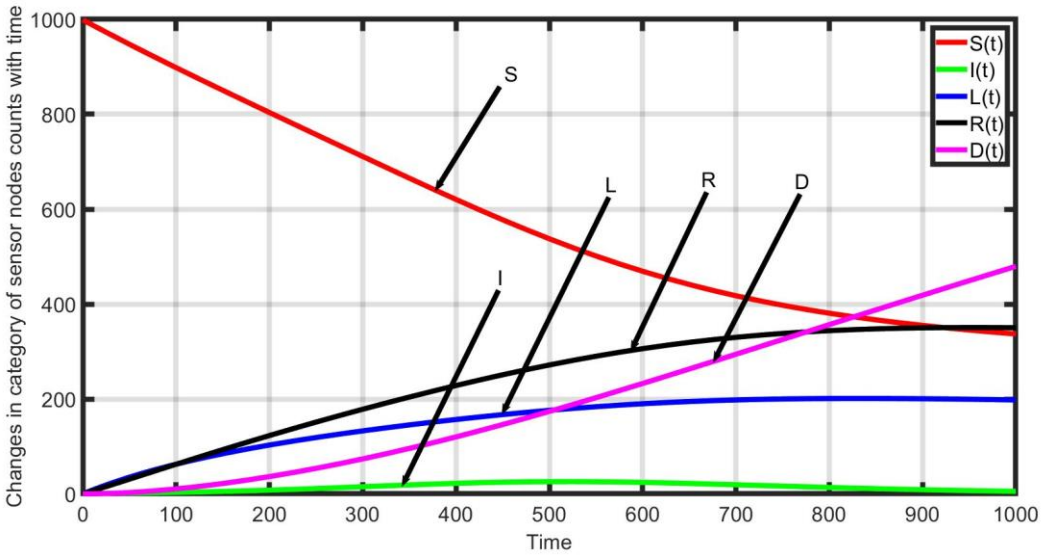

Figure 3.7(a): Malware transmission dynamics in WSN ($d = 4.4$)

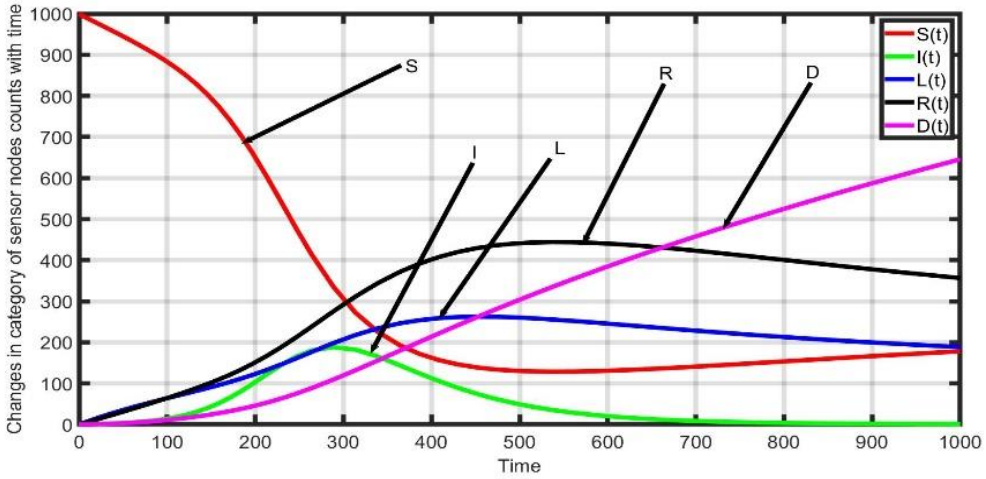

Figure 3.7(b): Malware transmission dynamics in WSN ($d = 6.94$)

Figures 3.7 (a-b) demonstrate malware transmission dynamics in WSN in case of $d \le d_{th}$ and $R_0^{th} \le 1$ or state of malware free state. The value of $d = 4.4$, $l = 15.07$ then $R_0^{th} = 0.504$ which is shown in figure 3.7 (a), in another case when the value of $d = 6.94$, $l = 12.004$ then $R_0^{th} = 0.794$ this is illustrated by figure 3.7 (b). Figures 3.7 (a-b) validate the theoretical findings. The count of infectious sensor nodes finally reaches to zero which can be observed from figures 3.7 (a-b), this satisfies the condition of malware free equilibrium and in this situation, system moves into the stable state. The results of the simulation confirm the theoretical findings as well as conditions of theorem 3.1 and 3.2. The count of dead nodes linearly increasing in the system due to exhaust of sensor nodes energy or failure of software/ hardware.

Case 2: If $d > d_{th}$ then $R_0^{th} > 1$ [10.,147], in this condition the system is in the endemic state and malware present in the system. This is supported by theorem 3.3. And in this case system will be in locally asymptotically stable state at endemic equilibrium.

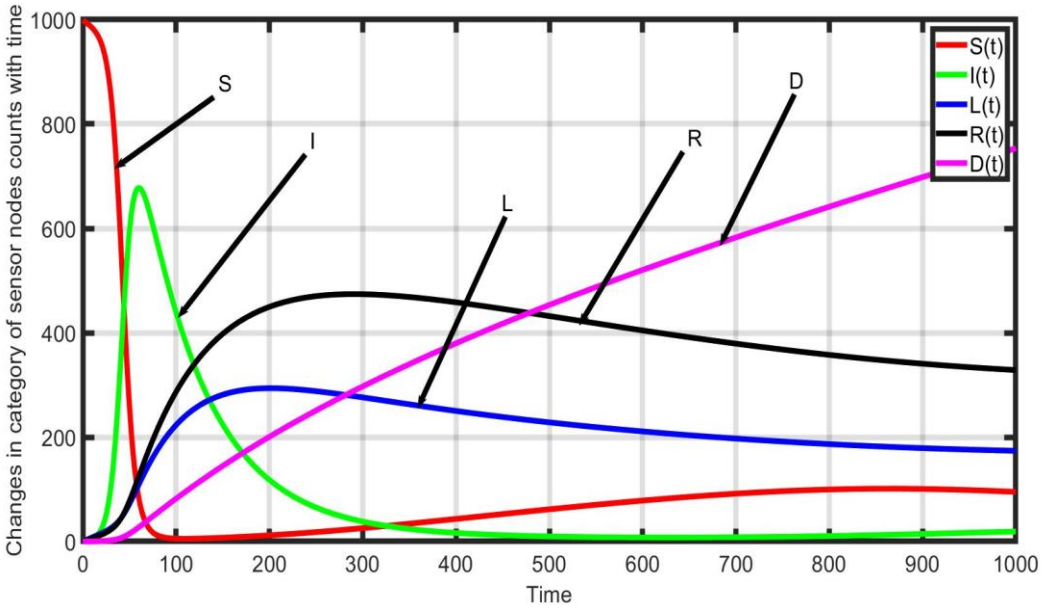

Figure 3.7(c): Malware transmission dynamics in WSN ($d = 28$)

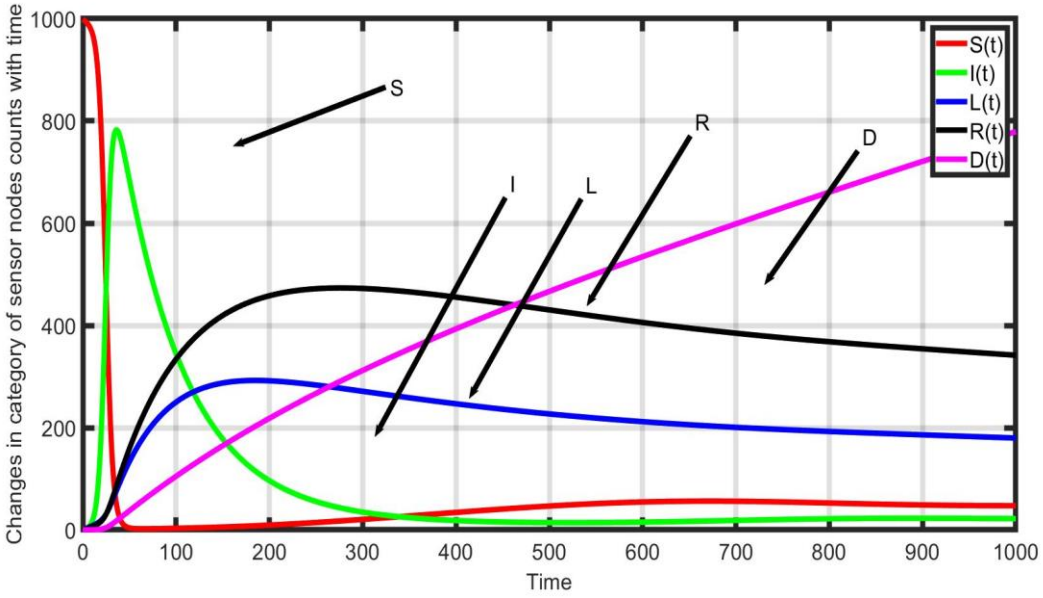

Figure 3.7 (d): Malware transmission dynamics in WSN ($d = 28$)

Figures 3.7 (c-d) demonstrate transmission dynamics of malware in endemic state when $d > d_{th}$ and $R_0^{th} > 1$. The value of $d = 28$, $l = 5.98$ then $R_0^{th} = 3.2$ which is shown in figure 3.7 (c), in another case when the value of $d = 47$, $l = 4.61$ then $R_0^{th} = 5.38$ this is illustrated by figure 3.7 (d). Figures 3.7 (c-d) validate the theoretical findings. It is noticed from figures 3.7 (c-d) that the count of susceptible sensor nodes is decreasing and other hand other

categories of sensor nodes are increasing at the same. The number of infected nodes attain the highest value after that it starts to decrease and on the other hand the susceptible number node starts to increase. Again after sometime susceptible and infectious category of sensor nodes attain the steady state. This establishes that malware exist in the system and realize the condition of endemic equilibrium. The outcomes of simulation substantiate the theoretical findings. Figures 3.7 (c-d) also support the theoretical findings and the condition of endemic equilibrium as well condition of theorem 3.3. The count of dead nodes linearly increasing in the system due to dissipation of sensor nodes energy or fault in software/ hardware.

The connectivity of the network is also affected by the node density (d) as the communication radius (r). On the basis of above study based on node density (d), the following are some key findings in relation to d:

1. From figures 3.7 (a-d), it is realized that as the value of node density increases the connectivity amongst the sensor nodes become strong, because the distance between the sensor decreases. This is achieved because area of sensor nodes deployment is constant and number of sensor nodes increases in the defined area. This is described in case 1 and case 2.
2. The value of R_0^{th} increases as the value of node density increases. This fades the stability of the system. If the node density is high then an infectious sensor node can communicate to many susceptible sensor nodes simultaneously and infect them. So, in strongly connected network malware transmit quickly. So, the value of R_0^{th} upsurges speedily because many number of infectious sensor nodes increase rapidly. This can be visualized from figures 3.7 (a-d).
3. To improve the lifetime of WSN method of optimization can be applied (by cautiously deployment of sensor nodes in the sensor field). By the use of concept of threshold of node density establish the malware free network and overcome the communication overhead in the network and made economically viable. Therefore, to analyse other parameters along with node density at the time of development of WSN.

3.7 Performance Analysis of the Proposed Model

To analyse the performance of the proposed it is necessary to investigate the impact of different parameters for example infection rate (β), sensor nodes charging rate (η), rate of recovery

from infectious state (τ), rate at which infectious node move into low- energy state (σ), response of susceptible state of sensor nodes etc. The effect of the different parameters is explained through many graphs which are illustrated in figures 3.8 to 3.13.

Figure 3.8 presents the impact of infection rate on transmission of malware in WSN. From figure draws a conclusion that when the value of infection rate (β) is increasing and recovery rate (τ) is constant then the count of infectious sensor nodes increases in the network, whereas if infection rate (β) is constant and recovery rate (τ) increases the count of infectious sensor nodes decreases. So, to restrict the movement of malware within the network it is required to increase the rate of patching or anti-malware installation in the system.

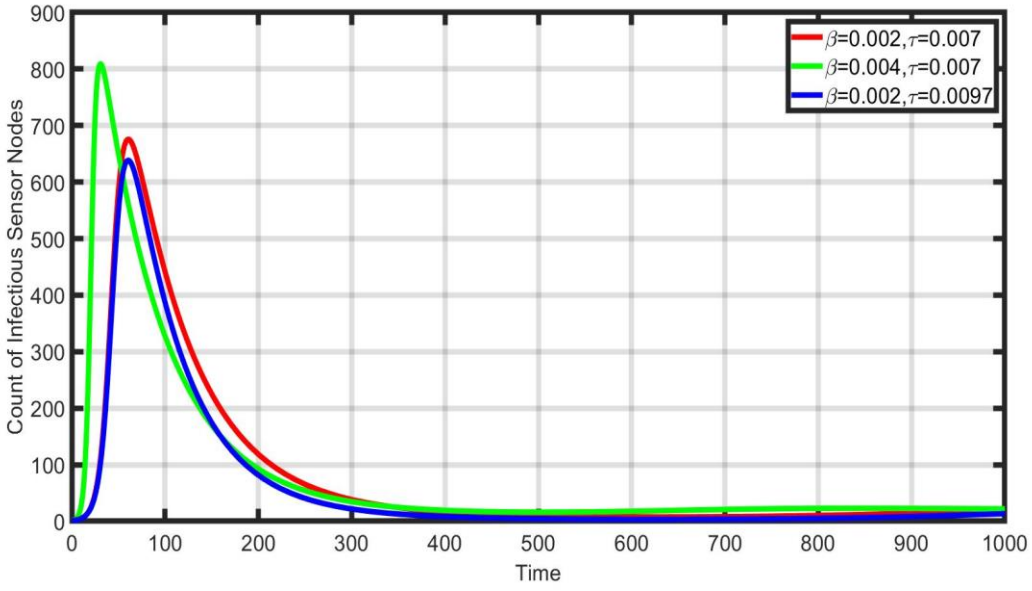

Figure 3.8: Impact of infection rate on malware transmission

The findings of figure 3.8 is supported by figure 3.9. The larger number of infectious sensor nodes exist in the system when infection rate (β) is high and other hand in this situation low count of susceptible sensor nodes exist. At the higher value of β maximum number of infectious sensor nodes present in the system. If the value of infection rate (β) is fix and recovery rate (τ) high then larger number of susceptible sensor nodes present in the system with higher value of τ .

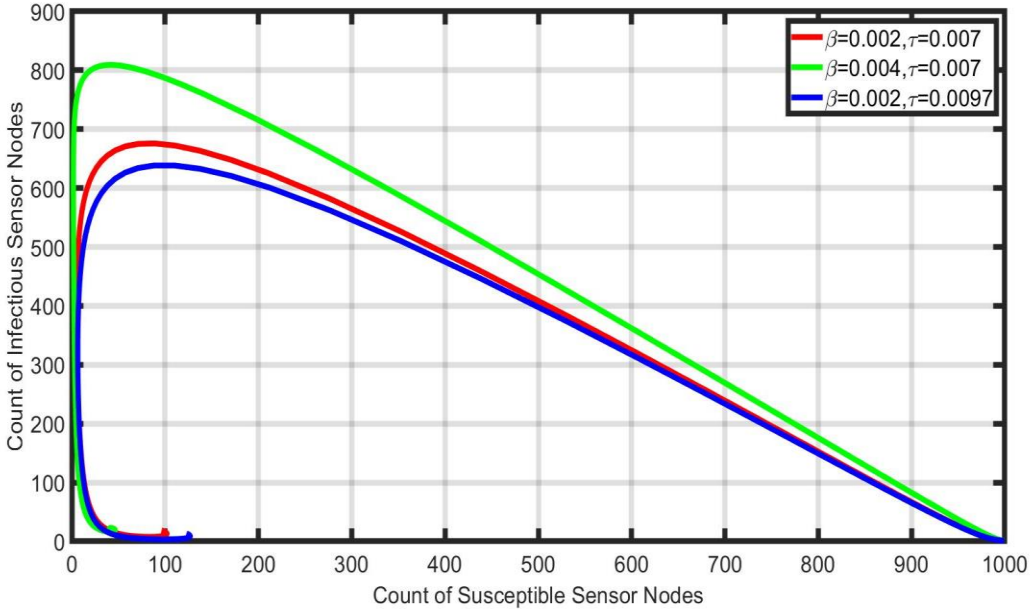

Figure 3.9: Impact of infection rate on susceptible sensor nodes

The inference drawn from figures 3.8 and 3.9 that and if rate of infection rate is higher count susceptible sensor nodes are lower and of infectious sensor nodes are greater.

The effects of different recovery rate are analysed with the help of figures 3.10 and 3.11. The recovery from infectious to recovered state is τ and η is the recovery rate from low-energy state to recovered state. Figure 3.10 shows that as the rate are increasing the count of recover state sensor nodes increase. Which shows that the life of network will be longer when recovery rate is high.

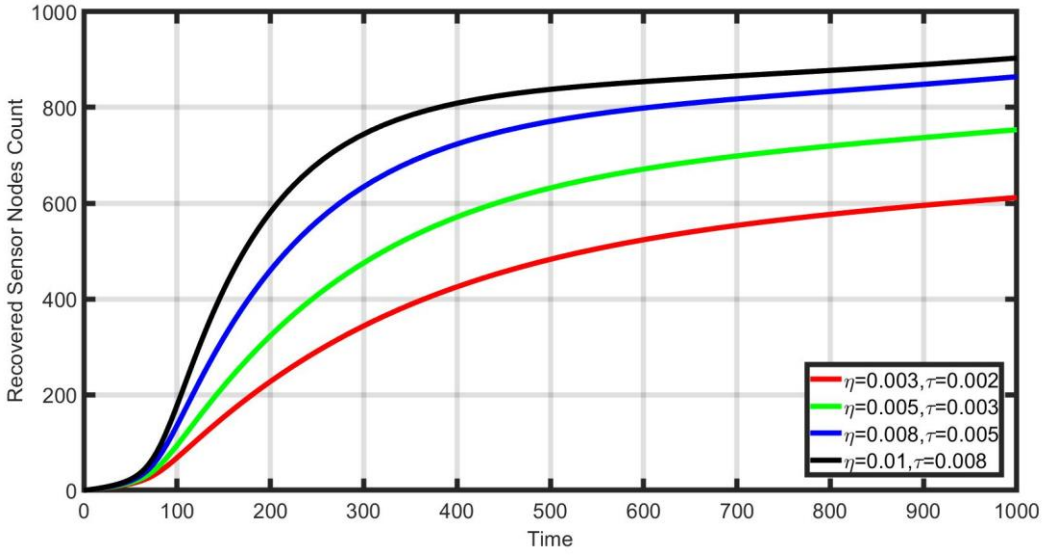

Figure 3.10: Effect of recovery parameters

Figure 3.11 illustrate that lesser number of sensor nodes come into domain of infection when anti-malware or patch install on time in the network.

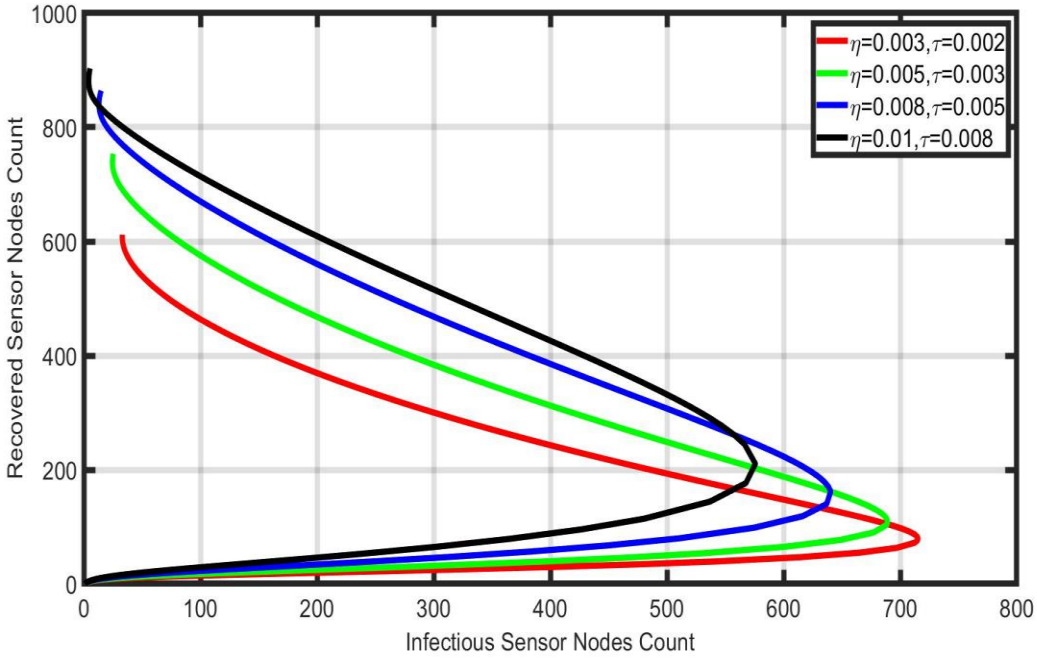

Figure 3.11: Effect of recovery parameters on infectious nodes

Figures 3.10 and 3.11demonstrate that recovery rate play a crucial role in survival of the network. The network will survive in long time with timely apply of recovery mechanism.

The effects of different parameters are realized through the figures 3.12 and 3.13. From figure 3.12 analysed that if the rate of infection is very high then whatever the recovery mechanism transmission of malware in the network will be fast. In figure 3.12 when β is highest among the three then irrespective of all parametric values count of infectious sensor nodes are maximum. And when β is fix and recovery rate τ is maximum then in these conditions minimum count of sensor nodes in infectious state.

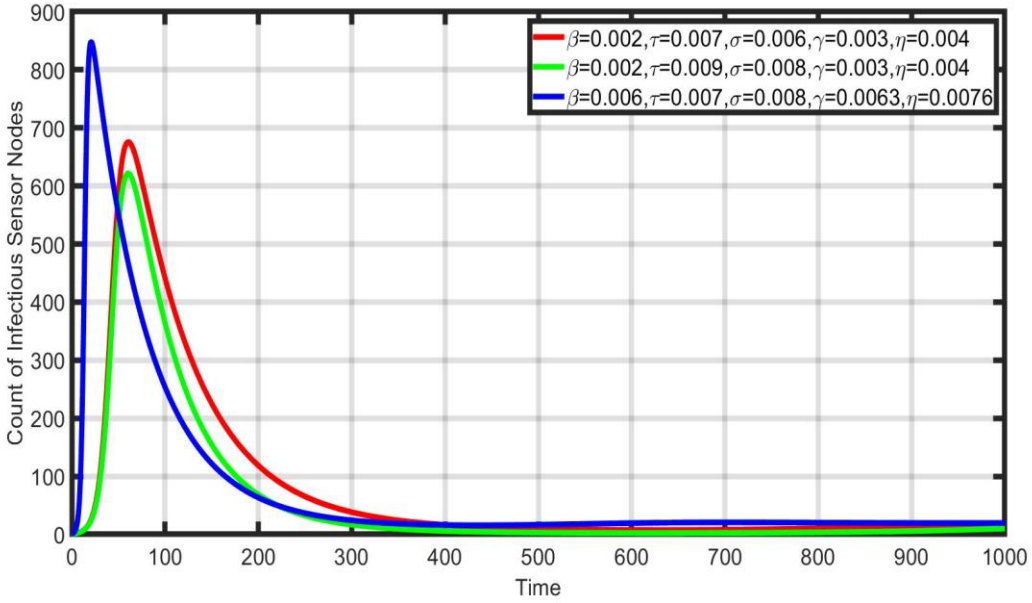

Figure 3.12: Effect of recovery parameters on infectious nodes

Figure 3.13 supports the analysis of figure 3.12, if β is maximum number of infectious nodes will be also maximum and number of recovered nodes will be minimum, whereas when recovery rate is maximum the number of recovered nodes will be maximum.

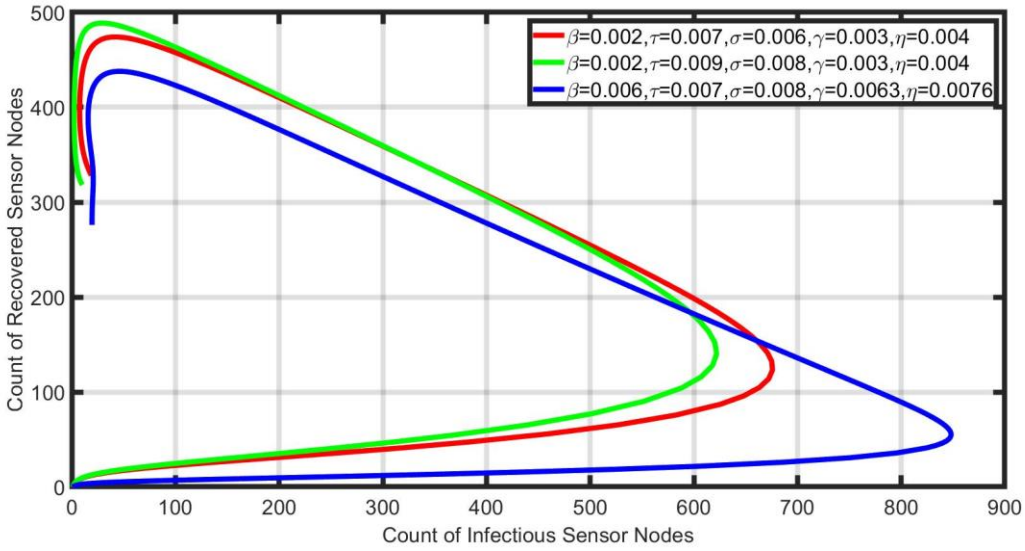

Figure 3.13: Effect of recovery parameters on infectious nodes

3.8 Comparative Analysis between Proposed Model and Other Model

In this section, comparative analysis is carried out between proposed model and SIRS [147] existing model. To perform the comparative study, consider all the parametric values are same

and change the value of communication radius (r). The communication radius is a critical design parameter for smooth network connectivity.

Figures 3.14 (a-b) demonstrate that the performance of proposed model is better in respect to the SIRS [147] existing model for the different value of communication radius (r). For comparative study the graph is depicted between the number of infected nodes and time. The number of infected sensor nodes is increasing with increase in the size of communication radius. The transmission behaviour of malware in both the cases proposed as well as existing is similar whereas in case of suggested model the increase in infected nodes is smaller in respect to existing model. The proposed model proposes the method for design of sensor node through which develop a protected and robust connecting system. Therefore, proposed model's performance is comparatively improved in terms of malware transmission control and lifetime enhancement of WSN.

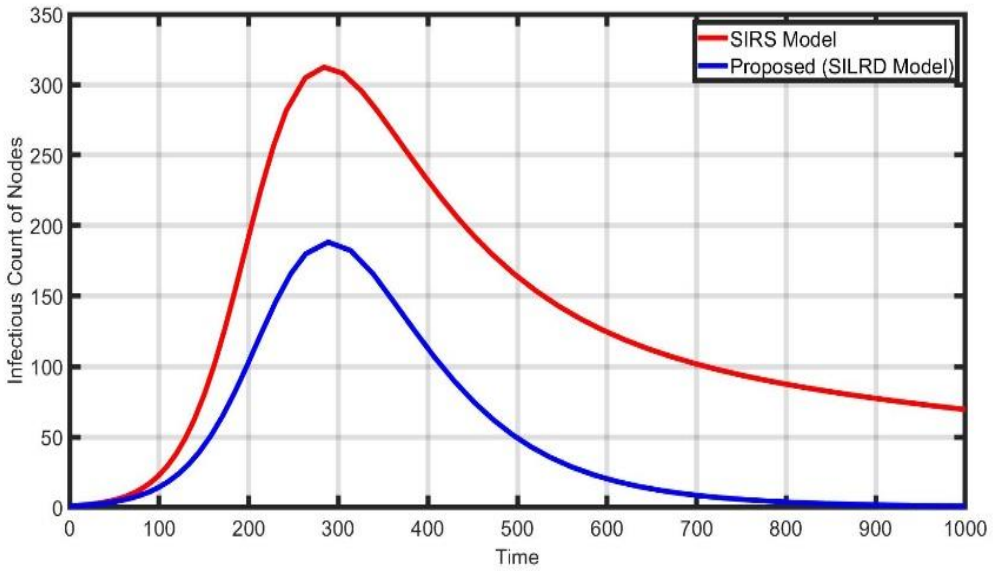

Figure 3.14 (a): Communication Radius ($r = 1.0$)

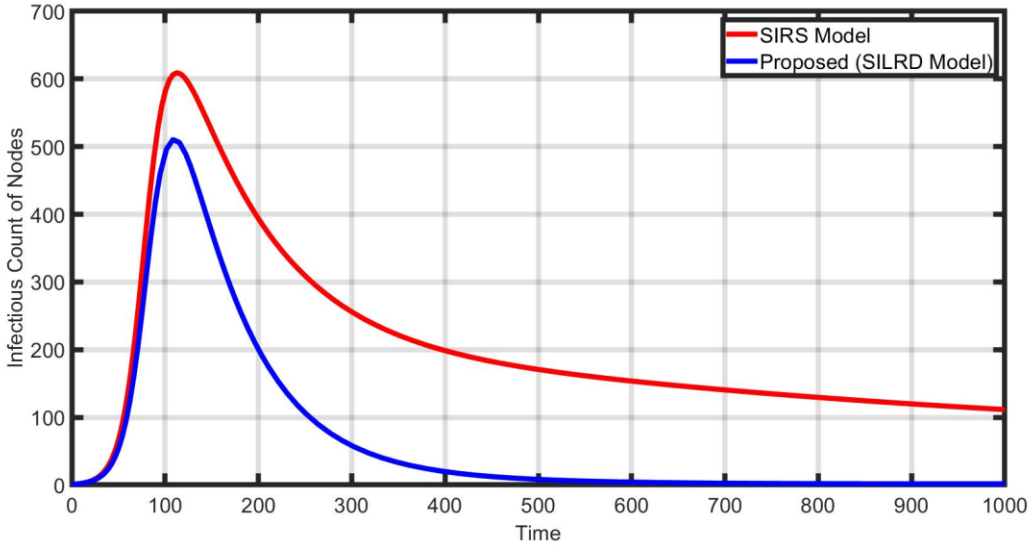

Figure 3.14 (b): Communication Radius ($r = 1.5$)

Figures 3.15 (a-b) demonstrate that the performance of proposed model is better in respect to the SIRS [147] existing model for the different value of node density (d). The graph is plotted between the count of infectious nodes and time. On increasing the node density, the infectious sensor nodes also increase. In both the cases proposed as well as existing model dynamics of malware transmission in the network is similar but in case of suggested model the increase of infectious nodes is low in number in respect to previous model. The model provides the method of deployment of sensor nodes in sensor field in optimum manner. So, proposed model suggesting the better mechanism for controlling of malware transmission in WSN.

