Query Rejection Techniques and Impact of Attacker's Position in Mobile Ad hoc Networks

MS Research Dissertation

By

Isma Munir

(434-FBAS/MSCS/S08)

Supervised By:

Prof. Dr Muhammad Sher

Co-Supervised By:

Mr. Zeeshan Shafi Khan

Department of Computer Science

Faculty of Basic and Applied Sciences,

International Islamic University, Islamabad

2010

A Dissertation submitted to the

Department of Computer Science

International Islamic University Islamabad

As a partial fulfillment of requirements for the award of

The degree of

MS in Computer Science

International Islamic University, Islamabad

Dated: --------------------

Final Approval

It is certified that we have examined the thesis titled "Query Rejection Techniques and Impact of Attacker's Position in Mobile Ad Hoc Networks" submitted by Isma Munir, Registration No: 434-FBAS/MSCS/S08, and found as per standard. In our judgment, this research project is sufficient to warrant it is acceptance by the International Islamic University, Islamabad for the award of MS Degree in Computer Science.

Committee

External Examiner

Prof. Dr. Muhammad Younas Javed
Associate Dean,
College of Electrical and Mechanical Engineering
NUST, Peshawar Road,
Rawalpindi

Internal Examiner

Mr. Qaisar Javaid
Assistant Professor
Department of Computer Science
International Islamic University,
Islamabad

8/4/11

Supervisor

Prof. Dr. Muhammad Sher
Chairman, Department of Computer Science
International Islamic University,
Islamabad

Co-Supervisor

Mr. Zeeshan Shafi Khan
Lecturer
Faculty of Computing
Riphah International University,
Islamabad

Dedication

My late Father: Thank you for supporting me unconditionally in all ways of my life especially in studies, and believing in me.

My Mother: Thank you for devotion and constant love in me. I will try my best to achieve all goals and to reach to your dreams.

My Siblings: Thank you for encouraging me, always be with me, and increasing my faith on that there is no mountain higher as long as Allah is on our side.

Declaration

We hereby declare that this work, neither as a whole nor as a part has been copied out from any source. It is further declared that we have conducted this research and have accomplished this thesis entirely on the basis of our personal efforts and under the sincere guidance of our supervisor Prof. Dr Muhammad Sher and our Co-Supervisor Mr. Zeeshan Shafi Khan. If any part of this project is proved to be copied out from any source or found to be reproduction of some other project, we shall stand by the consequences. No portion of the work presented in his dissertation has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Isma Munir

(434-FBAS/MSCS/S08)

Acknowledgement

First of all, I would like to praise Allah almighty Who is the most Merciful, knowledgeable and Worthy of all praises. He knowth what before, or after or behind us. Nor shall we compass aught of His knowledge except as He Willeth. All thanks are due purely to Allah, alone, not any of the objects that are being worshipped instead of Him, nor any of His creation. These thanks are due to Allah's innumerable favors and bounties, that only He knows the amount of. All thanks and praise are due to Allah for these favors from beginning to end.

Though only my name appears on the cover of this dissertation, a great many people have contributed to its production. I owe my gratitude to all those people who have made this dissertation possible and because of whom my research experience has been one that I will cherish forever.

My deepest gratitude is to my supervisor, Prof. Dr Muhammad Sher. I have been amazingly fortunate to have an advisor who gave me the freedom to explore on my own, and at the same time the guidance to recover when my steps faltered. He taught me how to question thoughts and express ideas. His patience and support helped me overcome many crisis situations and finish this dissertation. I hope that one day I would become as good an advisor to my students as Mr. Sher has been to me.

I am heartily thankful to my Co-Supervisor Mr. Zeeshan Shafi Khan, whose encouragement, supervision and support from the preliminary to the concluding level enabled me to develop an understanding of the subject. He has been always there to listen and give advice. I am deeply grateful to him for the long discussions that helped me sort out the technical details of my work. I am also thankful to him for encouraging the use of correct grammar and consistent notation in my writings and for carefully reading and commenting on countless revisions of this manuscript.

I would like to thank Dr. Neil Daswani, who let me experience this research. Without his co-operation and support, it will be difficult for me to achieve my goal.

I am also grateful to the following former or current staff at IIUI, for their various forms of support during my Studies and specially during this research.

Most importantly, none of this would have been possible without the love and patience of my family. My immediate family to whom this dissertation is dedicated to, has been a constant source of love, concern, support and strength all these years. I would like to express my heart-felt gratitude to my family. My extended family has aided and encouraged me throughout this endeavor. I also extend my thanks to my Grandmother for all her silent prayers. I also love to thanks my cute little nephew Hunain for all the innocent prayers, which is an encouragement in achieving success.

Many friends have helped me stay sane through these difficult years. Their support and care helped me overcome setbacks and stay focused on my graduate study. I greatly value their friendship and I deeply appreciate their belief in me. Specially, I would like to thank my friend, Taiba Toqeer. She was always there cheering me up and stood by me through the good times and bad.

Finally I am concluding here that, I would never have been able to finish my dissertation without the guidance of my committee members, help from friends, and support from my family.

While I am grateful to Prof. Dr Muhammad Sher and Mr. Zeeshan Shafi Khan for their help and assistance, I must clarify that the blame for errors in the empirical analysis (if any) lies with me alone.

Isma Munir

Project in Brief

Project Title:	Query Rejection Techniques and Impact of Attacker's Position in Mobile Ad hoc Networks
Undertaken By:	Isma Munir (434-FBAS/MSCS/S08)
Supervised By:	Prof. Dr Muhammad Sher
Co-Supervised By:	Mr. Zeeshan Shafi Khan
Start Date:	January 2009
Completion Date:	April 2010
Tools and technologies:	Network Simulator 2
Documentation Tools:	MS Word, EDraw, MS Excel, MS Visio
Operating System:	MS Windows XP professional
System used:	Pentium 4, 1.73 GHz

Acronyms

1xEVDO	EVolution Data Optimized
3G	Third Generation
3GPP	Third Generation Partnership Project
ACK	ACKnowledgement
AHCP	Ad-hoc Configuration Protocol
AODV	Ad-hoc On-demand Distance Vector
AODVU-UU	Ad-hoc On-demand Distance Vector Routing-Uppsala University
AWDS	Ad-hoc Wireless Distribution Service
BATMAN	Better Approach to Mobile Ad-hoc Networking
CDMA 2000	Code Division Multiple Access
CN	Core Network
CPU	Central Processing Unit
CRP	Cache Replacement Policy
DARPA	Defense Advanced Research Projects Agency
DoS	Denial of Service
DDoS	Distributed Denial of Service
DECT	Digital Enhanced Cordless Telecommunication
DHT	Distributed Hash Table
DNP	Dynamic Network Partitioning
DNS	Domain Name Service
DO	Drop Oldest
DS	Drop Strategy
DY	Drop Youngest
EDGE	Enhanced Data rates for GSM Evolutions

FCFS	First Come First Serve
FTTH	Fiber to the Home
GERAN	GSM Edge Radio Access Network
GPRS	General Packet Radio Service
GRAN	GSM Radio Access Network
GSA	Global Mobile Suppliers Association
GSM	Global System for Mobile Communications
GSM	GPRS Session Management
GUESS	Gnutella UDP Extension for Scalable Searches
HC	Hop Count
I/O	Input / Output
IAS	Incoming Allocation Strategy
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IDRM	Inter Domain Routing for MANET
IDSA	ID Smearing Algorithm
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
iMANET	Internet Based Mobile Ad Hoc Network
IMS	Internet Protocol Multimedia Subsystem
InVANET	Intelligent Vehicular Ad Hoc Network
IP	Internet Protocol
IPTV	Internet Protocol Tele Vision
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
ITU	International Telecommunication Union

LAN	Local Area Network
LANMAN	Local And Metropolitan Area Network
MAC	Media Access Control
MAC	Message Authentication Code
MANET	Mobile Ad Hoc Network
Mbps	Mega bits per second
MMS	Multimedia Messaging Service
MND	Malicious Node Detector
MNO	Mobile Network Operator
MPR	Malicious Ping Rate
MRU	Most Recently Used
MS	Mobile Station
MVNO	Mobile Virtual Network Operator
NIST	National Institute for Standards and Technology
NS-2	Network Simulator-2
NT	New Technology
NT	Network Termination
OLSR	Optimized Link State Routing
OS	Operating System
P2P	Peer-to-Peer
POTS	Plain Old Telephone System
PRNET	Packet Radio Network
QoS	Quality of Service
RAID	Redundant Array of Independent Disks

RAN	Radio Access Network
RPC	Remote Procedure Call
RW	Remote Work
SMS	Short Messaging Service
SPBM	Scalable Positioned Based Multicast
SP	Service Provider
TCP	Transfer Control Protocol
TTL	Time-to-Live
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network
VANET	Vehicular Ad Hoc Network
VOIP	Voice over Internet Protocol
W-CDMA	Wideband-Code Division Multiple Access
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
ZRP	Zone Routing Protocol

Abstract

Mobile Ad Hoc Networks (MANETs) are self organized infrastructure less, temporary networks. Since these networks are self organized, very cheaper and easy to establish, so their use in daily life is increasing with the passage of time. In Ad Hoc networks, information is mostly shared by using broadcast (flooding) techniques. The use of flooding is preferred because it is more reliable, faster and resilient against quick joining and leaving. Since every node of MANETs has some limited processing capabilities, so it is not possible to serve all the incoming queries. Few queries are served and few are dropped. Now, it is an open and critical issue that which queries should be entertained and which queries should be dropped in order to obtain efficient results. Moreover, position of the attacker also affects the performance of the network. We in this thesis will design and test different query dropped strategy in order to find the efficient solution and to enhance the network performance. Moreover, we will also analyze different positional attack models and their effect on network performance. The result will be validated by using NS-2.

Table of Contents

List of Figures

1. Introduction

1. Introduction

At the present era, wireless systems are evolving rapidly by providing standardized Cellular systems and Radio technology at a large scale. It has become possible due to the fact that the wireless high speed Local Area Networks (LANs) are enabling to provide high quality multimedia services (voice, video, and data) to the users throughout the world.

Denial of Service (DoS) attacks can bring many damaging effects along with them. When a network is under an attack, various techniques can be used to provide the degrade Quality of Service (QoS) to the clients in such a possible situation.

Wireless Ad Hoc networks are similar to Gnutella Peer to Peer (P2P) networks in some cases. Such as the radio broadcasts in wireless ad hoc systems are akin to the flooding mechanisms in Gnutella networks. The traffic management policies for attack containment techniques used in Peer-to-Peer (P2P) systems can also be applicable as a solution to this problem in wireless systems.

In an Ad Hoc network, the nodes must have enough battery power that can hold the incoming queries. The nodes utilize all of their battery powers if the number of incoming queries exceeded the capacity. In such a situation, the queries would be handled explicitly by determining how the traffic management schemes can be modified in that scenario. Usually polling is introduced in such a case to contain DoS attacks in wireless Ad Hoc networks.

In an application layer Denial of Service (DoS) attack, the number of packets in which the queries are sent by an attacker will consume all of the network's bandwidth, CPU cycles and disk I/Os so that the legitimate user can not be served using these resources. A DoS attack may cause the super nodes to be shut down, or may affect the entire network.The aim of flood attack is to make the network's services poor, or may shutdown the server's site completely. A flood attack is launched in order to cause traffic to exhaust the network, which can use up the remote resources at its best. In a flood attack, the traffic is generated continuously, to consume the CPU cycles and memory of the pointed server, or to consume the bandwidth and packet buffers of the entire network.

Basically, the term 'Quality of Service (QoS)' belongs to the Traffic Engineering category. In Computer Networking and Telecommunication Networks, QoS is used to consider the control mechanisms for resource reservation. Here, the already available service quality, achieved by the network is not the point of consideration.

A network can attain high level performance through best QoS. QoS guarantees the users that the applications and data flows requested by them, would be provided of best quality. In a situation when network capacity becomes a scarce resource, it will become necessary that the QoS must be guaranteed. It is specially required in real-time applications which use streaming multimedia (IP-TV, voice over IP, online games, etc.), and also in cellular data communication. The guarantees by QoS are required because these applications demanded a fixed bit rate, and they are delay sensitive. So, in case when the capacity is not plentiful, the user must know before starting a session.

The need for Quality of Service (QoS) has become a challenging issue for the current systems. As the technology is evolving day by day and introducing new techniques with enhanced and improved methods, it has become more difficult for the existing systems to maintain the high quality of the available services offered by the network.

In Figure 1.1, Quality of Service (QoS) of data or files can be affected by the Denial of Service (DoS) attacks which causes the nodes to offer degrade services and performance. Due to DoS attacks the malicious nodes in the network makes a file to be available and allow it to be downloaded upon receiving its request made by the user, but it serves the slow download speed which makes the client to cancel its request as the effected downloading procedure consuming a lot of time.

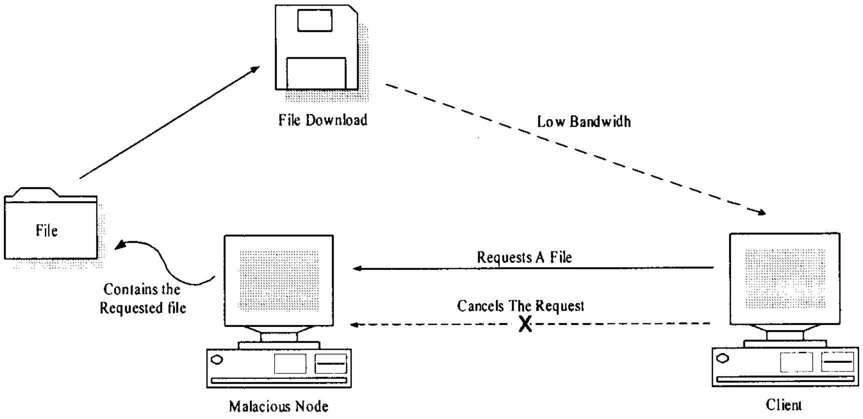

Figure 1.1: Effected Quality of Service (QoS) due to Attack.

Also the malicious node could be able to send the wrong file to the client and could claim that it has sent the right requested file to the client. For this problem, the client uses various techniques and methods to assure that the file it is receiving from the server is correct, and is downloaded at a better satisfactory speed.

1.1 Quality of Service (QoS) in Various Networks

Wireless networking is very popular in both fixed and mobile networks in which high quality multimedia services (voice, video, and data) are transferred with a high speed bandwidth. A fixed network wireless LAN is used to serve the residential and business atmospheres with up to 54 Mbps and much better high QoS. The QoS has become an important necessity for the most popular and common types of networks available today, which includes the following:

1.1.1 Peer-to-Peer (P2P) Network

Peer-to-Peer (P2P) networks consist of a number of peers (nodes) which can act both as a client and a server at the same time. The peers in the network work in co-operation with each other to perform various tasks, such as searching a document requested by a client. Various protocols are implemented in the network for this purpose. Peers in the network share the disk storage space and bandwidth amongst them. These peers work in a distributed environment, and they transfer huge amounts of data.

These networks are scalable; any peer could join or leave the network at any time. The peers are unreliable, autonomous, and highly dynamic in nature, for which different effective search techniques must be implemented and rigid search techniques must be avoided.

The role of a server is performed by the large number of peers in the network. So if one peer is failed to satisfy the client's queries, the other peers would be able to do so. The malicious peers can deny providing services and taking the favor of good peers to provide services on its behalf.

P2P networks are vulnerable to application layer attacks. In the application layer DoS attack, the service requested by the clients can be denied by the server. Due to the fact that the server's functionality is distributed among various peers, the effect of an attack can be minimized and the clients are allowed to continue their activities.

Different types of P2P systems have become popular for evolving applications. P2P has been classified into three types of architectures:

1 Unstructured.

2 Structured.

3 Non-forwarding.

1.1.2 Access Network

An Access Network is a communication network that allows the connection among subscribers and their service providers. Access network is constructed in co-operation with the Core network (CN), e.g., Network Switching Subsystem in GSM. The access network basic types are:

1 Feeder plant or Distribution network.

2 Drop plant or Edge network.

Fixed Line Access Network

The existence of fixed line telecommunication is not possible without having an access network. It is also known as Telephone or Outside Plant which provides the services physically to the consumer by connecting them to the local telephone exchange through cables, wires (copper or aluminum), and equipment. Access networks are also intended to use optical fibre technology and offer valuable services b means of Fibre to the Home (FTTH).

It is the most valuable and former type of telecommunications and is still improving day by day through the aid of new services and gaining a number of customers. Due to these reasons, it has become a complex task to maintain this complicated network.

Providing access has become a major and profitable aim of the operators today as they are facing revenue losses in Plain Old Telephone System (POTS) due to competitors and increasing usage of mobile phones and Voice over IP (VOIP) Services. For this purpose, the operators are intended to introduce xDSL based broadband and Internet Protocol Television (IPTV).

Radio Access Network (RAN)

Telecommunications uses Radio Access Network (RAN) which employs radio access technology. Logically it exists between Mobile Phone (Mobile Station (MS), User Equipment (UE), Terminal Equipment, etc.) and Core Network (CN). The UMTS and GSM are the currently used technologies of RAN. Dual-mode mobile phones are able to be connected to multiple RANs at the same time, e.g., a mobile phone supports both radio access technologies, GSM and UMTS. Thus it makes possible the transferring of an ongoing call among various RANs transparently, without causing any interference in the quality of service.

In an access network, the primarily focus is on radio spectrum management by the mobile operators. Types of RAN and standards for radio interfaces defined by IMT-2000 includes GRAN, GSM, GERAN, UTRAN, CDMA 2000, TD-CDMA/TD-SCDMA, DECT, 1xEVDO, WiMAX, UMTS, UWC, Wi-Fi, etc. UMTS also known as W-CDMA. It is based on layered services. UWC is commonly implemented with EDGE.

IEEE 802.11 networks are commonly known as Wi-Fi or WLAN networks. These networks are short range and developed for data with high bandwidth. It also provides low-level facilities to ad-hoc network in case when there is no access point is available. The nodes then restricted to send and receive data in their network only and cannot route across the network.

1.1.3 Mobile Network

International Telecommunication Union (ITU) has defined the requirements for Mobile Networking of Third Generation (3G) with IMT-2000 standard. 3rd Generation Partnership Project (3GPP) then defined standards and technologies for it and makes a system known as Universal Mobile Telecommunications System (UMTS). Using these standards, the operators are now capable of offering a variety of advanced technologies and services enhanced through spectral efficiency to the users over wireless environment.

