P-3519

IDENTIFICATION OF A SUITABLE COMMUNICATION SYSTEM FOR THE BATTLEFIELD MANAGEMENT SYSTEM

By

S.SATHIYAPRIYAH

Reg. No. 0920107020

of

KUMARAGURU COLLEGE OF TECHNOLOGY

(An Autonomous Institution affiliated to Anna University of Technology, Coimbatore)

COIMBATORE - 641049

A PROJECT REPORT

Submitted to the

FACULTY OF ELECTRONICS AND COMMUNICATION ENGINEERING

In partial fulfillment of the requirements
for the award of the degree
of
MASTER OF ENGINEERING
IN
COMMUNICATION SYSTEMS
APRIL 2011

BONAFIDE CERTIFICATE

Certified that this project report entitled "**A SUITABLE COMMUNICATION SYSTEM FOR THE BATTLEFIELD MANAGEMENT SYSTEM**" is the bonafide work of S.SATHIYAPRIYAH [Reg. no. 0920107020] who carried out the research under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other project or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

Project Guide

M.SHANTHI.,M.S

Head of the Department

Dr.RAJESWARI MARIAPPAN

The candidate with university Register no. 0920107020 is examined by us in the project viva-voce examination held on ..21.04.2011..

21|4|11

Internal Examiner

21|4|11

External Examiner

ACKNOWLEDGEMENT

First I would like to express my praise and gratitude to the Lord, who has showered his grace and blessing enabling me to complete this project in an excellent manner. He has made all things beautiful in his time.

I express my sincere thanks to our beloved Director **Dr.J.Shanmugam**, Kumaraguru College of Technology, I thank for his kind support and for providing necessary facilities to carry out the work.

I express my sincere thanks to our beloved Principal **Dr.S.Ramachandran**, Kumaraguru College of Technology , who encouraged me in each and every steps of the project work.

I would like to express my sincere thanks and deep sense of gratitude to our HOD, **Dr.Rajeswari Mariappan**, Department of Electronics and Communication Engineering, for her valuable suggestions and encouragement which paved way for the successful completion of the project work. I also thank her for her kind support and for providing necessary facilities to carry out the work.

In particular, I wish to thank and everlasting gratitude to the project coordinator **D.Mohanageetha(Ph.D).**, Associate Professor, Department of Electronics and Communication Engineering for her expert counseling and guidance to make this project to a great deal of success.

I am greatly privileged to express my deep sense of gratitude to my guide **M.Shanthi.,M.S** Associate Professor, Department of ECE, Kumaraguru College of Technology throughout the course of this project work and I wish to convey my deep sense of gratitude to all the teaching and non-teaching of ECE Department for their help and cooperation.

I am greatly thankful to express my deep sense of gratitude to respected **Mr.D.Ramanan,Technical officier** for giving me an opportunity to work at CVRDE, Avadi,Chennai.

I am greatly indebted to my external guides **Mr.S.Madivaanan, Sct.G., Assistant Director., IT Dept, CVRDE.** who boosted me to do this project work and for giving their excellent and valuable guidance and encouragement for successfully carrying out this training.

Finally, I thank my parents and my family members for giving me the moral support and abundant blessings in all of my activities and my dear friends who helped me to endure my difficult times with their unfailing support and warm wishes.

भाष / Phone : 044 - 26364031
x /फैक्स : 044 - 26383661
र/Grams : वहिकिलदेव /Vehicledev

भी पत्रदि निदेशक के पते से भेजे जाने चाहिए
और कोई अन्य अधिकारी के नाम से नहीं।
ll Correspondence should be
ddressed to DIRECTOR and not to
ny Officer by Name

ISO 9001 : 2000
CERTIFIED ESTT

भारत सरकार, रक्षा मंत्रालय
अनुसंधान तथा विकास संगठन
संग्राम वाहन अनुसंधान तथा विकास स्थापन
आवड़ी, चेन्नई - ६०० ०५४

Govt. of India, Min of Defence
Research & Dev. Orgn.
Combat Vehicles Res. & Dev. Estt.
Avadi, Chennai - 600 054

संख्या/Letter No. CV/IT/SM/SP

दिनांक / Date :28th March'11

CERTIFICATE

This is to certify that **S.SATHIYAPRIYAH, Reg No.0920107020** final year student of M.E. (Communication systems) from ***Kumaraguru College of Technology, Coimbatore*** have completed the Project work entitled **"Identification of a Suitable Communication System for a Battlefield Management System"** in our Establishment in partial fulfillment of the requirements for the award of **M.E. (COMMUNICATION SYSTEMS)** Degree. The Project has been designed, developed and tested successfully during the period from Aug 2010 to Mar 2011.