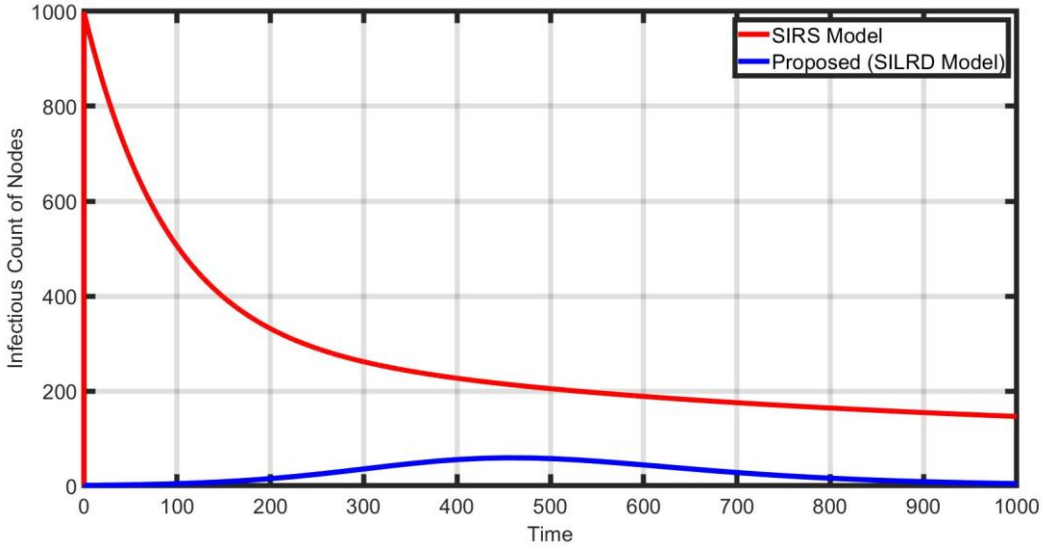

Figure 3.15 (a): Node Density ($d = 5$)

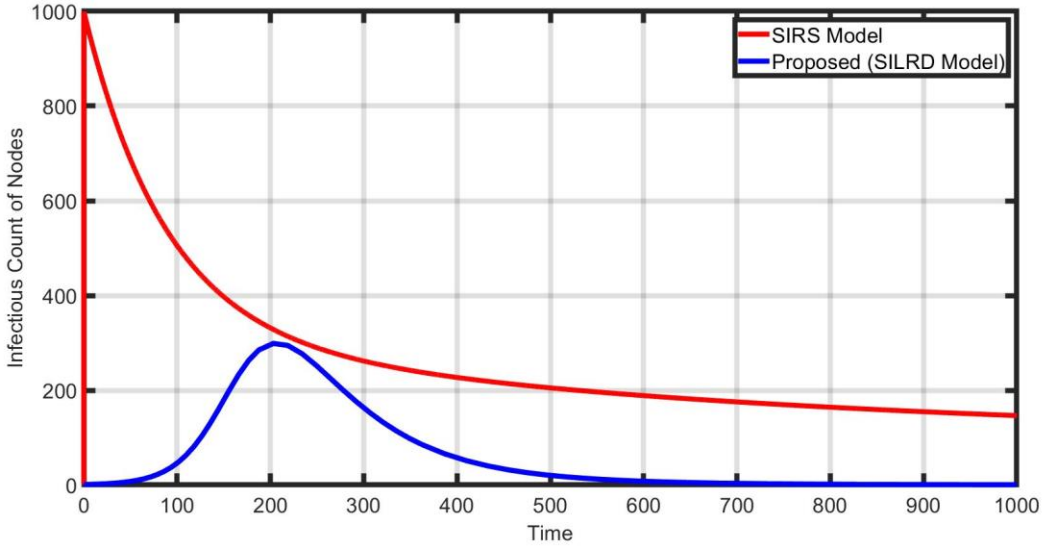

Figure 3.15 (b): Node Density ($d = 9$)

It is analysed from figures 3.14 (a-b) and 3.15 (a-b) that in both model count of infectious nodes increases initially and attain the maximum value then start to decline, in case of suggested model number of infectious node approaches to zero or malware free state, whereas in existing model under similar condition steady state achieve or endemic equilibrium. So, in the proposed model the method of charging and patching prevent the transmission of malware in the system.

3.9 Summary of the Chapter

The low-energy state SILRD model is proposed to control the transmission of malware and elongate the lifetime of WSN. The proposed model provides a mechanism of charging that supress the infection of malware and increase the lifetime of the network even in case of malware attack. The method of charging suggests an opportunity to maintain the network operation and stabilize them under diverse circumstances. The weaknesses of SIRS model overcome by a modified SILRD model through the technique of charging. The maintenance of the network is performed by taking the leverage of the sleep mode of sensor node. The better prevention method against malware attack provided by the proposed model. The proposed model does not require any extra hardware and not bear any burden of signal overhead. To investigate the malware transmission dynamics in WSN compute the value of R_0^{th} .

The value of R_0^{th} is instrumental and important parameter which can be used for prevention of the malware transmission in WSN.

Connectivity of the network is one of the vital issues in WSN and it is related with coverage. So, for that an improved SILRD model is discussed by taking into account of communication radius. The communication radius defines the coverage area of the sensor nodes. The improved SILRD model described in niceties about the coverage and connectivity of the network. Furthermore, the points of equilibriof the system are discussed and malware-free equilibrium is locally and globally asymptotically stable when the value of $R_0^{th} \leq 1$ is obtained. The theorems and proofs related to malware-free equilibrium is presented. The endemic stability If the value of $R_0^{th} > 1$ the system will be locally asymptotically stable in endemic equilibrium. The theorem and their proof are also discussed. For the development of secure and reliable network against malware attack the threshold value of communication radius is computed, that can be used to control the transmission of malware and increase the lifetime of WSN. The deployment of sensor nodes in the sensor field is one of another critical concern, therefore, to compute the threshold value of node density that can provide the relevant idea for sensor nodes deployment in the sensor field that can ensure smooth and secure communication and optimize the deployment cost of sensor nodes. The relationship with R_0^{th} and r is discussed and relationship of d with R_0^{th} is also investigated. The effect of charging and status of low-energy state is also explained in minutiae.

Moreover, to validate the proposed model simulation is carried out using MATLAB (R2018a). The consequence of diverse constraints on transmission of malware in WSN in dissimilar circumstances has been precisely analysed. The comparative evaluation between SILRD and SIRS model has been accomplished. The relative study demonstrations that lesser count of infectious sensor nodes in proposed SILRD model in respect to existing SIRS model. Over the analysis the results indicated that the proposed model ensures to enhanced the network for a longer period of time and improved security method against malware attack.

Chapter 4: Study of Malware Propagation in Rechargeable Wireless Sensor Networks: A Modified SILRD Epidemic Model

4.1.Introduction

Wireless Sensor Network is a kind of ad-hoc network, which can be installed any type of terrain. This is one of the beautiful advantages of WSN. Along with the advantages some problems are faced by WSN due to resource restrictions with sensor nodes. With increase the applications of WSN various types of problems arise such as security and lifetime of sensor node, due to vulnerable structure of network and limitations of battery. Malware attack becomes prominent in WSN due to these restrictions. Due to malware attack the information leakage begins from the network and energy dissipation also increase in comparison to the normal operation. To overcome the issue of limited storage capacity of energy and troublesome replacement mechanism of battery a technology is developed, which is known as Wireless rechargeable sensor networks (WRSNs). Denial of Charge (DOC) attacks also affect rechargeable sensor nodes with disastrous affects for real-time and pre-warning applications. Therefore, research on WSN security is crucial and essential.

The number of researchers has carried out research in this field. The researchers have studied virus spreading in computer network using the concept of epidemic theory. An improved SEI (susceptible-exposed-infected) model was proposed by Thommes et al. [163] to analyse the virus spread in computer network. They analysed the impact of latent period on virus spread. An another SEIR model was proposed by Yan and Liu [164] with assumption that recovered state of nodes cannot be infected again. But this is applicable in real world computer network because of emergence of new types of viruses in the digital world. Mishra and Saini overcome the drawback of SEIR model [165] by introduction of immune and latent periods. In this model when nodes exposed to the malware, after a fixed period they become infectious. This fixed period is known as latent period. To prevent the malware spread in the system employs anti-malicious software to recover the infected node and provide temporary immunity to the node in the network. The value of basic reproduction number and virus- free equilibrium is discussed by them.

The nature of malware propagation in WSN is similar as the computer network but not in all respect. Lopez et al. [148] considered the effect of random jamming due to malware attack in WSN and proposed a SEIS (Susceptible- Exposed-Infected-Susceptible) model to analyse the effect of malware attack in WSN. The value of basic reproduction number of the model is computed. The effect of latent period on spreading of malware in WSN is analysed by them. The model is verified through the simulation results. Another epidemic model for the study of worm propagation behaviour in WSN is developed by Keshri and Mishra [166] with two-time delay. The developed model is SEIR (Susceptible-Exposed-Infectious-Recovered) model. This model explains the use of exposed state for prevention of worm attack in WSN. The one delay is as exposed (latent) period and temporary immunity period considered as second delay due to multiple malicious signals outbreaks. They discussed the worm-free equilibrium and endemic equilibrium points of the system and compute the basic reproduction number of the model to investigate the system dynamics. The effect of exposed state on the stability of the system has been studied.

The method of epidemic modelling is applied to study the dynamics of malware in WSN. In chapter 3 the concept of low energy state along with other epidemic states has been discussed. The impact of coverage and connectivity on malware propagation in WSN is also discussed. In chapter 3 a SILRD model is proposed to investigate the dynamics of malware in WSN. The different aspects of the model such as equilibrium points, malware-free, endemic state and stability of the system are carried out. To enhance the security mechanism as well reduce the energy consumption of WSN, improve the SILRD model by inclusion of exposed state. The exposed state eases the detection of malware presence in WSN in early stage. In this chapter a novel model is proposed. The proposed model is Susceptible-Exposed-Infectious-Low Energy-Recovered-Dead (SEILRD) model.

The proposed model describes the propagation dynamics of malware in WSN. The mechanism is developed for prevention of malware attack and optimize the energy consumption of sensor nodes. The proposed model employs the concept of exposed state of epidemiology for detection of malware presence in WSN at early stage. Moreover, the model investigated the impacts of charging on malware spread. The model also studied the impact of communication radius with charging of sensor node, node density and area of deployment on spread of malware in WSN. Organization of the chapter.

The remainder section of this chapter is structure in the following order: Section 4.2 describes the proposed SEILRD model and their assumptions. In section 4.3, discuss the existence of different types of equilibrium points and the system stability under different conditions is analysed in section 4.4. In Section 4.5, evaluation of theoretical findings with simulation results presented. An improved SEILRD model, equilibrium points and stability study of the enhanced model, the impact of communication radius, node density and area of deployment on malware transmission in WSN is investigated in section 4.6. The performance analysis of the proposed model carried out in section 4.7. Comparative analysis between existing and proposed model is carried out in section 4.8. In Section 4.9 summary of the work is presented.

4.2 Proposed Model

SEILRD (Susceptible-Exposed-Infectious-Low Energy-Recovered-Dead) model based on the concept of epidemiology is proposed. The model helps in the study of malware dynamics in WSN. The outcome of malware attack on WSN is to steal the information from the network, consume the energy of sensor nodes and paralyse the network operations. Therefore, to prevent the malware propagation in WSN, the identification of malware presence/ attack in the network is important. So, for this purposed the exposed state of epidemic model is useful that helps in finding the malware presence in the network at early stage.

The important contribution of the chapter is:

- Developed the model based on epidemic theory for investigation of malware transmission dynamics in WSN and devise controlling mechanisms.
- The exposed state is used to identify the presence of malware in WSN at early stage, which helps in prevention of malware transmission.
- Analyse the effect of charging and patching on malware transmission and recovery on system responsiveness.
- Investigate the stability of the system in different conditions.
- Find the equilibrium points and analyse performance of the proposed models.
- The proposed models prove theoretically and verified with the extensive simulation results.

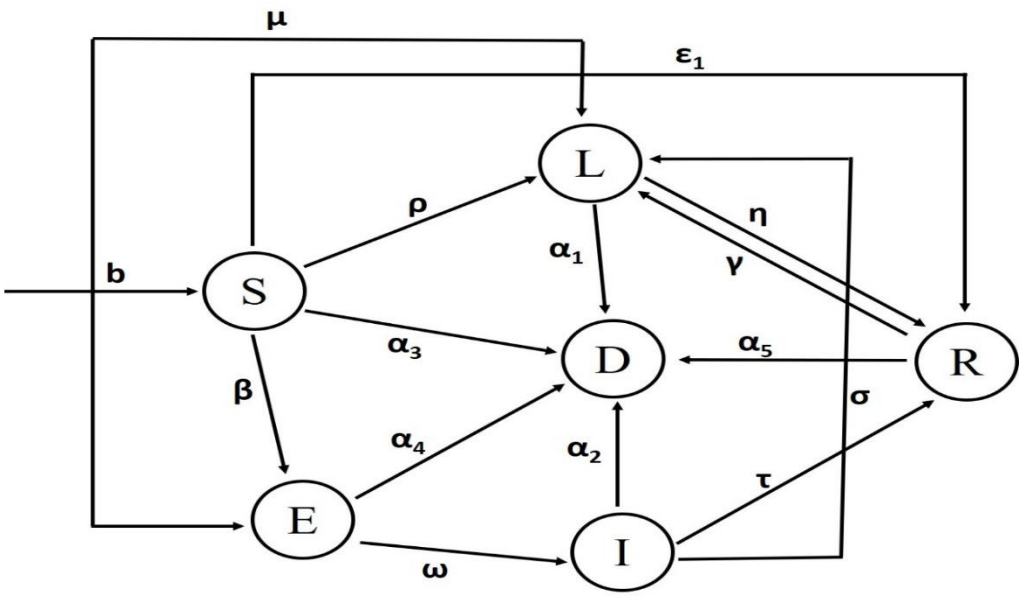

Figure 4.1: Transition state diagram of SEIRLD

The different states of the proposed models:

Susceptible State (S): Sensor nodes which are uninfected from any type of malware and having high-energy level. They can execute the assigned task in the normal way but due to lack of defense mechanism they are extremely vulnerable against attack of malware.

Exposed State (E): Susceptible sensor nodes when come in contact with malware converted into exposed state. Or when susceptible sensor nodes installed with malware becomes exposed node, but not executed completely. And after a time-interval (latent period) they become infectious.

Infectious State (I): Exposed sensor nodes become infected after latent period if not a corrective measure applies on time. These sensor nodes have ability to infect the surrounding. The consumption of energy increases rapidly when sensor node come into infectious state. If these nodes are not charge or installed anti-malware in time, they will lose its energy and die.

Low-Energy State (L): Sensor nodes when lose its energy due to operation or attack of malware. They have not sufficient energy to work in proper manner and cannot transmit data or infection to other sensor nodes.

Recovered State (R): Sensor nodes which are equipped with anti-malware and immune against malware attack. These nodes having high-energy level. The anti-malware installation and charging take place simultaneously. The anti-malware can protect sensor nodes against relevant malware attack. These nodes can lose its energy and protection against inhomogeneous malware attack.

Dead State (D): Sensor nodes have lost its energy due to use of energy during normal operation or or maybe failure of hardware/software. These nodes are dysfunction completely. These sensor nodes cannot be workable after charging also. They have not capability to perform any kind of operation like collection, process and transmission of data.

The key goal of proposed models is to develop method to control the malware transmission as well as to enhance WSN lifetime. The model describes the transmission of malware dynamics in WSN, the contributions of developed model are:

1. The proposed model studies the transmission dynamics of malware WSN. The model suggests the mechanism against malware attack.
2. For deterrence of malware transmission and consumption of sensor node's energy in WSN utilize the concept of Exposed state.
3. To include the idea of low-energy state in the epidemic model. This idea is used for maintenance of network operation. The method of charging is applied for enhancement of the network lifetime and supress the malicious activity and improve the security of WSN.
4. To analyse the system response due to attack of malware and investigate the method of fast recovery of WSN in steady state conditions.
5. To examine the system stability in different conditions and verify analytical study through comprehensive simulation outcomes.

Some assumptions are made in the formulation of the model. The sensor nodes are homogeneous and distributed in a field for collection of information. It is assumed that in the beginning, sensor nodes are of Susceptible (S) state. They are free from malware. The attacker installs a malware in WSN through a sensor node then state of the sensor node's changes which is shown in figure 4.1.

4.2.1 Model Description and Assumptions made in its Analysis

The defence mechanism is required for protection of WSN against malware attack. For this purpose, the model is proposed, which formulation is described in Fig. 4.1. There are three types of infectious state of the sensor nodes are considered in the model. These states are: Exposed state sensor node and Infectious state sensor node. Malware transmit in WSN with useful data through the neighbouring active mode sensor nodes. Malware transmissions stop in

two circumstances viz. (i) when nodes become dead or (ii) when nodes are in sleep mode. The meaning there by in these cases, the infection does not transmit in the sensor network.

For formulation of model the following assumptions has been made:

1. Initially sensor nodes are of Susceptible state (S) and they are vulnerable against malware attack. When malware installs in susceptible sensor node then susceptible sensor node becomes exposed node. Malware executed partially in exposed node. The rate of conversion of susceptible node into exposed node is β. Due to normal operation some of the susceptible sensor nodes loss its energy and move into low-energy state with rate ρ. Some of the sensor nodes go into dead state at a rate of α_3 because of hardware/software malfunction or drain of battery. The anti-malware installs in some of the susceptible nodes they acquire immunity against relevant malware attack and turn into recovered node with probability ε_1.

2. The abnormal behavior exhibits by the exposed state (E) of sensor node in WSN. In exposed node malware has installed successfully but not executed completely. Therefore, to stop the further transmission of malware in WSN apply a corrective measure on exposed state of nodes in time. Otherwise, these nodes become infectious with rate ω. Some of the exposed node enter into low-energy state due to loss energy or in contact of malware at the rate μ. Some of the exposed class of sensor nodes become dead with rate α_4 because of hardware/software malfunction or drain of battery or attack of malware.

3. Sensor node of WSN gets compromise with malware and begin to malicious activity in the network. Infected nodes start to spread malware with surrounding nodes and increase their own energy dissipation. At the same time, malicious programs may decide not to continue attacking the infected node, and these infected nodes are only infectious and not destructive. The corrective measure applies in time and install anti-malware successfully manner, the node will be safely converted to the recovered state at the rate τ. As the degree of damage from malicious programs increases, the node will die faster. Some of the infectious sensor nodes become dead with rate α_2 because of hardware/software malfunction or drain of battery or attack of malware. Infectious nodes loss their energy due to continuous attack of malware and enter into low energy state (L) with rate σ.

4. Recovered state of nodes in WSN not only immune to malware attack but they have also level of high-energy. Sensor nodes of the network turn into recovered state from susceptible and infectious state with level of high energy, anti-malware installed in these nodes without

charging. On the other hand, the low-energy nodes recharge and installation of anti-malware take place at the same time. The changing rate of low-energy state to recovered state is η. Though nodes turn into low-energy state from recovered state with rate γ due to normal consumption without energy replenishment. Some of the recovered class of sensor nodes enter into dead state with rate α_5 because of hardware/software malfunction or attack of malware.

5. Some low-energy state nodes are in immune state but not all. The low-energy state nodes drain speedily. Therefore, they enter into dead state quickly at the rate of α_1.

6. Susceptible sensor nodes are adding in the in the system is at the rate of b .

S.No.	Parameter	Meaning of the used Parameter
1.	b	Addition rate of susceptible nodes in the network
2.	α_1	Low-Energy node enter into dead node
3.	α_2	Rate at which infectious nodes destroy by malware attack and drain the energy completely move into dead state
4.	α_3	Rate of conversion of susceptible nodes into dead node
5.	α_4	Rate of conversion of exposed state into dead node
6.	α_5	Rate of conversion of recovered nodes into dead node
7.	σ	Probability of infectious state nodes enter into low-energy node
8.	η	Rate of conversion of low-energy state nodes into recovered nodes
9.	μ	Probability of exposed nodes enter into low-energy node
10.	ω	Probability of exposed nodes enter into infectious node
11.	ε	Probability of installation of anti-malware in susceptible nodes
12.	ρ	Probability of conversion of high-energy level susceptible nodes into low-energy level
13.	β	Probability of conversion of susceptible node to exposed node due attack of malware (rate of infection)
14.	τ	Rate of repairing of infectious nodes at high-energy level i.e. recovery rate of infectious nodes
15.	γ	Probability to turn recovered (high energy) to low energy

Table 4.1: Used parameters and their Meanings

Total number of sensor nodes in WSN at any time t is divided into six states. The $N(t)$ number of nodes in the system these names are as Susceptible State S(t), Exposed State E(t)); Low-Energy State L(t); Infectious State I(t) Recovered State R(t) and Dead State D(t).
Therefore, mathematically satisfy the following equation:

$N(t) = S(t) + E(t) + I(t) + L(t) + R(t) + D(t)$, for any time $t \geq 0$.

The transmission dynamics of SEILRD model is depicted in Fig. 4.1. To analyse the transmission dynamics of malware and state of change of sensor node presented by the set of differential equation. The state transition equations are written as:

$$\left.\begin{aligned}
\dot{S} &= b - \beta SI - (\rho + \alpha_3 + \varepsilon)S, \\
\dot{E} &= \beta SI - (\mu + \omega + \alpha_4)E, \\
\dot{I} &= \omega E - (\tau + \sigma + \alpha_2)I, \\
\dot{L} &= \mu E + \sigma I + \gamma R - (\alpha_1 + \eta)L + \rho S, \\
\dot{R} &= \tau I + \varepsilon S + \eta L - (\gamma + \alpha_5)R, \\
\dot{D} &= \alpha_1 L + \alpha_2 I + \alpha_3 S + \alpha_4 E + \alpha_5 R
\end{aligned}\right\} \qquad (4.1)$$

Meaning of the used symbols are given in Table 4.1.

4.3 Existence of Malware Free Equilibrium

In the system of equation (4.1) the first five equations do not contain the D state. It shows that the first five equations do not dependent on the fifth equation. Hence, to determine the points of system's equilibria equate the derivatives of first order of equations of the system to zero.

$$\left.\begin{aligned}
0 &= b - \beta SI - (\rho + \alpha_3 + \varepsilon)S, \\
0 &= \beta SI - (\mu + \omega + \alpha_4)E, \\
0 &= \omega E - (\tau + \sigma + \alpha_2)I, \\
0 &= \mu E + \sigma I + \gamma R - (\alpha_1 + \eta)L + \rho S, \\
0 &= \tau I + \varepsilon S + \eta L - (\gamma + \alpha_5)R,
\end{aligned}\right\} \qquad (4.2)$$

Solving equation (4.2) provides the point of system's equilibrium. The malware-free equilibrium (MFE) point is: $P_0^{MFE} = (S_0, E_0, I_0, L_0, R_0)$, where

$$S_0 = \frac{b}{(\alpha_3 + \rho + \varepsilon)},$$
$$E_0 = 0,$$
$$I_0 = 0,$$
$$L_0 = \left\{ \frac{\rho(\gamma + \alpha_5) + \varepsilon\gamma}{(\alpha_1\alpha_5 + \eta\alpha_5 + \alpha_1\gamma)} \right\} S_0,$$
$$R_0 = \left\{ \frac{\rho\eta + \eta\varepsilon + \varepsilon\alpha_1}{(\alpha_1\alpha_5 + \eta\alpha_5 + \alpha_1\gamma)} \right\} S_0$$

4.4. Stability Analysis of the Proposed Model

In this section, two different kinds of the system stability are described. Analysed the stability of system for malware-free equilibrium and endemic equilibrium. To investigate stability of the system theorems and their proofs are given.

4.4.1 Local and Global Stability Analysis of Malware Free Equilibrium

One of the major factors for the study of system stability in the presence of malware attack. For the analysis of system stability some theorems have been proposed to study the stability of the system. The following theorems and their proofs are utilized fot the study of system stability.

Theorem 4.1: At Malware free equilibrium (MFE) P_0^{MFE} If $R_0^{th} < 1$ then the model represented in (4.1) is locally asymptotically stable otherwise unstable when $R_0^{th} > 1$.

Proof. Stability of point P_0 of the system is obtained by using the Jacobian matrix which helps to obtain the eigen values. The Jacobian matrix can be represented as depicted below.

$$J(P_0^{MFE}) = \begin{pmatrix} -(\rho + \varepsilon + \alpha_3) & 0 & -\beta S_0 & 0 & 0 \\ 0 & -(\mu + \omega + \alpha_4) & \beta S_0 & 0 & 0 \\ 0 & \omega & -(\tau + \sigma + \alpha_2) & 0 & 0 \\ \rho & \mu & \sigma & -(\alpha_1 + \eta) & \gamma \\ \varepsilon & 0 & \tau & \eta & -(\alpha_5 + \gamma) \end{pmatrix} \quad (4.3)$$

Two Eigenvalues of (4.3) are: $\kappa_1 = -(\rho + \alpha_3 + \varepsilon), \kappa_2 = -(\mu + \omega + \alpha_4), \kappa_3 = -(\tau + \sigma + \alpha_2)$ and two other eigenvalues can be obtained from the roots of equation $a_0\kappa^2 + a_1\kappa + a_2 = 0$, Where,

$$a_0 = (1 - R_0), a_1 = (\alpha_1 + \eta + \gamma + \alpha_5)(1 - R_0), a_2 = (\alpha_1 + \eta)(\gamma + \alpha_5) - R_0(\alpha_1(\gamma + \alpha_5) + \eta\alpha_5),$$

since all coefficients a_0, a_1 and a_2 are positive when $R_0^{th} < 1$. Henceforth it is seen that all eigenvalues of the matrix are negative when $R_0^{th} < 1$. And if $R_0^{th} < 1$ the malware-free equilibrium is locally asymptotically stable at P_0 and otherwise unstable when $R_0^{th} > 1$.

Theorem 4.2: The Malware-Free Equilibrium (MFE) P_0^{MFE} is globally asymptotically stable if $R_0^{th} \leq 1$.

Proof. Consider the Lyapunov function as follows:

$L(t): \mathbb{R}^5 \to \mathbb{R}^+$ defined by $L(t) = \zeta_1 E + \zeta_2 I$ (4.4)

Now taking first derivative of (4.4), we get

$\dot{L} = \zeta_1 \dot{E} + \zeta_2 \dot{I} = \zeta_1 (\beta SI - (\mu + \omega + \alpha_4)E) + \zeta_2 (\omega E - (\tau + \sigma + \alpha_2)I) \leq (R_0{}^{th} - 1)I,$ where

$\zeta_1 = \omega, \zeta_2 = (\omega + \mu + \alpha_4)$ If $R_0{}^{th} \leq 1$ then $\dot{L} \leq 0$ holds. Moreover $\dot{L} \leq 0$ if and only if $I = 0$. Thus, the largest invariant set in $\left\{ (S, E, I, L, R) \in \Gamma : \dot{L} \leq 0 \right\}$ is the singleton set P_0. Hence the global stability of P_0^{MFE} when $R_0{}^{th} \leq 1$ according to LaSalle's [162] invariance principle.

