The Internet of Everything

De Gruyter Series on the Internet of Things

Edited by
Nilanjan Dey, Gitanjali Shinde, Parikshit Mahalle, Henning Olesen

The Internet of Everything

Advances, Challenges and Applications

Edited by
Nilanjan Dey, Gitanjali Shinde, Parikshit Mahalle,
Henning Olesen

DE GRUYTER

Editors
Prof. Dr. Nilanjan Dey
Rajarhat
700156 Kolkata
West Bengal
India
neelanjan.dey@gmail.com

Prof. Dr. Gitanjali Shinde
SKNCOE, Savitribai Phule Pune University
Vadgaon Budruk, Pune
411007 Maharashtra
India
gr83gita@gmail.com

Prof. Dr. Parikshit Mahalle
SKNCOE, Savitribai Phule Pune University
Vadgaon Budruk, Pune
411007 Maharashtra
India
aalborg.pnm@gmail.com

Prof. Dr. Henning Olesen
Communication, Media and Information Technologies
Frederikskaj 12
2450 Copenhagen
Denmark
olesen@cmi.aau.dk

ISBN 978-3-11-062548-6
e-ISBN (PDF) 978-3-11-062851-7
e-ISBN (EPUB) 978-3-11-062578-3
ISSN 2626-5443

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

Typesetting: Integra Software Services Pvt. Ltd.
Printing and binding: CPI books GmbH, Leck
Cover image: wacomka / iStock / Getty Images Plus

www.degruyter.com

Contents

List of Contributors

Rachana Ashetakr
SKNCOE, Savitribai Phule Pune University
Pune, Maharashtra, India
privacysurvey@gmail.com

Hari R. Bhapkar
ADT University's MIT School of Engineering,
Pune, Maharashtra, India
hrbhapkar@gmail.com

Sanjukta Bhattacharya
Department of Information Technology
Techno International Newtown, New Town
Kolkata, West Bengal, India
sbhattacharya.tict@gmail.com

Samhita Das
Department of Information Technology
Techno International Newtown, New Town
Kolkata, West Bengal, India
samhitad9@gmail.com

Manjusha Deshmukh
Computer Department, Pillai College of
Engineering, New Panvel, Navi Mumbai
Maharashtra, India
manjushad3112@gmail.com

Avinash S. Devare
Computer Department, Koneru Lakshmaiah
Education Foundation, Guntur, Andhra
Pradesh, India
devarea9@gmail.com

Shristee Ganguly
Department of Information Technology
Techno International Newtown, New Town
Kolkata, West Bengal, India
rajrajeshwari724@gmail.com

Vandana Jagtap
School of Computer Engineering and
Technology, MIT World Peace University
Pune, Maharashtra, India
vandana.jagtap@mitpune.edu.in

Sangeeta Kakarwal
Computer Science and Engineering
Department, PES College of Engineering
Aurangabad, Maharashtra, India
s_kakarwal@yahoo.com

Ananjan Maiti
Department of Information Technology
Techno International Newtown, New Town
Kolkata, West Bengal, India
ananjan.maiti@gmail.com

Parikshit N. Mahalle
SKNCOE, Savitribai Phule Pune University
Pune, Maharashtra, India
aalborg.pnm@gmail.com

Snehal Mane
School of Computer Engineering and
Technology, MIT World Peace University
Pune, Maharashtra, India
s30mane@gmail.com

G. Krishna Mohan
Computer Department, Koneru Lakshmaiah
Education Foundation, Guntur, Andhra
Pradesh, Indi
gvlkm@kluniversity.in

P. Muthu Kannan
Saveetha School of Engineering, Saveetha
Institute of Medical and Technical Sciences
Chennai, Tamil Nadu, India
pmkannan@gmail.com

Poonam N. Railkar
SKNCOE, Savitribai Phule Pune University
Pune, Maharashtra, India
poonamrailkar@gmail.com

Akshada Rathod
Department of Computer Science and
Engineering, MIT School of Engineering, ADT
University, Pune, Maharashtra, India
akshadarathod2@gmail.com

https://doi.org/10.1515/9783110628517-201

Sambhaji Sarode
Department of Computer Science and Engineering, MIT School of Engineering, ADT University, Pune, Maharashtra, India
sambhaji.sarode@mituniversity.edu.in

Gitanjali R. Shinde
SKNCOE, Savitribai Phule Pune University
Pune, Maharashtra, India
gr83gita@gmail.com

R. Thirukkumaran
Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences
Chennai, Tamil Nadu, India
kumaran.satinfo@gmail.com

Introduction

Internet of things (IoT) envisages a deep sense of connectivity and communication between the living and nonliving things. Nowadays, the vision of IoT has expanded to connect everything from industrial equipment, to everyday objects, to living organisms such as plants, farm animals and people. To create a niche for nonliving things to react, respond and work autonomously as and when required and as per their role, position and location in the ecosystem to provide services to the user, IoT is developing rapidly in the industrial settings.

Machine-to-machine communication and smart computing enhances the efficiency and helps minimize control cost of the industrial plants. IoT integrates the physical world with the information world so that every entity/device works for the betterment and in coordination with the other to help save the most valued resources and time. In this book, different approaches of the IoT and IoTPS (Internet of things, people and services) will be discussed.

Objective of the book

In the era before IoT, the World Wide Web, Internet, Web 2.0 and social media made people's lives comfortable by providing web services and facility to access personal data irrespective of their location. Further, to save time and improve efficiency, there is a need for machine-to-machine communication, automation, smart computing and ubiquitous access to personal devices. This need gave birth to the phenomenon of IoT and further to the concept of IoTPS. This book aims at presenting different aspects of IoT and IoTPS for smart computing, which comprises eight chapters.

Organization of the book

The book consists of eight chapters, and the brief description is as follows:

Chapter 1

Adaptive routing for emergency communication via MANET

Mobile ad hoc networks have emerged in past years due to their wide applicability in the field of disaster recovery, police operations, crowd management, emergency and military operations such as battle fields. Furthermore, through the advent of sensor-enabled intelligent mobile devices, MANETs have become a crucial element

https://doi.org/10.1515/9783110628517-001

in the framework of IoT and smart city developments. In this chapter, a novel energy-efficient counter-based scheme is introduced to address network challenges of MANET.

Chapter 2

Partial face recognition using image fusion

The conventional way of taking the attendance of students is strenuous and also lengthy. The lecture normally prolongs the maintenance of the student's attendance. This technique is ineffective, particularly if it is a lecture with a large number of students. This chapter recommends a novel technique to acknowledge students face to speed up the procedures of attendance in the classroom. The image fusion with the averaging method is used to improve the effectiveness of the system.

Chapter 3

Threat analysis and attack modeling for machine-to-machine communication toward Internet of things

The wide variety of IoT applications demands a secure and efficient communication channel that resists against a variety of modern attacks and fulfills application requirement. There are various IoT threats and challenges that must be addressed to make a communication secure in IoT. This chapter gives detailed analysis of attacks with its behavioral modeling. Furthermore, the chapter proposes a novel security framework, which emphasizes on making secure communication layer with the help of trust management policies, distributed access control framework and privacy-aware protocols.

Chapter 4

Security issues and trust management schemes in Internet of things

IoT is an emerging research field in the network domain and is applied to almost all the applications that can change the people's lives as smart. The number of security threats related to infrastructure, platform and application of IoT has been increased over the last few years. So, it is necessary to apply proper security solutions that ensure privacy and confidentiality of data. This chapter provides a detailed review of the security challenges and trust management techniques adopted for IoT to secure data in a cloud environment.

Chapter 5

Users' privacy at online social networks in Indian context: comprehensive multiaged group survey and discussion

Nowadays, social media has become an important part of life. People around the globe use social media for random purposes. However, they do not often realize that they are attracting very serious incidents that can occur due to their posts. Online privacy is one of the crucial points to safeguard our personal information. To provide privacy-aware online social networks, it is important to know user's awareness about privacy. To achieve this, survey is conducted and from the analysis of survey the user's awareness and requirements of privacy-aware mechanism is presented in this chapter.

Chapter 6

Early prediction of breast cancer from mammogram images using classification methods: a comparison

Nowadays, deaths of women in the age group of 15–54 are increasing due to malignant cells in breast. It is recognized as the main cause for the deaths of women. Day by day, the number of patients are increasing, because its important factors have not been identified yet, it is unable to prevent. So, the possibility of improvement is only the early diagnosis. This chapter provides survey of techniques that can help the prior detection of cancer using different classification methods such as support vector machine, decision tree, artificial neural network, logistic regression and machine learning-neural network.

Chapter 7

Deep brain monitoring using implantable sensor and microcontroller: a review

The consequent evolution in technologies is reaching toward the development of today's world. Micro-electro-mechanical system technology is one of the emerging paradigms that signify continuous affection in health-care systems. In hospitals, it is very necessary to constantly examine the health condition, monitor movements and physiological parameters of patients. In this chapter, the deep brain monitoring using implantable sensors and microcontroller is used for treating number of neurological disorders.

Chapter 8

Enhancement path assured transfer protocol to transmit urgent data

Sensor network is designed to provide monitoring services specifically for natural disaster. These natural disasters may affect the lives of human beings directly or indirectly. Congestion is a very important factor in wireless sensor network and also it reduces quality of services. It is very important to control the congestion as it may cause loss of packets or even more utilization of energy by sensor nodes. This chapter presents a protocol that checks for urgent data and gives priority to urgent data, so that this sensitive data will reach destination in time.

Manjusha Deshmukh and Sangeeta Kakarwal

1 Adaptive routing for emergency communication via MANET

Abstract: In the past, mobile ad hoc networks (MANET) have emerged due to their wide applicability in the field of disaster recovery, police operations, crowd management, emergency and military operations such as battle fields. Furthermore, through the advent of sensor-enabled intelligent mobile devices, MANETs have become a crucial element in the framework of Internet of things (IoT) and smart city developments. MANET is a decentralized system consisting of mobile nodes capable of forming a self-configurable, infrastructure-less and continuously evolving network. The lack of infrastructure empowers each mobile node to accomplish routing operation to confirm connectivity in MANET. Therefore, routing in MANET is an interesting operation. Most of the routing protocols used MANET as the basic broadcasting mechanism for flooding. In flooding, in order to find the route from source to destination, the packet is broadcasted to the neighboring nodes which in turn broadcast it to its neighboring nodes and this process sustains until the packet reaches to the destination. This neighborhood processing in MANET leads to broadcast storm problem. Traditional broadcast schemes have been presented to avoid broadcast storms by inhibiting some rebroadcasts. Another issue is the link failures caused by node mobility and energy exhaustion. In this chapter, we introduce a novel energy-efficient counter-based scheme and extend the scheme to reflect the mobility of node into an account to address these network challenges of MANET. In the proposed scheme, the decision of broadcasting is taken based on neighborhood, mobility and the energy of mobile nodes. The simulation results reveal that proposed schemes decrease the packet loss, the latency time and achieve lower energy consumption, better packet delivery and throughput when compared to ad hoc on-demand distance vector and hybrid counter-based broadcast routing protocol.

Keywords: MANET, CBB, emergency communications, broadcasting, energy-based schemes

1.1 Introduction

Recently, the wireless network has allured much concentration from researchers because of the technological growth of wireless communication. The wireless network can be categorized into two types: infrastructured and infrastructure-less. In infrastructured wireless networks, the wireless mobile nodes communicate with access points that are attached to the fixed infrastructure. Nowadays, we already have

https://doi.org/10.1515/9783110628517-002

over a dozen widespread infrastructured wireless networks in use: global system for mobile communications, universal mobile telecommunications service, wireless local loop, wireless local area network and others. In infrastructure-less or ad hoc wireless network, the wireless mobile nodes function as routers to confirm connectivity among the mobile nodes. These wireless mobile nodes establish a spontaneous network to interchange information without relying on any preexistent fixed infra-infrastructure. Various infrastructure-less networks are available, which include mobile ad hoc networks (MANET), wireless sensor networks (WSN), vehicular ad hoc networks (VANET) and flying ad hoc networks (FANET) [l–3]. A WSN is an infrastructure-less network of physically scattered self-governing devices using sensors to observe physical or environmental conditions. Furthermore, in the Internet of things (IoT), the WSNs become greatly popular [4]. VAHNET is an infrastructure-less network of smart vehicles set up with wireless devices [5]. FANET is an infrastructure-less network of a group of tiny flying vehicles equipped with camera, sensor and GPS [6]. The MANET is the most commonly used cost-effective infrastructure-less network. The wireless mobile nodes in MANET establish communication by forming a self-configurable and continuously evolving network [7]. The continuously changing and self-evolving feature of MANETs makes them most suitable for emergency communications. In emergency situations, during natural calamities such as earthquake, flood, tsunami and hurricanes, or man-made calamities such as terrorist attack and bomb blasts, the quick infrastructured network could be completely disrupted. Eventually, the rapid response and coordinated assistance become saturated and unmanageable. The MANET plays a vital role in the smooth conduction of rescue operations after the natural or man-made calamities [8].

Furthermore, through the advent of sensor-enabled smart mobile devices, MANETs have become a crucial element in the framework of smart city and IoT scenarios [9]. In addition, incorporation of multiple input–multiple output (MIMO) technology with MANET can enhance the performance of communication process in hazardous surroundings [10]. The framework of IoT with the keystone as an identity of wireless mobile computing devices has become the foundation for incorporating security methods such as authentication and authorization [11, 12]. The diverse applications of MANET received potential attention toward efficient network creation in MANET. The continuously evolving and uncertain behavior of MANETs makes routing a more interesting facet to emphasize upon [13]. Broadcasting is the most fundamental operation used for routing in MANET. Flooding is the elementary operation used for broadcasting in MANET. In flooding, when a node gets the broadcast packet relay on the packet to all its neighbors; in return, these neighbors get a broadcast packet relay on the packet to its neighbors. This process of relaying on the packet sustains until all reachable nodes in the network get the packet. The packets flood the network gradually and hence cause redundant broadcasts, collisions and contention

problem in the network. Such a severe problem is collectively known as broadcast storm problem (BSP) [14]. The fundamental solution on BSP is to minimize the number of redundant packets. There are several enhanced schemes that inhibit some nodes from broadcasting the packets through the network with the aim to reduce the impact of BSP. The flooding is simple to implement but it suffers not only from BSP and also incurs high energy consumption in the network.

The continuous mobility of the mobile nodes results in the varying network topologies of MANET that enables the mobile nodes to be either densely associated or sparsely associated. Accordingly, MANETs are classified as dense network and sparse network. In the dense network, nodes may run out of their energy quickly, which in turn cause partitioning of the network ensuring packet loss and link failure. The network partitioning can be inhibited by considering the energy of the nodes into account while forwarding packets from source to destination. In sparse networks, shared coverage is lower since very few nodes act as intermediate nodes. If these intermediate nodes are highly mobile, then link failure can occur, which decreases packet delivery. Hence, node mobility must be considered to improve it.

Inspired by addressing the issues of routing in MANET, we primarily bring the following contributions in this research study:

1) We provide a classification of routing schemes that is used to deal with issues of flooding. Along with, a review of broadcast schemes is found in the literature.
2) We introduce a method for the selection of next hop nodes in MANETs, which includes the following three aspects: number of packets received, neighborhood information of the nodes and residual energy of nodes. These three aspects have been considered as decision-making aspects in the selection of next hop nodes in MANETs.
3) We propose a novel energy-efficient counter-based broadcast (NEECBB) scheme for emergency communication in MANET. The algorithm reduces the energy consumption of mobile nodes, thereby increasing the lifetime of the network, which is of great importance in MANET.
4) We extend the NEECBB scheme to reflect the mobility of node into account to enrich the performance of the NEECBB.
5) We compare NEECBB and ENEECBB (extension of NEECBB) with HCBB (hybrid counter-based broadcast) and AODV (ad hoc on-demand distance vector), and the performance evaluation results show that the proposed algorithms perform better than other classical protocols in both energy consumption and packet delivery ratio (PDR) for long-term emergency communications.

The remainder of this chapter is organized as follows. Section 1.2 provides the general idea of related work about broadcast schemes. Section 1.3 proposes the NEECBB scheme and extension to NEECBB to enrich the performance of the system. Section 1.4 summarizes the performance evaluation through simulations. Section 1.5 concludes the chapter.

1.2 Background and related work

In the past, a lot of research has been contributed to deal with the issues of flooding. Together with there are major contributions on the way to address the link failures caused by node energy exhaustion. These schemes can be categorized as follows:

Neighbor knowledge-based schemes: The decision of broadcasting is taken based on local measures such as the number of neighbors and global measures such as the total number of nodes in the network. The basic idea is to reduce the broadcasts as the number of neighbors increases. Cartigny and Simplot [15] address that the forward probability is attuned to inverse proportion of the neighbor nodes and direct proportion to the efficiency parameter adjustable to topological parameters. Ejmaa et al. [16] described the average number of nodes that plays an important role in making broadcast decision replacing the total number of nodes of neighbor coverage-based probabilistic rebroadcast [17].

Distance-based schemes: The distance-based scheme can be categorized as the area-based schemes and the location-based schemes. The area-based schemes can further be categorized as density-based, received signal strength (RSS), Euclidean distance-based and hop count-based schemes. In the area-based schemes, the relative distance between the two nodes is used as the metric to make broadcast decision making. The density-based schemes [18] make use of distribution of neighbors within nodes transmission range to measure the relative distance between the two nodes for making the broadcasting decision. The constant distribution of neighbors is not the valid measure for making the broadcasting decision. The RSS-based schemes [19–21] use RSS as the metric to measure the distance between the two nodes, which is used as a decision parameter for making broadcast decision making. The Euclidean distance-based schemes [19, 21] make use of positioning system like a GPS to measure the distance between the two nodes, which decides the forward probability. In the hop count-based schemes [22], the number of hops is used as a distance metric to make a broadcasting decision. On the contrary, in the location-based schemes, position information of the nodes is collected using the location service. The regional GOSSIP [23] aims at inhibiting the number of retransmissions by permitting some nodes in the specified areas connecting the source and the end nodes to retransmit the incoming messages.

Counter-based scheme: The count of duplicate packets acknowledged at the node is used as a parameter for making the broadcasting decision. These schemes rely on the threshold in making broadcast decisions. In fixed counter-based broadcasting, a smaller threshold will cause broadcast saving and avoids the collision, thus minimizing the storm effect. In the sparse network, the nodes are dispersed far off and hence there remains less shared coverage; therefore, some nodes won't get broadcast packets except if the threshold value is high to achieve reachability. In the dense network, the nodes are dispersed nearby to incur redundant transmissions; hence, the threshold value is set low to achieve broadcast saving. There

exists a trade-off between broadcast savings and reachability [14]. This leads to dynamic adjustment of a threshold based on the network [24, 25]. These schemes dynamically assign the counter threshold based on the information collected from the nodes neighborhood in order to achieve reachability and broadcast savings.

Speed-based schemes: These schemes use the speed of nodes as the measure for broadcast decision making. In the network, if the mobility of nodes is high then it causes the link breakages which would affect the network lifetime. Hence, the idea is to eliminate many redundant broadcasts by the selection of low speed nodes as forwarder to rebroadcast the packets to discover a more stable path [26–29].

Energy-based schemes: In MANETs, mobile nodes are typically battery powered. As each mobile node in MANET is responsible for routing packets, battery energy should be efficiently utilized to avoid early power failure of the mobile nodes. Therefore, many research works have been carried out on the energy-efficient routing in MANETs, thereby aiming to surpass the issues incurred by the finite power capacity of the battery of the nodes and thus extending the lifetime of nodes and networks. In this chapter, the energy-based routing protocols are reviewed based on the energy metric used for investigating the energy-efficient routing protocols. As discussed in [30], energy-based measures used by these classical energy-based routing protocols can be categorized into three categories: transmission power, remaining energy capacity and combined energy measure. The major energy-based schemes discussed in this chapter are outlined in Table 1.1.

The schemes in [30, 31] are focused to minimize energy consumption of the network by reducing the total transmission power. They proposed the minimum total transmission power routing (MTPR) scheme, which chooses a route with the lowest transmission power of the route by implementing the modified version of Dijkstra's shortest path algorithm. Moreover, transmission power depends on the distance between the nodes, and MTPR is likely to choose routes with further hops that bring on the rise in the number of nodes and end-to-end delay of the routing path. Despite the achievement of minimum energy consumption per packet, MTPR could cause node exhaustion if the same set of nodes works on multiple paths. The nodes' energy exhaustion can disturb communication and even cause partitioning of network [32]. Hence, in the same study, the authors proposed the minimum battery cost routing (MBCR) scheme, which selects a route with the maximum remaining energy capacity. This scheme aims at balancing the remaining energy capacity over the entire network. However, the MBCR scheme does not guarantee the minimum energy cost path. Moreover, MBCR might select a route containing nodes with minimum remaining battery capacity. Therefore, to evade the route with nodes possessing minimum remaining battery capacity among all the nodes in all possible routes, the battery capacity of each node is considered to construct the route. Consequently, the authors proposed the improved MBCR scheme known as min–max battery cost routing (MMBCR) scheme, which always selects the route with the maximum bottleneck remaining battery capacity. However, the MMBCR

Table 1.1: Summary of major energy-based schemes in MANET.

S. no.	Routing scheme	Underlying protocol	Classical metrics	Energy metrics	Objective	Drawback
1	MTPR [30, 31]	AODV	Hop count	Total transmission power	Minimize energy consumption	– Tend to increase in end-to-end delay – Might lead to node exhaustion
2	MBCR [30, 31]	AODV	Hop count	Remaining energy capacity	Balance the remaining energy capacity over the entire network	– Does not guarantee the minimum energy cost path
3	MMBCR [30, 31]	AODV	Hop count	Bottleneck remaining energy capacity	Balance the remaining energy capacity over the entire network	– Does not promise minimum total transmission energy consumption per packet over a selected route
4	CMMBCR [30–32]	AODV	Hop count	Total transmission power and remaining energy capacity	Minimum energy consumption and balance remaining energy capacity over the network	– Difficult to find a balance between minimum energy consumption and fair remaining energy over the network
5	ESAODV [33]	AODV	Neighbor knowledge information	Remaining energy capacity	Balance energy consumption among all the nodes over the network	– Does not promise significant route discovery under moderate load networks

6	EEAODR [34]	AODV	Hop count and distance between the nodes.	Remaining energy capacity	Balance remaining energy capacity over the network	–	Does not work well in the network with all nodes having equal energy levels
7	ALMEL [35]	AODV	Neighbor knowledge information	Remaining energy capacity	Employ a maximum energy route and maintain backup route	–	Does not perform well in sparse networks
8	PEER [36]	AODV	Neighbor knowledge information	Total transmission power	Minimize energy consumption	–	Lead to significant routing overhead

scheme still does not promise minimum total transmission energy consumption per packet over a selected route. To achieve minimum energy consumption and fair remaining energy over the network, the authors proposed the conditional max–min battery capacity (i.e., above a threshold), then, they selected a route with minimum total transmission power from all possible discovered routes. Minimizing the total power required to transmit the packets for each connection leads to a significant reduction in the relaying load for most nodes and the extension of the lifetime of nodes. Moreover, CMMBCR avoids the routes with all the nodes possessing least remaining battery capacity to enlarge lifetime capacity routing (CMMBCR, conditional max–min battery capacity routing) scheme. The CMMBCR combines the MTPR and the MMBCR to achieve the goals. The CMMBCR scheme first discovers routes with all the nodes possessing sufficient remaining battery of these nodes.

Almost in most of the classical routing algorithms, the number of nodes is used as a metric to make broadcast decision making during route discovery, though this is not significant in ad hoc networks as it has other parameters to include in the optimized route discovery. Aside from the classical energy-based routing protocols, an energy-saving ad hoc on-demand distance vector (ESAODV) in [33] is proposed for routing in MANETs, which found a new parameter as energy comparison threshold induced from cumulative sum of remaining energy information of neighboring nodes and allows each intermediate nodes to broadcast route request packets if its remaining energy is larger than the energy comparison threshold. However, ESAODV does not promise significant route discovery under light load networks.

Dhurandher et al. [34] explored the energy-efficient ad hoc on-demand routing (EEAODR) algorithm, which aim at balancing the energy capacity of nodes over the network. An EEAODR makes use of remaining battery capacity, packet size and the distance between the nodes as routing metric and decides an optimized path, among all the discovered paths for efficient transmission in the network.

The alternate link maximum energy level (ALMEL) [35] algorithm chooses a maximum energy path for route selection to increase the network lifetime. During route selection, the nodes with the least residual energy are inhibited from broadcasting the packets. It allows intermediate nodes to update energy information in the route request packet. If the new path is evolved with better-accumulated energy sum, the destination node will insert newly evolved information into its route table. If there is a broken path, the source reinitiates route discovery and chooses an alternative path from the routing table.

The progressive energy-efficient routing (PEER) protocol [36] primarily focuses on the quick searching of route closer to the minimum energy route during the route discovery phase, which may lead to high end-to-end energy consumption than that of the minimum energy route. Ultimately, PEER includes a route maintenance phase to adjust the route to the energy-efficient route in view of further changes in topology and channel quickly.

These schemes are introduced in the literature to offer an optimized solution to broadcasting and to extend networks lifetime by utilizing the energy consumption of the network.

1.3 Novel energy-efficient counter-based scheme

The major existing schemes uses hop count, distance and neighbor knowledge information as the classical routing metrics and remaining energy as energy metric to achieve minimum energy. The NEECBB aims at minimizing energy consumption of network by the use of packet counter, neighbor knowledge information and remaining energy metric. In network, there exist some nodes that hold less energy and some that hold high energy. In dense network, nodes may run out causing link failure. Therefore, NEECBB favors the nodes with more remaining energy for broadcast process.

The different phases of NEECBB scheme are highlighted as follows:

A. Initialization phase
B. Computation phase
C. Characterization phase
D. Broadcast decision-making phase

Initialization phase: Upon receiving a packet at node (n), each node exchanges HELLO packets with each neighbor nodes to get one-hop neighboring nodes $N(\text{nbg})$. It does not immediately broadcast the packet to its neighbors; instead, it waits by initializing the timer to random delay. Next, to keep track of duplicate packets, it initializes a packet counter (c). Subsequently, sets up the initial energy $E(\text{Init})$ of each node in the network and the energy threshold ($E(\text{Th})$) before broadcast starts.

Computation phase: At the start, it computes the average neighboring nodes $N(\text{avg})$ at a node (n) in the network of an area, $A(M)$ and the total number of nodes (N) with transmission radius (R) using the following equation:

$$N(\text{avg}) = \frac{N \times \pi \times R^2}{A(M)} \tag{1.1}$$

Afterward, it computes the remaining energy $E(\text{Rem})$ as the difference of the initial energy of node $E(\text{Init})$ and the current energy of the mobile node $E(N)$.

Characterization phase: This phase evolves the two broadcast decision-making parameters, namely, neighborhood density $N(d)$ and the energy efficiency $N(e)$ of the mobile node. Initially, the algorithm characterizes a mobile node as sparse if the number of neighboring nodes $N(\text{nbg})$ is less than the average number of nodes $N(\text{avg})$ in the network, and characterizes the mobile node as dense otherwise. Afterward, it determines the energy efficiency $N(e)$ of the mobile node. The algorithm characterizes

a mobile node as strong if the energy of mobile node $E(N)$ exceeds the energy threshold $E(\text{Th})$ and as weak otherwise.

Broadcast decision-making phase: In this phase, NEECBB incorporates prior articulation of chances for the broadcast process before finding the optimal route. If a node evolves as a strong dense node, then the high dense threshold value is assigned to counter threshold to get more chances for broadcasting. On the contrary, if a node evolves as a strong–weak node, then counter threshold is set to low dense threshold value to get less chance for broadcasting. It works similarly for the sparse node and assigns high sparse threshold value and low sparse threshold value for a strong sparse node and weak sparse node, respectively, to decide chances for the broadcast process. Finally, the packet counter is compared with the rebroadcast threshold in order to find an optimal path.

1.3.1 NEECBB: the proposed protocol

This section explains the pseudocode of NEECBB protocol in detail in Algorithm 1.1. The NEECBB protocol reduces the energy consumption of mobile nodes, thereby increasing the performance of the network, which is of great importance in MANET.

1.3.2 Extension of NEECBB

Here, we extend the proposed NEECBB to include mobility of the mobile nodes to make more accurate decisions during route discovery. It considers the three main decision parameters that broadcast decision making: the neighborhood density $N(d)$, stability $N(s)$ and energy efficiency $N(e)$ in order to address the issues of MANET. These parameters are weighted to reflect their relative importance in the decision-making process. In this scheme, each time a node receives a broadcast packet it does not broadcast the packet immediately. It waits for random assessment time and initializes the packet counter to reduce the storm effect. Then it starts characterization of the network, which takes place in three different levels and forms the basis for incorporation of the preferences of the broadcast process. The first level broadly classifies the network as sparse or dense based on neighborhood density (d). If it classifies network as dense then n is set to 1, otherwise 0. The second level is used to decide preferences based on energy-efficient routes that use energy (e) of the mobile nodes. The third level decides preferences to form stable routes that use speed (e) of the mobile nodes. The weights of these parameters vary with neighborhood density. The ENEECBB constructs a rebroadcast threshold function to aggregate the multiple decision parameters into a single parameter, which decides the preferences of the broadcast process. The rebroadcast threshold function (f) is defined as follows:

Algorithm 1.1: Pseudocode of NEECBB protocol.

1. **Initialization :**
2. N = Number of Nodes
3. R = 250 m
4. A(M) = 1000 × 1000
5. E(Init) = 100 Joules
6. Initialize(C)
7. Call SendHello()
8. **Event:** On reception of packet at node (n_i)
9. Update(C)
10. Finds N(nbg) ← neighbour_list( )
11. Finds N(avg) = $\frac{N \times \pi \times R^2}{A(M)}$
12. Finds E(N) ← Energy( )
13. If N(nbg) > N(avg) then N(d) = Dense
14. Else N(d) = Sparse
15. End
16. If E(N) > E(Th) then N(e) = Strong
17. Else N(e) = Weak
18. End
19. If N(d) = Dense && N(e) = Strong then C(Th) = High_Dense
20. Else if N(d) = Dense && N(e) = Weak then C(Th) = Low_Dense
21. Else if N(d) = Sparse && N(e) = Strong then C(Th) = High_Sparse
22. Else if N(d) = Sparse && N(e) = Weak then C(Th) = Low_Sparse
23. End
24. If C < C(Th) then Broadcast (n_i)
25. Else
26. Drop (n_i)
27. End.
28. Exit.

$$f = c1.N(d) + c2.N(s) + c3.N(e) \tag{1.2}$$

$$\text{such that } N(d) = 0 \text{ or } 1 \& N(s), N(e) \propto N(d)$$

where $c1$,$c2$ and $c3$ are the performance values of respective decision parameters. Finally, if the packet counter does not reach the rebroadcast threshold, then the packet is transmitted; otherwise, the packet is dropped. The flow diagram of ENEECBB protocol is described in detail as shown in Figure 1.1.

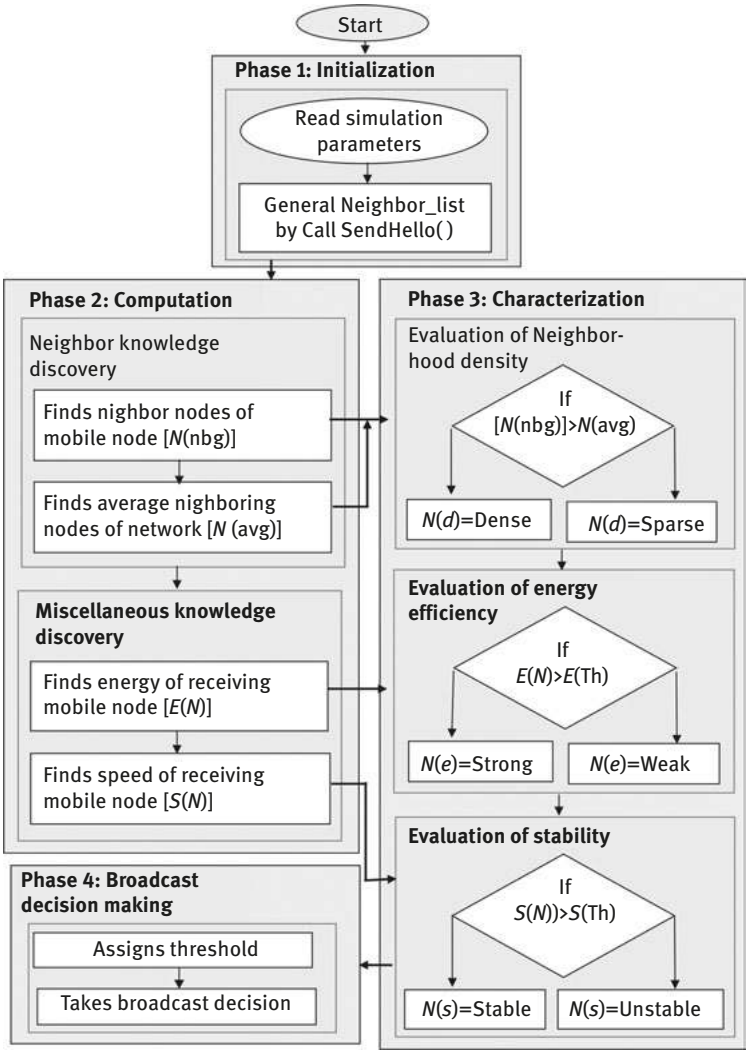


Figure 1.1: Flow diagram of ENEECBB protocol.

1.4 Performance evaluation

This section describes comparative protocols, simulation setup and performance measures used for evaluation of the proposed protocols.

1.4.1 Comparative protocols

In order to evaluate the effectiveness of the proposed scheme, the NEECBB and extended NEECBB are compared with the standard AODV protocol [37] and the well-known HCBB scheme [38].

AODV protocol

AODV is an on-demand distance vector routing protocol used for communication establishment among the nodes with no paths. AODV uses flooding as a basic mechanism for route discovery. It uses neighborhood information in order to find the route from source to end node. This neighborhood processing in MANET leads to BSP. The purpose of the proposed schemes is to reduce the impact of BSP; hence, AODV is considered as a good candidate for comparison with NEECBB and ENEECBB.

HCBB protocol

The HCBB is the hybrid scheme of the counter-based and neighbor knowledge-based schemes, which dynamically allocate the counter threshold dependent on the neighborhood information. HCBB provides broadcast savings achieving guaranteed transmission. Some major contributions attained by HCBB on the way to address MANET issues are as follows:

1. HCBB provides an efficient route discovery technique through the neighborhood propagation, which involves reduction in the redundant broadcasts.
2. Broadcasts are constrained on the basis of local measures such as the degree of the node (number of neighbors) and global measures such as the average number of nodes in the network.

1.4.2 Simulation setup

The performance of the proposed protocols for MANET is evaluated in network simulator (ns-2). The simulation parameters used for the evaluation of proposed protocols are listed in Table 1.2. The constant transmission range of the network is 250 m. The MAC layer scheme follows the IEEE 802.11 MAC specification. Each mobile node in MANET follows the random waypoint model to decide the movement pattern of them. The two-ray ground reflection model used for experimenting the routing protocols performs propagation to consider both the direct path and a ground reflection path. The omnidirectional antenna is used to configure the transceiver of MANET. The size of the network has been taken as 1,000 × 1,000. The simulation experiment runs for 225 ms over the varied network densities (50, 75, 100, 125).

Table 1.2: Simulation parameters.

	Parameter	Value
1.	Network area	1,000 × 1,000
2.	Transmission range	250 m
3.	Simulation time	225 ms
4.	Number of nodes	50, 75, 100, 125
5.	Traffic pattern	CBR(UDP)
6.	Receiving power	1.0
7.	Transmission power	2.0
8.	Routing protocol	AODV, HCBB, NEECBB, ENEECBB
9.	MAC protocol	IEEE 802.11
10.	Mobility model	Random waypoint mobility model
11.	Propagation model	Two-ray ground
12.	Antenna	Omnidirectional

1.4.3 Performance measures

The following measures are evaluated to measure the effectiveness of NEECBB and ENEECBB over AODV and HCBB. The total consumed energy, average consumed energy, delay, packet dropping, PDR and throughput obtained through simulation over varying network densities of 50, 75, 100, 125 for our proposed schemes, HCBB and AODV, are tabulated in Table 1.3.

- Total consumed energy: This defines the difference between the current and initial energies of all nodes during the simulation. This measure accounts for energy spent in transmission and reception of the packets. The average consumed energy provides accurate information about the energy consumed by the nodes involved in packet transmissions and receptions.
- Delay: This represents the total time required by a packet to move from the source to the destination. The link failure in networks incurs delay in networks as more time spent on route maintenance of the network.
- Packet dropping: The dropping of data packets occurs if the data packets traveling through network fail to reach the destination. The packets get lost if the network is congested. The reduction in retransmission has a substantial impact on the packet drops in the network.
- PDR: This represents the number of data packets that are successfully delivered to the destination. This measure is computed as the ratio of the number of received data packets by each destination to the number of data packets sent from each source.
- Throughput: This defines the number of bytes arrived at the destination over a period of time. The higher the throughput value means higher the performance of the network.

Table 1.3: Readings obtained through simulations over varied network densities of 50, 75, 100, 125.

S. no.	Performance measures	Schemes	Total number of nodes			
			50	75	100	125
1.	Total consumed energy (J)	AODV	1,610.6	2,395.4	4,046.54	5,853.61
		HCBB	1,287.84	1,692.38	3,287.93	3,857.49
		NEECBB	1,115.94	1,722.39	3,192.64	3,474.46
		ENEECBB	1,610.6	2,395.4	4,046.54	5,853.61
2.	Average consumed energy (J)	AODV	32.2119	31.9387	40.4654	46.8289
		HCBB	25.7567	22.5651	32.8793	30.8599
		NEECBB	22.3188	22.9652	31.9264	27.7957
		ENEECBB	26.1902	20.6683	30.5701	28.9164
3.	Delay (s)	AODV	0.280583	0.0784849	0.580178	0.322705
		HCBB	0.455561	0.0869934	0.51905	0.365155
		NEECBB	0.186596	0.0467458	0.273937	0.32558
		ENEECBB	0.296194	0.0600749	0.406911	0.416007
4.	Packet droppings (packets)	AODV	580	111	866	466
		HCBB	183	4	110	70
		NEECBB	22	0	37	13
		ENEECBB	15	3	30	37
5.	Packet delivery ratio (%)	AODV	78.0967	95.7811	63.7657	82.5468
		HCBB	94.4579	99.8789	96.6687	97.8801
		NEECBB	99.3337	100	98.8795	99.6063
		ENEECBB	99.5457	99.9091	99.0915	98.8795
6.	Throughput (bps)	AODV	99,264	132,666	87,085	110,879
		HCBB	138,622	146,578	141,867	143,644
		NEECBB	145,778	146,756	145,111	146,178
		ENEECBB	146,089	146,622	145,422	145,111

1.4.4 Simulation results

This section describes the simulation campaign to exploit the performance of the proposed protocol against HCBB and AODV. Figures 1.2 and 1.3 show an effect of total energy and the average energy consumed by the mobile nodes over varied node densities, respectively. It shows that the energy consumption increases from low-density network to high-density network for all the protocols considered in the simulation scenario.

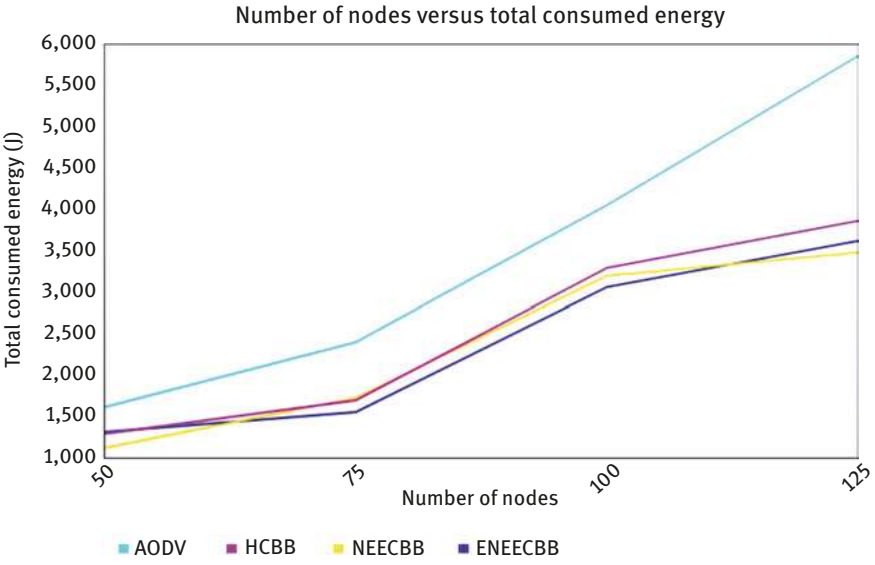


Figure 1.2: Total consumed energy over varied node densities.

The NEECBB schemes reduced the total energy consumption by more than 31% compared to the AODV routing protocol and ENEECBB maintains approximately the same consumed energy. The proposed schemes performed better than HCBB by reduction of the total energy consumption by approximate 6% more. As shown in Figure 1.3, the ENEECBB performed better than NEECBB in the low-density network. Certainly, both the proposed schemes outperformed best as both schemes aimed at inhibiting some nodes from broadcasting to cause fewer packets and less energy consumed by the selected nodes crossing the network.

Figure 1.4 presents the graph of delay over varied network densities. The NEECBB reduced more than 34% of the delay, and ENEECBB more than 6%, compared to the AODV routing protocol. Similarly, NEECBB and ENEECBB, when compared with HCBB, reduced more than 41% and 17% of the delay, respectively. While

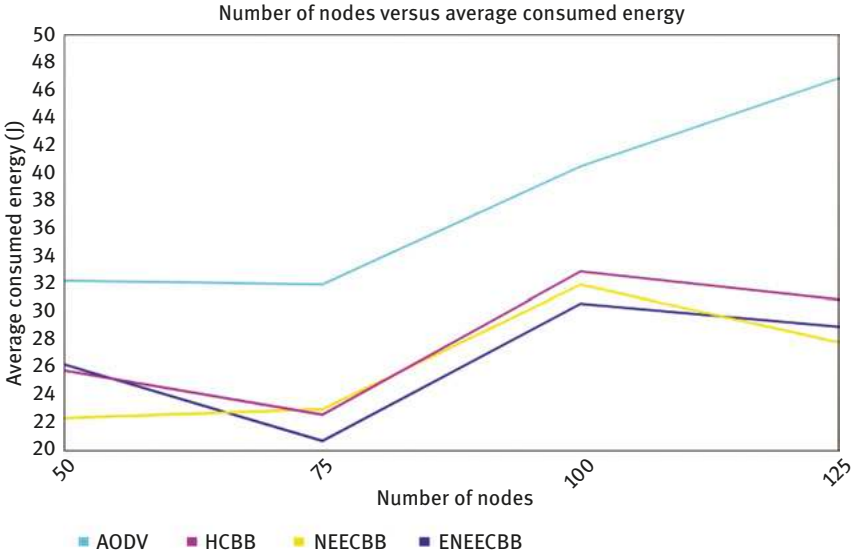


Figure 1.3: Average consumed energy over varied node densities.

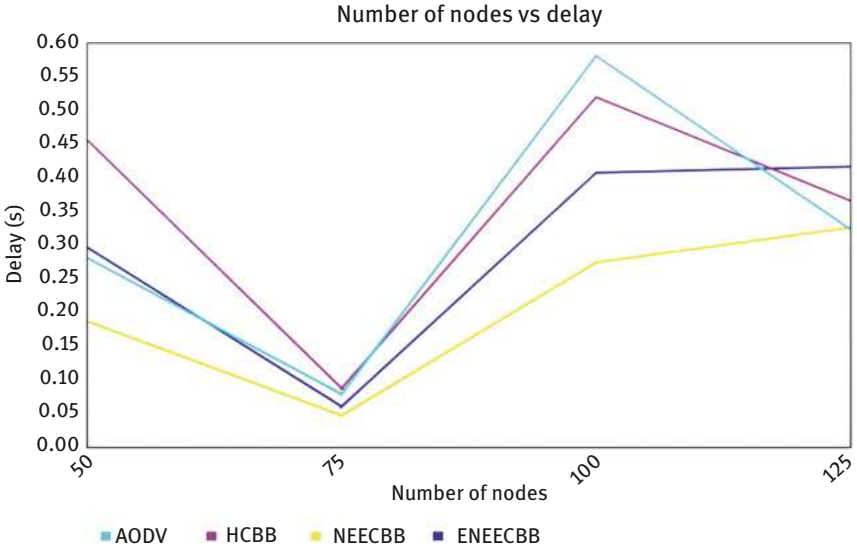


Figure 1.4: Delay over varied node densities.

the number of retransmissions is reduced in our proposed schemes, the overall routing process will speed up. Indeed, the result statistics reveals that the delay is increased in ENEECBB by an additional 41% than NEECBB. The ENEECBB does not perform well due to increased overhead of finding optimal stable network. Figure 1.5

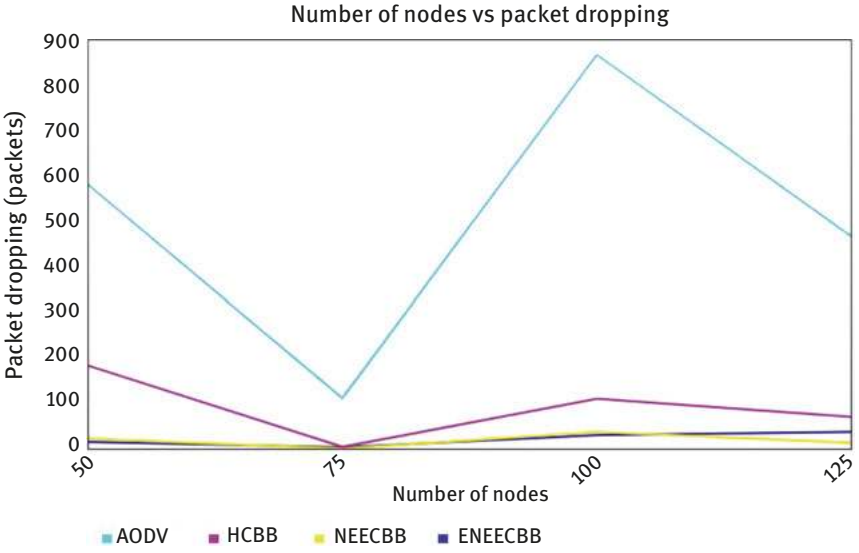


Figure 1.5: Packet droppings over varied node densities.

shows packet droppings over varied network densities. The reduced number of nodes for broadcasting of packets have significant impact on the packet droppings in the network. The NEECBB reduced more than 81% of the delay, and ENEECBB more than 47%, compared to the HCBB scheme. The proposed schemes outperform AODV by the reduction of packet dropping by more than 90%. Basically, the main objective of the proposed schemes is to adapt to dynamic changes of the mobile nodes; however, they achieve to uphold the PDR compared to HCBB and achieve significant enhancement compared to AODV. The greater is the PDR the better is the performance of the proposed scheme. Figure 1.6 illustrates a graph of PDR over varied network densities. As shown in Figure 1.6, the PDR was changing over varied network densities, more specifically in varied network configurations for the AODV protocol. However, for the proposed schemes, the PDR was constant due to the adaptation to network changes and reduction to packet loss. The proposed schemes caused considerable incremental growth of 24% in the PDR compared with the AODV routing protocol and least incremental growth of 2% in PDR compared with the HCBB scheme.

