ENERGY EFFICIENT & CONNECTIVITY HOLE AWARE ROUTING FOR IOT NETWORKS

A Dissertation Proposal submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

CHAVI KAPOOR

11606540

Supervisor

HARJIT SINGH

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

November 2017-18

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : P172::M.Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE548 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGD0036

Supervisor Name : Harjit Singh **UID :** 14952 **Designation :** Assistant Professor

Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Chavi Kapoor	11606540	2016	K1637	7508739706

SPECIALIZATION AREA : Database Systems **Supervisor Signature:** _____

PROPOSED TOPIC : Energy efficient & connectivity hole aware routing for IoT networks

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	7.75
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.50
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	7.50
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.75
5	Social Applicability: Project work intends to solve a practical problem.	7.50
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	7.50

PAC Committee Members		
PAC Member 1 Name: Kewal Krishan	UID: 11179	Recommended (Y/N): Yes
PAC Member 2 Name: Raj Karan Singh	UID: 14307	Recommended (Y/N): NA
PAC Member 3 Name: Sawal Tandon	UID: 14770	Recommended (Y/N): NA
PAC Member 4 Name: Dr. Pooja Gupta	UID: 19580	Recommended (Y/N): Yes
PAC Member 5 Name: Kamlesh Lakhwani	UID: 20980	Recommended (Y/N): Yes
PAC Member 6 Name: Dr.Priyanka Chawla	UID: 22046	Recommended (Y/N): Yes
DAA Nominee Name: Kuldeep Kumar Kushwaha	UID: 17118	Recommended (Y/N): NA

Final Topic Approved by PAC: **Energy efficient & connectivity hole aware routing for IoT networks**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11024::Amandeep Nagpal **Approval Date:** 04 Nov 2017

11/23/2017 11:07:35 AM

ABSTRACT

The IoT networks consists of many sensor nodes with limited computational power and energy (battery power). The lifetime of the node depends upon its battery size and volume of data processing (sensing and routing). The routing process consumes the large volumes of energy, which is increased with the presence of connectivity hole. The connectivity hole is one of the major problems in the IOT networks. The connectivity holes are the nodes, which can't process the data properly due to the software malfunctioning or attack. Hence, it becomes very necessary to eliminate the connectivity holes from the routing paths to avoid the data drop and minimize the end-to-end delay. Along with connectivity hole elimination, the multipath routing can play the vital role to handle the large volumes of data, which can further reduce the end-to-end delay.

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation proposal entitled "ENERGY EFFICIENT & CONNECTIVITY HOLE AWARE ROUTING FOR IOT NETWORKS" in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Harjit Singh. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of Candidate

Chavi Kapoor

11606540

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation/dissertation proposal entitled "**ENERGY EFFICIENT & CONNECTIVITY HOLE AWARE ROUTING FOR IoT NETWORKS"**, submitted by **Chavi Kapoor** at **Lovely Professional University, Phagwara, India** is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

(Harjit Singh)

Date:

Counter Signed by:

1) **Concerned HOD:**
   HoD's Signature: _____

   HoD Name: _____

   Date: _____

2) **Neutral Examiners:**

   External Examiner

   Signature: _____

   Name: _____

   Affiliation: _____

   Date: _____

   Internal Examiner

   Signature: _____

   Name: _____

   Date: _____

ACKNOWLEDGEMENT

I would like to convey my most heartfelt and sincere gratitude to my mentor Mr. Harjit Singh of Lovely Professional University, for his valuable guidance and advice. His willingness to motivate me contributed tremendously to achieve the goal successfully.

I would also like to express my gratitude towards my parents for their kind co-operation and encouragement.

CHAVI KAPOOR

TABLE OF CONTENTS

CONTENTS	PAGE NO.
Inner first page	i
PAC form	ii
Abstract	iii
Declaration	iv
Supervisor's Certificate	v
Acknowledgement	vi
Table of Contents	vii
List of Figures	ix
List of Tables	x
CHAPTER1: INTRODUCTION	1-9
1.1. INTERNET OF THINGS	1
1.2 IOT ARCHITECTURE	4
1.3 IoTs AND HEALTH CARE MONITORING NETWORKS	5
1.3.1 CHALLENGES	6
1.4 SECURITY AND SECURITY ISSUES IN IOT	7
CHAPTER2: REVIEW OF LITERATURE	10-15
CHAPTER3: PRESENT WORK	
3.1 RESEARCH GAPS	16
3.2 PROBLEM FORMULATION	16
3.3 PROPOSED ALGORITHM	17

TABLE OF CONTENTS

CONTENTS	PAGE NO.
3.1 OBJECTIVES OF STUDY	18
CHAPTER4: RESEARCH METHODOLOGY	19-21
4.1 TOOLS USED	19
4.1 MEHODOLGY	19
4.3 FLOWCHART OF PROPOSED WORK	21
CHAPTER5: CONCLUSION	22-24
5.1 EXPECTED OUTCOME	22
5.2 CONCLUSION	22
REFERENCES	24

LIST OF TABLES

TABLE NO.	TABLE DESCRIPTION	PAGE NO.
Table 1	Comparative Analysis of Various Routing Models	14

LIST OF FIGURES

FIGURE NO.	FIGURE DESCRIPTION	PAGE NO.
Figure1.1.1	An example of internet of things	1
Figure1.1.2	Internet Protocol (IP) based internet of things (IoT)	2
Figure1.1.3	Representation of a network in which a node goes down due out of battery	3
Figure1.2	IoT Architecture	5
Figure 1.4	Attacks on IoT	8
Figure 5.3	Flowchart of proposed work	21

CHAPTER 1

INTRODUCTION

1.1. INTERNET OF THINGS

Internet of things (IoT) combines a certain number of sensor node for incorporation of the network. Internet of Thing (IoT) network is created such that it gives continuous data and investigation of low level information in threatening condition. [1] The IoT sensor nodes speak with each other without physical system through radio flag. [3] The remote systems function as transmission media among a few gadgets. Internet of things gadgets are self-controlled and can adapt to the wireless network scenarios automatically. The hubs of remote system are made out of limited memory, sensor, a radio handset and adequate power source, for example, battery. IoT is an extraordinary kind of ad-hoc network system. [16]