4.4.2 Malware Endemic Equilibrium: Existence & Uniqueness

The uniqueness and existence of the malware endemic equilibrium (MEE) point is investigated through the equation (4.5).

$$\left.\begin{aligned} 0 &= b - \beta S^* I^* - (\rho + \alpha_3 + \varepsilon) S^*, \\ 0 &= \beta S^* I^* - (\mu + \omega + \alpha_4) E^*, \\ 0 &= \omega E^* - (\tau + \sigma + \alpha_2) I^*, \\ 0 &= \mu E^* + \sigma I^* + \gamma R^* - (\alpha_1 + \eta) L^* + \rho S^*, \\ 0 &= \tau I^* + \varepsilon S^* + \eta L^* - (\gamma + \alpha_5) R^*, \end{aligned}\right\} \quad (4.5)$$

The malware -endemic equilibrium (MEE) P^{*MEE} point is obtained through the mathematical computation which are as,

$$S^* = \frac{1}{R_0^{th}},$$

$$I^* = \frac{bR_0^{th} + (\alpha_3 + \rho + \varepsilon)}{\beta}$$

$$E^* = \frac{1}{(\mu + \omega + \alpha_4)R_0^{th}}\left[bR_0^{th} + \rho + \varepsilon + \alpha_3\right]$$

$$L^* = \frac{1}{(\gamma\alpha_1 + \alpha_5\alpha_1 + \alpha_5\eta)}\left[P_1 + P_2 + P_3\right]$$

$$\text{where, } P_1 = \frac{\left((bR_0^{th} + \rho + \varepsilon + \alpha_3) + \sigma(\gamma + \alpha_5) + \gamma\tau\right)}{\xi},$$

$$P_2 = \frac{\mu(bR_0^{th} + \rho + \varepsilon + \alpha_3)}{R_0^{th}(\alpha_4 + \omega + \mu)}, P_3 = \frac{\rho(\gamma + \alpha_5) + \gamma\eta}{R_0{}^{th}}$$

$$R^* = \frac{1}{(\gamma + \alpha_5)}\left[\tau I^* + \varepsilon S^* + \eta L^*\right]$$

where $R_0^{th} = \frac{\omega\beta b}{(\omega + \mu + \alpha_4)(\tau + \sigma + \alpha_2)(\rho + \varepsilon + \alpha_3)}$ is the basic reproduction number [161]. From the expression of R_0^{th}, it can be concluded that when $R_0^{th} > 1$ malware endemic equilibrium (MEE) point exists & unique.

4.5 Evaluation of theoretical findings with Simulation Results

In this section, to evaluate the theoretical findings simulation is performed. The simulation results for the proof of theoretical findings. The impact of various parameters on malware transmission in WSN has been analysed. MATLAB (R2018a) is utilized for the purpose of simulations. For computation, taking the value of various parameters are $b = 0.2, \beta = 0.001, \alpha_1 = 0.00012; \alpha_2 = 0.0015, \alpha_3 = 0.00001, \alpha_4 = 0.00011, \alpha_5 = 0.00013,$ $\rho = 0.002, \mu = 0.002, \omega = 0.001, \gamma = 0.004, \sigma = 0.005, \varepsilon = 0.0002, \tau = 0.003, \eta = 0.004.$ Assume that the number of nodes in the various state at time t=0 is S (0), E (0), I (0), L (0), R (0) and D (0) be 990, 9, 1, 0, 0 and 0 respectively.

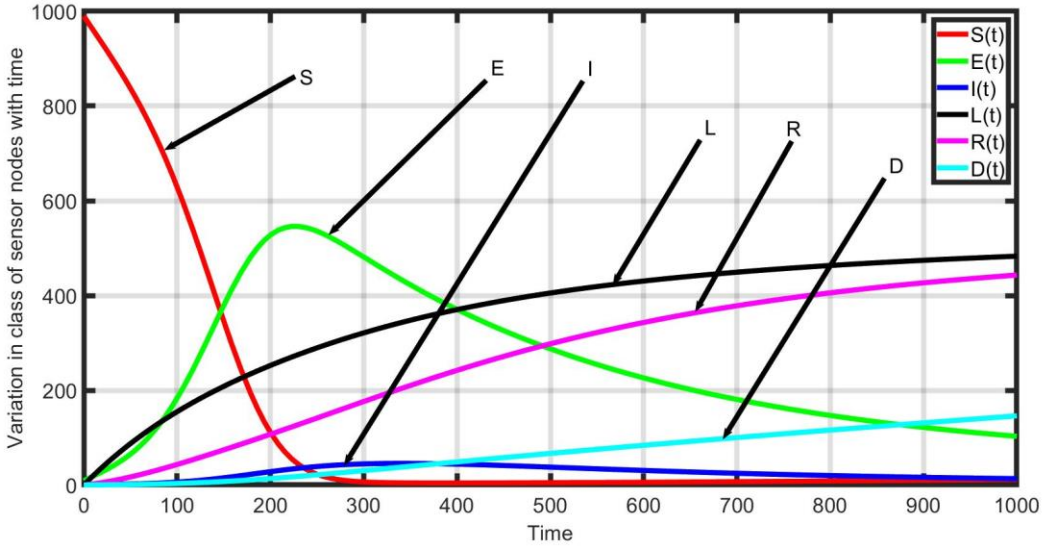

Figure 4.2: Transmission dynamics of malware when $R_0^{th} > 1$

Figure 4.2 shows the changes in number of sensor nodes in different states in respect to time when $R_0^{th} > 1$. The computed value of R_0^{th} =3.063047 which is greater than 1 that means malware persist in WSN. Malware transmit in the network continuously. From figure 4.2, it is noticed that in the beginning number of susceptible nodes are decreasing with time but others are increasing. It is noticed that number of dead nodes are increasing linearly with time. The reason of increasing the number of dead nodes is exhaust of their energy or failure of hardware/software. The figure 4.2 satisfy the second condition of theorem 4.1, when $R_0^{th} > 1$ system will be unstable.

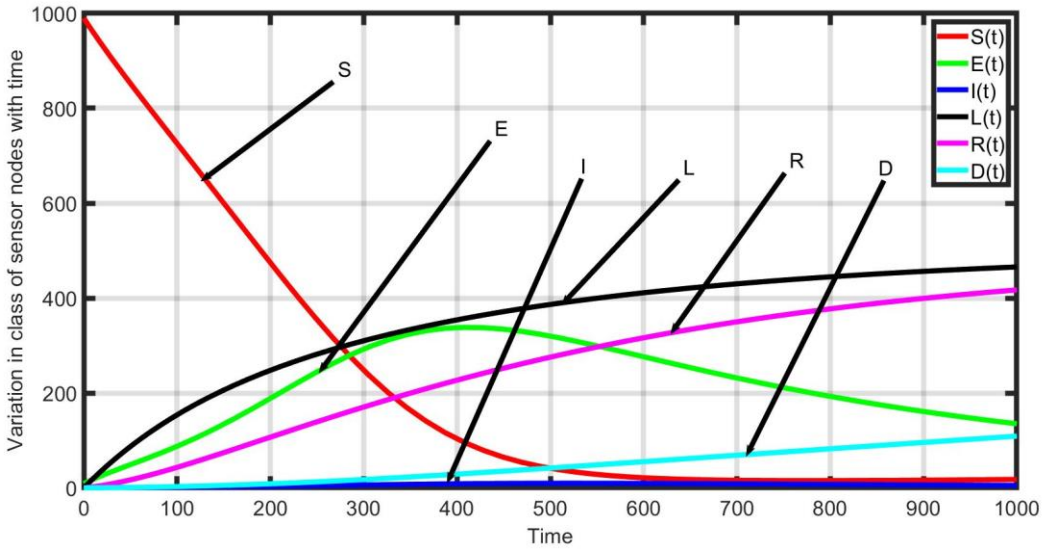

Figure 4.3: Transmission dynamics of malware when $R_0^{th} < 1$

When vary some parameters such as $b = 0.15, \omega = 0.0003$ the value of R_0 also vary. Now the commuted value of R_0^{th} =0.889364, which is less than 1. Figure 4.3 shows the changes in number of sensor nodes in different states in respect to time when $R_0^{th} < 1$. From figure 4.3 it is observed that number of susceptible nodes are decreasing in the beginning and other state of nodes are increasing. The infectious and exposed class of nodes reached to the maximum value then start to decrease and become zero with time. This indicate that malware will not exist in the network for long time or malware will be exterminates from WSN. The figure 4.3 satisfy the first condition of theorem 4.1, when $R_0^{th} < 1$ system will be stable. The analytical study verified by theorem 4.1 and 4.2. So, the system is stable locally and asymptotically at malware-free equilibrium. For designing of the network some parameters need to be considered such as coverage and connectivity. Therefore, to improve the model's performance include the concept of communication radius.

4.6 Improved SEILRD Model

To study the impact of coverage and connectivity on transmission of malware in the sensor network, the SEIRLD model is modified. In this model, the sensor nodes are homogeneous and distributed in uniform manner in a two-dimensional space of length l. Therefore, the total area (A) in which the sensor nodes are deployed is l^2. The total N number of sensor nodes are deployed in the specific area of $A = l^2$. So, the average node density is $d = \frac{N}{A}$.

The communication radius of each sensor node which is deployed in the area of A is r. Hence, the coverage area of each sensor node will be πr^2. The coverage area of sensor node indicates that a sensor node can communicate to all nodes which are lying in their coverage area. In WSN, the sensor node detects the events in their surrounding area and collect the event data first after that transmit to the destination node (sink node) in one hop or multiple hops. We assume that in the beginning all sensor nodes are in susceptible state that can be targeted by malware attack.

In this study, it is assumed that at any time t, total number of $N(t)$ sensor nodes are distributed in the area of l^2 and the number of susceptible sensor nodes are $S(t)$. A sensor node having the communication radius of r and its area of coverage is πr^2.

So, in per unit area density of susceptible nodes

$$d(t) = \frac{S(t)}{A} \tag{4.6}$$

Coverage area of a sensor node

$$A_r = \pi r^2 \tag{4.7}$$

Total number of sensor nodes which are lying under the coverage area of a susceptible sensor node

$$S^{'}(t) = A_r d(t) \tag{4.8}$$

From equations 4.6, 4.7 putting the value of $d(t)$ and A_r in equation 4.8, we get

$$S^{'}(t) = \pi r^2 \frac{S(t)}{l^2} \tag{4.9}$$

Therefore, as per relationship of state transition in figure 4.1, the mathematical model of malware transmission in WSN can be derivative as follows:

$$\left.\begin{aligned}
\dot{S} &= b - \xi SI - (\rho + \alpha_3 + \varepsilon)S, \\
\dot{E} &= \xi SI - (\mu + \omega + \alpha_4)E, \\
\dot{I} &= \omega E - (\tau + \sigma + \alpha_2)I, \\
\dot{L} &= \mu E + \sigma I + \gamma R - (\alpha_1 + \eta)L + \rho S, \\
\dot{R} &= \tau I + \varepsilon S + \eta L - (\gamma + \alpha_5)R, \\
\dot{D} &= \alpha_1 L + \alpha_2 I + \alpha_3 S + \alpha_4 E + \alpha_5 R
\end{aligned}\right\} \tag{4.10}$$

where $\xi = \frac{\pi r^2}{l^2}\beta$

4.6.1 Existence of Malware -Free Equilibrium and Endemic Equilibrium

The class D is not a part of the first five equations of equation (4.10). Therefore, the first five equations of equation (4.10) are not depending on the sixth equation. Hence, to determine the system's equilibrium points equate the first derivative of equation (4.10) to zero.

$$\left.\begin{aligned}
0 &= b - \xi SI - (\rho + \alpha_3 + \varepsilon)S, \\
0 &= \xi SI - (\mu + \omega + \alpha_4)E, \\
0 &= \omega E - (\tau + \sigma + \alpha_2)I, \\
0 &= \mu E + \sigma I + \gamma R - (\alpha_1 + \eta)L + \rho S, \\
0 &= \tau I + \varepsilon S + \eta L - (\gamma + \alpha_5)R,
\end{aligned}\right\} \tag{4.11}$$

Solving equation (4.11) provides the points of system equilibria . The malware-free equilibrium (MFE) point is: $P_0^{MFE} = (S_0, E_0, I_0, L_0, R_0)$, where

$$S_0 = \frac{b}{(\alpha_3 + \rho + \varepsilon)},$$
$$E_0 = 0,$$
$$I_0 = 0,$$
$$L_0 = \left\{ \frac{\rho(\gamma + \alpha_5) + \varepsilon\gamma}{(\alpha_1\alpha_5 + \eta\alpha_5 + \alpha_1\gamma)} \right\} S_0,$$
$$R_0 = \left\{ \frac{\rho\eta + \eta\varepsilon + \varepsilon\alpha_1}{(\alpha_1\alpha_5 + \eta\alpha_5 + \alpha_1\gamma)} \right\} S_0$$

Malware endemic equilibrium (MEE) uniqueness and existence is examined and after mathematical computation it is represented by,

$$S^* = \frac{1}{R_0^{th}},$$
$$I^* = \frac{bR_0^{th} + (\alpha_3 + \rho + \varepsilon)}{\beta}$$
$$E^* = \frac{1}{(\mu + \omega + \alpha_4)R_0^{th}} \left[bR_0^{th} + \rho + \varepsilon + \alpha_3 \right]$$
$$L^* = \frac{1}{(\gamma\alpha_1 + \alpha_5\alpha_1 + \alpha_5\eta)} \left[P_1 + P_2 + P_3 \right]$$

where

$$P_1 = \frac{\left((bR_0^{th} + \rho + \varepsilon + \alpha_3) + \sigma(\gamma + \alpha_5) + \gamma\tau \right)}{\xi},$$
$$P_2 = \frac{\mu(bR_0^{th} + \rho + \varepsilon + \alpha_3)}{R_0^{th}(\alpha_4 + \omega + \mu)}, P_3 = \frac{\rho(\gamma + \alpha_5) + \gamma\eta}{R_0{}^{th}}$$
$$R^* = \frac{1}{(\gamma + \alpha_5)} \left[\tau I^* + \varepsilon S^* + \eta L^* \right]$$

where $R_0^{th} = \frac{\omega\xi b}{(\omega + \mu + \alpha_4)(\tau + \sigma + \alpha_2)(\rho + \varepsilon + \alpha_3)}$ is the basic reproduction number [161]. From the expression of R_0^{th}, it concludes that when $R_0^{th} > 1$ malware endemic equilibrium (MEE) point does exists & is unique.

4.6.2 Evaluation of theoretical findings with Simulation Results

The importance of R_0^{th} is explained in above study. The R_0^{th} is the threshold value on the basis of which to analyse the status of malware in the network. From the analysis, it is concluded that when $R_0^{th} > 1$, fraction of infected nodes persists in the network; and when $R_0^{th} < 1$, fraction of infected nodes become extinct. The theoretical study verified through numerical results. In first case, the value of R_0^{th} (0.517506, 0.895959) when $R_0^{th} < 1$, in this case malware become extinct from the network as per the first condition of theorem 4.1 and theorem 4.2. In second case the value of R_0^{th} (1.51417, 3.951178) when $R_0^{th} > 1$, in this case malware persist in the network and network become unstable as per theorem 4.1 of second condition when $R_0^{th} > 1$. Analyse the transmission dynamics of malware in WSN by taking into account of different parameters simultaneously. Simulation has been performed to study the impacts of different parameters. Outcomes of all these findings are discussed in in following sections.

4.6.2.1 Impacts of Communication Radius of Node (r) on Performance of the System

We know that

$$R_0^{th} = \frac{\omega \pi b r^2 \beta}{(\omega + \mu + \alpha_4)(\tau + \sigma + \alpha_2)(\rho + \varepsilon + \alpha_3) l^2} \tag{4.12}$$

The threshold value of $R_0{}^{th} = 1$. Therefore, to find the threshold value of communication radius (r_{th}) putting the value of $R_0{}^{th} = 1$ in equation (4.12).

$$r_{th} = l\left(\frac{(\omega + \mu + \alpha_4)(\tau + \sigma + \alpha_2)(\rho + \varepsilon + \alpha_3)}{\omega \pi b \beta} \right)^{1/2} \tag{4.13}$$

For simulation the following parametric values are taking into account:

$b = 0.4, \beta = 0.005, \alpha_1 = 0.00012; \alpha_2 = 0.0015, \alpha_3 = 0.00001, \alpha_4 = 0.00011, \alpha_5 = 0.00013,$
$\rho = 0.002, \mu = 0.002, \omega = 0.003, \gamma = 0.004, \sigma = 0.005, \varepsilon = 0.0002, \tau = 0.003, \eta = 0.004, l = 14.$

Putting these parametric values in equation (4.13) and calculated value of $r_{th} = 1.056467$.

Assume that for the different value of r number of nodes in the various state at time t=0 is S (0), E (0), I (0), L (0), R (0) and D (0) be 990, 9, 1, 0, 0 and 0 respectively. The simulation results are illustrated in the figures 4.3(a-d).

Case 1: If $r \le r_{th}$ then $R_0^{th} \le 1$ [103,147], in this case the system is in the state of malware-free and if malware exist that will be extinct from the system and become stable at malware-free equilibrium. This is supported by theorem 4.2.

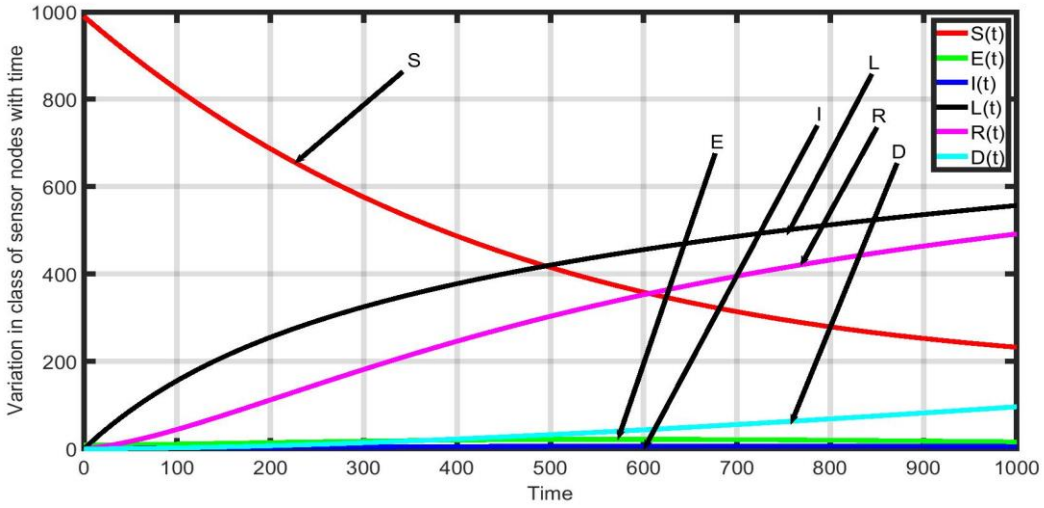

Figure 4.3 (a): Malware transmission dynamics in WSN ($r = 0.76$)

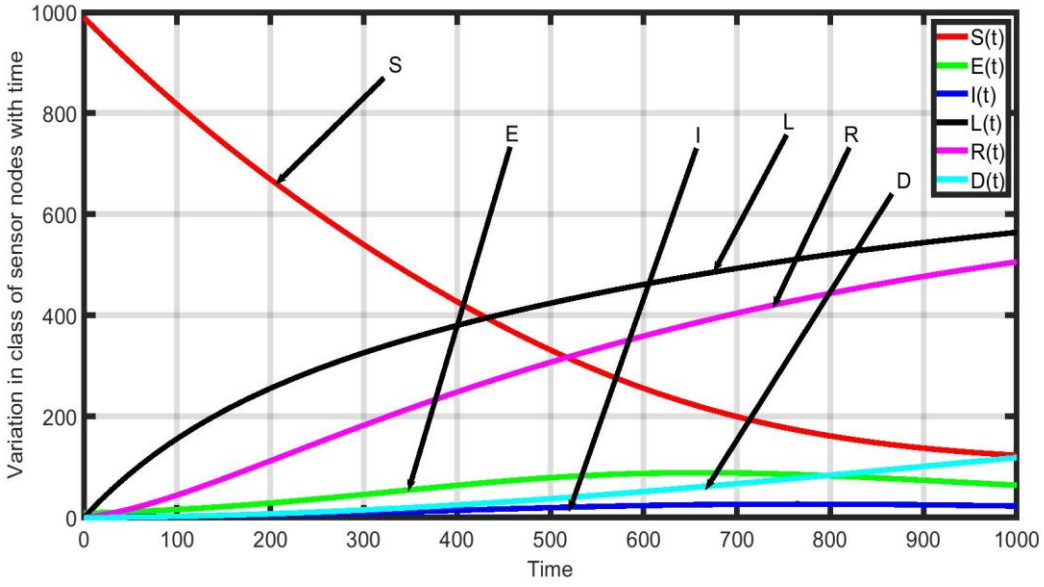

Figure 4.3 (b): Malware transmission dynamics in WSN ($r = 1.0$)

Figures 4.3 (a-b) show the system stability in malware free state and in this case value of $r \le r_{th}$ and $R_0^{th} \le 1$. For figure 4.3 (a), the value of $r = 0.76$ then $R_0^{th} = 0.517506$ and for figure 4.3 (b), the value of $r = 1.0$ then $R_0^{th} = 0.895959$. Both will satisfy the condition of malware free equilibrium and system exist in the stable state. The simulation outcomes are consistent with theoretical findings. Figures 4.3 (a-b) justify the theoretical findings. Figures 4.3 (a-b)

satisfy the condition of malware free equilibrium and system will exist in stable state. The number of dead nodes linearly increasing in the system due to drain of sensor nodes energy or failure of software/ hardware.

Case 2: If $r > r_{th}$ then $R_0^{th} > 1$ [103,147], in this case the system is in the unstable state and malware will exist in the system. This is supported by theorem 4.1 of second condition. And in this case system will be in stable state at endemic equilibrium.

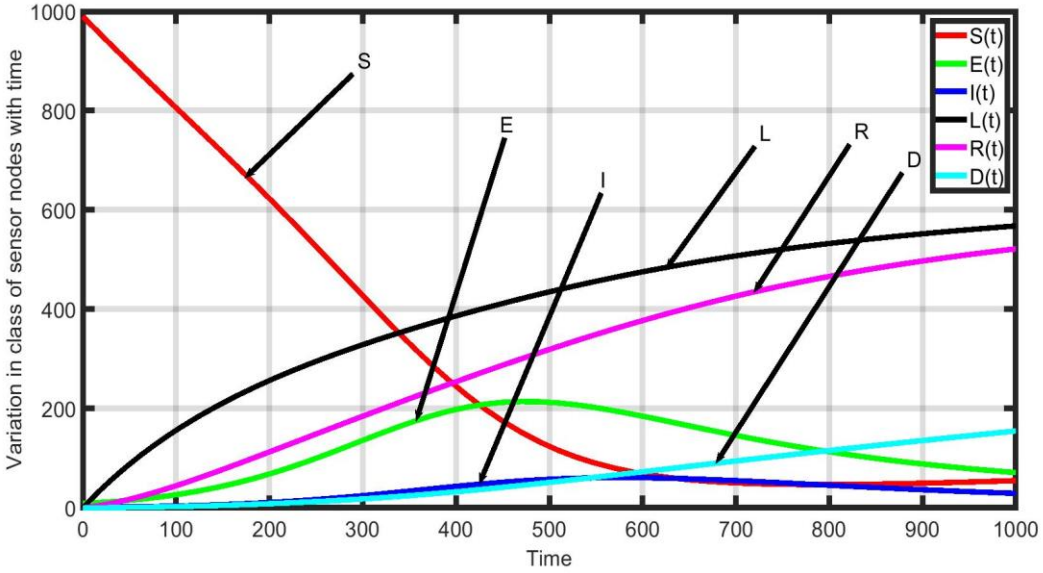

Figure 4.3 (c): Malware transmission dynamics in WSN ($r = 1.3$)

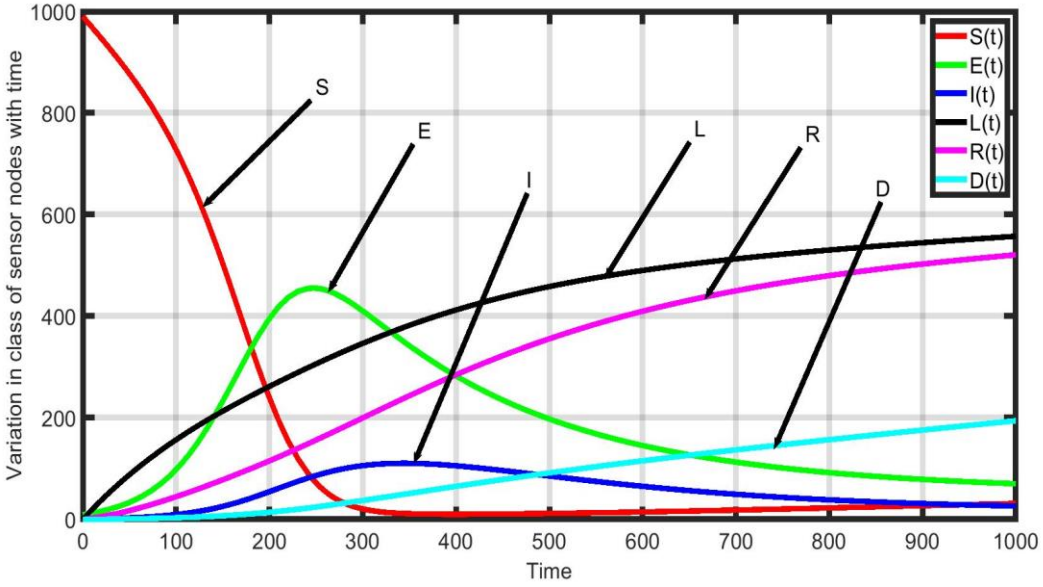

Figure 4.3 (d): Malware transmission dynamics in WSN ($r = 2.1$)

Figures 4.3 (c-d) show the system stability at endemic state and in this case value of $r > r_{th}$ and $R_0^{th} > 1$. For figure 4.3 (c), the value of $r = 1.3$ then $R_0^{th} = 1.514170$ and for figure 4.3 (d), the value of $r = 2.1$ then $R_0^{th} = 3.951178$. Figures 4.3 (c-d) satisfy the condition of endemic equilibrium and system in the unstable state. Figures 4.3(c-d) show that in the beginning susceptible number of nodes are decreasing and others are increasing. The number of exposed and infectious nodes reach to the maximum value after that start to decrease and attain the steady state and on other side then susceptible number node start to increase. This shows that malware exist continuously in the system. The simulation outcomes are consistent with theoretical findings. The number of dead nodes linearly increasing in the system due to drain of sensor nodes energy or failure of software/ hardware.

Connectivity establishment among nodes of WSN is a crucial problem; the important factor which influences the connectivity of network is communication radius (r). Therefore, connectivity is a function of r.

On the basis of above study based on communication radius (r), the following observations are highlighted.

1. For improvement in the connectivity of network it is required to increase the size of communication radius (r). With the increase in the size of r value of R_0^{th} start to increase. The system will be stable in malware free state when the value of $r \le r_{th}$. The details are discussed in case 1.
2. The infectious number of nodes increase with increase in the size of r because if size of r is large then the greater number of susceptible sensor nodes come in contact with an infectious node simultaneously. So, in this condition greater number of susceptible nodes converted into infectious state at a time. The details are discussed in case 1 and case 2.
3. The impact of r on transmission dynamic of malware shown that; the threshold value of r optimizes, that help in controlling the malware transmission, malware eradication, and enhancement in lifetime of WSN.
4. Basic reproduction number (R_0^{th}) is directly proportional to communication radius (r) from equation (4.12).

4.6.2.2 Impacts of Node Density (d) on Performance of the System

Putting the value of $R_0^{th} = 1$in equation (4.12), the threshold value of node density d_{th} is determined as follows:

$$1 = d_{th} \frac{\omega \pi r^2 b \beta}{N(\omega + \mu + \alpha_4)(\tau + \sigma + \alpha_2)(\rho + \varepsilon + \alpha_3)}$$

$$d_{th} = \frac{N(\omega + \mu + \alpha_4)(\tau + \sigma + \alpha_2)(\rho + \varepsilon + \alpha_3)}{\pi r^2 b \omega \beta} \tag{4.14}$$

For simulation the following parametric values are taking into account:

$b = 0.4, \beta = 0.005, \alpha_1 = 0.00012; \alpha_2 = 0.0015, \alpha_3 = 0.00001, \alpha_4 = 0.00011, \alpha_5 = 0.00013, r = 1.0,$
$\rho = 0.002, \mu = 0.002, \omega = 0.003, \gamma = 0.004, \sigma = 0.005, \varepsilon = 0.0002, \tau = 0.003, \eta = 0.004, N = 1000.$

Putting these parametric values in equation (4.14) and calculated value of $d_{th} = 5.694504$.

Assume that for the different value of d number of nodes in the various state at time t=0 is S (0), E (0), I (0), L (0), R (0) and D (0) be 990, 9, 1, 0, 0 and 0 respectively. The simulation results are illustrated in the figures 4.4 (a-d).

Case 1: If $d \le d_{th}$ then $R_0^{th} \le 1$ [103,147], in this condition the system is in the state of malware-free and if malware exist that will be extinct from the system and becomes stabilize at malware-free equilibrium. This is supported by theorem 4.2.