Figure 1.7 shows the impact of the throughput over varied network densities. Delay is the component that affects the throughput of the network. The low-latency network incurs small delays and achieves high throughput. The high-latency network incurs high delays and achieves low throughput However, as shown in Figure 1.7, throughput was changing over varied network densities in AODV protocol. For proposed schemes, the inverse was true because of choice of the more stable network for the broadcasting process. The proposed schemes raised the throughput by more than 35% compared to the AODV routing protocol and caused

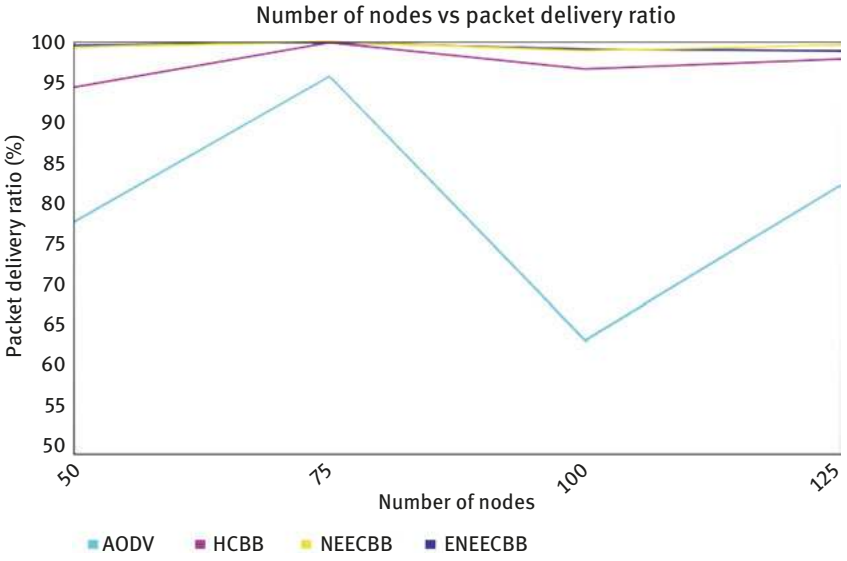


Figure 1.6: Packet delivery ratio over varied node densities.

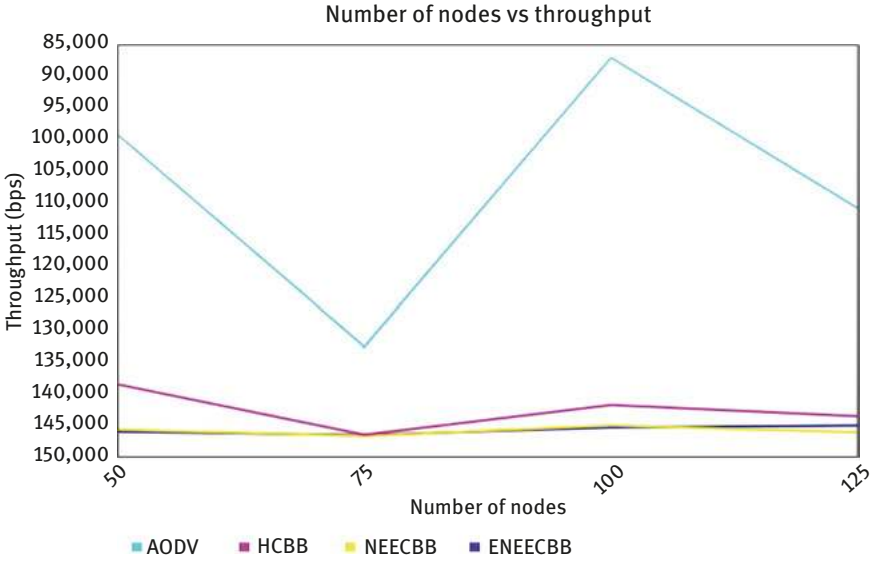


Figure 1.7: Throughput over varied node densities.

a raise of 2% more of the throughput when compared with HCBB protocol. The proposed schemes performed better than HCBB by reduction of the total energy consumption by approximate 6% more.

1.5 Conclusion

This study addresses the issues of MANETs. To address this, we proposed an NEECBB scheme for emergency communication via MANET. The NEECBB aimed at condensing the energy consumption of mobile nodes, thereby increasing the lifetime of the network. We introduced a method for the selection of next hop nodes in MANETs, which includes the following three aspects: the number of packets received, neighborhood information of the nodes and the residual energy of nodes. We extended the NEECBB scheme to reflect the mobility of the node into account to enhance the performance of the NEEECBB. Both the proposed schemes outperform over the HCBB and standard AODV protocol. The NEECBB schemes reduced the total energy consumption by more than 31% compared to the AODV routing protocol, and ENEECBB maintains approximately the same consumed energy. The proposed schemes performed better than HCBB by reduction of the total energy consumption by approximately 6% more. The proposed schemes not only addressed energy consumption of the network rather than achieved low latency and packet droppings by enhancing the packet delivery and throughput of the network. The results of simulation revealed that proposed schemes decrease the packet loss, the latency time, and achieves lower energy consumption, better packet delivery and throughput in the network.

Nomenclature

ALMEL	Alternate link maximum energy level
AODV	Ad hoc on-demand distance vector
BSP	Broadcast storm problem
CMMBCR	Conditional max–min battery capacity routing
EEAODR	Energy-efficient ad hoc on-demand routing
ENEECBB	Extended novel energy-efficient counter-based broadcast
ESAODV	Energy-saving ad hoc on-demand distance vector
FANET	Flying ad hoc network
HCBB	Hybrid counter-based broadcast
MAC	Medium access control
MANET	Mobile ad hoc networks
MBCR	Minimum battery cost routing
MMBCR	Min–max battery cost routing
MTPR	Minimum total transmission power routing
NEECBB	Novel energy-efficient counter-based broadcast
OLSR	Optimized link state routing
PEER	Progressive energy-efficient routing
RREQ	Route request
RSS	Received signal strength
VANET	Vehicular ad hoc network
WSN	Wireless sensor network

References

[1] Frodigh, M., Johansson, P., and Larsson, P. Wireless ad-hoc networking: the art of networking without a network, Ericsson Review, 4, 2000, pp. 248–263.

[2] IETF Working Group: Mobile Ad-hoc Networks (MANET). http://www.ietf.org/html.charters/manet-charter.html.

[3] Fujiwara, T., and Watanabe, T. An ad-hoc networking scheme in hybrid networks for emergency communications, Ad- hoc Networks, 3(5), 2005, pp. 607–620. doi:10.1016/j.adhoc.2004.08.007.

[4] Binh, H. T. T., Hanh, N. T., and Dey, N. Improved cuckoo search and chaotic flower pollination optimization algorithm for maximizing area coverage in wireless sensor networks, Neural computing and applications, 30(7), 2018, pp. 2305–2317.

[5] Divya, Dinesh, and Deshmukh, M. Challenges in Vehicle Ad Hoc Network (VANET), International Journal of Engineering Technology, Management and Applied Sciences, 2(7), 2014, pp. 76–88.

[6] Ilker, Bekmezci, Ozgur Koray, Sahingoz, and Samil, Temel. Flying Ad-Hoc Networks (FANETs): A survey, Ad Hoc Networks, ELSEVIER 11, 2013, pp. 1254–1270.

[7] Nair Swatichandra, Chandrasekharan,and Deshmukh, M. Advanced Location Based Efficient Routing in MANETs, Journal of Emerging Technologies and Innovative Research, 4(08), 2017, pp. 144–152.

[8] Shabana Anjum1, Shaik, Noori, Rafidah Md., and Hossein Anisi1, Mohammad. Review on MANET based communication for search and rescue operations. Wireless Personal Communications, Springer, 94(1), 2017, pp. 31–52.

[9] Jabbar, Waheb A., Ismail, Mahamod, Nordin, Rosdiadee, and Arif, Suki. Power-efficient routing schemes for MANETs: a survey and open issues, Wireless Networks, 23(6), 2017, pp. 1917–1952.

[10] Chowdhuri Swati, Chaudhuri Sheli Sinha, Banerjee P., Dey, N., Mandal A., and Santhil V. Secure minimum loss route selection of MIMO-based MANET in combined (indoor, outdoor, and forest) terrain, International Journal Advanced Intelligence Paradigms. 11(3–4), 2016, pp. 1–26.

[11] Babar S., Prasad N. R., and Prasad R. Identity management framework towards Internet of things (IoT): Roadmap and key challenges, In International Conference on Network Security and Applications. Springer, Berlin, Heidelberg. Part of the Communications in Computer and Information Science book series (CCIS), 89, 2010, pp. 430–439.

[12] Anggorojati, B., Prasad N. R., and Prasad R. Identity authentication and capability based access control for the internet of things. Journal of Cyber Security and Mobility, 1(4), 2013, pp. 309–348.

[13] Tarique, M., Tepe, K. E., Adibi, S., and Erfani, S. Survey of multipath routing protocols for mobile ad-hoc networks, Journal of Network and Computer Applications, 32(6), 2009, pp. 1125–1143.

[14] Ni, Sze-Yao, Tseng, Yu-Chee, Chen, Yuh-Shyan, and Sheu, Jang-Ping. The broadcast storm problem in a mobile ad-hoc network, Proceedings of 5th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom), 1999, pp. 151–162.

[15] Cartigny, J., and Simplot, D. Border node retransmission based probabilistic broadcast protocols in ad-hoc networks, In: Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS '03), 2003.

[16] Ejmaa, Ali Mohamed E., Subramaniam, Shamala, Zukarnain, Zuriati Ahmad, and Hanapi, Zurina Mohd. Neighbour-based dynamic connectivity factor routing protocol for mobile ad-hoc network, Journal of IEEE Access, 4, 2016, pp.8053–8064.

[17] Zhang, X.M., Wang, E.B., Xia, J. J., and Sung, D. K.. A neighbour coverage-based probabilistic rebroadcast for reducing routing overhead in mobile ad-hoc networks, IEEE Transactions on Mobile Computing, 12(3), 2013, pp. 424–433.
[18] Scott, D. J., and Yasinac, A. Dynamic probabilistic retransmission in ad-hoc networks, In: Proceeding of the International Conference on Wireless Networks (ICWN04), 2004.
[19] Ling, H., Mossé, D., and Znati, T. Coverage-based probabilistic forwarding in ad-hoc routing, In: Proceedings of 14th International Conference on Computer Communications and Networks (ICCCN 2005), pp. 13–18.
[20] Wisitpongphan, N., and Tonguz, O. K. Scalable broadcast strategies for ad-hoc routing protocols, In: 1st International Symposium on Wireless Pervasive Computing, 2006. pp. 1–6.
[21] Wisitpongphan, N., Tonguz, O. K., Parikh, J. S., Mudalige, P., Bai, F., and Sadekar V. Broadcast storm mitigation techniques in vehicular ad-hoc networks, IEEE Wireless Communications, 14(6), 2007, pp.84–94.
[22] Merkel, S., Mostaghim, S., and Schmeck, H. Hop count based distance estimation in mobile ad-hoc networks challenges and consequences, Ad-hoc Networks, 15, 2014, pp.39–52.
[23] Li, X., Moaveninejad, K., and Frieder, O. Regional gossip routing for wireless ad-hoc networks, Mobile Networks and Applications, 10, 2005. pp. 61–77.
[24] Aminu Mohammed Mohamed Ould-Khaoua, Lewis Mackenzie. An adjusted counter based broadcast scheme for mobile ad-hoc networks, 10th International Conference on Computer Modeling and Simulation, Cambridge, UK, 2008.
[25] Muneer Bani Yassein, Ahmed Y. Al-Dubai. Inspired counter based broadcasting for dynamic source routing in mobile networks, IEEE. International Conference on Computer and Information Technology, 2015.
[26] Khamayseh, Yaser, Darwish, Omar, and Wedian, Sana. MA-AODV mobility aware routing protocols for mobile ad-hoc networks, IEEE Transactions,23(4), 2009. pp. 25–29.
[27] Bani Yassein, Muneer, Asmahan Abu Al-hassan, and Zainab Abu Taye. Performance analysis of the effects of network density and network mobility on velocity based scheme in MANET. 7th International Conference on Systems, Signals and Devices (SSD), Amman, Jordan, 2010.
[28] Mustsfa Bani Khalaf, D, Al, Ahmed Y., and Abed, Mourad. New velocity aware probabilistic route discovery schemes for MANET. IEEE Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2012.
[29] Khamayseh, Yaser, Obiedat, Ghadeer, and Yassin, Munner Bani. Mobility and Load aware Routing protocol for ad-hoc networks, Journal of King Saud University – Computer and Information Sciences, 23(2), 2011, pp. 105–113.
[30] Toh, C. K., Maximum battery life routing to support ubiquitous mobile computing in wireless ad-hoc networks, IEEE Communications Magazine, 2001.
[31] Cao, L., Dahlberg, T., and Wang, Y. Performance evaluation of energy efficient ad-hoc routing protocols. In IEEE International on Performance, Computing, and Communications Conference, 2007. IPCCC 2007 pp. 306–313.
[32] Waheb A. Jabbar, Mahamod Ismail, Nordin, Rosdiadee, and Arif, Suki. Power-efficient routing schemes for MANETs: a survey and open issues. Wireless Networks, Springer, 23(6), 2016, pp. 1917–1952.
[33] Ren, Pinyi, Feng, Jia, Hu, Ping, and Cai, Jun, Energy saving ad-hoc on-demand distance vector routing for mobile ad-hoc networks, International Conference on Communications, IEEE, 2009.
[34] Dhurandher, S. K., Misra, S., Obaidat, M. S., Bansal, V., Singh, P. R., and Punia, V. EEAODR: An energy-efficient ad- hoc on-demand routing protocol for mobile ad-hoc networks, International Journal of Communication Systems, 22(7), 2009, pp. 789–817.

[35] Tie, T. H., Tan, C. E., and Lau, S. P. Alternate link maximum energy level ad-hoc distance vector scheme for energy efficient ad-hoc networks routing, In 2010 International Conference on Computer and Communication Engineering (ICCCE), 2010, pp. 1–6.

[36] Zhu, Jinhua and Wang, Xin,. Model and protocol for energy efficient routing over mobile ad-hoc networks, IEEE Transactions on Mobile Computing, 10(11), 2011, pp. 1546–1557.

[37] Perkins, C.E. and Royer, E. M., "Ad-hoc on-Demand Distance Vector (AODV) routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999, pp. 90–100.

[38] Nikumbh, P. J, and Deshmukh, M, "Improving performance of counter-based flooding in mobile ad-hoc networks", International Journal of Emerging Technologies & Applications in Engineering, Technology & Science, 3(1), 2010. pp. 763–768.

Sanjukta Bhattacharya, Ananjan Maiti, Samhita Das
and Shristee Ganguly

2 Partial face recognition using image fusion

Abstract: Several biometric partial face recognition researches have been performed by many scientists. In this chapter, a novel technique has been recommended, which acknowledges students face to speed up the attendance procedures in a classroom. Students' partial pictures have been used to prepare the image set, and preprocessed different partial faces to gray-level images. Initially, the technique like discrete wavelet transform has been used to obtain local features. Afterward, the effectiveness of the approach has been improved by employing image fusion with the averaging method. The fusion technique along with the correlation technique was executed to the contrast between the fused images, and the test images were selected from the entire image set. Results revealed practically 90% of the instances that were matched. The acceptance rate on an overall analysis has been found to prevail between 86.67% and 87.5%.

Keywords: Image fusion , 2D correlation , binning , partial face , Internet of things

2.1 Introduction

The conventional way of taking the presence of students is strenuous and also lengthy. The lecture normally prolongs it, upkeeping the student's attendance. This technique is ineffective, particularly if it is a lecture with a large number of students. It also triggers a great deal of disorder and hindrance when an examination is hosted. Furthermore, the attendance sheet is subjected to damage and also loss while being handed down between different students and teachers. In some cases, the lecturers have the tendency to call a couple of students' full name randomly, which is an unfair student assessment procedure either. Eventually, these attendance records are used by the lecturers to keep track of the students' attendance rates. This process could be comfortable and useful with a small number of students; however, dealing with the records of a large number of students often leads to human error.

Therefore, to prevent this mistake, computerized attendance recording system is offered to every student thus saving time, initiative and reduces disruptions. These particular systems might consist of the utilization of biometrics like fingermark, eye acknowledgment, retinal search and articulate acceptance. These kinds of systems are conclusively established in the current years; nevertheless, this is actually unpleasant and expense required when it comes to implementation on

https://doi.org/10.1515/9783110628517-003

huge scale gets increased significantly. Biometric iris acknowledgment uses template acceptance methods based on high-resolution and a distortion-free image of the irises from the human eyes. Iris is an organ, whose structure remains steady all throughout life. Therefore, this functions as an incredibly great biometric when it comes to developing identification of an individual. Speech identification is an one more individual recognition system through computer software application as well as an equipment tool along with the capability to decipher the individual's speech. In the event of this, we observe that an individual's speech could be rapidly captured and also utilized when it comes to an unexpected for any type of electronic device. This possesses low accuracy. A health problem like a cold could alter an individual's speech, making complete recognition challenging or difficult. To conquer these kinds of problems, the biometric function such as face identification could be utilized, which includes the stages like image acquisition, feature extraction, face classification [1] and also eventually marking the attendance. Likewise, some of the significant advantages that face recognition modern technology companies provide are the time participation monitoring, which enables leaving out the amount of time theft among the employees and also the paid hours start from this particular minute until the same check-out process. It is essential when it comes to entrepreneurs to rely on their employees, however, to watch on all of them. Face recognition describes a part of computer science which can determine individuals' facial expressions inside digital images. Face recognition technology may start through looking for human eyes. It could then utilize a genetic algorithm to spot face areas consisting of eyebrows, the mouth, nose, nostrils and also the iris. This particular technology is being used more often in digital photography since a way to assist cameras autofocus on individuals' faces. This system complements a person's face immediately against a data source of photos to develop the identity. Face detecting systems could utilize algorithms to forecast age, sex and also various other elements to serve up appropriate advertisements, and the acknowledgment explains a biometric innovation which heads way beyond identifying when a human face exists. The suggested work primarily handles the students face recognition within the class. Often, this similar procedure works using a computer application that catches a digital picture of an individual's face via video frame and also compares it to images in a database of stored records. Nevertheless, when it comes to the front or full face acknowledgment algorithm, there is a drawback that students in a class need to arrive near the electronic camera and provide their attention to obtain correct outcomes. It is because the students in a class do not regularly sit appropriately. Often it fails when the students are not in their frontal face and remain in a side face, that is, either left sided or right sided, the camera fails to determine the image of those students. The relative angle of the target faces affects the recognition score exceptionally. So we need to enroll faces in the recognition software; typically, several positions are used. The more direct the image and the higher its resolution, the

higher the score of any resulting matches. Finally, the subject must be holding a neutral expression and managing these specifications helps reduce variation between any two images.

Inside this particular succeeding study, in Section 2.3 we have talked about current research in biometric face recognition as well as its restrictions. The partial face recognition framework consisting of many collective actions are discussed in Section 2.4. Here, we have highlighted sequential phases of work in brief. The outcome of identification of the faces of students was compared in Section 2.5 and confirms the value of image fusion technique concerning student face recognition. Lastly, in Section 2.6, we have wrapped up study with limitation and potential scope.

2.2 Related work

Liao et al. [2] suggested a method that possesses absolutely no demand of face positioning and also eyeball coordinates. The analysis of the face images starts with identifying the descriptor via Multi-Keypoint Descriptors (MKD). By doing this, any probe face image, alternative or partial, could be sparsely represented through a comprehensive dictionary of gallery descriptors. Here, Gabor ternary pattern (GTP) produces a distinct keypoint descriptor for robust and biased face recognition. These experimental outcomes are stated on four public domain face data sources under each of the open-set recognition and verification scenarios. They dealt with the issue of identifying a face from its partial image and suggested an alignment-free approach called Multi-Key point Descriptors-Sparse Representation-based Classification (MKD-SRC). Their approach stands for every face image with a set of keypoint descriptors and constructs a large dictionary from all the gallery descriptors. By doing this descriptor of a partial probe image could be sparsely stood for by the dictionary, and the identity of the probe could be presumed appropriately.

Smeets et al. [3] offered the meshSIFT algorithm and also its utilization of 3D face acknowledgment. This approach consists of the neighborhood procedure, and every salient factor is explained in a feature vector, including concatenated histograms of shape indices and also slant angles. Afterwards, the feature vectors of two 3D facial surface areas are dependably fit through contrasting the angles in a feature space. As a result, the algorithm is robust to expression variations, missing information as well as outliers. It also showed that the amount of matching meshSIFT features is a reliable measure for expression-invariant face acknowledgment. It reveals the recognition rate of 93.7% and 89.6% for standard data sources, specifically.

Ding et al. [4] operated on recorded face images inside difficult scenarios that typically include essential position variant, which significantly deteriorates the efficiency

of algorithms developed to identify frontal faces. Here, the approach is of a novel face recognition framework that is efficient in dealing with the full variety of position variants inside 90 degrees. Finally, face matching was carried out in patch level rather than the holistic level. Extensive and also methodical testing on multi-PIE, CMU-PIE http://www.cs.cmu.edu/afs/cs/project/PIE/MultiPie/Multi-Pie/Home.html (last access date: 07.06.2019) and also The Facial Recognition Technology (FERET) database revealed that the proposed technique regularly surpasses single task-based standards in addition to cutting-edge techniques for the posed problem. Patch Based Partial Representation (PBPR) could be used to face images in the arbitrary position, which is a considerable benefit over presenting methods.

Lei et al. [5] suggested 3D face recognition with the accessibility of just partial information and also single training sampling is an extremely challenging task. This study offered an effective 3D face recognition technique to deal with this challenge. It examines face along with a collection of regional keypoint-based multiple triangle statistics (KMTS) that is robust to partial face information, large facial expressions as well as position variants. The suggested method stands for a 3D confront with a collection of regional geometric descriptors called KMTS. The suggested descriptor allows robust 3D PFR with inconsistent data, barricades and data corruptions. Finally, a durable prior classification database on the suggested local descriptor was the need for resolving the single sample issue.

Best-Rowden et al. [6] constructed an analytical system regarding a pair of mugshot data sources, which are the most comprehensive facial aging data sources examined to this day concerning several topics. The longitudinal evaluation revealed that in spite of reducing initial scores, 99% of topics could still be identified in 0.01% fixed false accept rates. In future, they would attempt to monitor an accuracy along with a global threshold.

Lahasan et al. [7] suggested optimized symmetric partial facegraphs that were a memetic-based framework to determine faces that are prone to unfavorable circumstances. Those situations could be a facial feeling, occlusions and lighting changes. This study combined an enhanced harmony search algorithm and a sensible single particle optimizer to have the benefit of their global as well as regional search aptitudes. These features further functioned as the foundation so as to without effort design the partial facegraph.

Fu et al. [8] mentioned the effectiveness of the sparse representation classifier that might perform classification through assessing which class results in the minimal representation inaccuracy. For that reason, they had created virtual samples through making use of original training samples along with the aim of enhancing the variety of training samples. The respective representation scores utilized weighted score-level fusion of the virtual samples, and also the original training samples are merged with each other to acquire the finished classification outcomes with an accuracy of 76.61.

2.3 Methodology

Image fusion is a process that is used to gather maximum useful information from various images and converts the inclusion of all images into a single image (sometimes more than one image). This individual fused image is more accurate and contains all the useful information from different images [9]. The image fusion method is used for reducing the data amount as well as this method is also used for constructing much more appropriate images that are easily understandable by human beings as well as machines. Moreover, it can be said that image fusion process is capable enough to integrate multiple sources of image [10]. The resultant fused image contains fully spectral and spatial resolution features. Image fusion technique must fulfill two very basis requirements: (1) fused resultant image always have the capability to reverse each and every required information that is obtained from input source image; and (2) image fusion technique does not allow any incorrect or inaccurate diagnosis. There are three levels, where image fusion can occur. The levels are (1) pixel level, (2) feature level and (3) decision level. In case of pixel-level method the pixels of the source images are processed and preserve all the required image information. The pixel-level fusion is defined as low-level fusion. This is a very simple and common method that is done at the stage of image preprocessing [11]. This pixel-level image fusion can be divided into two groups: image point fusion and single-level fusion. In case of single-level fusion, a set of high category signals from different sensors that are consistent with the actual image are obtained to amalgamate, where in case of image point fusion each and every point that is obtained from different images are amalgamated directly. Feature [12]-level fusion is also known as medium-level image fusion that occurred at the feature extraction phase. In this fusion level, extracting image features and at the same time synthesizing the similar features from various images is the major task. The different types of features that are commonly extracted are angle, texture, similar lighting area, shape, profile, similar depth of focus area and others.

Decision level is defined as the highest level of fusion. All the useful information that are extracted from either feature-level image fusion or pixel-level image fusion are used to get best decision to successfully achieve the desired objective. Decision-level image fusion results are responsible to take any type of control and decision for the next stage.

Image fusion technique is categorized into three major divisions such as spatial domain fusion, transform domain fusion and statistical domain fusion. The spatial domain fusion technique handles with the pixel values of images directly. This technique is used to manipulate the image pixel value to successfully achieve the desired objective. There are different and most commonly used spatial domain fusion methods available such as Intensity-hue-saturation (IHS)-based methods, averaging, principle component analysis, Bovey transform and high-pass filtering method. In case of frequency domain technique, first conversion of an image into frequency domain

occurs with the help of Fourier transform. The necessary operations occur on Fourier transform of the particular image and after that to achieve the desired result inverse Fourier transform can be applied. There are also available commonly used transform domain fusion methods such as pyramid transform and wavelet transform [13]. Statistical domain fusion uses statistics to get the desired output. The statistical variables, for example, local correlation average, local correlation average with respect to variation and least squares are most frequently used. Drawbacks of image fusion such as dataset or operator dependency and color distortion can be solved through statistical domain fusion method. Some of the most common methods that fall under the category of statistical domain fusion are local mean and variance matching, local correlation modeling, local mean matching, regression variable substitution and others. Averaging fusion method is used to achieve the resultant final image where all the regions are focused. The average value is found out by applying the summation of all pixel values of every input images, which is divided by the total number of input images. This average value is used to give the corresponding resultant pixel images. The speed of this averaging fusion method is very fast. Averaging fusion method is defined as a simplest technique that is used to calculate the weighted average value from all the images that are taken as input and then the results are reflected on final fused image. The application of image fusion can be seen in various fields, where the image analysis is needed such as satellite image analysis, robotics, medical image analysis, remote sensing application, microscopic imaging and computer vision.

2.4 Proposed method

There are two types of environment in which face detection can take place: controlled and uncontrolled environments. In a controlled environment, there is a camera mounted on the wall and the subjects are required to come in front of the camera to get their face recognized. The subjects need to stand in front of the camera in a specific angle, such as their full frontal face gets captured by the camera. There are other requirements that need to be confirmed to, for example, the proximity of the subject to the camera and proper lighting. In the uncontrolled environment, on the other hand, there are no face-to-face interaction between the camera and the subjects. The subjects are not required to stand in front of the camera in any specific angle as such. In the proposed method, the uncontrolled environment has been used. At first, the input video has been taken where the individual movement has been captured. Then the captured video is divided into frames. Binning technique is deployed on the whole set of frames. In our method, the bin size is set as 10. The middle frame is selected as a key frame from each and every bin. The selection is done in an adaptive way. Image fusion operation is taken place on all the key frames. At the next phase, the correlation is computed with the help of the

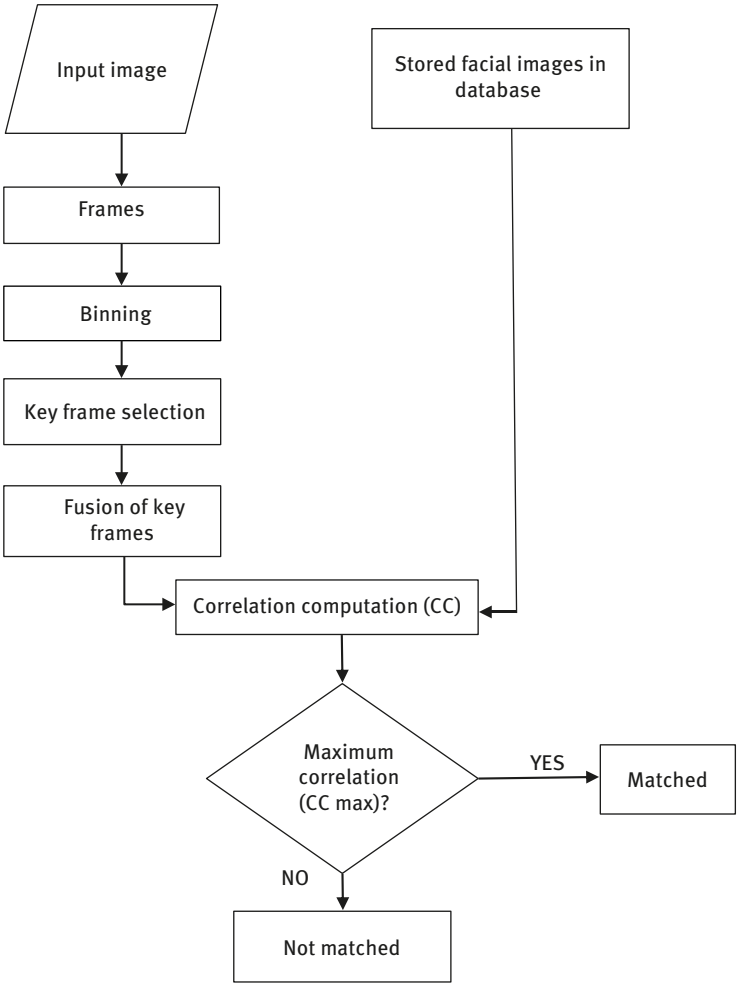


Figure 2.1: Proposed methodology.

fused key frame and the facial image gets stored in the database. The correlation values of each comparison are stored in a cell or array. Once all the comparisons are over, the image that has the highest correlation value is taken to be the matched image (Figure 2.1).

2.5 Experiments and results

In this proposed system, MATLAB R2013a software, 64-bit operating system, x64-based processor, Intel Core i3-4005U CPU @ 1.70 GHz has been used.

Figure 2.2: Database.

In the proposed method two database sets are used. The first database set that is shown in Figure 2.2 consists of 30 folders. Each folder consists of five images of an individual, so a total of 150 images are stored in the database. The images that are stored in the database are basically the frontal faces [14] as well as the partial faces of the individuals. The images are captured in an uniform lighting and same background environment. In the proposed method, the uncontrolled environment has been used. At first, the input video has been taken where the individual movement has been captured [15]. After that the captured video is divided into frames. Binning technique is deployed on the whole set of frames. In our method, the bin size is set as 10. The middle frame is selected as a key frame from each and every bin. The selection is done in an adaptive way. Image fusion operation is taken place on all the key frames. In this case, averaging method is used as an image fusion. At the next phase, the correlation is computed with the help of the fused key frame and the facial image is stored in the database. The correlation values of each comparison are stored in a cell or array. Once all the comparisons are done, the image that has the highest correlation value is taken to be the matched image. After performing the proposed method in the database 2, the acceptance rate is 86.67%.

Some of the accepted cases and some of the false cases are shown in Figures 2.3 and 2.4. Image fusion operation takes place on all key frames. In this case, averaging method is used as an image fusion.

At the next phase, the correlation is computed with the help of the fused key frame, and the facial image is stored in the database (Figure 2.5). The correlation

Figure 2.3: Accepted cases.

Figure 2.4: False cases.

Figure 2.5: Fused image.

values of each comparison are stored in a cell or array. After all the comparisons take place, the image that has the highest correlation value is taken to be the matched image. As the image area is quite large and the face position along with the facial expression varies for each image of an individual, the fused image gives a bit of a distorted image. This can be a reason for the low acceptance rate. That is, if the position of the face always remains constant, which is not the ideal case, the false acceptance rate can be reduced further. In the initial stage, the fusion of eye region of each image in the folder and then the correlation with the fused eye image has been done. The experimental result of eye region shows the lower acceptance rate than the current experiment with full face fusion. This is due to the fact that the fusion region, that is, the eye region, of all the images is very small and no noticeable changes are found in Figure 2.6; hence, the correlation value was high for all the fused images.

Figure 2.6: Eye sections.

We have created our own dataset, whose size is less in the pool to validate the robustness of the proposed system. In this database, the total number of images is 24. We have taken Official consent has been obtained from all participants in this study for fuse of their captured images. In this database set, both the partial faces along with the frontal faces are captured but the expressions of the individuals do not vary, and remain the same throughout. This database set makes use of uniform lighting and the images are captured against the same background (Figure 2.7).

Some of the accepted cases and some of the false cases are shown in Figures 2.8 and 2.9. After performing the proposed method in our own database, the acceptance rate is 87.5.

2.6 Face detection with Internet of things

At present, maximum technological advancements have taken place with the help of a concept named as Internet of things (IoT), where the various real-life physical devices are connected to the Internet [16, 17]. This IoT technology consists of very powerful, precise and riskless infrastructure along with features like minimum power consumption and cost effectiveness, where anything or anyone can be communicated or connected with each other anywhere or anytime to achieve the desired output. IoT can be implemented in different segments in our daily life, such as home automation, transportation, agriculture and healthcare segments. One of expandable areas using IoT infrastructure [18] is face recognition, which can be

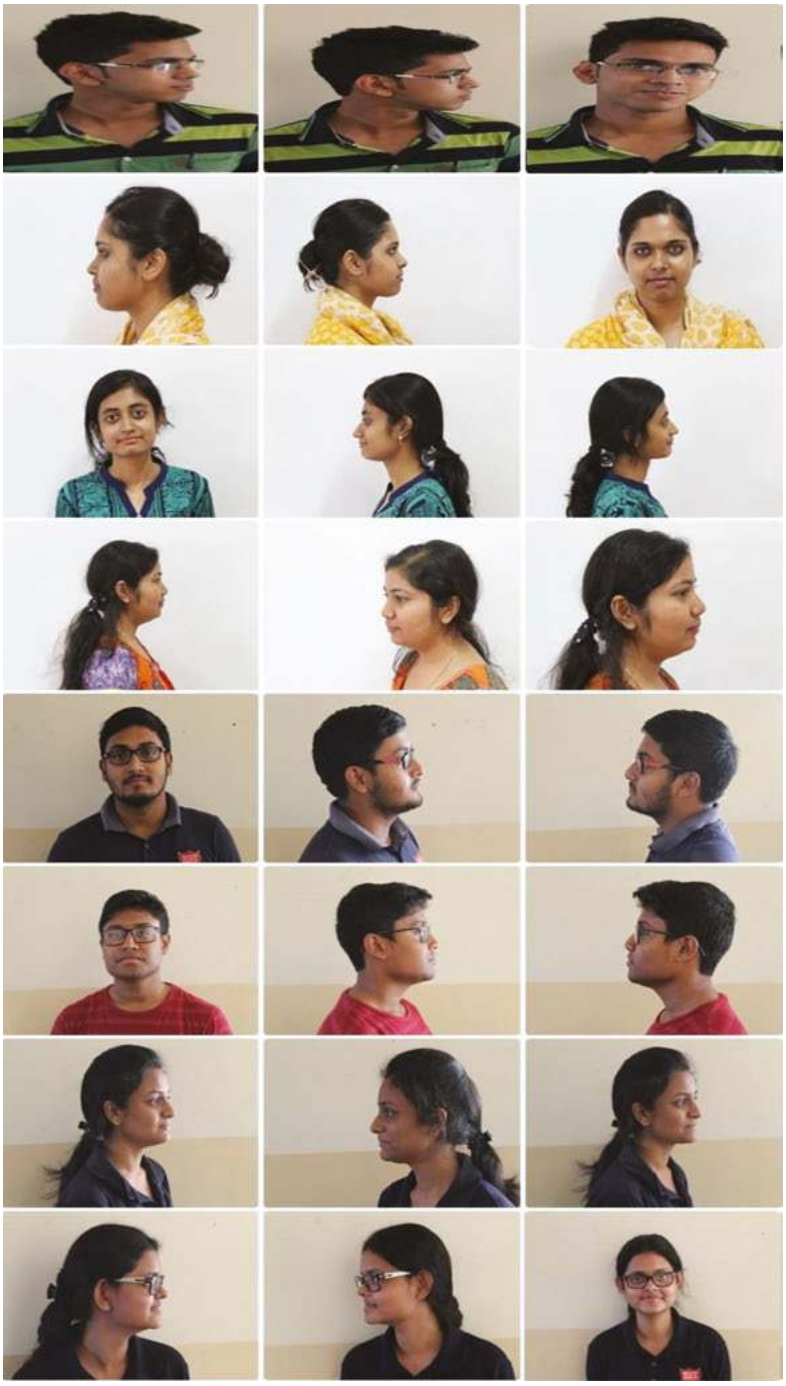


Figure 2.7: Prepared dataset.

Figure 2.8: Accepted cases.

Figure 2.9: False cases.

applied in different fields such as biometric system [19], attendance system and security reasons. Nowadays, attendance system is a mandatory prerequisite for any organization but maintaining the attendance manually is a very time-consuming and difficult task. To resolve this issue, several automated methods have been implemented which is not only easy to handle, but also the accuracy level of these systems can be better [20]. Face recognition system is one of the popular human identification processes, where the ambiguities such as time consuming, fake attendance, high cost and human errors are resolved [21]. This system can be used in any organization like school, college, bank and corporate office to reduce the probability of any complication such as fake attendance by feature [22, 23] identification. In this system, the attendance of each and every person is automatically recorded whenever they enter into their workspace through the continuous detection of each and every person's face. After that the detected faces are simultaneously compared with the previously taken database. If the detected image is matched with the stored image, then the attendance is given to that particular person, otherwise not. The partial face recognition system is a part of face recognition which is also a very challenging and interesting process. In this case, the picture of a person's partial face is taken with the help of a camera and the database consists of the full face as well as partial face of that person. The intermediate and all the other steps are similar with any face recognition process. This partial face recognition can also be implemented with the help of IoT technology, where the camera is connected to a raspberry pi and then the comparison of images is done with the stored images in the database. The accuracy level of this type of attendance system is generally better when compared with the manual attendance system.

2.7 Conclusions

Partial face recognition algorithm is a modern and advanced technique. The process includes various advantages as well as limitations. It is also an efficient method of biometric identification technique. The proposed method is applied in a large data set, which gives the acceptance rate of 86.67%. We have also created our own dataset, whose size is less in the pool and the proposed method is also applied in that dataset which gives the acceptance rate of 87.5%. In this proposed method, averaging technique of image fusion and after that correlation method is used but other fusion techniques also exist through which the value of the correlation method may vary affecting the acceptance rate; hence, the accuracy may be varied.

References

[1] Nath, S. S., Mishra, G., Kar, J., Chakraborty, S., and Dey, N. “A survey of image classification methods and techniques,” in Control, Instrumentation, Communication and Computational Technologies (ICCICCT),2014, International Conference, on, 2014, pp. 554–557. IEEE.

[2] Liao, S., Jain, A. K., and Li, S. Z. “Partial face recognition: alignment- free approach,” IEEE Transactions on pattern analysis and machine intelligence, 35(5), 2013, pp. 1193–1205.

[3] Smeets, D., Keustermans, J., Vandermeulen, D., and Suetens, P. “Mesh-SIFT: local surface features for 3d face recognition under expression variations and partial data,” Computer Vision and Image Understanding, 117(2), 2013, pp. 158–169.

[4] Ding, C., Xu, C., and Tao, D. “Multi-task pose-invariant face recognition,” IEEE Transactions on Image Processing, 24(3), 2015, pp. 980–993.

[5] Dey, N. (2019). Uneven illumination correction of digital images: A survey of the state-of-the-art. Optik, 183, 483–495.

[6] Best-Rowden, L. and Jain, A. K. “Longitudinal study of automatic face recognition,” IEEE transactions on pattern analysis and machine intelligence, 40(1), 2018, pp. 148–162.

[7] Lahasan, B., Lutfi, S. L., Venkat, I., Al-Betar, M. A., and San-Segundo, R. “Optimized symmetric partial facegraphs for face recognition in adverse conditions,” Information Sciences, 429, 2018, pp. 194–214.

[8] Fu, L., Chen, D., Lin, K., & Li, A. (2018). An improved SRC method based on virtual samples for face recognition. Journal of Modern Optics, 65(13), 1565-1576.

[9] Dey, N., Pal, M., and Das, A. “A session based blind watermarking technique within the NROI of retinal fundus images for authentication using DWT, spread spectrum and Harris corner detection,” arXiv preprint arXiv:1209.0053, 2012.

[10] Satapathy, S. C., Raja, N. S. M., Rajinikanth, V., Ashour, A. S., and Dey, N. “Multi-level image thresholding using Otsu and chaotic bat algorithm,” Neural Computing and Applications, June 2018, Volume 29, Issue 12, pp. 1285–1307

[11] Roy, P., Goswami, S., Chakraborty, S., Azar, A. T., and Dey, N. “Image segmentation using rough set theory: a review,” International Journal of Rough Sets and Data Analysis (IJRSDA), 1 (2), 2014, pp. 62–74.

[12] Dey, N., Ashour, A., & Patra, P. K. (2017). Feature Detectors and Motion Detection in Video Processing (pp. 1-328). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-1025-3

[13] Bhattacharya, T., Dey, N., and Chaudhuri, S. “A session based multiple image hiding technique using DWT and DCT,” arXiv preprint arXiv:1208.0950, 2012.

[14] Kamal, S., Dey, N., Ashour, A., Ripon, S., Balas, V., and Kaysar, M., “FbMapping: an automated system for monitoring facebook data,” Neural Network World, 27(1), 2017, pp. 27.

[15] Le, D. N., Nguyen, G. N., Van Chung, L., and Dey, N. MMAS algorithm for features selection using 1D-DWT for video-based face recognition in the online video contextual advertisement user-oriented system. Journal of Global Information Management (JGIM), 25(4), 2017, pp. 103–124.

[16] Sarowar, M. G., Kamal, M. S., and Dey, N. Internet of things and its impacts in computing intelligence: a comprehensive review–IoT application for big data. In Big Data Analytics for Smart and Connected Cities (pp. 103–136). IGI Global, 2019.

[17] Kumar, P. M., Gandhi, U., Varatharajan, R., Manogaran, G., Jidhesh, R., and Vadivel, T. Intelligent face recognition and navigation system using neural learning for smart security in Internet of Things. Cluster Computing, 2017, pp. 1–12. https://link.springer.com/article/10.1007/s10586-017-1323-4 (last access date: 07.06.2019)

[18] Dharavath, K., Talukdar, F. A., Laskar, R. H., and Dey, N. Face recognition under dry and wet face conditions, In Intelligent techniques in signal processing for multimedia security, Dey,

N.,V. Santhi (Eds.), Studies in Computational Intelligence Series, Springer, 2017, pp. 253–271.
[19] Chaki, J., Dey, N., Shi, F., & Sherratt, R. S. (2019). Pattern mining approaches used in sensor-based biometric recognition: A review. IEEE Sensors Journal, 19(10), 3569–3580.
[20] Surekha, B., Nazare, K. J., Raju, S. V., and Dey, N. Attendance recording system using partial face recognition algorithm, In Intelligent techniques in signal processing for multimedia security, Dey, N.,V. Santhi (Eds.), Studies in Computational Intelligence Series, Springer, 2017, pp. 293–319.
[22] Dey, N., Bhatt, C., and Ashour, A. S. Big data for remote sensing: Visualization, analysis and interpretation, Cham: Springer, 2018.
[23] Chaki, J., and Dey, N. Pattern analysis of genetics and genomics: a survey of the state-of-art, Multimedia Tools and Applications, 2019, 1–32.

Poonam N. Railkar, Parikshit N. Mahalle, Gitanjali R. Shinde and Hari R. Bhapkar

3 Threat analysis and attack modeling for machine-to-machine communication toward Internet of things

Abstract: The wide variety of Internet of thing (IoT) applications demands a secure and efficient communication channel that resists against a variety of modern attacks and fulfils application requirement. There are various IoT threats and challenges that must be addressed to make a communication secure in IoT. As growth in devices increases with their potential misuse, so there is a need to integrate security features into the available IoT algorithms and protocols. At the same time, we need to design new IoT protocols and algorithms for extended features of machine-to-machine (M2M) communication. This chapter has proposed a protocol stack that is mapped to the Transmission Control Protocol/Internet Protocol (TCP/IP) which is used for communication and connection of network devices on internet. The protocol present in a particular layer must acquire a security feature of associated layer. This chapter also elaborates on M2M communication in IoT. This chapter presents and discusses the literature survey corresponding to access control mechanism and trust management policies. From the literature survey it is observed that the existing security protocols, methods and algorithms are not suitable for IoT resource-constrained environment. The various resource-constrained devices are unable to cope up with different attacks. This chapter gives detailed analysis of attacks with its behavioral modeling. If the reader understands how attacks happen, then it will be easy to investigate solutions. From the extensive literature survey this chapter has drawn gap analysis, which gives insight into security requirements of IoT protocols and security algorithm. In addition, the chapter proposes a novel security framework that emphasizes on making secure communication layer with the help of trust management policies, distributed access control framework and privacy-aware protocols.

Keywords: Internet of things, M2M communication, threat analysis, IoT protocols, attacks

3.1 Introduction

The term “Internet of things” (IoT) was coined by Kevin Ashton at Procter & Gamble in 1999 [1]. At that time, he observed that radiofrequency identification (RFID) is required to the IoT, which would help computers to handle all individual things. In the era of computation, IoT is the important buzzword that drives global market. It is the

https://doi.org/10.1515/9783110628517-004

communication network of people, services and things. It also follows service-oriented architecture by providing service to other components of its architecture. It provides a communication channel to all varieties of devices for interaction with the help of the Internet. If we look from the architectural perspective, it is clear that it is a convergence of various technologies. The seamless integration of various technologies makes IoT more successful in global IT market. In near future, billions and trillions of devices are going to be connected over the Internet. According to a report given by global institute, considerable growth in devices of 300% has been observed in last half decade [2]. The same exponential growth is expected in near future. The objective of these connected devices is to bring betterment to human life. So, IoT is implemented in various domains such as agriculture, supply chain management, wireless sensor network (WSN) and health care. The advancement in each domain is observed in the last 5 years.

Since last few years, researchers have been trying to propose generic IoT architecture but still there is no standard architecture for IoT. Generic IoT architecture is composed of four layers, including application layer, middleware layer, network layer and perception layer [3]. According to the International Telecommunication Union (ITU), IoT architecture consists of five layers, which includes sensing layer, access layer, network layer, middleware layer and application layer [4].

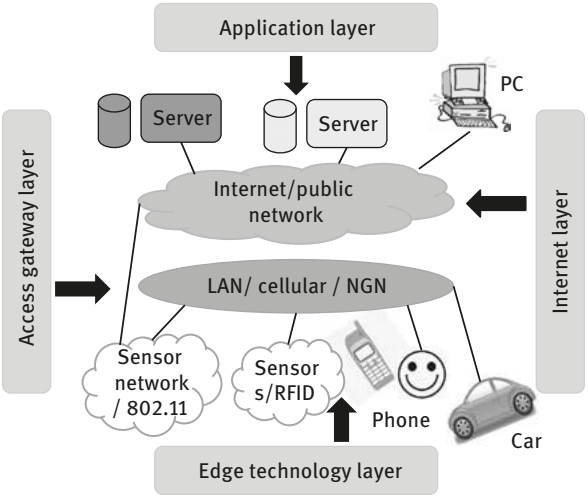


Figure 3.1: IoT layered perspective.