I wish them all success in their future endeavors.

(S.MADIVAANAN)
Scientist `G'
Additional Director

ABSTRACT

Combat operations has brought about the need for a large amount of data transfer. between command centers and the edge of the tactical communication network.This has necessitated the development of innovative MANET solutions catering to the reliability, security and scalability needs of the defense communications environment.

The Tactical networks are generally self forming and self healing in nature.They also have no fixed infrastructure and highly dynamic.Hence the communication technologies that are suitable for these networks are highly challengible and should be compatible with VHF/UHF range.In this project a suitable communication system for the battle field is proposed to overcome all these parameters. The project consists a reliable broadcasting protocol for a battle area.

The algorithm calculates the relative position of the nodes with respect to the broadcasting source node. The nodes that are farthest from the source node are scheduled to transmit first. If a node that is scheduled to transmit a message in a round realizes that its transmission cannot propagate the message to any new node, it will cancel its scheduled transmission. When compared with other broadcasting algorithms ,this algorithm would reduce routing load overhead and maximize packet delivery ratio, since the number of rebroadcasts made by the intermediate nodes is very less.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

MANET ------- **Mobile Adhoc Network**

TBA -------- **Tactical Battle Area**

PER -------- **Packet Error Rate**

RBCI -------- **Radio Based Combat Identification**

TDMA -------- **Time Division Multiple Access**

PRR -------- **Personal Role Radio**

DSSS -------- **Direct Sequence Spread Spectrum**

CNR -------- **Combat Net Radio**

N-LOS -------- **Non – Line Of Sight**

UHF/VHF -------- **Ultra High Frequency/Very High Frequency**

TOC -------- **Tactical Operation Center**

CHAPTER 1

INTRODUCTION

Combat operations has brought about the need for a large amount of data transfer between command centers and the edge of the tactical communication network.'This has necessitated the development of innovative MANET(MobileAdhoc Network) solutions catering to the reliability, security and scalability needs of the defense communications environment. The critical issues found in most of the battle areas are the delay, less packet delivery ratio and the network load. To overcome these challenges a reliable broadcasting protocol is implemented.

Overview of the project:

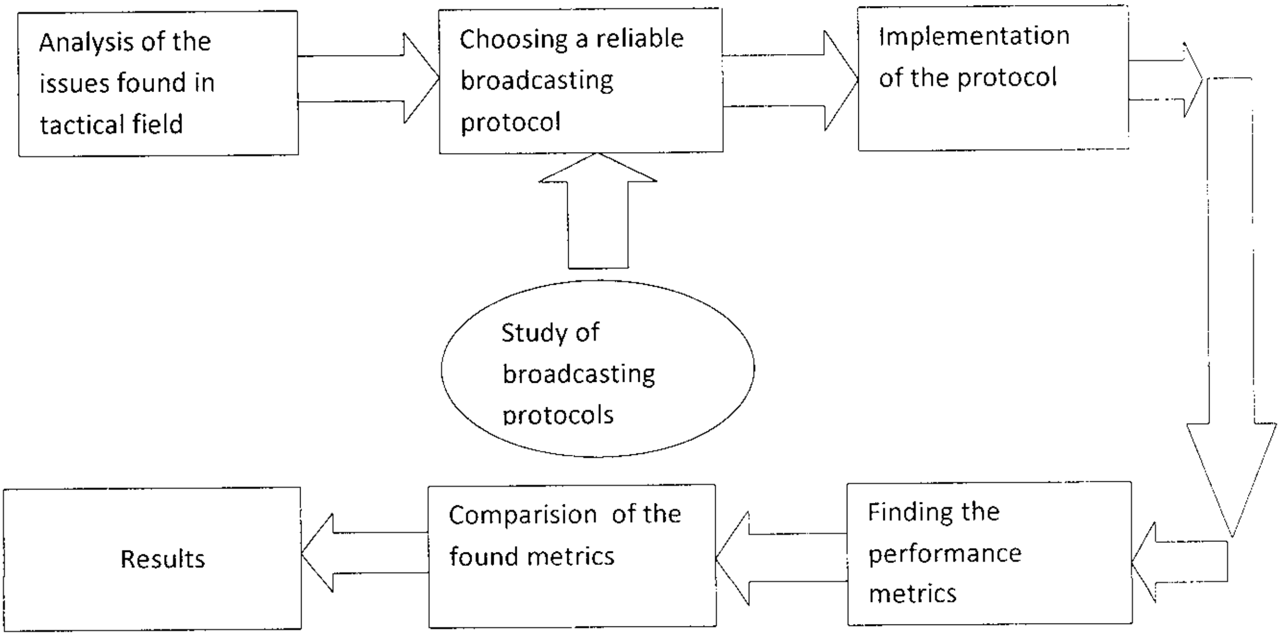


Figure 1.1: Block Diagram

The issues found in the tactical field are found to be less packet delivery ratio and network overload.The simple flooding and probability based broadcasting algorithms have been studied. To overcome the issues ,a reliable broadcasting protocol is implemented.

A new reliable broadcasting algorithm is implemented for tactical ad hoc networks. The nodes are mobile and can move from one place to another. On average, only a subset of nodes transmits and they transmit only once to achieve reliable broadcasting.

The algorithm calculates the relative position of the nodes with respect to the broadcasting source node. The nodes that are farthest from the source node are scheduled to transmit first. If a node that is scheduled to transmit a message in a round realizes that its transmission cannot propagate the message to any new node, it will cancel its scheduled transmission.

Two performance metrics, normalized routing load and packet delivery ratio are considered for evaluation. Normalized routing load is a ratio of number of routing packets transmitted by all the nodes for route maintenance and discovery and the number of data packets delivered to the destination nodes. Packet Delivery Ratio is the number of data packets received by the destination nodes divided by the number of data packets transmitted by the source nodes.

When compared with other broadcasting algorithms ,this algorithm would reduce routing load overhead and maximize packet delivery ratio, since only less number of control packets are sent to the destination and the number of rebroadcasts made by the intermediate nodes is very less respectively.

The Network simulator NS-2 is used to implement the reliable broadcasting protocol. The simulator supports simulation of protocols, routing, and broadcasting over wireless networks. When compared with other simulators, ns-2 would provide better accuracy, speed and ease of use. The performance measures are packet delivery ratio and the network load.

CHAPTER 2

MILITARY COMMUNICATIONS

2.1 INTRODUCTION:

Combat operations has brought about the need for a large amount of data transfer between command centers and the edge of the tactical communication network.'This has necessitated the development of innovative MANET(Mobile Adhoc Network) solutions catering to the reliability, security and scalability needs of the defense communications environment.' Today, MANETs enable war Figurehters to benefit from a sophisticated Internet protocol (IP)-based communications network that can be set up even in difficult terrain and in remote war zones.

Furthermore, tactical network applications of MANETs also include realization of automated battlefields, wherein autonomous robots and autonomous ground vehicles are used to explore hostile battlegrounds and check for land mines. These significant strides have made ad hoc networking a very valuable option in modern tactical military communication networks and the industry is facing significant demand for MANET solutions from defense establishments worldwide.

On the radio side, key enabling technologies for MANETs that are likely to have a strong impact include software-defined radios (SDR), cognitive radios (CR), and smart antenna techniques such as multiple input, multiple output (MIMO). Open air laser links are also likely to complement, and perhaps, eventually supplement, radio frequency (RF) links. In terms of networking, the fundamental Internet routing protocol and transmission control protocol/Internet protocol (TCP/IP) are known to be quite inadequate for MANET environments and are likely to be replaced by delay/disruption-tolerant networking (DTN) protocol. These enabling technologies are in various stages in the technology life cycle and each one is likely to have a different kind of potential impact on MANET solutions.