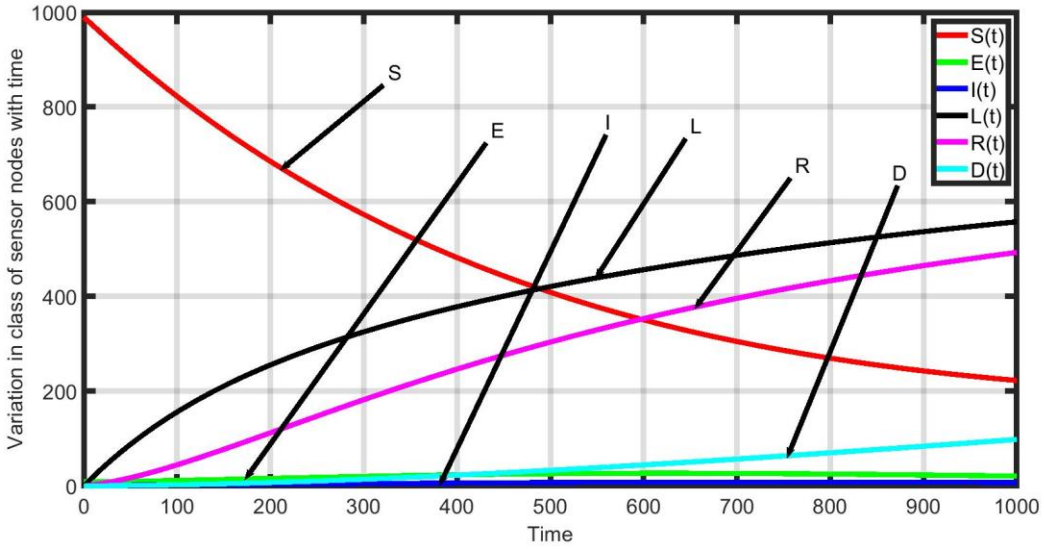

Figure 4.4 (a): Malware transmission dynamics in WSN ($d = 3.2$)

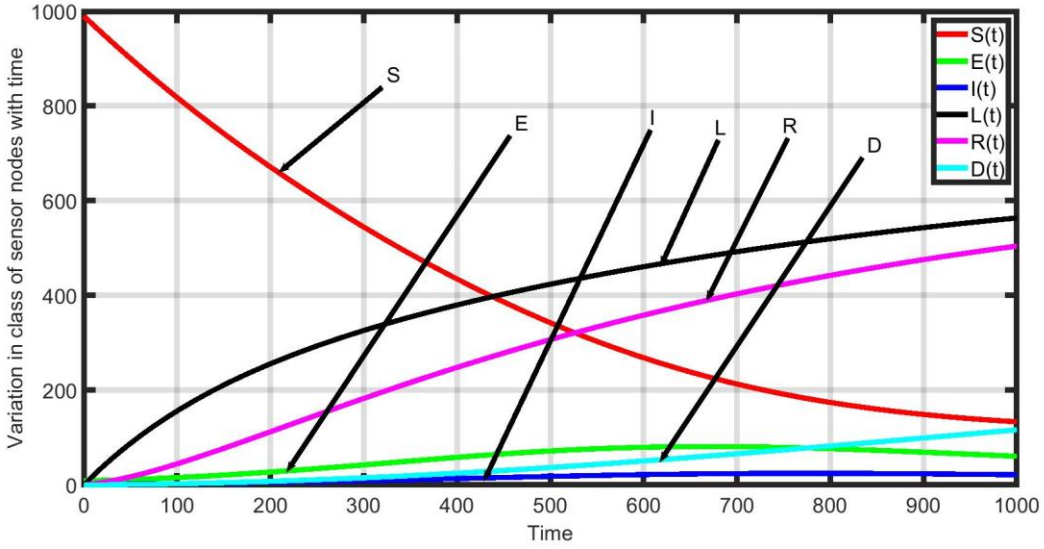

Figure 4.4 (b): Malware transmission dynamics in WSN ($d = 4.9$)

Figures 4.4 (a-b) show the system stability in malware free state and in this case value of $d \le d_{th}$ and $R_0^{th} \le 1$. For figure 4.4 (a), the value of $d = 3.2$, $l = 17.67767$ then $R_0^{th} = 0.561945$ and for figure 4.4 (b), the value of $d = 4.9$, $l = 14.285714$ then $R_0^{th} = 0.860479$. Figures 4.4 (a-b) justify the theoretical findings. In the beginning susceptible number of sensor nodes are decreasing and remaining are increasing. After some time, infectious number of nodes becomes zero in the system. This can be shown in simulation by increasing the time. Figures 4.4 (a-b) satisfy the condition of malware free equilibrium and system will exist in stable state. The number of dead nodes linearly increasing in the system due to exhaust of sensor nodes energy or failure of software/ hardware.

Case 2: If $d > d_{th}$ then $R_0^{th} > 1$ [103,147], in this case the system is in the unstable state and malware will exist in the system. This is supported by theorem 4.1 of second condition. And in this case system will be in stable state at endemic equilibrium.

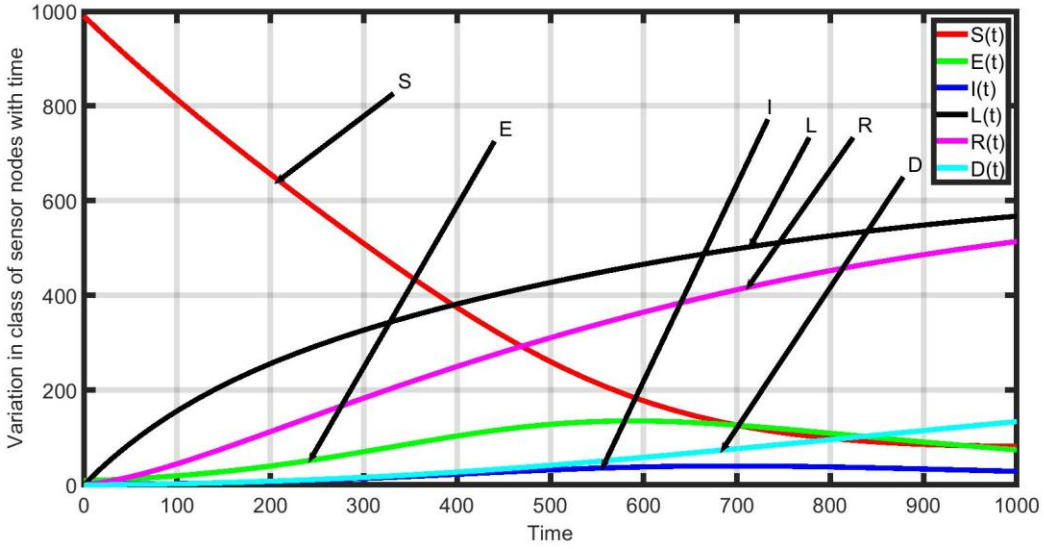

Figure 4.4 (c): Malware transmission dynamics in WSN ($d = 6.3$)

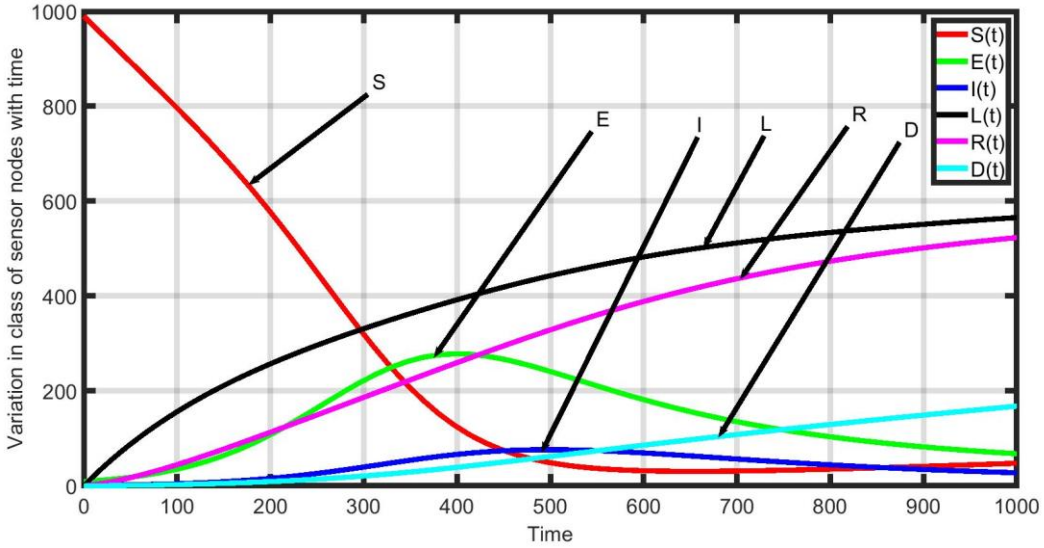

Figure 4.4 (d): Malware transmission dynamics in WSN ($d = 11$)

Figures 4.4 (c-d) show the system stability at endemic state and in this case value of $d > d_{th}$ and $R_0^{th} > 1$. For figure 4.4 (c), the value of $d = 6.3$, $l = 12.598816$ then $R_0^{th} = 1.10633$ and for figure 4.3 (d), the value of $d = 11$, $l = 9.534629$ then $R_0^{th} = 1.931687$. Figures 4.4 (c-d) satisfy the condition of endemic equilibrium and system in the unstable state. Figures 4.4 (c-d) show that in the beginning susceptible number of nodes are decreasing and others are increasing. The number of exposed and infectious nodes reach to the maximum value after that start to decrease and attain the steady state and on other side then susceptible number node start to increase. This shows that malware exist continuously in the system. The simulation outcomes are consistent with theoretical findings. The number of dead nodes

linearly increasing in the system due to drain of sensor nodes energy or failure of software/ hardware.

Node density (d) also effects the connectivity of WSN like communication radius (r). On the basis of above study based on node density (d), the following observations are highlighted.

1. It can be established from figures 4.4 (a-d), when increase in node density the connectivity among the nodes also increases. When number of sensor nodes increases and area of deployment is constant then the distance between sensor will be small. Hence, connectivity among the sensor nodes will be strong. This is explained in case 1 and case 2.
2. As the value of node density increases the value of R_0^{th} also increases. This weakens the system stability. In the case of high node density an infectious sensor node can communicate with large number of susceptible sensor nodes simultaneously and infect them. Hence, the value of R_0^{th} increases rapidly due to large number of infectious nodes increase quickly. This can be visualized from figures 4.4 (a-d).
3. To enhance the lifetime of WSN method of optimization can be applied (by cautiously deployment of sensor nodes in the sensor field). By the use of concept of threshold of node density, we can establish the malware free network and overcome of communication overhead in the network and made economically feasible.

4.7 Performance Analysis of the Proposed Model

The proposed model's performance is impacted by the different parameters such as rate of infection (β), charging rate of sensor nodes (η), recovery rate (τ), response of susceptible state of sensor nodes etc. The impact of parameters is elaborated through numerous graphs which are demonstrated in figures 4.5 to 4.11.

It is noted from figure 4.5 that if recovery rate (τ) value is fix and varying the value of infection rate (β), the count of infected sensor nodes changes. When increases the value of infection rate (β) the count of infected sensor nodes increases. Whereas if the value of infection rate (β) is fix and increase the recovery rate (τ) the count of infected sensor nodes decreases in the system with increase the value of τ .

Therefore, to overcome the problem of malware transmission in the network, it is necessary to execute the anti-malware at faster rate in WSN.

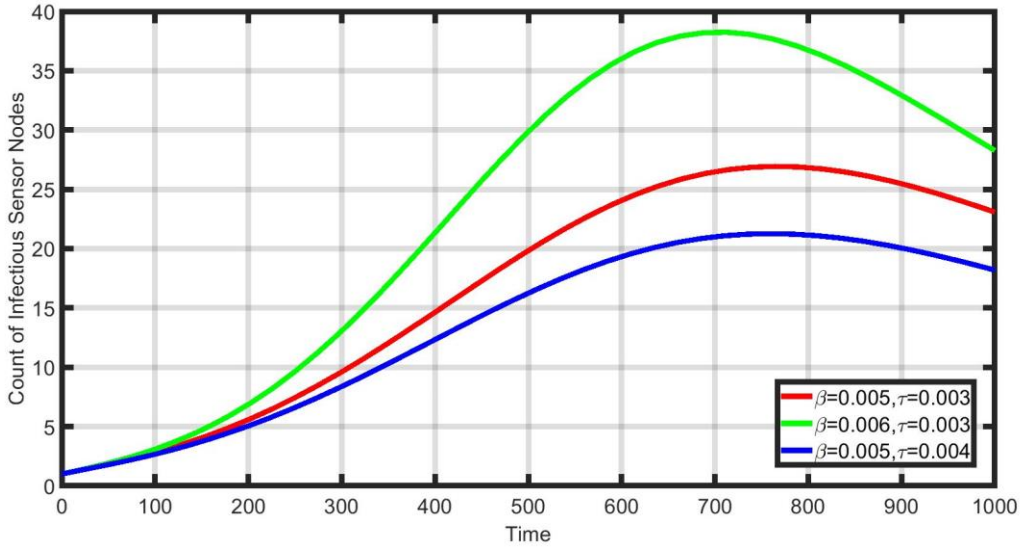

Figure 4.5: Impact of recovery rate on infectious nodes

The observations of figure 4.5 supported by the figure 4.6. From figure 4.6 it is noted that if the value of infection rate (β) is affix and increase in the value of recovery rate (τ) a greater number of susceptible sensor nodes exist in the system with higher recovery rate. On the other hand, if value of recovery rate (τ) is fixed and infection rate (β) changes the lesser number of susceptible nodes exist in the system when infection rate (β) is higher. The conclusion drawn from figures 4.5 and 4.6 if rate of infection is higher count of infectious sensor nodes are greater and susceptible sensor nodes are lower.

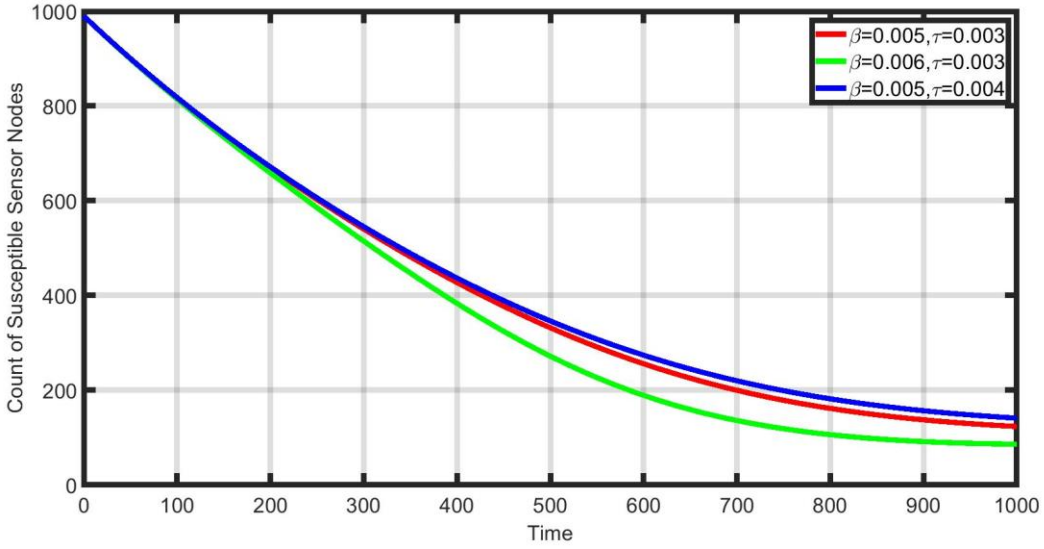

Figure 4.6: Impact of recovery rate on susceptible nodes

The impact of infection rate presented with the help of figure 4.7. It is noticed from figure 4.7 that as the rate of infection increases the count of infectious sensor node increase in the network. The count of infectious sensor nodes reaches to the maximum then begin to decline and attain the steady state or become zero, this depends on the value of R_0^{th}. The value of R_0^{th} depends on other parametric values including the rate of infection. In case of higher value of β transmission rate of malware is also high in comparison to lower value.

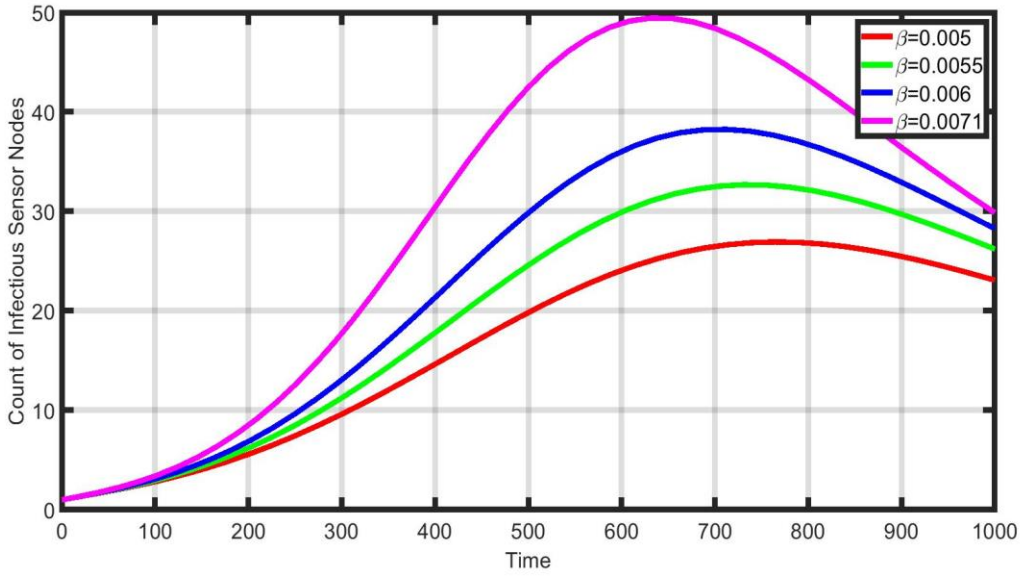

Figure 4.7: Impact of infection rate on malware transmission

The impact of infection rate (β) on exposed sensor nodes and infectious sensor nodes is plotted in figure 4.8. If the value of β is higher, then the count of exposed as well as infectious sensor nodes is higher. Because exposed nodes converted into infectious nodes after a certain interval of time that time is known as latent period. The latent period is used to control the transmission of malware in the network by applying the corrective action on time. When the node is in exposed state, it can be detected early in exposed state and apply preventive action on them to stop transmission.

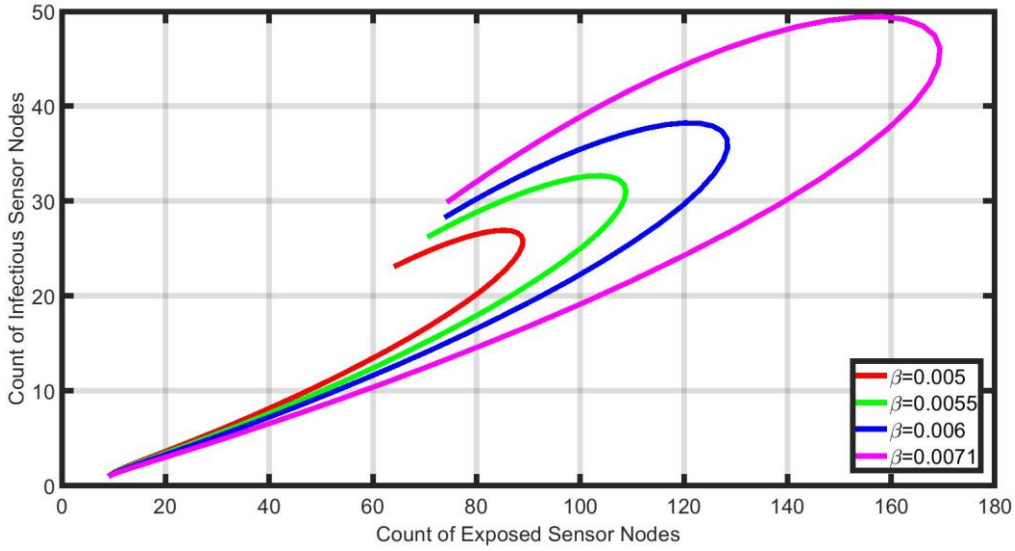

Figure 4.8: Impact of recovery rate on susceptible nodes

The impact of recovery rate on exposed state of sensor nodes is explained with the help of figure 4.9. If the value of recovery rate (τ) is fixed and change the value of ω from 0.003 to 0.007, as the value of ω increases count of infectious nodes increases and if value of ω is fixed and value of τ increases from 0.003 to 0.005. It is found that as the value of τ increases count of recovered nodes also increases. This indicates that if the rate of conversion from exposed state to infectious state is high then a greater number of nodes converted into infectious state. The corrective method applies in exposed state of nodes to prevent the malware transmission in WSN. If the execution rate of anti-malware is high the lesser count of exposed nodes converted into infectious state.

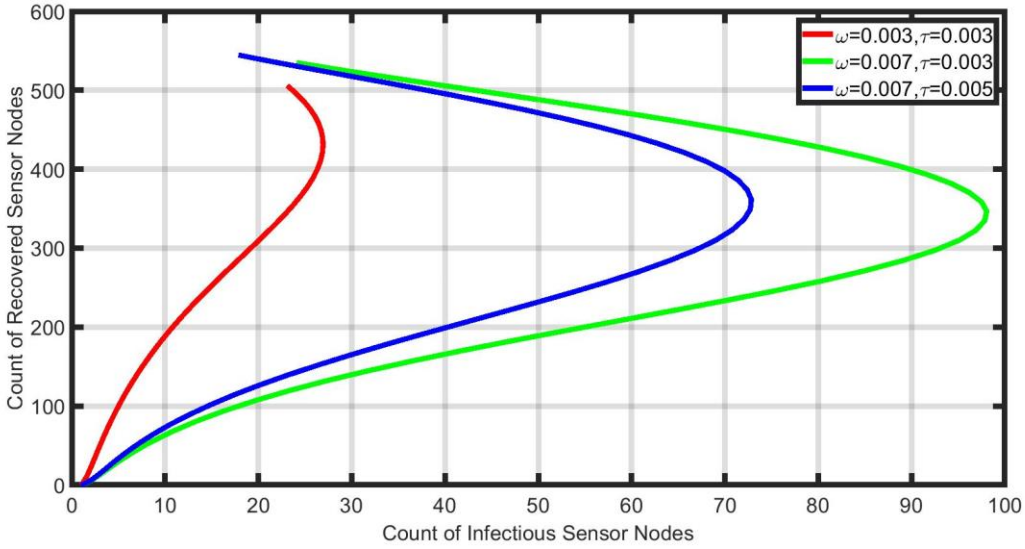

Figure 4.9: Impact of recovery rate on exposed nodes

The impact of various parameter is discussed in figure 4.10 and 4.11 such as infection rate, charging rate i.e., from low-energy state to recovered state, from infectious state to low-energy state etc. From figure 4.10 it is observed that if the rate of infection is high then initially count of infectious sensor nodes increases attain the maximum count and then start to decrease due effect of charging and rate of recovery.

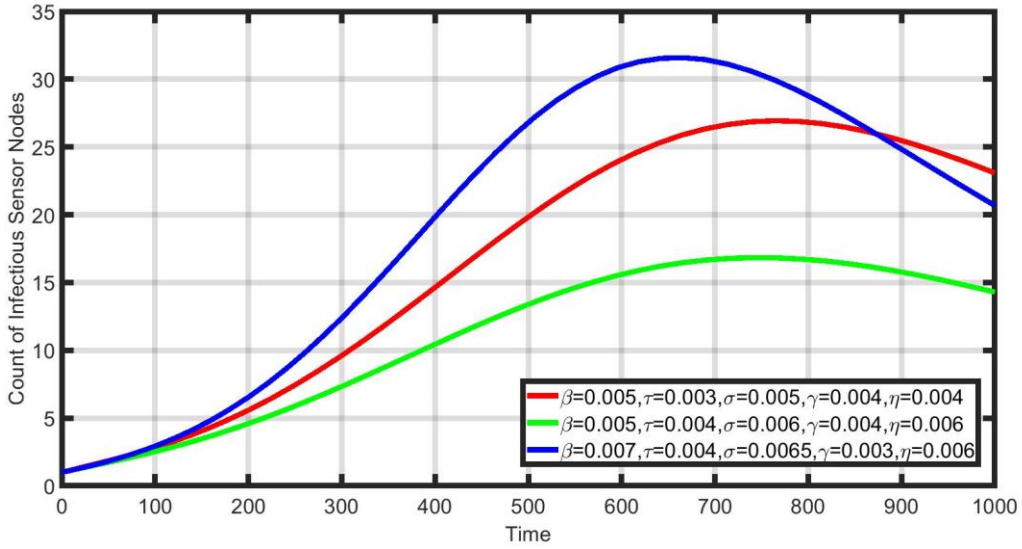

Figure 4.10: Impact of various parameter on recovered nodes

Figure 4.11 support the result of figure 4.10. The larger number of infectious sensor nodes converted into recovered state when rate of recovery and charging rate of sensor nodes are

high. The figure also illustrates the importance of charging of sensor nodes with low energy-state.

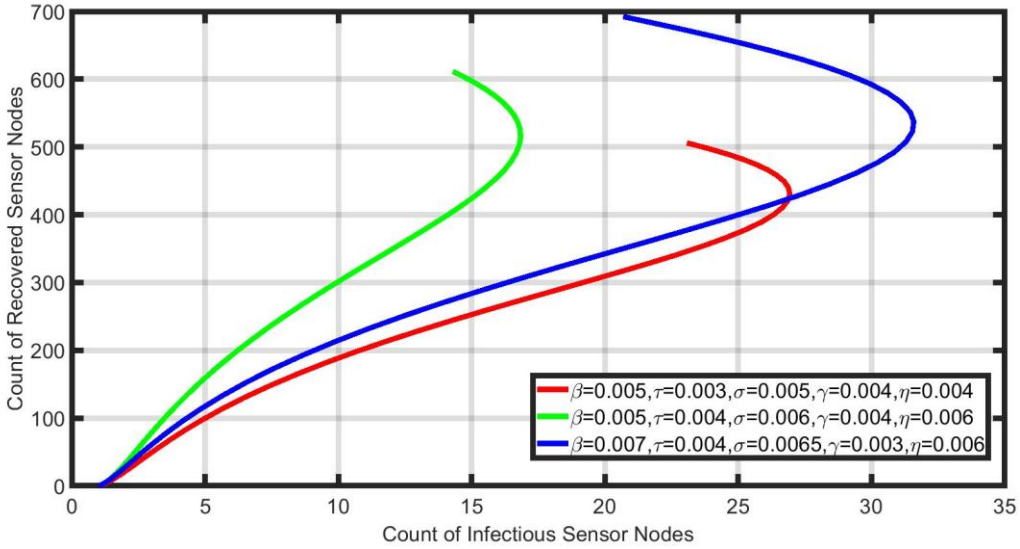

Figure 4.11: Impact of various parameter on infectious and recovered nodes

The effect of charging of low-energy sensor node is illustrated in figure 4.12 and 4.13. Consider the case of charging and without charging of low-energy sensor nodes. It is found from figure 4.12, that when apply the mechanism of charging of sensor nodes count of recovery nodes increases with time in respect to without charging. And figure 4.13 shows that lesser count of nodes resides in infected state with charging. The method charging enhance the network lifetime and overcome the problem of operational overhead.