Figure 3.1 mainly shows an architectural perspective of IoT [5]. This architecture can be viewed as a service-oriented architecture, in which each architectural component or layer provides service to other layers or component in the architecture. The edge technology layer helps to connect sensor networks, things and RFID to

access gateway layer. This access gateway layer is a collection of various network devices and middleware which supports connectivity between Internet layer and access gateway layer. Internet layer supports Internet protocols that are required for networking. Application layer handles all types of smart applications, for example, smart transportation and smart home.

In real-time application development, the data flows from sensor devices to middleware using edge technologies like Wi-Fi and Bluetooth. The middleware is a software or hardware component that acquires data and performs basic analytics to take local decisions. This data from middleware travels toward cloud end with the help of Internet. There are various cloud service providers such as AWS, Microsoft and IBM, which provide a platform for IoT application development. Finally, this collected data is used for the analytical purpose. These analytical results help to take best decisions and for building smarter applications.

IoT is mature enough in European countries; however, there are some developing countries that are facing problems in implementing IoT [6]. At some places, the picture of IoT is still very blur. So, another term that is used as the replacement of IoT is machine-to-machine (M2M) communication. Actually, the scope of IoT is not limited to only M2M communication, rather, we can say M2M communication is part of IoT network. In M2M communication, the machines or devices are connected to each other to control, monitor and exchange data with the remote machine. M2M communication enables the capability of embedded hardware for sensing, actuation and communication. In M2M communication the network can be developed with the help of wired or wireless media to communicate with other heterogeneous types of devices. This communication allows gathering information from the edge of all enterprises and applying various ways to make a positive impact on business growth. M2M communication is a subset of IoT. In M2M communication participating devices are independent of Internet connection. In M2M communication there are limited options for integration in the system because participating devices need to match communication standards. In the IoT, there are unlimited options for integration but it requires a solution that efficiently integrates all system components [7].

TCP/IP protocol stack gives a practical orientation of real-time communication. This suite consists of various protocols that work at different layers but the problem with the existing protocol is that it is not suitable for IoT [8]. IoT network consists of resource-constrained devices. Hence, IoT is in need of a protocol stack that accommodates lightweight protocols of IoT.

3.1.1 Various protocols used in IoT at all layers

IoT follows service-oriented architecture, which means one component of architecture provides service to another layer of architecture. If we look it as a layered architecture,

then one layer provides services to other layer. This task is beautifully carried out with the help of protocols. Figure 3.2 shows protocols used at different IoT layers.

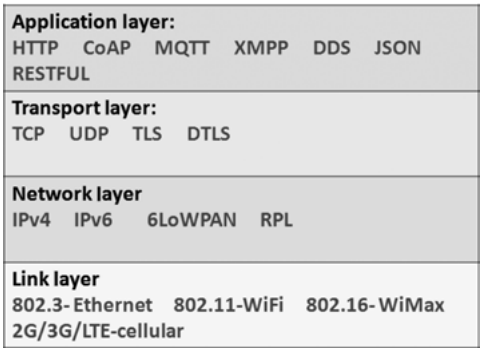


Figure 3.2: Protocols used in IoT at all layers.

1. **Link layer**
   Link layer decides to transfer data physically over network's physical layer or medium, for example, radio wave, coaxial cable or copper wire. The scope of link layer is a local network, a connection to which the host is attached. Data packets are exchanged over link layer by host using link-layer protocols. Link-layer protocols in context of IoT are 802.3- Ethernet, 802.11-WiFi, 802.16-WiMax and 2G/3G/LTE-cellular.
2. **Network layer**
   This layer is responsible for sending of IP datagram from the source network to the destination network. Protocols used in this layer are IPv4, IPv6, and 6LoWPAN.
3. **Transport layer**
   The protocols in this layer provide end-to-end message transfer capability. Protocols used in this layer are TCP, UDP, TLS and DTLS.
4. **Application layer**
   Protocols in this layer define how application interface with lower layer protocols to send the data over the network. Protocols used in this layer are HTTP, CoAP, MQTT, XMPP, and DDS.

3.2 Motivation

IoT promises a key role for information transaction and medium, management and computing since the beginning of the twenty-first century. As discussed in the above section, it is clear that IoT is open to the Internet and it is obvious that it is

open to the attacker to attack the system. Consider any application like health care, military, smart home, smart industries and so on. These industries use IoT-enabled systems. Now, in these systems, sensors sense an environmental parameter and pass data to the next IoT component and final destination of data is a cloud. In the above scenario, data travels from the sensor node to cloud environment, and in transit the data is open in Internet. Attackers try to attack the system and try to collapse the system. In order to provide security to the whole IoT network, it is required to analyze every type of attacks that can happen in IoT. Purely, security to data is not sufficient; we need to provide security at each layer and to each component of IoT architecture. IoT consists of resource-constrained devices for which we cannot use existing security protocols, algorithms and policies. In order to maintain security of each solution against every attack, we need to study behavioral modeling of each exposed attack. The objective of this chapter is to understand security in IoT as it is a fundamental pillar of IoT ecosystem. At the same time, it is required to analyze behavioral modeling of most possible attacks to provide a solution set in near future.

3.3 Threat analysis

3.3.1 Threats and attacks at various layers

Table 3.1 lists the threats and attacks at various layers.

A threat is something that may or may not happen, but has the capability to cause serious damage to network and data as well. Threats can lead to attacks on computer systems, networks and more. Security threats and vulnerabilities of the M2M communication in the IoTs are explored in this section.

3.3.2 Threat Analysis

Security and privacy is always a major concern when data and resources are open to Internet. In order to develop security solution it is required to analyze the behavior of each and every aspect of threats. Security threats have been explained in the context of M2M communication.

Cloning of thing

Many times an untrusted device manufacturer creates a clone device that is having identical security configuration, link-layer properties and unique identification of things of real one. To attract customers, these cloned faulty devices are sold at

Table 3.1: Threats and attacks at various layers.

Layer	Threats	Attacks
Application layer	– Warms and virus – Trojan horse – Buffer overflow – APP/OS weakness. – Identity theft and unsecured end devices – Insufficient patching and testing – Multilayer data management and security – Phishing – Ransomware – IoT botnets	– mpersonation attack or clone attack – Man in middle attack – DoS attack – Malware – Phishing – DDoS attack – SQL injections – XMAS attacks
Presentation layers	– Viruses – Wormwares	–
Session layers	– Personal information retrieval – Root privilege access – Net bios – DoS	–
Transport layer	– Port scanning – TCP sync flooding – UDP flooding	– DOS – DDOS
Network Layer	– Sniffing – IP alteration – DHCP attack – Phishing	– Man in the middle attack – ICMP attack – Sybil attack – DoS attack – Sinkhole attack
Data link layer	– ARP attack – MAC address alteration – MAC flooding	– ARP spoofing – Sniffing – MAC flooding attacks
Physical layer	– Cable disconnected – Cloning of things – Unauthorized access to tags – Tag cloning	– Passive sniffing over a media

lower price in the market. With the help of these devices, an attacker can hack original devices or degrade the performance of genuine devices. With cloned things, the manufacturer can observe the data traveling in the network and may perform a Sybil attack and node replication attack. A manufacturer can implement a backdoor for any confidential application. In the RFID system, tag cloning is easily possible because of weak authentication mechanism [9].

Commissioning of a thing

At the time of commissioning of things, things can be vulnerable to eavesdropping attack. Mostly configuration settings, security parameters and keying materials may be compromised through wireless medium. The attacker might be able to recover the secret key after obtaining keying material, thereby the authenticity and confidentiality may be compromised. If communication channels are not properly protected, M2M communication may eavesdrop or even session key can be compromised because of a long period of usage without key renewal or updates.

Malicious replacement of things

Sometimes attacker adds a new node in the network of participating node and assigned node identification information. The replaced node is involved in malicious activities. Sometimes it is possible that, in order to save the cost and increase profit from the system, the lower quality sensors are placed in the network. Attacker finds out such low-quality nodes and targets them for malicious activities, Due to this attack, the performance of the system is hampered. At the same time attacker can change the direction of packet toward malicious server enabling an attacker to monitor network activities [10].

Unreliable communication

If we use an unreliable communication link it raises the question of data integrity. The attacker can target this unreliable communication medium as a target and can perform a man in the middle attack. The unreliable communication link does not guarantee the successful delivery of the message. If packets are not delivered to destination, retransmission of packet takes place, which leads to dropping down the performance of the system. Due to multiple retransmissions, the time required to reach destination also increases, which affects the throughput of the system [11].

Resource constraints

The IoT network is mostly filled with embedded computing devices that appear to be resource constraint. The resource constraints are not only applied to the memory and processing capability but also to low bandwidth utilization, which leads to constraints on the network interface. Due to the resource-constrained devices, IoT system is vulnerable to security attacks.

a. Limited computing power and memory

These embedded devices require to possess sufficient amount of computational power with which they can complete the allocated task. To improve the lifetime of embedded devices, these devices should be designed in such a way that they can perform the required set of operations with minimum computational efficiency as it has limited memory and storage. For resource-constrained devices, we need to analyze bare minimum features that will be integrated into embedded devices. The researcher needs to develop lightweight security protocols that are complex to break by considering crucial security measures. There is always a trade-off between processing power and the memory requirement of security algorithm. For these protocols, we need to leave enough space for security software that strongly resists security threats [12].

b. Limited battery

IoT is a network of connected devices. The idea here is to connect everything to everything to collect data and obtain analytical results from that data to make an intelligent system. Most of the time the remotely placed devices are battery powered. Therefore, researchers are working on ideas/mechanism to increase the lifetime of the battery. There are lots of parameters that decide the lifetime of the battery. Security protocol, mathematical operation and network protocol are the key parameters that drain the major portion of the battery. The complex security protocols lead to battery drain, due to which lifetime of the device decreases. Hence, there is a need for lightweight security protocols with minimum computation and memory that does not harm the lifetime of devices [13].

Identity theft and unsecured end devices

In IoT, security plays an important role in real-time scenarios. In IoT, we need to take care of devices, especially those devices that hold important financial and private information. In some IoT systems, these devices are made secure with different security mechanism. But all IoT devices are not secure enough to prevent identity theft and security breaches, for example, there are a variety of vendors

selling a smartwatch but only 50% smartwatches allow its users to set authentication password. There are various enterprises that do not bother about vulnerabilities within IoT devices. The available security mechanisms try to prevent attack; however, the attacker hacks the data center or network. Due to this type of theft, impersonation attack or clone attacks are possible [14].

Privacy threat

In IoT, there are some applications that carry user's sensitive data. It is required to protect that data from being exposed to IoT environment. It is a major point of concern if devices carry health-related data. The services provided by these connected devices offer better human life but at the same time, the privacy of the user should not be compromised. The tracking of objects' location and its usage may lead to increased privacy risk to the end users. When information is passed inside IoT systems only, the attacker may infer the information by performing analytical operation and inferred data can predict the behavioral pattern of user's interest and such information will be sold for marketing purpose.

Insufficient patching and testing

Insufficient patching is the most common and the biggest problem faced by the IoT ecosystem. The problem of patching is mostly ignored by the system supervisor. The outdated devices may have some software issues, incompatibility with other devices, set of protocols used or it may contain some bugs or vulnerabilities. So, to break the security of the system, attacker may use these vulnerabilities as the door to open into systems. The patching is required to secure the system from the above-mentioned vulnerabilities. Now, it is important to monitor and test each updated path to maintain stability of the system. Insufficient patching and testing also give way to the attacker to enter into a system that leads to cloning attack or malware [15].

Multilayer data management and security

The IT industry is moving rapidly, so in a real-time scenario, it becomes very much necessary to adopt changes by deploying new technologies like cloud, big data and IoT. This deployment of new technology is more important than securing the infrastructure and network. As IoT drives the global market including financial organizations [16], it should not compromise with security threats. By considering all aspects of infrastructure, security should be placed at the central point of

investment. For any application development, we need to provide security at each and every layer of our network. The layers at which security is important are (1) end devices, (2) software configurations, (3) communication framework or channel and (4) web cloud and mobile environment.

Phishing

It is a kind of social engineering attack in which an attacker steals user's sensitive data like login credential or credit card information. It is not a new type of attack but despite growing awareness about this attack, organizations are unable to provide full resistance against sophisticated social engineering attack. This attack has a variety of results [17].

Ransomware

Ransomware is a kind of malicious software in which attacker threatens the victim to publish victim's sensitive information or purposefully block access to its resources until a ransom is paid to the attacker. This attack is performed through Trojan. This Trojan file hides behind the legitimate file and is sent to victims as an email attachment. When the victim opens this file, the malware takes the ownership rights of the victim's resources. For relieving access to victim, attacker demands ransom. The example of ransomware is "WannaCry" ransomware, which automatically travels in the network without any interaction with victims. The windows user is mostly affected by this attack. The evolution of this attack is still in progress. Generally, a target for attacker is a high-end server because it carries a massive amount of sensitive data [18]. The windows user mostly affected by this attack.

IoT botnet

The distributed denial of service (DDOS) performed on Dyn proves the potential of DDoS attack in IoT. This happens because of the lack of embedded security and fewer security considerations for participating devices. The botnet is the most widely used weapon to attack IoT devices. Botnet means the computer that is controlled remotely. The access to devices is gained by injecting malware inside the devices. These infected devices communicated with other participating nodes in the network or server and wait for an instruction from the attacker [19].

3.4 Attack modeling

The objective of this section is to provide information about how attacks are performed. This helps the researcher to work on mitigation technique to prevent the attack or to control the damage.

1) Sybil attack
In IoT, each individual device carries its own identity. In this attack, malicious nodes communicate with other nodes via separate communication link. For identity establishment, the attacker creates duplicate identity of the legitimate node and hides behind that node. In this attack, the attacker is present at multiple places at the same time. This can be done by identity spoofing [20].

In the given Figure 3.3, device 1 gets access from server after authentication. Then the attacker gets the id proof of device 1 from server and starts communicating with the other device pretending to be device 1 communicating with device 2. In this process, the id proof of device 1 gets compromised and is used by the attacker to retrieve data from device 2.

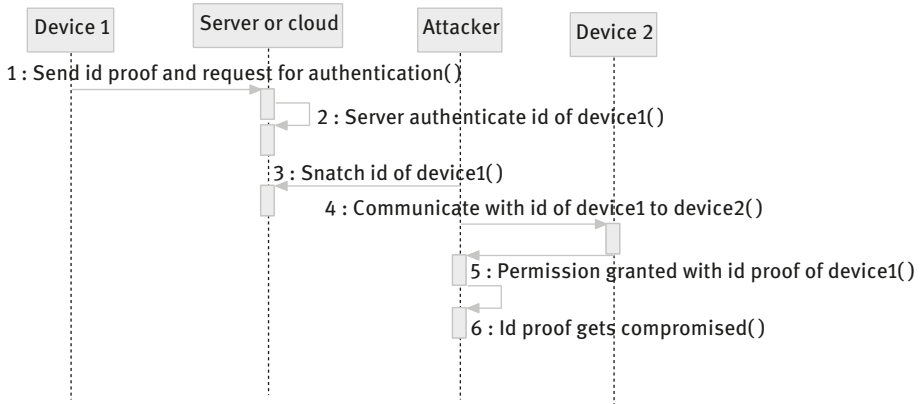


Figure 3.3: Sybil attack.

2) Data integrity attack
In this type of attack, the data is monitored or altered when it travels through the network. The attacker changes the contents of the data packet by injecting false information into the packet. By performing this attack, attacker increases impurity in the sensor data and by doing so he creates an obstacle in victim's research. We can say that it is a kind of DoS attack. The impure data gives poor decisions. The attacker adds impurities in victim's database that are in acceptable range. So, it is very difficult for the victim to find out and separate impurities in the dataset. Various practical approaches are presented to prevent this attack [21].

Figure 3.4 shows how data integrity attack happens. In data integrity attack, attacker targets any legitimate node of the network. Then attacker injects malicious code into that node. This infected node acts as a malicious node. An attacker can change the code of a malicious node; it alters data that is transmitted by the malicious node. This faulty data will be transmitted to all other nodes in the network. The communication between all these nodes has been represented in Figure 3.4.

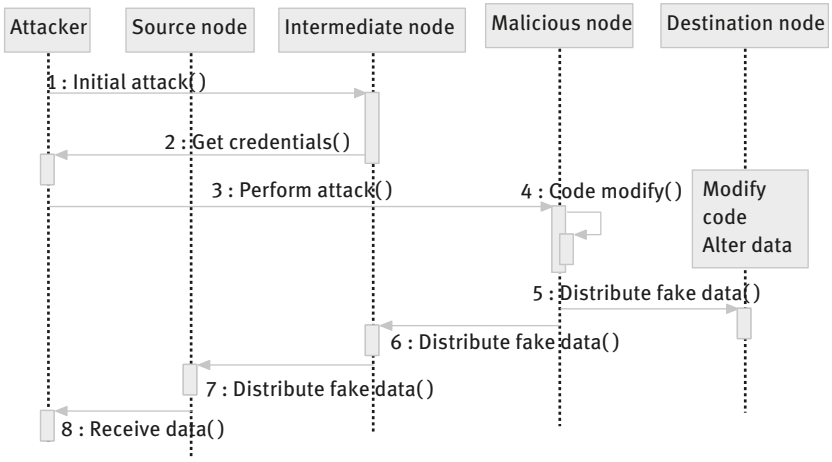


Figure 3.4: Data integrity attack.

3) Node replication attack

This is an application-independent attack. First, attacker captures a single legitimate node and gathers information like secret credentials, code and cryptographic material, and if required attacker can modify code and change the behavior of node. Further attacker replicates the same image to other node and deploys these replicated nodes in the environment. This type of attack is very destructive. The general-purpose authentication and security methods cope up with this attack [22].

The behavior of node replication attack is represented in Figure 3.5. Various entities participate in this communication. The attacker initiates the attack and targets any legitimate node of the network. Before the attack, attackers analyze all unsecured roots through which they can enter into the network. Once they are able to manage legitimate node then attacker collects all the secret information of node such as credentials and secret keys. Once an attacker gets this information of the legitimate node, the information will be modified. According to the attacker's requirement, the same information will be implanted in node memory. After that these infected nodes act according to the attacker's instructions. In this way attacker can make the target network unstable.

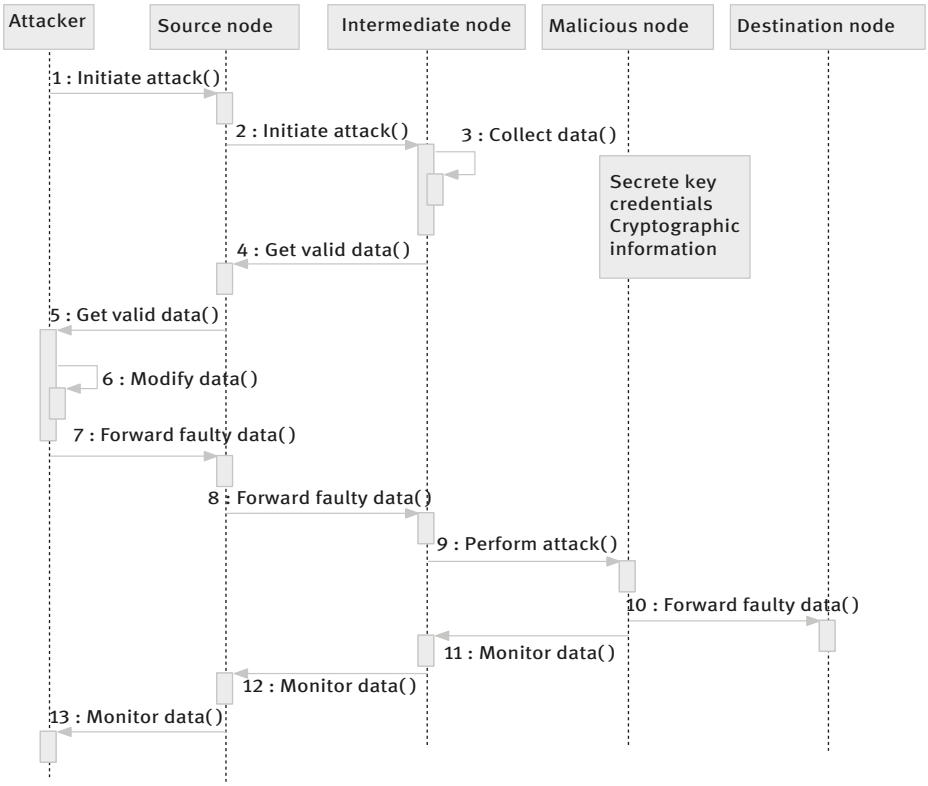


Figure 3.5: Node replication attack.

4) DoS attack

Denial of service (DoS) attack makes service unavailable. The attacker makes an attempt to prevent users getting services or access to resources. DoS is difficult to perform but it is dangerous. The attacker continuously sends request packets to the server. If the server is unable to handle these large number of requests, then it results in server unavailability [23].

In Figure 3.6, device 1 is able to get services from server after its identity is verified. After that device 1 gives encrypted data to server, which is retrieved by the intended device. Then device 2 gets authenticated from server and tries to access encrypted data stored on server by device 1. At the same time attacker uploads large file on server or continuously gives data to server, thereby preventing device 2 from getting its requested encrypted file from server leading to buffer overflow, due to which server is unable to give service to device 2. In this way, DoS attack is done by the attacker.

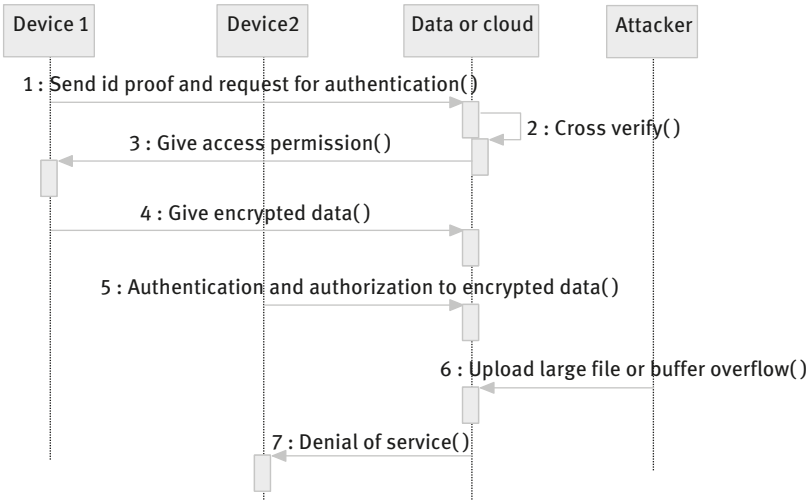


Figure 3.6: Denial of service attack.

5) Replay attack

It is a type of network attack in which data transmission on authenticated channel is observed by using legitimate user credentials and repeatedly transfers data to the destination node. This attack can be done by either originator of message or man in the middle. It is also a kind of man in the middle attack [20, 24].

The sequence diagram of replay attack is represented in Figure 3.7. In this type of attack, attacker attacks legitimate nodes of the network and collects all the information from the intermediate node. An identity is assigned to the compromised node. The attackers spread wrong data in the network or turn traffic of malicious node toward the compromised server. Valid data transmitted is repeated either by malicious node or source node. Malicious node can also intercept and modify data.

6) Man in middle attack

In this attack, attackers try to gain control of the communication link that connects the endpoints. This attack leads to compromised data confidentiality and data integrity. It is also referred as bucket brigade attack or fire brigade attack. There are various versions of this attack. In this type of attack, attacker can alter the data while two parties are communicating and we believe that they are directly communicating [25].

A public key cryptosystem is vulnerable as shown in Figure 3.8. For communication between two devices, key exchange is required in public key cryptosystems. When device A wants to communicate with device B, device A requests to device B for its B's public key. An attacker intercepts its request and sends its own public

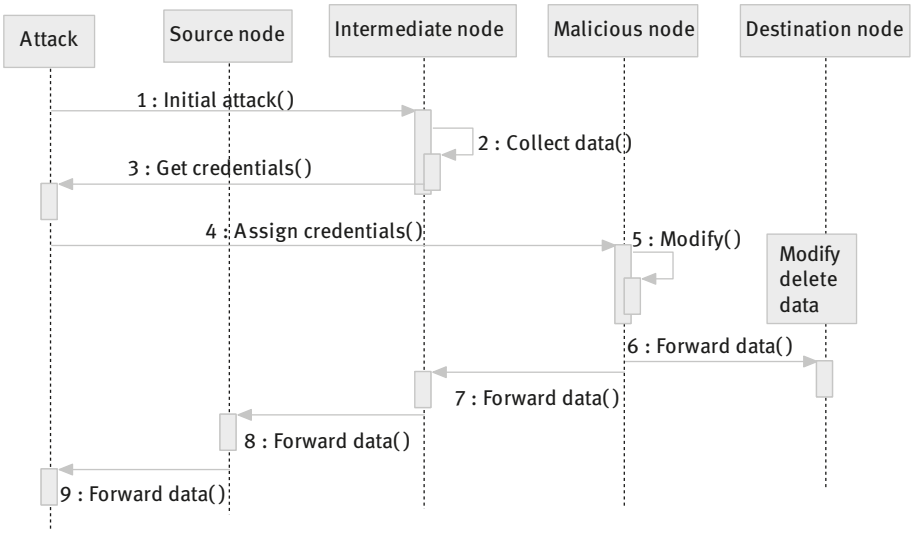


Figure 3.7: Replay attack.

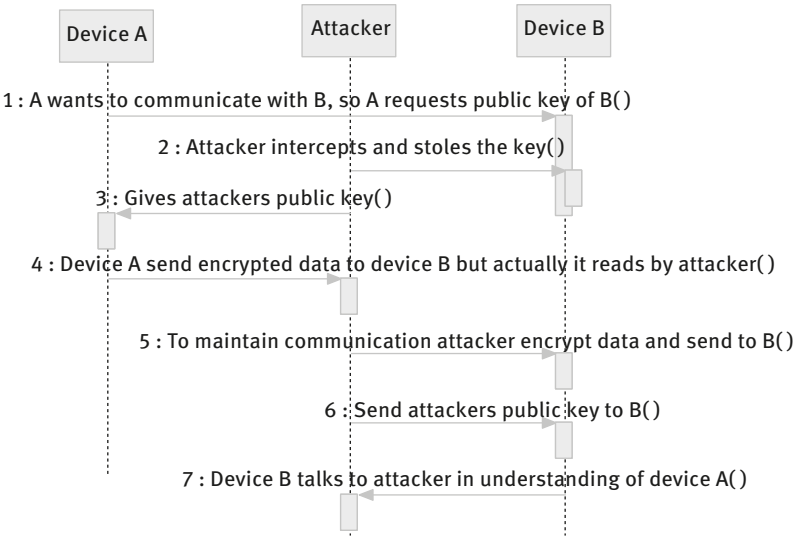


Figure 3.8: Man in middle attack.

key to device A. So whatever sent by device A to device B is intercept and read by an attacker. For maintaining communication, attacker re-encrypts this data by device B's public key and sends it to device B. Attacker also sends its own public key as A's public key to device B.

7) Sniffing
It is a program that monitors data traveling over the network. This sniffing is required for monitor-authenticated network as well as for stealing network information. These unauthorized sniffers are very much harmful because it is very difficult to identify sniffer-affected nodes and can be inserted at any node of network. This makes sniffing attack more popular in attacker community [26].

In Figure 3.9, devices 1 and 2 communicate with each other via server. The encrypted data is stored and is accessed by device 2 which is monitored or sniffed by the attacker. Finally, attacker gets the intended data that is sniffed by device 1 during the process of storing in server. Then attacker makes some changes into the encrypted data. Thus, device 2 receives corrupted data.

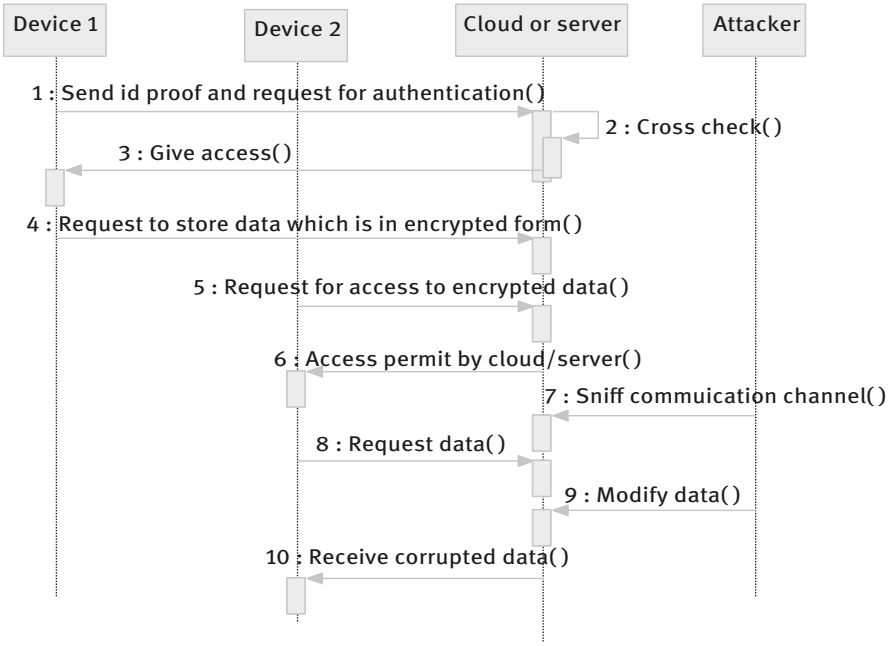


Figure 3.9: Sniffing.

8) Ransomware
It is a kind of malware that restricts the victim to access its own resources like important files of computers and demands for money to remove restriction on resources. There are two very common mediums through which these ransomwares enter the system, which are phishing email and USB drives that contain malicious software or files [27].

In Figure 3.10, attacker enters into the system through email attachment files, external hard disk drives or USBs, which causes worms or viruses to enter into the

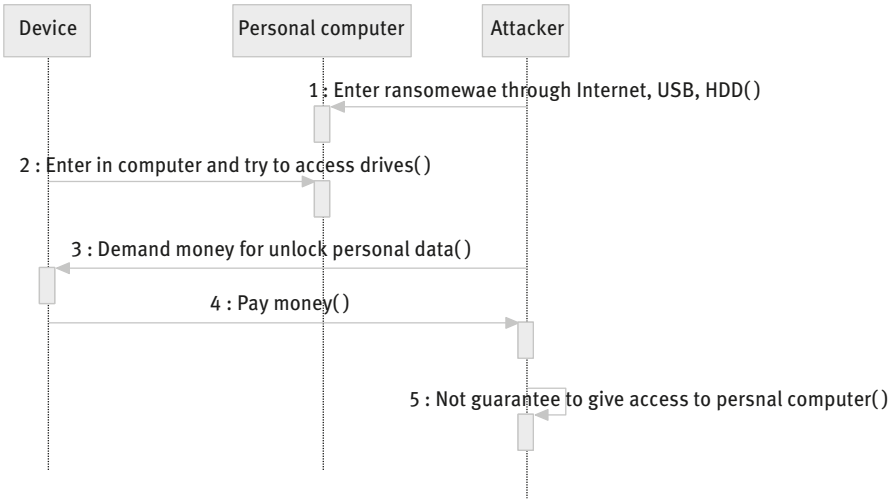


Figure 3.10: Ransomware attack.

system and blocks the personal data and drives of the device. When the device tries to access the personal data, then attacker demands money for unlocking of personal files. If device makes payment then also attacker does not guarantee to give access to its personal data or drives. As per Figure 3.10 attacker sends email with attachment and victim opens that attachment. Now, the malware restricts the victim from accessing its own resources like important files of computers and demands for ransom. Once payment is done then only attacker releases the victim's resources.

3.5 Literature survey

As outstanding research has been carried out in the field of IoT, however, there are still various vulnerabilities present, which makes IoT insecure. As a result of this, attackers have invented so many attacks on IoT even before IoT could mature in the IT industry. So there is a need to study the various leading attacks and threat analysis in IoT. The large scale of heterogeneous and resource-constrained devices with lack of uniformity makes it challenging to provide security in IoT environment.

Kaur and Singh [28], and Reed [29] classify attacks on the basis of the OSI layer. The variety of security attacks on RFID system have been addressed in [30]. The variety of attacks on RFID systems along with possible solutions have been proposed in [31]. General categorization of attacks has been proposed in [32]. This paper classifies attacks by considering properties and target layer into four categories, that is, encryption attack, software attack, network attack and physical attack. According to the literature survey, possible categorizations of attacks in IoT are shown in Figure 3.11.

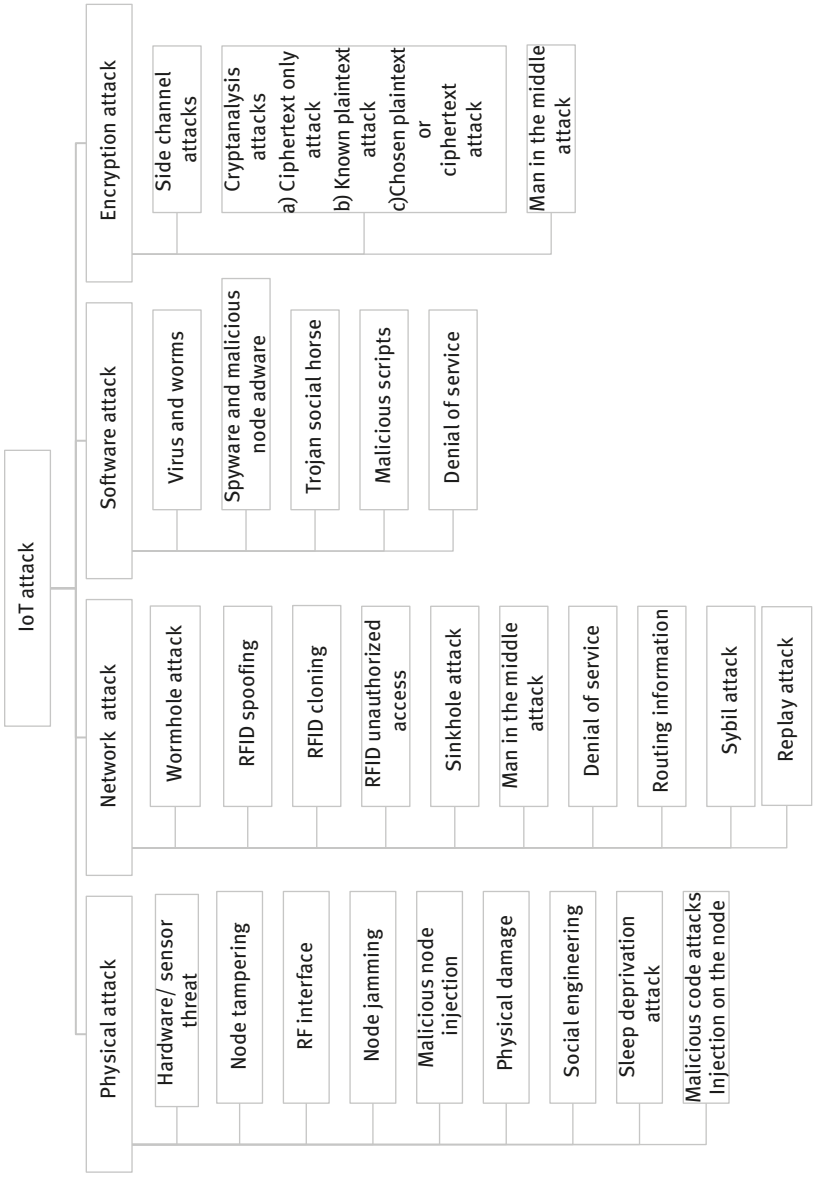


Figure 3.11: Security attacks of IoT.

Barki [33] emphasizes on M2M research and development works, which mainly addresses security, threats and vulnerabilities that occur in M2M communications. Sicari et al. [34] give an overview of research challenges with possible solution methodologies to make IoT ecosystem secure. There are various security issues but major ones are identified in eight categories: (1) proper authentication mechanism, (2) confidentiality, (3) access control policies, (4) trust-related issues, (5) policy enforcement, (6) mobile security, (7) security of middleware and (8) privacy policies. Firdous et al. [35] explain the MQTT threat model and they evaluate the performance of DoS attack that targets MQTT brokers.

In real-time scenario, millions and billions of devices are communicating with each other. Sometimes devices carry data from users' personal space and travel over the Internet. Therefore, there are more chances that the privacy of data gets compromised. In [36], the various privacy policies for different data have been proposed to protect user's privacy. Each privacy zone is mapped with the context-based method and is verified by Home Security Hub. This process is done before acceptance of joining or rejoining of requests to protect user data against unauthorized data sharing. However, the chances of locating smart devices directly bypassing the hub are not considered.

Que and Ma [37] propose a novel methodology for mutual authentication and key establishment scheme for the M2M communications, which uses 6LoWPAN networks. The session key will be established to authenticate each device with remote server in 6LoWPAN networks. This scheme also prevents various malicious attacks like Sybil attacks, replay attacks, MITM attacks and impersonation attacks. This scheme also incurs less computational overhead and transmission overhead.

Lin et al. [38] propose a local authentication and access control scheme, which is designed for verification of access rights and user privileges in M2M communication. Device heterogeneity is also supported by this scheme. In order to improve the scheme, a novel SOC (securely outsourcing computation) algorithm has been proposed. This algorithm offloads the computational cost from M2M devices to the user equipment. This algorithm is also energy efficient, and also satisfies the security criteria of user anonymity, secure key agreement, mutual authentication and SOC.

Mahalle et al. [39, 40] have designed an identity establishment and capability-based access control protocol. This scheme uses elliptical curve cryptography for security. This scheme also supports protection from replay attack, man in middle attack and DoS attack.

Esfahani et al. [41] have proposed a hash-based lightweight authentication mechanism, which uses XOR operations in M2M communications. The proposed methodology incurs low computational cost, and at the same time it removes the burden of communication and storage overhead for achieving session key agreement and mutual authentication, and holds a device's identity confidential. This scheme is also attack resistant to modification attack, replay attack, impersonation attack and man in the middle attack.

Chen et al. [42] propose a security gateway application that will help to improve gateway application of ITU-TM2M service layer. This ITU-TM2M service layer is a layer of IoT's reference model. This application also provides a secure end-to-end M2M message delivery and key exchange generation functions. This application supports mutual authentication and symmetric cryptographic negotiation function which is of lightweight. This application is resistant to data privacy attack and relay attack. It also prevents key guessing attack and undetectable online key guessing attack.

Mahalle et al. [43] present key challenges, design constraints and framework for identity management in IoT. Matrix required for identity is explained in this paper.

Dey et al. [44] cover applications of big data generated by IoT and how to manage big data generated with all sensors and embedded devices. Applications like smart cities, industrial IoT, health care, robotic sensor networks, and smart irrigation and green cities are described properly in their contribution. Security for electronic patient record is explained in detail and the system also tested against attacks. Security issues for big data generated by IoT and attacks like side channel attack are also discussed.

Dey and coworkers [44–47] give an overview and implementation details of IoT-based wireless body area network (WBAN) in health care. Layerwise WBAN architecture, challenges and required security are explained in [45]. IoT brings extreme changes in the field of health-care technology. Bhatt et al. [46] describe challenges in smart health-care systems and possible vulnerabilities in e-health context. They also introduced energy-efficient health-care systems. Privacy, trust and security issues are also addressed. IoT architecture is explained in [47]. They have also explained IoT applications in health care.

Hassanien et al. [48] address the problems related to the Internet of medical things. They have provided solutions to challenges of medical big data and also recent techniques for classification of medical big data and machine learning. Privacy of data and security analysis is also presented for the Internet of medical things.

There is tremendous growth in digital communication and massive growth in digitization of data from the last few years and it is continuously going to increase as there is an evolution in IoT. Sarowar et al. [49] gave examples of the mechanism of messaging in M2M communication, in mobile computing and in sensors. They have given new techniques for spoofing detection of location, new efficient processing ideas and clustering tools for next generation are also presented.

3.6 Evaluation of related work

This section gives the comprehensive analysis of various attacks. In the following table, the detailed analysis of some outstanding research papers has been done on the basis of the attack-resistant mechanism proposed.

In Table 3.2, Sybil attack, man in the middle attack, DDOS attack, replay attack and identity attacks are taken into consideration because these attacks are very common in today's connected world and is widely performed by a hacker. There is a need of distributed framework that considers all dynamic aspects of security in IoT ecosystem. This framework should be lightweight, scalable, adaptive and simple. There are many methods proposed by the researcher to resist the above-mentioned attacks. So, we need to design the framework in such a way that it accommodates Identity establishment, device authentication methods, light-weight key management schemes, access control policies and protects privileges of the user. Table 3.2 also represents solutions for security and also tells highlights which solution is resistant to which attacks. The gap analysis is also presented in this table. We can observe that there is a need for the security framework that protects the system against various attacks. Most of the researchers try to make the authentication process more secure with optimization in computational cost and memory. All proposed methodologies or algorithms fulfill the requirements of resource constraints and is mostly applicable to the device-to-device communication.

3.7 Proposed work

Looking at various threats and in the sequel several attacks in resource-constrained IoT and M2M communication, security is of prime concern. Therefore, we need access to control solution, trust management scheme and privacy-enabled communication scheme. In this view, secure communication framework is shown in Figure 3.12.

The proposed architecture is divided into three layers:

1. Device layer
2. Secure communication layer
3. Application layer

3.7.1 Device layer

Here devices are with network capabilities ranging from high-end devices such as mainframes to simple sensors that have communication capability. It is very difficult to deal with resource-constrained devices. This layer may include sensors, actuators, WSN and other things. It is required to enable capability of devices in terms of computing, communication and sensing ability. The data collection node helps to aggregate data and at the same time plays a vital role in device management task at physical layer. The quality of data determines the quality of result

Table 3.2: Evaluation of related work based on attacks.

S. no.	Reference	Sybil Attack	MiTM	DDOS	Replay	Identity Attack	Proposed solution	Advantages
1	[37]	Y	Y	N	Y	Y	Device securely authenticates with remote server with session key establishment having a consideration of 6LowPAN	– Require less computational and transmission overhead
2	[38]	N	Y	N	Y	Y	Local authentication and access control scheme that verifies access privilege	– Support mutual authentication – Key agreement – Computational outsourcing
3	[39]	N	Y	Y	Y	N	Identity establishment and capability-based access control using elliptical curve cryptography	– Distributed – Lightweight
4	[41]	N	Y	N	Y	Y	Lightweight authentication mechanism using XOR operation and hash	– Computational cost is low – Low communication and storage overhead
5	[42]	N	N	N	Y	N	Proposes a security gateway application This system uses the lightweight symmetric key cryptographic negotiation function, secure E2E M2M key exchange generation function and secure E2E M2M messages delivery function	– In the IoTs reference model the gateway application of the ITU-TM2M service layer is improved. The proposed SGA could provide a mutual authentication mechanism, and it protects from the key guessing attack, the undetectable online key guessing attack, the data privacy attack as well as the relay attack

6	[50]	Y	N	N	Y	N	Key management scheme with adaptive addressing	– Lightweight – Balance trade-off between security and storage
7	[51]	N	N	Y	N	Y	Proposes SEGB protocol to enhance authentication and key agreement	– Developed for M2M communication
8	[52]	N	N	Y	N	N	Proposes hybrid attack detection model along with forensic analysis model	– Developed for M2M communication – Distributed
9	[53]	N	N	N	N	Y	Novel device hijacking-resistant framework for M2M communication	– Network centric – Avoids overhead-intensive cryptographic function
10	[54]	N	Y	N	N	N	Proposes key establishment mechanism for secure communication	– Mobility consideration – Reliable
11	[55]	N	Y	N	N	Y	Proposes hybrid approach that uses Radix64 encryption method	Tests node authentication and confidentiality of nodes

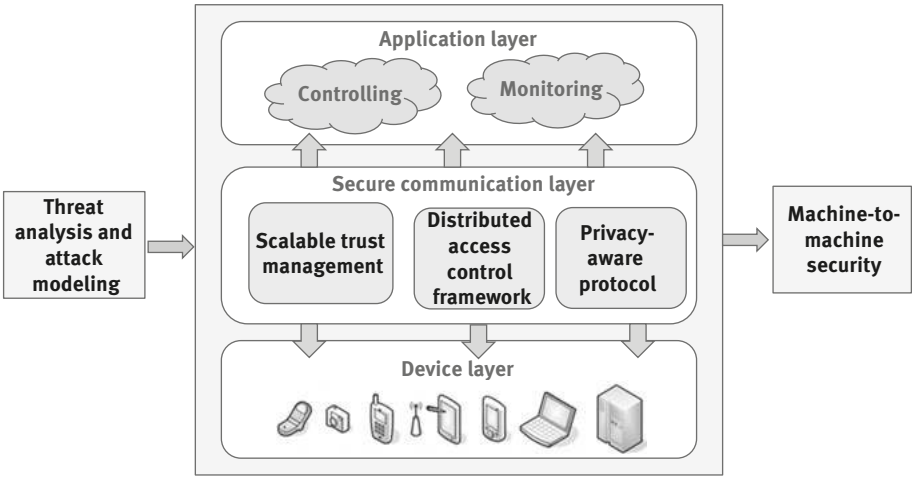


Figure 3.12: Proposed framework for secure machine to machine communication in IoT.

and accuracy of results. The collected data will be forwarded to secure communication layer

3.7.2 Secure communication layer

This one is the middle layer that securely manages relationships between machines and services. This layer basically consists of three stages: scalable trust management model for M2M, distributed access control scheme for constrained environment and privacy-aware protocol based on the principle of least privilege. The responsibility of this layer is to carry the data that is received from device layer to cloud or application layer. To design scalable, attack-resistant communication layer we need to do critical analysis of each threat and its behavior in real-time scenario. The objective is to provide communication security without losing privacy of user.

3.7.3 Application layer

This layer can support many applications, for example, autonomous controlling, managing small to high-end devices to provide and perform some services and applications. Whatever data received from secure communication layer, management of that data and its suitable representation is the responsibility of application layer.

The proposed framework is a generic framework and a distributed architecture by proposing attack-resistant access control scheme, trust management scheme as well as the privacy-aware protocol for M2M in IoT.

3.8 Conclusion and future work

The exponential growth of IoT in various domains in last few years leads to several threats and attacks. Unfortunately, IoT security has never been the central point of concern to researcher and developers. This chapter briefly discusses the threat analysis along with attack modeling in IoT network, and also presents a comparative analysis of various techniques that are required to secure IoT communication. The layerwise protocols along with possible attacks and threats are also presented in this chapter. The comprehensive gap analysis of existing mechanisms with respect to various attacks is presented. This chapter elaborated the requirement that must be fulfilled to make IoT secure.

In future, more efforts will be made to find out an optimum solution that resists multiple attacks at a time and to find out new opportunities in the field of IoT. In near future there is a need to develop lightweight algorithms that work in IoT network and prevent multiple attacks.