Mobile network or Cellular Telephone Network consists of mobile phones provides voice telephony, video calls, broadband data, and HSPA data transmission having speed up to 14.4 Mbps on the downlink and 5.8 Mbps on the uplink. It is a wide range network that has also deployed video telephony and speedy access to Internet. Today, the mobile communication contains the excessive use of multimedia applications, e.g., Multimedia Messaging Service (MMS), streaming, etc.

A Mobile Network Operator (MNO) is a company that supports an independent mobile network by providing the frequency allocation(s) and the necessary infrastructure to the end user. It has its own mobile license and maintains the customer relationship directly. It also handles network routing. It can create and share data traffic, voice minutes, SMS and MMS. It handles customer services, handset management, invoicing, etc. It deals with foreign MNOs for roaming.

A Mobile Virtual Network Operator (MVNO) is a company that only provides the mobile phone service without having frequency allocation and the necessary infrastructure required to run a mobile phone service. A Service Provider (SP) handles customer relationship, customer billing consumption data, handset management, and marketing and sales.

According to the Global Mobile Suppliers Association (GSA) there exist 190 3G networks that were operating in 40 countries, and 154 HSDPA networks in 71 countries. The W-CDMA technology is developed with 100 terminal designs to provide aid in operating 3G mobile networks by the telecommunication companies of Asia, Europe, Canada, and USA.

Security is assured in 3G networks by enabling the UE to authenticate the network, so the attackers can be kept away from the network. When certain application frameworks like IMS are accessed, end-to-end security is also provided to the users.

1.1.4 Ad-Hoc Network

A wireless network becomes an ad hoc network when the nodes send data dynamically to the other nodes. It is decentralized wireless network. DARPA has sponsored the former ad hoc networks known as Packet Radio Networks (PRNETs). Ad-Hoc Networks are classified according to their applications:

1 Mobile Ad Hoc Networks (MANETs).

2 Wireless Mesh Networks.

3 Wireless Sensor Networks.

Researchers develop test beds to understand ad-hoc networking theories and evaluate real-time performance practically through simulations. Advanced tools are used to construct overlay network topologies and data traffic situations to measure the efficiency of routing protocols in the network. Simulations allow researchers to test scenarios without having a real physical network, e.g., effects of wireless traffic, a sudden Denial of Service (DoS) attack on a network service, test new networking protocols, replay mobility, etc. the researchers then publish and present the results of evaluations in International Conferences.

1.2 Mobile Ad hoc Network (MANET)

A Mobile Ad-Hoc Network (MANET) is a type and subset of wireless Ad Hoc networks that is composed of a number of wireless nodes or mobile devices and routers, which are connected by wireless links to form a dynamic and self-configuring or self-organizing network without having the support of any existing network. It does not have any physical backbone and base stations are not needed for the communication among nodes.

1.2.1 MANET Traits

The mobile nodes make the MANET an autonomous system as they move and organize themselves. These nodes function as an end system. The links to other devices are continually changed as the devices have freedom to move in any direction. Thus, the issue arises for each node to maintain the information continuously needed for routing the network traffic. The wireless communication links disappeared when the various nodes come into and go out from node's communication environment.

Figure 1.2: Mobile Ad-Hoc Network (MANET).

MANETs support highly dynamic topology, fragile and low-capacity links, and no dedicated infrastructure components. Mobile devices cause the network topology to change rapidly and unexpectedly over time as there is no physical structure and centralized access control system exists.

MANET usually implements a routable network on the top of a Link Layer ad hoc network. Routers in MANET forward the queries that are irrelevant to its work in order to reduce the network traffic. A large number of mobile users interact autonomously by using bandwidth that is less constrained over the wireless links.

MANET is also referred to as short live network as it operates without the aid of fixed supporting infrastructure. Deploying a MANET is a quick and easy task. It is also said that Bluetooth (an advanced technology) has introduced the concept of MANET. It supports an immediate person-to-person, person-to-machine, and machine-to-person communications.

MANET is also known as Multihop mobile radio network as it provides a reliable quick implementation of Multihop wireless infrastructure to support rapidly growing applications. The network allows a few number of wireless channels through which the nodes communicate in a multi-hop fashion.

The users can communicate easily with others while freely roaming from one place to another. When a pair of users is communicating, their communication path consists of multiple links and heterogeneous radio. Thus, different links can form a part of a single network.

MANET provides the connectivity anywhere and anytime to the users. In a situation when there is no network service available, a group of people can form an ad-hoc network by connecting their machines (laptops). This is usually done in business meetings, where these networks are possible to be used.

1.2.2 Forms of MANET

MANETs can exist in the following forms:

1 As a standalone.

2 Or can be extended by connecting to the Internet.

1.2.3 Types of MANET

MANETs could exist in various forms. The following common three types of MANETs are discussed below:

1 Vehicular Ad Hoc Networks (VANETs) allows the vehicles to interact and communicate with other vehicles and roadside equipment.

2 Intelligent Vehicular Ad Hoc Networks (InVANETs) made the vehicles intelligent to find out solutions in case of vehicle-to-vehicle collisions, accidents, drunken driving etc.

3 Internet Based Mobile Ad-Hoc Networks (iMANET) consists of fixed nodes and mobile nodes (ad hoc network). Fixed nodes act as gateways and their purpose is to provide Internet facility to the users. Routing algorithms cannot be used directly in these networks.

1.2.4 Significance of MANET

MANETs are different from other networks in many ways, as it is wireless in nature. Some significant features that make Ad Hoc networks are as follows:

1 Links are formed by the networks instead the network is formed by the links.

2 Interfaces have half-broadcasting method.

3 Network structure is flat and decentralized, where all activities are carried out by the nodes themselves, such as discovering the topology and delivering messages. For this reason, routing functionality must be deployed into nodes.

4 Support micro-mobility.

1.2.5 MANET Hardware

MANET is also known as “Mobile Mesh Network” because it consists of the following:

1 Mesh Nodes uses Optimized Link State Routing (OLSR) protocol. It uses dynamic routing to automatically connect the nodes with each other. Also it is cost effective.

2 Mesh Cubes is a dedicated platform for WLAN mesh routing. It provides powerful security and protection, and flexible for modifications and applications.

1.2.6 MANET Software

MANETs use a variety of the following software types:

1 Ad-talk makes the Wi-Fi machines to setup their wireless interfaces automatically. The machines calculate the IP addresses by using their MAC addresses and then able to join an ad-hoc cell called "live folio". The nodes then discover their neighbor's nodes to exchange text messages. Thus, the manual network configuration is not required.

2 Ad-hoc On-demand Distance Vector Routing from Uppsala University (AODVU-UU) is under investigation by IETF, where mobile and routers act as end-users.

3 Better Approach to Mobile Ad-Hoc Networking (B.A.T.M.A.N.) is used for multi-hop networks.

4 NRL OLSR is the NRL's implementation of the OLSR protocol. It supports IPv4 and IPv6.

5 ZRPd which is a full implementation of the Zone Routing Protocol (ZRP) used for Linux.

6 UniK OLSR Daemon is an implementation of the Optimized Link State Routing protocol.

7 Qolyester is a C++ implementation of the OLSR protocol.

8 Ad-hoc Wireless Distribution Service (AWDS) is a layer 2 routing protocol.

9 Ahcpd is an implementation of the Ad-Hoc Configuration Protocol (AHCP).

10 Babel is a distance-vector routing protocol used for IPv6.

11 Hipercom Optimized Link State Routing is investigating by IETF.

12 NIST Ad-Hoc on Demand Distance Vector Driver is for Linux.

13 XIAN is a cross-layer Interface for experimenting designs.

14 MIPL Mobile IPv6 for Linux is used for Mobility support in IPv6.

1.2.7 Applications of MANET

MANET support diverse applications executing on both small static networks and large dynamic networks. Application's performance is evaluated through simulations. MANET applications can be employed in P2P networks as both are distributed networks.

MANETs can be deployed to provide efficient and dynamic communication for:

1 Emergency or rescue operations.
2 Search-and-rescue.
3 Disaster relief effort or Disaster Recovery.
4 Military operations or Military networks.
5 Home networking.
6 Personal area networking.

1.2.8 Issues in MANETS

As MANET is a wireless network, so it has its own distinguishing qualities, which are different from the wired networks. Specifications while developing a MANET must be considered. Following issues must necessarily be considered while developing a MANET:

Design Issues

While designing MANET architecture, the issues such as variable wireless link quality, propagation path loss, fading, multi-user interference, power expended, node mobility, and topological changes must be given the highest priority.

Efficient distributed algorithms (e.g., token circulation algorithm) are required to determine network organization, link scheduling, and routing that can support any MANET application. The efficiency of these algorithms will increase the network's performance.

Designing MANET for military, issues that must be focused includes preservation of security, latency, reliability, intentional jamming, and recovery from failure.

Security Issues

Most of the applications do not provide secure communication as security is the critical and major issue. Security must be implemented for availability, authenticity, integrity, confidentiality, and non-repudiation.

QoS Issues

The co-operation and intercommunication of routing protocols, resource reservation, and medium access control protocol is required to assure QoS in MANETs. Issues that must be focused for employing QoS includes rapidly changing connectivity, network partitions, higher error rates, collision interference, limited transmission power of wireless devices, bandwidth, battery limitations, and power constraints.

1.3 Security Attacks

The data assets and resources are the major subjects of the attackers. If the necessary and appropriate security measures are not implemented in the network, then the attacker can launch attacks easily against the vulnerable network, as the attackers knows the proper tact how to bring damage in the networks.

High consideration must be given to network security issues to determine the correct security measures and policies before an attack. Weak security can lead an attacker to crash the system or the whole network or grab the services offered by the network.

1.3.1 Passive Attacks

An attacker only monitors the data and information in passive attacks. The goal of a hacker is to obtain the information that is being transmitted.

1.3.2 Active Attacks

The data or networks can be damaged by making changes in data and information by an attacker. The hacker sub modifies the data stream or may create the faulty data.

1.4 Types of Network or Hacker Attacks

Several of types of attacks can be launched by an attacker to cause destruction in the network. These are called hacker attacks because these attacks cannot be automatically generated by computer destructing programs like virus, worm, trojan horse, logic bomb, etc. The hacker or an attacker intentionally launches these attacks by using the gaps in security unfairly, to paralyze the network. The most common types of attacks are as follows:

1.4.1 Eavesdropping

An "eavesdropper" or an attacker can take advantage of "listen in" or "read" the data, during a "cleartext" or unsecured communication among networks. When an attacker achieves access secretly in such a way, it is also known as "sniffing" or "snooping".

In order to implement security to avoid eavesdropping, cryptography based encryption techniques are required so that the attacker would not be able to monitor the network.

1.4.2 Data Modification

The data packet is modified by an attacker after reading it, without having any references of sender and receiver.

1.4.3 Password-Based Attacks

It is also known as "password cracking". The legitimate user can use the network resources by having an authenticated user name and password account. The attacker uses an account of any legitimate user or network administrator, and accesses all the privileges of the valid user. An attacker then could be able to modify, reroute, or delete the data, and may change the server or network configurations.

1.4.4 Compromised-Key Attack

In compromised-key attack, a code or digit number is used as a key, secretly known by the user, in order to encrypt and determine the secure data. It is extremely difficult for an attacker to get the secret key code of the legitimate user of the network, but even though, an attacker can get the key code. When the key becomes known to an attacker, it is known as "Compromised Key".

An attacker accesses the data paths transparently by using compromised key. So that he can easily decrypt and alter the secure secret data. While attacking a secure communication through a compromised key, an attacker may tries to get more keys in order to extend his access to more secured communications.

1.4.5 Sniffer Attack

Sniffer is a software application or a hardware device that is used to capture, monitor, and read the data exchanged among the networks. Sniffer also reads the data packets transferred over the networks. The data packets needs necessarily to be encrypted, otherwise the data in the packets can be viewed by an attacker through sniffer.

An attacker can break, open, and read the unencrypted packets, even if they are encapsulated. Else, if the packets are encrypted, the attacker cannot be able to attack, as he cannot get the key. In a sniffer attack, an attacker by accessing the network can be able to read the communications, obtain valuable data and information, which is used for crashing the network.

1.4.6 Server Spoofing

The server machine can request for LANMAN authentication from the client machines by using C2MYAZZ utility with Windows 95 on it. When the client tries to login, an attacker pretends as a server by running this utility. If the client pranks while sending LANMAN authentication, the packets sent to the server can be read by an attacker, containing user's username and password.

1.4.7 Identity Spoofing (IP Address Spoofing)

IP address of a machine is used to represent its identity in the network. In identity spoofing, for achieving access to the network, the fake computer's IP address is supposed by an attacker. An attacker creates IP packets by using various programs and sends them to victim servers, which seems to the receiver that the packets are incoming from valid sender IP addresses. After gaining success, the attacker can be easily modify, reroute, or delete the data. This attack can impose the operating systems to lock up or crash.

1.4.8 Man-in-the-Middle Attack

In Man-in-the-Middle attack, an attacker claims as an authorized user of the network or computer. An attacker starts communication with other nodes, by reading and replying the transferring messages. Thus, the user at the other node cannot distinguish that he is communicating with the authorized or unauthorized user. An attacker could capture, control, and monitor the communication process occurring between the network and the legitimate user, without letting the sender and receiver become aware about the attack.

Suppose the server is sending data to its authorized user, by getting access between both, an attacker can redirect the data to itself or another destination. It is also known as "session hijacking", as an attacker is observing the session actively and steal the session by pretending as an authorized user through IP spoofing.

An attacker can also take advantage of the fact that when the communication taking place at the lower levels of the network layer among machines, the machines could not be able to recognize that who is the sender or receiver of the data, means whether the user or machine is authenticated or not. In this way, an attacker can increase his knowledge about the entire network and can cause damage in the network in a similar way as in application layer attack.

To prevent this attack, the sender and receiver must share some secret information, which may be checked after short chunks of time during the whole session, to assure that the communication is taking place between the two authorized users.

1.4.9 DNS Poisoning

Misleading DNS information sent by an attacker can distract the network traffic. When a DNS request is made by a server, an incorrect DNS reply with fake knowledge is sent. The servers do not make verification of DNS replies and may cache the fake information sent from an attacker. In this way, an attacker also steals user's login information and the users are deceived by detracting from their required web servers.

1.4.10 Application-Layer Attack

In an application-layer attack, an attacker intentionally constructs flaws at the server's site operating system and applications. The purpose of an attacker behind this is to get access controls over the application, server, or the entire network. Eventually, an attacker can alter the original data or operating system, shutdown the operating system or applications, alter the route of data to be exchanged, terminates the security measures implemented in the network to

introduce attacks in the system, and define and spread the viruses throughout the network.
A sniffer program can also be used by an attacker to determine, and then damaging the network. An attacker can also disable all the security checks implemented in the network, so in future he can attack the network without any obstacle.

1.4.11 Denial-of-Service (DoS) Attack

The denial-of-service (DoS) attacks are launched against the machines which are in connection with Internet. DoS attacks make the network unable to use by the legal or authorized users. The DoS attack can be achieved through taking advantages from the flaws and weaknesses in TCP/IP protocols and operating systems.

An attacker can attack the network services by sending corrupt data to applications at server's site, so that the legal users cannot get the proper services, and the application may shutdown the server improperly. An attacker can also consume network resources and overload the network or the server by sending queries in a huge amount. As a result, the server get jammed in serving the attacker's requests and thus unable to perform legitimate user's operations. The contaminated machines becomes harmful and then removed from the Internet.

1.5 Preventing DoS Attacks

If the DoS attacks cause less harm, then by restarting the network, the user may get the normal services and perform usual activities. The DoS attacks can be devastating for corporate network or ISP. The DoS attacks are easier to accomplish and their occurrence on the Internet has become very common.

Defensive measures against DoS attacks are not very effective. The successful way to defeat DoS attacks is to configure the network properly, upgrade the network with updated security patches, making the system capable of determining and monitoring the source of incoming traffic, and block the IP from flooding of requests occur at once.

1.6 Levels of Dos Attacks

DoS attacks can be identified by different levels. Such levels are as follows:

1.6.1 Bandwidth Attacks

Hosting of sites provide a certain capacity of bandwidth to the sites. If the loading of a particular site utilizes all of its bandwidth by the visitors to the site, then site hosting can be prohibited. The hackers can attack the site in same manner. They can open several pages of a site and utilize all the bandwidth by refreshing those pages. The site serves the hacker, denying services to other visitors.

1.6.2 Logic Attacks

The hacker takes favor of the flaws in susceptible web server or the underlying TCP/IP stack of a network.

1.6.3 Protocol Attacks

The protocols installed at the victim server could be exploited by the hacker through the faulty features or breaches in installation of protocols, and utilizes the excess amount available to its resources.

1.7 Categories of DoS Attacks

Categorization of DoS attacks has major importance because there is slight difference between all the categories, which could help in determining and implementing the proper defending mechanism against them. DoS attack can be of two roughly categories, which are as follows:

1.7.1 OS-related Attacks

These attacks occur because Windows 95/NT and earlier Mac OS were easily susceptible to attack or damage. Now in later advanced versions these bugs have been refurbished by the vendors. The vendors improved the operating systems and solved those bugs through patches programs.

1.7.2 Networking-related Attacks

Researchers have discovered various security breaches which can give benefits to the opponents. The DoS attacks are considered as a serious federal crime according to National Information

Infrastructure Protection Act of 1996. Firewall is the most common technique used for defending against networking-related DoS attacks. Also the vendors set up patches for Windows 95 and Windows NT against DoS attacks. Another solution consists of filtering IP packets with spoofed source address, is the most successful security measure.

1.8 Types of DoS Attacks

The main purpose of DoS attacks is to bring down the services of a network. The types of network-related Dos attacks are as follows:

1.8.1 Ping of Death Attack

It is an old category of DoS attack and its attack mechanism is not complex. The IP devices which were used before 1996 can be crashed by sending IP datagram or ICMP datagram, which are of enormous size (larger than 65,535 bytes). The system or device upon receiving such datagrams becomes ruined.