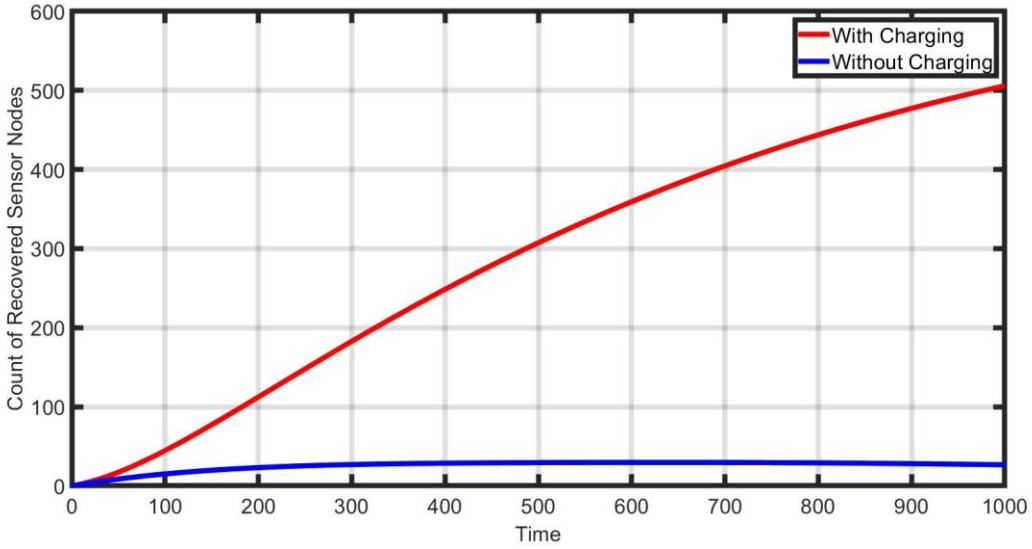

Figure 4.12: Impact of charging on recovery of sensor nodes

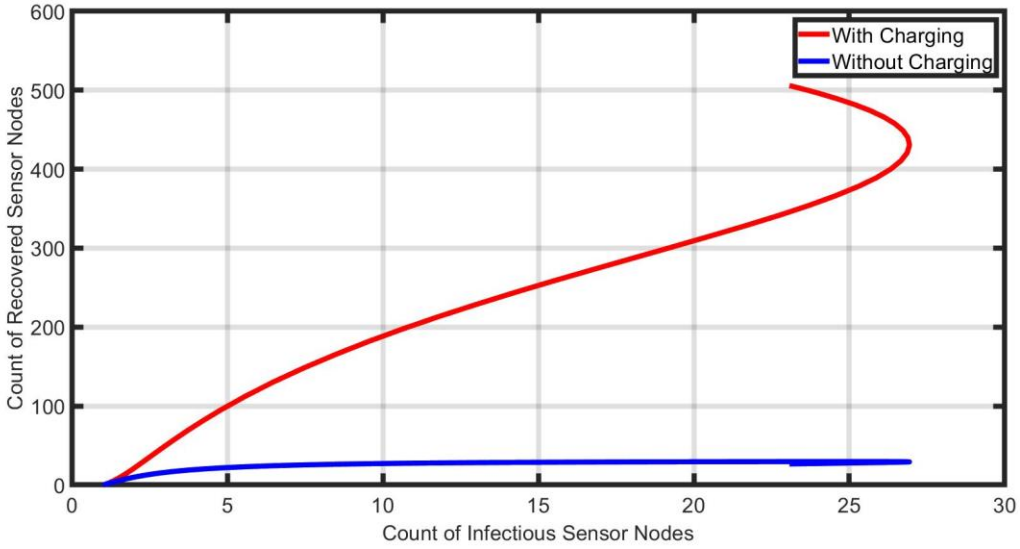

Figure 4.13: Impact of charging on infectious and recovered nodes

4.8 Comparative Analysis between Proposed Model and Other Models

In this section, comparative analysis is carried out between proposed model and SEIRS [149] existing model. For comparative analysis keep the all parameters same in both the cases and vary the communication radius (r). For better connectivity design communication radius is a crucial design parameter.

Figures 4.14 (a-c) illustrate that the performance of proposed model is better in respect to the SEIRS [149] existing model for the distinct value of communication radius (r). The graph is plotted between the count of exposed and infectious nodes and time. The count of exposed sensor nodes is increasing as the size of communication radius is increasing. The similar type of behaviour is also shown in case of infectious sensor nodes as exposed sensor nodes. In both the cases proposed as well as existing model dynamics of malware transmission in the network is similar but when compared with the proposed model the increment of exposed and infected nodes is lesser in comparing with existing model. The proposed model suggests the technique for design of sensor node through which develop a secure and strong connecting system. So, proposed model suggesting the better mechanism for controlling of malware transmission in WSN.

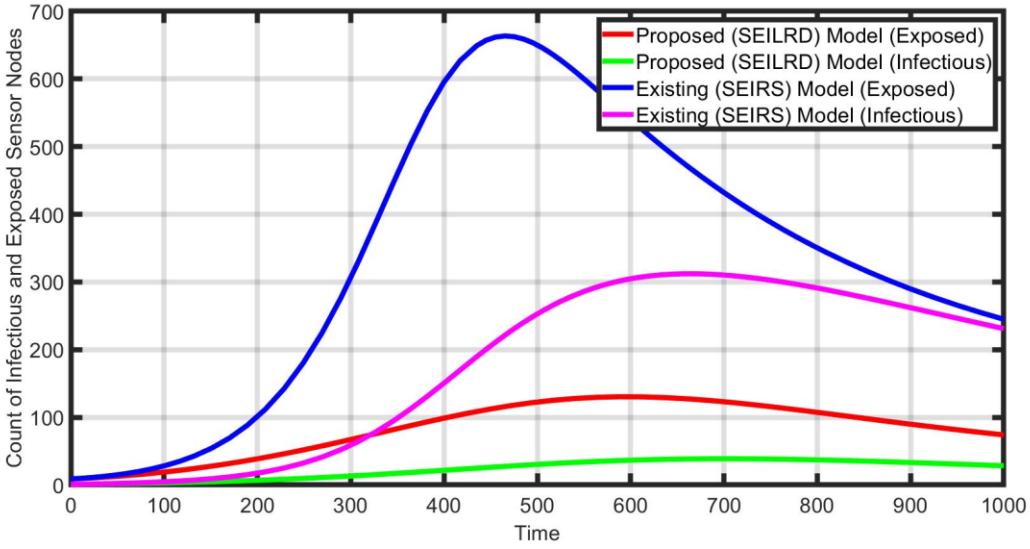

Figure 4.14 (a): Communication Radius ($r = 1.1$)

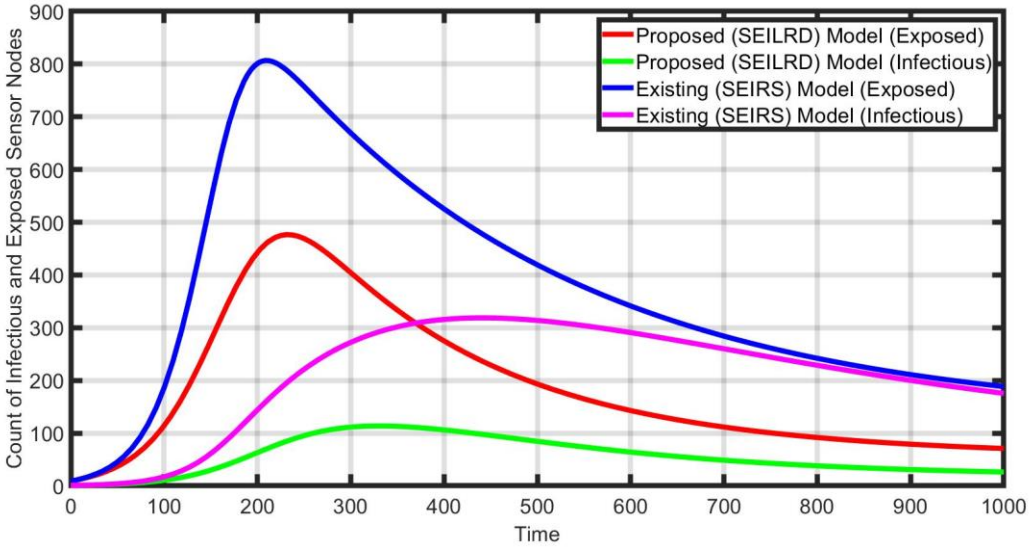

Figure 4.14 (b): Communication Radius ($r = 2.2$)

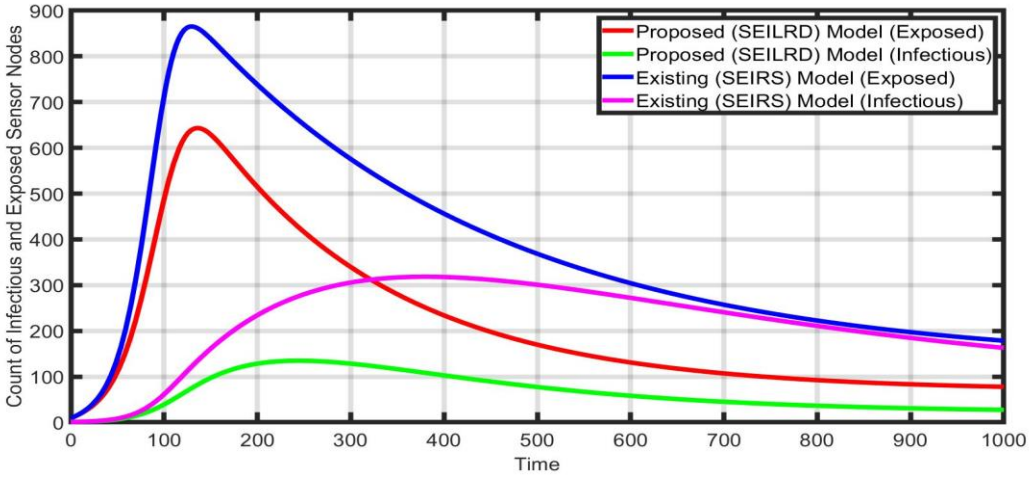

Figure 4.14 (c): Communication Radius ($r = 3.4$)

Figures 4.15 (a-c) illustrate that the performance of proposed model is better in respect to the SEIRS [149] existing model for the distinct value of node density (d). The graph is plotted between the count of exposed and infectious nodes and time. The count of exposed sensor nodes is increasing when the value of node density is increased. The similar type of behaviour is also shown in case of infectious sensor nodes as exposed sensor nodes. In both the cases proposed as well as existing model the dynamics of malware transmission in the network is similar but the increment of exposed and infected nodes is lesser in proposed model when comparing with existing model. The model provides the method of deployment of sensor nodes in sensor field in optimum manner. So, proposed model suggesting the better mechanism for controlling of malware transmission in WSN.

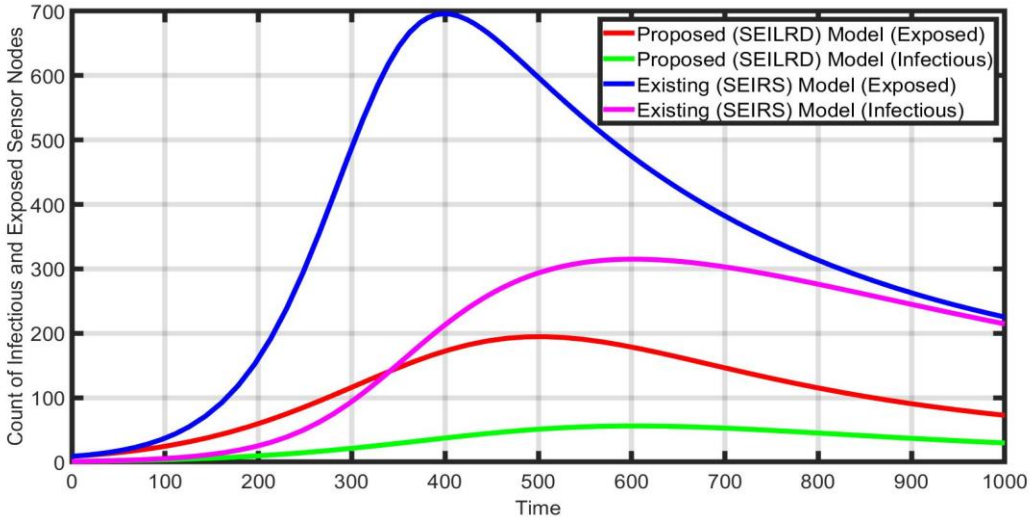

Figure 4.15 (a): Node Density ($d = 8$)

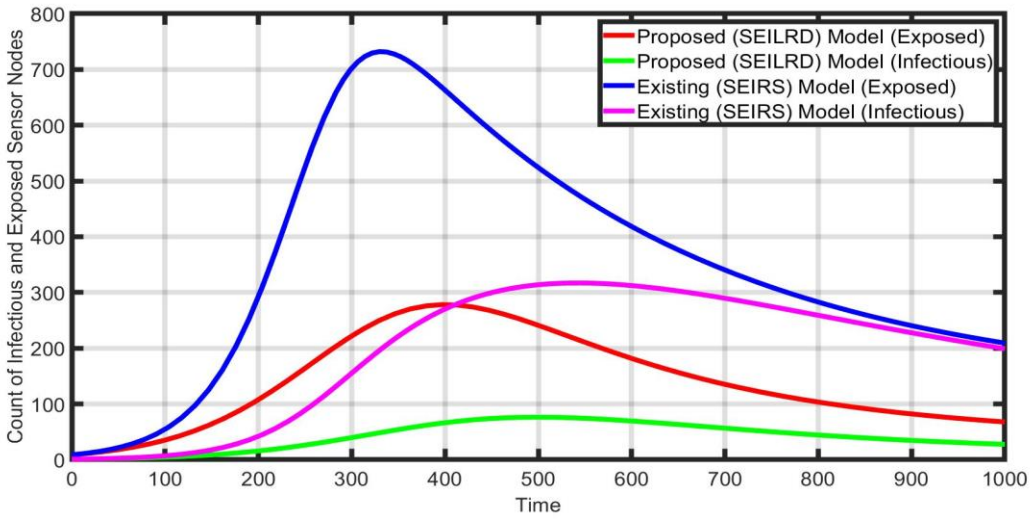

Figure 4.15 (b): Node Density ($d = 11$)

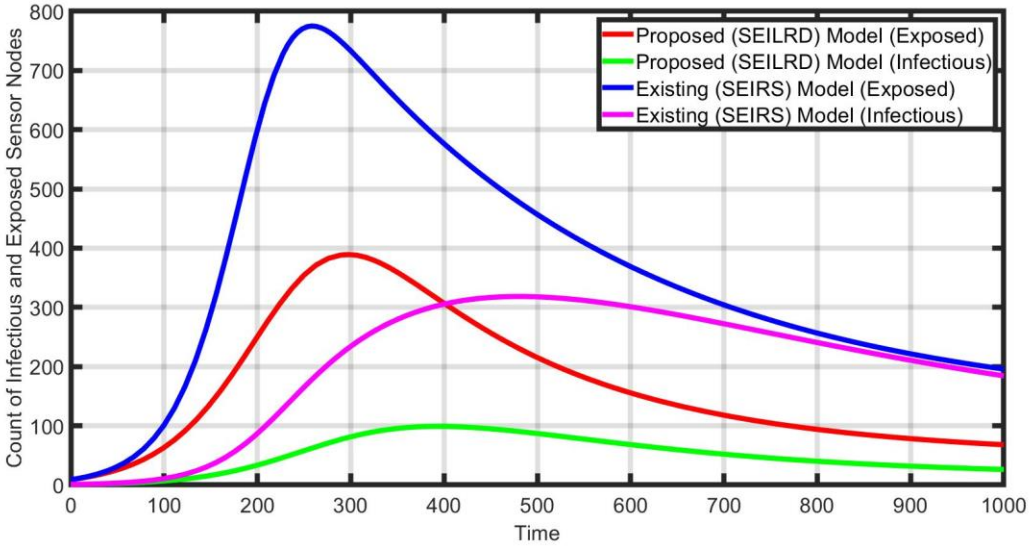

Figure 4.15 (c): Node Density ($d = 17$)

From figures 4.14 (a-c) and 4.15 (a-c) show that count of infectious nodes in both the models are not approaching to zero, this is the state of endemic equilibrium. Additionally, due to non-zero rate of infection, the peaks of both exposed and infectious sensor nodes are substantially greater. When an attack occurs in the system then an appropriate and pertinent security mechanism is needed to exterminate malware from the network for that purpose the mechanism applies through the proposed model. The model used the concept of exposed state and charging of low-energy state nodes.

4.9 Summary of the Chapter

An epidemic SEILRD model is proposed for controlling of malware transmission as well as elongate the lifetime of WSN. It is an extension of SILRD model which is discussed in chapter 3. Furthermore, in the proposed model an exposed state (E) is used to identify the movement of sensor nodes from susceptible to infected state in early stage. Such detection provides an opportunity to moreover implement methods to control the transmission of malware in WSN under the various situations. Early identification of malware presence helps in network maintenance and smooth operation. The limitations of SILRD model overcome by an amended SEILRD model through the mechanism of charging. The sleep mode of sensor node is used for maintenance of the system like malware detection and eradication. The proposed model use to improve the anti-malware potential for the network, it can perfectly and assuredly acclimate to new and different types of malwares. There is no need of any extra hardware and occurrence of signalling overhead in the proposed model. For the study of transmission dynamics of

malware in WSN the computation of R_0^{th} is essential. R_0^{th} is one of the critical parameters which play an important role in controlling of malware transmission in WSN.

Coverage and connectivity are also important parameter in WSN, therefore an improved SEILRD model is also discussed. Which explained in details about the coverage and connectivity of the system. Moreover, discussed that malware-free equilibrium is locally and globally asymptotically stable if the value of $R_0^{th} \leq 1$, network unstable condition is $R_0^{th} > 1$. The endemic stability (if the value of $R_0^{th} > 1$) is also explained by the simulation results. For better design of WSN computed the threshold value of communication radius, that help in controlling of malware transmission and lifetime enhancement of WSN. One another important concern is sensor node deployment in sensor field, for that purpose computed the threshold value of node density which provide the information the number of nodes required to deploy in the sensor fields for smooth and secure communication and optimize the cost of deployment. In this chapter also discussed the relationship of R_0^{th} with r and d. The impact of charging and importance of low-energy state is also discussed in details.

Additionally, for the validity of proposed model carried out the simulation using MATLAB (R2018a). The effect of different parameters on transmission of malware in WSN in different conditions has been meticulously analysed. The comparative evaluation between SEIRS and SEILRD has been performed. The comparative analysis shows that lesser count of exposed and infectious sensor nodes in proposed SEILRD model in respect to existing SEIRS model. Extensive outcomes provide substantial evidence that the proposed model ensures increased the network lifetime and better security mechanism against malware attack.

Chapter 5: Investigation of Multi-Malware Attack in Wireless Sensor Networks using Epidemic Model

5.1 Introduction

Today, the world is facing a new danger from the cyber world and that is the malware attack. With the emerging technologies like the Internet of things (IoT), industry 4.0, etc., the exposure of WSN to such malware attacks have become a common sight. As the usage of WSN is inevitable in these emerging technologies and since it is used in various fields like agriculture, medical, transportation, etc., preventing the malware attack in WSN is the need of the hour. There are thousands of sensor nodes in WSN and according to the usage of WSN in various applications, these nodes can be either randomly distributed or it could be distributed in a fixed way. The main works of these sensor nodes involve the gathering of information from the surrounding areas and also to deliver the information gathered to the destination node/sink/ terminal node. The data which is gathered by the sensor nodes are sent to the destination node/sink/ terminal node by using the technique of multi-hop because the distance of the sensor node is very large in comparison to the area to be covered of the sensor node. The WSN application is an advantage in varied areas but various issues like energy constraints, sensor nodes deployment, security issues, etc., also crop up due to the limited availability of energy, memory, processor etc., in WSN. As the malware attacks are becoming a threat to the normal workings of WSN and the security of WSN is becoming questionable, this problem needs a thorough analysis and a quick solution. The malware is implanted into the network by the attacker and does not naturally start by itself. It is created in an artificial manner by the attacker. But once it comes into the network, it can propagate on its own and spread into the network widely and quickly without any human help.

WSN is vulnerable to malware attack just as the computer network is vulnerable to virus and worm attacks. The method used for data transmission in WSN is wireless communication and this increases the chance of malware attacks on WSN and as the topology of WSN is complex, WSN is more prone to such attacks in comparison to the computer networks. The sensor nodes are spread widely in WSN and these nodes carry valuable and confidential information and if these nodes are attacked by the malware, there would be destruction of such valuable

information. The attacker does this purposefully. The attacker either wants to change the data or steal it or maybe he wants to destroy it completely. The attacker first infects the sensor nodes and from such infected nodes, the infection spreads widely to the rest of the nodes and then into the entire network. As a result, the functioning of the network would stop if precautions are not taken timely.

After a detailed analysis and study of the mannerisms of the malware attack in WSN, various researchers have devised varied procedures to prevent such attacks on WSN. One such mechanism is the epidemic modelling which may be considered appropriate to find out the spread of malware in WSN because any virus spreads in the same manner in the population too. So, theory of epidemiology is applied to investigate malware transmission in WSN.

SIR-M model proposed by Tang and Mark [131] and suggest a mechanism of maintenance during the sleep mode of WSN and describe the spreading dynamics of the virus process from a single sensor node to the whole WSN. They presume that everlasting immunity is achieved by the recovered sensor nodes, but this is far away from the truth in real cyber or digital world. So, the recovered sensor nodes of the network may again be infected by anew emergent worms. Feng et al. [147] have used the SIRS model in which the role of communication radius and the density of the node on the worm spread is discussed along with their threshold value. The contribution of the basic Reproductive number (R_0^{th}) has also been explained by them.

The idea of latent period or exposed state of model is introduced to identify the appearance of worm in the network at early stage. The different models which are based on epidemiology and considered the exposed state in the model is discussed in chapter 4. Some of the models are explained here. López et al. [148] has meticulously explained the arbitrary jamming through the SEIS model which further proves the efficacy of the model. Ojha et al. [149] presented a SEIRS epidemic model. Through this model, they have briefly explained the effect of parametric values on the worm spreading in WSN. An improved SEIR model is proposed by Liu et al. [150] with consideration of mutation of virus. The R_0^{th} of the imporoved SEIR model is computed and analysed the stability of the model for two equilibrium points local and global. Optimal control strategy is discussed and analyse the effects of different parameters on the value of R_0^{th}. The stability of the model is validated by simulation results.

Haghighi et al. [167] have ventured into explaining the outcome of geospatial structure on the worm through the geographical SI model which is a mix of epidemic model and geometrical structure. Keshri and Mishra [166] through the SEIRS epidemic model have discussed as to what would the effect of delay in transmission be on the dissemination of malevolent signals in WSN. They have taken into consideration both the delays in the model-the first one being the latent period and the next delay as the temporary immunity period.

There might be a possibility of many types of malware attack at a given point of time. The above-mentioned models are taking into consideration a single type of malware attack. But in case there are multiple attacks, then, preventive measures should be taken so that the functioning of the system is not hampered. Ojha et al. [168] proposed a model in which two types of malware attack at the same time have been considered. This model is based on epidemic modelling. Existence of equilibria and stability of WSN at various points have been discussed. Further, Liu and Zhang [169] extend the model [168] and include latent delay. They investigated the consequence of the latent delay on worm propagation in WSN. They investigated the local stability along with Hopf bifurcation existence at the equilibrium of worm-induced. They determined the threshold value of Hopf bifurcation and found that if latent delays are below the threshold value worm propagation can be control. The model suggests that to control the propagation of worm in WSN control the recruitment rate and execute the antivirus on time.

In the earlier papers [168,169] the authors failed to explain the effect of communication radius and the number sensor nodes are required to deploy in the sensor field (distributed node density) on the malware transmission if there are multiple malware attacks at the same time. It is of vital concern that these issues should be addressed. Hence in the proposed model, these issued have been discussed. The depletion of the energy is directly related to the malware attack and the area covered by the sensor nodes. The main purpose of this model is to prevent multiple malware attacks at the same time and ensure smooth functioning of the system along with a harmless process of communication. In this model the main focus is to solve the issue of the network when attacked by two malwares simultaneously having varied features.

Organization of the chapter. The chapter follows the structure in the following order: in section 5.2 modified SE_1E_2IR model formulation and its assumptions is discussed.

In section 5.3 existence of positive equilibrium is discussed. In section 5.4, investigated the stability of the system and explained its needful theorems along with their proof. In section 5.5 evaluate the theoretical findings along with their simulation outcomes and effect of various networks parameters are discussed. and in section 5.6 comparative analysis with existing model is carried out. Finally in section 5.7 summary of the chapter is presented.

5.2 Modified Multi-Malware Model: The SE_1E_2IR Model

The model considered that two types of malware presence in the network simultaneous with different latent period. The model named as SE_1E_2IR (Susceptible - Exposed category of 1 - Exposed category 2 – Infectious – Recovered). In this model, a novel view is presented related to the multiple malwares being present in WSN at the same time. This model also discusses how the malware transmits. The drawbacks of the existing model [168] have also been looked into. The main purpose of the model which is proposed is to stop the malware transmission in WSN and ensure smooth functioning of WSN by enhancing the stability of the network and increasing the working period of WSN. This model also discusses the effects of communication radius and the density of the nodes in malware transmission in WSN.

The major findings of the chapter are given below:

1. Modified a developed epidemic model and analyzed the dynamics of multi-malware (two malware) in WSN and devised a mechanism for controlling their transmission.
2. Used the concept of latent period of epidemic theory and detected the malware's presence in WSN at early stage as well as to applied corrective measure on time for their removal from the network.
3. Also, an in-depth analysis of how the system responds when attacked by multiple malwares in WSN was done. The stability of the system was ensured by a deep analysis. The equilibrium points when the system would be free from malware and would be in an endemic state were also found out.
4. The points of equilibrium for endemic state and malware-free are obtained and also analyzed the system stability in the various situations.
5. The proposed model has been verified for its exactness and correctness by thorough simulations.

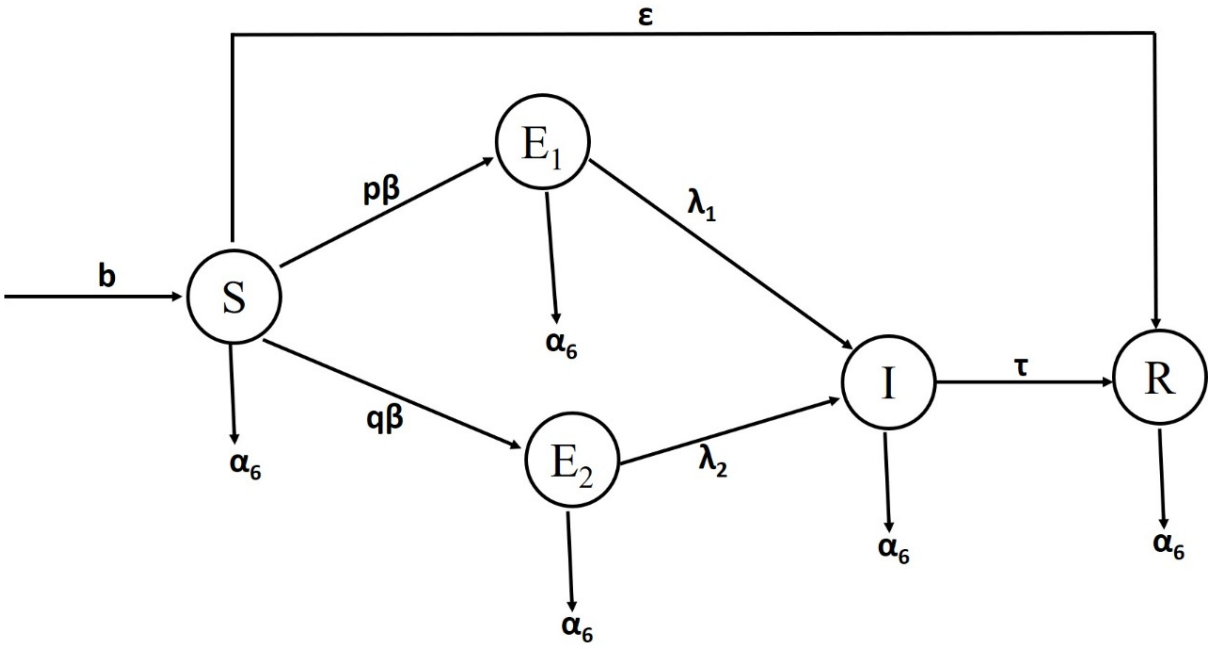

Figure 5.1: Transitions states of the node

This model describes the various states which are as follows:

1.**Susceptible State (S):** This is a state wherein the sensor nodes are not attacked by the malware but are prone to such attacks.

2. **Exposed State (E):** This is a state wherein the nodes have been infected with the malware but they do not transmit infection immediately but they can transmit infection after some time or latent period. There are two types of exposed nodes E_1 and E_2 are considered they possess different latent period, because two types of malware attack in the network simultaneously considered.

3.**Infectious State (I):** This is a state wherein the nodes are contaminated by malware attack and they transmit the infection to the neighboring susceptible nodes too.

4. **Recovered State (R):** This is a state wherein the sensor nodes acquire immunity from the infectious state through measures of security mechanisms.

The basic motive for development of the model is to prevent malware transmission and increase WSN's lifespan. The model describes the dynamics of malware transmission process in WSN when two types of malwares present in the network, the significant contributions of the proposed model is:

1. To investigate the dynamics of malwares transmission process in the sensor network when two types of malwares appear in the network simultaneously. The model analyses the transmission behaviour of malwares and suggests the mechanism for controlling of malwares transmission in WSN.

2. To utilize the concept of different latent period to protect the network against malwares attack. On the basis of latent period of different malwares apply the corrective measures to safeguard WSN. The suggested mechanism helps in securing and enhancing the lifetime of WSN.

3. To prevent the malware attack and reduce the energy consumption of sensor node in WSN through the method of recovery of susceptible sensor nodes.

4. To study the impact of spatial as well as temporal parameters on transmission of malware in WSN.

5. To analyse the stability of the system in different situations and validate analytical results through extensive simulation outcomes.

Some of the assumptions are made for formulation of the model. The identical type of sensor nodes is distributed in a field to gather the information from the environs and transfer to the destination/sink node/control centre in single hop or multi-hop. All sensor nodes are of in Susceptible (S) state in the beginning and free from malicious signals. A sensor node of WSN is targeted by the attacker and installs malware. When the malware is successfully installed on the network and begins communicating with other nodes on the network, the malware attack changes the state of the sensor node. The state transition diagram is shown in figure 5.1.