References

[1] Ashton, Kevin. "That 'Internet of things' thing", RFID Journal, 22(7), 2009, pp. 97–114.
[2] Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P. and Marrs, A., Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy, San Francisco, CA : McKinsey Global Institute, 2013.
[3] Ren, Zejun, et al. "Security and privacy on Internet of things." Electronics Information and Emergency Communication (ICEIEC), 2017 7th IEEE International Conference on. IEEE, 2017.
[4] Madakam, S., Ramaswamy, R., and Tripathi, S.. Internet of Things (IoT): A literature review, Journal of Computer and Communications, 3(05), (2015), pp. 164.
[5] Mahalle, Parikshit Narendra, and Poonam N. Railkar. "Identity management for Internet of things", River Publishers, 9220 Aalborg Denmark, Volume 39, ISBN: 978-87-93102-90-3 (Hard Copy) 978-87-93102-91-0 (Ebook), 2015.
[6] Lee, Suk Kyu, Bae, Mungyu, and Kim, Hwangnam. "Future of IoT networks: A survey", Applied Sciences, 7(10), 2017, pp. 1072.
[7] Al-Karaki, J. N., Chen, K. C., Morabito, G., & De Oliveira, J. "From M2M communications to the Internet of Things: Opportunities and challenges", Ad Hoc Networks, (18), pp. 1–2. Journal ISSN : 1570-8705, DOI:10.1016/j.adhoc.2014.03.006, 2014.
[8] Mahamure, S., Railkar, P. N., and Mahalle, N. Communication protocol and queueing theory-based modelling for the Internet of Things, Journal ICT, 3, 2016, pp. 157–176.
[9] Lee, P. Y., Yu, C. M., Dargahi, T., Conti, M., and Bianchi, G. MDSClone: multidimensional scaling aided clone detection in Internet of Things, IEEE Transactions on Information Forensics and Security, 13(8), 2018, pp.2031–2046.
[10] Chugh, K., Aboubaker, L., & Loo, J. (2012, August). "Case study of a black hole attack on LoWPAN-RPL" In Proc. of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy (pp. 157-162). Copyright (c) IARIA, 2012. ISBN: 978-1-61208-209-7, August 2012.
[11] Li, X., Lu, R., Liang, X., Shen, X., Chen, J., and Lin, X. Smart community: an Internet of things application, IEEE Communications Magazine, 49(11), 2011.

[12] Sehgal, A., Perelman, V., Kuryla, S., and Schonwalder, J. Management of resource constrained devices in the Internet of things, IEEE Communications Magazine, 50(12), 2012.
[13] Mahamure, S., Railkar, P. N., and Mahalle, P. N. Mathematical Representation of Quality of Service (QoS) Parameters for Internet of Things (IoT), International Journal of Rough Sets and Data Analysis (IJRSDA), 4(3), 2017, pp. 96–107.
[14] Vidalis, S., and Angelopoulou, O. (2014). Assessing identity theft in the Internet of Things. Journal of IT Convergence Practice. , Vol. 2 (1): 15-21, March 2014.
[15] Simpson, A. K., Roesner, F., and Kohno, T. (2017, March). Securing vulnerable home IoT devices with an in-hub security manager, In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 551–556). IEEE.
[16] Abu-Elkheir M., Hayajneh M., Ali NA. Data management for the Internet of Things: Design primitives and solution, Sensors. 13(11), 2013, pp.15582–15612.
[17] Gupta, B. B., Tewari, A., Jain, A. K., and Agrawal, D. P. Fighting against phishing attacks: state of the art and future challenges, Neural Computing and Applications, 28(12) 2017, pp.3629–3654.
[18] Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., and Guizani, M. The rise of ransomware and emerging security challenges in the Internet of Things, Computer Networks, 129, 2017, pp. 444–458.
[19] Bertino, E., and Islam, N. Botnets and Internet of things security. Computer, (2), 2017, pp. 76–79.
[20] Borgohain, T., Kumar, U., and Sanyal, S. Survey of security and privacy issues of Internet of things, arXiv preprint, arXiv:1501.02211, Advanced Networking and Applications Volume: 6 Issue: 4 Pages: 2372-2378 (2015) ISSN: 0975-0290, 2015.
[21] Liu, C., Yang, C., Zhang, X., and Chen, J. External integrity verification for outsourced big data in cloud and IoT: A big picture, Future generation computer systems, 49, 2015, pp. 58–67
[22] Parno, B., Perrig, A., & Gligor, V., May). Distributed detection of node replication attacks in sensor networks, In Security and Privacy, 2005 IEEE Symposium on (pp. 49–63). IEEE, 2005.
[23] Agah, A., & Das, S. K. Preventing DoS attacks in wireless sensor networks: A repeated game theory approach, IJ Network Security, 5(2), 2007, pp. 145–153.
[24] https://en.wikipedia.org/wiki/Replay_attack.
[25] Conti, M., Dragoni, N., and Lesyk, V. A survey of man in the middle attacks, IEEE Communications Surveys & Tutorials, 18(3), 2016, pp. 2027–2051.
[26] Sajid, A., Abbas, H., and Saleem, K. Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges, IEEE Access, 4,2016, pp.1375–1384.
[27] Azmoodeh, A., Dehghantanha, A., Conti, M., and Choo, K. K. R. Detecting crypto-ransomware in IoT networks based on energy consumption footprint, Journal of Ambient Intelligence and Humanized Computing, Volume 9, Issue 4, pp 1141–1152, August 2018.
[28] Kaur, Damandeep, and P. Singh, “Various OSI layer attacks and countermeasure to enhance the performance of WSNs during wormhole attack”,International Journal on Network Security 5(1) 2014, pp. 62.
[29] Reed, Damon, “Applying the OSI seven layer network model to information security”, SANS GIAC GSEC Practical Assignment Version 1.4 b Option One 2003.
[30] Mitrokotsa, A., Rieback, M. R., and Tanenbaum, A. S., “Classification of RFID attacks”, Gen, 15693 2010, Volume 12, Issue 5, pp 491–505, 2010.
[31] Li, H., Chen, Y. and He, Z., “The survey of RFID attacks and defenses,” 8th International Conference on Wireless Communications, Shanghai : Networking and Mobile Computing (WiCOM), 2012.
[32] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, 2017, pp. 32-37, doi: 10.1109/I-SMAC.2017.8058363, 2017.

[33] Barki, Amira, et al. “M2M security: Challenges and solutions”, IEEE Communications Surveys & Tutorials 18(2), 2016, pp. 1241–1254.
[34] Sicari, S., Rizzardi, A., Grieco, L., and Coen-Porisini, A. “Security, privacy and trust in Internet of Things The road ahead,” Computer Network, 76, pp. 146–164, Jan. 2015.
[35] Firdous, Syed Naeem, et al. “Modelling and evaluation of malicious attacks against the IoT MQTT protocol.” Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017 IEEE International Conference on. IEEE, 2017.
[36] Abdullahi Arabo, Ian Brown, and Fadi El-Moussa. Privacy in the age of mobility and smart devices in smart homes. In Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Conference on Social Computing (SocialCom). IEEE, 2012, pp. 819–826.
[37] Qiu, Yue, and Maode Ma. “A mutual authentication and key establishment scheme for m2m communication in 6lowpan networks”, IEEE Transactions on Industrial Informatics, 12(6) 2016, pp.2074–2085.
[38] Y. Lin, J. Huang, C. Fan and W. Chen, "Local Authentication and Access Control Scheme in M2M Communications With Computation Offloading," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3209-3219, Aug. 2018.
[39] Mahalle, Parikshit, et al. “Identity establishment and capability based access control (IECAC) scheme for Internet of Things.” WPMC. 2012.
[40] Mahalle, P. N., Anggorojati, B., Prasad, N. R., and Prasad, R. Identity authentication and capability based access control (iacac) for the Internet of things, Journal of Cyber Security and Mobility, 1(4), 2013, pp. 309–348.
[41] A. Esfahani et al., "A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 288-296, doi: 10.1109/JIOT.2017.2737630, Feb. 2019.
[42] Chen, Hsing-Chung, et al. “A security gateway application for End-to-End M2M communications,” Computer Standards & Interfaces, 44 2016, pp. 85–93.
[43] Mahalle, P., Babar, S., Prasad, N. R., and Prasad, R. (July). Identity management framework towards Internet of things (IoT): Roadmap and key challenges, In International Conference on Network Security and Applications (pp. 430–439), Berlin, Heidelberg: Springer, 2010.
[44] Dey, N., Hassanien, A. E., Bhatt, C., Ashour, A., and Satapathy, S. C. (Eds.). Internet of things and big data analytics toward next-generation intelligence, Berlin: Springer, 2018.
[45] Elhayatmy G., Dey N., Ashour A.S. (2018) Internet of Things Based Wireless Body Area Network in Healthcare. In: Dey N., Hassanien A., Bhatt C., Ashour A., Satapathy S. (eds) Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. Studies in Big Data, vol 30. Springer, Cham.
[46] Bhatt, C., Dey, N., and Ashour, A. S. (Eds.). Internet of things and big data technologies for next generation healthcare (Vol. 23). New York: Springer, 2017.
[47] Dey N., Ashour A.S., Bhatt C. (2017) Internet of Things Driven Connected Healthcare. In: Bhatt C., Dey N., Ashour A. (eds) Internet of Things and Big Data Technologies for Next Generation Healthcare. Studies in Big Data, vol 23. Springer, Cham
[48] Hassanien, A. E., Dey, N., and Borra, S. (Eds.). (2018). Medical Big Data and Internet of Medical Things: Advances, Challenges and Applications. CRC Press, Pub. location Boca Raton, eBook ISBN 9781351030380, 2018.
[49] Sarowar, M. G., Kamal, M. S., and Dey, N. (2019). Internet of Things and Its Impacts in Computing Intelligence: A Comprehensive Review – IoT Application for Big Data. In N. Dey, and S. Tamane (Eds.), Big Data Analytics for Smart and Connected Cities (pp. 103-136). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-6207-8.ch005

[50] Kimbahune, V. V., Deshpande, A. V., and Mahalle, P. N. Lightweight key management for adaptive addressing in next generation internet. International Journal of Ambient Computing and Intelligence (IJACI), 8(1), 2017, pp.50–69.
[51] Parne, B. L., Gupta, S., and Chaudhari, N. S. Segb: Security enhanced group based aka protocol for m2m communication in an IoT enabled LTE/LTE – a network, IEEE Access, 6, 2018, pp. 3668–3684.
[52] Wang, K., Du, M., Sun, Y., Vinel, A., and Zhang, Y. Attack detection and distributed forensics in machine-to-machine networks, IEEE Network, 30(6), 2016, pp. 49–55.
[53] Broustis, I., Sundaram, G. S., & Viswanathan, H. Detecting and preventing machine-to-machine hijacking attacks in cellular networks, Bell Labs Technical Journal, 17(1), 2012, pp. 125–140.
[54] Doh, I., Lim, J., Li, S., and Chae, K. July). Key establishment and management for secure cellular machine-to-machine communication. In 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013, (pp. 579–584). IEEE.
[55] Purohit, Kamlesh C., et al. “Hybrid approach for securing IoT communication using authentication and data confidentiality.” 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall). IEEE, 2017.

R. Thirukkumaran and P. Muthu Kannan

4 Security issues and trust management schemes in Internet of things

Abstract: Internet of things (IoT) is an emerging research field in the network domain and is applied to almost all the applications that can change the people's lives as smart. Moreover, in some cases, large volumes of sensitive data could be generated. The number of security threats related to infrastructure, platform and application of IoT has been increased over the last few years. Hence, it is necessary to apply proper security solutions that ensure privacy and confidentiality of data. To address the secure and reliable communication, various trust-based solutions were introduced. Most of the nodes in IoT system are heterogeneous and have limited storage space. Many of the existing trust-based solutions could not be able to achieve this requirement. This chapter provides a detailed review of the security challenges and trust management techniques adopted for IoT to secure data in a cloud environment.

Keywords: Internet of things, M2M communication, threat analysis, IoT protocols, attacks

4.1 Inroduction

The term Internet of things (IoT) is very popular in current research and industrial development [1]. In IoT, all the "things" also called as objects will be connected cooperatively to provide seamless communication and smart services. This enables "things" that can be accessed from anywhere at any time. In the beginning, M2M (machine-to-machine) communication protocols were focused by many researchers in the field of IoT, which are entirely different from the general communication of network in the aspect of deployment environment and the characteristics [2]. Along with the basic principles of authorization, integrity, authentication, availability and confidentiality, the network and security and privacy of the information should be equipped. IoT would be a significant part of the economy in the world rather than the Internet.

IoT is a technological revolution that has recently become more important to the real world as there are more than billion devices that connect to the Internet due to the growth of smart devices, embedded and ubiquitous communication technologies. The main components of IoT are the sensor, actuator, network, platform, services and users. IoT devices are combined with the cyber world to provide many smart services for different application domains like agriculture, energy, health care, retail market, logistics and industrial process [3]. They generate large volumes

https://doi.org/10.1515/9783110628517-005

of data that are valuable but not protected due to the nature of device constraints. The wireless sensor network (WSN) is one of the most important parts of IoT to collect data from end devices.

IoT and big data analytics are the promising technologies that address next-generation intelligence for various applications [4]. IoT applications promise to bring immense values into our lives. With newer wireless networks, superior sensors and revolutionary computing capabilities, the IoT could be the next frontier in the race for its share of the wallet [5]. A growing portion of IoT devices will be created in future, which includes connected vehicles, home automation, wearable technology, connected health, health-care analytics, industrial automation, smart agriculture, environmental monitoring and appliances with remote monitoring capabilities [6–8].

The communication between the IoT devices, cloud platform and users should consider proper security solutions to protect data because the sensor devices have limited capacity of power, computation and memory. IoT-enabled services are particularly creating and facing new challenges in security and privacy concerns. All the devices in the IoT are still subject to traditional security issues such as data confidentiality, integrity, availability and privacy. Intruders or attackers can target the data violation, bandwidth consuming and utilizing processing capacity of devices in the IoT-enabled network. The designing of security measures in IoT is quite challenging and should address the secure communication between sensor to sensor, the sensor to a gateway, gateway to server and server to the user.

4.2 IoT network components

IoT is an emerging and fast developing technology that connects billions or trillions of heterogeneous devices. The transformation process of interfacing, objects and smart devices to the network in order to function proficiently and remotely is the main objective of IoT. IoT is visualized as a completely connected world that makes it possible to represent the real world in a digital manner. The network interconnected devices implanted in the physical environment to improve the existing process [9]. Figure 4.1 illustrates various components of IoT network. IoT application covers most of the real-world business market like smart cities, industries, smart health and smart logistics.

4.2.1 IoT device

A sensor or an actuator along with the communication component constitutes an IoT device [10]. The principal component of IoT is sensor, which transmits the information gathered from the surrounding environment to the cloud server. There are

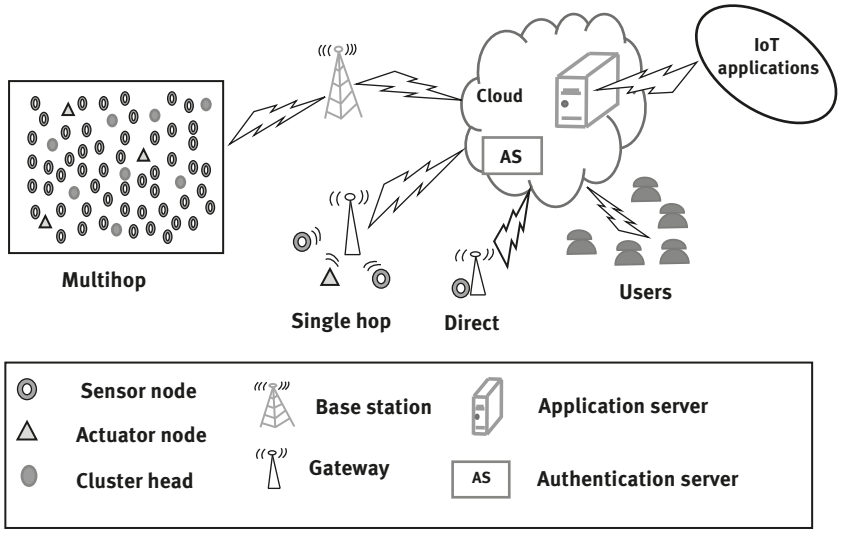


Figure 4.1: IoT network components.

numerous sensors available for various applications. Some of the usually utilized sensors are pressure sensor, sound sensor, temperature sensor, moisture sensor, light sensor, humidity sensor and others, in current and future applications. Sensors such as accelerometers are used for patient monitoring, biosensors for food testing, image sensor in surveillance, motion detectors in games and simulations.

IoT devices can make decisions locally, after aggregation and filtration of the collected information whenever central or global control is not required, reducing the processing and data transmission. By nature, IoT devices are heterogeneous, which vary in terms of communication protocols, computational and storage capabilities.

4.2.2 Connectivity

Connectivity represents the medium through which the gathered information from the IoT device is sent to the cloud infrastructure. The communication protocols such as Wi-Fi, ZigBee, radiofrequency identification, near-field communication, cellular networks, Bluetooth, wide area networks and satellite networks can be used to transport the collected data from the sensor to the cloud infrastructure [11]. Low-power wireless technologies such as Bluetooth, Wi-Fi, LoRaWAN and Z-Wave connect the smart devices and the sensors. Connectivity has its own advantages and disadvantages in terms of data transfer rate, efficiency and power.

4.2.3 Gateways

The data traffic between protocols and various networks are managed by the IoT gateway in a bidirectional manner. Gateway ensures the interoperability of the associated devices and sensors, also the translation of various network protocols. Configuration of the gateway includes the local preprocessing of the information gathered from a huge number of sensors before transmitting to the subsequent stages. In certain situations, it would be important due to the compatibility of the protocols such as Transmission Control Protocol (TCP) and Internet Protocol (IP). The information is transmitted through the IoT gateway ensuring network security with higher encryption standards. In order to protect the network from unauthorized access and malicious intruders, IoT gateway acts as a middle layer between the cloud and the devices.

4.2.4 Cloud

IoT generates large volume data from devices, applications, and users which must be managed in an efficient way. IoT cloud offers many service tools to collect, process, manage and store huge amount of data in real time [12]. It also provides a predictive analytics-based solution to enhance processes and products. To manage billions of devices and data traffic, IoT cloud is provisioned with high-performance server and storage. The application server, storage server, authentication and authorization server, message broker and IoT platform are the main components in the IoT cloud.

4.2.5 Services

An application consists of single or multiple services. It monitors and collects data from IoT devices and manages to store data. Further, it handles user authentication and access control policies. For example, in the smart city application environment monitoring, smart parking, transport system and water monitoring are the main services [13].

4.2.6 Users

User interface in the cloud environment provides the facility to interact user with the devices through different services [14]. By registering with different services, user can able to get the status of the devices and control it from anywhere. If any changes happened in the devices, the system generates alert and based on that user can react.

4.3 Security in IoT

In day-to-day life, the number of interconnected things drastically increases in various domains like industries, logistics, health and smart cities. More than 50 billions of interconnected devices are expected by 2020 [15]. Moreover, most of the IoT devices are resource-constrained devices due to their limited processing, memory and battery resources. When IoT devices are connected to the Internet, they are more vulnerable to the malicious attackers than PC and smart phones [16]. IoT devices generate a huge amount of valuable data like user location, health details and home security details that are unsecured due to lack of proper security protection.

IoT devices must authenticate themselves for each data communication between the server. When the IoT device or user wants to connect to the network, it should correctly identify their identity and credentials to grant access for authorization [17]. IoT is an emerging and fast developing technology but has no proper reference model and standards. It leads most of the security solutions that are not applicable to the IoT environment. New security solutions should be implemented to enhance the protection level of the IoT devices [18]. The explosion of the number of devices and users generates a large amount of data and it brings a new set of risk and security threats. The important challenges due to various technologies that drive and move forward the IoT into next level are discussed by Tan et al. [19].

Through the study of existing available resources, it has been clearly stated that IoT devices and users are severely affected by various security threats. Major security issues in IoT are the insecure network services, insecure web interface, insecure mobile interface, insecure cloud interface, insufficient authentication, insufficient authorization and lack of security configuration. Hence, it leads to a serious requirement for analyzing different security challenges in the IoT network.

Proactive measures such as cryptography and authentication are implemented as a first-line defense method. These mechanisms effectively protect the attacks from outside the network but fail to detect them from inside the network. The reactive measures are detection mechanism that dynamically monitors and decides whether the events are normal or of an attack. This research focuses on the reactive mechanism.

4.4 Security threats

The number of security threats directly relates to IoT devices that have increased over the last years [20]. The threats and risks are listed in Table 4.1. It shows that attacks take place at different levels in the infrastructures and throughout the process involved in the IoT ecosystem. The major attacks and their impacts are discussed in this section.

Table 4.1: Security threats and impacts.

Threat	IoT device	Platform	Infrastructure	Data	Communication	Decision	Application
Malware	✓	✓	×	×	×	×	×
Exploit kits	✓	×	✓	×	×	×	×
Targeted attacks	×	✓	✓	✓	×	×	×
DDoS	✓	✓	✓	×	×	×	×
Counterfeit	✓	×	✓	×	×	×	×
Attacks on privacy	✓	✓	×	✓	×	×	×
Modification of data	✓	✓	×	✓	×	×	×
Man in the middle	✓	×	×	✓	✓	×	×
Protocol hijacking	✓	×	×	✓	✓	✓	×
Session hijacking	✓	×	×	✓	✓	×	×
Data interception	✓	×	×	✓	✓	×	×
Network reconnaissance	✓	×	✓	✓	✓	×	×
Data gathering	✓	×	×	✓	✓	×	×
Replay of messages	✓	×	×	✓	×	✓	×
Data leakage	✓	✓	×	✓	×	×	×
Software vulnerabilities	✓	✓	✓	×	×	×	✓
Device modification	✓	×	×	×	✓	×	×

✓ represents the impact; × the no impact

4.4.1 IoT attacks

Against IoT device

This type of attackers modifies the configuration of sensors and actuators like generate out-of-range sensor values and changing the threshold value of the sensor to detect the event during installation time. Due to wireless nature, sensor network has led to the vulnerability of attacks either from inside or outside the networks. If one sensor were compromised, it could be identified by using the readings obtained from another sensor [21]. But in IoT, large number of sensors are deployed and attack also targeted to multiple devices at the same time. Packet dropper, data modifier, selfish node, Sybil, node replication, flooding, distributed denial of service (DDoS) and man in the middle are some of the attacks found in sensor networks [22–29].

Against server

This type of attacker comprises different stages to gain the server admin control of an IoT system [30]. It can be easily achieved if a weak authentication method is used. An attack in IoT admin server could affect the communication between devices and disabled the devices.

Against the network link between controller and actuators

The main impact of this type of attack is the leakage of sensitive and operational information. The advanced persistent threat (APT) attacks, eavesdropping and information gathering are the types of attack that identify a weak spot in the network and devices and further it can able to do attack and malicious activities [31].

4.4.2 Method of attacks

Exploits

This type of exploitation is successful. It creates an entry point to the system and may crash the system, making it as the unstable one. These exploits are generated by malware and are used to get access to an unauthorized restricted system. It is worked as part of a larger attack and leads to launch of other malicious contents to the network.

Command inject

This type of attacker launches or injects command into IoT devices and executes malfunction remotely through a console. If one system is getting compromised through that machine, then the attacker is able to attack another system in the same environment. It creates a chain of multiple compromised devices.

Steppingstone attack

This is one of the anonymous attacks used by the intruders by hiding their identities. In the first step, the attacker compromises some nodes in the network. Then by using that compromised node identity, attacker moves a step forward to attack another set of nodes in the network. Further, this process is continued to attack the entire network.

IoT botnet

This type of attack finds the list of vulnerable devices in IoT by sending exploits and enrolling them into botnet after that it launches a DDoS attack, flooding attack, and targets the server with malicious traffic [32].

Ransomware

It has many possible targets within the IoT through malware patching into the system. This type of attack blocks the access of data from the victim and also its request to pay for access grant. It can able to hold a power grid, a smart thermostat and a hospital system, and makes the risk for the safety of the people [33].

4.4.3 Security challenges in IoT

Security is a very important aspect as well as a challenge for implementing IoT solutions, rather than considering the benefit of IoT, where inappropriate access and privacy are the main categories of the top list [34]. Moreover, it is necessary to maintain proper authorization because these devices are open networks in which any device can join and communicate with any other devices [35]. With the adoption of new technologies, the IoT environment has become complex, and privacy issues have become more complicated [36]. Furthermore, because of terminal equipment, network structure, scene and other factors of IoT, these concerns are rising,

respectively [37]. Moreover, with a traditional firewall or authentication, protocols or keychain pair might not offer a solution [38].

From the aspect of security and technology, the safety of IoT especially accesses control of miniaturized things that have become the most challenging one. Hence, the access control system (ACS) design will address features such as a solution to eradicate the threats of privacy and security, related with IoT, the solution to protect security [39]. Most of the existing access control methods are based on role-based access control (RBAC), attribute-based access control (ABAC) and access control list (ACL) [40].

ACS allows accessing resources like IoT device, sensor or URL file only for authorized users [41]. Due to lower bandwidth in IoT devices, low power requirements, ad hoc and distributed systems nature, a unique set of access control challenges are increasing. The standard authorization models must be analyzed in depth before applying them to the IoT.

The role of wireless infrastructure in IoT applications is expected to become more prominent with the deployment of mobile nodes and WSNs [42]. If the WSNs are being open to Internet connectivity, it becomes more vulnerable to attackers from anywhere in the world [43].The important challenges due to various technologies that drive and move forward the IoT into next level are discussed in this section [44].

Availability

To achieve persistent connectivity between end devices, users and their respective services, new technologies have to be designed [45]. The power constraints of lightweight endpoints should be addressed in secure communication. Low-power wide area network should be implemented with the same level of security used in recent mobile communication [46]. During the migration of the IoT endpoints across network boundaries, the same level of security should be supported by the multiple mobile operators [47], which need to address how the network trust can be forwarded from gateway to endpoint communication.

Identity

In an IoT product or service echo system end-point device should be securely identify itself to its peers and services. This is a critical and fundamental aspect to guarantee the data is being delivered to the certified peers and services [48]. In IoT environment services and peers should verify the identity of the end-user and end-point device. Focusing security technology should be capable of securely authenticating peers and services. The identity of a device should be secured from tampering and manipulation.

Privacy

Privacy must be designed to ensure that each action is authorized, device identity is verified, and the data are not exposed to unauthorized users [49]. All the physical world entities are directly affected by digital world actions. It should be considered during the design of the architecture of the endpoint device or service.

Scalability

Scalability is defined as that increase in the number of nodes after the deployment of WSN [50]. The expansion support of the networking protocol is very important in the design of the protocol. The design of the services, protocols and the endpoint devices should ensure that they are scalable under varying load conditions.

Secure routing

Routing and data forwarding is an important service for allowing communication in WSNs and IoT [51]. Existing routing protocols suffer from several security vulnerabilities.

To overcome different security threats in the IoT network, the trust-based mechanism is developed; hence, the next section provides a detailed review of existing trust-based security mechanism adopted in IoT

4.5 Trust management in IoT

This section briefs the existing trust management (TM) schemes and their related application. Further, the challenges in trust-based security solutions and the outcome of this survey are outlined.

4.5.1 Trust management

TM plays a vital role in IoT for enhanced user information security and privacy, for the process of data fusion and data mining and for the qualified data services with intelligence, whereas reputation is a measure to assess the trust level which is put into an entity that is derived from the experiences or knowledge (direct or indirect) on earlier interactions of entities [52].

Trust

The behavior of the node or data is classified as good or bad based on the trust value. A trustor and a trustee are the two entities involved in a trust relationship, and for mutual benefits, they rely on each other. The relationship of trust resides in the context such as the trust environment, the purpose of the trust, and the risk of trust [53].

Direct trust

Direct trust is a technique which is based on experiences or observations, direct interactions between the two entities that are the trustor node and the trustee node [54].

Indirect trust

In indirect trust, there are no past interactions or experiences for the trustor and the trustee. In such a scenario, based on the recommendations and opinion of the other nodes trust is built [55]. Indirect trust can be established if a subject node cannot directly observe the communication behaviors of the object node.

Recommended trust

Recommended trust calculates filtered reliable recommendations. The third-party recommendations are not reliable. Therefore, an effective solution needs to be addressed to detect and filter unreliable recommendations [56].

4.5.2 Trust management model

Most of the existing work calculates the trust value based on node behavior. In the wireless multihop environment, cooperation among neighbor nodes is important. The various applications of trust-based solution for the wireless environment are data aggregation, routing, node selection, localization and malicious attacker detection. Based on the management scheme, trust models can be classified into centralized and distributed. In the distributed approaches, all the participating nodes can be able to calculate their trust values. The base station or any server is used to calculate the trust value for all nodes in the centralized approach. This approach may not be suitable for all applications because this management consumes more energy. In the IoT context, both distributed and centralized approaches can be used

in the different level. The distributed approach is used for device–device communication and centralized approach is used in the user ACS [57].

Several studies developed TM models to enhance security and privacy but based on the architecture modeling of IoT [58]. This research splits IoT into three layers based on the network composition of IoT, namely the application layer, the core layer, and the sensor layer. TM mechanism is deployed in these layers for multiservice, effective routing and malicious detection [59]. The selection of metrics is based on the kind of attacks that we are going to defend. In each layer different metrics are collected for trust calculation. The selection of a computing method is also an important one. Some of the methods are a weighted average method, probability theory, fuzzy logic, game theory and machine learning concepts. The trusted authority or ACS is responsible for taking the final decision based on trust information.

4.5.3 Trust-based applications

TM scheme provides solutions for security issues in routing, clustering, target localization, malicious node detection and ACS. In this section, applications of trust model are discussed.

Routing

Routing is generally carried in IoT for the sensor network, which is used for multihop communication [60]. From the sensor devices, data should be forwarded through intermediate nodes to the base station or gateway. Presence of malicious nodes in the network causes the routing behavior. This section discusses the implementation of secure routing through TM scheme.

Airehrour et al. [61] introduced a lightweight trust-based routing framework called SecTrust. The trust value is calculated based on the past successful interactions of the IoT device communication. Based on the trustworthiness, routing attackers are isolated from the network.

Khan et al. [62] illustrated a resilient routing mechanism for low power and lossy network using the trust. Each node in the network computes trust value using trust metrics like belief, disbelief and uncertainty.

Cluster

The IoT devices are grouped together to form a cluster. The clustering method provides an efficient way to forward data from devices to base station or gateway. Cluster-based techniques in IoT achieve energy efficient by minimizing the number of

control packets used in network communication. The selection of cluster head (CH) is challenging in terms of selection parameter and selection method. Many techniques were proposed to select CH and cluster member (CM) assignment. The CH selections are broadly classified as centralized and distributed. In IoT context distributed approach gives good performance [63]. CM senses the environment and sends the information to CH. Further, it forwards to base station or gateway in most of the IoT-enabled WSN application scenario. Many trust-based solutions and access control methods are proposed for secured communication [64]. The objective of secure, energy and bandwidth-aware CH selection is not addressed by many of the research work. In general, CH is elected based on node degree, delay, distance and energy.

Rani et al. [65] illustrated a minimum energy consumption chain-based cluster coordinator algorithm (ME-CBCCP) for the energy-efficient IoT. A hierarchical network design was introduced based on different communication levels like local cluster communication, intercluster communication and cluster-to-base station communication. The cluster coordinators balance the load of the CH. The network lifetime and delay performance of the ME-CBCCP were analyzed.

Tsai and Chen [66] presented virtual CH election method for the WSN. By applying virtual ID concept, it avoids nearby CHs and also fully covers all cluster nodes. For energy-efficient CH election highest residual energy parameter is also considered. The performance analysis carried in terms of the number of live nodes, energy consumption and the number of CH elected.

Praveen Kumar Reddy and Rajasekhara Babu [67] demonstrated the CH election method using the combination of gravitational search algorithm and artificial bee colony algorithm for the IoT-enabled WSN. It takes the distance, delay, energy, load and temperature parameters of the sensor devices to select the CH. The performance of this algorithm analyzed in terms of network sustainability and convergence evaluation.

John et al. [68] introduced a dynamic CH election method for IoT applications. The large-scale network area is divided into small clusters with a minimum coverage area by using the Voronoi diagram. The CH is selected at two stages. First one is based on perceived probability and the second one is based on survival time estimation method. The performance analysis shows the improvement in energy savings and network lifetime.

Karthick [69] demonstrated a secure and energy-aware routing protocol for the WSN. At the initial stage, *k*-means clustering is used later on based on link quality appraisal parameter of nodes' grade points. By using trust and distrust concept, secure path is established. The performance of the proposed system is analyzed in terms of throughput, delay and energy consumption.

Bader et al. [70] presented a CH selection scheme for IoT-enabled sensor network by using trust value. Only the trusted nodes were selected as CH. The trust value is computed based on successful interaction. The forgetting factor is used to assign a different weight value for old entries in the history.

Secure localization

Target localization and tracking is an important application for IoT. To track the exact location of the moving object and to find the event-generated position are challenging one. The location spoofing attacks are the major risk of implementing localization in IoT. The localization method utilizes the reference position information from the neighbor nodes. If the reference node is a malicious node, then the result of the localization will get an error. Several existing methods are proposed to avoid malicious nodes. This section discusses some of the secure localization methods used in IoT environment.

Zhang et al. [71] demonstrated secure localization using a trust evaluation method called trust-based secure localization. Final trust value is computed based on identity and behavior. The identity is evaluated based on an authentication method. If the authentication fails, the parameter is set to zero. The behavior evaluation parameter is calculated by using both self-evaluation and reference evaluation method. It uses transmission radius of the beacon node and distance between the position claimed node and the position estimated node. For the attackers, the final trust value will be low. To find the localization of the node, the reference location information is gathered from trustworthy nodes. This method ensures the secure location information.

Chen et al. [72] presented a detailed survey about security and privacy issues in localization, location information and location-based services. Cryptographic solutions were addressed to secure localization.

Zhang et al. [73] presented the framework of secure location of things for geospatial tagging in the IoT. Further, the impact of spoofing attacks in traditional localization algorithm was analyzed. Based on the reachability of access point the suitability information is scored. This algorithm calculates the maximum likelihood estimator to find the tag location.

Access control system

ACS allows accessing resources like sensors, actuators, medical equipment and data in the server only for authorized users. Due to lower bandwidth between the Internet and IoT devices, low power requirements of IoT devices, network ad hoc, systems distributed nature, a unique set of access control challenges are presented by IoT. The standard authorization models must be analyzed in depth before applying them to the IoT, which includes RBAC, ABAC and ACL.

Mahalle et al. [74] presented trust-based access control using the fuzzy approach based on identity management using the trust level. To address access control in IoT, the fuzzy-based approach for trust calculations deals with the linguistic information of devices. Simulation results demonstrate that the fuzzy approach for trust-based

access control guarantees scalability and it is energy efficient. Finally, the most important works that emphasize access control in an IoT environment are discussed.

Yeh et al. [75] developed a technique of cloud-based fine-grained in health care for access control using lightweight IoT devices with attribute revocation functions and data dynamics auditing. This proposed scheme handles the problem of cloud reciprocity, wherein cloud service providers reduce the amount of data loss that occurs in the network system. Experimental analysis of the results shows that the proposed approach exhibits significant security analysis and performance comparisons, which makes it an excellent design for cloud-based PHI system.

Authorized users of each resource are stored by the ACL, that is, the matrix of access control that stores in a row-wise order. This is a major challenge for IoT because it is hard to update the user list in a distributed system due to low processing power in devices [76].

A widely used protocol is an RBAC system that designs and builds access control. It provides security for the system regarding authorization, but the ACS and authentication provide critical functionalities even in the Internet resource access. Further, there are three perspectives of role-based access model such as the end user, access control and administrator [77].

A different approach to authorization is provided by ABAC as it provides access based on specific attributes of the user [78]. By combining both attributes and other data such as Mac address, the location and IP address, this method provides a better ACS. It combines various attributes to make a context-aware decision instead of using an authorized user role for a sensor at runtime [79].

4.5.4 Challenges in trust-based security solutions

Trust and reputation system face some of the challenges such as heterogeneity, scalability, infrastructure, identity, integrity, and network resources.

Trust and reputation systems must consider the heterogeneity as the first challenge. Because the future Internet will exhibit high heterogeneity levels like web-enabled, digital virtual and cyber-physical [80]. The second challenge is scalability. To stay fully functional, the trust and reputation system must scale with the growth in the number of devices [81]. Trust and reputation systems must consider infrastructure as the third challenge. Because it collects information from the public area. Most of the entities need others to interact with them and also they must be able to find them within the network [82]. Both challenges and the opportunity to improve security are offered by identity management in IoT [83]. The underlying mechanism and identity of things are not the same, and it is the most important aspect of this challenge [84].

The prevention of unauthorized modification to hardware and software is ensured by the concept of integrity. Authorized or unauthorized personnel does not

do an unauthorized modification of data, and that data should be internally and externally consistent [85]. The last challenge is exhibited from connections of various things and different network capabilities [86]. This means that bandwidth, availability and the latency difference must be considered especially if certain aspects of the interactions are critical in a time.

4.5.5 The outcome of the survey

To design efficient trust-based security solution, the following set of points needed to be considered:

Trust model should be lightweight and easy to implement. Trustworthiness of the nodes should be continuously updated. If the numbers of interactions between the nodes are increased, the trust value can be able to achieve a good level of accuracy. For the recommendation approaches, we need to select proper filtering and aggregation models to remove unwanted recommendation. Trust model should consider different attacks. Need more flexibility to integrate data trust, device trust and user trust based on the application use-case.

4.6 Conclusion

To protect the data in an IoT network, TM scheme has been widely used and hence this review examines the TM scheme for securing data in the IoT in different aspects. The chapter reveals that even though the TM scheme provides a significant advantage for various threats, yet it requires some effective modification.

References

[1] Da Xu, Li., Wu, He. and Shancang, Li. Internet of Things in industries: A survey, IEEE Transactions on Industrial Informatics, 10(4), 2013, pp. 2233–2243.

[2] Sathish Kumar, J. and Patel, Dhiren R.. A. survey on Internet of Things: Security and privacy issues, International Journal of Computer Applications, 90(11), 2014, pp. 20–26.

[3] Sarowar, M G., Kamal, M S. and Dey, N. Internet of Things and its impacts in computing intelligence: A comprehensive review–IoT application for big data, In Big Data Analytics for Smart and Connected Cities (pp. 103-136). Hershey, PA: IGI Global, doi:10.4018/978-1-5225-6207-8.ch005.

[4] Elhayatmy, G., Dey, N. and Ashour, A S. (Eds.)Internet of Things based wireless body area network in healthcare, In Internet of things and big data analytics toward next-generation intelligence, Cham : Springer, 2018, pp. 3–20.

[5] Dey N., Hassanien, A. E., Bhatt, C., Ashour, A. and Satapathy, S C. (Eds.). Internet of things and big data analytics toward next-generation intelligence, Berlin : Springer, 2018.

[6] Hassanien, A. E., Dey, N., and Borra, S. (Eds.). Medical Big Data and Internet of Medical Things: Advances, Challenges and Applications, CRC Press, 2018.
[7] Bhatt, C., Dey, N., and Ashour, A. S. (Eds.). Internet of things and big data technologies for next generation healthcare, 23, New York : Springer, 2017.
[8] Dey, N. Ashour, A. S. and Bhatt C. (Eds.)Internet of things driven connected healthcare, In Internet of things and big data technologies for next generation healthcare, Cham : Springer, 2017, pp. 3–12.
[9] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. Internet of Things (IoT): A vision, architectural elements and future directions, Future Generation Computer Systems, 29(7), 2013, pp. 1645–1660.
[10] Jovovic, I., Forenbacher, I. and Perisa M. Massive machine-type communications: An overview and perspectives towards 5G, 3rd International Virtual Research Conference in Technical Disciplines, DOI: 10.18638/rcitd.2015.3.1.73 2015.
[11] Atzori, L., Iera, A. and Morabito, G. The Internet of Things: A survey, Computer Networks, 54 (15), 2010, pp. 2787–2805.
[12] Kantarci, Burak and Mouftah, Hussein T. Trustworthy sensing for public safety in cloud-centric Internet of Things, IEEE Internet of Things Journal, 1(4), 2014, pp. 360–368.
[13] Mohammed, Farah Hussein. and Esmail, Roslan. Survey on IoT services: Classifications and applications, International Journal of Science and Research, IJSR, 4(1), 2015, pp. 2124–2127.
[14] Shelby, Zach. Embedded web services, IEEE Wireless Communication, 17(6), 2010, pp. 52–57.
[15] Asghar, MH., Negi, A. and Mohammadzadeh, N. Principle application and vision in Internet of Things (IoT), International Conference on Computing, Communication &Automation, IEEE, 2015, pp: 427–431.
[16] Padmavathi, G., Shanmugapriya, D. A survey of attacks, security mechanisms and challenges in wireless sensor networks, International Journal of Computer Science and Information Security, IJCSIS, 4(1 & 2), 2009, pp. 1–9.
[17] Kim, Hokeun., Wasicek, Armin., Mehne, Benjamin and Lee, Edward A. A secure network architecture for the Internet of Things based on local authorization entities, IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud, 1, 2016, pp. 114–122.
[18] Waz, Ibrahim R., Sobh, Mohamed Ali and Ayman, M Bahaa-Eldin. Internet of Things (IoT) security platforms, 12th International Conference on Computer Engineering and Systems, ICCES, 2017, pp. 500–507.
[19] Tan, L. and Wang, N. Future internet: The Internet of Things, 3rd International Conference On Advanced Computer Theory and Engineering, ICACTE, 2010, pp. 376–380.
[20] Gautam, G. and Sen, B. Survey on different types of security threats on wireless sensor networks, International Journal of Computer Science and Information Technologies, 6(1), 2015, pp. 770–774.
[21] Cai, Jiwen., Ping Yi, Jialin Chen, Zhiyang Wang and Ning Liu. An adaptive approach to detecting black and gray hole attacks in ad hoc network, IEEE International Conference on Advanced Information Networking and Applications, 2010, pp. 775–780
[22] Wang, Chuang, Feng, Taiming, Kim, Jinsook, Guiling, Wang and Zhang, Wensheng. Catching packet droppers and modifiers in wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems, 23(5) 2012, pp. 835–843.
[23] Prathap U., Shenoy, P. D. and Venugopal, K. R. CPMTS: Catching packet modifiers with trust support in wireless sensor networks, IEEE International WIE Conference on Electrical and Computer Engineering, WIECON-ECE, 2015, pp. 255–258.
[24] Sowmyadevi, D. and Karthikeyan, K. Merkle-Hellman knapsack-side channel monitoring based secure scheme for detecting provenance forgery and selfish nodes in wireless sensor

networks, 2017 Second International Conference on Electrical, Computer and Communication Technologies, ICECCT, 2017.
[25] Zhang, K., Liang, X., Lu, R., and Shen, X. Sybil attacks and their defenses in the Internet of Things, IEEE Internet of Things Journal, 1(5) 2014, pp. 372–383.
[26] Chia-Mu, Yu., Tsou, Yao-Tung, Chun-Shien Lu. and Kuo, Sy-Yen. Localized algorithms for detection of node replication attacks in mobile sensor networks, IEEE Transactions on Information Forensics and Security, 8(5), 2013, pp. 754–768.
[27] Kamaldeep, Malik M., and Dutta, M. Contiki-based mitigation of UDP flooding attacks in the Internet of things, 2017 International Conference on Computing, Communication and Automation (ICCCA), IEEE, 2017, pp. 1296–1300.
[28] Yan, Q., Yu, F. R., Gong, Q. and Li, J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges, IEEE Communications Surveys & Tutorials, 18(1), 2016, pp. 602–622.
[29] Xu, Y., and Liu, F. Hybrid key management scheme for preventing man-in-middle attack in heterogeneous sensor networks, 2017 3rd IEEE International Conference on Computer and Communications, ICCC, 2017, pp. 1421–1425.
[30] Shikha Singh, Binay Kumar Pandey, Ratnesh Srivastava, Neharawat, Poonamrawat and Awantika. Cloud computing attacks: A discussion with solutions, Open Journal of Mobile Computing and Cloud Computing, 1(1), 2014, pp. 1–7.
[31] Liao, CH., Shuai, HH. and Wang, LC. Eavesdropping prevention for heterogeneous Internet of Things systems, 15th IEEE Annual Consumer Communications& Networking Conference (CCNC), 2018.
[32] Hachinyan, O., Khorina, A. and Zapechnikov, S. A game-theoretic technique for securing IoT devices against Mirai botnet, 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus, 2018, pp. 1500–1503.
[33] Sajjan, R. S. and Ghorpade, V. R. Ransomware attacks: Radical menace for cloud computing, International Conference on Wireless Communications, Signal Processing and Networking WiSPNET, 2017, pp. 1640–1646.
[34] Jin-cui, Yang and Bin-xing, Fang. Security model and key technologies for the Internet of things, The Journal of China Universities of Posts and Telecommunications, 18(2), 2011, pp. 109–112.
[35] Godha, R., Prateek, S. and Kataria, N. Home automation: Access control for IoT devices, International Journal of Scientific and Research Publications, 4(10), 2014, pp. 1–4.
[36] Pereira, Pablo Punal, Eliasson, Jens and Delsing, Jerker. An authentication and access control framework for CoAP-based Internet of Things, 40th Annual Conference of the IEEE Industrial Electronics Society ECON, IEEE, 2014, pp. 5293–5299.
[37] Fielding, R. T. and Taylor, R. N. Principle and design of the modern web architecture, ACM Transaction Internet Technol, 2(2), 2002, pp. 115–150.
[38] Song, Y. Security in Internet of Things, THES, school of information and communication technology (ICT), KTH, http://kth.diva-portal.org/smash/get/diva2:702223/FULLTEXT01.pdf, 2013.
[39] Liu, Jing, Xiao, Yang and Philip Chen, C.L. Internet of Things' authentication and access control, International Journal of Security and Networks, 7(4), 2012, pp. 228–241.
[40] Cruz-Piris, L., Rivera, D., Marsa-Maestre I., De La Hoz, E. and Velasco, J.R. Access control mechanism for IoT environments based on modelling communication procedures as resources, Sensors (Switzerland) 18(3), 2018, pp. 917.
[41] Ouaddah, Aafaf, Bouij-Pasquier, Imane, Abou Elkalam, Anas and Ait Ouahman, Abdellah. Security analysis and proposal of new access control model in the Internet of Thing, International Conference on Electrical and Information Technologies, ICEIT, IEEE, DOI: 10.1109/EITech.2015.7162936.2015

[42] Duan, J., Gao, D., Yang, D., Foh, C.H., and Chen, H-H. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications, IEEE Internet of Things Journal,1(1), 2014, pp. 58–69.
[43] Fagen, Li. and Xiong, Pan. Practical secure communication for integrating wireless sensor networks into the Internet of Things, IEEE Sensors Journal, 13(10), 2013, pp. 3677–3684.
[44] Said, Omar and Masud, Mehedi. Towards Internet of Things: survey and future vision, International Journal of Computer Networks IJCN2013, 5(1), 2013, pp. 1–17.
[45] Proano, Alejandro and Lazos, Loukas. Packet-hiding methods for preventing selective jamming attacks, IEEE Transactions On Dependable And Secure Computing, 9(1), 2012, pp. 101–114.
[46] Petajajarvi, Juha, Mikhaylov, Konstantin, Pettissalo, Marko, Janhunen, Janne and Jarilinatti. Performance of a low-power wide-area network based on LoRa technology: Doppler robustness, scalability, and coverage, International Journal of Distributed Sensor Networks, 13(3), 2017, pp. 1–16.
[47] Khan, R., Khan, S. U., Zaheer, R. and Khan, S. Future internet: The internet of things architecture, possible applications and key challenges, 10th International Conference On Frontiers of Information Technology (FIT), 2012, pp. 257–260.
[48] Keoh, Sye Loong, Kumar, Sandeep S and Tschofenig, Hannes. Securing the Internet of Things: A standardization perspective, IEEE Internet Of Things Journal, 1(3), 2014, pp. 265–275.
[49] Tabane, Elias and Zuva, Tranos. Is there a room for security and privacy in IoT?, International Conference on Advances in Computing and Communication Engineering, ICACCE, 2016, pp. 260–264.
[50] Compton, M., Barnaghi, P., Bermudez, L., Garca-Castro, R., Corcho, O., Cox, S., Graybeal, J., Hauswirth, M., Henson, C., Herzog, A., Huang, V., Janowicz, K., Kelsey, W. D., Phuoc, D. L., Lefort, L., Leggieri, M., Neuhaus, H., Nikolov, A., Page, K., Passant, A., Sheth, A., and Taylor, K. The SSN ontology of the W3C semantic sensor network incubator group, Journal of Web Semantics, 17, 2012, pp. 25–32.
[51] Teng, Liping and Zhang, Yongping. SeRA: A secure routing algorithm against sinkhole attacks for mobile wireless sensor networks, 2nd International Conference on Computer Modeling and Simulation, 2010, pp. 79–82.
[52] Chen, I.R., Guo, J. and Bao, F. Trust management for service composition in SOA-based IoT systems, IEEE Wireless Communications and Networking Conference, WCNC, 2014, pp. 3444–3449.
[53] Yan, Z., Zhang, P. and Vasilakos A.V. A survey on trust management for Internet of Things, Journal of Network and Computer Applications, 42, 2014, pp. 120–134.
[54] Eder, T., Nachtmann, D. and Schreckling, D. Trust and REPUTATION in the Internet of Things, conference seminar ss2013 – real life security (5827HS), https://web.sec.uni-passau.de/projects/compose/papers/Eder_Nachtmann_Trust_and_Reputation_in_the_Internet_of_Things.pdf, 2013.
[55] Raha, A., Naskar, M. K., Chakraborty, A., Alfandi, O. and Hogrefe, D. A novel indirect trust based link state routing scheme using a robust route trust method for wireless sensor networks, 5th International Conference on New Technologies, Mobility and Security, NTMS, 2012.
[56] Govindan, K., and Mohapatra, P. Trust computations and trust dynamics in mobile ad hoc networks: A survey, IEEE Communications Surveys & Tutorials, 14(2), 2012, pp. 279–298.
[57] Boswarthick, D., Elloumi, O., and Hersent, O. (2012). M2M Communications: A systems approach. Hoboken, N.J: ETSI. 2012.
[58] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. Internet of Things (IoT): A vision, architectural elements and future directions, Future Generation Computer Systems, 29(7), 2013, pp. 1645–1660.