An attacker takes benefit from the flaws in TCP/IP protocol. This attack was caused due to bug found in Berkeley TCP/IP stack. The systems which copied the Berkeley network code became affected. Currently, the outdated systems are obsolete, thus ping of death attacks are not successful in today's updated and advanced systems and devices, because security measures against this attack are available in modern systems.

1.8.2 Ping Broadcast Attack

This attack occurs when a packet containing ping request, created by using a "ping" command, reaches to the broadcast address of a network. The IP address of the victim machine is sent in the packet as a source address. When this packet broadcasts on the other hosts of a network, all the machines send ping replies to the victim machine. The victim machine overwhelmed with these ping reply packets and could not be able to continue its normal operations in the network, which might be resulting in lock up of a machine. It is possible that the victim machine may available on another network. This attack can be prevented if the incoming packets are rejected by the broadcast network address.

1.8.3 Land Attack

Land attack resembles with SYN flooding attack. The hacker floods the network by sending SYN messages containing spoofed source IP address of the victim server.

1.8.4 Snork Attack

The hackers launch an attack against Windows NT RPC service, known as a snork attack. This attack enables an attacker to utilize the 100% CPU usage for undefined limit of time, on a remote NT machine by using at least resources.

1.8.5 Teardrop Attack

Like ping of death attack, teardrop attack also becomes a part of past. A hacker uses IP's Packet fragmentation algorithm and sends debased IP packages to the targeted machine, which makes the machine confuse. Eventually, bugs in the code of TCP/IP fragmentation could corrupt the operating system and crash the systems. The operating system vulnerable to teardrop attacks includes Windows NT, Windows 95, Windows 3.1x, and all versions of Linux.

1.8.6 Smurf Attack

Smurf attack is a new category of flooding DoS attack. The capability of a computer to process the incoming requests can be exploited by using Spoofed IP address of a particular computer and make a ping request to the broadcast network address or broadcast server. The network becomes "smurf amplifier" and ping request is broadcasted to all hosts in the network, which in turn send the ping replies to the computer, whose IP address has been spoofed by an attacker. Hence, the computer gets stucked with the traffic flood and ends up all the other activities (services offered to the users of the network will be stopped); spending all of its time to response the ping replies. Also, all the bandwidth of the network is consumed rapidly.

The challenge faced by a hacker in this attack is to locate the broadcast server in the network. It is difficult to defend against smurf attack. However, necessary and appropriate measures in the network can avoid smurf attack. Also services like "Smurf Amplifier Registry" are available on the Internet which enables the service providers of the network to determine the location of misconfigured devices, to take precautionary actions like "filtering", before an attack.

1.8.7 TCP SYN Flood Attack

In SYN attack, an attacker also takes benefit from the flaws in three-way handshaking process in TCP/IP protocol. When two machines have to communicate which each other, they first establish the connection between them, containing SYN and ACK messages. If the hacker at sender machine overload the receiving machine with SYN messages, its SYN buffer becomes filled and its capability to send ACK messages to the sender becomes failed. Thus, no TCP/IP connection establishes between two machines. Also, other machines could not communicate with the effected machine.

Considering a small flood of fake packets in comparison with a large flood of fake packets, are enough to cause deadlock and consuming the server's site applications, memory and CPU, resulting the server to be shutdown. By using cryptographic techniques, security measure like "SYN cookies" is used to defeat SYN flooding DoS attacks. This method has become a part of Linux as a standard.

1.8.8 Flood Attack

Flooding is the main, oldest, and commonly known category of DoS attacks. The attacker uses the simple mechanism by sending enormous traffic to exhaust the server. The attacker sends requests in such a large number that it exceeds the capacity of a server to serve all of them. For this purpose, an attacker must have more bandwidth than the server.

If the administrator provides sufficient bandwidth to the server, then the attack can be failed. But the server will still too busy in serving all the requests, as it cannot be distinguished that which requests are coming from legitimate or illegitimate uses. Flooding is almost hardly avoidable. The chances to launch a successful attack are more in DDoS environment.

1.9 Security Measures for MANETs

Security measures allow the network to continue its normal functions and operations in a situation, when an illegal access or an attack is made against the network. Security is required to protect the network against various types of attacks, unauthentic data, illegal attempt to access data or resources, hacking the system or data, etc. To ensure security, the network must use different tools and techniques to prevent, detect, contain, and recover the system or network from an attack. Proper and appropriate security measures are required to be implemented in the network in order to achieve the adequate performance, efficiency, and reliability.

1.9.1 Attack Prevention

This technique ensures the failure of attacks that are attempted towards the network in order to cause damage. An attack prevention technique does not allow an attack to be occurring in the network. The system or network is designed in such a way that it makes impossible for an attacker to cause any attack or problem in the network. Attack prevention technique prevents the security issues to cause any problem. By employing firewalls in the network, the opponents (illegitimate users) and DoS attacks can be prevented. Such security measures are implemented so the attackers are not able to attack the system.

This technique keeps away the illegal and unauthorized user from the network. By implementing the idea of digital signatures, the fake and malicious users who pretend to be the legal user of the network are prevented as the digital signatures of the original users are needed. Hence it prevents the user from lying. It prevents the malicious nodes from entering in the network. However, in P2P systems, during a DoS attack, preventive techniques may become ineffective and failed to disallow the malicious nodes to join the network.

It uses techniques such as Physical Security, Uninterruptible power and Firewalls in the case of failure, Authorization, Authentication, Access Control, Digital Signatures, Time-Stamping, and Non-repudiation in the case if the user attempts to lying, Hardware Protection and Firewalls in case of infiltration. Prevention disallows the effects of an attack made by the attacker to be entered in the system. However, in many systems it becomes difficult to prevent a DoS attack against system's availability. Prevention may not be perfect in some critical cases and the attacks can be occurred even if preventive techniques are implemented.

1.9.2 Attack Detection

This technique detects and identifies the malicious nodes that have entered in the network and tries to eliminate those nodes from the network, also cancel the privileges given to those nodes. Attack detection process may take some time to identify the malicious node or attack occurring in the system. After identification the nodes are eliminated from the system.

When a network is under an attack, the detection algorithms are being used in parallel to offering degraded QoS. Detection is useful in determining when the DoS attacks occur in a network. Detection of an attack also provides awareness about the occurred problem or damage to the system administrators and users. It uses techniques such as Watchdog Processors Polling and Beacons in the case of failure, Fail-Stop Digital Signatures if the user attempts to lying, Virus Scanners and Tripwire in case of infiltration.

1.9.3 Attack Containment

The harmful nodes that have joined the network and not being detected started to cause damages in the network, the containment technique tries to overcome the damages and reduce the number of problems occurred, by using detection and recovery algorithms. These techniques are applied during the attack occurrence. So attack containment techniques are lessening harmful effects till the attack has been detected. If the effects of an attack are not removed, then it is possible to minimize its effects. The valid techniques must be applied in the situation when the attack is occurring. The attack which is in the process of taking place is contained in the network, and along with this attack these techniques allow the clients to take advantage of the (degraded) services. Therefore, the systems are allowed to continue to operate its functionality.

Replication method is used to replicate and manage multiple copies of data or files at multiple storage devices or nodes. It helps in continuing the clients activities if a storage device is failed due to crash or any other reason. The client's request will be fulfilled by retrieving data from another storage device that contains the replicated data. During the process in which malicious nodes have entered in the network and are detected for disconnection, the negative effects that cause failures to the normal operations are contained. If a certain level of autonomy, decentralization, and distribution is given to the nodes in a P2P system, then the containment techniques provide protection to the nodes even if the malicious nodes are still present in a P2P network. It uses techniques such as Redundant Array of Independent Disks (RAID), Non-Stop Processes, Fault-Tolerance, Replication and Backups in the case of failure, Byzantine Agreement and Reputation Systems if the user attempts to lying, Intrusion Tolerance and Virus Cleaners in case of infiltration.

1.9.4 Attack Recovery

This technique is used when an attack has occurred and cause damages in the network. Various techniques and methods are applied to recover the network to its original state (as it was before the occurrence of an attack) by repairing the damages. After an attack, the damaging effects can be repaired. If a failure results in loss of a portion of data or information, its recovery can be possible after the failure. The system can also be recovered by eliminating the malicious nodes from the network in order to continue the normal operations of the network.

It uses techniques such as Fail-Over, Hot Swapping, Key Escrow, and Rebooting or Restarting in the case of failure, Auditing if the user attempts to lying, Certificate Revocation in case of infiltration. After detection, the malicious nodes should be eliminated from the network for a recovery process. In a condition when a malicious node is used for the routing purpose, then on its removal this action could be assign to a certain good node after reconfiguring it such that the other nodes can have its updated routing entries. The network must adopt specialized re-construction algorithms when it is recovering from an attack that can cause network fragmentation.

1.10 Thesis Outline

Chapter 1 presents the detailed Introduction of MANETs, DoS attacks, it's types, ways how to prevent DoS attacks, Flooding algorithms, how they can provide beneficial for MANETs, and the necessary security precautions for MANETs.

Chapter 2 is about Literature Survey which presents the work and experiences of researchers related to our domain.

Chapter 3 belongs to Problem Definition and Research Objectives. There, we have defined the problem domain and scope of our research. All the tasks are clearly discussed which are accomplished in the next two chapters.

Chapter 4 is all about our Proposed Solution and Methodology. There, we discussed our proposed strategies according to the problems which were declared in the previous chapter.

Chapter 5 shows our Results based on simulation. By considering various scenarios, we have proved how our strategies perform and give better results, as compared to current situations.

Chapter 6 is based on Conclusion. There, we have summarized some of the issues that can be discovered by the future researchers.

2. Literature Survey

2. Literature Survey

The researchers are always in search to discover the ways that could bring improvement in the current scenarios. As research is very ample field, so anyone can contribute and share his valuable knowledge and experiences, in order to flourish the technologies, techniques, methodologies of currently existing system scenarios.

To define a problem domain, one should needs to be refine his knowledge by studying what has been done till today. Research is not to steal the ideas or strategies of authors or researchers that have implemented in the running systems. It is all about to know what the current system lacks and how to come up with new strategies which would fulfill this gap.

Literature survey of the papers related to the fields of flooding types in MANETs, flooding attacks at network layer, query flooding at application layer, DoS attacks, broadcasting in MANETs, attack containment in MANETs, provision of quality of service (QoS) in MANETs, are reviewed and categorized under the following sub-headings:

2.1 Literature Survey related to Application Layer Query Flooding

Daswani et.al in 2004 [1] stated the challenges faced by the P2P networks that must be controlled by implementing the searching techniques efficiently. Scalability of P2P networks can bring many issues, such as it becomes difficult to locate and identify the peers and resources in the network, the distribution of bandwidth and data among peers, and may welcome the unreliable or fake data from the opponent, in the network. As a result, the peers, resources, and requirements for resources are changing constantly.

The solution proposed to this problem is to develop a "Resource Market Place" or "Data Trading". Using Resource Market Place, peers can share the resources as needed according to the scenario. An incentive is given to the peers to respond queries. This makes the search faster and reduces the network traffic overloading. Using Data Trading, the local peer can replicate its data to a remote peer by giving some incentive to the remote peer, and hence becomes a peer-to-peer replication network. It helps in reducing failures at the local site.

Daswani et.al in 2005 [2] described the problem of blasting (application layer DoS attack) in

Chord network (Structured P2P systems or Distributed Hash Tables (DHTs). The malicious node sends a huge amount of useless queries to the server peer, to keep the server busy in processing all of its queries, and hence wasting the server's resources (as the server has become overloaded with the queries). Blasting of queries causes the nodes to serve degrade performance and deny service to the requested queries.

As a solution, the authors presented a "Traffic Model" to improve the performance of the network, and run simulations on it, in order to determine how queries flow through the system, how the harmful nodes blast the queries and cause damage in the network. The traffic management schemes and traffic limits are defined that apply containment techniques to overcome the effects of blasting in the network, and to increase the remote work (even in the presence of malicious nodes). So thus the effects of malicious nodes could be contained and maintained. This model leads to successfully recovering the network from the damaging effects of the attack, and also to reduce the network traffic.

Daswani et.al in 2002 [3] stated that Gnutella (Unstructured P2P system) network is extremely susceptible to application layer DoS attacks, as it uses the flooding (broadcasting) algorithms. Gnutella network consists of super nodes (server) and regular nodes (clients). Super node is responsible for spreading application requests to all of its neighbor nodes in the network. A large number of requested queries or useless queries generated by the users cause the server peers not to provide the requested services by the client peers. Hence results in blockage of resource availability.

As a solution, the authors developed a "Traffic Model" and run simulations on it, for the purpose of knowing how queries flow through the system, how the good and contaminated nodes in the network are damaged by the attack, and how this loss is spread in the network. The authors propose the "Load-Balancing" techniques to mitigate the effects of Query Flooding DoS attacks, and provide each node enough shares of resources, in order to process their queries or requests.

Daswani et.al in 2004 [4] discussed the problem of resource discovery in Unstructured Peer-to-Peer network, using a P2P protocol, known as GUESS (Gnutella UDP Extension for Scalable

Searches), which make the peers less vulnerable to attacks. "Ping" and "Pong" messages are used to know which nodes are currently available in the system. Each node maintains a "Pong cache (host)" to keep the ids of available nodes, and finds out the ids of more nodes. A good node's pong cache can be poisoned by having the id of a harmful node. Thus it requires more security.

As a solution, the authors determined that how IDSA, DNP, MND are used to limit the poisoning in steady state. They define a model, which keep track of how pong caches become poisoned through the exchange of ping and pong messages, run simulations on it to determine the patterns of good and malicious nodes, evaluate the effects of poisoning, and suggests new mechanisms. ID smearing algorithm (IDSA) is designed for limiting the poisoning in slow state. Malicious Node Detector (MND) is used when the number of malicious nodes exceeds the size of pong cache. Also the prevention, detection, and containment techniques are proposed to mitigate the effects of pong cache poisoning. Most Recently Used Cache Replacement Policy (MRU CRP) is used to slow down the amount of poisoning. Dynamic Network Partitioning (DNP) is used to minimize the number of malicious nodes ids.

Sun et.al in 2006 [5] explained the disadvantages of using flooding algorithms, e.g., a useless query can be replicated and could deny service to the legitimate queries, the node flood the queries to a limited number of its neighbors, etc. The malicious nodes generate queries flood in order to produce a negative impact on remote work throughput.

As a solution, the authors proposed the ways to determine that how many queries requested by the remote nodes must be responded by each super node, and methods of maximizing the remote work by deciding and controlling the query injection rate at the individual super nodes. Remote work can also be used as a metric for the evaluation of overlay topologies.

Daswani et.al in 2003 [6] described the problems related to Peer-to-Peer (P2P) Systems. P2P Systems are very famous for exchanging enormous data, bandwidth, CPU cycles, disk storage capacity, and other resources amongst all the peers within the network. P2P Systems are currently facing the problems of security, efficiency, performance, scalability, quality of service, robustness, autonomy, unreliability of peers, implementation of effective search mechanisms, expressiveness and comprehensiveness of searching methods.

Existing searching techniques and security measures are not enough today for P2P Systems. New techniques and methods must be developed, and improvements are required for the wide spread of P2P Systems. Security is required due to open and autonomous nature of P2P System. Security is ensured if a P2P System guarantees the availability, file authenticity, access control, and anonymity.

2.2 Literature Survey Flood Types in MANETs

Williams et.al in 2002 [7] discusses the various broadcasting techniques used in MANET, their benefits, and as well as their tradeoffs. The authors presented detailed analysis and views about protocols that belongs to different categories. They compare each protocol with other protocols to realize how protocols act in certain way with its respective situation. The purpose of examining the protocols is to build up standards for routing techniques in MANETs, which are based on broadcasting (flooding) strategies.

The various categories of protocols (Simple Flooding, Probability Based Methods, Area Based and Neighbor Knowledge Methods) are described briefly, tested and simulations are performed for the evaluation of these protocols, to show that how various protocols behave under different conditions and circumstances of varying networks (such as bandwidth congestion and dynamic topologies). The results of simulation help the network designers and administrators to determine which specific protocol will be well suited in which particular scenario. The evaluated results are depicted in graphical form, so they could be easily understand by network makers.

Schollmeier et.al in 2002 [11] have made a detailed analysis and comparison on Mobile Ad Hoc Networks (MANETs) and Peer-to-Peer Networks (P2P). Both networks are famous and flourishing day by day. The authors have discussed the similarities among both networks. They also highlighted the features in which both networks behave differently.

The major focus of this paper is to determine the various ways of routing and the ways in which the routing algorithms are implemented in both networks. The similar features among both networks include the network management policies, routing strategies, use of flooding techniques, decentralized and self organizing nature of nodes or peers. The dissimilar characteristics among both networks include network topology or underlying architecture, behavior, routing protocols, and bandwidth issues. As the MANETs are radio networks and P2P are IP networks, so it is obvious that the mechanism of routing the queries or data packets is also different in both networks.

2.3 Literature Survey related to Network Layer Flooding Attacks

Chau et.al in 2008 [8] discussed the worth of inter-domain routing, which is an important communicating element among various networks that possess different characteristics, and also administered by different organizing bodies. The problem highlighted here is that even though inter-domain routing has served as a foundation for Internet, but inter-domain routing mechanism has not been thrived in multi-domain MANETs. Inter-domain routing have some disputes in MANETs, including varying network topology due to freely moving nodes, and various forms of intra-domain routing protocols.

In order to cater with this problem, the authors has proposed a framework for enabling the inter-domain routing after considering the design issues for inter-domain routing in MANETs. This framework is called as IDRM (Inter-Domain Routing for MANET). IDRM technique is designed as a workable strategy that enables the network makers to understand the inter-domain routing policies precisely. It makes the multiple domains capable of communicating with each other, much easily than ever. Also, IDRM has made the exchange of information efficient among end-to-end users. The techniques to cope with the liberty of MANET nodes are also proposed in this paper. Hence, using such technologies can make a MANET better and efficient network to be used by a large number of users.

Tarkoma et.al in 2008 [9] discusses the challenges related to node mobility within a network where data is broadcasted according to needs (user requirements), and problems that occur while exchanging data among end-to-end users of the network. The network communicates in data driven form. The authors made a brief study towards the worth of network topology and find it very useful, effective and a fundamental element for network architectures. They have considered a network as a collection of black boxes, as hiding the internal infrastructure of a network and only exposing the titles and data of user's interest to the end users is black box's property.