5.2.1 Model Description and Assumptions

The model proposes to control the attack of malwares in the sensor network. In the area of l^2 the N number of sensor nodes are distributed randomly. The usage of these nodes is to gather the important information from nearby environment. The sensor nodes are categoried into varied groups. These are Susceptible (S), Exposed category 1 (E_1), Exposed category 2 (E_2), Infectious (I) and Recovered (R) states. In Figure 5.1, the diagram illustrates the various transition states of the proposed model SE_1E_2IR .

At any given point of time, $t \geq 0$, the number of all the sensor nodes in the network is always $N(t)$ and fulfils the conditions.

$$N(t) = S(t) + E_1(t) + E_2(t) + I(t) + R(t)$$

The assumptions are given below for formulation of the model:

1. Initially, all the sensor nodes of WSN are in the state of susceptibility and away from malwares but these sensor nodes are susceptible, and they can be easily targeted by malwares. Attackers can try to launch the attack of malwares on the sensor nodes those are in susceptible state. In this model two types of malware attack are considered at a time in which one category with shorted latent period in comparison to another category. There is a possibility that some of the susceptible sensor nodes with probability p and infection rate β attacked by a category 1 malware turn into exposed state of category 1. And another set of the susceptible sensor nodes with probability q and infection rate β attacked by a category 2 malware turn into exposed state of category 2 (where $p+q=1$). Some of the susceptible class of sensor nodes of the network may be damaged with rate α_6 due to drain of sensor nodes battery or malfunction of hardware/software.
2. If exposed nodes of WSN are detected on time, they can be prevented from becoming infectious nodes by applying the corrective measure. They become infectious over the latent period. One category of exposed nodes moves into an infectious class of sensor nodes with a rate of $E_1\lambda_1$ and another by $E_2\lambda_2$. The latent period of malware is different. The exposed class of nodes may be damaged due to weariness of sensor nodes battery or failure of hardware/software with rate α_6.
3. The infectious nodes of the network are recovered with the rate τI. The recovered node of the network may be again infected by the same or new type of malware. The recovered nodes may also be damaged due to the discharge of sensor nodes' battery or failure of hardware/software with rate α_6. Infectious nodes may be crashed due to drain of sensor nodes battery or failure of hardware/software.
4. In the beginning some of the susceptible nodes are protected by antivirus and they have temporary immunity against the malware attack. The meaning of temporary immunity is that the different class of malware can invade them. The rate of susceptible nodes protection is taken as εS.
5. The new sensor nodes are added in the network with rate β.

S.No.	Parameter	Meaning of the used Parameter
1.	b	Addition rate of susceptible nodes in the network
2.	α_6	Damage rate of sensor nodes due to failure of hardware/software or exhaust of sensor node's battery
3.	λ_1	Rate at which exposed category 1 class of nodes turn into infectious class of sensor nodes
4.	λ_2	Rate at which exposed category 2 class of nodes turn into infectious class of sensor nodes
5.	ε	Probability of installation of anti-malware in susceptible nodes
6.	β	Probability of conversion of susceptible node to infectious node due attack of malware (rate of infection)
7.	τ	Recovery rate of infectious nodes

Table 5.1: Used parameters and their Meanings

The sensor nodes have an equal scope to contact each other and are distributed randomly. In the proposed model, at the same time, two types of malware attacks are possible in the network. The exposed state gives a better mechanism for the earlier identification of malware in WSN. In WSN this technique is useful in the prevention of malware outbreaks. The ordinary differential equation (ODE) can be used to explain the malware transmission dynamics in WSN. Therefore, a set of ODEs is used to characterize the dynamics of malware. The total number of nodes in WSN at any time t is N, and they are scattered uniformly throughout the specified area. The coverage area of sensor node is πr^2 with a radius of communication r, and in a unit area the susceptible node density is $d(t) = \frac{S(t)}{l*l}$. Total number of sensor nodes which are covered by a susceptible sensor node of radius r is given as $S'(t) = \frac{S(t)\pi r^2}{l*l}$. According to the transition diagram of the states of the nodes represented through figure 5.1, the ODEs description of the rate of modification in each class are as stated below:

$$
\left.
\begin{aligned}
\dot{S} &= b - \beta \frac{\pi r^2}{l^2} SI - \alpha_6 S - \varepsilon S, \\
\dot{E}_1 &= p\beta \frac{\pi r^2}{l^2} SI - (\lambda_1 + \alpha_6) E_1, \\
\dot{E}_2 &= q\beta \frac{\pi r^2}{l^2} SI - (\lambda_2 + \alpha_6) E_2 \\
\dot{I} &= \lambda_1 E_1 + \lambda_2 E_2 - (\alpha_6 + \tau) I, \\
\dot{R} &= \tau I - \alpha_6 R + \varepsilon S
\end{aligned}
\right\} \qquad (5.1)
$$

For convenience, let $\varphi = \frac{\pi r^2}{l * l} \beta$, equation (5.1) can be written as:

$$
\left.
\begin{aligned}
\dot{S} &= b - \varphi SI - \alpha_6 S - \varepsilon S, \\
\dot{E}_1 &= p\varphi SI - (\lambda_1 + \alpha_6) E_1, \\
\dot{E}_2 &= q\varphi SI - (\lambda_2 + \alpha_6) E_2 \\
\dot{I} &= \lambda_1 E_1 + \lambda_2 E_2 - (\alpha_6 + \tau) I, \\
\dot{R} &= \tau I - \alpha_6 R + \varepsilon S
\end{aligned}
\right\} \qquad (5.2)
$$

The system is defined in the domain $\Gamma = \left\{ (S, E_1, E_2, I, R) \in \Re_+^5 \right\}$. As this model checks the various states of the sensor nodes, all the state variables remain positive for all $t \geq 0$.

5.3 Proof of Positive Equilibrium Existence

To determine the system's equilibrium points, the first order derivatives of the system of equations are set to be equal to zero.

$$
\left.
\begin{aligned}
0 &= b - \varphi SI - \alpha_6 S - \varepsilon S, \\
0 &= p\varphi SI - (\lambda_1 + \alpha_6) E_1, \\
0 &= q\varphi SI - (\lambda_2 + \alpha_6) E_2 \\
0 &= \lambda_1 E_1 + \lambda_2 E_2 - (\alpha_6 + \tau) I, \\
0 &= \tau I - \alpha_6 R + \varepsilon S
\end{aligned}
\right\} \qquad (5.3)
$$

The equilibrium points of the system are obtained by solving the equation (5.3) and malware-free equilibrium point is: $P_0 = (S_0, E_{10}, E_{20}, I_0, R_0) = \left(\frac{b}{\alpha_6 + \varepsilon}, 0, 0, 0, 0, \frac{\varepsilon b}{\alpha_6 \left(\alpha_6 + \varepsilon \right)} \right)$ and

endemic equilibrium point is $P^* = (S^*, E_1^*, E_2^*, I^*, R^*)$ with,

$$S^* = \frac{b}{(\alpha_6 + \varepsilon) R_0{}^{th}},$$

$$E_1^* = \frac{(R_0{}^{th} - 1) pb}{R_0{}^{th} (\alpha_6 + \lambda_1)},$$

$$E_2^* = \frac{(R_0{}^{th} - 1) qb}{R_0{}^{th} (\alpha_6 + \lambda_2)},$$

$$I^* = \left[\frac{(R_0{}^{th} - 1)(\alpha_6 + \varepsilon)}{\beta} \right],$$

$$R^* = \frac{1}{\varepsilon_1} \left[\frac{\varepsilon b}{(\alpha_6 + \varepsilon) R_0{}^{th}} + \frac{\tau (\alpha_6 + \varepsilon)(R_0{}^{th} - 1)}{\beta} \right]$$

where R_0 [161] is the basic reproduction number which is given as

$$R_0{}^{th} = \frac{b\beta\pi r^2}{l^2 (\alpha_6 + \tau)(\alpha_6 + \varepsilon)} \left[\frac{p\lambda_1}{(\alpha_6 + \lambda_1)} + \frac{q\lambda_2}{(\alpha_6 + \lambda_2)} \right]$$

It is evident that P^* exists and unique if and only if $R_0{}^{th} > 1$.

5.4 Analysis of System Stability

One of the key concerns is the scrutiny of the system stability due to malware invasion. Some theorems have been set up to analyse the stability of the prospective system and to ascertain stability of WSN. The new theorems are modified in accordance with existing theorems for the stability analysis of the proposed model.

Theorem 1: The system (5.1) is locally asymptotically stable at a malware-free equilibrium P_0 if all of the eigenvalues of (5.4) are negative.

Proof. To acquire the condition of asymptotically stable system at a malware-free equilibrium P_0, the Jacobian matrix is

$$J(P_0)=\begin{bmatrix} -(\alpha_6+\varepsilon) & 0 & 0 & \varphi S_0 & 0 \\ 0 & -(\lambda_1+\alpha_6) & 0 & p\varphi S_0 & 0 \\ 0 & 0 & -(\lambda_2+\alpha_6) & q\varphi S_0 & 0 \\ 0 & \lambda_1 & \lambda_2 & -(\alpha_6+\tau) & 0 \\ \omega & 0 & 0 & \tau & -\alpha_6 \end{bmatrix} \quad (5.4)$$

The roots of the equation are $\theta_1=-\alpha_6, \theta_2=-(\alpha_6+\varepsilon)$ and other three roots are the roots of the cubic equation: $L_0\theta^3+L_1\theta^2+L_2\theta+L_3=0$ (5.5)

where

$$L_0=1$$

$$L_1=(\lambda_1+\lambda_2+2\alpha_6+2\tau)$$

$$L_2=(\lambda_2+\tau)(\alpha_6+\tau)+(\lambda_1+\alpha_6)(\alpha_6+\tau)+(\lambda_1+\alpha_6)(\lambda_2+\alpha_6)-p\beta S_0\lambda_1-q\beta S_0\lambda_2$$

$$L_3=p\beta S_0\lambda_1(\lambda_2+\alpha_6)+q\beta S_0\lambda_2(\lambda_1+\alpha_6)-(\lambda_1+\alpha_6)(\lambda_2+\alpha_6)(\alpha_6+\tau)$$

It is obvious that:

$L_0>0, L_1>0$

$L_2>0$ if $(\lambda_2+\tau)(\alpha_6+\tau)+(\lambda_1+\alpha_6)(\alpha_6+\tau)+(\lambda_1+\alpha_6)(\lambda_2+\alpha_6)-p\beta S_0\lambda_1-q\beta S_0\lambda_2>0$

and

$L_3>0$ if $p\beta S_0\lambda_1(\lambda_2+\sigma)+q\beta S_0\lambda_2(\lambda_1+\alpha_6)-(\lambda_1+\alpha_6)(\lambda_2+\alpha_6)(\alpha_6+\tau)>0$.

As a result, all of the roots of equation (5.5) have non-positive real parts, so as per the Routh Hurwitz criterion, equilibrium is asymptotically stable locally.

Theorem 2: Malware -Free equilibrium (MFE) is globally asymptotically stable if the fundamental reproduction number $R_0 \leq 1$.

Proof. To decide the global stability of the malware-free equilibrium, we use the Lyapunov function which is given by

$$L=a[\lambda_1(\lambda_2+\alpha_6)E_1^*+\lambda_2(\lambda_1+\alpha_6)E_2^*+(\lambda_1+\alpha_6)(\lambda_2+\alpha_6)I]$$

where $a = \dfrac{1}{(\alpha_6 + \lambda_1)(\alpha_6 + \lambda_2)(\alpha_6 + \tau)}$

Differentiate the Lyapunov function L with respect to time t,

$$\dot{L} = \varepsilon[\lambda_1(\lambda_2 + \alpha_6)\dot{E}_1 + \lambda_2(\lambda_1 + \alpha_6)\dot{E}_2 + (\lambda_1 + \alpha_6)(\lambda_2 + \alpha_6)\dot{I}]$$

$$= [\lambda_1(\lambda_2 + \alpha_6)(p\beta SI - (\lambda_1 + \alpha_6))E_1 + (q\beta SI - (\lambda_2 + \alpha_6)E_2)\lambda_2(\lambda_1 + \alpha_6) +$$

$$(\lambda_1 E_1 + \lambda_2 E_2 - (\alpha_6 + \tau)I(\lambda_1 + \alpha_6)((\lambda_2 + \alpha_6)]\varepsilon$$

$$= I^*[p\beta SI\lambda_1(\lambda_2 + \alpha_6) + q\beta SI\lambda_2(\lambda_1 + \alpha_6) - (\lambda_1 + \alpha_6)(\lambda_2 + \alpha_6)(\tau + \alpha_6)]\varepsilon$$

$$= [R_0{}^{th} - 1]I^*$$

From above it is clear that if $R_0^{th} \le 1$ then $\dot{L} \le 0$ holds. Furthermore $\dot{L} \le 0$ if and only if $I = 0$.

Thus, the largest invariant set in $\left\{(S, E_1, E_2, I, R) \in \Gamma : \dot{L} \le 0\right\}$ is the singleton set P_0. Therefore, according to LaSalle's [162] invariance principle the system will be global asymptotically stability at P_0, if $R_0^{th} \le 1$.

5.5 Evaluation of theoretical findings with Simulation Results

In this section, the theoretical findings of the above studies are validated through simulation outcomes using MATLAB (R2018a). The effect of various parameters on transmission of malware is analysed. The basic reproduction number (R_0^{th}) is a crucial parameter for analysis of the system stability. Taking the value of different parameters for simulation are $b = 0.4, \beta = 0.002, \lambda_1 = 0.002, \lambda_2 = 0.001, \alpha_6 = 0.0001, \tau = 0.003, \varepsilon = 0.004, r = 1.5, l = 10, p = 0.7$. At time $t = 0$, assume that different state of nodes in the network $S(0), E_1(0), E_2(0), I(0)$ and $R(0)$ S (0) are 990, 3, 5, 2 and 0 respectively and computed value of $R_0^{th} = 4.177$, which is $R_0^{th} > 1$. This is depicted in figure 5.2. In this situation malwares will persist in WSN continuously. Changing some parametric values which are $\beta = 0.001, \alpha_6 = 0.001, r = 1, l = 12$ and other parameters remain same the value of $R_0^{th} = 0.269$, which is $R_0^{th} < 1$. This is represented by figure 5.3, in this situation the malwares will not persist in WSN. Malwares die out from network. This satisfies the condition of theorem 5.1 and 5.2. The dynamics of malware propagation in WSN is presented by figures 5.2 and 5.3.

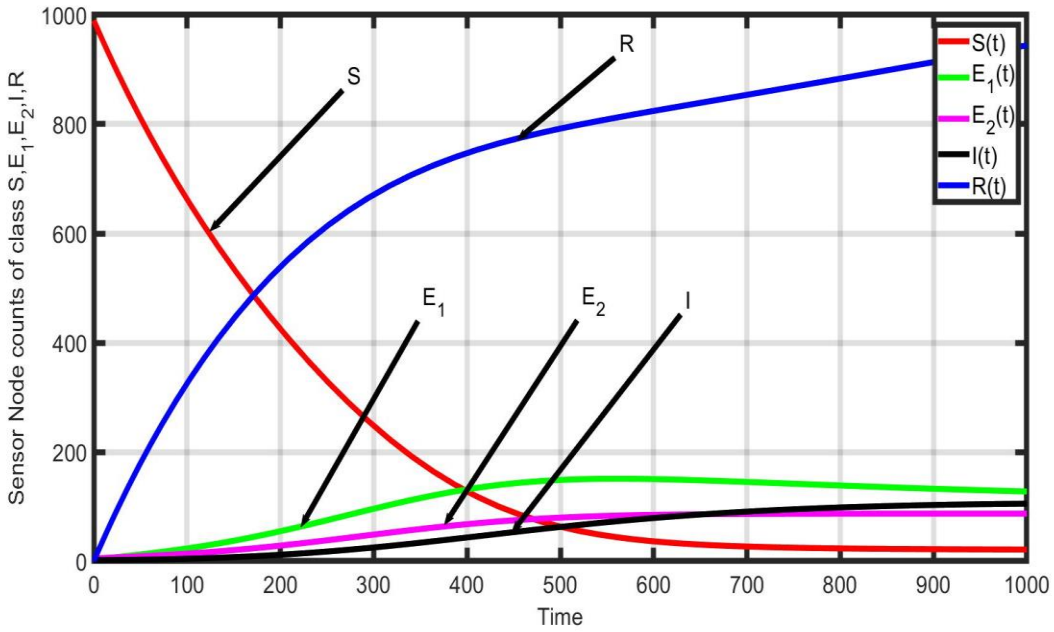

Figure 5.2: Malware transmission dynamics when $R_0^{th} > 1$

Figure 5.2 is demonstrating the variation in the count of different class of sensor nodes in the system with respect to time when $R_0^{th} > 1$. In the beginning count of susceptible nodes are decreasing and others are increasing and other class of sensor nodes are increasing in the system. The count of infectious nodes as well as susceptible nodes become stable with time.

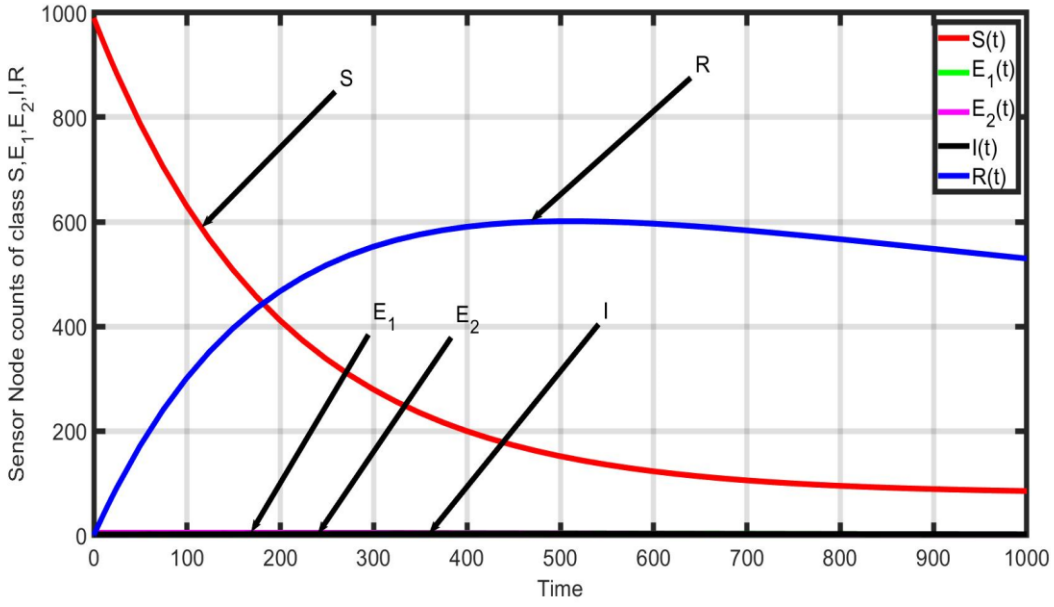

Figure 5.3: Malware transmission dynamics when $R_0^{th} < 1$

Figure 5.3 is demonstrating the variation in the count of different class of sensor nodes in the system with respect to time when $R_0^{th} < 1$. In the beginning count of susceptible nodes are decreasing and count of recovered class of sensor nodes are increasing in the system and others are almost negligible. In this system only susceptible and recovered class of nodes are visible. From figure 5.3, it can be concluded that some of the susceptible sensor nodes by attacked by the malwares and they are detected on time. The implementation of corrective measures on time stops the transmission of malwares in the system and recovered the sensor nodes of exposed or infectious class to recovered class. So, the visibility of infectious class of sensor nodes are almost negligible.

Figure 5.4 elucidates the impacts of recovery on the system in the diverse conditions. As the value of recovery rate (τ) increases the count of recovered nodes also increases with the time. From figure 5.4 it is apparent that in these three cases, initially, recovery counts are almost the same. Thereby the impact of infection is slower in the initial point. The reason behind that lesser number of sensor nodes in contact with infectious nodes. The infected counts also increase with time.

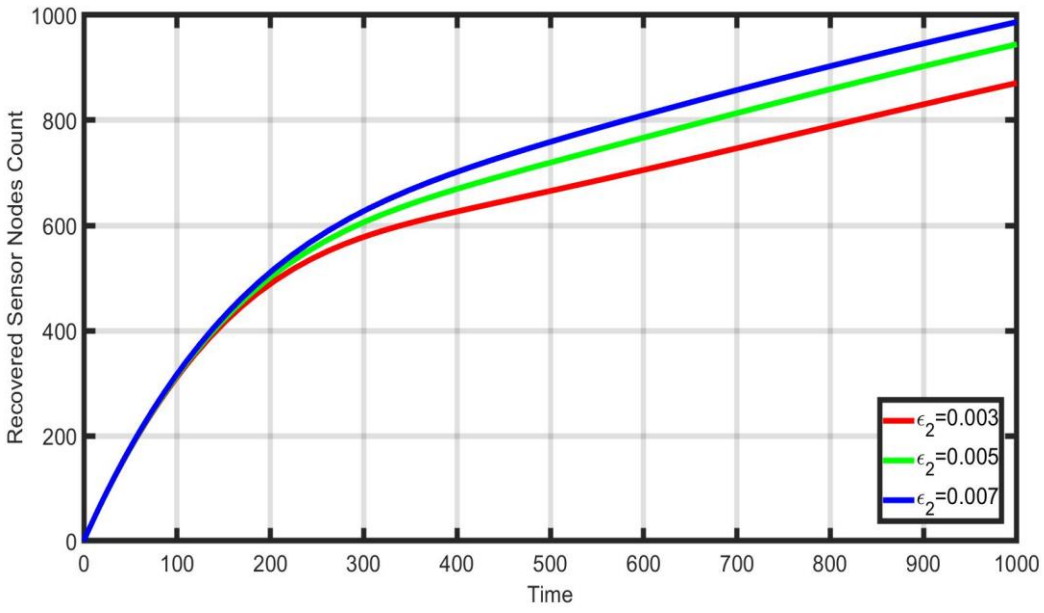

Figure 5.4: Variation in Recovered number of nodes with time

Figure 5.5 supports the result of figure 5. 4, in figure 5.5 it is witnessed that count of recovered nodes is more when the value of recovery rate is higher. As the value of recovery rate increases the count of recovered nodes also increases in lesser time.

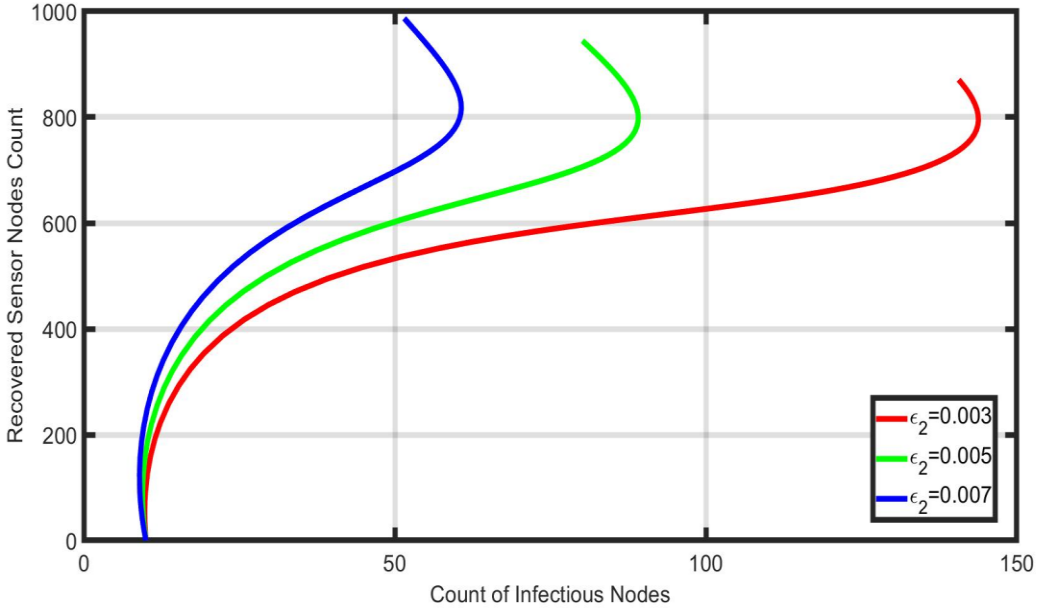

Figure 5.5: Effect of Recovery on Infectious nodes

5.5.1 Effect of Communication Radius on malware propagation

For designing of secure WSN one of the important parameters is communication radius. So, it is important to determine the threshold value of communication radius (r_{th}). The expression of R_0^{th} is

$$R_0{}^{th} = \frac{b\beta\pi r^2}{l^2(\alpha_6+\tau)(\alpha_6+\varepsilon)}\left[\frac{p\lambda_1}{(\alpha_6+\lambda_1)}+\frac{q\lambda_2}{(\alpha_6+\lambda_2)}\right] \tag{5.6}$$

We know that the threshold value of $R_0^{th}=1$.Therefore, put the value of $R_0^{th}=1$ in equation (5.6).

$\frac{b\beta\pi r^2}{l^2(\alpha_6+\tau)(\alpha_6+\varepsilon)}\left[\frac{p\lambda_1}{(\alpha_6+\lambda_1)}+\frac{q\lambda_2}{(\alpha_6+\lambda_2)}\right]=1$, after computation obtained the value of threshold communication radius (r_{th}) is

$$r_{th} = l\sqrt{\frac{(\alpha_6+\tau)(\alpha_6+\omega)(\alpha_6+\lambda_1)(\tau+\lambda_2)}{b\beta\pi[p\lambda_1(\lambda_2+\alpha_6)+q\lambda_2(\alpha_6+\lambda_1)}} \tag{5.7}$$

To compute the value of threshold communication radius (r_{th}) taking the parametric values are as $b = 0.4, \beta = 0.001, \lambda_1 = 0.002, \lambda_2 = 0.001, \alpha_6 = 0.001, \tau = 0.003, \varepsilon = 0.004, l = 10, p = 0.7$, the computed value of $r_{th} = 1.61$.

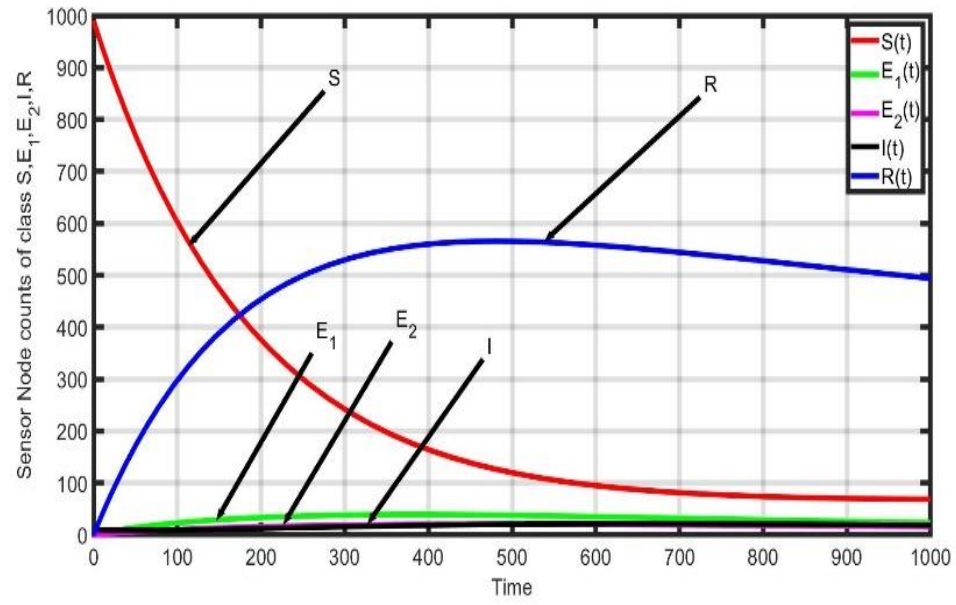

Figure 5.6: When r_{th} (1.61) > r (1.3)

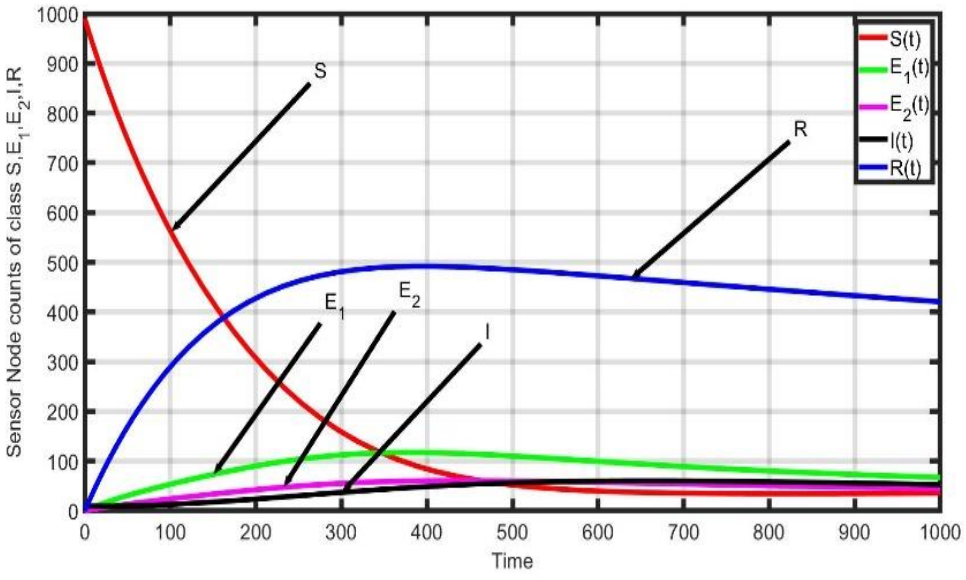

Figure 5.7: When r_{th} (1.61) < r (1.9)

Figures 5.6 and 5.7 demonstrate the status of malware in the network, when $r_{th}(1.61) > r(1.3)$ the malware will die out from the system. This can be realized from figure 5.6. And when $r_{th}(1.61) < r(1.9)$ the malware will continuously be present in the system. This can be realized from figure 5.7. The infectious counts of the sensor nodes increase in the system when the communication radius increases. The infectious count of sensor nodes increases in the network due to larger radius size of sensor node, because in this case the coverage area of infectious nodes is larger. In this condition an infectious node will cover many numbers of susceptible nodes at a time. The value of threshold radius depends of the various parameters. Therefore, according to requirement the design of sensor node can be changed.