[59] Lize, G., Jingpei, W. and Bin, S. Trust management mechanism for Internet of Things, China Communications, 11(2), 2014, pp. 148–156.
[60] Zhu, Jianping, Tao, Zhengsu and Chunfeng Lv. Performance improvement for IEEE 802.15.4 CSMA/CA scheme in large-scale wireless multi-hop sensor networks, IET Wireless Sensor Systems, 3(2), 2013, pp. 93–103.
[61] Airehrour, David, Gutierrez, Jairo and Ray, Sayan Kumar. A Lightweight Trust Design for IoT Routing, IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress, Auckland, New Zealand, IEEE, pp. 552–557, 2016
[62] Khan, Zeeshan Ali, Ullrich, Johanna, Voyiatzis, Artemios G and Herrmann, Peter A. Trust-based resilient routing mechanism for the Internet of Things,12th International Conference on Availability, Reliability and Security, ARES, 2017.
[63] Hamzeloei, Fahimeh, Dermany, Mohammad Khalily. A TOPSIS based cluster head selection for wireless sensor network, Procedia Computer Science, 98, 2016,pp. 8–15
[64] Al-Hamadi, Hamid and Chen, Ing-Ray. Trust-based decision making for health IoT systems, IEEE Internet of Things Journal, 4(5), 2017, pp. 1408–1419.
[65] Rani, Shalli, Talwar, Rajneesh, Malhotra, Jyoteesh, Ahmed, Syed Hassan, Sarkar, Mahasweta and Song, Houbing. A novel scheme for an energy efficient internet of things based on wireless sensor network, Sensors, 15(11), 2015, pp. 28603–28626.
[66] Tsai, Ming-Yu and Chen, Yaw-Chung. A virtual cluster head election scheme for energy-efficient routing in wireless sensor networks, 3rd International Conference on Future Internet of Things and Cloud, 2015, pp. 341–348.
[67] Praveen Kumar Reddy M. and Rajasekhara Babu M. Energy efficient cluster head selection for Internet of Things, New Review of Information Networking, 22(1), 2017, pp. 54–70.
[68] John, Aniji, Rajput, Anagha, Babu, Vinoth. Dynamic cluster head selection in wireless sensor network for internet of things applications, IEEE International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology, ICIEEIMT, (2017), pp 45–48.
[69] Karthick, Suyambu. TDP: A novel secure and energy aware routing protocol for wireless sensor networks, International Journal of Intelligent Engineering and Systems, 11(2), 2018, pp. 76–84.
[70] Bader A., Ali Hanady M., Abdulsalam and Alghemlas, Aseel. Trust based scheme for IoT enabled wireless sensor networks, Wireless Personal Communications, 99(2), 2018, pp. 1061–1080.
[71] Zhang, Ting, Jingsha He and Zhang, Yang. Trust based secure localization in wireless sensor networks, International Symposium on Intelligence Information Processing and Trusted Computing, 2011, pp:55–58.
[72] Chen, Liang, Thombre, Sarang, Jarvinen, Kimmo, Lohan, Elena Simona, Al´en-Savikko, Anette, Leppakoski, Helena, Zahidul, M., Bhuiyan, H., Bu-Pasha, Shakila, Ferrara, Giorgia Nunzia, Honkala, Salomon, Lindqvist, Jenna, Ruotsalainen, Laura, Paivi Korpisaari and Kuusniemi, Heidi. Robustness, security and privacy in location-based services for future IoT: A survey, IEEE Access, 5, 2017, pp. 8956–8977.
[73] Zhang, Pengfei, Nagarajan, Sai Ganesh, and IdoNevat. Secure Location of Things (SLOT): Mitigating localization spoofing attacks in the Internet of Things, IEEE Internet of Things Journal, 4(6), 2017, pp. 2199–2206.
[74] Mahalle, Parikshit N., Thakre, Pravin A., Prasad, Neeli Rashmi and Prasad, Ramjee. A fuzzy approach to trust based access control in Internet of Things, Wireless VITAE, IEEE, 2013, pp. 1–5.

[75] L. Yeh, P. Chiang, Y. Tsai and J. Huang, "Cloud-Based Fine-Grained Health Information Access Control Framework for LightweightIoT Devices with Dynamic Auditing andAttribute Revocation," in IEEE Transactions on Cloud Computing, 6(2) 2015, pp. 1–13.

[76] Suominen, Ilpo. Access control for Internet of Things – Intopalo. [Online], https://www.intopalo.com/blog/2015-05-25-access-control-for-internet-of-things/, 2015.

[77] Habib, Muhammad Asif, Ahmad, Mudassar, Mahmood, Nasir and Ashraf, Rehan. An evaluation of role based access control towards easier management compared to tight security, International Conference on Future Networks and Distributed Systems – ICFNDS '17, New York, New York, USA : ACM Press, 2017, pp. 1–6.

[78] Wang, Junshe, Wang, Han, Zhang, Hongbin and Cao, Ning. Trust and attribute-based dynamic access control model for Internet of Things, International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, IEEE, 2017, pp. 342–345.

[79] Monir, S. A lightweight attribute-based access control system for IoT, University of Saskatchewan, https://ecommons.usask.ca/bitstream/handle/10388/7556/MONIR-THESIS-2016.pdf?sequence=1, 2017.

[80] Sundmaeker, Harald, Guillemin, Patrick, Friess, Peter and Woelfflé, Sylvie. Vision and challenges for realizing the Internet of Things,[online], http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf, 2010.

[81] Evans, D. The Internet of Things – how the next evolution of the internet is changing everything, CISCO white paper, 1, 2011, pp. 1–11.

[82] Cho, J.H., Swami, A. and Chen, I.R. A survey on trust management for mobile ad hoc networks, IEEE Communications Surveys & Tutorials, http://ieeexplore.ieee.org/document/5604602/, 13 (4), 2011, pp. 562–583.

[83] Mahalle, P., Babar, S., Prasad, N. R., and Prasad, R. (July). Identity management framework towards internet of things (IoT): Roadmap and key challenges, In International Conference on Network Security and Applications Berlin, Heidelberg : Springer, 2010, pp. 430–439.

[84] Roman, Rodrigo, Alcaraz, Cristina, Lopez, Javier and Sklavos, Nicolas Key management systems for sensor networks in the context of the Internet of Things, International conference on Computers and Electrical Engineering 37, 2011, pp. 147–159

[85] Hintzbergen, Jule, Hintzbergen, Kees, Smulders, André and Baars, Hans. Foundations of information security based on ISO27001 And ISO27002 (Best Practice), Van Haren Publishing, Zaltbommel, https://www.vanharen.net/shop/amfilerating/file/download/file_id/328/, 2015.

[86] Mahalle, P. N., Anggorojati, B., Prasad, N. R., and Prasad, R. Identity authentication and capability based access control (iacac) for the internet of things. Journal of Cyber Security and Mobility, 1(4), 2013, pp. 309–348.

Rachana Ashetakr, Parikshit N. Mahalle and Gitanjali R. Shinde

5 Users' privacy at online social networks in Indian context: comprehensive multiaged group survey and discussion

Abstract: Nowadays, social media has become an important part of life. People across the world use social media for random purposes. They post their accomplishments, achievements, vacation photos and others on the social media. However, they do not often realize that they are attracting very serious incidents that can occur due to their posts. Online privacy is one of the crucial points to safeguard our personal information. However, protecting privacy in online social networks (OSNs) is challenging as OSNs follow the strategy "Take it or Leave it." Users need to provide information asked by the service providers in order to use the OSNs that may lead to compromise the users' data privacy.

To provide privacy-aware OSNs it is important to know user's awareness about privacy. To achieve this, survey is conducted and from analysis of survey the user's awareness and requirements of privacy-aware mechanism is presented in this chapter. Survey analysis shows that users of OSNs required to have trusted third party to manage their preferences and attributes to protect their privacy. Furthermore, user required new privacy law in Indian context and they need to hide their identity on OSNs.

Keywords: Online social network security, user data privacy, user identity privacy

5.1 Introduction

In today's era of online social networks (OSNs), everything we can find online starting from entertainment to business. But this availability also gives rise to one of the important aspects, that is, privacy [1–3].

Social network services and its popularity are widely spreading, where all age users are being attracted to it across the world. Reasons for using social network may vary like relationships, interests, friendship, knowledge or other social reasons. Popular examples of social networking sites (SNSs) used worldwide include Facebook, Twitter and LinkedIn [4]. This openness raises risks of vulnerabilities, data breaches and compliance violation. Also lack of regulation and standardization brings more opportunity for hackers to live and spread attacks in OSNs. It is the newest platform for security attacks.

Now with social networks, everyone is aware of the value of information being placed online as "data is money." People with profit motives or political agendas

https://doi.org/10.1515/9783110628517-006

are few of the main causes for the attacks on data confidentiality. Service providers (SPs) may misuse users' data for advertisements and may sell these data to third party without their consent, for example, Facebook data is misused by Cambridge Analytica for US president elections [5].

Currently, the effectiveness of security policies considering data leakage is an important concern to society. Social security sites do provide security mechanism but not seem to provide a way to stop privacy compromising.

There is a need of security mechanism for protecting use's' sensitive data shared on ONSs and there should be a method to bargain for users' data sharing instead of "Take it or Leave it" strategy. Successively, we can say that there is a need to develop a mechanism for protecting user's sensitive data shared on OSNs.

5.2 Motivation

Nowadays, social media has become an important part of life. People across the world use social media for random purposes. They post their accomplishments, achievements, vacation photos and others on the social media. However, they do not often realize that they are attracting very serious incidents that can occur due to their posts. Furthermore, to use location-aware services, users share their location with their SPs so that they can lead to compromise their privacy. These incidents can potentially put themselves and everyone around them in potential danger.

A serious incident happened because of the post. There was a woman who used social media very extensively. She used to post every now and then on social platform.

The incident happened on one uneventful afternoon. She was at home with her husband when armed burglars broke into their home. They stole huge amount of cash along with some personal gadgets.

After the robbery when police started their investigation, a fact came into light that the woman in question had posted photos of herself with huge amount of cash on social media. This woman is the wife of CEO of the construction firm, having turnover in crores. She is shopaholic and net-freak. She frequently uploads her activities and photos of her family on Facebook and other OSNs. Robbers understood about her financial and family background with analysis of her pattern of uploads. After post robbers took advantage of the situation and planned the heist. She and her husband were planning for some vacation, so for that purpose she had taken that money out of the bank.

In this scenario, the woman is not aware about people viewing her personal data like marital status, kids' age, school, photos and many more.

From the above and many more other scenarios shown in Figure 5.1, we can say that there is a need to make people aware about the importance of privacy and how to achieve it as a fact that OSNs cannot say everything is ok and full proof by

Figure 5.1: Consequences of privacy leakage in OSNs.
Note: https://www.zdnet.com/article/infographic-80-of-robbers-check-twitter-facebook-google-street-view/
https://theweek.com/speedreads/455792/familys-home-burglarized-after-post-vacation-photos-facebook
https://www.myrtlebeachonline.com/news/local/crime/article223765610.html
https://www.springfieldnewssun.com/news/local/criminals-use-social-media-choosing-their-victims/7zJvddM93fSEuVTe1Be9XI/

just securing server systems and application on servers [which are hosted by social network sites (SNSs)], underneath awareness about privacy is also important (which is not in OSN's control).

Other issues with OSNs are data stored by OSNs may be misused by the third party for advertisement or business growth or some other personal benefits/crimes. Today's third party has far more resources available to facilitate an attack and it has greater technical depth, focus plus it is well funded and is better organized.

Moreover, as end user communicates to server, end user's device security also becomes important (again this is not in SNS's hand). If user's device is with weak security mechanisms, then attack on data confidentiality is possible. Let's go one step ahead, assume user's device is safe but if user's knowledge is weak about data sharing and there comes possibility of misuse of user's data. There are fair chances that user identity attack will succeed here and start damaging user's privacy.

Also, at present there is no centralized mechanism directly available that will increase collaboration between SNSs, users and security teams to set standards or guidelines for preventing and reducing attacks on user's privacy. This is because social sites have different priorities and users have different priorities.

Consequently, from literature work we can say that there is a need to research mechanism for user identity protection and data confidentiality on OSNs to analyze behavioral modeling of most possible attacks to provide a solution set in near future.

5.3 Related work

Analysis of different privacy and security risks is presented by Fire et al. [6], due to users' unawareness about privacy and security settings they share their personal information on OSNs may put them in risk. The different types of threats presented in this chapter are, for example, clickjacking, anonymization attack, fake profiles, identity clone attacks, inference attacks, information leakage, location leakage, socware, online predators, cyberbullying. Few recommendations for protecting their privacy are suggested like removing unnecessary information shared on OSNs, adjust privacy and security settings of OSNs account, not to accept friend requests from strangers, install Internet security software, remove installed third-party applications, not to publish location, not to trust on friends on OSNs and to keep eye on children's OSN activities.

The attacks on OSNs are categorized as attacks on users and attacks on OSNs by Kayes and Lamnitchi [7]. Inference/de-anonymization attacks, attacks from other users, OSNs are categorized as attacks on users. Sybil attack, crawling attacks, social spam and distributed denial of service attack and malware attacks are considered as attacks on OSNs. The procedure of attack launch and defense techniques is presented in this work.

Comprehensive survey of personal information disclosure by members while joining OSNs especially Facebook, Instagram, Twitter and Snapchat is done by Aljohani et al. [8]. The analysis is done on the data collected in duration of 3 months, with 30 different questions and over 500 responses. The analysis concludes that in general people disclose their gender, name, age and education very frequently. Survey results show that the friend requests are accepted without knowing the person 50% of times. The privacy setting "only visible to friends" doesn't make any sense in such scenarios.

Survey of privacy risks and challenges of OSNs, cloud and big data are presented rigorously in the literature [9–19]. In these research works, different attacks on OSNs and their solutions are presented.

The effect of understanding of privacy setting and policies on the information disclosure on OSNs is presented by Fred et al. [20]. The survey is taken from 122 Facebook users. This survey shows that after reading privacy policy the information disclosure can be reduced as users are aware about the importance of privacy of their personal information.

Survey of Facebook users aged 18–29 is taken by Madejski et al. [21], to understand the awareness of users about privacy settings of Facebook. The survey results

show that 44% users take efforts to limit their personal information disclosure, About 71% users have changed their privacy settings and 47% users take actions like deleting unwanted comments to keep privacy.

In digital era, use of android apps increases in large number; however, using android apps may lead to privacy leakage as at the time of installation of apps, users unwillingly allow access to their smart phone camera, contact list, microphone and so on. Li et al. [22] presented intercomponent communication taint analysis tool to protect the privacy of android users.

Savla and Martino [23] have carried out survey about privacy. It is based on 35 OSNSs that are used frequently in the United States. Survey shows that the users' privacy is at risk if the privacy policies are not implemented as per standards. Another survey carried out at countries like Saudi Arabia [24], UK [25] and India [26–27], survey shows that to protect privacy of OSNs there is a need to understand users' view about SPs and policies.

Zeadally and Winkler [28] carried out a survey to understand users' knowledge and awareness of the privacy policy. Facebook, LinkedIn, Twitter and others are selected for this survey, Findings of this survey state that people doesn't understand what they agree while registering membership on such OSNs.

From related works mentioned earlier, we can conclude that privacy surveys are done mainly in developed countries and they are in initial phases in country like India. Surveys taken in related works focus on participants who are of middle age; however, nowadays youngsters spend most of their time on OSNs, which is making necessary to research privacy issues in Indian context and it should be more focused on lower age group participants. Therefore, this research provides details of users' awareness about privacy in Indian context.

5.4 Issues and challenges

In this section we will discuss issues and challenges to provide privacy-aware secure access to OSNs. An architecture to provide secure and privacy-aware OSNs could face different challenges as today's technoworld is heterogeneous and scalable. Security and privacy algorithms need to support these heterogeneity and scalability. From the above discussion of literature and gap analysis, OSN system requirements, few challenges are mentioned below:

- Heterogeneity: Devices that are involved in OSNs are different in computational capabilities, information format, connectivity and many more. Performance of the security and privacy algorithms may vary with such heterogeneity.
- Scalability: As aforementioned, number of people using OSNs has increased tremendously and will continue to increase in the future. The privacy algorithms must perform best with such scalable environment.

- Awareness: Users need to accept policies with terms and conditions about sharing their personal data before accessing services of OSNs. SP asks these information for their business betterment; however, users may not be aware of "why, how and where their personal data being used." Due to personal data sharing with the SP could possibly result in the infringement of privacy rights. People using OSNs are not aware of the fact that their personal data is used by the third party and moreover they not aware about consequences of privacy leakage. Hence, users should be made aware about privacy policies and their right to protect personal data.
- Standardization: Standards are not being used for protecting users' privacy on OSNs, and lack of standardization is a major issue faced by OSNs.
- Policy interpretation: Reading and understanding of privacy policies is difficult for users of OSNs. There is a need to have understandable way to provide insight of privacy policies.
- Attribute negotiation: SP asks personal attribute for usage of OSNs. Users need to share all attributes asked by SPs. However, for protecting privacy, there should be facility of attribute negotiation. Thus, selection of basis of attribute negotiation is very challenging as users and SPs viewpoint about sharing information are contradictory to each other.

5.5 Proposed work

Quantitative analysis can be the best way to understand users' awareness about privacy. We have conducted survey of Indian people of different age groups, different educational backgrounds and different work cultures. This survey was intended to learn about users' activities, practices on OSNs, knowledge about privacy policies, laws related to privacy and what is missing in current privacy mechanisms.

In the survey, we have formatted questionnaire in such a way that participants' responses will provide their suggestions and opinions about the type of privacy mechanism they wish to have with OSNs. A total of "47" questions are prepared, and these questions are formed in such a way that any layman can understand. We tried to make survey as simple as possible and users are selected randomly for survey as per principles of the survey [29]. Survey is done online using Google form, and this form is sent to the participants via email. Method of online collection of responses is used in survey instead of the off-line method to save time of the survey. Few assumptions are made while survey like participants are excited to give survey, they were honest and gave responses voluntarily.

The questions are formed in such a way to understand users' viewpoint about what is privacy?, How user's information get compromised?, Why SPs steal users' information?, What benefits SPs are getting by stealing users' information?, What actions should be taken by the user to protect their personal information? and

Where user should seek for help if information compromised?. It is depicted in Figure 5.2. These questions are categorized in six sections. The first section, that is, introduction, we formalized this section to know details of participants like age, status as whether working or student, from where they access OSNs and which type of online facility they use. The second section of questionnaire is targeted to know participants awareness about online privacy like, which information is recorded by the SPs, what happens further with these information, what is SPs aim to collect these data and so on. Third and fourth section questions are related to know participants awareness about privacy laws and agencies, and what individuals will do if their privacy compromised. In section five, questions are formed to understand participants' expectations from SPs about the privacy of their data. related to SPs. In this digital era, people are using Internet to use health facilities with the help of the Internet of things, section six questions are focused to know about users' understanding about the privacy of their health parameters that they share through Internet.

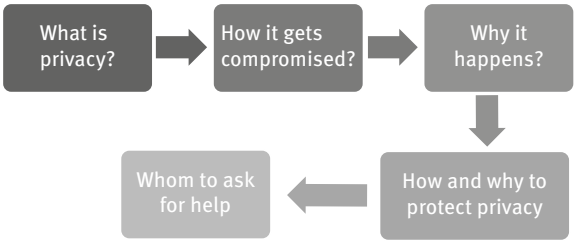


Figure 5.2: Overview of questionnaire.

5.6 Results and discussion

As aforementioned, for unbiased analysis survey is taken for users with different educational background, different working culture and different age groups, which is depicted in Figure 5.3. A total of 671 responses have been received; among which 55.3 (371)% were males and 44.7% (300) were female users who participated. Among 671 participants 42.3% (283) participants consider themselves as very new to computer field, that is, having less knowledge of computer field, 45% (301) participants see themselves as having satisfactory knowledge about computers and only 12.7% (85) claim them as experts in the computer field. This analysis shows that very few people know about risks that may happen while handling Internet as only 12.7% participants are expert in computer and Internet field.

In the survey, few questions are formed to know details like from where participants access Internet, what is the purpose of accessing Internet and how much work they get it done using Internet. The survey analysis shows that the common

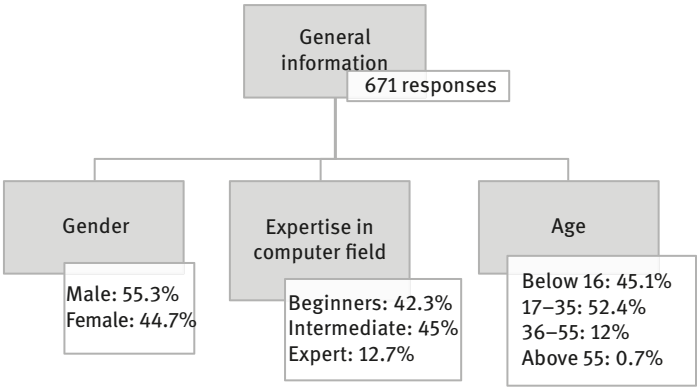


Figure 5.3: General information about survey.

answer was that participants (i.e., 87.8%, Q5) access Internet at home, office, college and school, and only 12.2% participants access Internet from cybercafé and other places. The survey shows that 58.3% people use Internet for online shopping and 72.9% people use it for OSNs and search engines. Only 32.6% [Q.6] participants use Internet for other works than online shopping and OSNs. This analysis shows the increasing popularity of OSNs.

5.6.1 Which information may leak while using Internet/OSNs?

We tried to understand participants' response on question-related information leakage, that is, Q9. As per your knowledge, response to the question "Which information is recorded by server while you are online?" is shown in Figure 5.4. It is observed that majority of participants, that is, 65%, 62%, 52.5% think that email id,

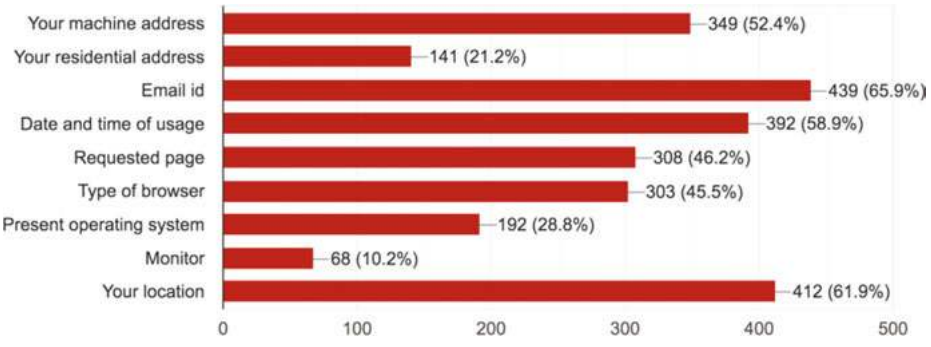


Figure 5.4: Analysis of types of information leakage.

location and machine address may be stored by SPs, respectively. However, in reality more information stored and fetched by SPs and response shows that participants may not be aware about this.

5.6.2 Why privacy get compromised?

In question 11, we tried to know participants' views about information leakage by SPs, question formed as "Q.11 What would you think about the primary usage of collecting personal information by service providers?" 52.3% participants thought that SPs steal users' data for analysis purpose that could be further used for recommendation systems, few people thought that SPs store users' data for detection of fraud, case studies and for implementation of new laws, depicted in pie chart, that is, Figure 5.5. These responses show that people are not aware of the fact why data is stored and used by SPs.

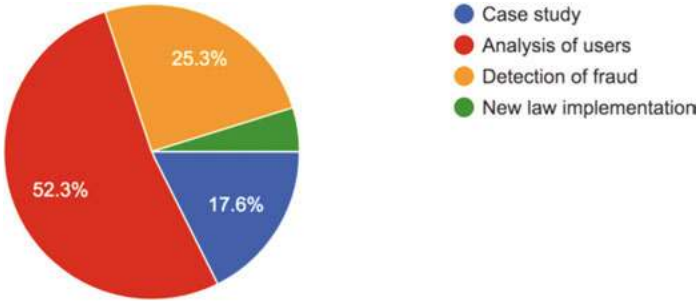


Figure 5.5: Analysis of users' responses: reasons of privacy compromise.

5.6.3 How privacy gets compromised?

Privacy may be compromised due to fact that most of the people are not aware that they are providing personal information online, without knowing what can be done with their data. This may lead to harm their privacy and, furthermore, people are not even aware about consequences of privacy leakage.

In sequel to this, few questions of survey are formed to know users' views about privacy leakage, which is depicted in Table 5.1. Most of the people share their data online without thinking protection of their personal information. Analysis of survey shows that 72% people frequently share their data<Q15/> and furthermore 23.8% people even don't know the consequences of privacy leakage [16].

Table 5.1: Analysis of users' responses: awareness about data sharing.

Question	Response
Q15. In general, have you frequently shared your personal information with organizations that they ask for it?	72% people shared their personal information online.
Q16. Are you aware of consequences if your privacy is compromised?	23.8% people are not aware about the consequences of privacy leakage.
Q18. Have you ever asked an organization that requested personal information from you "why they want it" and "what they will do with it"?	Most of people, that is, 52.1% people never asked any question while sharing their personal information.
Q34. How regularly do you read the privacy policies of websites/service providers you visit/doing registration?	Only 15.1% people read privacy policies regularly while registering online.
Q35. Do you think that the privacy policy is very lengthy, unable to understand and descriptive?	Among those who read privacy policies, 77.1% people think it is very lengthy and not in understandable format.

5.6.4 Whom to ask if privacy gets compromised?

Privacy of personal data is an important issue in this digital era as we frequently share data on OSNs, assuming that third parties, SPs, are trusted. However, this is not the reality that privacy may compromise if these are not trusted; hence, users should be aware what steps they should take if privacy gets compromised. In the survey, few questions are formed to know users' awareness about actions that they should take if privacy gets compromised, which is depicted in Table 5.2. The analysis shows that 61.6% people are even not aware about privacy law in India [Q.12] and 59.3% people never take any action to protect their data [Q.24].

5.6.5 How and why to protect privacy

Nowadays, people use OSNs and Internet frequently. Survey analysis shows that 40% people do their 80% work like banking, shopping and so on using online services. People think life will be easier using online services as in Q.7, and 96.3% people say that online service made their life easier; however, this is one side of the coin. Other side is that, to use these facilities they need to share their personal data and accept terms and condition that may lead to compromise their personal data. SPs are using "Take it or Leave it" approach, which needed to be changed. There should be some mechanism by way that an users can use online facilities without losing their data privacy [Q.25, Q.31]. There should be new privacy laws to protect

Table 5.2: Analysis of users' responses: awareness about privacy law.

Question	Response
Q24. Do you personally take any steps/actions to limit tracking of your Internet/online activities?	38.5% people never took any action to protect their privacy.
Q14. Have you ever actively hunted out for information about your privacy rights, for example, by visiting a website searching on the Internet contacting an agency/organization or reviewing a standard publication for help?	Most of the people, that is, 59.3% didn't search any help to protect their privacy.
Q12. Are you aware of any federal institutions/ law that help Indians to deal with privacy and the protection of personal information from wrong collection use and exposing publicly?	61.6% people are not aware about privacy law that can help to protect their privacy.
Q38. Where do you ask the question if security/ privacy is breached?	Majority of the participants (55.4%) respond that they will take help from security specialist and system admin, and very few participants (30%) choose to take help from government agencies.

privacy as once people are aware about consequences of privacy leakage, people may think not to use online services on cost of privacy [Q. 22, Q.28], which is listed in Table 5.3.

5.7 Conclusion and future work

Analysis of this survey shows that users are not aware of the privacy compromise and consequences of it. Moreover, users are not aware where to seek for help if privacy gets compromised, and what actions they should take to protect privacy. In the sequel of this we wanted to know what are the expectations of users from OSN privacy systems.

These expectations may lead us to provide a novel method to provide privacy-aware OSNs, as people prefer privacy over services Q.22. In Q29, "I support the establishment of a personal trust manager (where a trusted entity/party keeps my preferences/experience to build trust between me and the service provider)" we tried to understand that whether trusted third party can be a solution to build trust between the user and SP. The analysis is depicted in Figure 5.6. It shows that 83.5% participants agree to have trusted third party to store their preferences and build trust between them and SPs.

Table 5.3: Analysis of users' views on "Privacy vs Services".

Question	Response
Q22. What do you most prefer, *privacy* or *utilities/services*.	86.5% people prefer privacy over services and online utilities.
Q25. Do you think that service provider/Internet companies should ask your consent/permission to track what you do on the Internet?	Majority of people (83.2%) think that service providers should ask consent before tracking online activities.
Q28. There should be new laws to protect user privacy on the Internet.	Almost every person (97.6%) thinks that there should be a new law to protect user privacy.
Q31. A user should have complete control over which sites that collect the user's important and critical information.	In the view of protecting users' privacy, users should have control over sites that collect their information.
41. Do you feel that the service provider should notify you when they deal (access sale share) your personal information?	87.1% people demand for such service providers, which will notify users while using their personal data.
44. Have you ever decided not to install an app because of the amount of personal information you need to provide?	80.6% people choose not to install app due to the risk of personal information sharing.

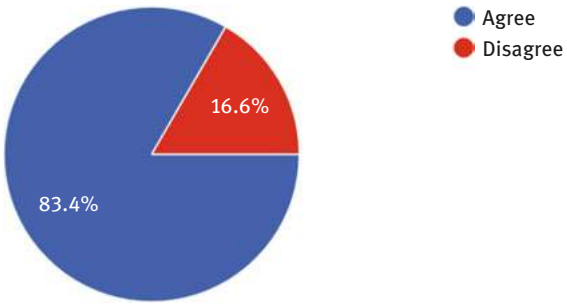


Figure 5.6: Users' response on privacy solutions: "Trusted Third Party."

In another question Q32, we wanted to know users' viewpoint on their identity, whether they want to keep their identity hide from OSNs, to protect their privacy. Question formed as "Q.32. I will be interested in being anonymous when visiting sites on the Internet." The analysis of users' responses is depicted in Figure 5.7. Among 671 users, 77.9% of them expect to have trusted third party to protect their identity while working on OSNs.

Based on the above analysis of users' responses on privacy, we can build privacy-aware mechanism to protect users' privacy on social media. The features of

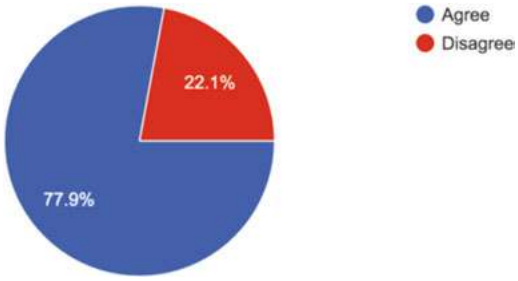


Figure 5.7: Users' response on "protecting their identity."

such a mechanism will be as follows: it will have an "algorithm to protect users' identity across OSNs," and a "trusted data management algorithm to maintain data confidentiality."

References

[1] Dey, N., Babo, R., Ashour, A. S., Bhatnagar, V., and Bouhlel, M. S. (Eds.). Social networks science: Design, implementation, security, and challenges: From social networks analysis to social networks intelligence, Springer International Publishing: Springer, 2018.
[2] Marpaung, J.A.P.; Sain, M. and Lee, Hoon-Jae, "Survey on malware evasion techniques: State of the art and challenges" in IEEE, Advanced Communication Technology (ICACT), 14th International Conference, 2012, pp. 744–749.
[3] Das, N., Borra, S., Dey, N., and Borah, S. Social Networking in Web Based Movie Recommendation System, In Social Networks : Design, Implementation, Security, and Challenges Science, Cham : Springer, 2018, pp. 25–45.
[4] Hashimoto, G.T.,"A security framework to protect against social networks services threats", in IEEE, Systems and Networks Communications (ICSNC), Fifth International Conference, 2010, pp. 189–194.
[5] https://techcrunch.com/story/facebook-responds-to-data-misuse/
[6] Fire, Michael, Roy Goldschmidt, and Yuval Elovici. "Online social networks: threats and solutions", IEEE Communications Surveys & Tutorials, 16(4), 2014, pp. 2019–2036.
[7] Kayes, Imrul, and Adriana Iamnitchi. "A survey on privacy and security in online social networks," arXiv preprint arXiv:1504.03342 2015.
[8] Aljohani, Mashael, Nisbet, Alastair, and Blincoe, Kelly. "A survey of social media users privacy settings & information disclosure", 2016.
[9] Ajami, Racha, et al. "Security challenges and approaches in online social networks: A survey", IJCSNS, 11(8), 2011, pp. 1.
[10] Zheleva, Elena, and Getoor, Lise. "Privacy in social networks: A survey," Social network data analytics, Boston, MA : Springer, 2011, pp. 277–306.
[11] Cavoukian, Ann. "Privacy in the clouds", Identity in the Information Society , 1.1, 2008, pp. 89–108.
[12] Chewae, Mafaisu, et al. "How much privacy we still have on social network?", International Journal of Scientific and Research Publications, 5(1), 2015, pp. 2250–3153.
[13] Rubinstein, Ira. "Big data: the end of privacy or a new beginning?." 2012.

[14] Jayalakshmi, N., and R. G. Kavitha. “A survey on privacy in social networking websites,” Adarsh Journal of Information Technology, 5(2), 2016, pp. 30–37.
[15] Zhang, Chi, et al. “Privacy and security for online social networks: challenges and opportunities,” IEEE network, 24(4), 2010, pp. 13–18.
[16] Kayes, Imrul, and Adriana Iamnitchi. “Privacy and security in online social networks: A survey,” Online Social Networks and Media, 3, 2017, pp. 1–21.
[17] Gao, Hongyu, et al. “Security issues in online social networks,” IEEE Internet Computing, 15 (4), 2011, pp. 56–63.
[18] Wang, Yang, and Alfred Kobsa. “Privacy in online social networking at workplace.” Computational Science and Engineering, 2009, CSE’09. International Conference on, 4, IEEE, 2009.
[19] Toch, Eran, Yang Wang, and Lorrie Faith Cranor. “Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems,” User Modeling and User-Adapted Interaction, 22(1–2), 2012, pp. 203–220.
[20] Stutzman, Fred, Robert Capra, and Jamila Thompson. “Factors mediating disclosure in social network sites,” Computers in Human Behavior, 27(1), 2011, pp. 590–598.
[21] Madejski, Michelle, Maritza Lupe Johnson, and Steven Michael Bellovin. “The failure of online social network privacy settings.,” Department of Computer Science, Columbia University, 2011.
[22] Li, Alexandre Bartel, Bissyandé, Tegawendé F., Klein, Jacques, Traon, Yves Le, Arzt, Steven, Rasthofer, Siegfried, Bodden, Eric, Octeau, Damien, and Patrick McDaniel. “IccTA: Detecting inter-component privacy leaks in android apps,” In Proceedings of the 37th International Conference on Software Engineering, 1, IEEE Press, 2015, pp. 280–291.
[23] Savla, P., and Martino, L. D. Content analysis of privacy policies for health social networks. Proceedings – 2012, IEEE International Symposium on Policies for Distributed Systems and Networks, POLICY 2012, 2012, pp. 94–101. http://doi.org/10.1109/POLICY.2012.20
[24] Alsagri, H. S., and Alaboodi, S. S. Privacy awareness of online social networking in Saudi Arabia. 2015, International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2015,2015. http://doi.org/10.1109/CyberSA.2015.7166111
[25] Khan, R., and Hasan, R. The story of naive alice: Behavioral analysis of susceptible internet Users, Proceedings – International Computer Software and Applications Conference, 1, 2016, pp. 390–395. http://doi.org/10.1109/COMPSAC.2016.206
[26] Kumaraguru, Ponnurangam, and Niharika Sachdeva. “Privacy in India: Attitudes and awareness v 2.0.” Available at SSRN 2188749 2012.
[27] Dhawan, S., Singh, K., and Goel, S. Impact of privacy attitude, concern and awareness on use of online social networking, Proceedings of the 5th International Conference on Confluence 2014: The Next Generation Information Technology Summit, 2014, pp. 14–17. http://doi.org/10.1109/CONFLUENCE.2014.6949226
[28] Zeadally, S., and Winkler, S. Privacy policy analysis of popular web platforms. IEEE technology and society magazine (June), 2016, pp. 75–85.
[29] Susan Farrell 28 Tips for creating great qualitative surveys,. Retrieved May 29, 2017, from https://www.nngroup.com/articles/qualitative-surveys/, . 2016.

Snehal Mane and Vandana Jagtap

6 Early prediction of breast cancer from mammogram images using classification methods: a comparison

Abstract: Today the deaths of women in the age group 15–54 are increasing due to malignant cells in breast. It is recognized as the main cause for deaths of women. Day by day, the number of patients are increasing, because its important factors have not been identified yet, and it is unable to prevent. Therefore, the possibility of improvement is only the early diagnosis. Machine learning (ML) techniques can assist the physicians by expanding tools for detection at initial stage and analysis of breast cancer, thus increasing the probability of patient's survival. For routine breast screening, currently mammography is the commonly accepted imaging method. First, aim of this survey is to develop techniques that are helpful for the prior detection of cancer using different classification methods such as support vector machine, decision tree, artificial neural network (NN), logistic regression and ML-NN, and a comparative study of extracting the feature with and without removing pectoral muscle in the initial stage [1] using a different and effectual method is the another goal behind this study.

Keywords: *Breast cancer*, *data analysis*, *machine learning*, *classification*, *prediction*

6.1 Introduction

Nowadays, women's death has been increasing because of the breast cancer (BC). The abnormal growth of the cell is the main reason of the BC. Generally, identifying the cancer specifically in middle-aged women is quite difficult. It cannot be totally prevented, because the main reason behind this is not known till yet. To decrease the death rate, there is a need to identify BC in the early stage and the better treatment must be an available option to patients. If BC is identified in the earlier stage, number of patients suffering from this disease will be decreased. Mammography enables to detect cancer in its initial stage. It cannot eliminate the cancer, but can protect the life of cancer patients. So, they help to detect intangible tumors and increase the durability rate. In biological and medical field, preprocessing is the very important concept.

It is used for diagnosing abnormal cases, image analyzing and extraction of useful information.

https://doi.org/10.1515/9783110628517-007

This mammogram image is examined by radiologists (Figure 6.1). It detects the abnormalities. It can also classify whether the cancer is in benign or malignant category. The radiologist predicts unsuccessful result at many times to identify the false negative (FN) and false positive (FP). Therefore, it is impossible to detect the correct abnormality by a human radiologist. From digitized mammogram, automatically detect the suspicious lesion; for increasing the quality of the image some preprocessing steps have been done. Better quality image can be obtained by eliminating unwanted areas in the background of the mammogram image. Two main preprocessing steps are the removal of pectoral muscles and noise. The main goal of eliminating the noise from image is to develop noise-free data for further preprocessing. Pectoral muscle is another important thing, as it interrupts the accuracy for identification of bosom malignant growth from the mammogram picture. Hence, extraction of pectoral muscles stage performs a significant part in successful identification of cancer.

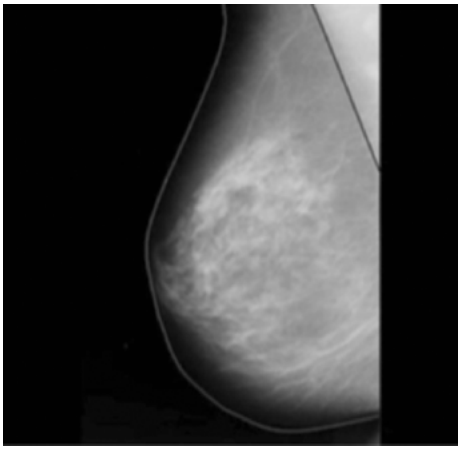


Figure 6.1: Breast anatomy of women.

6.1.1 Breast abnormalities features

Characteristics of circumscribed masses

Breast mass is a 3D lesion that looks more pronounced from the surrounding breast tissue. The mass appears as a dense area of different sizes and characteristics. They can be round, oval, lobular or irregular/inferred. This is shown in Figure 6.2.

Sometimes, the mass is also displayed with microcalcifications (MC). Fluid collection forms a tumor that is noncancerous. In the mammography film, it looks like a lump. The intensity of the mass tissue is a time similar to that of

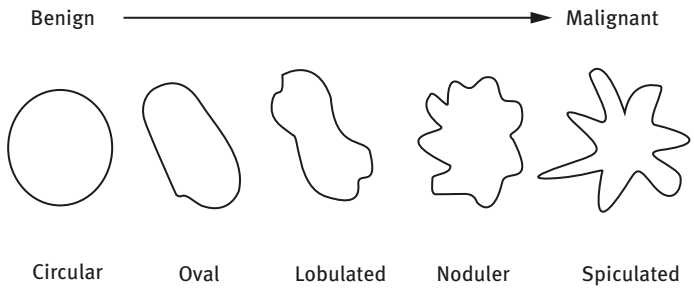


Figure 6.2: Morphologic spectrum of mammographic masses.

normal tissue. The morphology of the mass region coincided with that of the other normal tissues in the breast. This makes the job of mass detection very challenging. The radiologist estimates the probability of cancer using information about the location, size, shape, density and boundary characteristics of the mass. Features of benign lesions are well defined and compact, and are approximately circular or elliptical border. Malignant lesions are characterized by unclear and uneven boundaries. Malignant masses are sometimes surrounded by radial spiny lines.

The example of the margins associated with circular, lobular and ill-defined masses is shown in Figure 6.3.

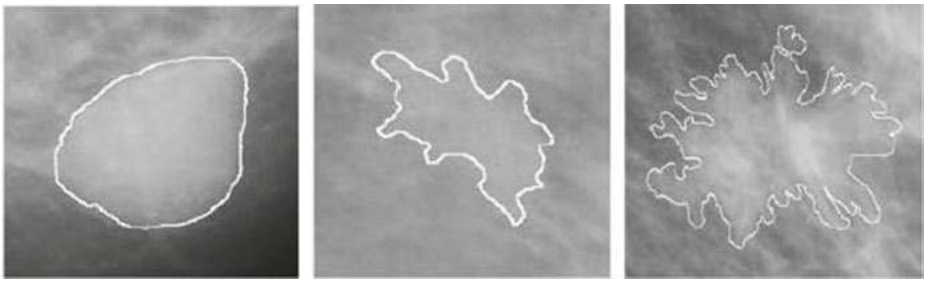
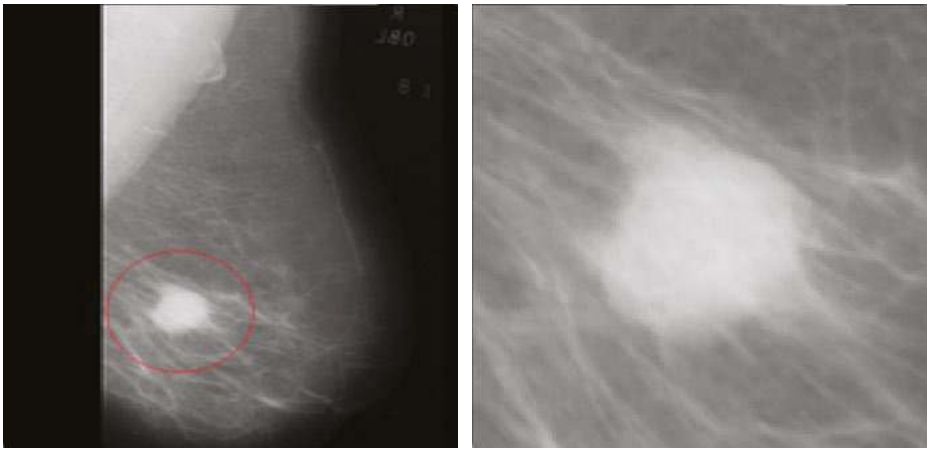


Figure 6.3: Mass examples with different shapes and borders: (a) circular shape, (b) lobular shape and (c) ill-defined shape.

The example of mammogram with malignant circumscribed mass from MIAS database is shown in Figure 6.4.

Undefined boundaries and spiky boundaries have a high probability of malignancy. Benign processes are usually associated with the presence of a round or



(a) (b)

Figure 6.4: (a) Example of mammogram with circumscribed mass mdb028 and (b) zoomed encircled abnormal region.

oval mass. However, large fluctuations in the mass appearance are an obstacle to correct mammographic analysis.

Characteristics of microcalcifications

Calcification appears as a small bright spot on a relatively dark background normal tissue. These are basically small-sized calcium deposits. Important signs of malignant breast disease are the existence of calcification cluster. Malignant calcification is small and has a variable size and shape. A relatively large number of MCs exist in the cluster form. They appear as a prickly oriented branch. Benign calcifications are usually small in number, large, scattered, uniform in size and shape, and have a smooth, circular margin. They are easily visible on a mammogram. The roughness of the shape and the distribution of calcifications are used as important features for distinguishing benign and malignant calcifications. Figure 6.5 shows a mammogram with malignant MC clusters.

A careful study of the features of calcification will help the radiologist whether it is benign, which requires regular examination, and a biopsy is necessary. Size of individual calcification is not so important, but its form is determining its classification. Usually the size of the calcification is very small (0.1–1 mm) and is typical that the diameter is 0. It is 3 mm. This is a major challenge in detecting calcifications. Small calcifications may go undetected due to partial cover by the breast parenchyma. It is very difficult to find small MCs in dense background tissues. If the

(a) (b)

Figure 6.5: (a) Example of mammogram with microcalcification mdb249 and (b) zoomed encircled abnormal region.

background is inhomogeneous, and the calcifications have a low contrast, then the calcifications may be mistakenly regarded as noise.