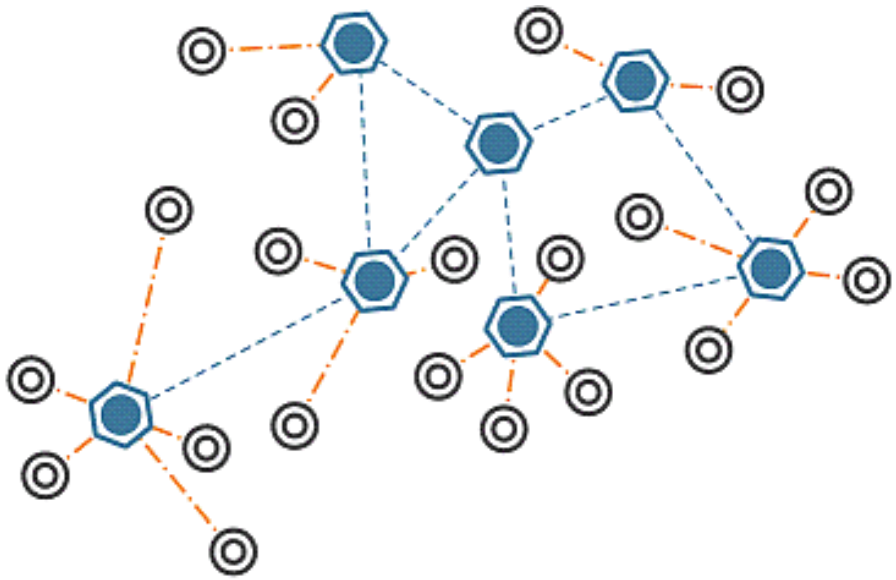


Figure 1.1: An example of internet of things

The correspondence or data given by IoT is required to have information respectability, the information which is exchange by the sender is not temper or changed on the way from sender to collector. [2] In the remote system time synchronization is normal with the end goal that there is nonattendance of deferral in parcels when it is exchange between two hubs. Classified data is foreseen in remote system it signifies specific data must be kept from endowed outsider. [6] The hubs of remote sensor arrange is conveyed in ill-disposed

condition so it is energy preservation capability against attacks. IoT are imperiled to security assault inferable 2from communicate nature of transmission medium. [1, 5-7]

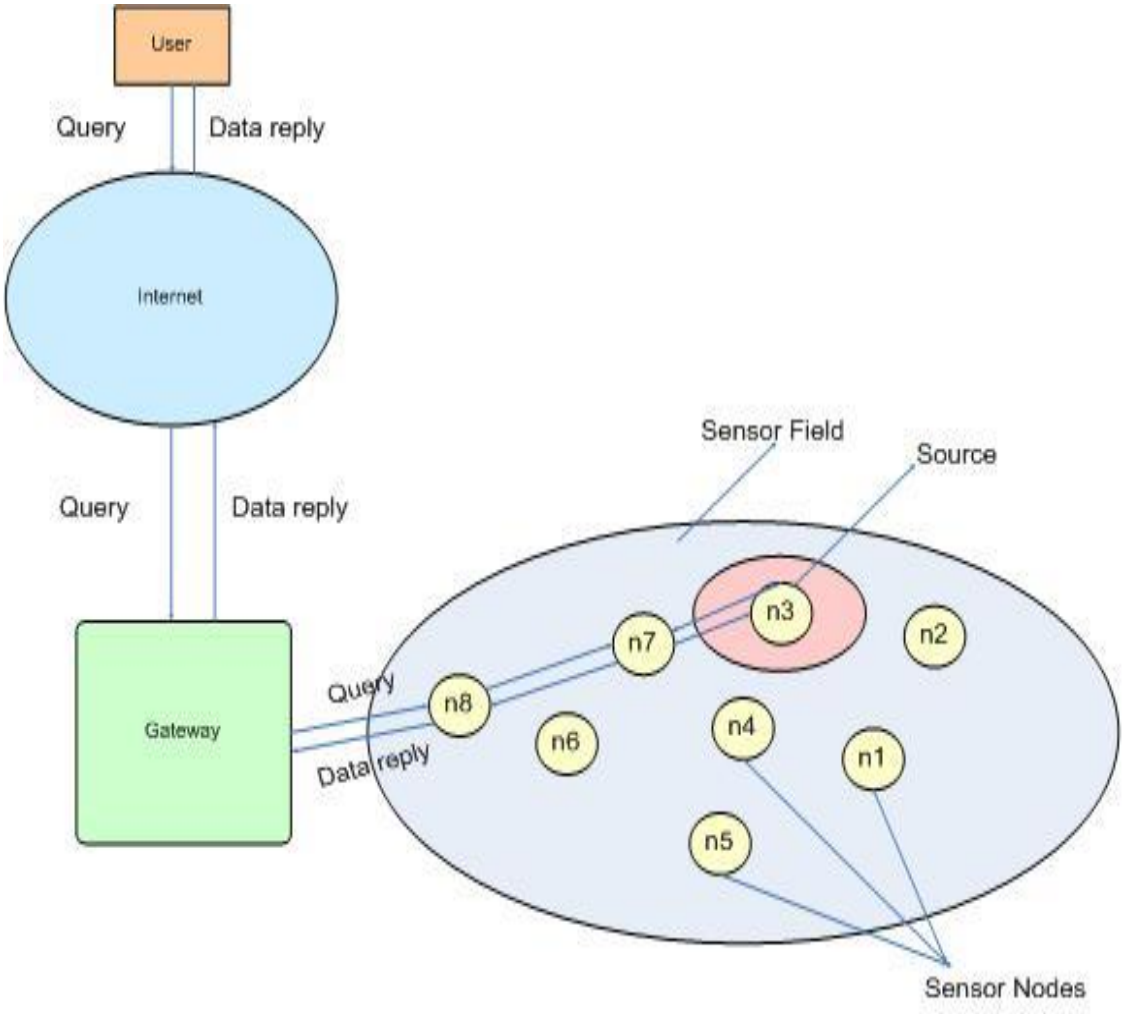


Figure 1.2: Internet Protocol (IP) based internet of things (IoT)

A Internet of Things network is an accumulation of IoT sensor nodes, which develops a system utilizing radio correspondence in a self-governing and circulated way. [5] Nodes are detached over a specific field, and can collect and transfer data about nature, keeping in mind the end goal to give fine-grained perceptions of a marvel. [14] A sensor hub is ordinarily outfitted with at least one sensors that are utilized to catch occasions from the earth, a simple advanced converter, a radio handset, a focal preparing unit with constrained computational capacities, a little measure of memory and a battery control supply. Sensor gadgets work together with each other so as to perform fundamental operations, for example, detecting, correspondence and information preparing. [21]

In the latest analysis on IOT, researchers try to seek out and overcome the constraints of IOT networks like restricted energy resources, move energy consumption by location, the high price of transmission, and restricted process capabilities [25] of these characteristics of IOT networks square measure completely opposition their cable counterparts network, that energy consumption isn't a problem, the price of transmission is comparatively low cost, and network nodes have lots of process power. [6] Routing approaches that have worked therefore fine for ancient networks over twenty years won't be enough for this new generation networks.

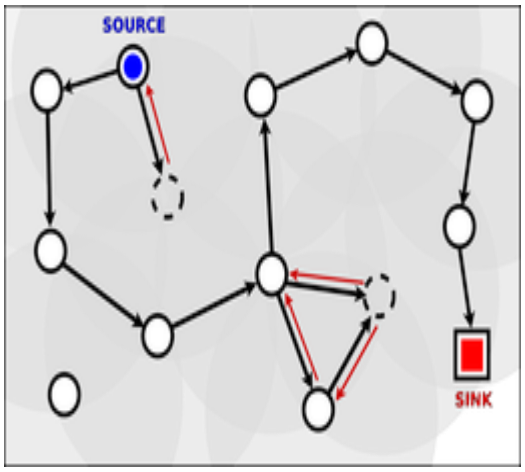


Figure 1.3: The simple representation of the wireless directed towards the Base Station or Sink Node

Besides increasing the time period of IOT nodes, it's best to share out the energy dissipated across the IOT network to reduce maintenance and maximize overall system performance. [9] A communication protocol that involves synchronization between peer nodes incurs some overhead of putting in place communication. IOT routing protocols or cluster to work out whether or not the advantages of a lot of advanced routing algorithms overshadow the extra management messages every node should communicate. [9,17] Every node might build the foremost wise call on communications choices if they'd complete information of the complete configuration and also the levels of all the nodes within the offer network.