5.5.2 Impact of Distributed Node Density on propagation of malware

Like the communication radius, it is also significant to know how many minimum numbers of nodes are mandatory to distribute in the area to finish the task in protected and competent manner. For this purpose, compute the threshold value of distributed node density $d_{th} = \frac{N}{l^2}$.

We know that the threshold value of $R_0^{th} = 1$.Therefore, put the value of $R_0^{th} = 1$ in equation (5.6).

$$d_{th} = \frac{(\alpha_6 + \tau)(\alpha_6 + \varepsilon)(\alpha_6 + \lambda_1)(\tau + \lambda_2)}{b\beta\pi r^2[p\lambda_1(\lambda_2 + \alpha_6) + q\lambda_2(\alpha_6 + \lambda_1)} \qquad (5.7)$$

To compute the value of threshold distributed node density (d_{th}) taking the parametric values are as $b = 0.4, \beta = 0.001, \lambda_1 = 0.002, \lambda_2 = 0.001, \alpha_6 = 0.001, \tau = 0.003, \varepsilon = 0.004, l = 10, p = 0.7, N = 1000,$ $r = 1.61$ the computed value of $d_{th} = 9.96.$

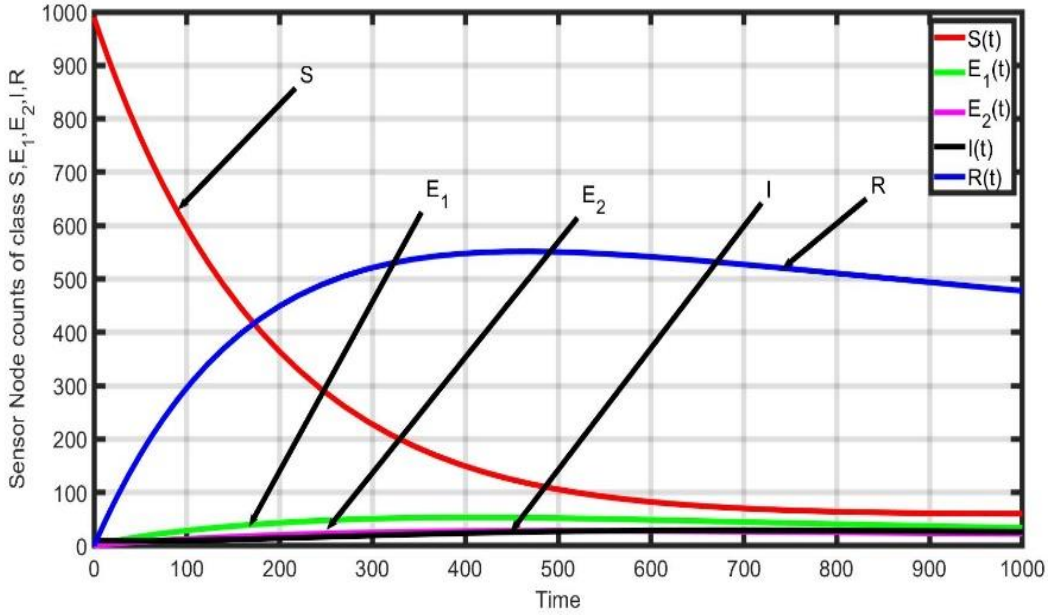

Figure 5.8: When $d_{th}(9.96) > d(8)$

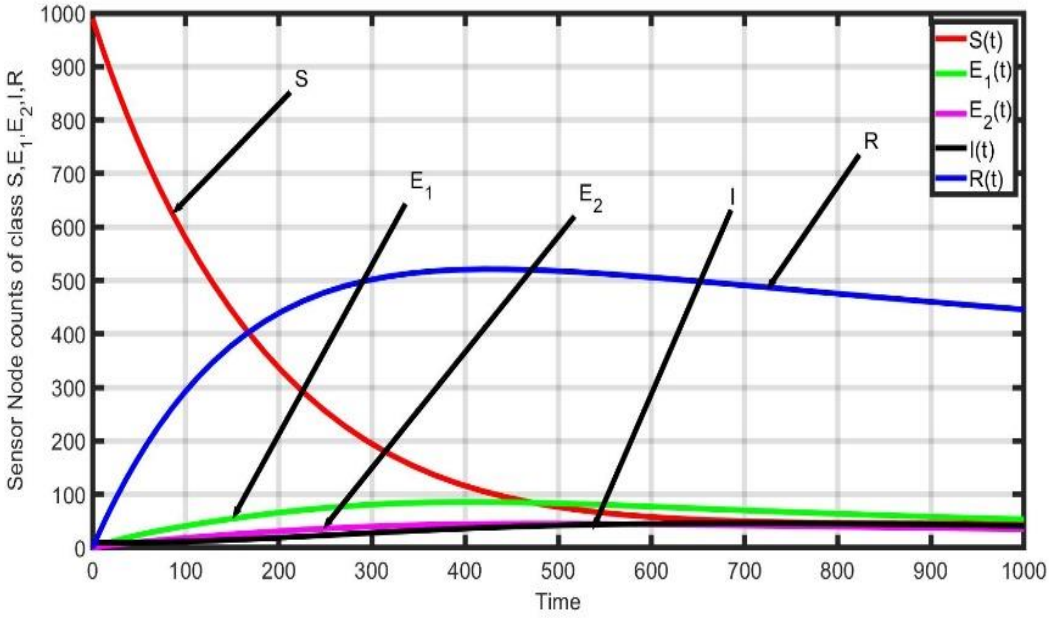

Figure 5.9: When $d_{th}(9.96) < d\ (11)$

Figures 5.8 and 5.9 demonstrate the impact of distributed node density on the transmission of malwares in WSN, when $d_{th}(9.96) > d(8)$ the malware will become extinct from the system with time, this is presented in figure 5. 8. And on the other hand, when $d_{th}(9.96) < d\ (11)$ the malware will constantly present in the system. This can be realized from figure 5.9. As the value of distributed node density surges in the specified disseminated area the infectious counts of the sensor nodes also increase in the system. The infectious count of sensor nodes increases in

WSN due to close vicinity between the sensor nodes in the definite area. In case of dense distribution of nodes in the specified area larger number of vulnerable interact with infectious nodes instantaneously. The value of threshold distributed node density depends of the various parameters. Thus, it is indispensable to comprehend the compulsion of sensor nodes installed in the specific area.

5.6 Comparative Analysis with Existing Model

In this section, the comparative analysis is performed with existing model [168] and proposed model. To carry out the comparative analysis, taking all the values of parameters are equal and variation in the value of communication radius (r). The communication radius is a key design parameter for smooth network connectivity.

Case 1: When change the value of communication radius and other parameters remain same. Figures 5.10 (a-b) present that proposed model performance is better in comparison to existing model for the changed value of communication radius (r). To carried out the comparative analysis the graph is plotted between time and the number of infectious nodes. From figures 5.10 (a-b) found that the count of infectious sensor nodes increases with increase in the communication radius size increase in proposed model whereas in case of existing model there is not noticed any change in the count of infectious nodes with change in the value of communication radius. But the transmission pattern of malware in both the cases is similar. The reason behind no change in the count of infectious sensor nodes in the existing model is that the communication radius parameter not taking into account in existing model. This is one of the important drawbacks of existing model. Therefore, to design a secure and robust network communication radius is one the important parameter. The increase in infectious count of sensor nodes is smaller in the proposed model in respect to existing model. The performance of the proposed model is comparatively improved in terms of malware transmission control and lifetime improvement of WSN.

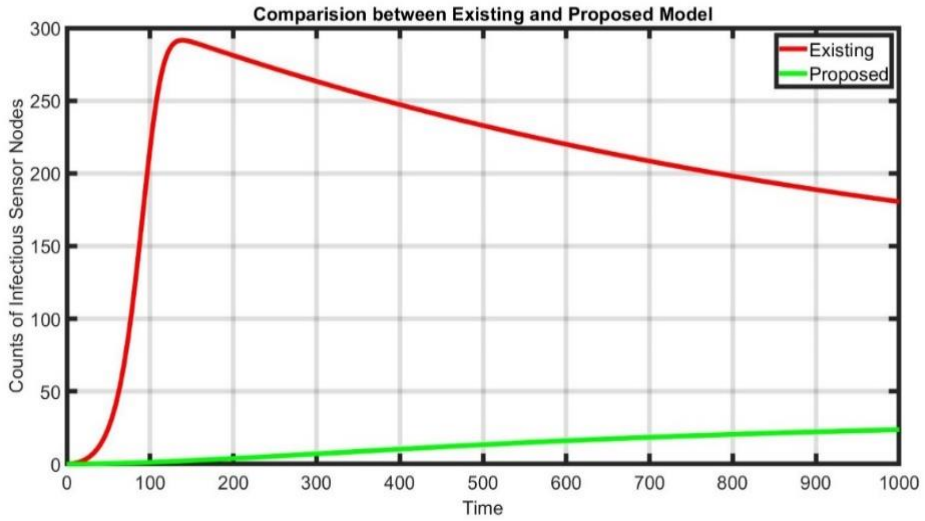

Figure 5.10 (a): Communication Radius ($r = 1.0$)

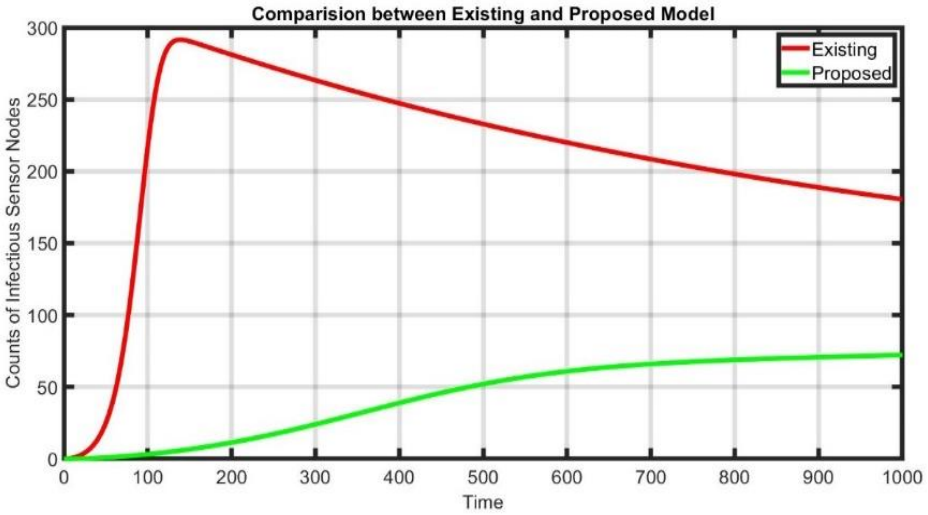

Figure 5.10 (b): Communication Radius ($r = 1.5$)

Case 2: When change the value of distributed node density and other parameters remain the same. Figures 5.11 (a-b) present that proposed model performance is better in comparison to existing model for the changed value of node density (d). To carried out the comparative analysis the graph is plotted between time and the number of infectious nodes. From figures 5.11 (a-b) it is noticeable that the counts of infectious nodes vary with variation in the value of distributed node density in proposed model but constant in existing model. But the transmission pattern of malware in both the cases is similar. There is no change in the count of infectious sensor nodes in the existing model because node density not considered in existing model. This is another important drawback of the existing model. Therefore, to develop a secure and robust network node density is also taking into consideration. The increase in infectious count of sensor nodes is smaller in the proposed model in respect to existing model. The proposed

model provides the method of deployment of sensor nodes in sensor field in optimum manner. So, proposed model suggesting the better mechanism for controlling of malware transmission and lifetime enhancement of WSN.

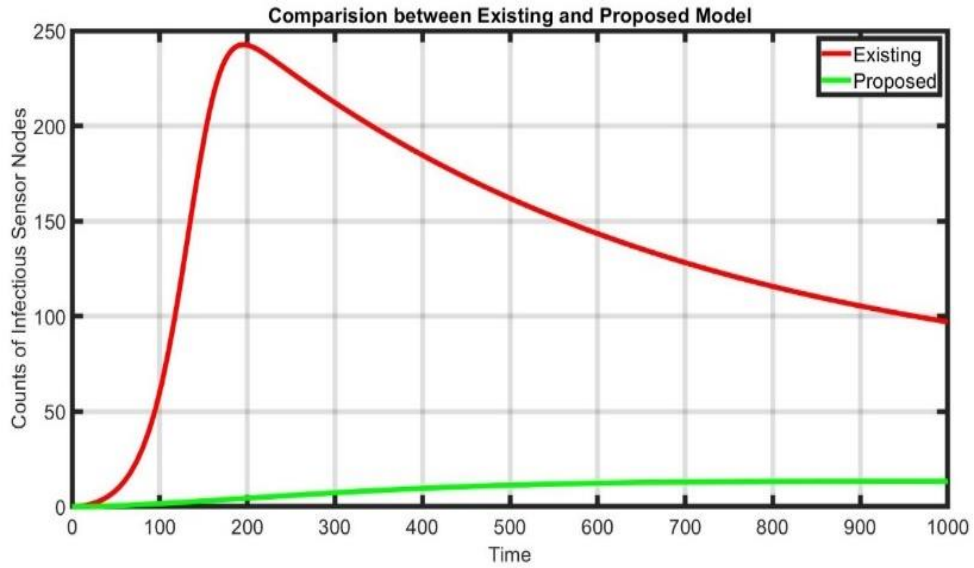

Figure 5.11 (a): Node Density ($d = 11$)

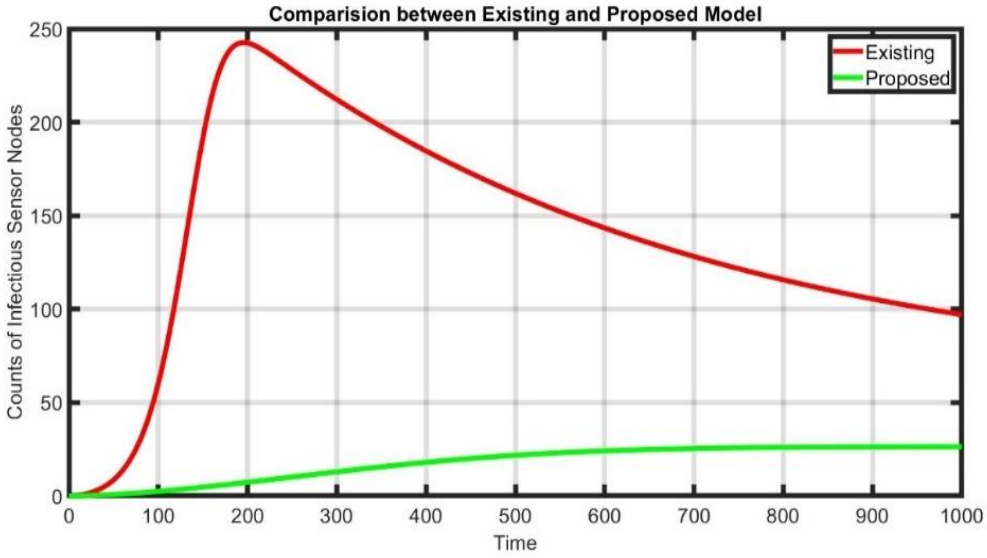

Figure 5.11 (b): Node Density ($d = 16$)

Hence, from the above analysis, it is established that the design parameters such as communication radius of sensor node is needed to determine as per requirement. And also, accordingly it is important to compute the requirement of sensor nodes which will be deployed in the specified area.

5.7. Summary of the Chapter

To study the transmission dynamics of multi-malware (two-malware) in WSN this proposed model is come into existence. Idea of epidemic modelling is being enforced to examine the propagation process of multi-malware. The facts of equilibrium of WSN have been acquired for malware-free and endemic state. Basic reproduction number (R_0^{th}) has been calculated to analyse the critical constraint system dynamics. This parameter uses to investigate the system stability conditions. From various observations it is established that on the one hand when the value of $R_0^{th} < 1$, WSN will be stabilize in malware-free state and on the other hand if $R_0^{th} > 1$ WSN will exist in the endemic state. The stability of the network is discussed in different conditions and consequently their theorem and its proof have been conferred. The recovery method used to overcome the problem of malware attack has also been analysed. The impact of communication radius on malware propagation is investigated and noted that the counts of infectious nodes increase when increase the value of communication radius. The impact of distributed node density on transmission of malware is also discussed. For security and lifetime enhancement of WSN against malware attack calculated the threshold value of communication radius, and for same purpose also calculated the threshold value of distributed node density. These are the important parameters for WSN security against malware attack. The correlative study has been executed with present model and conquer its limitations. In advance study some other state of epidemic model and concept of charging method can be useful.

Chapter 6: Conclusion and Future Scope

6.1 Conclusion

WSN (Wireless Sensor Network) has a wide range of applications. The importance of such communication networks consists in the fact that they execute in-network processing to convert data streams into aggregated data. Finally, and most importantly, their security must be ensured. WSN's nodes face particular challenges, such as deployment issues and limited capabilities, making them more vulnerable to attacks. Existing security systems are insufficient and, to a degree, lack the durability needed to assure security. A thorough literature review was conducted, and a gap in the literature was identified. It has been found that most of the existing models do not fully address many issues, such as malware identification, low energy, and communication radius, node density impacts and other parameters. As a result, mathematical analysis was used in this study to close the gap in the literature. The outcomes of the proposed models in this thesis were compared to those of existing models. The stability of many systems under different conditions has been investigated, and associated theorems and proofs have been developed. The impact of different parameters on WSN performance has also been investigated. To confirm the analytical findings, simulation of all recommended models was conducted.

The thesis is subdivided into six chapters. The first chapter covers the Wireless Sensor Network (WSN), its applications, and the fundamentals of mathematical modeling. There is a need for the development of efficient models for network protection against malware attacks due to the broad range of applications and scope. The second chapter contains an extensive literature review on mathematical modeling, epidemic modeling, and the basic reproduction number. It also discusses similar work in the field of malware attacks from a security perspective. The effects of malware on the performance of WSN is also discussed.

This thesis' novel contribution is discussed in three chapters, numbered 3 to 5. In Chapter 3, the transmission dynamics of malware and its impacts on WSN has been studied. The malware attacks also increase the consumption rate of sensor nodes' energy. This is one of the issues in WSN. So, in view of these issues a SILRD (Susceptible - Infectious - Low Energy - Recovered-Dead) model has been proposed. The low-energy state is also included with other epidemic state in the proposed state, the method of charging is applied. The charging method supress the transmission rate of malware. The proposed model is used to prevent malware transmission

throughout the system. The impact of charging on infected nodes has been investigated, and it has been found that as rate of charging increases, the number of susceptible and recovered nodes grows, while the number of infected nodes drops. The proposed model protects the sensor network against malware attack and controls the malware transmission and also decrease the consumption rate of sensor node's energy. To analyse the system stability in different conditions when malware attack takes place, the controlling parameter basic reproduction number (R_0^{th}) has been determined. The points of equilibria of malware-free and endemic are determined, and for system stability, theorems are established and their proofs are given. Theoretical findings and simulation results are compared and discussed. The impacts of different parameters on transmission of malware have been analysed. The impact of the communication radius on the dynamics of malware transmission is also analysed and it is found that when the communication radius is large, a greater number of susceptible nodes are infected at the same time, and on the other hand, when the communication radius is small, then lesser number of susceptible sensor nodes are infected at the same time. The threshold values of communication radius and node density have been computed and their relationship with R_0^{th} is established. The impact of various parameters has been meticulously studied. Performance analysis of the proposed model has been carried out and the comparative analysis is accomplished with the existing model and found that the proposed model provides an ameliorate mechanism. The theoretical findings are verified by extensive simulation results.

The emphasis of Chapter 4 is on early detection of malware presence in the network. With the help of SEILRD (Susceptible –Exposed- Infectious - Low Energy - Recovered-Dead) epidemic model, a structured model is being developed which describes the transmission malware in WSN. The SILRD model explained in the chapter 3 is extended through including the concept of exposed state. The SILRD model failed to detect the appearance of malware in the network at an early stage, this problem was overcome with the inclusion of exposed state. The exposed state (E) included in SILRD model is utilized to identify the suspected sensor nodes at earlier stage in the sensor network. Such identification provides an opportunity to apply remedial corrective measures to protect the sensor nodes and stop malware transmission in the sensor network. This is an enhancement over the SILRD model. The SEILRD model is proposed for controlling the malware transmission and to improve the lifetime of WSN. Mathematical analysis for this model has been carried out. It has been established that with the theorems and their proofs, malware-free equilibrium is locally and globally asymptotically stable. This is

also validated through simulation results. The expression for reproduction number is acquired and found that if basic reproduction number is less than equal to one, then the malware-free equilibrium is globally asymptotically stable and malware will vanish from the network. Otherwise the malware always continues to stay in the network. The results after the comparative analysis that was performed over existing SEIRS model and proposed SEILRD model was observed to be much better in the case of proposed model rather than that of the existing model. The Comparison of theoretical findings and simulation results are elaborated.

The concept of propagation dynamics of multi-malware in WSN was proposed in Chapter 5. Idea of epidemic modelling is being enforced to examine the propagation process of multi-malware. The points of equilibria have been obtained for both the malware-free and endemic situations. Basic reproduction number has been calculated to analyse the critical constraint system dynamics. This parameter investigates the system stability conditions. From various observations it is established that when the value of $R_0{}^{th} < 1$, system will stabilize at malware-free state and on the other hand if $R_0{}^{th} > 1$, system will exist in the endemic state. The stability of the network is discussed in different conditions and consequently their theorem and its proof have been conferred. The recovery method used to overcome the problem of malware attack has also been analysed. The impact of communication radius on malware propagation is investigated in this chapter and noted that the counts of infectious nodes increase when the value of communication radius is increased. The impact of distributed node density on transmission of malware is also discussed. For security and lifetime enhancement of WSN against malware attack the threshold value of communication radius is calculated, and for same purpose the threshold value of distributed node density is also calculated. These are the important parameters for WSN security against malware attack.

6.2 Future Scope

As a part of future work, the concept of modeling and their methodical study may be extended for many other situations. For example, vulnerability investigation on transmission models to incorporate network mobility can be performed. Proposed model can be extended to incorporate the concept of bifurcation. By utilizing the concept of bifurcation, controlling of malware propagation in WSN can be accomplished. This is likely to enhance the security methods. The proposed models may be extended with the consideration of certain existing issues such as localization, reliability etc.

References

1. Yunting, T., Kong, F.,Yu,J., and Xu,O., (2022). "EPPSA: Efficient Privacy-Preserving Statistical Aggregation Scheme for Edge Computing-Enhanced Wireless Sensor Networks." *Security and Communication Networks* 2022.
2. Akyildiz, I.,F.,Su, W., Sankarasubramaniam, Y., and Cayirci,E.,(2002). "Wireless sensor networks: a survey". Computer Networks.38(4):393-422.
3. Zhao, C., Wu,Q., Lin,D., Zhang, Z., Zhang,Y., Kong,L., and Guan,Y.L., (2022)." An energy-balanced unequal clustering approach for circular wireless sensor networks", Ad Hoc Networks,Volume 132,102872.
4. Angurala,M., Bala,M., Bamber,S.S., (2021). "A novel technique for energy replenishment and load balancing in wireless sensor networks", Optik, Volume 248,168136.
5. Yick, J. , Mukherjee, B. , and Ghosal, D. , (2008). "Wireless sensor networks survey, Computer Networks", vol. 52, no. 12, pp. 2292 -2330.
6. Majid, M.,Habib, S., Javed, A.R., Rizwan, M., Srivastava, G., adekallu, T.R., and Lin, J.C.W. , (2022). "Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review". Sensors 22, 2087.
7. Yetgin, H. , Cheung, K. T. K. , El-Hajjar, M. , and Hanzo, L. H. , (2017). "A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks", IEEE Communications Surveys Tutorials, vol. 19, pp. 828-854.
8. Modieginyane, K. M. , Letswamotse, B. B. , Malekian, R. , and Abu-Mahfouz, A. M. , (2018). "Software defined wireless sensor networks application opportunities for efficient network management: A survey," Computers and Electrical Engineering, vol. 66, pp. 274 -287.
9. Shen, J. , . Tan, H.-W , Wang, J. , Wang, J.W. ,and Lee, S.Y. , (205). "A novel routing protocol providing good transmission reliability in underwater sensor networks," Journal of Internet Technology, vol. 16, no. 1, pp. 171-178.
10. Zhang, X. , Wang, H. , Shi, Y. , Fu, C. , Wang, H. , and Wang, G. , (2016). "A measure system of zero moment point using wearable inertial sensors," China Communications, vol. 13, pp. 16-27.
11. Borges, L. M. , Velez, F. J. , and Lebres, A. S. , (2014), "Survey on the Characterization and Classification of Wireless Sensor Network Applications," IEEE Communications Surveys Tutorials, vol. 16, pp. 1860-1890.
12. Amin, R., Islam, S. H. , Biswas, G. , Khan, M. K. and Kumar, N. "A robust and anonymous patient monitoring system using wireless medical sensor networks," Future Generation Computer Systems, vol. 80, pp. 483-495, 2018.

13. Wang, T. , Peng, Z. , Liang, J. , Wen, S. , Bhuiyan, M. Z. A. , Cai, Y. , and Cao, J. , (2016). “Following Targets for Mobile Tracking in Wireless Sensor Networks," ACM Transactions on Sensor Networks (TOSN), vol. 12, no. 4, pp. 31:1-31:24.
14. TWang, . , Peng, Z. , Wang, C. , Cai, Y. , Chen, Y. , Tian, H. , Liang, J. , and Zhong, B. , (2016). “Extracting Target Detection Knowledge Based on Spatiotemporal Information in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 12, no. 2, pp. 1-11.
15. Yoon, S. , Ye, W. , Heidemann, J. , Little_eld, B. , and Shahabi, C. , (2011). “Swats: Wireless sensor networks for steamood and waterood pipeline monitoring," IEEE Network, vol. 25, pp. 50..
16. Zeng, B. and Yao, L. ,(2015). “Study of vehicle monitoring application with wireless sensor networks," in 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015), pp. 1-4.
17. Wan, J. , Yu, Y. , Wu, Y. , Feng, R. ,and Yu, N. , (2012). “Hierarchical Leak Detection and Localization Method in Natural Gas Pipeline Monitoring Sensor Networks," Sensors, vol. 12, no. 1, pp. 189- 214.
18. Aziz, K. , Tarapiah, S. , Alsaedi, M. , Ismail, S. H. and Atalla, S. , (2015). “Wireless Sensor Networks for Road Tra_c Monitoring," International Journal of Advanced Computer Science and Applications, vol. 6, no. 11, pp. 265-270.
19. Pule, M. , Yahya, A. , and Chuma, J. , (2017). “Wireless sensor networks: A survey on monitoring water quality," Journal of Applied Research and Technology, vol. 15, no. 6, pp. 562-570.
20. Jamali-Rad, H. , Campman, X. , MacKay, I. , Walk, W. , Beker, M. , Brand, J.V.D., Bulten, H. J. , and Beveren,V.V., (2018). “IoT-based wireless seismic quality control," The Leading Edge, vol. 37, no. 3, pp. 214-221.
21. Rahaman,M.M., Azharuddin,M. , (2022). "Wireless sensor networks in agriculture through machine learning: A survey" , Computers and Electronics in Agriculture, Volume 197,2022,106928.
22. Zelalem, B.A., Morales, J., Assabie, Y., and Rolf A. D.B, (2022). "Utilization of Internet of Things and Wireless Sensor Networks for Sustainable Smallholder Agriculture." *Sensors* 22, no. 9 : 3273.
23. Ajij, M., Pratihar, S., Luhach, A. K., and Roy, D. S. (2022). A Quasistraight Line Routing Protocol for Square Grid-Based Wireless Sensor Networks. *Wireless Communications and Mobile Computing*.
24. Godase, M., and Bhanarkar, M. K., (2021). "Wsn node for air pollution monitoring". In 2021 6th International Conference for Convergence in Technology (I2CT) (pp. 1-7). IEEE.
25. Wu, M., Tan, L. , and Xiong, N. , (2016). “Data prediction, compression, and recovery in clustered wireless sensor networks for environmental monitoring applications," Information Sciences, vol. 329, pp. 800-818.
26. Yuan, F. , Zhan, Y. , and Wang, Y. , (2014). “Data Density Correlation Degree Clustering Method for Data Aggregation in WSN," IEEE Sensors Journal, vol. 14, pp. 1089-1098.
27. Illiano V. P. , and Lupu, E. C. , (2015). “Detecting Malicious Data Injections in Wireless Sensor Networks: A Survey," ACM Comput. Surv., vol. 48, pp. 24:1-24:33.