They have proposed a rendezvous which act as a central functional point of a black box. Rendezvous would provide functionality only when the network is reliable in terms of communication, cost, and performance. The main theme behind designing rendezvous functions is to hold up the policy-based routing, management operations, serve the requirements of various applications of a network, and upgrades the networks architecture. The authors has realizes that rendezvous is the need of a network topology at the early stage of development.

Scheuermann et.al in 2008 [10] highlighted the importance of multicast mechanism in MANETs, as well as the problem of congestion control facing by multicasting technique in MANETs. In MANET, all the existing nodes share the same medium capacity, thus the limited bandwidth can be congested with the traffic of packets. Multicasting provides the benefit to save the bandwidth when packets have several recipient nodes. The authors have presented the idea of deploying an implicit hop-by-hop congestion control protocol for resolving the multicast traffic issue in multi-hop MANETs.

This idea of congestion control puts into practice with Multicast Congestion Control (BMCC) protocol, in addition with Scalable Positioned-Based Multicast (SPBM), in order to determine how this mixture acts in geographic multicast routing. For this purpose, the Multihop Backpressure is implemented by utilizing simple rules for packet forwarding, which uses implicit feedback. As a result, the authors have come to a successful conclusion that with highly congested bandwidth and lower protocol overhead, the proposed methodology can achieve the high throughput and packet delivery quantity.

2.4 Literature Survey related to Containment in MANETs

Castaneda et.al in 2004 [12] focused on a class of routing protocols known as On-Demand Routing protocols. A query is broadcasted throughout the network in order to search a source to destination route. Each query has assigned a unique identifier to avoid the same query to be multiply propagated from the similar node. So when a query is reached at the destination node, it responses back to the sender node with a route reply packet. After that, all the traffic is sent to the destination through the determined route. This overall process increases the routing overload in the network because the query was flooded to all nodes when it was initiated, in order to search a successful route towards receiver node.

The solution to this problem is to reduce routing load from the network by introducing the concept of Query Localization, i.e., the query flood has been localized to a limited region of the network. This approach makes use of route histories to contain the query flood to a limited region and thus does not require any location information as it restricts the query flood only to its neighboring nodes. The simulated results are tested and evaluated the query localization technique against various on demand routing protocols.

Abdelhafez Mohamed Abdelfattah in 2007 [13] has worked on techniques that are used to mitigate the effects of an attack in the network. His dissertation's major attention is towards the impact of worms and their effects. Once worms have become active, they replicate and expand themselves rapidly on a vast scale. To prevent and defend against them is a challenging security issue. Many techniques have existed to control worms, but worm impacts are not being tested and analyzed on any running traffic.

The author has made three contributions to this domain. First, a comparative analysis of performance and the effectiveness of all the existing defensive measures is made by running them on live traffic. Also, another technique is introduced which is more efficient and mitigates the multiplying rate of worms with TCP connections working for infiltration. Second, a detailed comparative study is made among the worm Flash and its variant Compact Flash (CFlash). It has shown through simulations that with same parameters, the new worm's propagation rate is more increasing. Third, the behavioral study of TCP worms in MANETs. An Analytical Model has been presented to minimize their effects, and the results are evaluated through simulations.

Cheng et al. in 2008 [14] have introduced the concept that effects of malicious nodes can be contained in an intrusion detection systems (IDS). IDS are developed to detect the activities of malicious nodes in MANETs. But due to having some of inappropriate IDS response mechanisms, even the best IDS is failed to achieve the desired results, as the entry of malicious nodes in the network is not quickly conveyed.

As a solution, the authors enhance the functionality of IDS by introducing containment strategies. They presented a T-SecAODV protocol which provides rapid responses and disseminates the malicious node's information rapidly to all the other good nodes in the network. Thus alerts enable the nodes to reset their routing tables to detect and isolate the malicious node from the network easily. The results are analyzed through simulations to show that how the attack's effects are lessened.

2.5 Limitations of the Literature Surveyed

In [1-6], existing searching techniques and security measures are not enough today for P2P Systems. New techniques and methods must be developed, and improvements are required for the wide spread of P2P Systems. Security is required due to open and autonomous nature of P2P System. Security is ensured if a P2P System guarantees the availability, file authenticity, access control, and anonymity.

In [1-6], the features and traits of P2P are discussed only. As the P2P networks are wired networks and based on some type of a fixed topology, so techniques used here can not applied in MANETs, because MANETS are wireless and dynamic based topology networks. There is not any fixed infrastructure of MANET and its topology is formed on the fly.

In [1-6], the nodes in MANETs (usually mobiles or laptops) require battery power and energy to keep them alive. While the nodes in P2P do not have this constraint. Thus, all the strategies proposed by the authors are failed to be workable in MANETs, as these papers are related to P2P networks. Peers in P2P does not require their batteries to be recharged for communicating, because the peers are fixed systems handled by the end users, so direct power can be supplied to them. So this can be the major hindrance in a way of interoperation among the nodes of MANET.

The exchanging data functions will be failed if one node tries to send a query request to other node, and the receiver node is shutdown due to limited battery power.

In [2-4], the application layer DoS attack, its effects, and security techniques to prevent these attacks (especially the attack containment technique has given much importance by the authors) are discussed only according to the P2P networks. In these papers, no one has considered any attack containment strategy for the Ad Hoc networks. We cannot apply the P2P security techniques against attacks in MANETs because of the fact that P2P is a fixed topology network and MANET is a dynamic network, having no topology. So the strategies introduced and designed for P2P are inapplicable for MANETs.

In [2], the authors have developed a number of incoming allocation strategies (IAS) and drop strategies (DS). The load balancing techniques works at the expense of active connections and network stability. While considering MANETs, we cannot ignore the battery issues which cannot afford much active links.

In [3], the authors have built an understanding about how a single malicious node can affect a network when it is placed at different positions in various simple topologies. The strategies proposed for such a scenario could not be implemented in large, complex networks that are resilient to flood based DoS attacks with multiple malicious nodes.

In [4], P2P traffic management policies are designed by assuming the possibility that all the queries received at the specific links could be noticeable by the legitimate nodes. This possibility cannot be supposed in case of MANETs because of the liberty of nodes. Also, the MANET nodes must spend more battery resources for this purpose, such as in case if the rate of incoming queries becomes high at a link, then the node might drain out its battery for checking all the incoming queries.

In [4], the authors has discussed that the pong cache size of good nodes can accommodate less percentage of nodes ids in network. While large size cached must be used to mitigate the pong cache poisoning.

In [5], the authors have worked on remote work where forwardable and answerable queries are not differentiated. The remote work is definably stated as to serve or fulfill the queries of other nodes of the network. Remote work would not be able to accomplished until and unless the other node's query is being satisfied and answer by the server. The authors allocate same value to the forwardable queries and to the answerable queries. But in reality answerable queries require more network resources as compared to forwardable queries. So we cannot differentiate that whether the query is answerable or forwardable. Thus, it cannot be decided that which queries must be dropped and which would be entertained.

In [10], the author have discussed that the limited bandwidth can be congested with the traffic of packets. So the strategy will not work properly if enough bandwidth is not available.

In [12], for query localization techniques, maintaining and searching for routing histories can consume more resources which also require extra processor's energy, which can be an issue in MANETs.

2.6 Chapter Summary

MANETs are emerging day by day. Thus, its importance and applications are increasing rapidly at a large scale. There are certain critical issues regarding to MANETS because it is a wireless network that occurs on the spot according to situation. So, effective and highly strong security is needed to maintain such networks. The former security measures presented by various authors in this chapter are not much enough now to deal with Application layer Query Flood DoS attacks in MANETs. It requires such efficient security precautionary measures which can ensure the tight security of the network.

3. Requirements Analysis

3. Requirements Analysis

Requirement analysis is a critical process of understanding needs of the users, studying the problems in current situations, gathering information about the system, and realizing that which new evolving technologies can solve the problem, and fulfill the needs of end users. The requirement analysis forces to introduce new dynamic changes in the present network and to fulfill the system's and system user's expectations.

Ad Hoc networks possess characteristics such as, self organization, self healing, distributed, dynamism, etc. Ad hoc networks use wireless transmission techniques as they are distributed networks. Ad hoc networks come into existence as gathering of nodes communicating through wireless media. Symmetric solutions are achieved through randomization and it helps to increase the network's performance and efficiency. Mobile Ad hoc networks (MANETs) are subset of Ad hoc networks. MANETs needs more security then other networks.

MANETs contains the following features due to which it requires necessary and immediate proper security measures.

1 MANET is very cheaper and easy to establish. So the security for MANETs must not be a difficult and complicated task. Security must also be easily provided.

2 Nodes form a wireless network. More security must be required as compared to wired network as wireless links can be easily attacked.

3 Nodes are not fixed. They can move freely anywhere. So it must be ensured that all the nodes are under protection by security control.

4 Nodes are decentralized. Thus security solutions need to be coping and distributed among all the far spreader nodes.

5 Nodes are easily scalable. During a session, the available nodes can be in the range from 10-1000. So such security is required that can manage a small as well as large network.

6 Nodes can join and leave the network easily and quickly. Hence security must be implemented to check whether a malicious node has not injected in to the network.

7 Nodes form an unreliable network. So the network is always under attack threats. Security measures must be formulated against this major problem.

8 Nodes form dynamic and temporary network topology. Security checks must ensure that

when a node disjoins the network, it must not be infected.

9 Nodes cover limited geographical area. Nodes cannot be span up to whole world. Enough security must be guaranteed in the known area.

10 Nodes have power, energy, or battery limitations. Such security measures must be implemented which can deal with rare energy resources.

11 Nodes create a network for short period of time. So no need to create complicated security measures. They must be simple and easy to deploy.

12 Nodes take security decisions on the fly. So appropriate, adequate, and proper security solutions must be available in the network to provide guidance to the nodes.

13 Nodes are susceptible to attack or damage. Even the whole network can be ruined. Security must be capable of saving the network from open threats.

14 Nodes use flooding or broadcasting techniques. Thus they are vulnerable to application layer DoS attacks. Security must be implemented against DoS flooding attacks.

3.1 Problem Definition

It is clear from the topic of the thesis that the problem has been defined into two sub categories, i.e., Query Rejection Techniques and Impact of Attacker's Position, which are discussed under the following sub-headings.

3.1.1 Query Rejection Techniques

Since every node of the Ad hoc network has limited processing capacity, so it is not possible to entertain all the incoming queries from different nodes of the network. Few queries need to be dropped at the node. Currently in Ad hoc networks the queries are served in First Come First Serve (FCFS) fashion. The nodes accept or reject the queries according to FCFS technique implemented on a node. The details of the FCFS approach are shown in the following Figure 3.1.

In figure 3.1, the receiver's node has the capacity to fulfill only four requests. According to the FCFS principle, queries A, B, C, and D are entertained from different nodes of the network, and all the other queries except the first four queries will be just simply ignored by the node and could not take any of the services offered by the node.

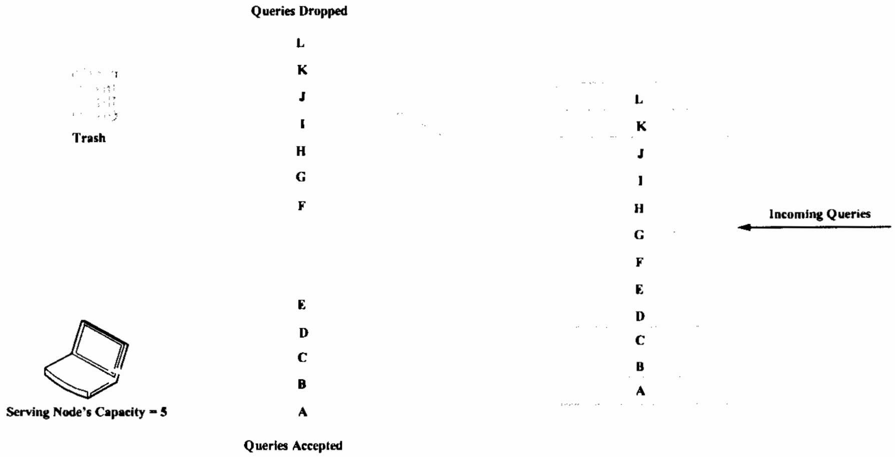

Figure 3.1: First Come First Serve (FCFS) Mechanism to Drop Queries.

This technique has various drawbacks, but the major problem which we are considering in our thesis is that the age of the query is also totally ignored by the current approach. In other words, the Time-To-Live (TTL) value of the query is not considered in FCFS. If age of the query is considered then we can estimate how much time has been passed when the query was generated, how much nodes or hops it has been traveled through flooding algorithms and how much resources are consumed, is the query is acceptable or it needs to be dropped.

3.1.2 Impact of Attackers Position

In Ad hoc networks information is shared by using broadcasting or flooding techniques. In wireless Ad hoc networks, only flooding technique is used for building and deploying the higher level protocols. The use of flooding is preferred because it is mostly used in networks as it is more reliable, faster, simple and easy to build and deploy, get search results quickly, and resilient against quick joining and leaving the network by nodes. A node is made to be completely overcome through a flood of queries which are continuously arrived at a receiver node. The flood of queries results in the consumption of resources, such as, CPU cycles, memory, bandwidth, packet buffers, etc. Flooding degrades the network services and cause destruction.

Moreover, the position of the malicious node also effects the security measures and leaves different impact upon the overall network performance. By assuming the location of an attacker or malicious node is known to us, we can analyze how much damage can be caused at a particular position of an attacker and victim, an attacker can flood a single query up to how many levels or hops, or how many nodes can be targeted by selecting a specific location. Through this analysis, we can recommend which nodes are most deserving of security. Security measures then could be implemented to the nodes that have more threats of damaging. The Figures 3.2 (a, b, c), 3.3 (a, b, c) represents how flooding algorithms and attacker's position effects the MANETs.

Attacker A at Central Position

Let us consider an attacker A attacks from a malicious node located at the centre of a network, and wants to sends its queries to a receiver node located somewhere at the corner of the network. In the figure 3.2, the node A is an attacker in a network of 29 nodes (Figure 3.2 (a)), in the first hop an attacker will flood the 11 other nodes (Figure 3.2 (b)), and in the second hop an attacker will flood the total 25 nodes (Figure 3.2 (c)) from the total 29 nodes of the network.

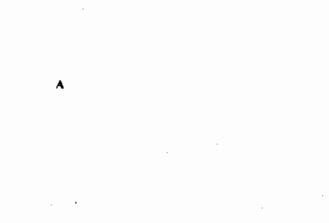

Figure 3.2 (a): When Node A is an attacker

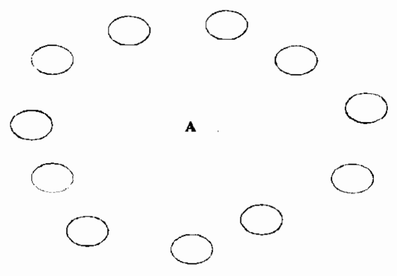

Figure 3.2 (b): Effect of Node A's Attack at First Hop.

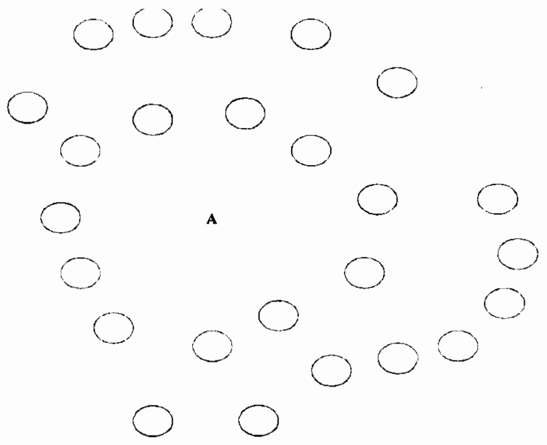

Figure 3.2 (c): Effect of Node A's Attack at Second Hop.

When an adversary node is situated at the center of the network, it will cause the maximum damage as it is easy to overload the network with blast of queries here. So we conclude that if we assume the malicious node is placed at the center of the network, more receiver nodes can have attack threats. Thus, more security is required to all the receiver nodes.

Attacker E at Cornered Position

Let us consider an attacker E attacks from a malicious node located at the left corner of a network, and wants to sends its queries to a receiver node located somewhere at the center of the network. In the figure 3.3, the node E is an attacker in a network of 29 nodes (Figure 3.3 (a)), in the first hop an attacker will flood the 1 other node (Figure 3.3 (b)), and in the second hop an attacker will flood the total 2 nodes (Figure 3.3 (c)) from the total 29 nodes of the network.

Figure 3.3 (a): When Node E is an attacker.

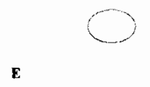

Figure 3.3 (b): Effect of Node E's Attack at First Hop.

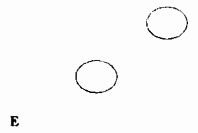

Figure 3.3 (c): Effect of Node E's Attack at Second Hop.

When an adversary node is situated at the corner of the network, the attack will cover a few nodes of the network. So we conclude that if we assume the malicious node is placed at the corner of the network, less receiver nodes can have attack threats. But security must be provided to all the receiver nodes.

3.2 Research Objectives

Objectives of the research are the basis of any solution design strategy. These objectives are obtained after understanding vexes in current system. The main theme behind outlining the objectives is to propose a solution that treats the present faulty facts and define the aims or goals to be achieved that avoid perplex scenarios. According to the problems which were formulated above in problem definition (section 3.2), we stated the following research objectives.

3.2.1 Enhancing Quality of Service (QoS)

The query denying techniques and the use of flooding protocols degrades the QoS of the network. The main objective of this research is to enhance the QoS of Ad hoc networks by designing and testing some efficient and effective query drop strategies.

3.2.2 Improvising Network Performance

We have design and test different query dropped strategies in order to find the efficient solution and to enhance the network performance. We have also analyzed how flooding and different positional attack models effect on network performance.

3.2.3 Providing Attack Containment Techniques

We have assumed that if we could become aware of the attacker's location in the network, then we could be able to protect that particular victim node with more security solutions and attack containment techniques. The security would be gained on the fly when attack has been initiated by an attacker.

3.2.4 Reducing Starvation

One of the main objectives is to minimize the chances of starvation by avoid serving an attacker. Thus starvation does not occur to legitimate users.