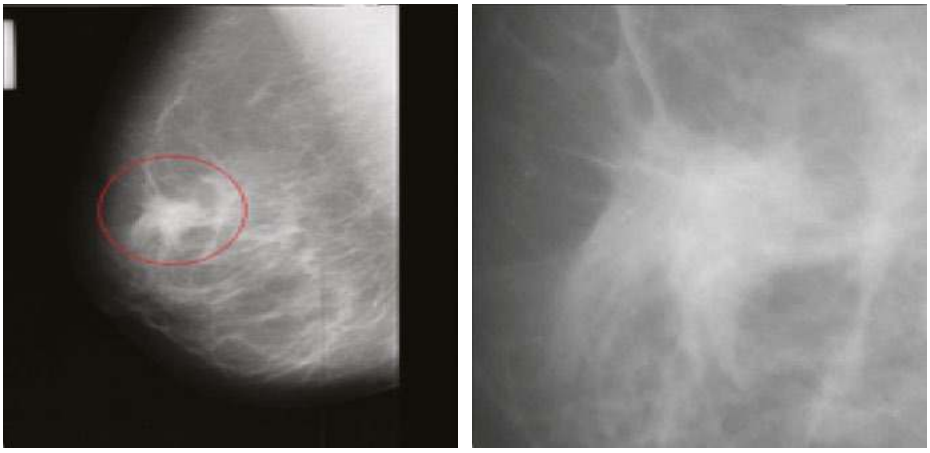
Characteristics of architectural distortion and spicules

The third most common mammographic sign of cancer is architecture distortion. It strongly hints at malignant tumors. Architectural distortions are defined as a spiked deformation emanating from a point and an ordinary architectural deformation with focal bending at the edges of the real without the presence of visible masses. Figures 6.6 and 6.7 show the breast and malignant architecture distortion in the diseased area, respectively.

As one of the visible abnormalities and architectural distortion of the chest mass, asymmetry or calcification appear together, which indicates a high probability of malignancy. Injury or soft tissue damage is caused by trauma to the building distortion that is a good type. Accurate identification of architectural distortion early BC assumes an imperative job in early identification.

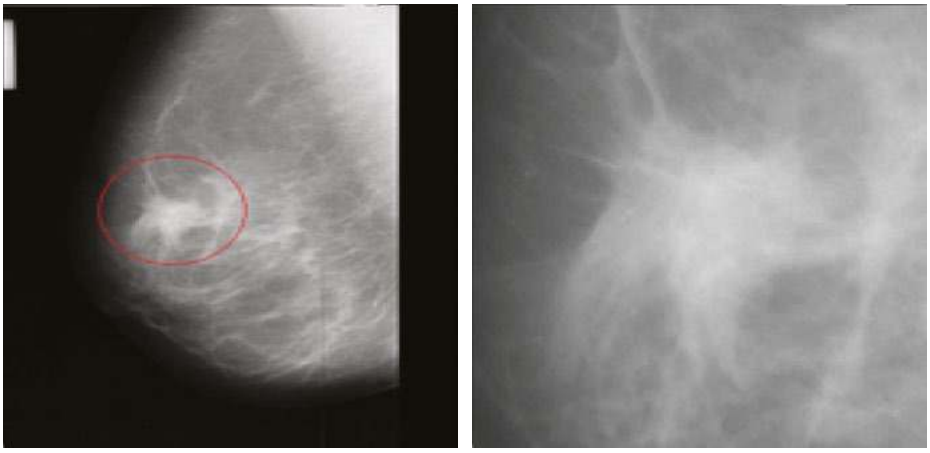
6.1.2 Features used for the detection of abnormalities

As explained in the previous section, the bounding mass of a mammogram is characterized by its shape, texture and appearance of the perimeter. MC is characterized by roughness of shape and size, homogeneous or heterogeneous tissue, the number



(a) (b)

Figure 6.6: Example of mammogram with architectural distortion mdb249 and (b) zoomed encircled abnormal region.



(a) (b)

Figure 6.7: (a) Example of mammogram with spicule mdb206 and (b) zoomed encircled abnormal region.

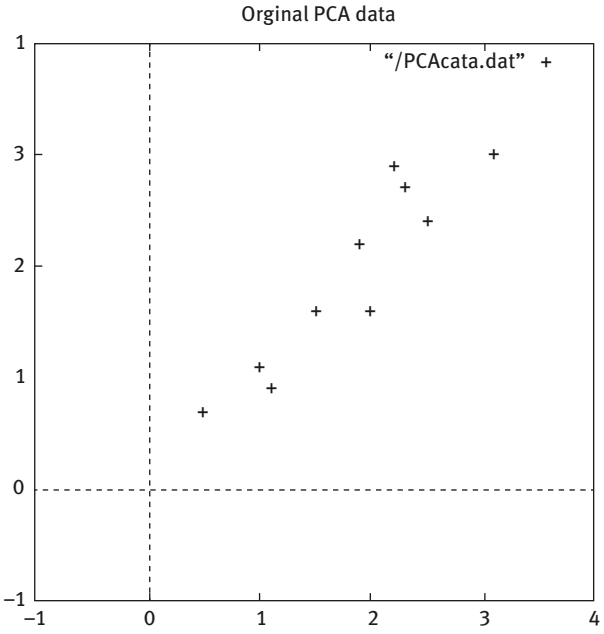
of calcifications per unit area and so on, which is useful for detecting architectural distortions and spicule-oriented patterns. All of these functions are grouped into major shapes and features such as the texture, the features and orientation of the features.

6.1.3 The analysis of PCA–ICA for detection of abnormalities

Principal-Component Analysis

The principal component analysis (PCA) is an established way to deal with statistical data analysis, feature removal and data compression. In the case of PCA, the goal is to find a small set of less redundant variables to represent the signal in much the same way as the original signal representation. In the case of independent component analysis (ICA), the goal is to determine independent components. In PCA, redundancy is estimated by connections between data elements. In ICA, decreasing the number of variables is of less importance. PCA uses only secondary statistics and is used as a preprocessing step with ICA to reduce dimensions.

PCA is popular because of its strengths, general applications and its calculations. PCA converts the initial dataset in the form of a vector into a new vector sample set that allows you to select the desired dimensions. In high-dimensional data, it is very difficult to identify patterns. PCA can be used as a powerful tool for analyzing data as it reduces its dimensions. Figure 6.8(a) indicates a plot of the two-dimensional zero-mean data. Figure 6.8(b) indicates a plot of the data plotted with the eigenvectors above it.



Original data on left, mean subtracted data on right side and plot of the data

Figure 6.8: (a) Plot of mean subtracted data.

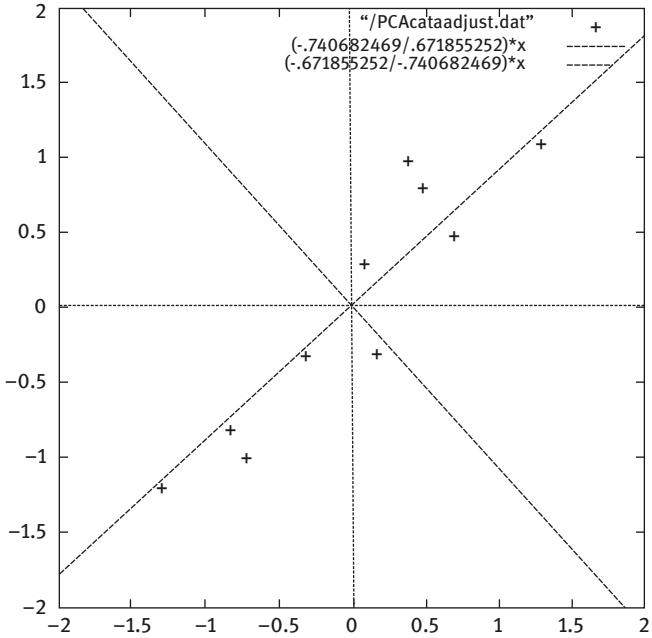


Figure 6.8: (b) mean subtracted data and eigenvectors on top.

They appear as oblique dashed lines and are perpendicular to each other, and provide important information about the patterns in your data. First, data is concentrated near the first eigenvector; second, eigenvector indicates a nonsignificant pattern in the data.

In general, images appear in large sizes. Whenever we take a picture of any type, processing, feature extraction or classification, we need to take more numbers; finally, the total size of the data matrix is significantly increased. Thus, if the size is huge, then the complexity of the calculations, time needed and the memory requirements automatically increase significantly. Hence, there is a need of dimension reduction. In an image, you can discard those redundant or less distributed features that have redundant functionality and provide less important information about the image.

PCA comes to our rescue in this situation. Suppose you have 50 images as input data. Each image is transformed into a single dimensional vector. Now all 50 images are placed as rows of a matrix and a data matrix is generated. As you can already see, the covariance of the image is calculated, and the eigenvectors and eigenvalues are given. The covariance matrix is a symmetric matrix with off-diagonal elements. The diagonal element of the covariance matrix is actually the variance of its own

dimension. By discarding the redundant elements directly, we can obtain a new image set of reduced size with only the principal components that give the most important information from the image. Figure 6.9 shows the principal components with corresponding variance.

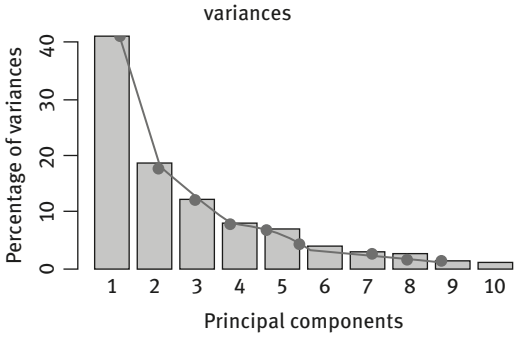


Figure 6.9: Plot of principal components with corresponding variances.

Independent component analysis

When the image is transformed from the original space region to another region, explore some of the key features of image data that are useful for image analysis. One of the simplest techniques is the main component, which is described earlier. Efficient methods for characterizing natural images are higher order statistics, but these are overlooked by the principal component. The use of independent components can overcome this limitation of the PCA. Each image can be represented as a linear combination of unnecessary independent components. Direct calculation of independent components is possible by determining the joint distribution that is not feasible. The optimization of some independence-related criteria is used to develop algorithm to determine ICA.

A statistical "latent variables" model can be used to define ICA. Vector X is formed by n random variables $x_1, x_2, \ldots, x_n$. Vector X can be represented by linear combinations of n random variables $s_1, s_2, \ldots, s_n$, which are statistically mutually independent, denoted by a random vector s, and then ICA is defined as

$$X_i = P_{i1}S_1 + P_{i2}S_2 + \cdots + P_{in}S_n \quad \text{for all } i = 1, \ldots, n$$

where the "p_{ij}" are some real coefficients. In vector–matrix form X can be represented as

$$X = PS$$

Sometimes the columns of matrix P are needed; denoting the columns of matrix P by p_j the mixing model can also be given by

$$X = \sum_{i=1}^{n} P_i S_i$$

ICA is based on the assumption that if components S_i are unnecessary independent, and independent components must have unknown non-Gaussian distributions. Then, after calculating the matrix P, its inverse W is computed, and the independent components are obtained by

$$S = WX$$

6.2 Review of literature

This section discusses the literature review in detail about the women BC prognosis prediction.

In biotechnology and medical field, image processing is an important task. Extracting important features of the images they used a texture-based method. First, Farzam et al. applied discrete wavelet transform on the image and approximation matrix is changed into 1D, utilizing zigzag scanning and finally volatile signal features are removed. These features are more delicate to light and edge so that they can be different from the abnormal and normal individuals. Experimental result shows that the accuracy is better than the previous system. Limitations: it requires large number of cases [1].

Clustering classification of breast MC into malignant and benign category is a challenging task for the computerized algorithm. Alan et al. [2] used multiview classification for the classification of MC, and it is implemented using logistic regression classification. This experiment is conducted on the digital database for screening mammography and this dataset includes demographic data of the patients. Poor accuracy is its limitation:

$$P(x) = \frac{1}{1 + \exp(-(\beta 0 + \beta 1 x))}$$

where $P(x)$ is interpreted as the probability of the dependent variable, X is the design matrix and β the shared parameter.

Computerized clustered MCs in mammograms suffer from the existence of FP results. Maria et al. explored the statistical estimate to determine some amount of FP that exists in the identified MC. First, they found out some amount of true positives (TP) by using Poisson-binomial probability distribution of training they used logistic regression models. Three different methods are used for MC detectors, namely context-sensitive classification model detector, support vector machine (SVM) detector

and DoG detector. Limitations: without any MC it includes the number of normal cases. The huge part in a mammogram image does not have a few MCs [3].

Ting et al. used self-regulated multilayer perceptron (MLP) neural network (NN) for the classification of BC. Machine learning (ML)-NN utilizes MLP to support medical specialists in diagnosis. For categorizing the images into normal patients, benign and malignant trained ML-NN is used. Oriented ridge-like function can be expressed by only single perceptron and MLP-NN in layer-by-layer basis. But it requires high computation cost [4].

Dongdong Sun et al. [5] proposed prognosis prediction of BC techniques such as multimodal deep NN by combining multidimensional. In this they integrate the multidimensional data, which include copy number alternation profile, clinical data and gene expression profile. They used multidimensional data, and performance of multidimensional techniques is compared with the single dimensional data. The proposed system gives more appropriate result than the current system and it can be identified by experimental results. This method established on single source of information that has some restrictions such as an absence of noisy data, nonuniversality and singularity.

In the CAD (computer-aided detection) techniques, preprocessing of images is divided into two main steps such as removal of pectoral muscles and noise. Sreedevi et al. [6] combined ROR (robust outlyingness ratio) mechanism with the elongated nonlocal means filters that depend on the discrete cosine transform for removal and discovery of noise. For identified pictorial muscles they used a global thresholding, recognized the edge of full breast and used edge detection processes. The limitation for this strategy on a reserved database for processing, application of a straight line-based strategy is used.

Glioblastoma multiforme (GBM) is an aggressive type of brain cancer with the lowest median survival rate of patients. Chen Peng et al. [7] proposed mRMR feature selection method with multiple kernel learning classification method for the prediction of GBM prognosis. The survival rate of patients is different for every subtype of glioma. For this experiment they used the cancer genome atlas dataset of various types of cancers. They improves the prognosis prediction accuracy of GBM and compared the performance with the one kernel method using same dataset. Because of the different datasets and process, method cannot compare with other researches directly:

$$k' = \sum_{i=1}^{n} \beta_i k_i$$

where β is the vector of coefficients for each kernel, K the kernels and N the number of kernels.

In this advanced technology, new possibilities are coming from a scientist to gather multimodal data in the different applications such as medical imaging, brain/body machine interface, bioimaging and omics. Fabian et al. [8] provide a deep study on utility with dissimilar biological data and relative study of the deep

learning techniques, reinforcement learning and the combination of deep learning and reinforcement learning in mining of biological data. Heavy computing memory and power desired by this method are the main limitations.

Khan et al. [9] proposed techniques designed for irregular classification of breast mass from the digitized mammography images. They considered for texture feature as a local binary pattern (LBP) and this feature is categorized by the ML techniques such as SVM. Mammography is a technique used to take multiple views and angles of the breast. They classified "mediolateral-oblique" views and "cranial-caudal" views separately and finally combine the classification results for accurate diagnosis. This technique reduces the classification error and it reaches the high reorganization rate. It contains extra local spatial information. Effectiveness of system is not good:

$$\left[\frac{1}{n}\sum_{i=1}^{n}\max(0,1-y_i(w.x_i-b))\right]+\lambda w^2$$

where y_i is the itch target (i.e., in this case, 1 or –1), $(w.x_i - b)$ is the current output and λ is the tradeoff between increasing the margin size.

Farag Alhsnony et al. [10] proposed a new automated technique and detected the region of pectoral muscle by utilizing a bit depth and edge processes system for segmenting a digital mammogram image. For more accuracy, CAD system is required. To determine the BC, it was found that the third-order fitting curve can be used. Limitation is recognition of pectoral muscle region in mammogram image needs a series of mathematical analysis method to be recognized.

Qiao Pan et al. [11] proposed a novel NN that depends just on character-level representation for disease classification. Their model gives information through the CNN (convolutional neural network) and remaining network over characters. Output of this is given to a GridLSTM (grid long–short-term memory). GridLSTM model is used to capture both forward and backward long-term dependencies between characters. For character-based grid CNN, they need to extract thick feature vectors.

BC is a very dangerous disease in the United States and the United Kingdom. It is also one of the leading diseases with the highest mortality rate. This BC is an irregular growth of cells from the blood tissue and tumors can be malignant or benign. Early recognition builds the odds of survival and decreases the mortality rate. The method of classifying the mammogram based on the characteristics extracted using LBP and the LGP (local gradation pattern) with the result, and histograms are compared. LBP and LGP techniques are commonly used for finding pattern in textural analysis. The generated pattern is used to classify tumors using an SVM to classify BC [12].

BC is one of the important reasons for death among women. Many techniques have been developed to detect and diagnose the disease, but have not improved the results among the number of deaths caused by this disease. Therefore, early detection

and diagnosis is the only way to prevent them from death. Previously, radiologists used to manually check the signs of cancer with mammographic images, but they did not give an effective result. Therefore, in this chapter, a new technique has been implemented for detecting and diagnosing the BC, and for the classification of cancer, image processing techniques such as texture method and KNN method were used, and it was possible to obtain the result where the reliability was high [13].

The underlying motivation of this study to a number of various mechanisms, specifically the remodeling of collagen fibers in tumor-related stroma, is that the redesigning of collagen fibers, hematoxylin and eosin has been accounted for to be identified with the survival of patients in the tumor microenvironment. The purpose of this chapter is to classify interstitial regions with maturity level and show that this classification coincides with the classification of skilled observers, and the method in which we combined a random decision tree classifier for the categorization of BC intertissue regions, the basic image features of multiscale and the LBPs [14].

Detection of breast muscle is an important invention in improvement in diagnostic detection of BC. The author proposes an intensity-based technique for the pectoral muscle boundary detection in the mammogram images. A 3×2 enhancement filter mask has been proposed and it is applicable for the image of thoracic region of the mammogram. Thorax boundary point was detected by the threshold method. Finally, the boundary of the pectoral muscle was obtained by connecting all the detected boundary points. The 322 mammography of the 320 digital mammography (MIAs) database was examined. The mean FP rate and the FN rate showed the accuracy of the proposed method [15].

Recognition image processing technology related to medical image is explained. There are a few assortments of proliferative malignancy that are now famous by researchers who have hit an aggregate to 100. Every single malignant growth is unique in its kind to be acclaimed along with the signs. This chapter has some expertise in more than a few image processing algorithms that are included in the diagnosis of breast melanoma, which is a risky cancer inspired in women worldwide. On measurements for this addition, learning is taken from the international body of cancer research – the WHO (World Health Organization) and the American Cancer Society. Benchmarking of current and previous studies has been shown to enhance long-term findings [16].

Breast malignant growth is the most widely recognized disease of ladies everywhere throughout the world. The most commonly used screening technique is mammography. To decrease the expense and remaining task at hand of radiologists, we used a computer-assisted approach to classify and localize calcifications and masses in mammogram images. Author improves the conventional approach and applies a deep CNN for automatic feature learning and classifier construction. In computer-aided mammography, the deep CNN classifier loses the details of an image from resizing at the input layer, so instead of directly resizing to the full mammogram image, the trained classifier labeled the image patches, and the full

mammogram image of the work adapted to it does not have a significant anomaly. The most advanced deep CNNs are analyzed on the performance of classifying the anomalies. From the experimental results, Vgnet was 92.3% in classification. It was shown that it received the highest overall accuracy at 53%. To localize the anomaly, ResNet is selected to calculate the class activation map [17].

In their lives, among 8% of women diagnosed with BC, and after lung cancer, BC is the second most basic reason for death in both developed and underdeveloped countries. BC is characterized by gene mutations, consistent torment, change in size, color (redness), texture of the skin of the breast. BC classification indicates to the fact that pathologists locate a deliberate and target prognosis, and generally the most regular classification is binary (benign/malignant) cancer. Currently, ML technology is widely used in BC classification problems. They provide high labeling exactness and efficient diagnostic functions. Two dissimilar classifiers for the classification of BC are naive Bayes classifiers and near-knee stop classifiers. They propose the examination of two new classifiers and assess their precision utilizing cross-validation [18].

Faye et al. [19] examined the normal and abnormal tissues in mammography using the deep learning method. VGG-16CNN deep learning architecture with a convolution filter of (3 × 3) from the Irma dataset is implemented on the mammogram ROI. The deep feature matrix is the first completely linked layer. The results have been calculated using a cross-validation of binary tree, SVM, simple logistical and 10 times on KNN (k = 1, 3) classifiers. In this method, AUC1, the categorization accuracy of 100% was obtained at 0.

In [20], CAD system, extraction of the breast region which removed the pectoral muscle and delineation of the breast contour are indispensable pretreatment processes. Predominantly, it allows the study for anomalies limited to the area of the breast without an excessive effect from the background of the mammogram. A new method for identification and removal of pectoral muscles in the mediolateral oblique (MLO) field of mammogram using the iterative threshold method is presented. The algorithm also identifies the presence of abnormal axillary lymph nodes, which are the main signs of BC, and detects the boundaries of the breast.

Over the past few years, a few ML methods have been proposed to structure an accurate categorization system for some medical problems. In this chapter, the authors relate and analyze the classification of bosom malignant growth with various AI calculations utilizing k-fold cross-validation (K-CV) technology. The decision tree is a simple Bayesian classify classifier using SVM algorithm three dissimilar kernel features using NN original and predictive Wisconsin BC. A relative investigation of the study focuses on the effects of k in k-fold cross-validation and achieves higher accurateness. The author uses the benchmark dataset from the UCI in experimental theory. It is common to choose k = 10 for KCV. But this is due to the increase in computational costs. It is necessary to train more models. Overall results showed significant conclusions. k-Value of k is in fold cross-validation [21].

The most general cause of BC deaths in women and the reasons for its cause are not yet fully known; however, quick detection of BC can be decreased with associated morbidity and death rate. Accurate removal of pectoral muscle is based on accurate detection to pectoral muscle boundaries. This suppression in gray-scale mammogram images can increase the accuracy of the results of CAD techniques used in previous detection of BC. This chapter proposes a new approach based on similarity between strength to delineate pectoral muscle boundaries, using a measure of semantic similarity between words in natural language processes and features of information retrieval Fi. To achieve good results, use morphological operations to remove unnecessary element mammograms from such radiation-impermeable artifacts [22].

Digital breast tomosynthesis gives huge chances in both cancer diagnosis and detection. It provides a high-quality picture and beats some inherent limitations of traditional 2D digital mammography due to the coinciding tissues that make cancer detection difficult. Unluckily, the quality of the tomographic images is straightly correlated to the radiation dose of the patient and there is significant pain due to the parameters established by the specialist throughout the mammographic examination. Typically, the tomosynthesis breast provides a small increase in the dose of radiation with respect to the mammography 2D. The aim of the study was to compare the performance of digital mammography and tomosynthesis, and to investigate the relationship between the dose of radiation to the patient and the quality of the image obtained [23].

Clustered MCs is the earliest symbols of BC. Moghaddam et al. [24] planned a new CAD system for the automatic detection of two-step MC. First, the pixel corresponding to the possibility of fine mineralization is found for multilayer feed forward control using NNs employing the input of the network of four wavelets, which are characterized by two gray levels. The output of the network is transformed into a probable MC object using a four-point spatial connection. Next, they remove 25 features from potential MC objects and use a variety of Adaboost SVM (DA-SVM) and three other classifiers to identify individual Mc. Free response operating characteristic curve was issued to calculate CAD system performance and one per image by utilizing the DA-SVM.90 at a cost of 043fp. The average TP detection rate of 44% was achieved, and the very good detection performance of the CAD system was shown.

A CAD system can be provided as a second view for radiologists. This chapter describes the outline of recent development in CAD technique. Anomaly detection, anomaly classification and content-based image retrieval are outlined. On the abnormality detection, the following were introduced: microcalcium detection, mass detection and multiview base detection. On the abnormal classification, the microcalcium classification and the mass classification are shown (Table 6.1) [25].

Table 6.1: Comparative analysis.
(a) comparative study for image preprocessing.

S. No.	Feature extraction	Methods	Advantages	Disadvantages
1.	Texture	Gray-level co-occurrence matrix (GLCM) [26]	It describes the texture of image by calculating precise pixel values and then removing statistical measures from this matrix.	It takes additional time.
		Local binary pattern (LBP) [11] Local gradient pattern (LGP) [11]	Lower intensity pixels can be split more accurately than LGP. LGP has better accuracy. LGP has smaller detection fault in comparison to LBP and better computational simplicity.	Not more accurate than LGP. It cannot split the lower intensity pixels.
		Chebyshev moment	Used for distinct and orthogonal moment values.	Random variable differs from its mean by more than k standard deviation.
		LAWS measures of texture [12, 27]	LAWS technique uses a 5 × 5 mask of convolution matrix to calculate the texture energy. Four main characteristics are level, edge, spot and ripple. It takes less time.	
2.	Shape	Compactness	For circle, compactness value is zero and this value grows with roughness of elongation of the main object.	For translation, rotation, starting point and the size of the contour compactness measure is invariant.
		Spiculation index	Measure of the degree of thinness of spicules, and has supportable consumption level.	A good performance would occur when there is a very high level of instability.
		Fourier factor/ Fourier transform	It is not difficult to appliance and is based on a well-built theory of Fourier analysis	Fourier transform does not supply limited shape information. After the Fourier transform, local shape information is spread to all coefficients and not limited in the frequency area.

(b) comparative study for classifiers.

S. no	Classifiers	Advantages	Disadvantages
1	SVM [1]	It has a regularization parameter, which makes the user think about avoiding overfitting, Utilize a structural risk minimization to diminish error of learning machine.	Long training time for large datasets.
2	Multiview [2]	Other characteristics in both views and density types are performed by curvelet rotation-invariant feature.	Time consuming.
3	CADx [3, 28]	Information provided by model helps reader to increase the accuracy for detection.	Existence of high levels of FPs affects the accuracy of CADx classifier.
4	ML-NN [4]	ML-NN can categorize the input data into three classes such as normal patients, benign and malignant.	It is difficult to show the problem to the network.
5	DNN [8]	DNN always uses multiple features and to display the outcome of model, it uses hidden layers.	Needs large dataset, typical feed forward network where the input flows from the input layer to the output layer through number of hidden layers, which are multiple layers.
6	KNN	For parallel implementation it is easy to work with local info.	Requires more space for storage. It sometimes slows in categorizing tuples.
7	CNN [17]	Mainly used for accuracy in image recognition. CNNs are very good feature extractors.	High computational cost.

6.3 Methodology

6.3.1 Multilayer perceptron

Preprocessing stage

The mammogram images can be preprocessed to improve its quality and highlight the agency of images. Input mammograms shall conform to the appropriate resolution for training. The digital mammograms of normal patients and patients with BC are included in the training data. Medical imaging may contain undesirable noise;

therefore, medical imaging is tortured to improve image quality. The improved images are then tagged and entered as training datasets to enter ML-NN for the purpose of training(Figure 6.10).

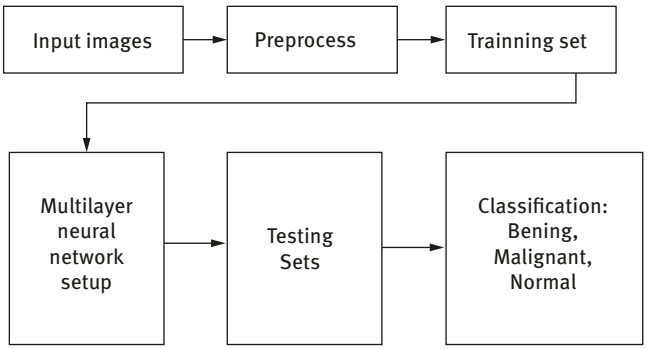


Figure 6.10: Multilayer Perceptron Neural Network for Classification of breast cancer.

Multilayer perceptron

The main objective of the this chapter is the operation of multilayer perceptron (MLP) to classify BC. The MLP consists of neurons called perceptron. In regard to the weights of neurons in the input nodes, the generation of the output by the employment of the mathematical function of activation is not linear, and the linear combination is generated by the perceptron by computing a neuron of output from multiple inputs that are valued real. The input node signal spreads through the MLP NN layer by layer.

Generally, MLP is adopted to solve problems involving supervised learning. It is indicated that a training dataset with input–output combination pairs and tags are used for input. Therefore, the MLP should be determined on the basis of training equipment.

The MLP is created with many properties like bac propagation. The flow of MLP with backpropagation is shown in Figure 6.11.

It can be used in combination of two or more phases in Figure 6.12. The black node represents the initial input. The main two stages participate in the training of this network. During the first phase, the input nodes are generated forward and the outputs of each output node are calculated. Then from expected output value each output node is subtracted. Therefore, in phase 2, all generated output node errors are passed to the opposite side, and the error weight is stable. These two phases are looped until an acceptable value is reached.

The authors propose to introduce a new technique for early prediction and comparative study of extracting the feature with and without eliminating pectoral muscle in the preprocessing phase.

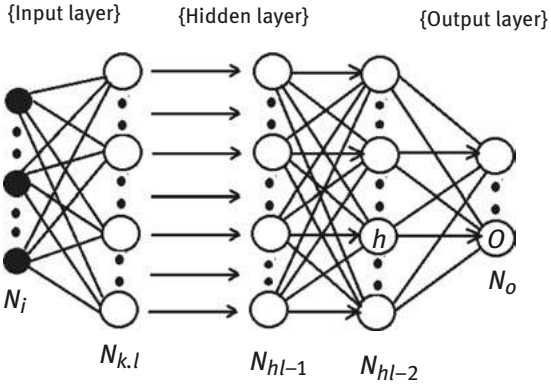


Figure 6.11: MLP with back propagation.

In the proposed system, results will be compared with the other techniques of classification. The comparison will show the accuracy and performance of system for prediction. As a result, proposed architecture should be able to predict cancer at early stage.

6.3.2 Algorithm

```
Input: I = Mammogram image from MIAS database
Output: P = Detection of abnormalities
Begin
Read MIAS image I from the MIAS database.
Calculate number of rows and columns in the MIAS image
Apply GLCM algorithm. It describes the texture of image by calculating precise pixel
      values and then removing statistical measures from this matrix.
After that we perform LBP algorithm.
Detect the edges using Fourier Factor/ Fourier Transform.
Detect the Growing part in the image
Find out the shape of growing part calculates the area of Growing part.
Detect the type of abnormalities
End.
```

6.3.3 Dataset used

Two databases are used to carry out the proposed research work: a digitized database of the mammographic image analysis society (MIAS) and a full-field digital nonpublic.

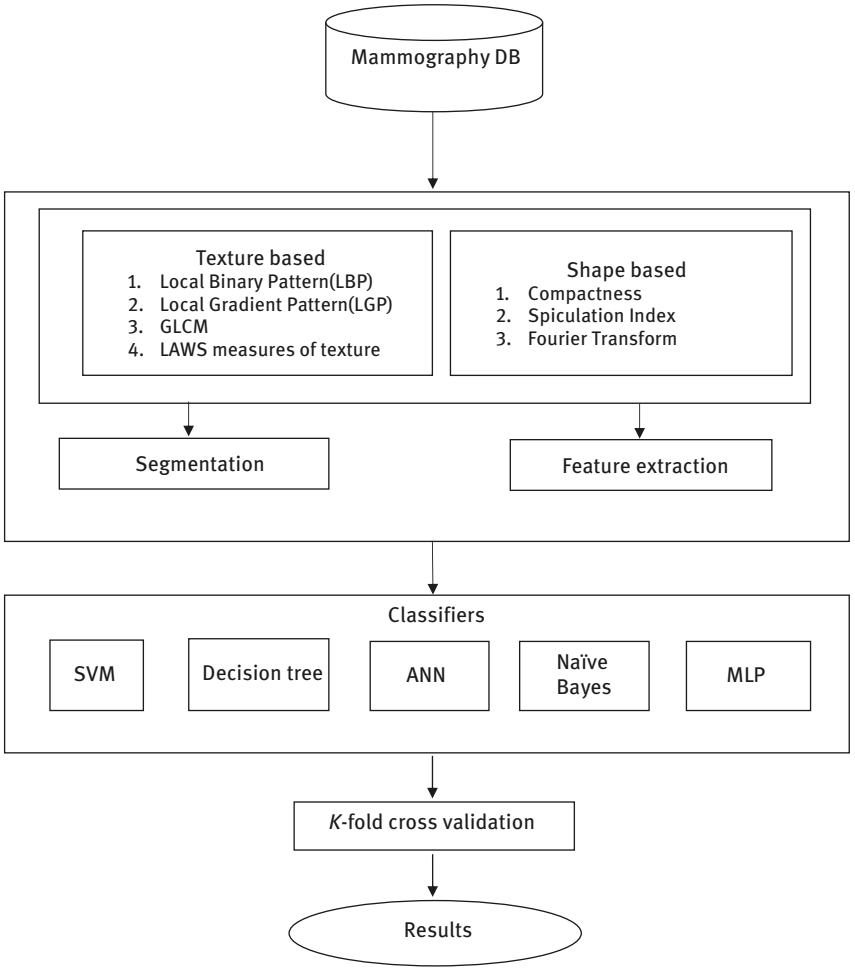


Figure 6.12: System architecture.

MIAS database

Two databases are used to carry out the proposed research work. One of it is a digitized database of the Mammographic Image Analysis Society (MIAS) and the other is Full field digital non public.

MIAS dataset

Mammograms from this dataset are caught in the MLO view and scanned at a resolution of 0.05 mm pixel size with a thickness determination of 8 bits. The size of

each image is 1,024 pixels. There are a total of 322 digitized images from the UK Breast Screening Program. The 322 images contain data of 161 patients in the MIAS dataset [27]. Therefore, the MIAS dataset consists of 322 mammogram images that are divided between 208 normal patients, 66 benign and 48 malignant. These images are carefully diagnosed to identify the type and position of the abnormality. For every image in the MIAS dataset, type of background tissue, type of irregularity, center and radius of irregularity are supplied [29].

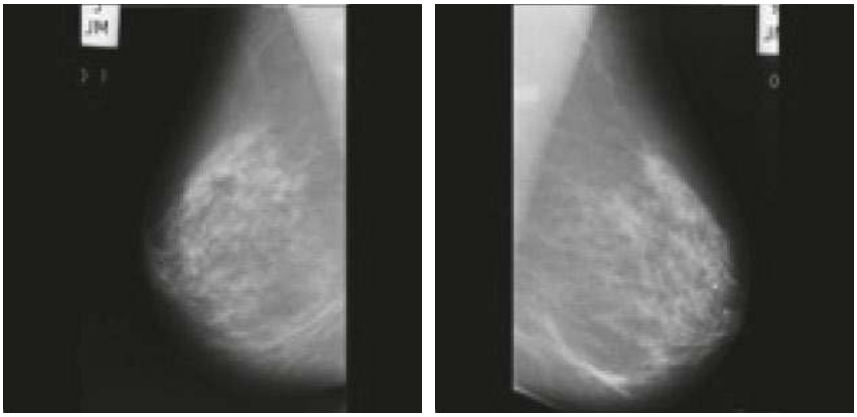
This database from the normal image with a sample anomaly is shown in Figures 6.13–6.16. For a normal breast, there are three types of breast arrangements: Fatty, fatty glandular and dense glandular (Figure 6.13). The mammogram is always captured for the breasts of both the left and right. Therefore, it is a pair of all types of mammograms. The oncologist first looks for the asymmetry of the left and right breast, and if there is asymmetry, then it is analyzed further. Figure 6.14 shows examples of benign patients and malignant patients circumscribed and other masses.

Figure 6.15 shows examples of benign and malignant patients' architectural distortion spiculations. Benign and malignant MCs are shown in Figure 6.16. In all these images, there is an anomaly in either the left or the right breast. Abnormalities can easily be seen on a fat background, whereas if the breast composition is dense, the abnormality is not visible. This can be clarified from the mammogram mdb032 from Figure 6.14(b) and mdb239.3.22 from Figure 6.16. In mdb032, other clusters exist, and in mdb239, there are MC clusters that are not clearly visible due to the dense breast background.

Some preprocessing steps have been completed successfully on MIAS dataset. Figure 6.17 contains original dataset images. On that data our novel approach, that is, LBP method, helps convert it to binary format that is 0 (black) or 1 (white). It is shown in Figure 6.18. Second method is applied, that is, Laplacian filter/Laplace transform in Figure 6.19, which is used to find areas of rapid changes in edge of images. Next GLCM (gray-level co-occurrence matrix) method is used [30]. It shows features like entropy, correlation, variance and angular moment. Hence, both LBP and GLCM methods are finding texture features of images.

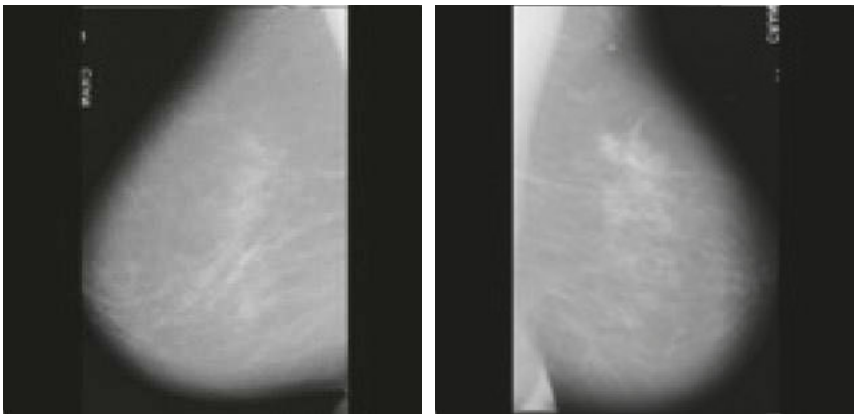
6.4 Conclusion

This chapter discussed about the early diagnosis of BC and the preprocessing of image and its importance. The main aim is to develop techniques that are helpful for early detection and a comparative study of extracting the feature with and without eliminating the pectoral muscle in preprocessing phase using a new method. The main contribution is to perform strong preprocessing and powerful feature extraction and selection before classification. Some abnormalities were found, such



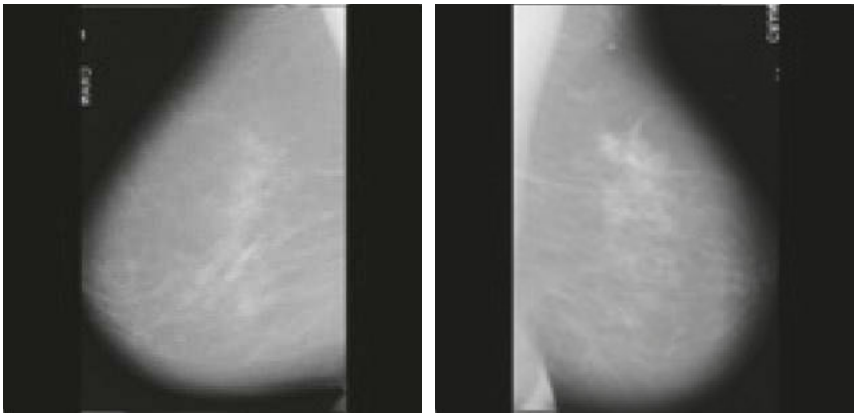
mdb003 mdb004

(a)



mdb007 mdb008

(b)



mdb173 mdb174

(c)

Figure 6.13: Sample normal images from MIAS dataset [27]: (a) fatty dense; (b) fatty glandular; and (c) fatty..

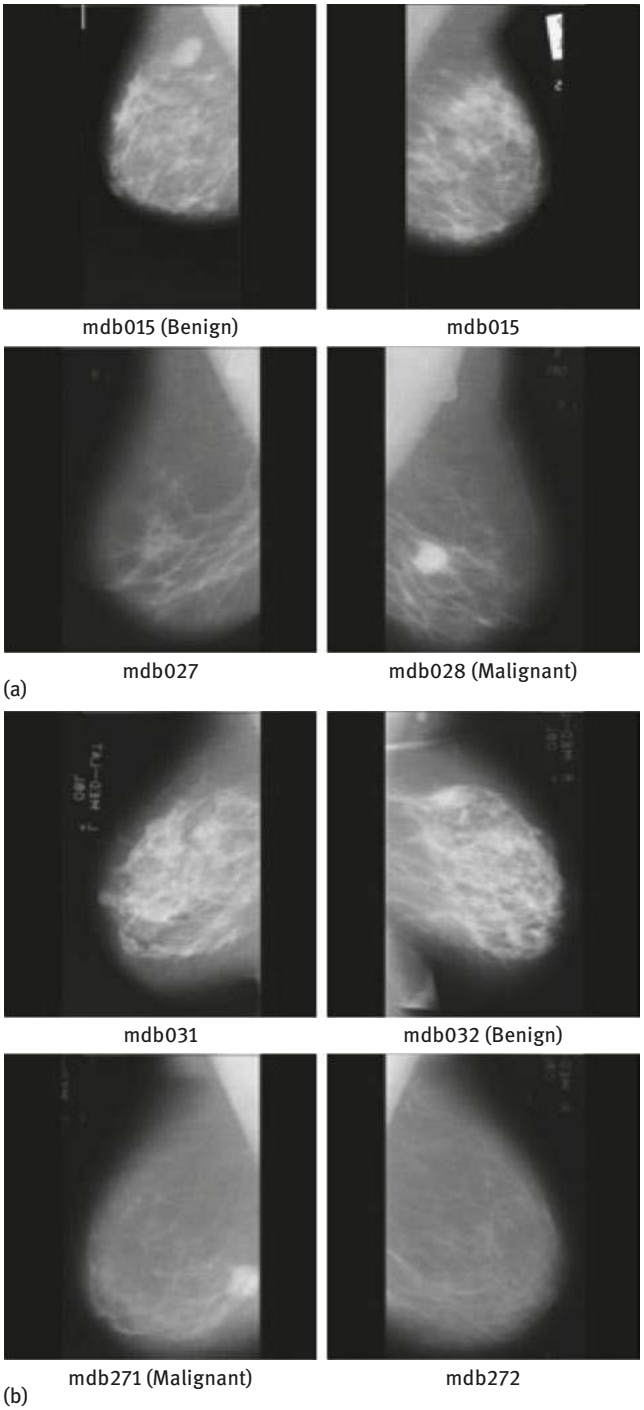
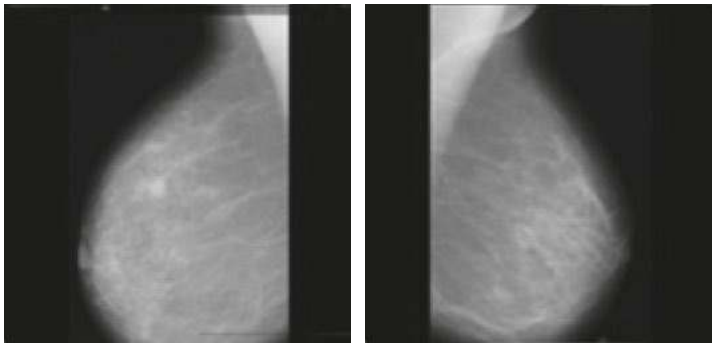
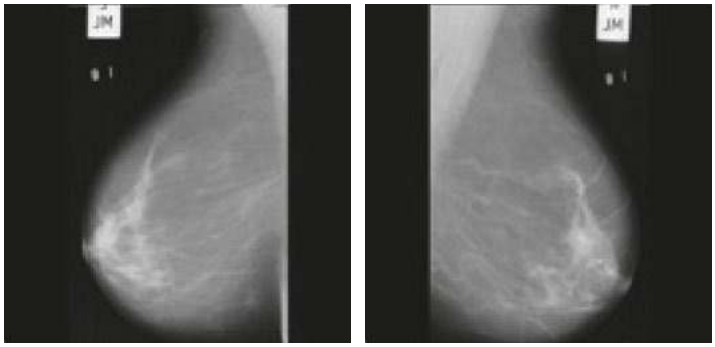


Figure 6.14: Circumscribed (a) and miscellaneous masses (b) from MIAS database.

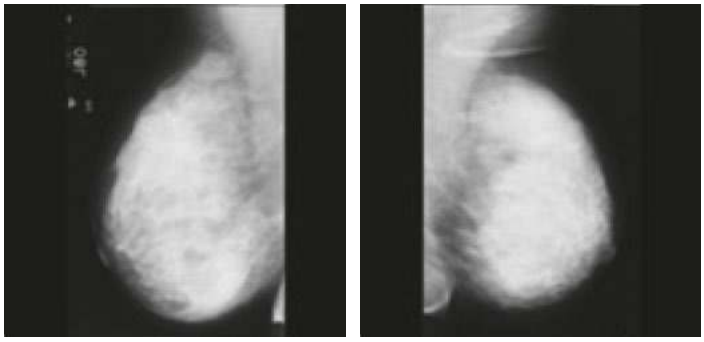


(a) mdb 155 (Malignant) mdb 156



(b) mdb195 (Benign) mdb196

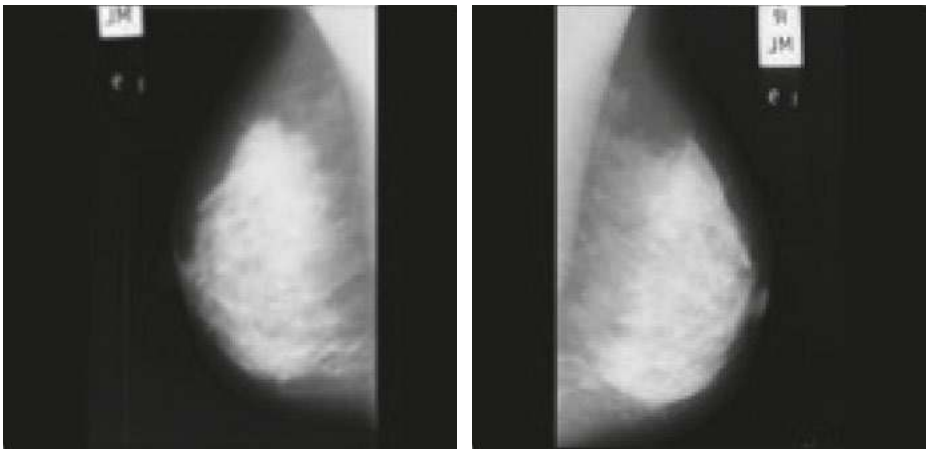
Figure 6.15: Architectural distortion (a) and spiculations (b) from MIAS database.



mdb239 (Malignant) mdb240

Figure 6.16: Microcalcifications from MIAS database.

as identification of masses like circumscribed and ill defined, identification of MCs and identification of spiculated lesions and architectural distortions. In that



mdb003 mdb004

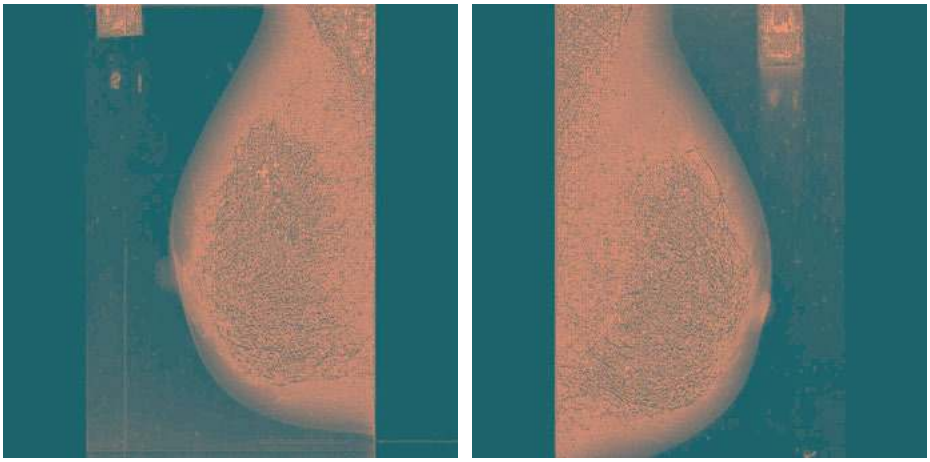
Figure 6.17: Original data.

mdb003 mdb004

Figure 6.18: Performing LBP.

clusters of MC is useful for early detection. For detection of abnormalities, statistical data analysis and feature extraction, ICA is used.