This proves so to induce the simplest performance if the synchronization messages don't seem to be taken under consideration. However, as all nodes would still got to have a comprehensive understanding, the price of synchronization messages would ultimately terribly overpriced. For each diffusion and clump algorithms we are going to analyze the systems each realistic and optimum to achieve insight into the properties of the 2 approaches.

[5, 2]The common topology of IOT networks involves having several network nodes scattered in a very definite physical space. [4] it's typically not design or specific hierarchy in situ and thus, IOT networks area unit thought of unintended networks. A network of unintended wireless sensors will operate in a very standalone mode, or it is connected to different networks, like the biggest web through a base station. [17] The bottom stations area unit typically a lot of advanced than straightforward network nodes and frequently have indefinite power supply. relating to the restricted power of the wireless IOT nodes of abstraction utilise of wireless information measure, and also the nature of radio communication price that's a operate of the space square transmitted, it's ideal to send info many smaller jumps than transmission over an extended distance communication. [27] typically, IOT networks clump were of nice interest. Grouping nodes in clusters, resulting in gradable routing and knowledge assortment protocols, was thought of the foremost effective approach to support measurability in IOT networks. the first objective of most of the present protocols lies on a way to extend the time period of the network and the way to create a a lot of economicaluse of important resources, like power butter. additionally, the combined would like for speedy convergence time and minimum power consumption (in relevancy the cluster formation process) results in acceptable probabilistic (random or clearly hybrids) distributed clump algorithms quick that shortly became the foremost widespread and wide employed in the sector.

Real applications utilizing IoTs include: natural observing, human services, mind-set based administrations, situating and creature following, amusement, coordinations, transportation, home and office, modern and military applications. The innovative headways in remote correspondence and microelectronics have brought about a developing enthusiasm for the field of remote sensor systems.

1.2 IOT ARCHITECTURE

It is hard to establish a common ground for IOT standards for the evolution of the IOT reference architecture. As proposed by[2] a Reference Architecture Model for IOT provides a model for the transmission between many heterogeneous IOT devices and the Internet as a whole.

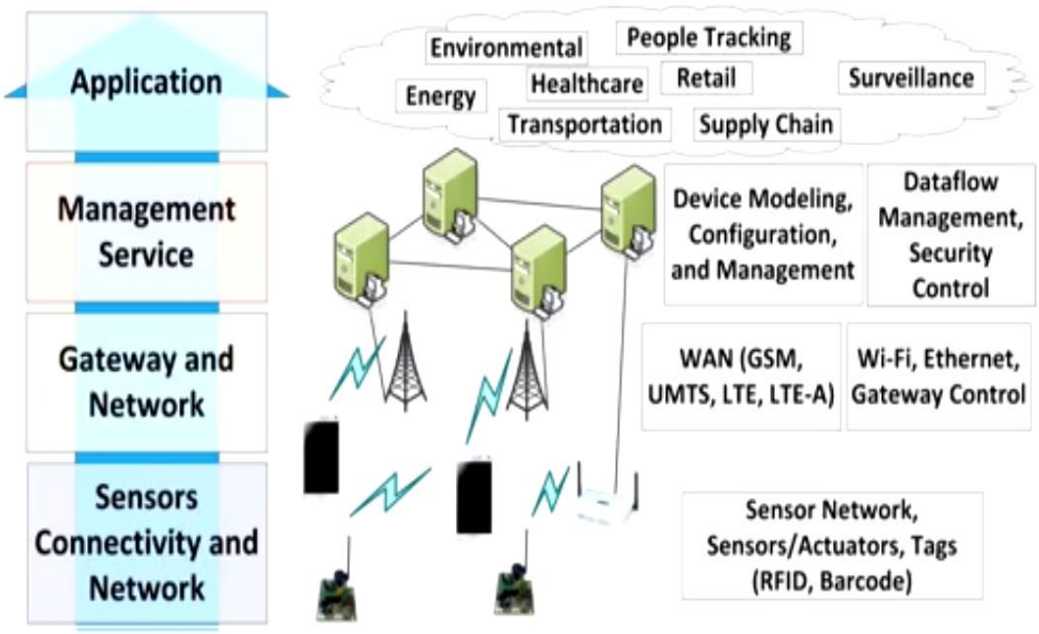


Fig 1.2.1 IOT Architectural Layers

Each device in the network contains IP address which unambiguously identifies it on the internet. The physical layer contains sensor devices ex RFID, barcode, Actuators, which are used to collect real time information and make use of low power and low data rate.

It requires strong and authentic performance for the private, public or hybrid network model. Thus network models are designed to communicate QoS requirements for latency error, probability, scalability and bandwidth, security while achieving high level of energy efficiency.

Information analysis, security control, process modelling and device management are contained in Management service layer .

In application layer various small and industry sector use IoT for service enhancement. This can be classified by courage, size, availability, heterogeneity and business model. Areas like personal and homes, utility, enterprise, mobile etc are included.

1.3 IoTs AND HEALTH CARE MONITORING NETWORKS

Social insurance is dependably a major worry, since it includes the personal satisfaction a given individual can have. It is constantly preferable to keep an ailment over to treat it, so singular observing is required as an intermittent action. The maturing populace of created nations show a developing cut of government's financial plan, and introduces new difficulties to social insurance frameworks, to be specific with elderly individuals living on

autonomous senior lodging. Customarily, wellbeing observing is performed on an occasional check premise, where the patient must recall its manifestations; the specialist plays out some check and defines a demonstrative, at that point screens understanding advancement along the treatment, if conceivable. In any case, a few side effects just show themselves in day by day exercises, where an individual may feel some torment or inconvenience. Human services uses of remote sensor systems permit in-home help, shrewd nursing homes, clinical trial and research expansion. In-home human services winds up plainly compulsory for sicknesses like Parkinson or Alzheimer, giving memory improvement through drug updates, mental incitement through sounds or pictures of question's area, control over home machines, medicinal information query, and crisis circumstances. Such approach may prompt a multi-layered design, with lightweight portable PCs and savvy sensors in conjunction with all the more intense computational gadgets. Before portraying and reviewing restorative applications for human services, this segment concentrates on a few difficulties and general angles that describe this sort of advances.