3.2.5 Defending Flooding Techniques

A single useless query can degrade the network's functionality by replicating itself so many times through broadcasting algorithms. A simple solution suggests avoid flooding based protocols. But in MANETs, the quality protocols can be deployed on nodes only through flooding techniques.

3.2.6 Preventing Energy Compels

Query traffic load needs to consume battery power of the MANET nodes. The proposed query dropping techniques would drop the queries on hop count basis and processing of queries would save node's energy and time.

3.2.7 Evaluation and Formulation

Each query drop strategy and attacker's node placement is formulated and evaluated against various situations and achieve results by using NS-2.

3.3 Chapter Summary

Flooding algorithms or broadcasting techniques in MANETs is vitally an important issue. Since every node of the Ad hoc network has some limited processing capability, so it is not possible to serve all the incoming queries. Few queries are served and few are dropped. Position of attacker is one of the important parameters in Ad hoc network while analyzing the overall network security.

4. Proposed Solution and Methodology

4. Proposed Solution and Methodology

In the previous chapter, we have stated in detail the problems and security challenges facing by the current Mobile Ad Hoc Networks (MANETs). The problem definition (section 3.1) contains a brief discussion on query's rejection and acceptance techniques available today (section 3.1.1). Also, the issues occur due to the attacker's location (section 3.1.2) were highlighted. We have proposed and design the solutions in order to excel the research objectives outlined in the previous chapter (section 3.2).

In consideration with the problem definition, we realize to design such solutions that can be enough to cope with the problematic MANETs situations. In this chapter, we have proposed the strategies for denying the queries (section 4.1). Also, we make an understanding that how much impact can bring in a network along with the malicious nodes by assuming the attacker's location is known (section 4.2). The purpose of designed solution is to provide just and fair rights to all the nodes in order to achieve Quality of Service (QoS), and to provide a better, safe and sound network.

4.1 Query Rejection Techniques

When there are enough queries arrived at a receiver node, then the task of managing and handling the blast of queries becomes hard. Selecting and dropping the queries by a receiver node is a major issue. To bring efficiency and to get better Quality of Service (QoS) in Ad Hoc networks, we have designed different Query Rejection Techniques.

These strategies will help to decide a receiver node that which queries should be dropped. This decision will be taken by the receiver node according to the network's situation by assuming that the receiver node has all the previous history or records of such challenging situations experienced by the network so that the node will study those patterns and take the decision wisely. Rejection strategies do not consider that the query is coming from legitimate or illegitimate nodes.

To implement the proposed solution, we will assign a Time-To-Live (TTL) or Hope Count (HC) value to every query at the time of its birth. When a node wishes to inject a query in to the network, it assigns a value to the query. The requester node will set the value of its own query to zero (0) and after that every other node will increase it by one. That is, when the query will be flooded to various neighbor nodes throughout the network, the nodes will mark the query's HC value as one (1). It tells us that the query has traveled only one hop since its birth. Then after again broadcasting, the query's age will become two (2), which means the query has traveled now two hops of the network, and so on. The abstract architecture of the proposed solution is shown in the figure 4.1.

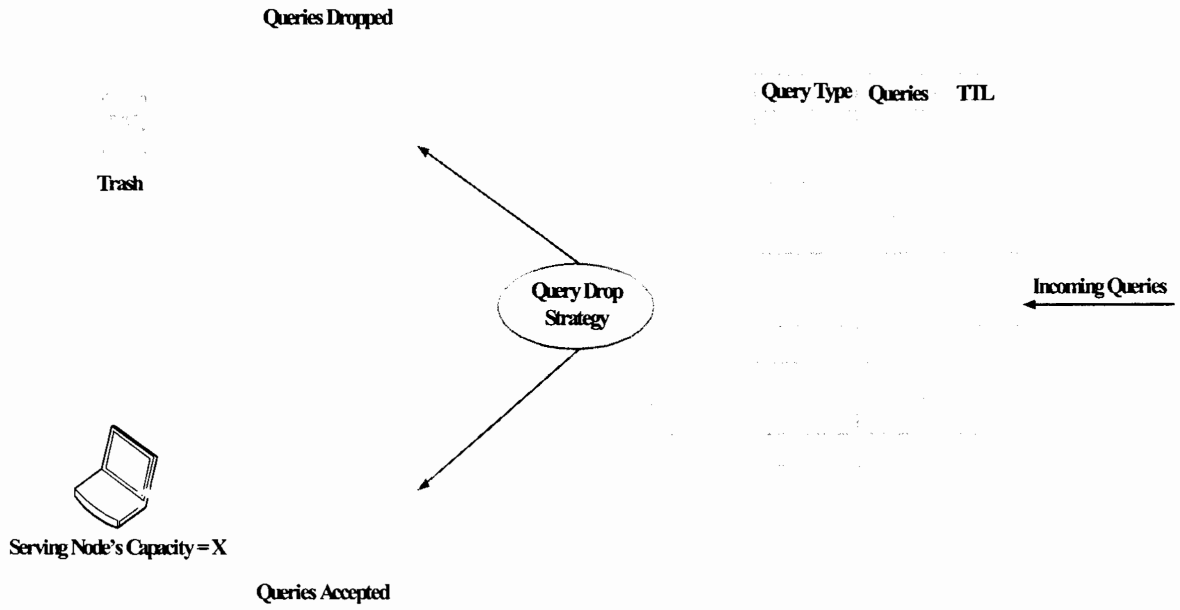

Figure 4.1: Proposed Query Drop Model.

4.1.1 Drop Youngest Queries

In this approach, the receiving node will entertain the queries with higher HC (oldest age). Since the query with higher HC has consumed more of network resources, so serving those queries will results in efficient utilization of resources. If a query has traveled so far, then it may possible that it is near to its destination. And if a query has a small HC, then the possibility exist that this query is far from its destination. Neglecting an oldest query could result in wastage of the resources that has been utilized by the query while passing through every hop. Figure 4.2 explains the scenario in detail.

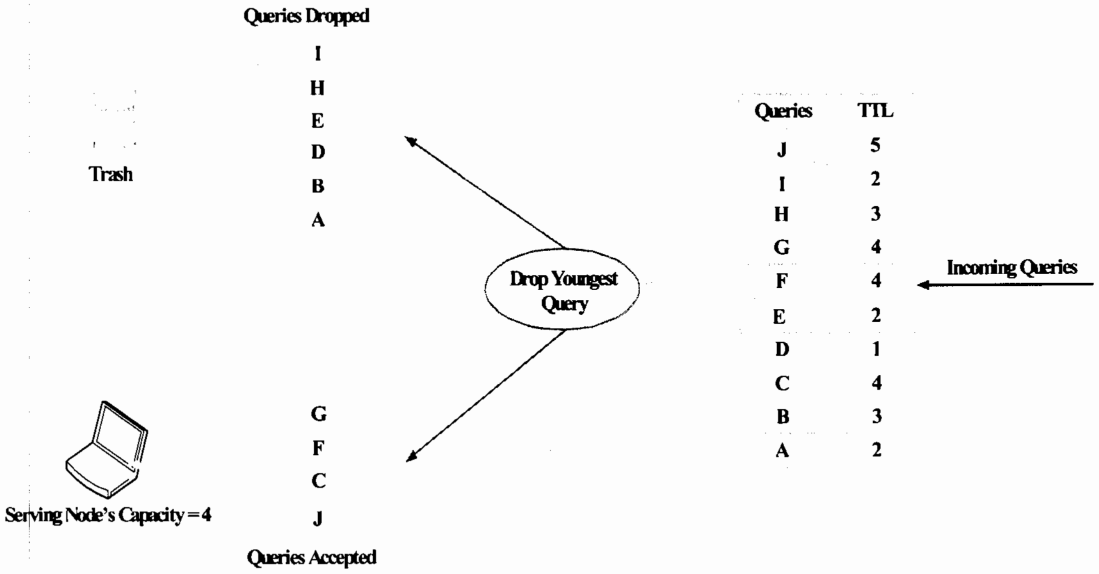

Figure 4.2: Drop Youngest Queries.

The receiver node will analyze the received queries and determine that the queries which have existed since a long time should be accepted for processing, and the queries that have born recently must be discarded.

4.1.2 Drop Oldest Queries

In this approach, the receiving node will drop the queries with higher HC (oldest age), because older query have chances to be processed by some other node before reaching to a node which is under observation. Another reason to drop the query with higher HC is that the requester might not require this information now, as the request could be fulfilled by another path followed by a query. Serving older queries will generate more and more useless replicas of a single query in the network, and the query will become older and older. Since younger queries with lower HC are fresh and have consumed fewer resources yet, so serving them will automatically enhance the network performance. Figure 4.3 describes this policy in detail.

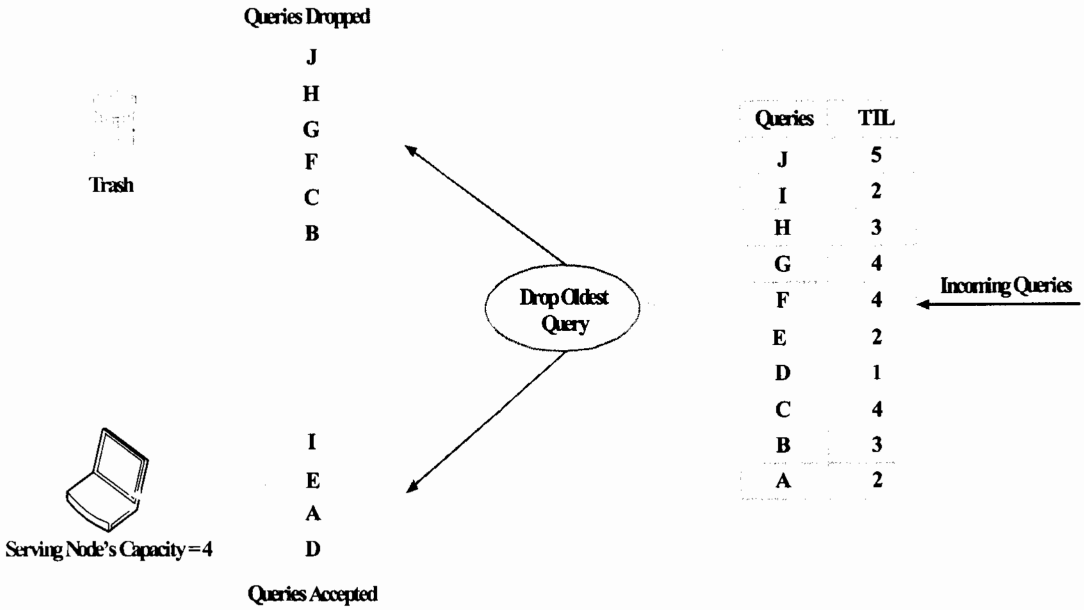

Figure 4.3: Drop Oldest Queries.

The receiver node will analyze the received queries and determine that the queries which have existed since a long time should be discarded, and the fresher queries must be served.

4.2 Impact of Attacker's Position

Attackers establish attacks by creating overwhelming scenes through flooding strategies. Attacker's aim is to inject malicious queries in the network as many as possible. Through utilizing and exploiting broadcasting algorithms in MANETs, an attacker can cause a blast of malicious queries in order to occupy all the processing capacity of receiver's node deceivingly.

We have assumed that the adversary or an attacker has complete knowledge of the topology of the network and interested in injecting a query to a receiver or victim node, which can be any node of the network and can be located anywhere in the network. As we are focusing on service degradations experienced by different victim nodes in the network, so we build an understanding of how much impact a malicious node can have on various relative placements of the malicious and victim nodes in MANETs.

Figure 4.4 represents different locations of a malicious node in the network when it is placed on the following positions in the network:

Attack Hubs

Malicious nodes are placed next to the receiver node in the network. So attackers are one hop far from the receiver node.

Attack Hub Neighbors

Malicious nodes are placed in positions that are directly connected to the hubs. So attackers are two hops far from the receiver node.

Attack Corners

Malicious nodes are placed at the corner positions in the network and an attacker launch attacks towards victim node. So attackers are multiple hops far from the receiver node.

Figure 4.4: Malicious nodes at various placements.

We have assumed that the attacker can attack through the above discussed positions to a receiver node. After realizing from where the threats of attack are coming to a receiver node, immediate security would be provided on the fly. We have assumed that a receiver have all the knowledge about the network topology, the previous patterns of attacks and the recovery and security techniques. The security will defend the network from an attack by reducing the effect of an attack. The damage cause in the network through flooding attacks can also be minimized by introducing and deploying security safety rule at the spot.

4.3 Chapter Summary

In this chapter, we have developed different cost effective query rejection techniques to get efficient results and to enhance the network QoS. These strategies also results in saving energy and power of network nodes. Position of attacker at malicious node plays an important role to launch an attack. The MANETs performance can also be enhanced by assuming different attacker's locations. The impact of attacker's position is studied on two assumptions, i.e., we have assumed that the attacker's location is known, and the receiver node have all the nowlwdge about the network to determine the attack alerts.

Chapter 5

Results

5. Results

The proposed query rejection techniques are evaluated in this chapter by using NS-2. We have created various different scenarios for performing simulations and evaluating results. The results are represented in graphical form. One can easily analyze the performance of our designed strategies with respect to attacker's position by having a look at these graphs. Hence, NS-2 based simulations have validated our proposed theories.

NS-2 is used for performing network simulations and evaluating results for validation. Basically it is an object oriented simulator, developed in C++ and uses OTcL interpreter as an interface. NS-2 has to maintain a hierarchy at both backend and frontend. In C++, this hierarchy is known as Compiled hierarchy, and Interpreted hierarchy in OTcL. The hierarchies have one-to-one correspondence with each other.

NS-2 is a discrete event network simulator and amply used to perform simulations for routing, multicast protocols and MANETs. As NS-2 is a widely used simulator, so many helpful guides are available on the Internet. Moreover, it is a freeware and its interacting environment is much easier and interesting as compared to other simulators.

5.1 Results Validation

In order to defend our solution and analyze the performance of proposed techniques, we develop a simulated network, create different situations and conduct experiments to see the flow of traffic. The performance is evaluated using the following criteria:

Simulation Parameters:

- ✓ An Ad-hoc network comprising of 30 nodes.
- ✓ Size of the each packet is 100 Bytes.
- ✓ The simulation is run for 100 seconds.
- ✓ Number of malicious nodes can vary from 0 to 10.
- ✓ MAC protocol is 802.11 and bandwidth is 4 Mbps.
- ✓ Routing is performed through AODV Routing protocol.
- ✓ Every node can send 50 to 300 queries per second to the receiver node.

- ✓ Maximum number of queries a node can send to the receiver is 300.
- ✓ The receiver node can serve maximum 1000 queries per second from all over the nodes.

Query Rejection Techniques:

- ✓ Default First Come, First Serve.
- ✓ Drop Youngest.
- ✓ Drop Oldest.

Malicious Nodes Placements:

- ✓ Attack Hub.
- ✓ Attack Neighbor.
- ✓ Attack Corner.

Performance Matrix:

- ✓ Remote Work.
- ✓ Energy Consumption.

5.2 Simulated Scenarios

The scenarios developed to generate results from simulations are presented here. Each following case has a detailed description of its respective graph.

Case 1:

Legitimate Queries Served when Drop Oldest technique is used.

In this experiment, we have measured how many legitimate queries are served when the query rejection technique is drop oldest, and get the results as shown in fig.5.1. It can be clearly seen that when the strategy is drop oldest, 92% legitimate queries are served by keeping attackers at the corners of a network. Since attacker is at corner, so attacker's queries do always have higher TTL value and the drop oldest strategy drops these illegitimate queries. So it is obvious that corner positioned attackers can cause very little damage. While in contrast, if the attacker nodes are placed at hub position, it causes maximum damage and serves almost 70% legitimate queries.

It is so because the TTL values of hub queries are very low and drop oldest serves these queries on first preference. Hub Neighbor serves 80% legitimate queries.

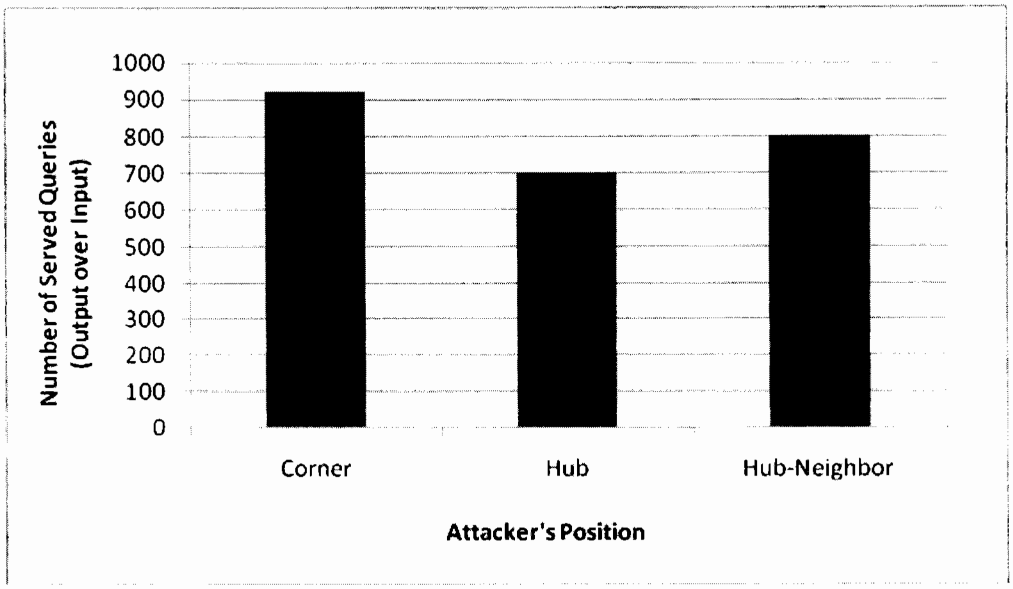

Figure 5.1: The number of legitimate queries served when strategy is Drop Oldest.

Case 2:

Legitimate Queries Served when Drop Youngest technique is used.