From comparison it was found that for texture feature, LAWS measures of texture, and for shape, compactness methods are best. MLP with recurrent NN provides more accuracy when compared with other classifiers. The proposed model is expected to predict the cancer at early stage, whether it is benign, malignant or



mdb003 mdb004

Figure 6.19: Laplace transform.

normal. Results can be improved without the removal of pectoral muscle from mammograms that minimize the computation.

References

[1] Nezhadian, F. K., and Rashidi, Saeid. "Breast cancer detection without removal pectoral muscle by extraction turn counts feature", Artificial Intelligence and Signal Processing (AISP), 2017.

[2] Bekker, A. J., Shalhon, M., Greenspan, H. and Goldberger, J., "Multi-view probabilistic classification of breast microcalcification," IEEE Transaction on Medical Imagine, 2015.

[3] Yang, Y., Nishikawa, R. M. and Cea, S. de. "Estimating the accuracy level among individual detections in clustered microcalcifications", IEEE Transaction on Medical Imaging, May 2017.

[4] Sim, K. S. and Ting, F. F. "Self-regulated multilayer perceptron neural network for breast cancer classification", IEEE International Conference on robotics, automation and science (ICORAS)-27–19 November 2017.

[5] Sun, Dongdong, Wangand, Minghui and Li, Ao. "A Multimodal Deep Neural Network for Human Breast Cancer Prognosis Prediction by Integrating Multi-Dimentional Data", IEEE Transaction on Computational Biology and Bioinformatics, 15 Feb 2018.

[6] Sherly, E. and Sreedevi, S., "A Novel approach for removal of pectoral muscles in digital mammogram", Elsevier, 46, 2015.

[7] Ao. Li, Chen, Peng and Zhang, Ya. "Improve glioblastoma multi-forme prognosis prediction by using feature selection and multiple kernels learning", IEEE/ACM transactions on computational biology and bioinformatics, 07 April 2016.

[8] Romero, E., Tarquino, J. and Naraez, F. "Applications of deep learning and reinforcement learning to biological data", IEEE Transactions on Neural Networks and Learning Systems, 2018.

[9] A1, A. Helal, K. I. Ahmed, H. A. Khan and Mostafa, R. “Abnormal mass classification in breast mammography using rotation invariant LBP”, 2017.
[10] Farag H. Alhsnony, Abdolrasol, Maher G. M., and Abadelrsool, Samei G. M. “Auto-identification of pectoral muscle region in digital mammogram images”, International Journal of e-Education, e-Business, e-Management and e-Learning, February 2014.
[11] Pan, Yuanyuan Zhang, Chen, Dehua, and Guangwei Xu. “Character-based convolutional grid neural network for breast cancer classification”, IEEE 2017 International Conference on Green Informatics, 15–17 Aug, 2017.
[12] Ponraj, Narain, and Mercy, Poongodi Merlin, “Texture analysis of mammogram for the detection of breast cancer using LBP and LGP: A comparison”, IEEE Eighth International Conference on Advanced Computing, 2016.
[13] Dcruz, Michelle, and Dr. Sarode, Tanuja. “Feature exraction in mammograms using NSCT and LAWS texture analysis approach”, International Journal of Engineering Research and Application, 7(8), (Part-6) August 2017, pp. 2248–9622.
[14] Reis, Sara, Gazinska, Patrycja, Hipwell, John H., Mertzanidou, Thomy, Naidoo, Kalnisha, Williams, Norman, Pinder, Sarah, and Hawkes, David J. “Automated classification of breast cancer stroma maturity from histological images”, IEEE transaction on biomedical engineering, 2016.
[15] Vikhe, P. S., and Thool, V. R. “Intensity based automatic boundary identification of pectoral muscle in mammograms, ELSEVIER, 7th International Conference on Communication, Computing and Virtualization, 2016.
[16] Saranyaraj, D., and Manikandan, M., “Medical image processing to detect breast cancer – A cognitive-based investigation”, IEEE 4th International Conference on Signal Processing, Communications and Networking (ICSCN -2017), March 16–18, 2017.
[17] Pengcheng, Xi, Goubran, Rafik and Shu, Chang. “Abnormality detection in mammography using deep convolutional neural networks”, arXiv:1803.01906v1 [cs.CV] 5 Mar 2018.
[18] Meriem, AMRANE, Saliha, OUKID, Ikram, GAGAOUA and Tolga, ENSARI “Breast cancer classification using machine learning”, IEEE, 2018.
[19] Faye, Ibrahima, Awais, Muhammad, Meriaudeau, Fabrice and Jamal, Syed and Gardezi, Safdar. “Mammogram classification using deep learning features”, IEEE, 2017.
[20] Hassan, Shayma’a A., Gouhar, Ghada K., Mohammed, S. Sayed and Farag, Fathi. “Pectoral muscle identification in mammograms for computer aided diagnosis of breast cancer”, CIBEC 2012.
[21] Nematzadeh, Zahra, Selamat, Ali and Ibrahim, Roliana. “Comparative studies on breast cancer classifications with K-fold cross validations using machine learning techniques”, IEEE, 2015.
[22] Chaima Derouiche and Akram Boukhamla, “Pectoral muscle boundary detection using digital mammograms” 2014.
[23] Andria, G., Nisio, A. D., Lanzolla, A. M. L., and Attivissimo, F., Spadavecchia, M. “Image quality evaluation of breast tomosynthesis,” IEEE, 2016.
[24] Moghaddam, H. A., Harirchi, F., Radparvar, P., Dehghan, F., and Giti, M.. “Two-level algorithm for mcs detection in mammograms using diverseadaboost-svm,” International Conference on Pattern Recognition, 2010.
[25] Cao, L., Li, Y., Chen, H. and Ma, J., “A survey of computer-aided detection of breast cancer with mammography,” Journal Health Med Informat, 2016.
[26] Cheriguene, S., Azizi, N., Zemmal, N., Dey, N., Djellali, H., and Farah, N. ”Optimized tumor breast cancer classification using combining random subspace and static classifiers selection paradigms.”, In Applications of intelligent optimization in biology and medicine, Springer, 2016.

[27] Virmani, J., Dey, N., and Kumar, V. ” PCA-PNN and PCA-SVM based CAD systems for breast density classification”, In Applications of intelligent optimization in biology and medicine, Cham : Springer, 2016.
[28] Bhattacherjee, A., Roy, S., Paul, S., Roy, P., Kausar, N., and Dey, N., “Classification approach for breast cancer detection using back propagation neural network: a study.” In Biomedical image analysis and mining techniques for improved health outcomes, IGI Global, 2016.
[29] Baker, Abu, Ayman A., Qahwaji, R.S, Aqel, Musbah J., Al-Osta, Hussam, and Saleh, Mohmmad H.. “Efficient Pre-processing of USF and MIAS Mammogram Images”, Journal of Computer Science, 2007.
[30] Zemmal, N., Azizi, N., Dey, N., and Sellami, M., “Adaptive semi supervised support vector machine semi supervised learning with features cooperation for breast cancer classification.” Journal of Medical Imaging and Health Informatics, 6(1), 2016.

Akshada Rathod and Sambhaji Sarode

7 Deep brain monitoring using implantable sensor and microcontroller: a review

Abstract: The consequent evolution in technologies is reaching toward development in today's world. Microelectromechanical system (MEMS) technology is one of the emerging paradigms that signify continuous affection in healthcare systems. In hospitals, it is very necessary to constantly examine the health condition, monitor movements and physiological parameters of a patient. Collection of data, long-term connectivity of sensors with the network, data privacy maintenance, treatment over a number of neurological disorders and storage of diagnostic results is a very critical task in such organizations. Every bit of data is required to store in some specific format, and loss of data will generate the false result. To overcome such problem, different types of biomedical sensors and instruments are developed using MEMS technology. In this chapter, the deep brain monitoring using implantable sensors and microcontroller is used for treating number of neurological disorders, such as dystonia, tremor, Tourette syndrome, Parkinson's disease, cluster headaches and major depression. The technique includes electrodes embedded inside specific regions of brain and monitoring activity of patients remotely.

Keywords: Pulse generator (PG), Internet of everything (IoE), real-time brain monitoring, biomedical sensor, microcontroller, stimulation parameters

7.1 Introduction

Today's healthcare system is dominated with IoE (Internet of everything), which uses ambient intelligence (AmI) system. Aml is a collection of several smart devices that are active in the environment. They are well designed and developed in such a way that it automatically sync, control and manage connectivity with other sensor devices. Various applications depend on the sensors like a wireless body sensor network (BSN), biometric sensors, a wearable sensor, motion detection sensor and implantable sensors, these are developed using AmI and Internet of things (IoT). Advancement of a micro-electro-mechanical system (MEMS) technology leads to growth in these devices in recent years.

eHealth technologies give prominent features for minimizing healthcare expenses and enhance patient care in large scale. For measuring different parameters like pressure, temperature, and sugar level of humans, a "smart implant" technology is manufactured by the medical researcher, and also wearable sensors like smart watch, which is used to detect blood pressure (BP), heartbeat count

https://doi.org/10.1515/9783110628517-008

and posture aid. Biosensors could detect the internal state of the human body using electromagnetic radiation. Cancer cell within the body has been identified using nanotechnology. Because of enhancement in such sectors using MEMS technology [1], patients are not needed to visit the hospital on an everyday basis and it made really easy for caretakers to keep track of every activity of patients remotely.

Embedded devices are used to transmit and receive the signal to the devices present in the vicinity. Emerging evolution is occurring with the development of an IoE [2]. IoE has the ability to sense and collect data from around the world and share data across the network, where it is being processed and utilized sequentially. IoE is the collection of various devices, which are based on standard communication protocols. This technology extensively used to communicate about their internal and external environment between several device components. Communication between the devices is managed via secure networking and standard wired or wireless communication protocols. Embedded devices are capable to collect heterogeneous data from the proximity and can be processed, monitored and controlled remotely; these devices are components of IoE. Analysis of collected data locally is done using edge or mobile devices. IoE-based microcontrollers, microprocessors and sensors are integrated collectively to accomplish an appropriate task to minimize the human interaction with computers [2, 3].

In the United States, Medtronic is the world's largest medical technology organization. They have an advanced product named deep brain stimulator (DBS) device, which safely and efficiently manages tremor, rigidity and bradykinesia related to Parkinson's disease (PD). The drawback of this product is its high cost. At present, in India 35–45% of the population suffering is from PD, out of which 28–35% population cannot afford such high-value products [4]. An expected 30% of individuals with PD are analyzed before the age of 50.

In India, current research on DBS is carried out to provide proper medical care for PD patients [5–7]. DBS technique is a neurosurgical procedure in which electrodes are inserted inside specific region of the brain that connects to the device through an extension cable. This device helps in delivering electrical stimulation to those specific regions. Same as cardiac pacemaker shown in Figure 7.1, the technique uses a biomedical device called a pulse generator (PG) [8] to control the flow of electrical pulses inside the brain, thereby preventing the production of irregular nerve signal that causes PD. The general system for deep brain monitoring consists of an electrode implanted into the brain of the patient, which is connected to the implanted device located in the chest area or the abdomen through extension lead wire. The electrode and implanted device form a closed circuit. The device communicates with the external software application. The whole system runs on rechargeable battery that resides inside the implantable device and is periodically charged wirelessly from outside the body.

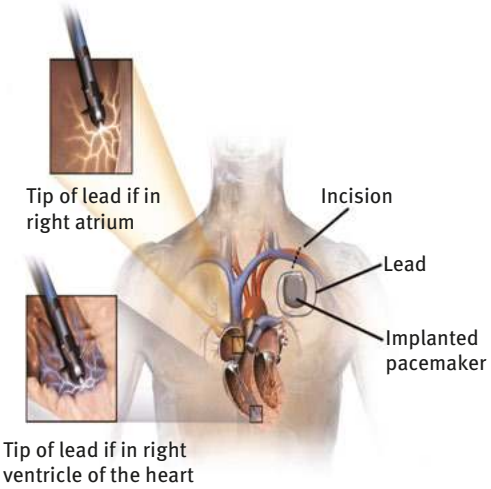


Figure 7.1: Cardiac pacemaker.

7.2 Related work

A brief glimpse of this study gives the overall idea of what exactly the e-health care system works to track and monitor the activities of patients remotely. The related work gives an overview of medical sensor-based different application such as various real-time e-healthcare application, remote monitoring of the patients, doctor–patient relationship management, "cloud network to store data related to the patient [22]." IoT cloud infrastructure and stimulation of pulse parameter using sensors. Finally, the summary of the survey has been carried out by reviewing related studies.

Behari et al. [4] focused on philosophical data on PD by investigating two risk components, as there is no data on transmission and control of Parkinson's available in India. For the investigation, they studied few Parkinson's patients and the same number of healthy people of the approximately same age. As PD is a rare disease and only occur at age above 60 years, it makes the study of risk components little difficult. Data for this chapter was collected by face-to-face interview with the patients. Information was classified based on the structure of the human population, various environmental components, history of depression and PD in the family and occupation. Authors set some rules to collect more accurate data. While studying, authors considered various use cases, which include case-matched control and age-matched control. Data were categorized with the help of different combinations of use cases. They also calculated McNemar chi-square value, which is a contingency table for paired data. Authors also calculated the *p*-value (potential risk component value). Their results showed that the probability of growing PD is more if

a person has PD in his family, if that person has a history of depression and is a male, and if he drinks well water, but spending time with pets and alcohol intake can reduce the chances of PD. They also found that a vegetarian diet, living in a population-less environment has no relation between these components and PD. According to the authors, these environmental components are also critical as genetic components.

Albayrak et al. [9] implemented the system based on an electronic survey for health care. This system is designed for early discovery of diseases like an epidemic disorder, which can be remotely monitored. The system dynamically activates to perceive the health status of patients. Doctors and health specialists can actively control and monitor the status of individuals by collecting the survey from individuals through electronic devices and create geographical risk maps. The proposed system has been tested in two sections: one is professional and another is an individual. In a professional method, the medical status evaluation has been carried out by clinicians as they distribute blueprint of reports to each patient through a software application. In an individual method, patients fill those reports and provide all the information about their health condition. Clinicians can easily evaluate the medical status of patients as per the response given by patients in the form of a report. Web-based application for monitoring of patients with PD was proposed by Chen et al. [10], wherein system provides an integration platform for services to execute at three different layers. Wearable sensors attached on patients' body gather accelerometer data. The web-based user interface permits two-route communication among patient and clinician hosts. Clinicians can get to the sensor and patient information and communicate to patients using the video conferencing. Authors evaluated latencies and bandwidth prerequisites at various levels of the framework. To guarantee estimation precision, all hosts synchronized to a similar network.

Chen et al. [11] studied and implemented a real-time remote monitoring system for PD patients with DBS. The system comprises four modules: a patient client, a physician client, video communication and a server station. This system provides web service on the Internet, the server station sets up a virtual connection between the patient and physician client. The physician client helped nurses to observe adequate data about the patients and giving alteration guidelines to the patient client through the wireless communication channel. After instruction execution, the patient client uploads the history records and results to the server station. Li et al. [12] proposed a pervasive healthcare monitoring system that can transmit patients' vital signs continuously to remote medicinal applications. For implementation authors focused on two modules: first the data acquisition module and second the data transmission module. The first module is responsible to collect data from biomedical sensors and forward it to the connector in short distance. In the second module, remote services receive sampled data from sensors and results are displayed to cardiologists in real time.

Monti et al. [5] investigated difficulties occurring in medical implantable devices operated at low-frequency range, which uses same wireless communication link for transmission of data and power. Authors examined wireless energy connection interface working in the MedRadio band. From the detailed analysis, authors illustrated the energy transfer efficiency of about 10.62%. Cubo et al. [6] present DBS therapy for PD, developed in order to reduce the seriousness of diseases by adjusting stimuli parameters. The authors described the methodology by simulation and clinical information acquired through medical imaging, electrical estimations and target side effect measurement. This system is developed using open- and closed-loop methodology. Stimulus parameters are manually set by doctors in open loop, whereas closed loop illustrates strategies used for evaluating motor symptoms and electrical estimations.

Smart DBS (SDBS) is implemented by Khan et al. [7] for evaluating the performance of stimulator. The essential functions of the SDBS incorporate movement recording, data interpretation, signal processing, stimulus waveform creation and optimization. Gope et al. [8] describe the importance of security requirements in BSN-based popular healthcare application. The authors proposed a protected IoT-based healthcare application using the authentication protocol and BSN, which helps in minimizing various existing security problems. BSN model includes two types of sensor networks (SNs): first is on-body SN, which provides a connection between wearable devices [19] and a coordinator; second is in-body SN, which provides a connection between implanted devices and the base station. Authentication protocol also includes two phases: first is the registration phase, where safety credentials are provided to the system through a secure channel; second is the anonymous authentication phase, where data transmission takes place.

Rahmani et al. [17] studied fog computing and its usage in IoT-based application. Smart gateway application offers several services at the network edge like processing, storing, compressing, standardizing and notifying. Fog computing forms an intermediary layer between sensor nodes and cloud for executing several services at the network edge. In processing service, a huge volume of sensitive data is controlled continuously in less time and response gets generated appropriately in different states. In filtering service, sensors receive multiple types of data to execute a proper processing algorithm at the network edge. In compression service, transmission latency and power consumption get reduced throughout the performance. Depending on the application requirement compression service is applied. In the fusion service, amount of data reduced by enabling the system efficiently. In analysis service, utilizing local data analysis at the endpoints increases the sensitivity of the application. It helps the system to recognize the emergency circumstances. In the local storage service, it ensures that the system can easily retrieve the data. An entry point should store the incoming data in nonvolatile memory of local storage.

Alelaiwi et al. [18] proposed smart services for the elderly and physically impaired individuals. The smart home system is designed and developed using

technologies like 5G network, cloud intelligence, BSN and wearable computing. This system is helped to provide an advantage over cost reduction, patient care remotely. Authors provided a solution to overcome some technical difficulties related to the smart home system. This system utilizes distributed computing and IoT framework to gather real-time data of environmental state from home for a secure living of patients. Systems generate the health report and broadcast alert message to family members and doctors. BSNs gather information regarding body temperature, electrocardiograph (ECG) and BP. The collected data was forwarded using Bluetooth technology to the cell phone and afterward, the same data was transferred through the Internet to a cloud server. Cloud server uses the central processing unit, a memory unit, a transmission unit, a graphical processing unit and different data mining algorithms.

Baktir et al. [14] proposed cloud computing (CC) and communication design for end-user devices. The active designed administration demonstrates all arrangements connected inside this system that completes an idea for programmable systems as software defined networking (SDN). To demonstrate the idea designed by the authors, they implemented a fall risk evaluation service. An experimental evaluation was carried out for accurate detection and performance-designed framework. The final output represents that the designed framework can be modified in real time and provides advantages over conventional methods. Mahmoud et al. [15] introduced CoT (cloud of things) models and the execution of model with human services also defined. Authors resolve missing institutionalization-related issues by model. Enhancement in quality of service and execution is needed for improving the productivity of the system. CoT is the combination of CC and the Internet. Table 7.1 illustrates the wireless communication standard protocol used in BSN.

Buston et al. [20] studied about the volume of tissues activated in different patients. They found out intersection between the activated volume of tissues and anatomical structures and compared the results with the actual clinical outputs. The system consists of three models. First is a 3D anatomical model that is derived from magnetic resonance imaging (MRI). Second is a finite element model (FEM), and third is volume of tissue activated (VTA) prediction deriving model. This approach is used to monitor subthalamic nucleus DBS in the patients suffering from PD. Here the postoperative MRI report is used to find out electrode location. Intensity values near to electrode are compared with slightly lower values of intensities. The first step is to correlate the MRI image and brain atlas wrapping. This is done using software tool from Surgical Navigation Technologies. The second step is to create biometric field model where variable resolution meshing algorithm is used to minimize the number of nodes and increase accuracy of the result. The third step is VTA prediction that is done using voltage solution of FEM. Clinical evaluation of patient is done followed by data analysis. The authors performed various clinical experiments held around 1-year post-medical procedure. Information is accounted for the left DBS anode. The patient's health was evaluated using two clinical

Table 7.1: Wireless communication protocol used in BSN [5, 13–16, 27, 28].

Parameter	Bluetooth (IEEE 802.15.1)	ZigBee (IEEE 802.15.4)	6lowPAN (IEEE 802.15.4)	Wi-Fi (IEEE 802.11)	NFC (ISO/IEC 18000–3)	LoRaWAN (IEEE 802.15.4)
Description	Exchange of data in small chunks	Intermittent data exchanges at low data rates	Exchange IPv6 packets over network	Exchange of large data in vicinity of wireless router	Exchange of data by putting devices very close together	Exchange of data over long distance with network server
Uses	IP configuration infrastructure	Low power digital radio signals	Header compression mechanism	Radiowaves for connectivity	Peer-to-peer communication	Chirped modulation format
Data rate	1 mbps	250 kbps	250 kbit/s	54–600 Mbit/s	100–420 kbps	0.3–50 kbps
Frequency	2.4 GHz	2.4 GHz	2.4 GHz	2.4 and 5 GHz	13.56 MHz (ISM)	433, 868, 915 MHz
Range	50–150 m	10–100 m	116 m	50 m	10 cm	2–5 km (urban area), 15 km (suburban area)

methods. Each analysis was conducted in the morning when the patient is in the vaccination state. During the first trials, the following conditions are required to produce monopolar stimulation: 2 Hz of frequency, 60 μs of pulse width and 0 to −10 V of the reference voltage with 20 s of the time interval. During the second trials, reference voltage differs from 0 to −4.5 V with 130 Hz of frequency, 60 μs of pulse width needed to produce monopolar stimulation.

7.3 Methodology of existing systems

Monti et al. [5] proposed a wireless connectivity provided by DBS for stimulating pulse. Implantable therapeutic devices perform an important function for treating diseases, for example, cardiovascular disease, neurological dysfunctions and intense type of diabetes. Wireless technologies [21] deliver an essential function to enhance the execution of these devices.

The wireless connection comprises two magnetically coupled resonators, that is, external resonator and implanted resonator illustrated in Figure 7.2. Both resonators possess a thickness of 1.18 mm and a frequency of 403 MHz. An external resonator occupies an area of 1.986 × 1.986 cm from the skin surface. An implanted resonator occupies an area of 1.594 × 1.594 cm that working at a profundity of 0.5 cm beneath a 0.2 cm layer of skin, a 0.2 cm-layer of fat and a 0.1 cm layer of muscle. The rate at which energy is consumed by the human body due to interaction with electromagnetic radiations is defined as specific absorption rate. It also defines the power dissipation rate per unit mass of tissue. Scattering parameters of a wireless connection were determined by methods of full wave stimulation.

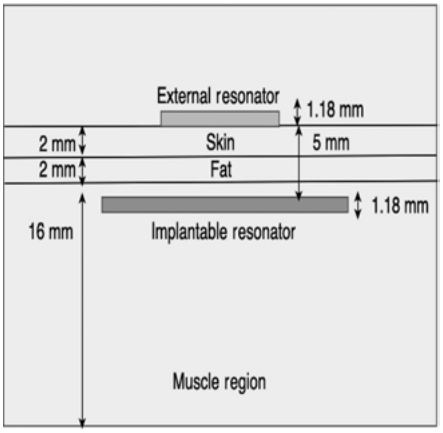


Figure 7.2: Geometry of external and implantable resonator.

DBS therapy is facilitated by numerous communicating elements. An implanted pulse generator (IPG) that is precisely put under the skin close to the collarbone produces the electrical oscillations. These oscillations transmitted within a lead to the brain. The user interface is used for the doctor and the patients to impart the best possible settings to the PG and determine the real-time status. The authors define specification of stimulation parameters properly in the study [6]. IPG produces 10 V of amplitude, few milliamperes of current, 100–250 Hz of frequency and pulse width up to 60–120 μs. A disease-specific stimulation target is characterized before the operation. With mathematical modeling, the preferred target must be prepared from medicinal pictures of the patient's brain. This can be performed by utilizing programming or physically.

Special conjectures must be made to measure neuron activation. In the stationary stimulation state, the thresholding of activation function and electric field are obtained. The threshold rate relies upon a few variables, that is, neuron thickness, neuron connectivity, pulse width and pulse polarity. Average thresholds utilized in the method are 20 mV for the activation function and 150–200 V/m for the electric field.

Authors developed the system using an open-loop and closed-loop model is depicted in Figure 7.3. In the open-loop stimulation, using the trial-and-error mechanism doctors physically adjust stimulus parameters. In the closed-loop stimulation, local field potential (LFP) desynchronization and impedance control approaches are reviewed. Computation of LFP in the region of the lead and evaluation of signal power in the beta-band is accomplished by LFP desynchronization method. The drawback of the LFP method is that this approach lacks additional functionality and power. Impedance measurements utilized in the evaluation of the electric properties of the lead–brain tissue interface.

As per the architecture of SDBS [7] designed by the authors, the intelligent anode can send important information to the outer controller through the secure wireless remote connection and the cathode. In this case, RFID (radiofrequency identification) is used as outer controller. The precise study explains system design methodology and its uprightness with the current RFID standard. The LTE/Wi-Fi connection provided to outer controller work acts as an entry point to/from the processing layer. The SDBS prototype configuration has two essential building blocks, one is an analog front end and another is digital core. Analog front end includes an antenna, network, modulator, demodulator and signals block, whereas design core includes implementation of the standard communication protocol, activity capturing and waveform generation methodology. Implementation of the digital core was carried out with the help of a well-known hardware module known as ARM CortexM0 and ATSAMD20E18 microchip.

Generation of stimulus waveform is based on two techniques: one is the commands and another is arbitrary sampled information collected from the brain. The command-based technique of SDBS is demonstrated in Figure 7.4. The decoder translates the command sent by the outer controller and transfers pulse

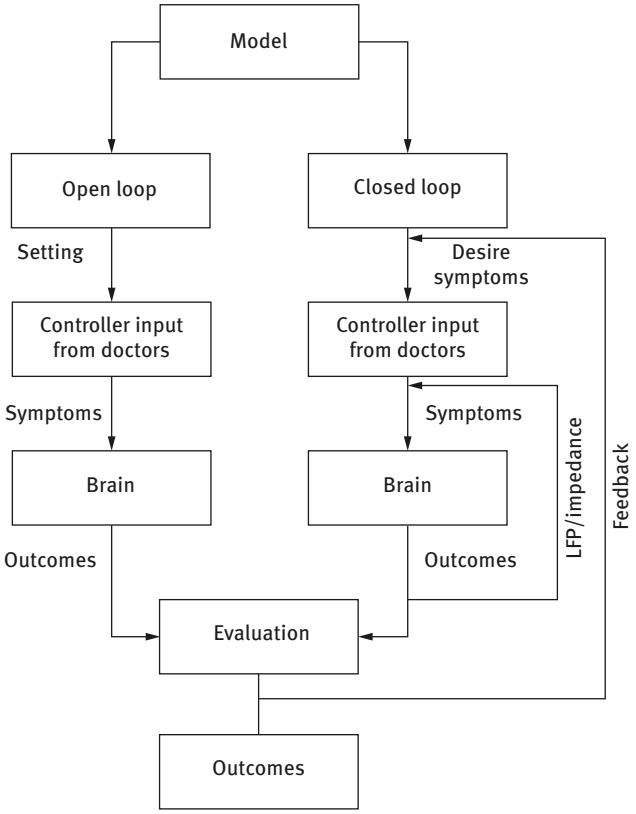


Figure 7.3: Flowchart of open-loop and closed-loop model.

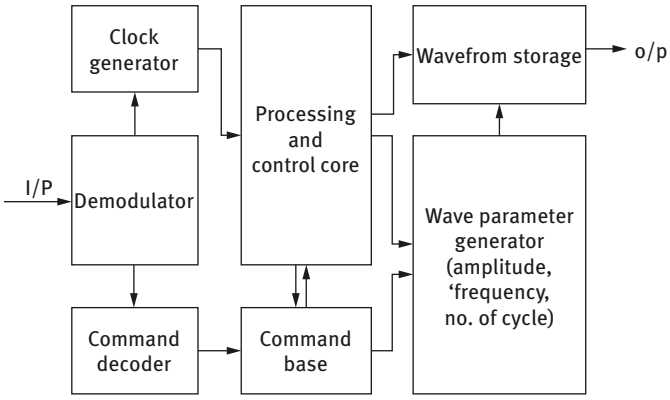


Figure 7.4: Block diagram of the stimulation generation [7].

amplitude, pulse frequency and stimulation duration parameters. Command base stores related parameters temporarily for smaller scale handling unit. In SDBS design, 8-bit resolution (digital–analog converter) DAC operating with the 1 MHz clock frequency and the reference voltage of 2.5 V, electrode uses 3.9 kHz of frequency to generate a waveform. The extreme value for pulse amplitude and pulse frequency is set as 2.5 V and 2.5 kHz, respectively. Neuroactivity recording and processing module comprises a CPU, processing unit and (analog–digital converter) ADC that is designed to record the LFP of the neural activity. Eight-bit ADC operating with the reference voltage of 2.56 V is required for converting analog signals to digital signals. The intelligent electrode produced a stimulation waveform parameter depicted in Table 7.2.

Table 7.2: Sinusoidal waveform parameters.

Parameters	Amplitude (mV)	Frequency (kHz)	No. of cycle
Test 1	800	2.5	5
Test 2	800	2.5	10
Test 3	800	2.5	20

Heart disease is a major cause of death nowadays. Immediate treatment to a patient suffering from heart disease is crucial. However, heart patients call the service themselves very late when the condition of disease is irreversible. This happens because the patient realizes the problem very late. Therefore, work needs to be done early for diagnosis of heart diseases. Internet of things solve this problem potentially. Patient's physical status is monitored by the physician continuously irrespective of where the patient is and what he is doing and based on the situation the physician will decide when to give treatment to the patient. Li et al. [12] have described IoT-based solution for constant monitoring of patients' physical parameters like BP, ECG and SpO_2. The authors described system architecture using four different transmission modes based on the medical need and feasibility of communication technologies [29].

A prototype implementation is done to represent the system data acquisition part or sensing layer comprises sensors worn or carried by patients. The sensor device is chosen based on parameters to be monitored and the sampling frequency of each parameter. Considering medical demands and a practical feasibility-monitoring scheme is decided. The sampling frequency of ECG signals is set to 128 Hz. Sensing of BP, pulse rate and SpO_2 level is carried out in the interval of 2 s. Testing of blood fat and blood glucose is conducted before and after a meal. The data transmission process is subdivided into two processes. Communication technologies required for these two subprocesses are different.

Data transmission from the sensor to the connector happens in short distance, which requires high bandwidth. Authors chose Bluetooth technology and smartphone as a connector for first subprocess. Once connector receives the data from the sensor it transfers these data to a remote site through another communication technology comprising second subprocess. The range of technology is a crucial part of the second subprocess. Cellular wireless technologies (GSM, GPRS) and wired technologies (ADSL) are used for the second subprocess. The data transmission [30] is performed in four modes: (a) in the first mode, continuous transfers of all data to the physician in real time are achieved. This is the highest monitoring level used for the patients who are at high risk of relapse by heart diseases. (b) In the second mode, a continuous transfer of data in the fixed time period is performed. Empirically heart attack takes place from 3 to 4 pm or within 2 h after waking up. Thus in this mode data transfer is continuously done during this period. (c) In the third mode, sampled data is sent to the connector using an event-triggered transmission mechanism. At connector, analysis of these parameters is performed and if the parameters are beyond the normal range it triggers an event. When an event triggered, transmission of data from the connector to the physician's server is carried out experimentally. (d) In the fourth mode, the physician's server receives the sensed parameters from the patient's body whenever they feel uncomfortable. As explained, the four modes are not quite the same as one another in the measure of information sent to the remote server, the necessity for network quality and the applicability for various kinds of patients.

Authors developed a system using MercuryLive architecture [10], which incorporates programming services running at three levels: a central server, patient's hosts and clinician's hosts. A central server provides a secure channel for data gathering and video forum service. The secure channel includes encrypted services, a secure sockets layer, Secure Shell and a virtual private network. In this layer, both patients and doctors can have direct access to the web server, database, data forwarding service and a video conferencing service. In the patient's host layer, doctors can set an ideal battery life status. As sensor information is being gathered, an information transfer demon keeps running in the interface background and then transfer the collected sensor information deftly to the central server. In clinician's host layer, doctors manage information-gathering sessions remotely. Doctors get the patient information and address patients utilizing the video conferencing administration if necessary. To describe MercuryLive architecture, authors surveyed latencies and bandwidth prerequisites at a various layer of the framework. Latency measurement depended on either timestamp gathered at each host or packet delivery at every MercuryLive layer. To guarantee estimation precision, framework clock was synchronized to a similar Network Time Protocol.

7.4 Components required for deep brain monitoring

This section describes the general components for brain monitoring e-healthcare system, which consists of implantable components and external components [6, 7]. There are three types of implantable components, namely, a lead, PG and an extension. Main external components for brain monitoring system are desktop application (DA), mobile application (MA) and wireless charger (WC). General architecture of PG for deep brain monitoring is shown in Figure 7.5. Description of each of the components is as follows.

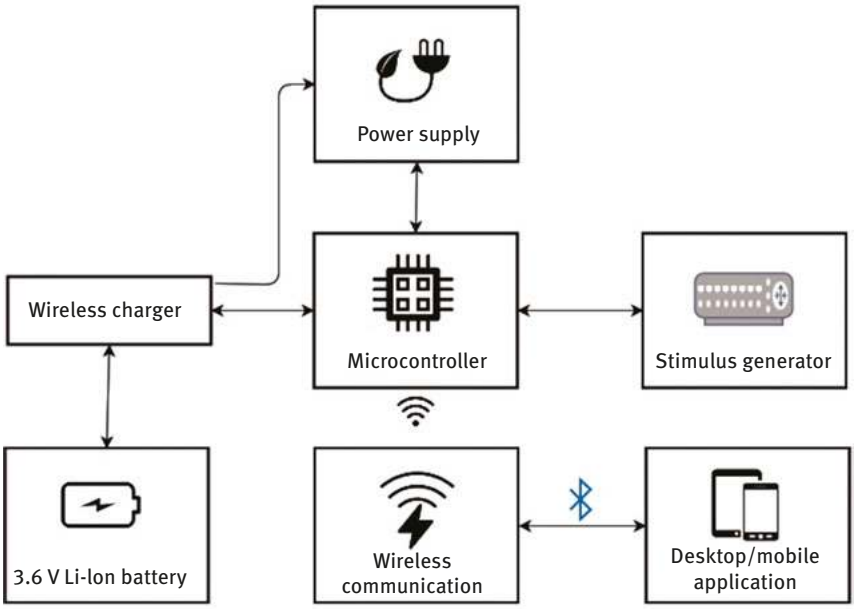


Figure 7.5: Architecture of pulse generator (PG) for deep brain monitoring.

7.4.1 Implantable components

Electrode leads: The leads consist of four electrodes that provide stimulation parameters to a certain region of the brain [6]. These stimulation parameters are generated by PG. The leads are stereotactically introduced into the affected region of the brain as depicted in Figure 7.6.

Extension: The extension is a combination of wires. Electrode leads are attached with PG through an extension cable that provides an electrical path. The extension cable is embedded inside the scalp area, where it connects leads with an implantable device.

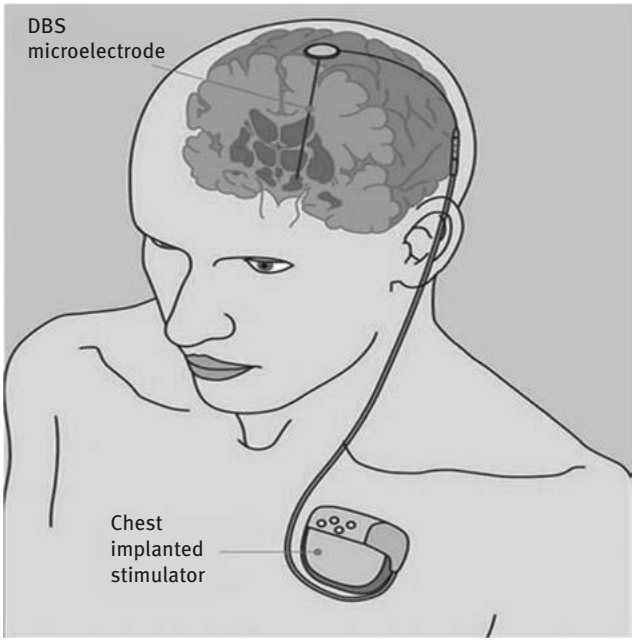


Figure 7.6: Placement of implantable components inside the human body.

PG: The PG is the heart of the DBS. Its main function is to generate stimulus parameters from an external software application over a wireless communication interface. It works from a rechargeable battery with a wireless charging interface. PG consists of the following parts: (a) stimulus generator, (b) rechargeable battery, (c) wireless charging interface, (d) wireless communication interface [31, 32] and (e) microcontroller for overall control and monitoring of the device [5, 6]. Specifications of PG are have programmable pulse parameters in the following ranges: (a) Pulse Amplitude – 0 to 5 V (voltage mode) adjustable in steps of 0.1 V and 0–20 mA (current mode) adjustable in steps of 0.1 mA, (b) pulse frequency – 200 Hz range approximately, (c) pulse width – 30–400 μs, adjustable in steps of 10 μs, electrode configuration – two leads for two brain hemispheres and four electrodes per lead. Pulse parameters are depicted in Figure 7.7.

Generation of waveform carried out using timer/counter function facilitated by the microcontroller. The timer in UP/DOWN mode is used for an electrode to generate pulse signals. Generation of waveform controlled by DAC with the reference voltage of 2.5 V named as (D0). Selection of electrode is controlled by MUX (M0). Once the timer started, 500 kHz of frequency is required to generate each pulse that takes around 1 μs of the period. Timer consists of register, that is, A1 to A6 and B1 to B6 to store obtained values as represented in Figure 7.8.

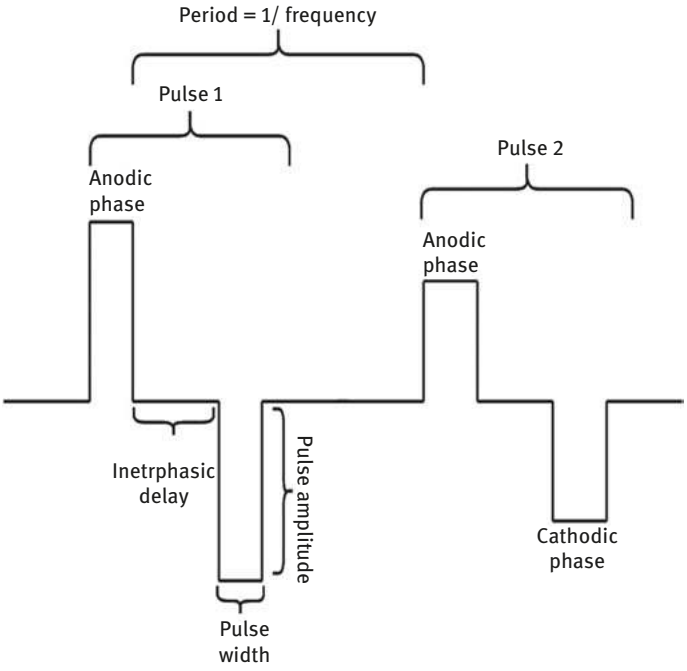


Figure 7.7: Pulse generation parameters.

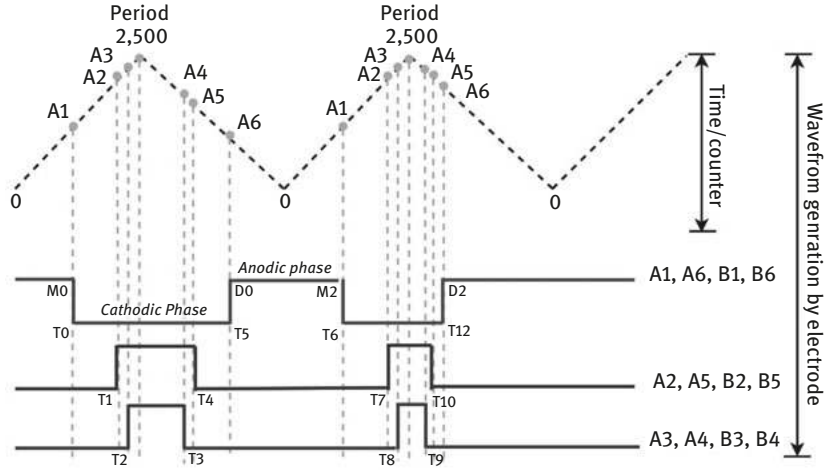


Figure 7.8: Pulse waveform generation by an electrode.

7.4.2 External components

DA: The DA is designed for use by a clinician, doctors and expertise to verify parameters settings. Using this software interface doctors can monitor the state of patients. This is designed to provide appropriate wireless interface for communicating with the implanted device.

Mobile application (MA): The mobile-based application communicates with PG via Bluetooth technology. Functionalities of this module are as follows: (a) patient or caregiver can control therapy state, (b) the user can check the status of the implanted battery and (c) allow the user to adjust the setting of pulse amplitude, pulse width and pulse rate within the clinician-prescribed limits.

WC: A wireless battery charger is used to charge the implanted device. Rechargeable frequency and time for WC is 1 day and less than 5 h, respectively. Algorithm 1 illustrates the DBS using MCU (microcontroller unit) system implementation initiating via software interface.

The advantage of the deep brain monitoring system is to enhance motor function, improve personal satisfaction and diminish medicine for patients. Treatment can enable patients to have an increasingly ordinary and autonomous way of life. It also helps in improving medicate-related confusions.

Algorithm 1: DBM using MCU system implementation.

Input: Clinician / Patient input parameter (Login details, Stimulus parameter setting)
Output: Actions (Therapy Program – START/STOP, Pulse Generator – Activate/Deactivate, External Components – Active/ Non-Active, Battery State – ON/OFF)
Begin: DBM using MCU
Connect PG to external component using wireless communication protocol.
Case 1: START / STOP the therapy session
If Patient health status is abnormal **then**
START therapy program session //via MA
Else If Patient health status is normal **then**
STOP therapy program session //via MA
End If
End If
Case 2: Continuously monitor health of patient using software interface. //via MA and DA
Case 3: Wireless charging
If Battery State == Low **then**
ON Battery Charging process using wireless charger
Else if Battery State == Full **then**
OFF Battery Charging process
End if
End;

Table 7.3: Comparison between different existing systems.

Parameters	Aim	Technology	Advantage	Future scope
Albayrak et al. [9]	Providing health services instantly and efficiently via the transmission channel independent of space and time between health experts and the patient.	Bootstrap 3 CSS framework for front-end and PHP and MySQL for back end.	Provides active control over patients' own health status.	To generate geographical risk maps of diseases.
Chen et al. [10]	Data gathering using wearable sensors via a web interface.	MercuryLive architecture, Red5 server	Latencies and bandwidth at various levels of the framework is evaluated.	To store and display results of gathered data in a home setting.
Chen et al. [11]	Providing remote adjustment service and real time monitoring of PD patients with DBS.	Microsoft .NET framework, Bluetooth module, RF module	The framework provides remote control to caregivers and allows to check the historical record and also implement programming in real time.	To perform a first clinical trial under real time to test the usability and efficiency.
Li et al. [12]	Assist remote expert to be informed about patients' condition and diagnose serious conditions of heart diseases.	Bluetooth technology, cellular and wired technologies	Remote services receive sampled data from biomedical sensors and results displayed to cardiologists in real time.	To combine the data stream management system (DSMS) technologies into the existing system to improve its functions.
Cubo et al. [6]	Manipulation of stimulus pulse parameters using mathematical modeling, so patient can adjust stimulus parameters.	Low-frequency wireless technology.	Treatment over a number of neurological conditions using implantable sensors.	To work on safety measurements at a higher level.

(continued)

Table 7.3 (continued)

Parameters	Aim	Technology	Advantage	Future scope
Rahmani et al. [17]	Local data processing, data filtering, data compression, data fusion, data analysis.	Fog computing, 6LoWPAN, cloud server, eHealth gateway, geo-distributed fashion at the edge of the network.	Use of multiple data processing algorithms.	To improve API for gateway management using different transport layer protocol sockets for easy interoperability with different protocols.
Alelaiwi et al. [18]	Distributed computing and IoT real-time data collection of environmental state from home for a secure living of patients.	5G network, cloud intelligence, BSN, wearable computing	Generating health report (a) Monitoring of biosignals from BSN and smart phone, (b) context-aware sensing and (c) context-based recommendation. Alerting via broadcast message to family members and doctors.	To use different gadgets to recognize passionate information.
Baktir et al. [14]	Implemented load-balancing mechanism at edge servers. Real-time fall risk assessment using wearable sensors.	Machine learning model	Update and tracking the locations of the personal records regularly for each user.	To store data for long term.
Mahmoud et al. [15]	IoT cloud acts as middleware for managing cloud IoT foundations. IoT body sensors collect the required information, investigate and concocted in the cloud. CoT-based architecture model for isolation.	IoT cloud, Wi-Fi, WPAN	Helps to understand new technology for improvising healthcare sector.	To focus on an energy-aware allocation strategy for future research.
Buston et al. [19]	Using DBS to detect how much volume of tissue gets activated and calculate the range of pulse stimulation parameter.	3D nonlinear warping algorithm	User-friendly software interface developed for doctors and researcher to design their private DBS model.	To concentrate on treating other neurological diseases.

7.5 Observation

This section describes the general comparison between various existing applications using Table 7.3.

7.6 Conclusion

This study introduces the architecture and concept of deep brain monitoring and controlling using implantable sensors. IoE-based e-healthcare survey helps to deliver a unique medication approach to PD patients from India. The fundamental functions of the deep brain monitoring include patient activity monitoring, waveform generation using PG, therapy status checking, body movement controlling, information gathering, data forwarding, data analysis and many more. The existing application is developed to treat patients suffering from neurological disorder and research carried out by various researchers. These systems describe different methodologies used for healthcare applications that provide great practical significance approach in the treatment of PD patients. The research represents functionalities of the electrode and the stimulation pulse parameters in such a way that the DBS system is able to provide an adequate amount of stimulation without causing any harmful side effects to the tissue or patients body.

References

[1] Gardner, Julian W., and Varadan, Vijay K.. Microsensors, MEMS and smart devices, John Wiley & Sons, Inc., New York, NY, USA, 2001. (MEMS)

[2] Miraz, Mahdi H., Ali, Maaruf, Excell, Peter S., and Picking, Rich. "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," 2015 Internet Technologies and Applications (ITA), Wrexham, 2015, pp. 219–224.doi: 10.1109/ITechA.2015.7317398.