1.3.1 Challenges

Human services applications introduce a few difficulties: low power, restricted calculation, material limitations, persistent operation, heartiness and adaptation to internal failure, versatility, security and obstruction, and administrative prerequisites. The power challenge is available in practically every territory of utilization of remote sensor systems, yet restriction of a keen sensor embedded on a man still stances significantly additionally challenge, albeit progressing research tries to give control remotely. Another test as far as power originates from the operational warmth. For example, at times it is impractical to chill off the sensor by permitting contact with the earth. A commonplace soluble battery, for instance, gives around 50 watt-hours of vitality. This may mean not as much as a time of ceaseless operation for every hub in full dynamic mode. By and by, for some applications, it will be important to guarantee that a system can stay operational with no substitutions. Calculation is specifically restricted because of the constrained measure of energy. Ordinarily, biosensors are not anticipated that would have an indistinguishable computational power from traditional Internet of Things hubs. Since correspondence is indispensable and impression is little, little power stays for calculation. An answer can be information combination, which involves a few hubs pooling their data together for expanded computational power handling and precision. Additionally, it might be normal

that for a few applications, for example, blood glucose checking, the capacity to transmit information to an outer gadget will be required for encourage information handling. A few sensors may have differing capacities that speak with each other and convey one community information message. Material requirements is another issue for remote sensor systems application to medicinal services. A biosensor must be in contact with human body, or even on it. In the event that the biosensor is inside a pill, the decision of development materials must be cautious, particularly on batteries. Likewise compound responses with body tissue and the transfer of the sensor is of most extreme significance. In numerous applications, it is conceivable to dispose of at least one brilliant sensors without the requirement for any administrator intercession. Ceaseless operation must be guaranteed along the lifecycle of and openings. The regularly inspiration for aggressor is advantage from information. Aggressor openings extend from physical get to, remote correspondence, assaults on coordination and self-design, up to organize perceivability. Administrative necessities should dependably be met, significantly more with medicinal applications. There must be some confirmation that these gadgets won't hurt; even model gadgets should meet the strict guidelines of patient security before any human testing should be possible. The remote information transmission must not hurt human body and the incessant working and power usage of these gadgets should likewise be kind. Plan for security must be a key component of biomedical sensor advancement, even at the soonest arranges. Sensible confirmation of plan viability will be required notwithstanding for model gadgets.

1.4 SECURITY AND SECURITY ISSUES IN IOT

The security of internet of Things (IOT) is often listed removed from varied views. An overseas finish consumer reaching to base station knowledge are often unbroken from doing in {and of itself} in an assortment of the way. Correspondence between the bottom station and IoT sensing element nodes are often blocked. this may be skilful by easy protruding of signs or by computerised protruding as DoS (Denial of Service) assaults that surge the system, base stations or each. Directed DoS assaults on key hubs within the IOT will likewise piece correspondence of big components of the system with the bottom station. Correspondence between base stations and alternative IoT sensing element nodes are often averted by putting in incorrect directional knowledge with the goal that movement goes to the incorrect goal or circles. One approach to try and do this is often to parody the bottom station and beguile hubs into rerouting all bundles to the caricature base station instead of the real

basestation.[23,24] Another methodology for breaking security is to decimate the bottom station itself. This may be skillful by checking the amount and bearing of parcel activity toward the bottom station so the world is within the long-term uncovered. [7] Destruction will likewise be skillful by standardization in to the RF signs to limit and triangulate the world of the bottom station. The 3rd risk is listening in. this is often created less exigent by remote bounce to-jump correspondence. Listening stealthily are often used to trace and derive the world of the bottom station for demolition. There are varied completely different methods to rupture the IOT security. [18]

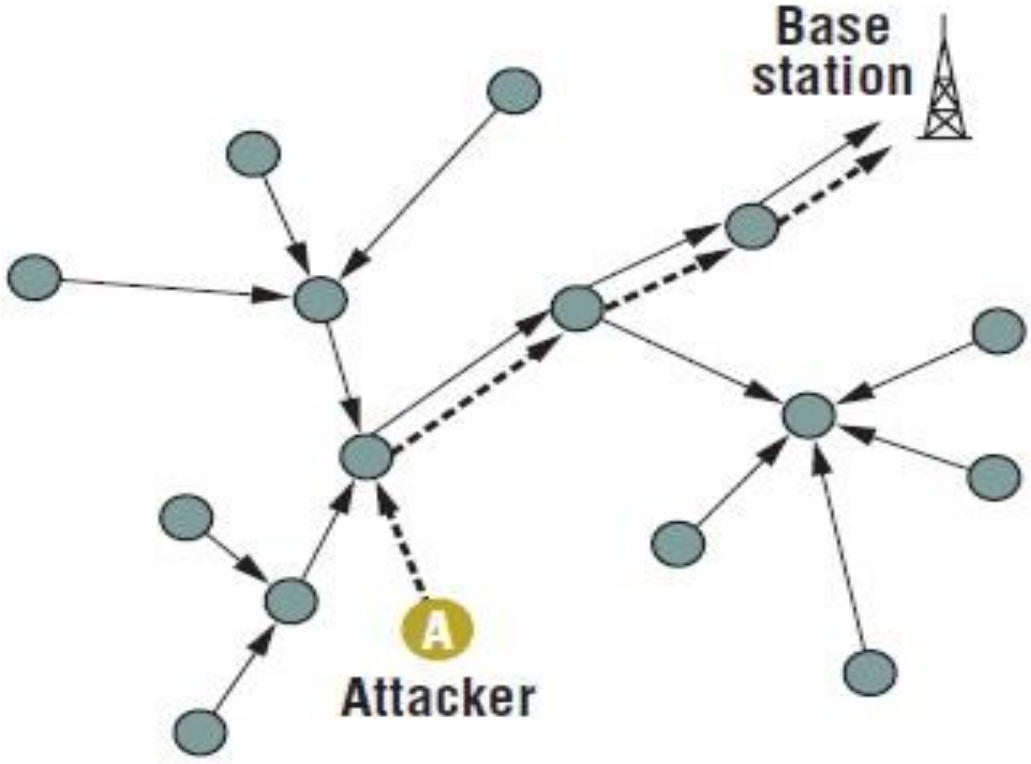


Figure 1.4: Attacks on Internet of Things [23]

Assault on IOT can be happening in various techniques. IOT is inclined to security assaults which are submissive in character. [7] The most natural security assaults on IoT sensor nodes is Monitor and Eavesdropping in this assault the adversary could without much of a stretch discover the data content by snooping the data. [12-13] Security of IOT is the most noticeable issue.False steering Information is a Routing Attacks in Sensor Networks the programmer change the directing information of steering conventions through malignant

code. [12-13] In wormhole assault the foe hold data from one area in the system transmit into another area and on the other hand retransmit into the system. Specific Forwarding is a dynamic assault in this sort of assault the programmers assaults the specific hub and contaminate with the vindictive data the irresistible hub act like a typical hub in organize this hub does not forward the parcels or information to next hub it just which make them act like a fizzled hub. [34]

CHAPTER 2
REVIEW OF LITERATURE

Renita Machado [13] IOT newtorks (IOT) including tiny knots, limited powers are gained the higher popularity in the data collection applications. The potential of IOT models is quite higher, which is characterized by its flexibility, scalability and high adaptability to the versatile environments. Although these environments detection targets are unique and depends on the application, the criteria of common performance for IOT newtorks extends the service life while satisfying the network coverage and connectivity in the deployment area. Pau Closas [8] in this paper, the subject of control of the network topology using a totally distributed algorithm is considered in wireless networks. While the proposed disseminated calculation is outlined applying the concepts of game theory to implement a non-helpful diversion, organize availability is possible on the basis of asymptotic results of network connectivity. Yenumula B [18] the problem of sensing malicious nodes in IOT newtorks is considered in this paper. So current safety mechanisms are inadequate for IOT newtorks, in this article the author should develop a new environment to sense malicious nodes using Zero-Sum game technique and selective acknowledgments node in the path data forward. Harilton da S. Araújo et al. [6] proposed a protocol to decrease consumption of energy in the network by changing the protocol called Directed Diffusion routing protocol. The proposal uses a Geocast approach in which all the broken roads are repaired by rebuilding new route computation tree so that the energy cost can be reduced. Abdellah et.al [1] propose a hierarchical protocol called Adaptive of effective and fair energy Routing Protocol (from HABRP) to reduce the chances of failure of of hubs and drag out the time interim before the passing of the primary hub (stable period)and the increase in lifespan diverse IOTs, which is critical for many applications. Bomgni Alain Bertrand et al. [3] propose an algorithm which is based clique. This algorithm guarantees the delivery of packets sent by the receiving node to all nodes that are deployed in various Geocast regions. In this proposal, the proposed algorithm is a hybrid classification system.