In this experiment, we have measured how many legitimate queries are served when the strategy is drop youngest, and get the results as shown in fig.5.2. It can be clearly seen that when the query drop strategy is "Drop Youngest", more 95% legitimate queries are served by keeping the attackers at the Hub. Since attacker is at Hub, so attacker's queries do always have lowest TTL value and drop youngest strategy drops the queries with lowest TTL value. So it is obvious that Hub positioned attackers can cause very little damage. While in contrast, if the attacker nodes are placed at Corner, it causes maximum damage and serves almost 75% legitimate queries. It is so because the TTL values of Corner based nodes are very high and "Drop Youngest" serves these queries on first preference. Hub Neighbor is next to Hub and serves 84% legitimate queries.

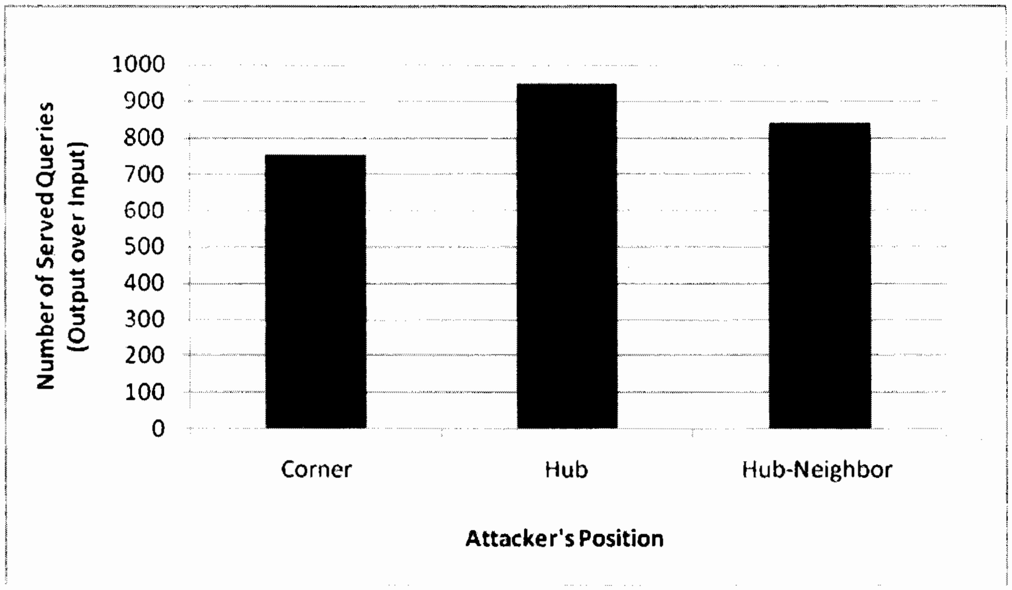

Figure 5.2: The number of legitimate queries served when strategy is Drop Youngest.

Case 3:

Legitimate Queries Served when First Come First Serve (FCFS) technique is used.

In this experiment, we have measured that how many legitimate queries are served when the strategy is default FCFS, and get the results as shown in fig.5.3. FCFS strategy drops the queries

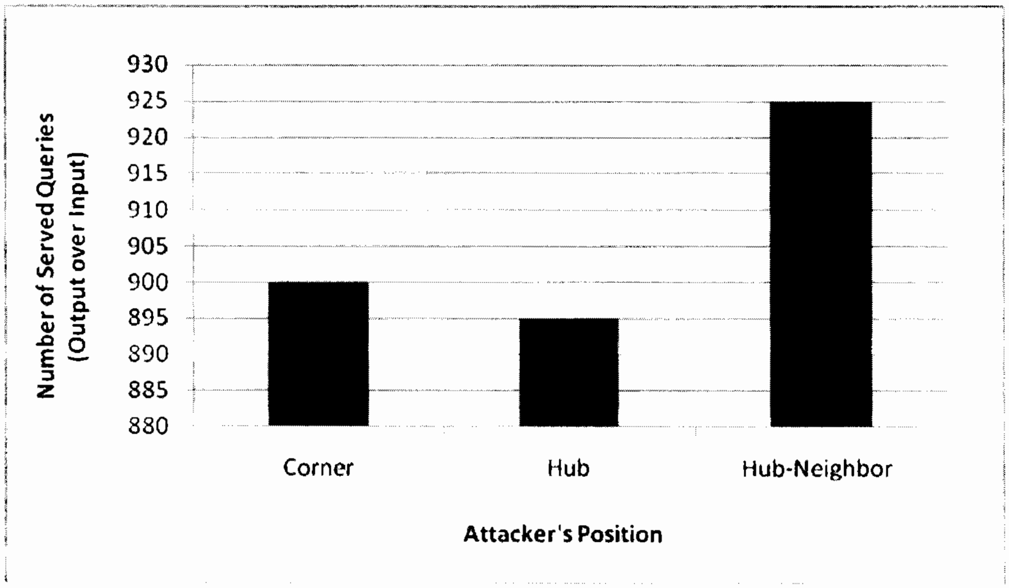

Figure 5.3: The number of legitimate queries served when strategy is FCFS.

blindly, i.e. without considering lower or higher TTL value of a query. It can be clearly seen that when the query drop strategy is FCFS, more legitimate queries are served by keeping attackers at Hub Neighbor position. While in contrast, if the attacker nodes are placed at Hub, it causes maximum damage and serves almost 89% legitimate queries. Corner based nodes serves 92% legitimate queries.

Case 4:

Illegitimate Queries Served with Attack Corner position.

In this experiment, we have measured how many illegitimate queries are served by using various strategies, when malicious node(s) is located at Corner of the network, and get the results as shown in fig.5.4. It can be clearly seen that when the query drop strategy is "Drop Youngest", more 26% illegitimate queries are served by keeping attackers at the Corners. Since attacker is at the Corner, so attacker's queries do always have higher TTL value and drop youngest strategy drops the queries with lower TTL value. So it is obvious that malicious queries generated by Corner positioned attackers would be quickly picked up by the receiver node. While in contrast, when the query drop strategy is "Drop Oldest", it results minimum 8% illegitimate queries to be served. It is so because the TTL values of Corner based nodes are very high and "Drop Oldest" reject these queries. When the query drop strategy is "FCFS", it serves 13% illegitimate queries.

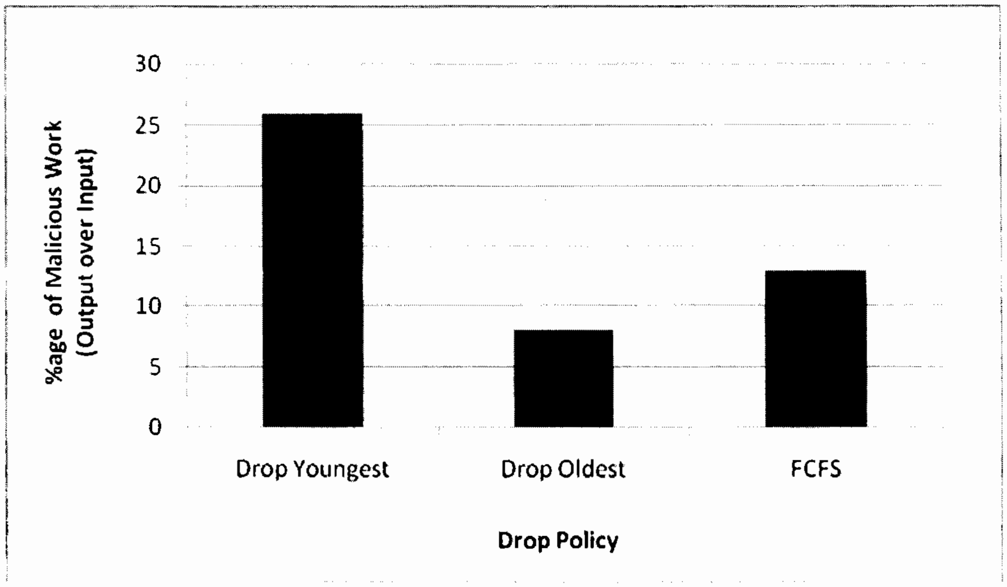

Figure 5.4: The number of illegitimate queries served when malicious node is at Corner.

Case 5:

Illegitimate Queries Served with Attack Hub position.

In this experiment, we have measured how many illegitimate queries are served by various strategies, when malicious node(s) is placed at Hub, and get the results as shown in the fig.5.5.

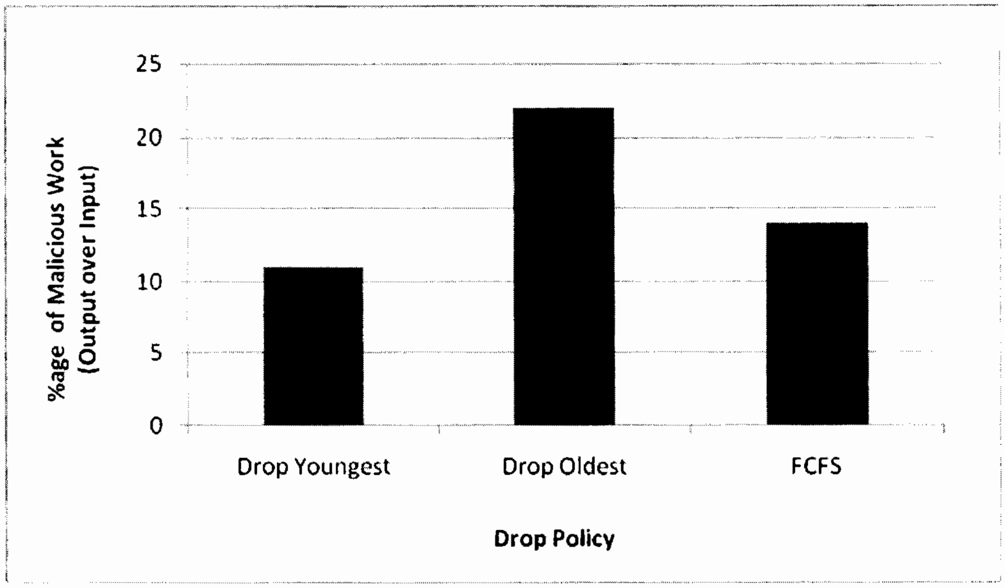

Figure 5.5: The number of illegitimate queries served when malicious node is at Hub.

It can be clearly seen that when the query drop strategy is "Drop Oldest", more 22% illegitimate queries are served by keeping attackers at Hub. Since attacker is at the Hub, so attacker's queries do always have lowest TTL value and drop oldest strategy drops the queries with higher TTL value. So it is obvious that malicious queries generated by Hub positioned attackers would be quickly picked up by the receiver node. While in contrast, when the query drop strategy is "Drop Youngest", it results minimum 11% illegitimate queries to be served. It is so because the TTL value of Hub based nodes are very low and drop youngest reject these queries. When the query drop strategy is "FCFS", it serves 14% illegitimate queries. So when the position is "Attack Hub", query drop strategy "Drop Oldest" is the best choice.

Case 6:

Illegitimate Queries Served with Attack Hub Neighbor position.

In this experiment, we have measured how many illegitimate queries are served by various strategies, when malicious node(s) is located at Hub Neighbor, and get the results as shown in the fig.5.6. It can be clearly seen that when the query drop strategy is "Drop Oldest", more 20% illegitimate queries are served by keeping attackers at the Hub Neighbor. Since attacker is at the Hub Neighbor, so attacker's queries do always have lower TTL value and drop oldest strategy drops the queries with higher TTL value. So it is obvious that malicious queries generated by the Hub Neighbor positioned attackers would be quickly picked up by the receiver. While in contrast, when the query drop strategy is "Drop Youngest", it results minimum 13% illegitimate queries to be served. It is so because the Age values of hub neighbor based nodes which are very low, and "Drop Youngest" reject these queries. When the query drop strategy is "FCFS", it serves 15% illegitimate queries.

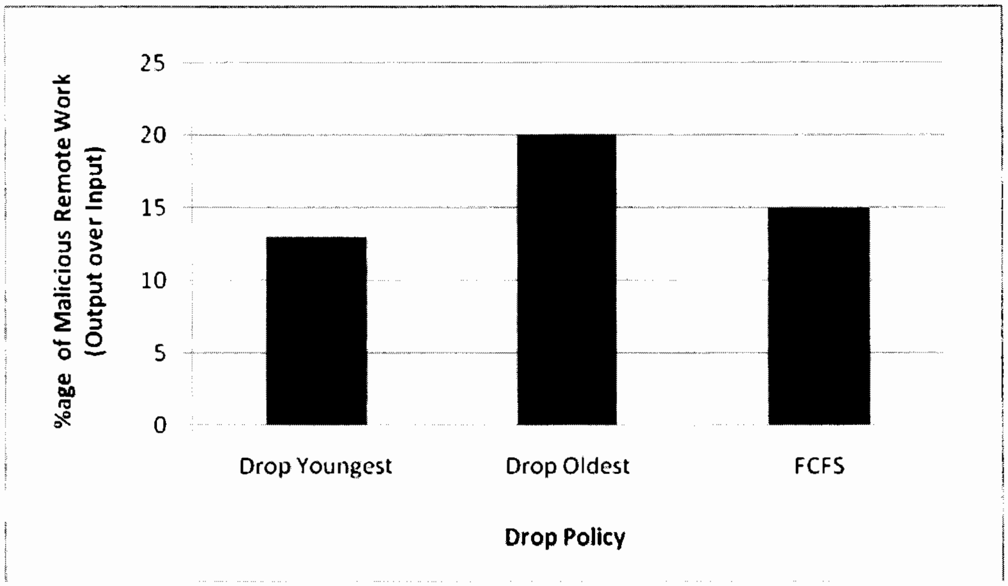

Figure 5.6: The number of illegitimate queries served when malicious node is at Hub Neighbor.

Case 7:

Legitimate and Illegitimate Queries Served with Attack Corner.

In this experiment, we have measured and compared how many legitimate and illegitimate queries are served when the malicious node is at the corner of the network, and get the results as shown in fig. 5.7.

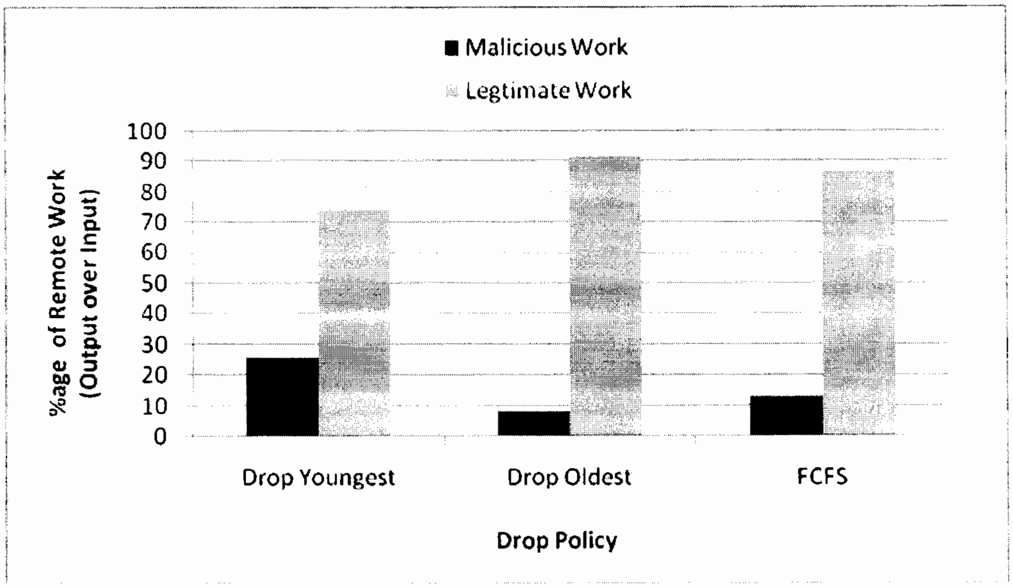

Figure 5.7: The number of legitimate and illegitimate queries served when malicious node is at Corner.

In this graph, we summarized Legitimate and Malicious remote work under the proposed two drop and one default strategies by keeping attack nodes at corners. We saw that when the drop policy was "Drop Youngest", 26% malicious remote work is reported that reduces the legitimate remote work to 74% only. In "Drop Oldest", these figures are much improved and malicious remote work is reduced to 8% only and legitimate remote work goes upwards by touching the figure of 92%. In "FCFS", 13% malicious work is noticed which leaves the legitimate work to 87%. So when attacker is at corner, "Drop Oldest" is the best strategy to be deployed.

Case 8:

Legitimate and Illegitimate Queries Served with Attack Hub.

In this experiment, we have measured and compared how many legitimate and illegitimate queries fig. 5.8.

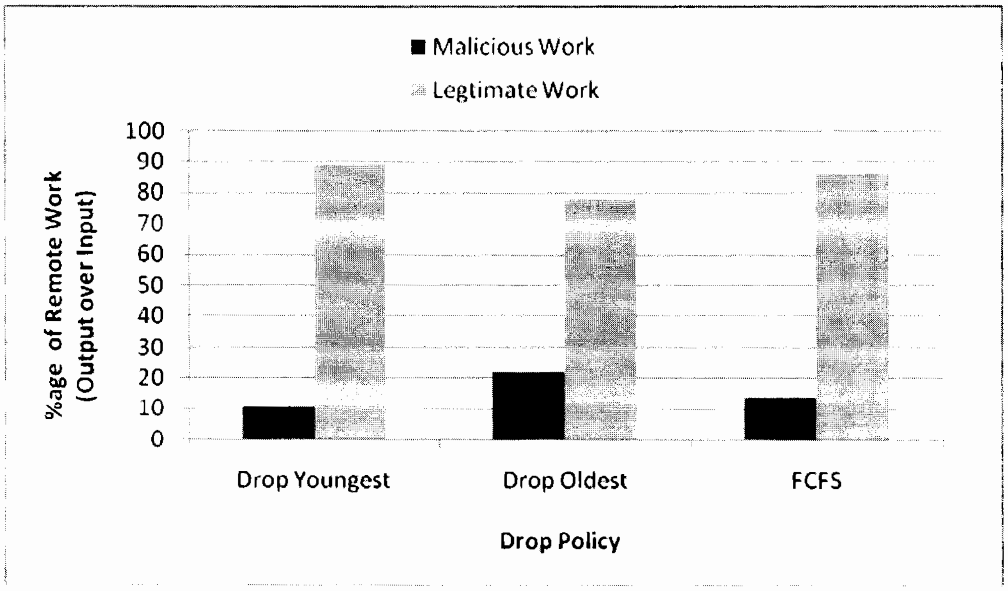

Figure 5.8: The number of legitimate and illegitimate queries served when malicious node is at Hub.