28. Dalal, B., and Kukarni, S. , (2021). "Wireless Sensor Networks: Applications". In (Ed.), Wireless Sensor Networks - Design, Deployment and Applications. IntechOpen.
29. Yong-Min, L., Shu-Ci, W., and Xiao-Hong, N., (2009). "The architecture and characteristics of wireless sensor network". In *2009 International Conference on Computer Technology and Development* (Vol. 1, pp. 561-565). IEEE.
30. Kandris, D., Nakas, C., Vomvas, D., Koulouras, G.. (2020). "Applications of Wireless Sensor Networks: An Up-to-Date Survey". *Applied System Innovation*.3(1):14.
31. Mao, J., Jiang, X. and Zhang, X., (2019). " Analysis of node deployment in wireless sensor networks in warehouse environment monitoring systems". *J Wireless Com Network* **2019,** 288.
32. Khan, S. , (2016). "*Wireless sensor networks [M]"*, CRC Press, Boca Raton, pp. 10–12
33. Hou, Y. , Chen, C. , Jeng, B. , (2010). " An optimal new-node placement to enhance the coverage of wireless sensor networks". Wireless Networks **16**, 1033–1043.
34. Zhigang, F. , (2008). "*Wireless sensor network coverage and node deployment research*", University of Electronic Science and technology, Chengdu.
35. SMN, A. , Haas, Z.J. , (2015)., " Coverage and connectivity in three-dimensional networks with random node deployment". Ad Hoc Networks 34, 157–169.
36. Priyadarshi, R., Gupta, B. and Anurag, A. , (2020). "Deployment techniques in wireless sensor networks: a survey, classification, challenges, and future research issues". *J Supercomput* **76,** 7333–7373.
37. Hossain, A. , Chakrabarti, S. ,and Biswas, P. K. , (2012). "Impact of sensing model on wireless sensor network coverage, IET Wireless Sensor Systems, vol. 2, pp. 272–281.
38. Mohapatra, H., and Rath, A. K., (2020). "Fault-tolerant mechanism for wireless sensor network". *IET wireless sensor systems*, *10*(1), 23-30.
39. Liu, T. , Li, Z. , Xia, X. , and Luo, S. , (2009). "Shadowing Effects and Edge Effect on Sensing Coverage for Wireless Sensor Networks," in 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–4.
40. Ou, A. , Yang, T. , Yu, J. , Wu, J. , and Wu, Y. , (2011). "Modeling wireless sensor network coverage based on random radius," in 2011 4th International Congress on Image and Signal Processing, vol. 5, pp. 2603–2606.
41. Kumar, S. , and Lobiyal, D. K. , (2013). "Sensing Coverage Prediction for Wireless Sensor Networks in Shadowed and Multipath Environment," Scientific World Journal, vol. 2013, pp. 1–11.
42. Kaiwartya, O. , Abdullah, A. H. , Cao, Y. , Raw, R. S. , Kumar, S. , Lobiyal, D. K. , Isnin, I. F. , Liu, X. , and Shah, R. R. , (2016). "T-MQM: Testbed-Based Multi-Metric Quality Measurement of Sensor Deployment for Precision Agriculture - A Case Study," IEEE Sensors Journal, vol. 16, pp. 8649–8664.
43. Kaiwartya, O. , Kumar, S. , and Abdullah, A. H. , (2017), "Analytical Model of Deployment Methods for Application of Sensors in Non-hostile Environment," Wireless Personal Communications, vol. 97, no. 1, pp. 1517–1536.
44. Banerjee, P. S., Mandal, S. N., De, D., and Maiti, B. (2020). "iSleep: Thermal entropy aware intelligent sleep scheduling algorithm for wireless sensor network". *Microsystem Technologies*, *26*(7), 2305-2323.
45. Jurdak, R. , Ruzzelli, A. G. , and O'Hare, G. M. P. , (2010). "Radio Sleep Mode Optimization in Wireless Sensor Network," IEEE Transactions on Mobile Computing, vol. 9, pp. 955–968.

46. Yadav, S. , and Yadav,R.S., (2015). "A review on energy efficient protocols in wireless sensor networks," Wireless Networks, vol. 22, p. 335–350.
47. Piyare, R. , Murphy, A. L. , Kiraly, C. , Tosato, P. , and Brunelli, D. , (2017). "Ultra-Low Power Wake-Up Radios: A Hardware and Networking Survey," IEEE Communications Surveys Tutorials, vol. 19, pp. 2117–2157.
48. L. LoBello and E. Toscano, "An Adaptive Approach to Topology Management in Large and Dense Real-Time Wireless Sensor Networks," IEEE Transactions on Industrial Informatics, vol. 5, pp. 314–324, August 2009.
49. Luo, J. , Hu, J. , Wu, D. , and Li, R. , (2015). "Opportunistic Routing Algorithm for Relay Node Selection in Wireless Sensor Networks," IEEE Transactions on Industrial Informatics, vol. 11, pp. 112–121.
50. Achar, S. J., Baishya, C., and Kaabar, M. K. (2022). "Dynamics of the worm transmission in wireless sensor network in the framework of fractional derivatives". *Mathematical Methods in the Applied Sciences*, *45*(8), 4278-4294.
51. Nwokoye, C. H., Madhusudanan, V., Srinivas, M. N., and Mbeledogu, N. N., (2022). "Modeling time delay, external noise and multiple malware infections in wireless sensor networks". *Egyptian Informatics Journal*.
52. Afsar, M.M. and Tayarani-N, M.H. , (2014). "Clustering in sensor networks: a literature survey", J. Netw. Comput. Appl., 46 (2014), pp. 198-226.
53. Razak, M. F. A. , Anuar, N. B. , Salleh, R. , and Firdaus, A. , (2016), "The rise of "malware": Bibliometric analysis of malware study," Journal of Network and Computer Applications, vol. 75, pp. 58–76.
54. Rey , A.M.D, and Peinado, A. , (2018). "Mathematical Models for Malware Propagation in Wireless Sensor Networks: An Analysis", pp. 299–313. Cham: Springer International Publishing.
55. Ali, S. , Al Balushi, T. , Nadir, Z. and Hussain, O. K. , (2018). " Wireless Sensor Network Security for Cyber-Physical Systems", pp. 35–63. Cham: Springer International Publishing.
56. Shen, S. , Ma, H. , Fan, E. , Hu, K. , Yu, S. , Liu, J. , and Cao, Q. , (2017). "A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion," Journal of Network and Computer Applications, vol. 91, pp. 26–35.
57. Granjal, J. , Monteiro, E. , and Silva, J. S. , (2015). "Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey," Ad Hoc Networks, vol. 24, pp. 264–287.
58. Kobo, H. I. , Abu-Mahfouz, A. M. , Hancke, and G. P. , (2017). "A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design Requirements," IEEE Access, vol. 5, pp. 1872–1899.
59. Jeong, J. , and Haas, Z. J. , (2007). "An integrated security framework for open wireless networking architecture," IEEE Wireless Communications, vol. 14, pp. 10–18.
60. Guo , X. , and Zhu, J. , (2011). "Research on security issues in Wireless Sensor Networks," in Proceedings of 2011 International Conference on Electronic Mechanical Engineering and Information Technology, vol. 2, pp. 636–639.
61. Zhang, H. , Cheng, P. , Shi, L. , and Chen, J. , (2016). "Optimal DoS Attack Scheduling in Wireless Networked Control System," IEEE Transactions on Control Systems Technology, vol. 24, pp. 843–852.

62. Nwokoye, C. H., and Madhusudanan, V. , (2022)." Epidemic Models of Malicious-Code Propagation and Control in Wireless Sensor Networks: An Indepth Review". *Wireless Personal Communications*, 1-30.
63. Zhu, X., and Huang, J., (2021). "Malware propagation model for cluster-based wireless sensor networks using epidemiological theory". *PeerJ Computer Science, 7*, e728.
64. Bettany, A. and Halsey, M. ,(2017). "Windows Virus and Malware Troubleshooting". Berkely, CA, USA: Apress.
65. Peng, S. , Wang, G. , Zhou, Y. , Wan, C. , Wang, C. , and Yu, S. , (2018). "An Immunization Framework for Social Networks through Big Data Based Influence Modeling," IEEE Transactions on Dependable and Secure Computing, pp. 1–1.
66. Lai, W. K. , Fan, C. S. , and Lin, L. Y. , (2012). "Arranging cluster sizes and transmission ranges for wireless sensor networks," Information Sciences, vol. 183, no. 1, pp. 117–131.
67. Tang, S., and Li, W.,(2011), "An epidemic model with adaptive virus spread control for Wireless Sensor Networks", International Journal of Security and Networks, vol.6(4), pp. 201–21.
68. Ojha, R.P., Srivastava, P.K., Sanyal, G. *et al.(2021). "* Improved Model for the Stability Analysis of Wireless Sensor Network Against Malware Attacks". *Wireless Pers Commun* **116,** 2525–2548.
69. Mahmood, M. A. , Seah, W. K. , and Welch, I. , (2015). "Reliability in wireless sensor networks: A survey and challenges ahead," Computer Networks, vol. 79, pp. 166–187.
70. Hosseini, S. , Azgomi, M. A. , and Rahmani, A. T. , (2016). "Malware propagation modeling considering software diversity and immunization," Journal of Computational Science, vol. 13, pp. 49–67.
71. Dadlani, A. , Kumar, M. S. , Murugan, S. , and Kim, K. , (2016). "System Dynamics of a Refined Epidemic Model for Infection Propagation Over Complex Networks," IEEE Systems Journal, vol. 10, pp. 1316–1325.
72. Ali, I., Sabir, S., and Ullah, Z. ,(2019). "Internet of things security, device authentication and access control: a review". *arXiv preprint arXiv:1901.07309*.
73. Liu, G. Y. , Peng, B. H. , Zhong, X. J. , and Lan, X. J. , (2020). "Differential games of rechargeable wireless sensor networks against malicious programs based on SILRD propagation model," *Complexity*, vol. 2020, Article ID 5686413, pp13 .
74. Liu, G.,Peng, B.,Zhong, X., (2021). " A novel epidemic model for wireless rechargeable sensor network security" . *Sensors*, *21*, 123.
75. Vasanthi, G., and Prabakaran, N., (2019)." An improved approach for energy consumption minimizing in WSN using Harris hawks optimization". Journal of Intelligent and Fuzzy Systems, (Preprint), 1-12.
76. Dong, N. P., Long, H. V., and Giang, N. L., (2022). "The fuzzy fractional SIQR model of computer virus propagation in wireless sensor network using Caputo Atangana–Baleanu derivatives". *Fuzzy Sets and Systems*, *429*, 28-59.
77. Mart´ın, R. A. , (2015). "Mathematical modeling of the propagation of malware: a review," Security and Communication Networks, vol. 8, no. 15, pp. 2561–2579.
78. Khouzani, M. H. R. , Sarkar, S. , and Altman, E. , (2012). "Maximum Damage Malware Attack in Mobile Wireless Networks," IEEE/ACM Transactions on Networking, vol. 20, pp. 1347–1360.

79. Zhang, T., Yang, L. X., Yang, X., Wu, Y., and Tang, Y. Y., (2017). Dynamic malware containment under an epidemic model with alert. *Physica A: Statistical Mechanics and its Applications*, *470*, 249-260.
80. Shakhov, V. V. ,(2013). "Protecting wireless sensor networks from energy exhausting attacks". In *International Conference on Computational Science and Its Applications* (pp. 184-193). Springer, Berlin, Heidelberg.
81. Shakhov, V., Koo, I., and Rodionov, A., (2017). " Energy exhaustion attacks in wireless networks. In *2017 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON)* (pp. 1-3). IEEE.
82. Hsueh, C. T., Wen, C. Y., and Ouyang, Y. C. , (2015). "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks". *IEEE Sensors journal*, *15*(6), 3590-3602.
83. Yu, S., Gu, G., Barnawi, A., Guo, S., and Stojmenovic, I. , (2014). "Malware propagation in large-scale networks". *IEEE Transactions on Knowledge and data engineering*, *27*(1), 170-179.
84. Driessche,PV.D., and Watmough, J. , (2002). "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," Mathematical Biosciences, vol. 180, no. 1, pp. 29–48.
85. Kumar, S., Saini, M., Goel, M., and Aggarwal, N., (2020). "Modeling information diffusion in online social networks using SEI epidemic model". *Procedia Computer Science*, *171*, 672-678.
86. Hu, X., Zhu, T., Zhai, X., Wang, H., Zhou, W., and Zhao, W. , (2022). "Privacy Data Diffusion Modeling and Preserving in Online Social Network". *IEEE Transactions on Knowledge and Data Engineering*.
87. Rao, Y. S., Keshri, A. K., Mishra, B. K., and Panda, T. C., (2020). "Distributed denial of service attack on targeted resources in a computer network for critical infrastructure: A differential e-epidemic model". *Physica A: Statistical Mechanics and Its Applications*, *540*, 123240.
88. Mishra, B. K. and Jha, N.,(2010), "SEIQRS model for the transmission of malicious objects in computer network," Applied Mathematical Modelling, vol. 34, no. 3, pp. 710–715.
89. Tuyishimire, E., Niyigena, J. D. D., Tubanambazi, F. M., Rutikanga, J. U., Gatabazi, P., Bagula, A., and Niyigaba, E. (2022). "A Novel Epidemic Model for the Interference Spread in the Internet of Things". *Information*, *13*(4), 181.
90. Yadav, P., and Keshri, A. K. (2022). "The Dynamics of SEIQR-V Malware Propagation Model in IoT Networks". In *2022 International Conference on IoT and Blockchain Technology (ICIBT)* (pp. 1-6). IEEE.
91. Grassly, N. C. and Fraser, C.,(2008), "Mathematical models of infectious disease transmission," Nature Reviews Microbiology, vol. 6, no. 6, pp. 477–487.
92. Ajelli, M. , Gon¸ B. , calves, Balcan, D. , Colizza, V. , Hu, H. , Ramasco, J. J. , Merler, S. ,and Vespignani, A. , (2010). "Comparing large-scale computational approaches to epidemic modeling:Agent-based versus structured metapopulation models," BMC Infectious Diseases, vol. 10, p. 190.
93. Duan, W., Fan, Z. , Zhang, P. , Guo, G. , and Qiu, X. ,(2015), "Mathematical and computational approaches to epidemic modeling: a comprehensive review," Frontiers of Computer Science, vol. 9, pp. 806–826.

94. Kr¨amer, A.,Kretzschmar, M., and Krickeberg, K.(2010) ” Modern Infectious Disease Epidemiology: Concepts, Methods, Mathematical Models, and Public Health”. Springer.
95. Kermack, W. O., and McKendrick, A. G., (1927), “A contribution to the mathematical theory of epidemics, The Royal Society”, Volume 115, Number 772, pages 700-721.
96. Macdonald, G. (1957). “The epidemiology and control of malaria”. *The Epidemiology and Control of Malaria.*
97. Anderson, R. M., and May, R. M., (1979). "Population biology of infectious diseases: Part I". *Nature*, *280*(5721), 361-367.
98. Heesterbeek, J. A. P., and Dietz, K. (1996). “The concept of Ro in epidemic theory”. *Statistica neerlandica*, *50*(1), 89-110.
99. Karyotis, V., and Khouzani, M. H. R. (2016). “Malware diffusion models for modern complex networks: theory and applications”. Morgan Kaufmann.
100. Peng, S., Yu, S., and Yang, A. (2013). “Smartphone malware and its propagation modeling: A survey”. IEEE Communications Surveys and Tutorials, 16(2), 925-941.
101. Hosseini, S., Abdollahi Azgomi, M., and Rahmani Torkaman, A. (2016). “Agent-based simulation of the dynamics of malware propagation in scale-free networks”. Simulation, 92(7), 709-722.
102. Wei, S., and Chen, J. (2009). “Modeling the spread of worm epidemics in wireless sensor networks”. In 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing (pp. 1-4). IEEE.
103. Singh, A., Awasthi, A. K., Singh, K., and Srivastava, P. K. (2018). “Modeling and analysis of worm propagation in wireless sensor networks”. Wireless Personal Communications, 98(3), 2535-2551.
104. Srinivas, M. N., Madhusudanan, V., Murty, A. V. S. N., and Tapas Bapu, B. R. (2021). “A review article on wireless sensor networks in view of e-epidemic models”. Wireless Personal Communications, 120(1), 95-111.
105. Zhang, Z., Kundu, S., and Wei, R., (2019)." A delayed epidemic model for propagation of malicious codes in wireless sensor network" . Mathematics, 7(5), 396.
106. Wang, Y., Wen, S., Xiang, Y., and Zhou, W. (2013). “Modeling the propagation of worms in networks: A survey”. IEEE Communications Surveys and Tutorials, 16(2), 942-960.
107. Xiang, Y., Fan, X., and Zhu, W. (2009). “Propagation of active worms: a survey”.
108. Fan, X., and Xiang, Y. (2010).”Defending against the propagation of active worms”. The Journal of Supercomputing, 51(2), 167-200.
109. Hu, J., and Song, Y. (2014).”The model of malware propagation in wireless sensor networks with regional detection mechanism”. In China Conference on Wireless Sensor Networks (pp. 651-662). Springer, Berlin, Heidelberg.
110. Ahmed, A., Abu Bakar, K., Channa, M. I., Haseeb, K., and Khan, A. W., (2015). "A survey on trust-based detection and isolation of malicious nodes in ad-hoc and sensor networks". Frontiers of Computer Science, 9(2), 280-296.
111. Wang, X., He, Z., and Zhang, L. (2014). “A pulse immunization model for inhibiting malware propagation in mobile wireless sensor networks”. Chin. J. Electron, 23(4), 810-815.

112. Gu, Q., Ferguson, C., and Noorani, R. (2011). “A study of self-propagating mal-packets in sensor networks: Attacks and defences”. Computers and Security, 30(1), 13-27.
113. Nakano, T. (2010). “Biologically inspired network systems: A review and future prospects”. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 41(5), 630-643.
114. Charalambous, C., and Cui, S. (2010). “A biologically inspired networking model for wireless sensor networks”. IEEE network, 24(3), 6-13.
115. Leibnitz, K., and Murata, M. (2010). “Attractor selection and perturbation for robust networks in fluctuating environments”. IEEE network, 24(3), 14-18.
116. Yang, L. X., and Yang, X. (2017). “The effect of network topology on the spread of computer viruses: a modelling study”. International Journal of Computer Mathematics, 94(8), 1591-1608.
117. Byun, H., Son, S., and Yang, S. (2015). “Biologically inspired node scheduling control for wireless sensor networks”. Journal of Communications and Networks, 17(5), 506-516.
118. Byun, H., and So, J. (2015). “Node scheduling control inspired by epidemic theory for data dissemination in wireless sensor-actuator networks with delay constraints”. IEEE Transactions on Wireless Communications, 15(3), 1794-1807.
119. Beebe, N. H. (2021). “A Complete Bibliography of ACM Transactions on Autonomous and Adaptive Systems (TAAS)”.
120. Kułacz, Ł., and Kliks, A. (2021). “Brain-inspired data transmission in dense wireless network”. Sensors, 21(2), 576.
121. Cohen, F. (1987). “Computer viruses: theory and experiments. Computers and security”, 6(1), 22-35.
122. Murray, W. H. (1988). “The application of epidemiology to computer viruses”. Computers and Security, 7(2), 139-145.
123. Meisel, M., Pappas, V., and Zhang, L. (2010). “A taxonomy of biologically inspired research in computer networking”. Computer Networks, 54(6), 901-916.
124. Venkatramanan, S., and Kumar, A. (2014). “Co-evolution of content spread and popularity in mobile opportunistic networks”. IEEE Transactions on Mobile Computing, 13(11), 2498-2509.
125. Chen, P. Y., Cheng, S. M., and Chen, K. C. (2014). “Optimal control of epidemic information dissemination over networks”. IEEE transactions on cybernetics, 44(12), 2316-2328.
126. Khayam, S. A., and Radha, H. (2005,). “A topologically-aware worm propagation model for wireless sensor networks”. In 25th IEEE international conference on distributed computing systems workshops (pp. 210-216). IEEE.
127. Khayam, S. A., and Radha, H. (2006). “Using signal processing techniques to model worm propagation over wireless sensor networks”. IEEE Signal Processing Magazine, 23(2), 164-169.
128. De, P., Liu, Y., and Das, S. K. (2006). “Modeling node compromise spread in wireless sensor networks using epidemic theory”. In 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06) (pp. 7-pp). IEEE.

129. De, P., Liu, Y., and Das, S. K. (2007). “An epidemic theoretic framework for evaluating broadcast protocols in wireless sensor networks”. In 2007 IEEE International conference on mobile adhoc and sensor systems (pp. 1-9). IEEE.
130. De, P., Liu, Y., and Das, S. K. (2008). “An epidemic theoretic framework for vulnerability analysis of broadcast protocols in wireless sensor networks”. IEEE Transactions on mobile Computing, 8(3), 413-425.
131. Tang, S., and Mark, B. L. (2009). “Analysis of virus spread in wireless sensor networks: An epidemic model”. In 2009 7th international workshop on design of reliable communication networks (pp. 86-91). IEEE.
132. Wang, X., and Li, Y. (2009).”An Improved SIR Model for Analyzing the Dynamics of Worm Propagation in Wireless Sensor Networks”. Chinese Journal of Electronics, 18(1), 8-12.
133. Srivastava, A. P., Awasthi, S., Ojha, R. P., Srivastava, P. K., and Katiyar, S. (2016). “Stability analysis of SIDR model for worm propagation in wireless sensor network”. Indian Journal of Science and Technology, 9(31), 1-5.
134. Wang, X., Li, Q., and Li, Y. (2010).”EiSIRS: a formal model to analyze the dynamics of worm propagation in wireless sensor networks”. Journal of Combinatorial Optimization, 20(1), 47-62.
135. Tang, S. (2011).” A modified epidemic model for virus spread control in wireless sensor networks”. In 2011 IEEE global telecommunications conference-GLOBECOM 2011 (pp. 1-5). IEEE.
136. Tang, S. (2011).” A modified SI epidemic model for combating virus spread in wireless sensor networks”. International Journal of Wireless Information Networks, 18(4), 319-326.
137. Wang, Y. Q., and Yang, X. Y. (2013).”Virus spreading in wireless sensor networks with a medium access control mechanism”. Chinese Physics B, 22(4), 040206.
138. Yang, Y., Zhu, S., and Cao, G. (2008).” Improving sensor network immunity under worm attacks: a software diversity approach”. In Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing (pp. 149-158).
139. Yang, Y., Zhu, S., and Cao, G. (2016). “Improving sensor network immunity under worm attacks: A software diversity approach”. Ad Hoc Networks, 47, 26-40.
140. Tang, S., Myers, D., and 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), 99-108.
141. Biswal, S. R., and Swain, S. K. (2019). “Model for study of malware propagation dynamics in wireless sensor network”. In 2019 3rd International conference on trends in electronics and informatics (ICOEI) (pp. 647-653). IEEE.
142. “Zhu, L., and Zhao, H. (2015). “Dynamical analysis and optimal control for a malware propagation model in an information network”. Neurocomputing, 149, 1370-1386.
143. De, P., Liu, Y., and Das, S. K. (2009). “Deployment-aware modeling of node compromise spread in wireless sensor networks using epidemic theory”. ACM Transactions on Sensor Networks (TOSN), 5(3), 1-33.

144. Di Pietro, R., and Verde, N. V. (2013). “Epidemic theory and data survivability in unattended wireless sensor networks: Models and gaps”. Pervasive and Mobile Computing, 9(4), 588-597.
145. Aliberti, G., Di Pietro, R., and Guarino, S., (2017). "Epidemic data survivability in Unattended Wireless Sensor Networks: New models and results". Journal of Network and Computer Applications, 99, 146-165.
146. Yang, Y., Wang, X., Zhu, S., and Cao, G. (2008). “SDAP: A secure hop-by-hop data aggregation protocol for sensor networks”. ACM Transactions on Information and System Security (TISSEC), 11(4), 1-43.
147. Feng, L., Song, L., Zhao, Q., and Wang, H. (2015).”Modeling and stability analysis of worm propagation in wireless sensor network”. Mathematical Problems in Engineering, 2015.
148. López, M., Peinado, A., and Ortiz, A. (2016). “A SEIS model for propagation of random jamming attacks in wireless sensor networks”. In International Joint Conference SOCO’16-CISIS’16-ICEUTE’16 (pp. 668-677). Springer, Cham.
149. Ojha, R. P., Srivastava, P. K., and Sanyal, G. (2019). “Improving wireless sensor networks performance through epidemic model”. International Journal of Electronics, 106(6), 862-879.
150. Liu, G., Chen, J., Liang, Z., Peng, Z., and Li, J. (2021). “Dynamical analysis and optimal control for a SEIR model based on virus mutation in WSNs”. Mathematics, 9(9), 929.
151. Muthukrishnan, S., Muthukumar, S., and Chinnadurai, V. (2021).” Optimal control of malware spreading model with tracing and patching in wireless sensor networks”. Wireless Personal Communications, 117(3), 2061-2083.
152. Xu, B., Lu, M., Zhang, H., and Pan, C. (2021). “A novel multi-agent model for robustness with component failure and malware propagation in wireless sensor networks”. Sensors, 21(14), 4873.
153. Mishra, B. K., and Keshri, N. (2013). “Mathematical model on the transmission of worms in wireless sensor network. Applied Mathematical Modelling”, 37(6), 4103-4111.
154. Liu, G.Y., Peng, B.H., Zhong, X.J., Cheng, L.F., Li, Z.F.(2020) “Attack-Defense Game between Malicious Programs and Energy-Harvesting Wireless Sensor Networks Based on Epidemic Modeling”. Complexity 2020, 3680518.
155. Liu, G.,Peng, Z., Liang, Z., Li, J., Cheng, L. (2021) “Dynamics Analysis of a Wireless Rechargeable Sensor Network for Virus Mutation Spreading”. Entropy 2021, 23, 572.
156. 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, pp. 1-21
157. Liu, G.,Peng, Z., Liang, Z., Zhong, X., Xia, X.,(2022) ” Analysis and Control of Malware Mutation Model in Wireless Rechargeable Sensor Network with Charging Delay” Mathematics, 10, 2376.
158. Jr, G. L. (2005) “Not teaching viruses and worms is harmful,” Communications of the ACM, vol. 48, no. 1, p. 144.

159. Bahi, J. M., Guyeux, C., Hakem, M., and Makhoul, A. , (2014). "Epidemiological approach for data survivability in unattended wireless sensor networks". Journal of Network and Computer Applications, 46, 374-383.
160. Mo, L., You, P., Cao, X., Song, Y. Q., and Chen, J. (2015, December). Decentralized multi-charger coordination for wireless rechargeable sensor networks. In 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC) (pp. 1-8). IEEE.
161. Diekmann, O., Heesterbeek, J. A. P., and Metz, J. A. (1990). On the definition and the computation of the basic reproduction ratio R 0 in models for infectious diseases in heterogeneous populations. Journal of mathematical biology, 28(4), 365-382.
162. La Salle, J. P. (1976). The stability of dynamical systems. Society for Industrial and Applied Mathematics.
163. Thommes, R. W., and Coates, M. J. (2005, December). Modeling virus propagation in peer-to-peer networks. In 2005 5th International Conference on Information Communications and Signal Processing (pp. 981-985). IEEE.
164. Yan, P., and Liu, S. (2006). SEIR epidemic model with delay. The ANZIAM Journal, 48(1), 119-134.
165. Mishra, B. K., and Saini, D. K. (2007). SEIRS epidemic model with delay for transmission of malicious objects in computer network. Applied mathematics and computation, 188(2), 1476-1482.
166. Keshri,N., and Mishra, B. K.(2014). “Two time-delay dynamic model on the transmission of malicious signals in wireless sensor network,” Chaos, Solitons and Fractals, vol. 68, pp. 151–158.
167. Haghighi, M. S., Wen, S., Xiang, Y., Quinn, B., and Zhou, W. (2016). On the race of worms and patches: Modeling the spread of information in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 11(12), 2854-2865.
168. Ojha, R. P., Srivastava, P. K., and Sanyal, G. (2018). Mathematical model for wireless sensor network with two latent periods. In Next-Generation Networks (pp. 497-504). Springer, Singapore.
169. Liu, J., and Zhang, Z. (2019). Hopf bifurcation of a delayed worm model with two latent periods. Advances in Difference Equations, 2019(1), 1-27.