A lot of work is done on the wireless mesh network. Most cases, the authors claimed the best performance of routing protocols and improved energy in WMN node using the clustering, compared to active systems presented at that time. The following work is studied.

Dai et al. [9] proposed the workload through a mesh network, balancing of nodes decreases the hot spots in the sensor array and increase the life of the power of the mesh network. In the article the author to propose an algorithm on node-centric that builds a network loads balancer shaft asymmetric architecture sensors. The author evaluated the algorithm reaches routing trees which are additional efficiently fair routing based on the BFS and shortest path got by the Dijkstra algorithm.

Dragan et.al [17] proposed routing algorithm, permits the network to significantly reduce the amount of energy spent on the configuration of the communication and control, a major concern in communication with low data rate. This is achieved by sending a single stream of data from a family of sensors to the sink instead of a current from each individual sensor to the data destination. This also minimizes the chances of packet collisions in the wireless network because the same amount of information can be transmitted with some nodes send larger packets. Additional gains can be achieved by efficient data compression. This is achieved by lossless compression data by encoding information in the order of sensor packages.

Al-Karaki et al. [4] Wireless mesh networks contains tiny nodes with the capabilities like sensing, computation and wireless communication. Many steering, control administration, and information dispersal conventions have been particularly intended for work systems where vitality mindfulness is a basic plan issue. The mesh networks in routing protocols may vary on the basis of the network's application and network architecture. In the editorial, the author presents a study of the technical state of the art routing in mesh networks. The author first proposed an overview of the propose challenge for routing protocols in mesh networks, followed by an exhaustive study of routing techniques. Global routing approaches are categorised into three types according to the network structure underlying flat, hierarchic, and routing base on location.

Karim et.al [21] suggested that previous models of radio transmission are not always applicable to wireless mesh networks due to the nature endless long links. The document is of interest to the geolocation problem in that it offers new transfer strategies to improve

geographic routing performance with network losses by reducing the amount of time and energy consumed by the communication nodes in a wireless mesh network.

Raymond et.al [26] Multiresolution analysis, processing and promising compression for mesh network applications, progress has been confused by two factors. First, the typical sensor data is irregularly spaced, which is incompatible with the wavelet techniques. Second, communication overload multiscale algorithms can become prohibitive. In this article, the authors take a first step in the fight against deficiencies by introducing two new distributed multiresolution transformations. The Haar wavelet sampled irregular pyramid and the telescopic Haar wavelet basis provide effective approximations constant pieces of sensor data. The authors illustrate their hypothesis with compression examples of distributed data network and wavelet denoising.

Briles Scott et al. [6] describes the graphical programming tools used to implement a new geolocation algorithm consists of windowing, FFT, multiply complex spectral average and arctan function. The presentation may be of interest to our GUI efforts.

Sundeep et.al [25] analyzes the presentation of existing routing with compression programs in wireless mesh networks victimization joint entropy sources to count the dimensions of the compressed info and to a small degree hop metric quantify the full price of joint routing with compression. though the character of optimum routing with the compression depends on the amount of correlation, amazingly, there's a sensible static grouping theme that will give performance near the optimum for a large vary of abstraction correlations. They formalize the notion of Associate in Nursing virtually optimum size cluster and show that it depends on wherever the compression is performed within the network. This result's of nice sensible importance, as a result of it shows that the easy cluster-based system style will perform moreover as subtle adjustive systems for joint routing and compression.

Hailin Zhang [30] In mesh networks, conservation of energy is that the main goal, whereas the flow and delay are smaller. So, the energy used is negotiated for a rate and delay. During this paper, a replacement conception of the speculation of cooperative games is incompletely employed in mesh networks to realize all the objectives at the same time. within the game, each node sets its equilibrium state policy of the calculable game. when introducing the utility perform of the sport, the equilibrium atmosphere for the sport in mesh networks is conferred, additionally, a theory of straightforward games macintosh protocol (G-MAC) is regular for mesh networks, victimization Associate in Nursing automobile regressive

backward mechanism that's straightforward to implement. during this article, the author instructed that the cooperative game that is uncompleted will increase system turnout and cut back delay and packet loss rate, whereas maintaining affordable power consumption which G-Mac takes support the sport effectively.

Renita Machado [13] wireless mesh networks (WMN) as well as little knots, restricted power are getting quality as a result of their potential to be used during a sort of environments like watching environmental attributes, the detection of intrusion, and numerous military and civilian applications. though these environments detection targets ardistinctive and depends on the appliance, the standards of common performance for wireless mesh networks extends the service life whereas satisfying the network coverage and property within the preparation space. Another vital performance parameter in wireless mesh networks is security, wherever adverse and remote methods cause differing kinds of threats to the operation of the reliable network. during this article the author to appear the issues of safety and energy potency and completely different formulations of those drawbacks on the premise of the sport theory approach. The robust relevancy of environments to persona non grata detection mesh networks additionally lends itself to theory of games formulation of those environments, wherever the pursuit-evasion games give Associate in Nursing applicable framework for modeling detection applications, monitoring and surveillance.

Pau Closas [8] during this paper, the difficulty of management of the configuration employing a completely distributed rule is taken into account in wireless networks. whereas the planned distributed rule is meant applying the ideas of theory of games to implement a non-cooperative game, network property is feasible on the premise of straight line results of network property. during this article, the author proposes that for a relatively low node density, the probability that the planned rule ends up in a connected network is near one. during this paper the author studies the matter of power and management of the topology during a WMN distributed victimization the tools of theory of games. The novelty of labor is that network property is gained with a distributed rule on the premise of a non-cooperative game that the density nodes increase. For network property the planned rule relies on a non-cooperative game and straight line results.

Yenumula B [18] the problem of sensing malicious nodes in wireless mesh networks is considered in this paper. So current safety mechanisms are inadequate for wireless mesh networks, in this article the author should develop a new environment to sense malicious

nodes using Zero-Sum game technique and selective acknowledgments node in the path data forward. The nodes derived the model to sense malicious nodes using the probability of recognition at source.