In this graph, we summarized Legitimate and Malicious remote work under the proposed two drop and one default strategies by keeping attack nodes at hub. We saw that when the drop policy was "Drop Youngest", 13% malicious remote work is reported that reduces the legitimate remote work to 87% only. In "Drop Oldest", these figures are much decreased and malicious remote work is increased up to 20% and legitimate remote work goes downwards by touching the figure of 80%. In "FCFS", 15% malicious work is noticed which leaves the legitimate work to 85%. So when attacker is at hub, "Drop Youngest" is the best strategy to be deployed.

Case 9:

Legitimate and Illegitimate Queries Served with Attack Hub Neighbor.

In this experiment, we have measured and compared how many legitimate and illegitimate queries are served when the malicious node is at the hub neighbor of the network, and get the results as shown in fig. 5.9.

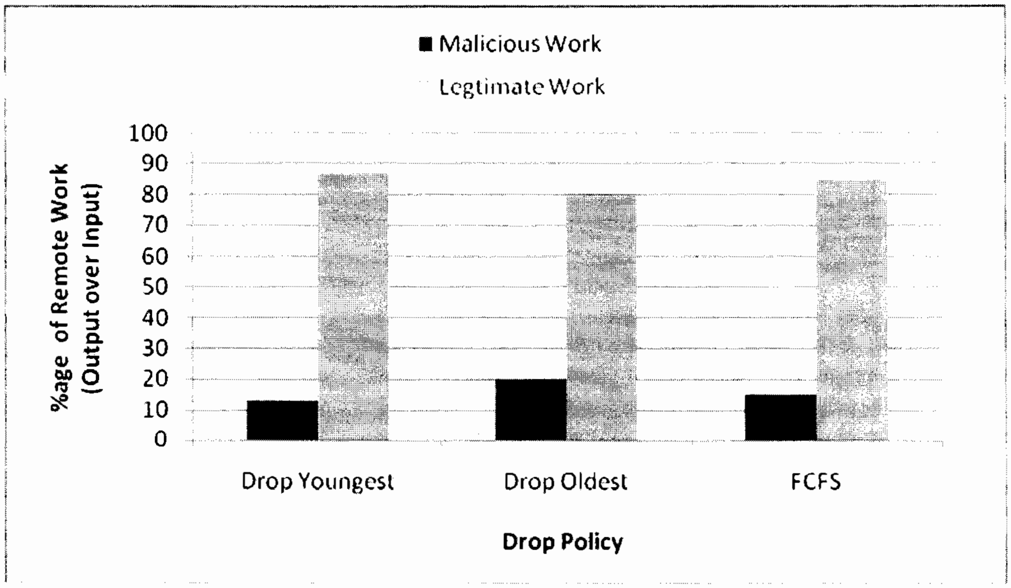

Figure 5.9: The number of legitimate and illegitimate queries served when malicious node is at Hub Neighbor.

In this graph, we summarized Legitimate and Malicious remote work under the proposed two drop and one default strategies by keeping attack nodes at hub. We saw that when the drop policy was "Drop Youngest", 18% malicious remote work is reported that reduces the legitimate remote work to 82% only. In "Drop Oldest", these figures are much decreased and malicious remote work is increased up to 20% and legitimate remote work goes downwards by touching the figure of 80%. In "FCFS", 19% malicious work is noticed which leaves the legitimate work to 81%. So when attacker is at hub, "Drop Youngest" is the best strategy to be deployed.

Case 10:

Legitimate Queries Served with Multiple Attack Corners.

In this experiment, we have measured how many legitimate queries are served when numerous malicious nodes are present at the corners of the network topology, and get the results as shown in fig. 5.10.

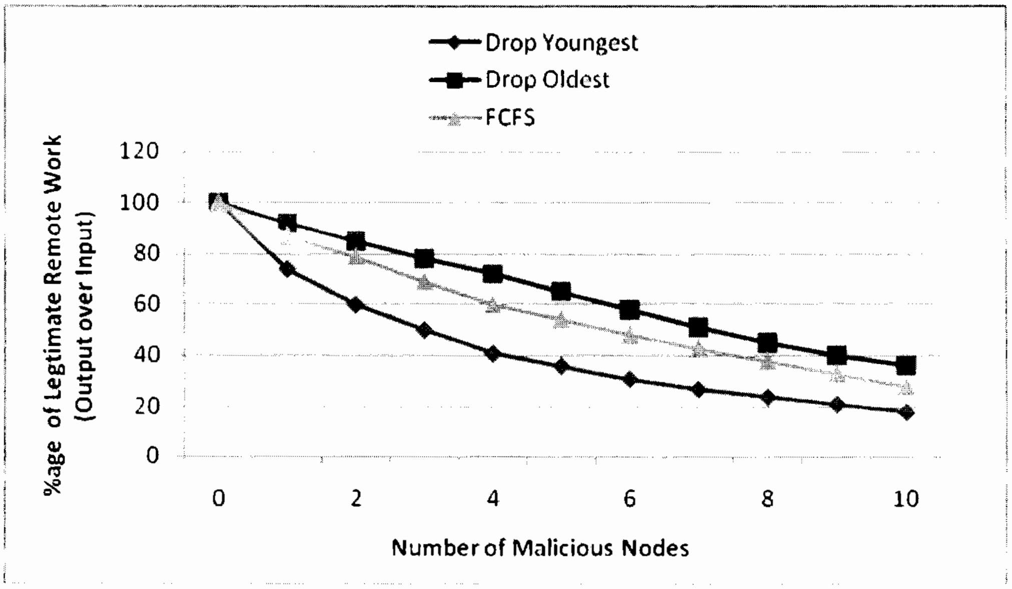

Figure 5.10: The number of legitimate queries served when multiple malicious nodes are at Corner.

In this graph, we summarized legitimate remote work under the proposed and default strategies by keeping multiple attack nodes at the corner. We saw that when the drop policy was "Drop Oldest", legitimate remote work decreased with the increase of malicious nodes. When there was no malicious node in the network, 100% legitimate remote work has been served, and when there were 10 malicious nodes available in the network, the percentage of legitimate remote work goes downwards by touching the figure of 28%. In "FCFS", these figures are much decreased from 100% to 30%. In "Drop Youngest", the legitimate work was much degraded from 100% to 18%. So when a group of attackers are at the corners of topology, "Drop Oldest" is the best strategy to perform legitimate work.

Case 11:

Illegitimate Queries Served with Multiple Attack Corners.

In this experiment, we have measured how many malicious queries are served when numerous malicious nodes are present at the corners of the network topology, and get the results as shown in fig. 5.11.

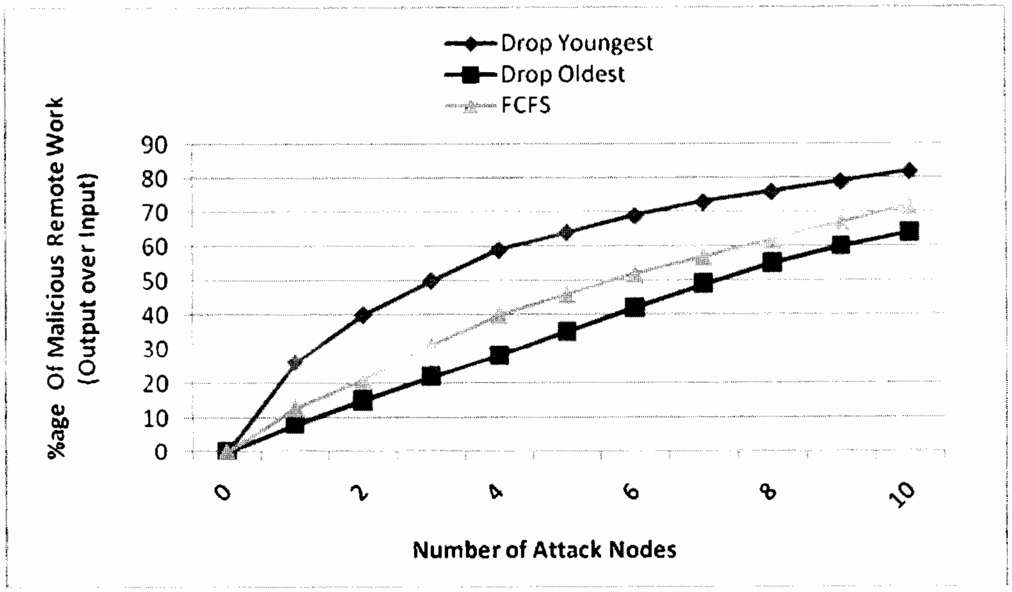

Figure 5.11: The number of illegitimate queries served when Multiple malicious nodes are at Corner.

In this graph, we summarized malicious remote work under the proposed and default strategies by keeping multiple attack nodes at the corner. Numbers of malicious nodes are representing themselves on x-axis, and y-axis is showing the amount of served malicious remote queries. We saw that when the drop policy was "Drop Youngest", malicious remote work increased with the increase of malicious nodes. When there was no malicious node in the network, 0% malicious remote work has been done, which means 100% legitimate remote work has been served, and when there were 10 malicious nodes available in the network, the percentage of malicious remote work goes upwards by touching the figure of 82%. In "FCFS", these figures are much decreased from 0% to 72%. In "Drop Oldest", the malicious work was much degraded from 0% to 64%. So when a group of attackers are at the corners of topology, "Drop Youngest" is the best strategy to perform malicious work.

Case 12:

Legitimate Queries Served with Multiple Attack Hubs.

In this experiment, we have measured how many legitimate queries are served when numerous malicious nodes are present at the hub and get the results as shown in fig. 5.12.

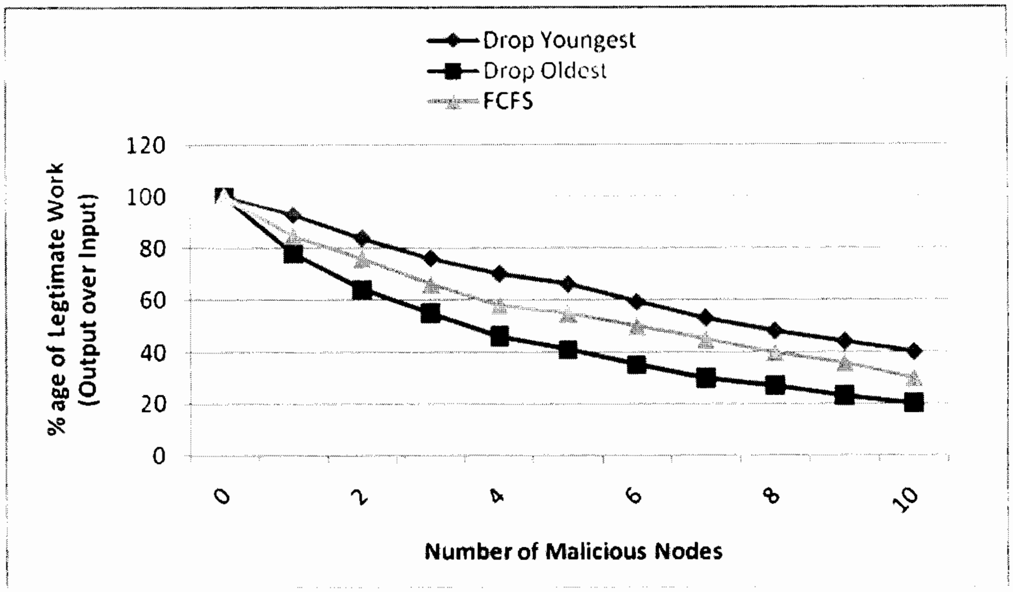

Figure 5.12: The number of legitimate queries served when multiple malicious nodes are at Hub.

In this graph, we summarized legitimate remote work under the proposed and default strategies by keeping multiple attack nodes at the hub. Numbers of malicious nodes are representing themselves on x-axis, and y-axis is showing the amount of served legitimate remote queries. We saw that when the drop policy was "Drop Youngest", legitimate remote work decreased with the increase of malicious nodes. When there was no malicious node in the network, 100% legitimate remote work has been served, and when there were 10 malicious nodes available in the network, the percentage of legitimate remote work goes downwards by touching the figure of 40%. In "FCFS", these figures are much decreased from 100% to 30%. In "Drop Oldest", the legitimate work was much degraded from 100% to 20%. So when a group of attackers are at the hubs of topology, "Drop Youngest" is the best strategy to perform legitimate work.

Case 13:

Illegitimate Queries Served with Multiple Attack Hubs.

In this experiment, we have measured how many malicious queries are served when numerous malicious nodes are present at the hub, and get the results as shown in fig. 5.13.

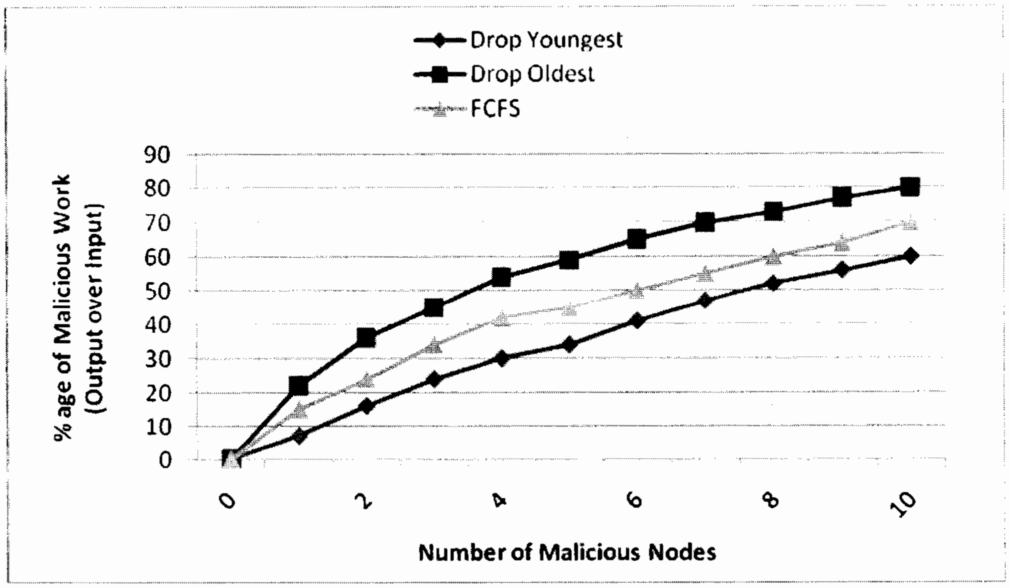

Figure 5.13: The number of illegitimate queries served when multiple malicious nodes are at Hub.

In this graph, we summarized malicious remote work under the proposed and default strategies by keeping multiple attack nodes at the hub. We saw that when the drop policy was "Drop Oldest", malicious remote work increased with the increase of malicious nodes. When there was no malicious node in the network, 0% malicious remote work has been done, which means 100% legitimate remote work has been served, and when there were 10 malicious nodes available in the network, the percentage of malicious remote work goes upwards by touching the figure of 80%. In "FCFS", these figures are much decreased from 0% to 70%. In "Drop Youngest", the malicious work was much degraded from 0% to 60%. So when a group of attackers are at the hubs of topology, "Drop Oldest" is the best strategy to perform malicious work.

Case 14:

Energy Consumption when Legitimate Queries Served with Multiple Attack Corners.

In this experiment, we have measured how much energy is consumed while serving the legitimate queries when numerous malicious nodes are present at the corners of the network topology, and get the results as shown in fig. 5.14.

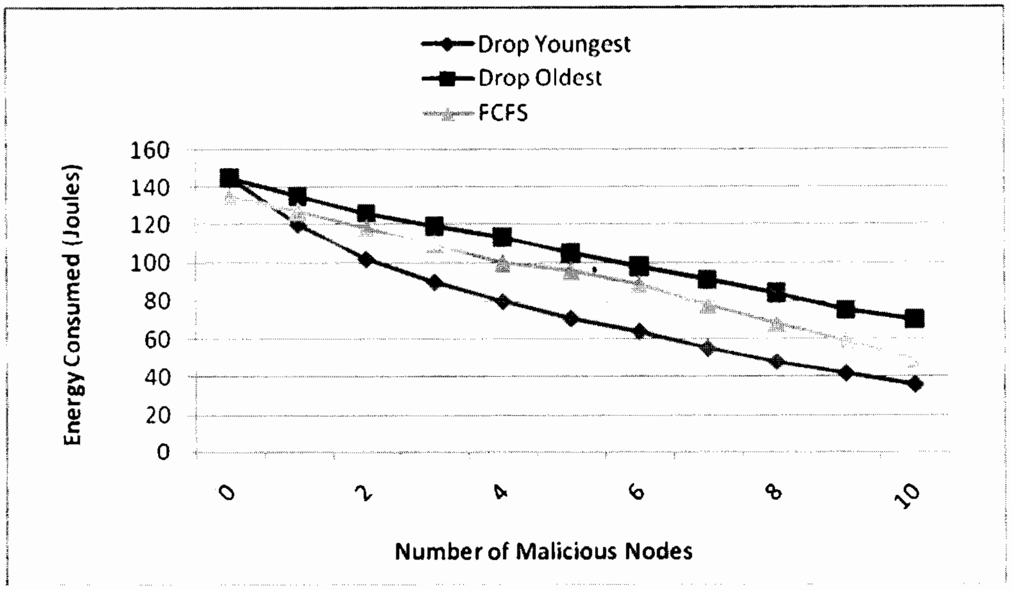

Figure 5.14: Energy consumed by legitimate queries served when multiple malicious nodes are at Corner.

In this graph, we saw how much level of energy consumption is required by legitimate work under the proposed and default strategies by keeping multiple attack nodes at the corner. We saw that when the drop policy was "Drop Oldest", whole energy was consumed to serve legitimate work, as there was no malicious node in the network. But the energy level started decreasing with the increase of malicious nodes, because the energy has been started to be consumed by the malicious queries. When there were 10 malicious nodes available in the network, the percentage of energy given to legitimate queries goes downwards by touching the figure of 05 mili joules. In "FCFS", these figures are much decreased from 135 to 49 mili joules. In "Drop Youngest", the energy consumption was much degraded from 145 to 36 mili joules. So when a group of attackers are at the corners of topology, "Drop Oldest" is the best strategy that consumes less energy to perform legitimate work.