[3] Mineraud, Julien, Mazhelis, Oleksiy, Xiang Su, and Tarkoma, Sasu. "A gap analysis of Internet-of-Things platforms," Computer Communications, 89, 2016, pp. 5–16.

[4] Behari, M., Achal K. Srivastava, Radhika R. Das, and R. M. Pandey. "Risk factors of Parkinson's disease in Indian patients," Journal of the neurological sciences, 190(1–2), 2001, pp. 49–55.

[5] Monti, Giuseppina, De Paolis, Maria Valeria, and Tarricone, Luciano. "Wireless power transfer link for rechargeable deep brain stimulators," In Microwave Symposium (MMS), 2015 IEEE 15th Mediterranean, IEEE, 2015, pp. 1–4 doi: 10.23919/ACC.2017.7962938

[6] Cubo, Ruben, Alexander Medvedev, and Helena Andersson. "Deep brain stimulation therapies: A control-engineering perspective," In American Control Conference (ACC), 2017, IEEE, 32(5), 2017, pp. 104–109.

[7] Khan, Muhammad, and Hai Deng. "Design and Prototyping a Smart Deep Brain Stimulator: An Autonomous Neuro-Sensing and Stimulating Electrode System," in IEEE Intelligent Systems, vol. 32, no. 5, pp. 14-27, September/October 2017.doi: 10.1109/MIS.2017.3711648

[8] Andreu-Perez, Javier, Leff, Daniel R., Ip, Henry MD, and Yang, Guang-Zhong. “From wearable sensors to smart implants-–toward pervasive and personalized healthcare,” IEEE Transactions on Biomedical Engineering, 62(12), 2015, pp. 2750–2762.
[9] Albayrak, Muammer, and K. Turhan, “E-survey based approach for pervasive healthcare” 2017 Medical Technologies National Congress (TIPTEKNO), Trabzon, 2017, pp. 1-4. doi: 10.1109/TIPTEKNO.2017.8238077
[10] Chen, Bor-Rong, Patel, Shyamal, Buckley, Thomas, Rednic, Ramona, McClure, Douglas J., Shih, Ludy, Tarsy, Daniel, Welsh, Matt, and Bonato, Paolo. “A web-based system for home monitoring of patients with Parkinson’s disease using wearable sensors,” IEEE Transactions on Biomedical Engineering, 58(3) 2011, pp. 831–836.
[11] Chen, Yue, Hao, Hongwei, Chen, Hao, Tian, Ye, and Luming Li. “The study on a real-time remote monitoring system for Parkinson‘s disease patients with deep brain stimulators,” 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Chicago, IL, 2014, pp. 1358-1361.
[12] Li, Chao, Xiangpei Hu, and Lili Zhang. “The IoT-based heart disease monitoring system for pervasive healthcare service,” Procedia Computer Science, 112, 2017, pp. 2328–2334.
[13] Gope, Prosanta, and Hwang, Tzonelih. “BSN-Care: A secure IoT-based modern healthcare system using body sensor network,” IEEE Sensors Journal, 16(5) 2016, pp. 1368–1376.
[14] Baktir, Ahmet C., Tunca, Can, Ozgovde, Atay, Salur, Gülüstü, and Ersoy, Cem. “SDN-Based Multi-tier computing and communication architecture for pervasive healthcare,” IEEE Access, 6, 2018, pp. 56765–56781.
[15] Mahmoud, Mukhtar ME, Rodrigues, Joel JPC, Ahmed, Syed Hassan, Shah, Sayed Chhattan, Al-Muhtadi, Jalal F., Korotaev, Valery V., and Victor Hugo C. Albuquerque, De. “Enabling technologies on cloud of things for smart healthcare,” IEEE Access, 6, 2018, pp.31950–31967.
[16] Alemdar, Hande, and Cem Ersoy. “Wireless sensor networks for healthcare: A survey.” Computer networks, 54(15), 2010, pp. 2688–2710.
[17] Rahmani, Amir M., Gia, Tuan Nguyen, Negash, Behailu, Anzanpour, Arman, Azimi, Iman, Jiang, Mingzhe, and Liljeberg, Pasi. “Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach,” Future Generation Computer Systems, 78, 2018, pp. 641–658.
[18] A. Alelaiwi, M. M. Hassan and M. Z. A. Bhuiyan, “A Secure and Dependable Connected Smart Home System for Elderly,” 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, 2017, pp. 722-727.
[19] Yin, Hongxu, and Jha, Niraj K.. “A health decision support system for disease diagnosis based on wearable medical sensors and machine learning ensembles,” IEEE Transactions on Multi-Scale Computing Systems, 3(4), 2017, pp. 228–241.
[20] Butson, Christopher R., Cooper, Scott E., Henderson, Jaimie M., and McIntyre, Cameron C.. “Patient-specific analysis of the volume of tissue activated during deep brain stimulation,” Neuroimage, 34(2), 2007, pp. 661–670.
[21] Sarode, S. and Bakal, J.. “PriTLP: A Priority-based Transport Layer Protocol for low rate wireless sensor networks,” American Journal of Sensor Technology, 4(1), 2017, pp. 21–29. doi: 10.12691/ajst-4-1-3.
[22] Sharma, Sagar, Keke Chen, and Amit Sheth. “Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems,” IEEE Internet Computing, 22(2), 2018, pp. 42–51.
[23] Balasubramaniam, Sasitharan, Wirdatmadja, Stefanus A., Barros, Michael Taynnan, Koucheryavy, Yevgeni, Stachowiak, Michal, and Jornet, Josep Miquel. “Wireless

communications for optogenetics-based Brain stimulation: Present technology and future challenges," IEEE Communications Magazine 56(7), 2018, pp. 218–224.
[24] Sarode, Sambhaji, and Bakal, Jagdish. "Performance analysis of beacon enabled prioritized CSMA/CA for IEEE sensor networks," International Journal of Applied Engineering Research, 12(8), 2017, pp. 1622–1627.
[25] Sarode, S. and Bakal, J.. "A real time priority based scheduler for low rate wireless sensor networks," International Journal of Computer Networks & Communications,9(3), May 2017, pp. 87–103.
[26] Sarode, Sambhaji S, and Bakal, Jagdish W.. "A data transmission protocol for wireless sensor networks: A priority approach," Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 10(3), 2018, pp. 65–73.
[27] Sarode, Sambhaji, and Bakal, Jagdish. "PFPS: Priority-first packet scheduler for IEEE 802.15. 4 heterogeneous wireless sensor networks," International Journal of Communication Networks and Information Security, 9(2), 2017, pp. 253–263.
[28] Sarode, Sambhaji. "VSRS: Variable Service Rate Scheduler for low rate wireless sensor networks," Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(4), 2017, pp. 37–44.

Avinash S. Devare and G. Krishna Mohan

8 Enhancement path assured transfer protocol to transmit urgent data

Abstract: Sensor network is designed to provide monitoring services especially for natural disaster. These natural disasters may affect lives of human beings directly or indirectly. Congestion is a very important factor in wireless sensor network (WSN) and also it reduces quality of services. Different types of data are generated in WSN and sensor nodes also depend on meant factors. It is very important to control the congestion as it may cause loss of packets or even more utilization of energy by sensor nodes. Congestion can be reduced by increasing the number of resources, reducing the transfer from source node or prioritizing the data that has to be sent. The data is categorized into two types, urgent data and normal data. Urgent data or sensitive data should be given more priority than the normal data. The proposed system checks for urgent data and give priority to urgent data, and by this the sensitive data will reach destination in time. In many previous systems, normal data was discarded. In the proposed system, normal data will not be discarded but it will be sent by some other alternative path to the sink node. The result shows better performance.

Keywords: wireless sensor network, urgent data, enhancement path assured transfer protocol, normal data, sink node

8.1 Introduction

Wireless sensor networks (WSN) acquired more attention just because of its varied and attractive applications in numerous fields. WSNs are the wireless networks and having remotely distributed sensors to coordinately observe, monitor and store the environmental conditions or any required information. There are many applications related to WSNs and also it is an integral part of day-to-day life. Monitoring applications depend on WSNs. They are used to monitor pressure, sound, temperature and so on. The applications include target tracking [1], online anomaly detection [2], biometrics and health care [3], wireless body sensor networks in medical applications [4], object tracking [5] and many other useful applications. A WSN consists of huge quantity of sensor nodes and these preprocess the raw data by some easy computations and transmit the essential preprocessed data. A sensor is used to sense, computate and communicate, and it is equipped with a small battery. There are some characteristics of sensor like small size, lightweight and portability that makes WSN as best choice among various applications. The WSN is an advanced technology that helps the society to be more safe,

https://doi.org/10.1515/9783110628517-009

comfy and secure. WSN as a social infrastructure is capable to transfer critical data very quickly and is more reliable than some other data. WSNs of this type would generally transmit both urgent and normal data. This data should be handled differently as priority of data will be different. The system transmits important data with lower delay and higher reliability related security, environment, disaster or condition monitoring applications. So we can say that WSN is able to categorize critical and noncritical data and give priority to packets based on its importance and urgency depending on the request that comes from the application layer. The objective of this idea is to get awareness of quality-enabled networks for environmental observation and monitoring mainly for calamity avoidance and urgent reply situations.

The real-time communication is one of the challenging problems in WSN. Sensor nodes can transmit very limited, irreversible and power sources because of their ad hoc strategy of deployment and low cost. Thus, a standout among the many constraints is to decrease the energy consumption as less as possible of sensor network. The different WSN applications such as border surveillance must be able to operate for quite a long time without any wired power providers. Along these lines, specifically, the delay requirements of packets must be met at very less energy value in WSN.

WSNs can interact with their environment through different sensors, process the data in sensor node itself as it has simple computation capability, and communicate processed data with all their neighbors. Following components are included in the sensor node:

- Wireless modules are the main constituents of WSN. They have the communication abilities and the memory for programming the application code. A module contains a transceiver, microcontroller, power source, few sensors and programmable memory unit.
- A sensor board that is attached on the wireless module is embedded with many types of sensors. Sensor board contains a prototyping area.
- Programming boards provide many interfaces that connect wireless modules to an enterprise or any PC/laptop or industrial network. The programming boards are used either to program the wireless modules or gather data from wireless modules [6].

There are different types of sensor nodes based on application in which it is used. They have different storage memory size, speeds, transmission rate and operating frequency.

The data packets can be transferred from one node to another by using different transmitting paths that may utilize different times to reach. Many different and alternative paths will be available at different times. Hence, we need the device or protocols that will send data packets in comparatively less time. This path that uses minimum time is called the best path among all available paths. These protocols

are the routing protocols. The disadvantage of these routing protocols is that they ignore the power levels of the nodes in the available minimum time path. By this, nodes may end up sending noncritical or nonurgent data packets repeatedly using all the power of these nodes. Therefore, these nodes will run out of power and come out of WSN. Later data packets need to transmit from different available nodes that may use more time. By this, the critical data may not reach on time to its destination and incur huge loss. It is required to deal with these problems. Normal data and urgent data should be categorized and transmit by different paths. Urgent data only should be transmitted using best path. We proposed an algorithm that will categorize the urgent data from normal data by checking the priority. And then dedicate the best path to the urgent data transmission. Normal data will be transmitted using the alternative paths.

8.1.1 Characteristics in transport protocol design

Characteristics of transport layer protocol are as follows:

- Connection oriented: The Sender and receiver establish the connection before the data transmission begins. When the sender sends the data, it gets the positive/negative per packet response or selective ACK/NACK response from its recipient.
- Same order delivery: When the sender divides the packets into number of fragments by assigning the sequence number to each for transmission, then transport layer protocol transfers packets sequentially to the receiver in the same order as they were at the source node in order to reconstruct it again.
- Reliable data: If all the packets reach the base station (BS) successfully in the same order, then the BS send the selective acknowledgment to sender; otherwise, BS sends the negative acknowledgment to increase the reliability.
- Flow control: If the flow rate of sensor nodes is huge prominent than that of processing rate of receiver node, then congestion happens around the receiver node. To minimize the congestion, the flow rate of sender has to be controlled.
- Congestion detection and avoidance: Network congestion is detected by checking the buffer level and load on channel. At the node level, congestion can be avoided by setting the threshold value to buffer. When it increased more than the threshold of buffer, it sends backpressure message to sender to decrease flow rate in order to solve the congestion. Second issue is: Load on channel; if downstream node does not receive the packet within the predefined time, then it assumes that the congestion occurred in the network due to large delay. Solution to this problem is also the same, that is, to adjust the reporting rate of sender, so that the receiver can handle and process the packets.

- Loss recovery: It is a very sensitive issue for some applications such as military surveillance and many more. Some application may tolerate the loss of packets such as temperature monitoring. Many researchers have contributed their efforts to achieve the loss recovery with minimum energy expenditure. The cache and noncache techniques allow the transport layer protocol to achieve the loss recovery. Also, the retransmission mechanism is helpful to recover the lost packets by checking the packet numbers.

8.1.2 Issues in transport protocol design

Issues in transport protocol (TP) design are discussed below.

- **Congestion control:** Perform reliable delivery and congestion control of data. As large amount of data is transferred from the source node to master node, the congestion may occur around the master node. In spite of the fact that MAC convention can get back the lost packets because of bit error, there is no chance of taking care of packet loss because of buffer exceeding its limit. WSNs require a component for packet loss recovery, for example, acknowledgment and specific acknowledgment utilized in TCP. Moreover, in WSNs reliable delivery may have a different importance in comparison to the long-established networks; accurate transfer has to be ensured. Some sensor applications just need to get data appropriately from a few nodes around the region. It is not important to get data from all nodes in the respective region. This perception may cause a vital contribution in the plan of WSNTP. Likewise, it might progressively be powerful to utilize a level-by-level approach that can control overcrowding and diminish loss of packets, and along these lines it conserves energy. The level-by-level system may likewise bring down buffer necessity at intermediate nodes.
- **Quality of service (QoS):** WSNs sending data protocol ought to make the underlying connection establishment method simpler or go through connectionless protocol to improve the process speed, reduce the transmission delay and enhance throughput. Many applications of WSNs are reactive, so it implies that they monitor passively and trust that occasions will happen before transferring the data to the master node. These types of applications can have several packets to transfer as the outcome of an event.
- **Packet dropping rate:** In order to avoid energy waste, TP in WSNs ought to avoid the packet losses, however, much as could be expected. To avoid this, TP utilizes active congestion control (ACC) to bring down the connection use by some margin. ACC triggers congestion evasion before congestion really happens. For instance, of ACC, intermediate or sender nodes decrease its transfer rate as buffer size of neighboring nodes surpasses up to specific limit.

- **Throughput:** The TCP is supposed to ensure fairness for various nodes all together as every node can accomplish reasonable throughput.
- **Cross-layer optimization:** If feasible, TP ought to be structured with this optimization. For instance, if a routing method tells the TP about failure of route, then the protocol ought to have the capacity to derive that loss in data or packet is from path failure and not because of overcrowding in network. In such a scenario, the sender may continue with its current rate.

Issues of WSN are coverage ability, need of specialized hardware, QoS, security, congestion in network, network connectivity, prolong the network survival time, network expansibility support, algorithm complexity and others [7, 8].

This chapter deals with congestion control in network. The data transmitted can be urgent data or normal data. Urgent data has to be transmitted by giving it the most priority. There are many different protocols that are made only for urgent data transfer. The existing systems mainly focus on urgent data transfer and discard other information. The proposed enhanced path assured transfer (e-PAT) system transmits both urgent and normal data but more priority will be given to the urgent data, and the dedicated path will be assigned for transmission of urgent data [9].

8.1.3 Constraints of WSN

Despite the fact that a large number of protocols have been useful to wireless or wired network, these protocols cannot be utilized to sensor network as they hold unique characteristics that recognize it from different kinds of wireless or wired networks. The attributes are as follows:

- The sensor nodes equipped with short-range radio communication are prone to high latency, high failure rate and limited bandwidth.
- Sensor's range of transmission is short and mostly impacted by transmission power.
- The sensors are normally equipped with batteries and are supposed to operate unattended for longer time. Therefore, energy consumption is the essential requirement. A sensor acquires more energy on communication rather than computation.
- Sensors have restricted computational ability and have less memory. This restricts the different algorithms and results in processing of a sensor.
- The communication is affected by obstacle or noise.
- There are large numbers of sensor nodes, so they do not contain global ID.
- Due to movement or including more number or failure of sensor nodes changes the WSN topology.

8.1.4 Path-assured protocol for WSN to transfer urgent data

This protocol consists of the following steps:

i) For blocking normal data transfer, the urgent data node starts blocking request to all other nodes. Blocking of data transfer is a help to clear the path.
ii) Here critical or urgent data is transmitted directly to the sink node, and the sink node will give ACK for the received message, then actual data transmission takes place and when it is done the sink node sends the release message for releasing the node. Here data transmission takes place without collision because direct path is generated from source to sink and also by doing so it decreases delay because of retransmission, packet drop.
iii) This technique increases the network lifetime and reduces network overload by simulation

8.1.5 To develop a PDNC method with security for WSN

Selective packet discarding technique is also used in the proposed system. These techniques help congestion control by removing unwanted packets from communication. We also use Remote Control Protocol (RCP) protocol for congestion control in wireless networking. RCP-CA helps to control the traffic by

i) Quality control: Establish a target flow rate, such as Control Packet Rate (CPR).
ii) Acceleration control: it limits the acceleration.
iii) Feedback control: main aim of this is to decrease packet loss occurred during transfer.

Advantages of planned system controlling congestion from WSN using RCP protocol: It increases energy efficiency for discarding congestion control and the results are compared with the PAT and e-PAT based on the performance metrics like energy consumption, packet delivery ratio, delay and packet drop.

8.1.6 A proposed system to transfer urgent and normal data e-PAT method

Here a number of protocols are designed for data transmission (urgent). In the PAT protocol, the node first asks for urgent data transmission to destination. In that case, the sensor node also stops transfer of normal data so that it sends a blocking request. This will block the transmission of normal data and clear the path; hence, it transmits urgent data very fast and don't have to wait for data transmission also there is no any fear of collision and packet loss and also avoid congestion in

network and provide 100% reliability for urgent data so here normal packets are blocked and not sanded in network and which is not stored at node because of memory shortage. So this is a major issue resolved in the proposed system by using intelligence. The proposed system is compared with the Packet Discarding Node Clustering (PDNC), and PAT depends on its performance metrics like energy consumption, packet drop ratio, delay and packet delivery ratio. Hence, the proposed technique increases the data protection and decreases latency.

The chapter is organized as follows. A brief literature survey on existing systems is given in Section 8.2. System flow and working of system is explained packet discarding node clustering in Section 8.3. In Section 8.4, results are discussed. Section 8.5 concludes.

8.2 Literature survey

Alipio and Tiglao [9] proposed a cache-aware congestion control protocol. They designed a protocol with a mechanism, which is mainly based on management of cache rules that increase cache consumption. They conducted simulations, and derived method to evaluate the efficiency with occurrence of loss of packets in WSN.

Tao and Yu [10] proposed an enhanced congestion recognition and prevention system. This system is an energy-efficient control system for WSN. For recognition of congestion it measures congestion that uses weighted buffer difference and dual buffer thresholds. Queue scheduler is used to select next packet that has to be sent. Whenever congestion is caused the packets are selected based on channel loading and packets urgency.

In WSNs, the capacitor is used to store harvested energy. These capacitors discharge over time or discharge when there is data transmission. To transmit data only this harvested energy can be used and harvesting of energy requires more time. Hence, using this mode, transmission of urgent data to sink node is impossible [12]. The hybrid access point exuded energy to users and the received information is transmitted to sink node by using harvested energy by users [13]. By using backscatter communication system, the users receive sudden excitation energy radiated by the hybrid access point.

Sridevi et al. [14] projected a model based on various traffic in WSN of many different paths. This protocol assigns bandwidth that is directly proportional to number of applications running in sensor nodes at the same time. The dataflow will be forwarded to multiple paths towards destination node.

Wan et al. [16] proposed PSFQ. It is a trustworthy communication from master node to sensor nodes. Pump Slowly Fetch Quickly (PSFQ) is intended to be energy efficient and scalable, attempting to limit the quantity of signaling messages and depending on various local timers. It expects to share out data from the master node to other sensor hubs by pacing information at a generally moderate rate, yet

permitting hubs that encounter loss in data to bring any lost segments from prompt neighbors forcefully. It consists of three operations: pump, report and fetch. It issues Negative ACK in turn around way to recovering lost fragments. Master node can make sensor hubs to input information conveyance status to it through a basic level-by-level report operation.

Few disadvantages of PSFQ are as follows:

1) It cannot distinguish the single packet loss.
2) It utilizes statically and gradually pumps the outcome in huge wait.
3) Level-by-level recuperation with cache will increasing buffer. To lessen the impacts among these packets, the nodes utilize random delays before replying. At last, to check data delivery status information, the report activity/operation is started by the source.

Wan et al. [16] studied the CODA protocol, which is related to upstream congestion control. It explained energy-efficient congestion control plot with three plans, that is,

i) Open-loop level-by-level backpressure
ii) Congestion detection
iii) Source-to-destination multisource rule

Congestion Detection and Avoidance (CODA) endeavors to distinguish overcrowding by checking the present buffer use and remote channel load. The node identifying overcrowding will tell its next neighboring node about decreasing the transfer speed. The next neighboring hubs will generate to reduce yield speed as that of Additive Increase/Multiplicative Decrease (AIMD). At last, CODA manages multisource rate with the use of closed-loop end-to-end approach as pursued, and as a sensor rate overwhelms the hypothetical throughput, it will set “regulation” bit in even packets. In occurrence the occasion packet obtained by destination has a “regulation” bit. An ACK control note is send by the sink nodes to sensors for informing them to increase their data transfer speed. If overcrowding is reduced, the destination node will effectively mail ACK control note to sensor nodes and to illuminate them to expand their speed. To regulate sensors rate CODA utilizes the mode similar to AIMD in TCP.

It has some disadvantages:

1) Result in decreased reliability, particularly in situations with inadequate source and more data speed
2) Response/delay time required will be expanded under substantial overcrowding

Dipti Patil et al. [17] described the PCCPprotocol. It gives congestion control in upstream and fairness. PCCP figures a congestion degree with a solitary measure that is proportional to mean packet arrival time to the mean packet service time. PCCP utilizes implicit overcrowding warning by piggybacking blockage data in header of information parcels. In this manner, maintaining a strategic distance from extra control bundles of Priority-based congestion control protocol (PCCP) utilizes

a bounce by jump rate modification plot called need-based rate alteration, and the three utilizations needs identified with hub need file to arrange traffic are source traffic need, travel traffic need and worldwide need. In any case, in PCCP, the need is characterized from a hub perspective rather than the traffic stream perspective. Along these lines, the traffic streams from a hub can't be separated.

8.3 Proposed system

The e-PAT protocol is proposed. This protocol transmits both normal and urgent data. In this, the path is dedicated if urgent information is detected and transferred through dedicated path. At the same time, if normal data has to be transmitted then it will be transmitted through alternate path toward sink node. Obviously, priority will be given to urgent data but normal data will not be discarded. Figure 8.1 shows the system flow diagram of e-PAT. First, data will be checked whether it is urgent data. This is checked by the eflag bit in the end device table. If it is an urgent data, then first send a broadcast message to all neighboring nodes and allocate a dedicated path for transfer of that urgent data to the destination node and transfer the data. If it is not an urgent data then it will be the normal data and continue sending normal one. In between if normal data gets detected, then send this data through nodes that are not in the dedicated path. Once urgent data transmission gets over, transmit normal data to the next hop level and then to the sink node.

8.3.1 Proposed system flow diagram

In WSN, urgent data transfer is considered to be very important. The proposed system is e-PAT protocol. There are three steps when end nodes detect the urgent data.

1. It broadcast urgent data detection message to all other neighboring nodes.
2. Once urgent data detection message is received, these nodes stop transmitting normal data and give priority to urgent data and dedicate the specific path to urgent data.
3. The normal data will then be transmitted by using alternate path nodes that are not in the dedicated path for urgent data transmission. Hence, urgent data and normal data will be transmitted by different paths to the next hop toward sink node.
4. As soon as urgent data transmission completes, sink node will be free to accept normal data.

This increases performance of the system.

Some procedure is required to check whether the data is urgent or normal. The system will not know about the type of data it is receiving. It is required to tell the system which one is urgent data. For that, there is one end device table. In this

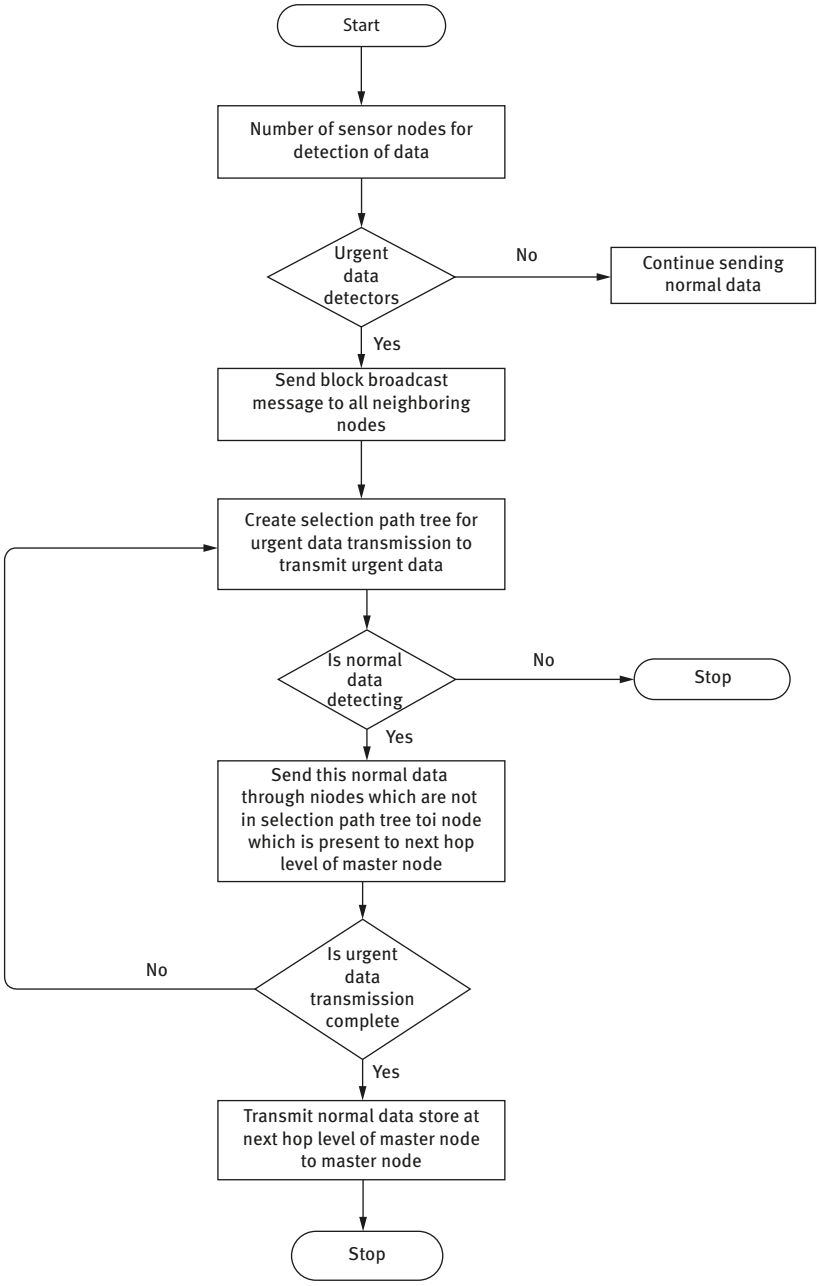


Figure 8.1: Proposed system flow diagram.

table, 1 bit is eflag bit, that is, emergency flag, and this bit gives the information about urgent data.

8.3.2 Enhanced path assured transfer algorithm

e-PAT algorithm is given below. Data or information from different sensor nodes is input for this algorithm. The output is based on the priority of data, that is, whether data to be transmitted is normal or urgent. At the sink node, all data will be received. Priority of urgent or sensitive data is more than that of normal data. Based on priority, data will be received by the destination node.

Algorithm: Enhanced Path Assured Transfer
Input: Data from Sensor network.
Output: Data received by sink node based on priority (urgent or normal data). The priority of urgent data is more than normal data.

{
1. If data is urgent data then
  Send block broadcast message to all neighboring nodes.
Else
  Continue sending normal data
2. Create selected path tree for urgent data transmission.
3. If normal data detected then
    Send this normal data through nodes which are not in selected path tree.
Else
  Stop
4. If urgent data transmission complete than
  Transmit normal data
Else go to step 2
}

8.3.3 Mathematical model enhanced path assured transfer algorithm

Let S be the system.
S = {Di,Do,F}
  Where
  I/P-Di={d1,d2,d3..dn}
    Where d1 is data from s1

d2 is data from s2
dn is data from sn
where {s1,s2,. . ...sn} are sensor nodes
O/P-Do={du,dn}
Where du is data (urgent) received by sink node
dn is data (normal) received by sink node
F={PDR,PLR,AD,T}
PDR=packet delivery rate=∑packet received/ time
PLR=packet loss rate=∑sent packet- received packet/ time
AD=Average delay =∑(packet received time-packet sent time)/n
T=Throughput=∑packet delivered/ packet received

8.4 Results and analysis

The accompanying measurements are considered during analysis of e-PAT protocol performance.

- Transmission delay: This delay is estimated as an interim between transmissions of data packet from its sensor nodes to the destination of data packet at the destination node:
  Average delay = ∑(packet received time – packet sent time)/n
- Packet delivery ratio: It is proportion of packets received at master hub to the number of packet transmitted. Packet delivery ratio is determined as that of individual sensor node and that of overall network.
- Throughput: Throughput = ∑packet delivered/packet received

Simulation parameter

An e-PAT is implemented in an NS2 simulator environment and a wide-ranging simulation experiment is conducted. In simulation experiments, different sensor hubs are consistently distributed in 500 m × 500 m two-dimensional area with a sink node at the lower point. We occupy a general broadcast-based and unicast-based routing protocol for network layer. In these routing protocols, it is thought that each node knows its distance from the sink node.

To evaluate e-PAT, PDNC and PAT performance, the parameters are measured in two scenarios:

1. Urgent data transfer
2. Normal data transfer

Main attributes used in checking of e-PAT, PDNC and PAT system are interval, node and packet size.

8.4.1 Interval

Figure 8.2(a) gives comparison of PDNC, PAT and proposed e-PAT system based on its interval and packet delivery ratio. Red line denotes less packet delivery ratio as distinguished by the black line. Red line is for PDNC protocol and black line indicates the PAT protocol. And blue line for e-PAT system in that packet dropped is very high when compared with others.

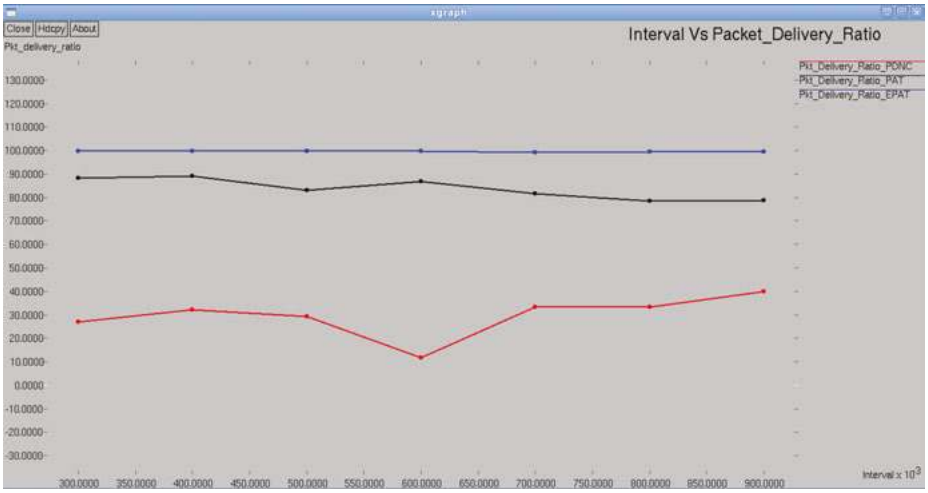


Figure 8.2: A comparative study of PDNC, PAT and e-PAT: (a) interval versus packet delivery ratio and.

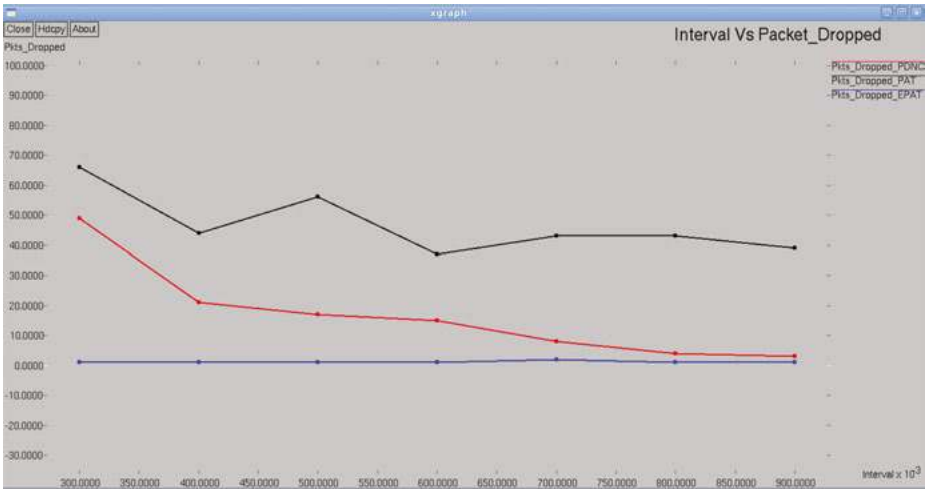


Figure 8.2: (b) interval versus packet dropped.

Figure 8.2(b) gives a comparison of PDNC, PAT and the proposed e-PAT system based on interval and packet drop ratio. Red line denotes less packet delivery ratio as distinguished by a black streak. Red line is for PDNC protocol and black line indicates the PAT protocol. And blue line for e-PAT system in that packet dropped is very less (Table 8.1).

Table 8.1: Comparison of PDNC, PAT and e-PAT (packet delivery ratio vs interval).

Interval	PDNC (%)	PAT (%)	e-PAT (%)
0.3	40	60	80
0.4	35	50	60
0.5	20	40	55
0.6	17	38	50
0.7	15	35	48
0.8	10	33	45

Figure 8.2(a) provides the interval versus packet delivery ratio in PDNC, PAT and proposed e-PAT system. The black line shows more packet delivery ratio when compared with red line. Black line indicates the PAT protocol and red line indicates the PDNC protocol. And blue line for e-PAT system in that packet dropped is very high when compared with others.

Figure 8.2(b) provides the interval versus packet drop ratio in PDNC, PAT and the proposed e-PAT system. The black line shows more packet delivery ratios when compared to red line. Black line indicates PAT protocol and red line indicates PDNC protocol. And blue line for e-PAT system in that packet dropped is very less.

8.4.2 Node

Figure 8.3(a) gives a comparison of PDNC, PAT and proposed e-PAT system based on node and packet delivery ratio (Table 8.2). PAT protocol is shown in black line and PDNC protocol in red line. Red line denotes less packet delivery ratio as distinguished by a black line. And blue line for e-PAT system in that packet dropped is very high as compared to the three whenever we consider a different node scenario: 10, 20, 50,100 nodes.

Figure 8.3(b) gives a comparison of PDNC, PAT and the proposed e-PAT system based on node and packet drop ratio. PAT protocol is shown in black line and PDNC protocol in red line. Red line denotes less packet drop ratio as compared to black line. And blue line for e-PAT system in that packet dropped is very less as compared to three whenever we consider different node scenario: 10, 20, 50,100 nodes.

Table 8.2: Comparison of PDNC, PAT and e-PAT (packet delivery ratio versus node).

Node	PDNC (%)	PAT (%)	e-PAT (%)
100	42	65	70
125	36	50	55
150	30	45	55
175	17	42	56
200	15	35	48

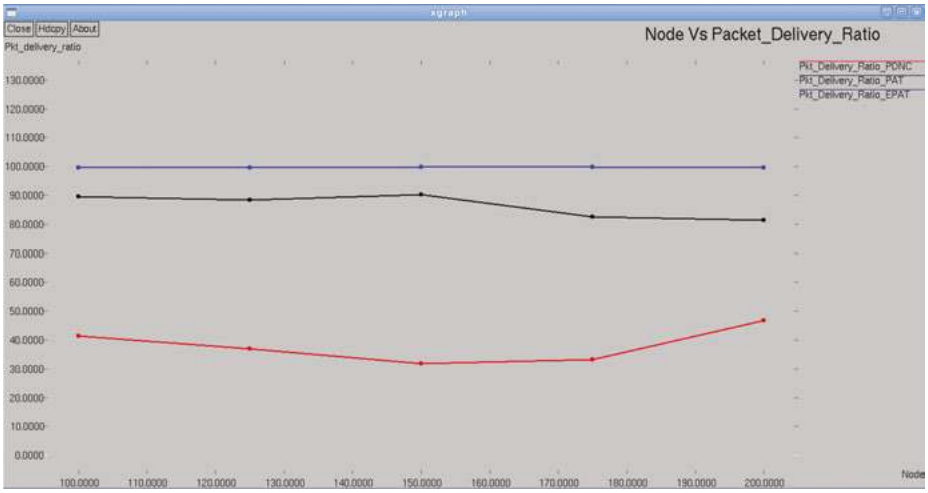


Figure 8.3: A comparative study of PDNC, PAT and e-PAT: (a) node versus packet delivery ratio and.

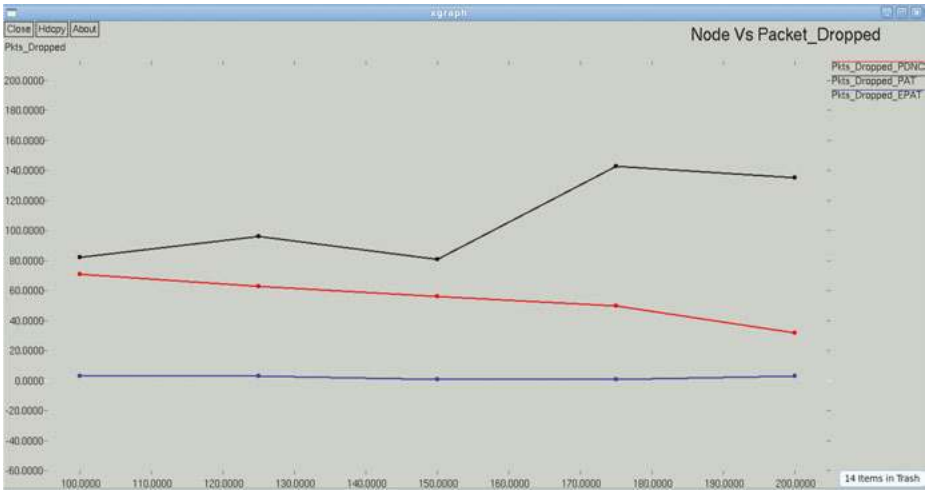


Figure 8.3: (b) node versus packet dropped.

8.4.3 Packet size

Figure 8.4(a) provides the packet size versus packet delivery ratio in PDNC, PAT and proposed e-PAT system. PAT protocol is shown in black line and PDNC protocol in red line. The red line denotes less packet delivery ratio as compared to black line. And blue line for e-PAT system in that packet dropped is very less as compared to the three whenever we consider different packet size (Table 8.3).

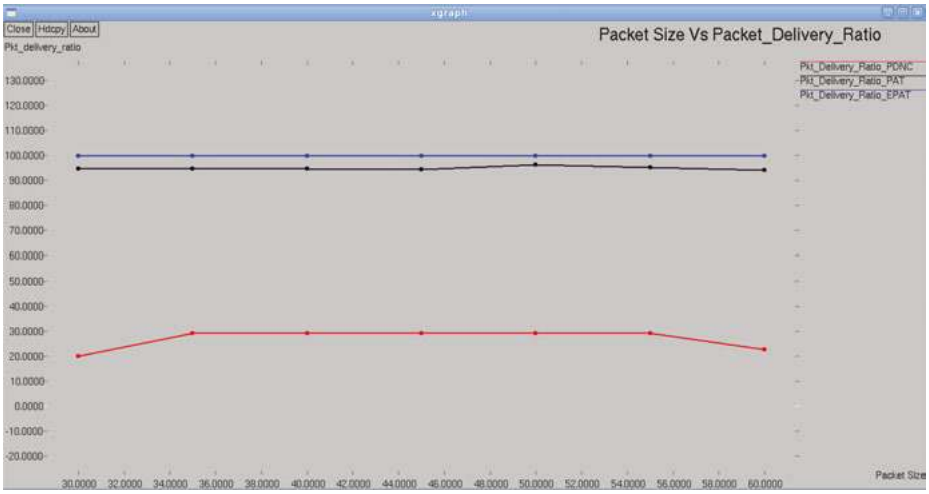


Figure 8.4: A comparative study of PDNC, PAT and e-PAT: (a) packet size versus packet delivery ratio and.

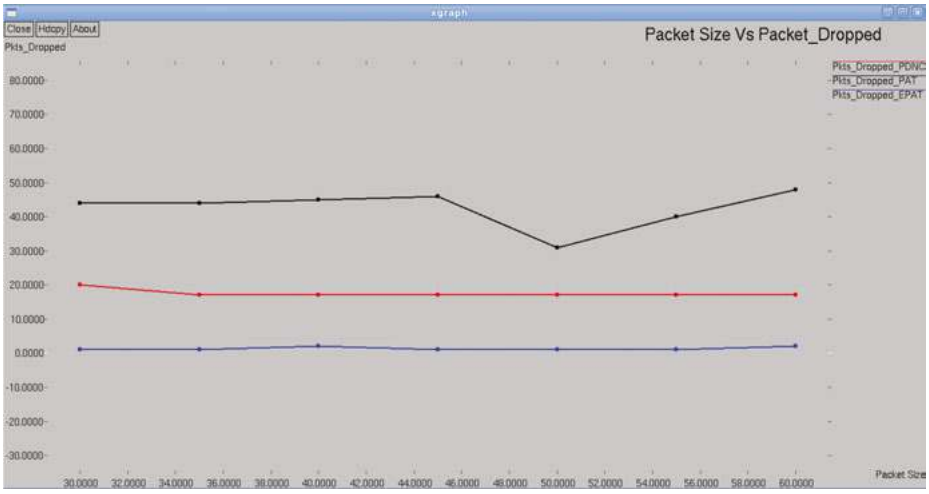


Figure 8.4: (b) packet size versus packet dropped.

Table 8.3: Comparison of PDNC, PAT and e-PAT (packet delivery ratio vs packet size).

Packet size	PDNC (%)	PAT (%)	e-PAT (%)
30	42	65	68
35	38	55	58
40	36	42	45
45	20	37	39
50	18	35	38
55	15	34	35

Figure 8.4(b) provides the node versus packet drop ratio in PDNC, PAT and proposed e-PAT system. PAT protocol is shown in black line and PDNC protocol in red line. The red line denotes less packet drop ratio as compared to black line. And blue line for e-PAT system in that packet dropped is very high as compared to the three whenever we consider different packet sizes.

8.5 Conclusion

Data is categorized into two types, urgent data and normal data, which will be sent to the sink node. Urgent data or sensitive data should be given more priority than the normal data. In this system, the system checks for urgent data and gives priority to urgent data; by this the sensitive data will reach destination in time. In many previous systems, normal data was discarded. In this proposed enhanced path assured system, normal data will not be discarded but it will be sent by some other alternative path to sink node, or normal data will be sent once the congestion is reduced. Both normal and urgent data will reach the sink node, and more priority is given to urgent data; hence, it reaches first. The result shows better performance and throughput.

References

[1] Song L., and Hatzinakos D. A cross-layer architecture of wireless sensor networks for target tracking, IEEE/ACM Transactions on Networking (TON), 2007 Feb 1;15(1), pp. 145–58.

[2] Xie M., Hu J., Han S., and Chen HH.. Scalable hypergrid k-NN-based online anomaly detection in wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems, Aug; 24 (8), 2013, pp. 1661–70.

[3] Chen SL., Lee HY., Chen CA., Huang HY., and Luo CH. Wireless body sensor network with adaptive low-power design for biometrics and healthcare applications. IEEE Systems Journal, Dec;3(4), 2009, pp, 398–409.

[4] Zhang X., Jiang H., Zhang L., Zhang C., Wang Z., and Chen X.. An energy-efficient ASIC for wireless body sensor networks in medical applications, IEEE transactions on biomedical circuits and systems,Feb;4(1), 2010, pp. 11–8.
[5] Brooks RR., Ramanathan P., and Sayeed AM.. Distributed target classification and tracking in sensor networks, Proceedings of the IEEE, Aug;91(8), 2003, pp. 1163–71.
[6] Akyildiz IF., and Vuran MC. Wireless sensor networks, Edition 1, John Wiley & Sons, 2010 Jun pp. 10.
[7] Lei Y., Zhang Y., and Zhao Y.. The research of coverage problems in wireless sensor network, In 2009 International Conference on Wireless Networks and Information Systems, Dec 28, 2009, pp. 31–34 IEEE..
[8] Sharma S, Bansal RK, and Bansal S. Issues and challenges in wireless sensor networks, In 2013 International Conference on Machine Intelligence and Research Advancement, 2013, Dec 21 pp. 58–62 IEEE.
[9] Alipio MI., Tiglao NM. RT-CaCC: A reliable transport with cache-aware congestion control protocol in wireless sensor networks, IEEE Transactions on Wireless Communications, Jul;17 (7), 2018, pp. 4607–19.
[10] Tao LQ., Yu FQ. ECODA: enhanced congestion detection and avoidance for multiple class of traffic in sensor networks, IEEE transactions on consumer electronics, Aug;56(3), 2010, pp. 1387–94.
[11] Kim SH., Kim DI. Hybrid backscatter communication for wireless-powered heterogeneous networks, IEEE Transactions on Wireless Communications. Oct;16(10), 2017, pp. 6557–70.
[12] Ju H., Zhang R. User cooperation in wireless powered communication networks, In 2014 IEEE Global Communications Conference, Dec 8 2014, pp. 1430–1435. IEEE.
[13] Boyer C., Roy S. – Invited paper – Backscatter communication and RFID: Coding, energy, and MIMO analysis, IEEE Transactions on Communications, Mar;62(3), 2014, pp. 770–85.
[14] Sridevi S., Usha M., Lithurin GP. Priority based congestion control for heterogeneous traffic in multipath wireless sensor networks, In 2012 International Conference on Computer Communication and Informatics, Jan 10 2012, pp. 1–5. IEEE.
[15] Wan CY., Campbell AT., Krishnamurthy L. Pump-slowly, fetch-quickly (PSFQ): a reliable transport protocol for sensor networks, IEEE Journal on selected areas in Communications, Apr;23(4), 2005, pp. 862–72.
[16] Wan CY., Eisenman SB., Campbell AT. CODA: congestion detection and avoidance in sensor networks, In Proceedings of the 1st international conference on Embedded networked sensor systems, 2003, Nov 5 pp. 266–279. ACM.
[17] Patil D., Dhage SN. Priority-based congestion control protocol (PCCP) for controlling upstream congestion in wireless sensor network, In 2012 International Conference on Communication, Information & Computing Technology (ICCICT), 2012 Oct 19 pp. 1–6.IEEE.