Author	**Title**	**Technologies Used**	**Merits**	**Demerits**
Ahmed Al-Saadi, Rossitza Setchi, Yulia Hicks, Stuart M. Allen, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 65, NO. 12, DECEMBER 2016	Routing Protocol for Heterogeneous Wireless Mesh Networks	Cognitive Heterogeneous routing with WiFi integration over LTE networks	Efficient to handle the heavy traffic. Robust to handle the directional routes for moving nodes.	Updates the complete path, whenever required. Does not incorporate the segmental or phase routing.
Manlio De Domenico, Antonio Lima, Marta C González and Alex Arenas, EPJ Data Science (2015)	Personalized routing for multitudes in smart cities	Distributed routing with personalized maps establishes the vigorous routing mechanism.	Adaptable to Big Data situation (heavier data loads) Handles the individual or group paths towards the similar source,	Does not account the path manipulation. Converge the complete path in the path failure situation.
Murugeswari, R. et. al., Elsevier, December 2015	A multi-objective evolutionary algorithm based QoS routing in wireless mesh networks	Dynamic crowding distance with quality of service	Utilizes the Patero graph to compute best solution. Establishes the low delay situations.	Does not work towards path repairing. Uses complex solution to update the path.
Anfu Zhou, Min Liu, Zhongcheng Li, Eryk Dutkiewicz, IEEE Transactions on Vehicular Technology, 2015	Joint Traffic Splitting, Rate Control, Routing and Scheduling Algorithm for Maximizing Network Utility in Wireless Mesh Networks	Traffic shaping with dynamic traffic rate control mechanism.	Adapt to different situations with dynamic properties. Scheduling model enables the time slots for the users to receive and	No dynamic hop-to-hop path manipulation program.

			transmit data.	
Igor Ganichev, Bin Dai, P. Brighten Godfrey, Scott Shenker, ACM SIGCOMM Computer Communication Review, October 2010	YAMR: Yet Another Multipath Routing Protocol	External Routing protocol with inter-autonomous system routing capability.	Works on multiple paths simultaneously. Creates the dynamic inter-domain links.	Distance vector non-segmental route update. Path quality is not considered properly.
Wen Xu and Jennifer Rexford, SIGCOMM, September 2006	MIRO: Multi-path Interdomain Routing	Inter-domain & inter autonomous system routing with dynamic multipath capability.	Choose dynamic and best performing paths. Implements scalable autonomous system routing.	Recognize the whole path from source to destination. Doesn't recognize local paths under the autonomous systems

Table 1: Comparative Analysis of Various Routing Models

CHAPTER 3

PRESENT WORK

3.1. RESEARCH GAPS

1. The existing model is not capable of handling the dynamic routing for the mobile nodes in the given heterogeneous wireless mesh network. The handling of the dynamic routes for the mobile nodes in the case of wearable devices, healthcare tracking equipments, vehicular networks, etc becomes mandatory in the smart cities, and must be incorporated to make the wider adaptability of the target systems.
2. The existing model is also not capable of handling the dynamic internal routing table, which must be incorporated in order to handle the mobility of the nodes within the zone and out of the mesh network zone. The micro or segmental route updates as well as the complete route updates mechanism can be utilized dynamically to facilitate the high order mobility from zone to zone.
3. The existing model is tested with maximum 30 nodes, which is not sufficient to handle the internet of things (IoT) clusters. The incorporation of this model in the case IoT requires many critical improving, which includes the handling of the different kinds of data, data stream interoperability and smart route selection mechanism to minimize the network load for the efficient routing among the IoT clusters.

3.2 PROBLEM FORMULATION

In the existing scheme, authors used distributed-smart distance based metric computation mechanism to solve the problem of efficient route selection for traffic congestion control in the smart cities also by avoiding the connectivity holes and the dead ends to minimize the data propagation control. The distributed-smart distance based routing mechanism is able to solve the difficulty of efficient-route selection up to the level in the nodes connected in tree structure but can’t be considered efficient enough for efficient metric calculation in the distributed environment based smart city scenarios.

The problem of connectivity holes has increased with the increase in the network size. The connectivity holes must be discovered and eliminated from the networks as earlier as possible in order to improve the overall network performance. The existing scheme belongs to the

proactive routing protocols, where the network resources are aligned to prepare and schedule the data routes. The tree routing concept has been utilized in the existing routing scheme, which expands towards the network outline and contracts towards the center of the network. The tree routing scheme are usually used to handle the rising network data volumes on the network nodes near the base station or center. The existing scheme provokes the transmission of data through the relay nodes, which are known as the nodes within the active routing path. The existing scheme does not use the intelligence to detect and eliminate the connectivity holes, and does not take an account of the path length before and after detection of the connectivity holes. Hence, the existing model is prone to the problem of choosing of the longer paths than pre-blackhole elimination paths. The longer paths also increase the routing cost, which may degrade the network performance, and creates an inefficient network performance.

3.3. PROPOSED ALGORITHM

The existing system will be enhanced for its metric calculation to seelect the finest route and route for balancing of load while sending the data towards the BTS. The BTS gets the data from the cluster heads in the wireless networks.The value of metric calculation would be improved by joining the values of the next hop trust, overall hop count, dynamic node id and bandwidth existing between the source and destination nodes in the smart-city environment. The dynamic route update algorithm will be proposed and designed for the dynamic route updation in the segmental (micro) routing mechanism when operating within the given zone. The inter-zone handovers will be treated with the complete route updates in order to remove the chances of bad route origination. The adaptive load balance balancing based new methodl use this new metric route to find the shortest route with balanced, efficient and higher bandwidth based route selection mechanism to make the delivery process faster and to avoid the congestion and data loss. The route cost estimation for balancing of load will be based on the individual load on the relay node/s, the other routes with the minimum load will be also measured to discover the alternative route. Between the shortlisted routes using the load as metric, the route with low total route cost will be used to forward the data. The existing algorithm will be compared to our proposed algorithm using end to end delay/latency, packet delivery ratio, network/route load and packet Efficiency of the alternative route. The project will be developed using MATLAB simulator. The algorithm to spot the connectivity hole or failure of link will be used to renewthe routing table while the primary route becomes busy. Reply back method will be used to detect the link failure, and to execute the backup and load

balance route finder event base enhanced adaptive load balancing rainbow protocol for smart cities

3.4 OBJECTIVES OF THE STUDY

- To review the critical problems in the existing models in order to discover the possible improvements
- The create a model that is able to handle the dynamic routing for the mobile nodes in the given heterogeneous wireless mesh network
- The create a model that can test more than 30 nodes, so that it is sufficient to handle the internet of things (IoT) clusters.
- To design the proposed model to overcome the shortcomings associated with proposed model.
- To implement the proposed model using the MATLAB simulator with essential input and output parameters.