Case 15:

Energy Consumption when Illegitimate Queries Served with Multiple Attack Corners.

In this experiment, we have measured how much energy is consumed while serving the malicious queries when numerous malicious nodes are present at the corners of the network topology, and get the results as shown in fig. 5.15.

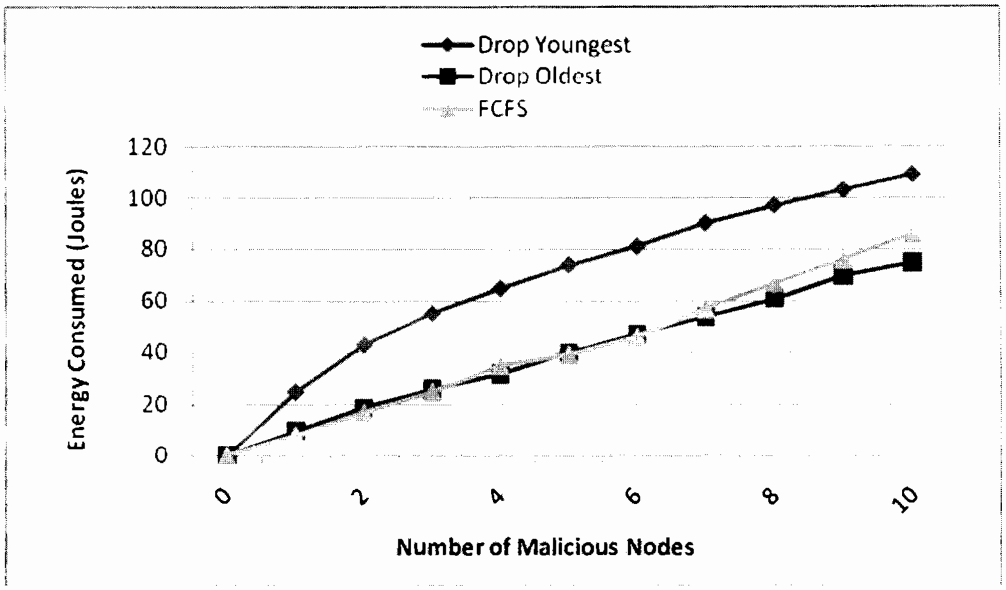

Figure 5.15: Energy consumed by illegitimate queries served when multiple malicious nodes are at Corner.

In this graph, we saw how much level of energy consumption is required by malicious work under the proposed and default strategies by keeping multiple attack nodes at the corner. We saw that when the drop policy was "Drop Youngest", the energy level started increasing with the increase of malicious nodes. When there were 10 malicious nodes available in the network, the percentage of energy given to malicious queries goes upwards by touching the figure of 109 mili joules. In "FCFS", these figures are decreased up to 86 mili joules. In "Drop Oldest", the energy consumption was much decreased till 75 mili joules. So when a group of attackers are at the corners of topology, "Drop Youngest" is the best strategy that consumes less energy to perform malicious work.

Case 16:

Energy Consumption when Legitimate Queries Served with Multiple Attack Hubs.

In this experiment, we have measured how much energy is consumed while serving the legitimate queries when numerous malicious nodes are present at the hubs of the network topology, and get the results as shown in fig. 5.16.

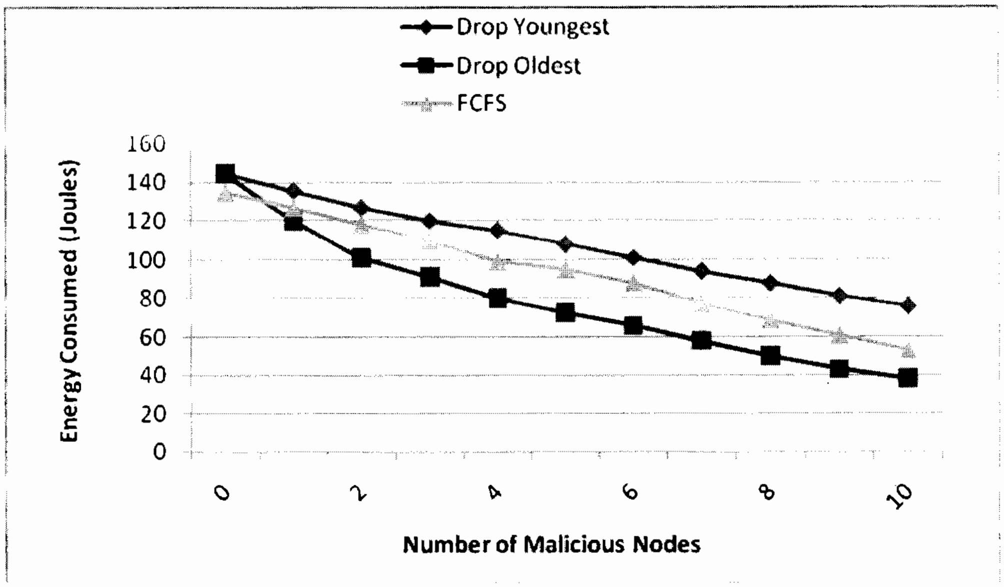

Figure 5.16: Energy consumed by legitimate queries served when multiple malicious nodes are at Hub.

In this graph, we saw how much level of energy consumption is required by legitimate work under the proposed three drop strategies by keeping multiple attack nodes at the hub. We saw that when the drop policy was "Drop Youngest", whole energy was consumed to serve legitimate work, as there was no malicious node in the network. But the energy level started decreasing with the increase of malicious nodes, because the energy has been started to be consumed by the malicious queries. When there were 10 malicious nodes available in the network, the percentage of energy given to legitimate queries goes downwards by touching the figure of 76 mili joules. In "FCFS", these figures are much decreased from 135 to 53 mili joules. In "Drop Oldest", the energy consumption was much degraded from 145 to 38 mili joules. So when a group of attackers are at the hubs of topology, "Drop Youngest" is the best strategy that consumes less energy to perform legitimate work.

Case 17:

Energy Consumption when Illegitimate Queries Served with Multiple Attack Hubs.

In this experiment, we have measured how much energy is consumed while serving the malicious queries when numerous malicious nodes are present at the hubs of the network topology, and get the results as shown in fig. 5. 17.

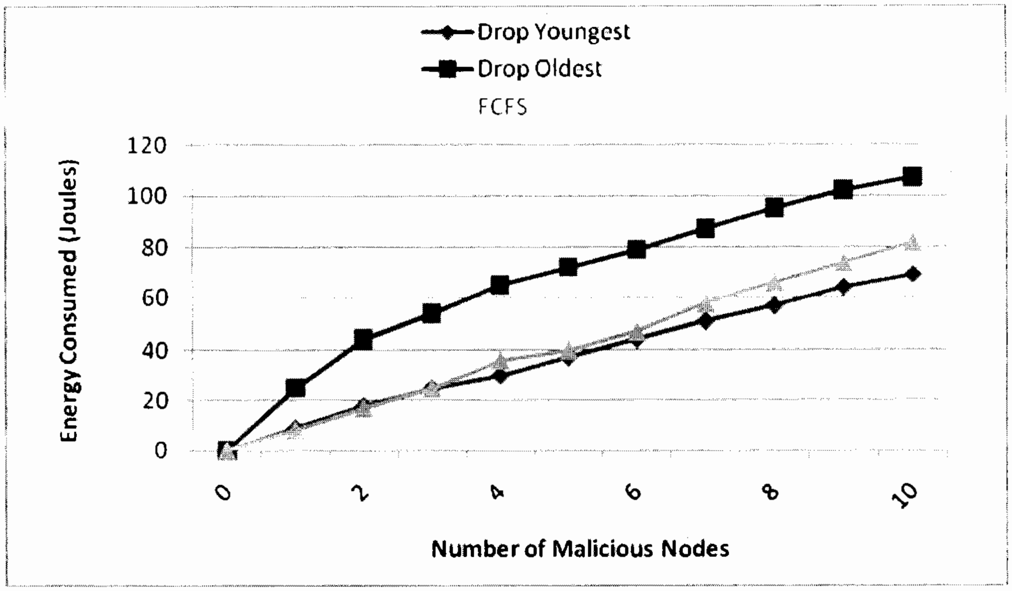

Figure 5.17: Energy consumed by illegitimate queries served when multiple malicious nodes are at Hub.

In this graph, we saw how much level of energy consumption is required by malicious work under the proposed and drop strategies by keeping multiple attack nodes at the hub. We saw that when the drop policy was "Drop Oldest", the energy level started increasing with the increase of malicious nodes. When there were 10 malicious nodes available in the network, the percentage of energy given to malicious queries goes upwards by touching the figure of 107 mili joules. In "FCFS", these figures are decreased up to 82 mili joules. In "Drop Youngest", the energy consumption was much decreased till 69 mili joules. So when a group of attackers are at the hubs of topology, "Drop Oldest" is the best strategy that consumes less energy to perform malicious work.

5.3 Chapter Summary

In this chapter, we have analyzed the detailed discussions regarding to the performance of all the Query rejection strategies by implementing all of them in NS-2. There performance evaluation has been shown by graphs created, using various parameters against which each of the strategy and attacker placement is tested and evaluated. Also, we have compare our proposed solutions with the default existing strategy.

6. Conclusions and Future Work

6. Conclusions and Future Work

After a detailed account on requirements analysis, proposed solution and methodology, implementation and results, we have come to the conclusion of our dissertation. It leads us to decide what work can be chosen for future enhancements.

6.1 Conclusion

Ad Hoc networks are widely accepted nowadays. Day by day, the graph of popularity of MANETs is growing up higher and higher. With growing fame, MANETs are also vulnerable to threats and attacks. The flooding algorithms are also gaining popularity along with Ad Hoc networks. As the flooding techniques are capable of providing high QoS in MANETs, thus such broadcasting techniques cannot be ignored, and hence become a major part of MANETS.

Accepting the fact that the flooding techniques are useful and advantageous for efficient performance of a network, these broadcasting techniques also have some drawbacks as well. Flooding can bring disastrous effects in the network, along with them. As flooding is a form of application layer Denial of Service (DoS) attack, so MANETs are susceptible to open attacks and challenges. The attacks could be launched against the availability, file authenticity, anonymity, access control, etc. of a network. As a result, a node can be corrupted, as well as the whole network is imposed to be shutdown.

Amongst the disputes currently facing by MANETs, security is the top most issue to be resolved on first priority. The best possible security defense is a guarantee of a network with high QoS. Various security measures are designed to detect an attack in a network, prevent an attack, contain an attack by minimizing its effects, and recover the network from an attack.

In our dissertation, we focus on improving the efficiency, performance, reliability, and QoS of a network. For this purpose, we set and define our research goal in chapter 3. And we excel to achieve our objectives in chapter 4 by designing various Query Rejection Techniques and studied service degradations from a victim node's point of view, by assuming the attacker's location is known and hence the victim node is protecting itself by assuming threats. Reduction in quality of a network is a result of an attack. And the location of a malicious node in a network implies that the network is not in the safe mode, and is unsecure. Also, the impact of an attack varies with the placement of victim and attacker nodes.

In our dissertation, chapter 5 contains the simulated results which we have appraised by using Network Simulator-2 (NS-2). The evaluated conclusion has enabled us to determine which query drop mechanism will be suitable for which specific scenario.

6.2 Future Work

Creative ideas and works are not restricted to any boundary. As the technologies and techniques are evolving day by day, thus enhancement in current system's environments becomes necessary for their survival. Improving and updating the systems that keeps them alive.

MANET is an emerging category of wireless network. It is a new field as compared to other wired networks, so a lot of work is needed to be discovered and done by the researchers. Flooding algorithms have been already studied by many researchers in wired networks, but in wireless networks, currently it has become the source of attraction.

A fact behind researcher's attention on flooding (DoS) attacks in wireless networks is MANETs demands for high alert security. We have tried to highlight security issues in MANETs and propose solutions according to it. Yet, there exist many issues in security areas which are still undiscovered and need to be highlighted. And too much work is still left to be done by the upcoming future researchers.

In query drop strategies, we have developed different strategies to describe a situation when the network will get efficient results. But it is not discussed that how we can distinguish between urgent and unimportant queries. Priority can be added along with certain queries. So future work can be done in how dropping useless, non urgent and unimportant queries, the network can safe its cost in terms of battery powers of wireless nodes. Moreover, Forwardable and answerable queries can be distinguished. A node can decide that how much quantity of bandwidth must be utilized for answerable or forwardable queries. New attack models can be designed to address more complex scenarios, with different placements of victim and attacker nodes.

References

[1] Mayank Bawa, Brian F. Cooper, Arturo Crespo, Neil Daswani, Prasanna Ganesan, Hector Garcia-Molina, Sepandar Kamvar, Serigo Marti, Mario Schlosser, Qi Sun, Patrick Vinograd, Beverly Yang, "Peer-to-Peer Research at Stanford", ACM SIGMOD Record, http://www-db.stanford.edu/~bawa/./Pub/stanford.ps

[2] Neil Daswani, Hector Garcia-Molina, "Blasting in Chord", Stanford CS Technical Report, January 2005.

[3] Neil Daswani, Hector Garcia-Molina, "Query-Flood DoS Attacks in Gnutella", ACM Conference on Computer and Communication Security, Washington, DC, November 2002.

[4] Neil Daswani, Hector Garcia-Molina, "Pong-Cache Poisoning in GUESS", ACM Conference on Computer and Communications Security, Washington, DC, October 2004.

[5] Qixiang Sun, Neil Daswani, Hector Garcia-Molina, "Maximizing Remote Work in Flooding-based Peer-to-Peer Systems", Journal of Computer Networks, Elsevier, Science Direct Publishers, 2006, 17th International Symposium on Distributed Computing (DISC), October 2003, Sorrento, Italy.

[6] Neil Daswani, Hector Garcia-Molina, Beverly Yang, "Open Problems in Data-Sharing Peer-to-Peer Systems", Database Theory-ICDT 2003, 9th International Conference of Database Theory, Siena, Italy, January 8-10, 2003, Proceedings, Volume 2572 of Lecture Notes in Computer Science. Springer, 2002.

[7] Brad Williams, Tracy Camp, "Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks", ACM MOBIHOC, 15 March 2002.

[8] Chi-Kin Chau, Jon Crowcroft, Kang-Won Lee, Starsky H.Y. Wong, “Inter-Domain Routing for Mobile Ad Hoc Networks”, 2008.

[9] Sasu Tarkoma, Dirk Trossen, Mikko Särelä, “Black Boxes: Making Ends Meet in Data Driven Networking”, 2008.

[10] Björn Scheuermann, Matthias Transier, Christian Lochert, Martin Mauve, Wolfgang Effelsberg, “Backpressure Multicast Congestion Control in Mobile Ad-Hoc Networks”, 2008.

[11] Rüdiger Schollmeier, Ingo Gruber, Michael Finkenzeller, “Routing in Mobile Ad Hoc and Peer-to-Peer Networks: A Comparison”, 2002.

[12] Robert Castañeda, Samir R. Das, Mahesh K. Marina, “Query Localization Techniques for On-Demand Routing Protocols in Ad Hoc Networks”, 2004.

[13] Mohamed Abdelhafez, “Modeling and Simulations of Worms and Mitigating Techniques”, 2007.

[14] Bo-Chao Cheng, Huan Chen and Ryh-Yuh Tseng, “A Good IDS Response Protocol of MANET Containment Strategies” IEICE Transactions on Communications, 2008.

[15] Min Shen, Dongmei Zhao, ‘Throughput Analysis of IEEE 802.11 and IEEE 802.11e MAC”, ACM, The Third International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks, August 7-9 2006, Waterloo, ON, Canada.

[16] S-Y. Ni, Y-C Tseng, Y-S Chen and J-P Sheu, “The broadcast storm problem in mobile ad hoc networks”, Proc. ACM MobiCom’99, Seatle, USA, Aug. 1999.

[17] Joon Yoo, Hong-ryeol Gil, Chong-kwon Kim, “INK: Implicit Neighbor Knowledge Routing in Ad Hoc Networks”, IEEE 2003.

[18] Sudipto Das, “Security Issues in Mobile Ad Hoc Networks”, 2006.

[19] Gokhan Korkmaz, Eylem Ekici, “Urban MultiHop Broadcast Protocol for InterVehicle Communication Systems”, ACM VANET’04, October1, 2004, Philadelphia, Pennsylvania.

[20] Dragos, Niculescu and Badri Nath, “Trajectory Based Forwarding and Its Applications”, ACM MobiCom’03, September 14–19, 2003, San Diego, California, USA.

[21] Timo Kosch, Christian J. Adler, Stephan Eichler, Christoph Schroth, Markus Strassberger, “the scalability problem of vehicular ad hoc networks and how to solve it”, IEEE Wireless Communications, October 2006.

[22] Radha Poovendran, “Information Assurance in MANET and Sensor Networks”, University of Washington. 2005.

[23] Yihong Zhou, dapeng Wu, Scott M. Nettles, “On MAC-layer denial of service attacks in lEEE 802.11 ad hoc networks: analysis and counter measures”, International Journal of Wireless and Mobile Computing, 2006.

[24] H. Wu et al., “Mddv: A Mobility-Centric Data Dissemination Algorithm for Vehicular Networks”, Proc.1st Int’l. Wksp.Vehic. Ad Hoc Networks (VANET), Oct. 2004, pp.47–56.

[25] Aniruddha Chandra, “Ontology for MANET Security Threats”, Electronics and Telecommunication Engineering Department Jadavpur University Kolkata 700032, India.

[26] Antonio Martin, Jeffrey Smith and Manfred Koethe, "A Platform Independent Model and threat Analysis for Mobile Ad hoc Networks", 2007

[27] Antonio Martin, "A Platform Independent Risk Analysis for Mobile Ad hoc networks", Boston University Conference on Information Assurance and Cyber Security, Dec 2006.

[28] Chakeres, et al. Internet-Draft on MANET Architecture October 2006. RFC 3753, June 2004. RFC 2461, December 1998. RFC 2501, January 1999.

[29] Sunsook Jung, Nisar Hundewale, Alex Zelikovsky, "Energy Efficiency of Load Balancing in MANET Routing Protocols", IEEE, 2005.

[30] Wikipedia, The biggest Encyclopedia, www.en.wikipedia.com