CHAPTER 4

RESEARCH METHODOLOGY

5.1. TOOLS USED

Hardware Requirements

- SYSTEM: Dual Core, 1.70 GHz CPU or above
- HARD DISK: 80 GB
- MONITOR: colour, Any size
- RAM: 2 GB

Software Requirements

- Operating system: Windows 7/8 or Above
- Application: MATLAB v2013a or above
- Coding Language: MATLAB Programming

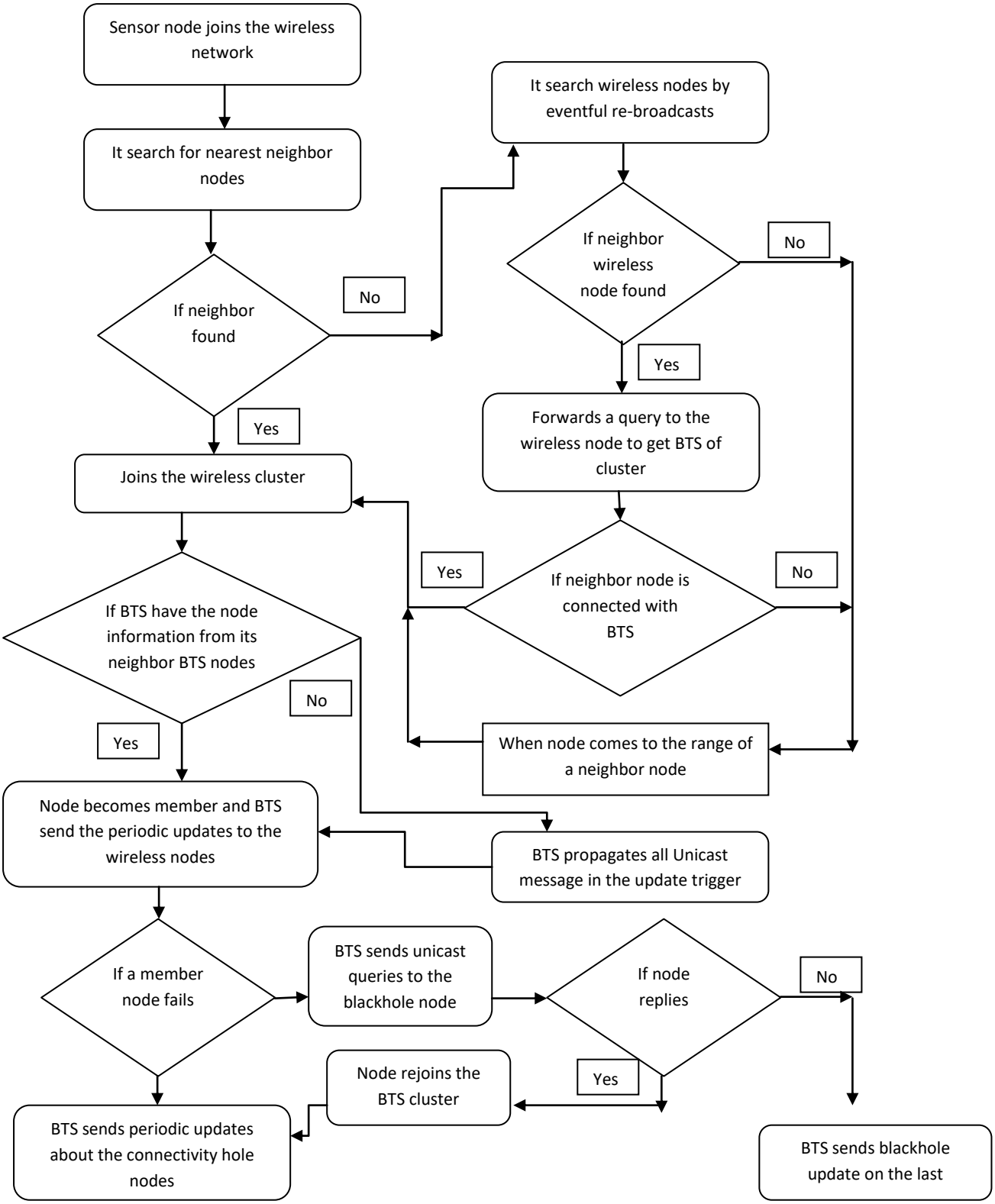
5.2. METHODOLOGY

The existing scheme will be enhanced by using the smart routing scheme based upon the segmental computation. This means the network divided in the individual cluster will involve the each cluster's nodes individually to discover the stable and robust path. This path is maintained within the clusters, rather than maintaining the whole source to destination path at once. This makes the path management easier and quicker, which means now the network path can be easily manipulated within the lesser delay, which must improve the overall performance of the networks. The number of possible paths may be higher than one to elect a path between the point A and B in the given network. Choosing the best path is a typical problem, which must be handled with the proposed scheme. The selection of the paths should be based upon the path performance rather than the number of nodes (i.e. hop count), route cost or other such factors used traditionally in the routing scheme (also existing scheme). The network performance will be analyzed using the variety of the performance parameters, which includes the transmission delay, network load, throughput, number and volume of

dropped packets and data, etc. The simulation model will be prepared using the MATLAB simulator, which includes the various essential tools and built-in modules for rapid and robust development. The reply back method will be utilized for the detection and elimination of the node failures in the network segment. This method also helps to find the best alternative path among the given wireless network.

This work can be demonstrated using the MATLAB platform, which can easily work on a normal PC or laptop with 4 GBs of RAM and dual-code processor (i3/i5 or above). The Hard Disk Drive (HDD) space required to install MATLAB is under 10 GBs. The project simulation will begin with simulation of an IOT topology, which can handle the dynamic number of nodes. The IOT topology will further undergoes the incorporation of routing, which will improve the connectivity of the network in the presence of connectivity holes. Afterwards, the new mechanism would be analyzed for its performance with the appropriate parameters

5.3. FLOWCHART OF PROPOSED WORK



CHAPTER 5

CONCLUSION

5.1 EXPECTED OUTCOME

- The proposed model is expected to improve the end-to-end delay in the IOT networks, specifically in the presence of connectivity hole and larger data volumes.
- Also, the network lifetime and energy consumption would be optimized by decreasing the chances of data drop in the given IOT networks.

5.2 CONCLUSION

The proposed model is aimed to improve the end-to-end delay and data drop rate. These can be improved by designing the new routing protocol with the ability to avoid or eliminate the connectivity holes from the routing paths and to handle the larger volumes of data across the multiple paths. This work can be demonstrated using the MATLAB platform, which can easily work on a normal PC or laptop with 4 GBs of RAM and dual-code processor (i3/i5 or above). The Hard Disk Drive (HDD) space required to install MATLAB is under 10 GBs. The project simulation will begin with simulation of an IOT topology, which can handle the dynamic number of nodes. The IOT topology will further undergoes the incorporation of routing, which will improve the connectivity of the network in the presence of connectivity holes. Afterwards, the new mechanism would be analyzed for its performance with the appropriate parameters.

The following points must be kept in consideration while framing the design of the proposed model:

1. The existing model does not analyze the connectivity holes in the IOT network while constructing the routing paths, which is the major reason for the data drop and increased end-to-end delay. In the existing demonstration, the effect of connectivity holes is not analyzed. The proposed model will resolve the issues related to the connectivity holes, while constructing the network routes in the given topology.

2. The existing model is also not capable of handling the larger volumes of data, which is now a day very common scenario in the urban areas. Hence, the proposed routing

model can be further improved to handle the larger data volumes by planning the multipath routing between the sources and destinations facing larger volumes of data. Hence, the multipath routing will act as an on-demand service, which would be activated only during heavier loads.

REFERENCES

[1] Agah, A., Asadi, M., & Das, S. K. (2006). Prevention of DoS Attack in Mesh networks using Repeated Game Theory. In *ICWN* (pp. 29-36).

[2] Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless mesh networks. *Ad hoc networks*, *3*(3), 325-349.

[3] Alain Bertrand, B., & Jean Frédéric, M. (2010). An energy-efficient clique-based geocast algorithm for dense mesh networks. *Communications and Network, 2010*.

[4] Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless mesh networks: a survey. *Wireless communications, IEEE*, *11*(6), 6-28.

[5] Ben Alla, S., Ezzati, A., Beni Hssane, A., & Hasnaoui, M. L. (2011, April). Hierarchical adaptive balanced energy efficient routing protocol (HABRP) for heterogeneous wireless mesh networks. In *Multimedia Computing and Systems (ICMCS), 2011 International Conference on* (pp. 1-6). IEEE.

[6] Briles, S., Arrowood, J., Turcotte, D., & Fiset, E. (2005, May). Hardware-In-The-Loop Demonstration of a Radio Frequency Geolocation Algorithm. In *Proceedings of the Mathworks International Aerospace and Defense Conference*.

[7] Byers, J., & Nasser, G. (2000). Utility-based decision-making in wireless mesh networks. In *Mobile and Ad Hoc Networking and Computing, 2000. MobiHOC. 2000 First Annual Workshop on* (pp. 143-144). IEEE.

[8] Closas, P., Zamora, A. P., & Rubio, J. A. F. (2009, April). A game theoretical algorithm for joint power and topology control in distributed WMN. In *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on* (pp. 2765-2768). IEEE.

[9] Dai, H., & Han, R. (2003, December). A node-centric load balancing algorithm for wireless mesh networks. In *Global Telecommunications Conference, 2003. GLOBECOM'03. IEEE* (Vol. 1, pp. 548-552). IEEE.

[10] Dufwenberg, M., & Kirchsteiger, G. (2004). A theory of sequential reciprocity. *Games and economic behavior*, *47*(2), 268-298.

[11] Han, Z. (2012). *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge University Press.

[12] Ishmanov, F., Malik, A. S., & Kim, S. W. (2011). Energy consumption balancing (ECB) issues and mechanisms in wireless mesh networks (WMNs): a comprehensive overview. *European Transactions on Telecommunications, 22*(4), 151-167.

[13] Machado, R., & Tekinay, S. (2008). A survey of game-theoretic approaches in wireless mesh networks. *Computer Networks, 52*(16), 3047-3061.

[14] MacKenzie, A. B., & DaSilva, L. A. (2006). Game theory for wireless engineers. *Synthesis Lectures on Communications, 1*(1), 1-86.

[15] Meshkati, F., Poor, H. V., & Schwartz, S. C. (2007). Energy-efficient resource allocation in wireless networks. *Signal Processing Magazine, IEEE, 24*(3), 58-68.

[16] Park, G. Y., Kim, H., Jeong, H. W., & Youn, H. Y. (2013, March). A novel cluster head selection method based on K-means algorithm for energy efficient wireless mesh network. In *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on* (pp. 910-915). IEEE.

[17] Petrovic, D., Shah, R. C., Ramchandran, K., & Rabaey, J. (2003, May). Data funneling: Routing with aggregation and compression for wireless mesh networks. In *Mesh network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on* (pp. 156-162). IEEE.

[18] Reddy, Y. B., & Srivathsan, S. (2009, June). Game theory model for selective forward attacks in wireless mesh networks. In *Control and Automation, 2009. MED'09. 17th Mediterranean Conference on* (pp. 458-463). IEEE.

[19] Sakarindr, P., & Ansari, N. (2007). Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless mesh networks. *Wireless Communications, IEEE, 14*(5), 8-20.

[20] Sarkar, S., & Datta, R. (2014, February). A secure and energy-efficient stochastic routing protocol for wireless mobile ad-hoc networks. In *Communications (NCC), 2014 Twentieth National Conference on* (pp. 1-6). IEEE.

[21] Seada, K., Helmy, A., & Govindan, R. (2004, April). On the effect of localization errors on geographic face routing in mesh networks. In *Proceedings of the 3rd international symposium on Information processing in mesh networks* (pp. 71-80). ACM.

[22] Seada, K., Zuniga, M., Helmy, A., & Krishnamachari, B. (2004, November). Energy-efficient forwarding strategies for geographic routing in lossy wireless mesh

networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems* (pp. 108-121). ACM.

[23] Shi, H. Y., Wang, W. L., Kwok, N. M., & Chen, S. Y. (2012). Game theory for wireless mesh networks: a survey. *Sensors*, *12*(7), 9055-9097.

[24] Stojmenovic, I., & Lin, X. (2001). Power-aware localized routing in wireless networks. *Parallel and Distributed Systems, IEEE Transactions on*, *12*(11), 1122-1133.

[25] Upadhyayula, S., & Gupta, S. K. (2007). Spanning tree based algorithms for low latency and energy efficient data aggregation enhanced convergecast (dac) in wireless mesh networks. *Ad Hoc Networks*, *5*(5), 626-648.

[26] Wagner, R., Sarvotham, S., Choi, H., & Baraniuk, R. (2005). *Distributed multiscale data analysis and processing for mesh networks*. RICE UNIV HOUSTON TX DEPT OF ELECTRICAL AND COMPUTER ENGINEERING.

[27] Xu, J. Q., Wang, H. C., Lang, F. G., Wang, P., & Hou, Z. P. (2011, June). Study on WMN topology division and lifetime. In *Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on* (Vol. 1, pp. 380-384). IEEE.

[28] Yadav, S., & Lakhani, K. (2013). A Cluster based Technique for Securing Routing Protocol AODV against Black-hole Attack in MANET. *International Journal of Distributed and Parallel Systems*, *4*(2), 17.

[29] Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless mesh networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications*, *35*(3), 867-880.

[30] Zhao, L., Zhang, H., & Zhang, J. (2008, March). Using incompletely cooperative game theory in wireless mesh networks. In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE* (pp. 1483-1488). IEEE.

[31] Agah, A., Asadi, M., & Das, S. K. (2006). Prevention of DoS Attack in Mesh networks using Repeated Game Theory. In *ICWN* (pp. 29-36).

[32] Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless mesh networks. *Ad hoc networks*, *3*(3), 325-349

[33] Al-Saadi, Ahmed, Rossitza Setchi, Yulia Hicks, and Stuart M. Allen. "Routing Protocol for Heterogeneous Wireless Mesh Networks." *IEEE Transactions on Vehicular Technology* 65, no. 12 (2016): 9773-9786.

[34] Murugeswari, R., S. Radhakrishnan, and D. Devaraj. "A multi-objective evolutionary algorithm based QoS routing in wireless mesh networks." *Applied Soft Computing* 40 (2016): 517-525.

[35] De Domenico, Manlio, Antonio Lima, Marta C. González, and Alex Arenas. "Personalized routing for multitudes in smart cities." *EPJ Data Science* 4, no. 1 (2015): 1.

[36] Zhou, Anfu, Min Liu, Zhongcheng Li, and Eryk Dutkiewicz. "Cross-layer design with optimal dynamic gateway selection for wireless mesh networks." *Computer Communications* 55 (2015): 69-79.

[37] Ganichev, Igor, Bin Dai, P. Godfrey, and Scott Shenker. "YAMR: Yet another multipath routing protocol." *ACM SIGCOMM Computer Communication Review* 40, no. 5 (2010): 13-19.

[38] Xu, Wen, and Jennifer Rexford. *MIRO: multi-path interdomain routing*. Vol. 36, no. 4. ACM, 2006.