2.2 COMMUNICATION TRENDS IN TACTICAL BATTLE AREA(TBA):

Success on the battlefield depends to a large extent on the timely receipt of accurate information presented in a format that can be grasped readily by the commander and staff to allow them to prepare appropriate plans. This information then helps the commanders to by a feed back mechanism for the commanders to assess the effects of the previous action and plan the next phase. The speed of execution of OODA cycle is directly proportional to the strength of communication infrastructure both at tactical and strategic level. The communication elements therefore, must have matching mobility and the flexibility to support all plans of the commanders. Thus the receipt of sensor data, information processing and communication of orders, all require the provision of suitable Tactical Communication Systems providing high-speed data networks and voice communications. The range and capabilities of such systems must extend into the Tactical Battle Area (TBA) for providing the necessary decision support system to the commanders at all levels. Without the communications in the TBA on the modern battle field the commander is deaf, dumb and blind.

Tactical Battle Area (TBA):

In recently conducted, Operation Iraqi Freedom, V Corps of US Army led the main thrust into Iraq. V Corps was lead by Commanding General William S. Wallace. During most of the operations Commanding General Wallace was leading his troops from his mobile Assault Command Post. This mobile Command post moved along with his troops through the desert and up to Baghdad. Communications enabled him, as the first US commander in modern military history, lead the troops from the front. The V Corps used the comn network both for data and voice transmission. Application included e-mail, ftp, information systems, video conferencing and telephony. V corps also got access to the US Department of Defense's Non-secure Internet Protocol Router (NIPR) network and the Secure Internet Protocol Router (SIPR) network. SIPR-Net is the secure part of the Defense information systems Network and provides classified access to web based applications, bulk file transfers, e-mail and telnet. It also supports US Department of Defence's global command and control system, global combat support system, defence message system, collaborative planning tools, situational awareness applications, intelligence sharing databases and system for distributions of air tasking orders. NIPR Net is the US Department of Defence's unclassified network. All transmissions over the broadband communication network were encoded using KIVs, a US approved government encryption technology.

Salient Observations:

(b)Space Segment: Commercial space segment is dominating and can be used for military operations successfully.

(c)Equipment: Its usage at all operational levels lead to the need for mobility, ease of use and smaller sizes particularly in Highly Mobile Scenarios.

Hence it can be easily appreciated that as compared to the earlier times today there is a greater need to have all modes of communication available in TBA with special emphasis on mobility, small size, ease of use and greater bandwidth.

Users :-

(a) Corps.

(b) Division.

(c) Brigade.

(d) Battalion.

(e) Company/Squadron/Platoon.

(f) Recce Warriors.

Figure 2.1: Tactical Battle area

Need for comprehensive communication network and the challenges therein:

Establishment of a comprehensive communication network connecting all the above users is a very challenging and demanding task.

While the backbone can take advantage of commercial technologies, the maneuvering elements are facing many challenges that are not addressed by the commercial technology.

Comprehensive communication network for large scale defence force requires the use of many different technologies in all layers. With the success of the Internet Protocol (IP) in the commercial world and the availability of various COTS equipment and application it is the leading candidate to operate in this network. However, the environment in which defence forces operate is unique and poses many requirements and technical limitations which the commercial world is normally not required to deal with

The tactical networks are based on tactical radios (e.g. VHF, UHF and other media) and characterized by high mobility, non-stable and faulty communication. One of the major challenges in this layer is to handle the ad-hoc nature of the forces (expressed in geographical maneuvering and mobilization of forces between networks) without relaying on a single point of failure or a connection to other networks. The standard technologies in the commercial world are not designed to deal with such environment and thus in many cases a tailored solution is required. Moreover the suitability of commercial standards like IP in tactical networks is yet an open question.

The tactical networks are based on combat radios and may connect to each other and to the first and second tier networks via various utilities such as gateways, in the form of IP or application gateways. The major problem is how to connect the tactical forces to provide all-to-all communication services.

The ad-hoc nature of the tactical networks poses many harsh challenges both on the routing algorithms in the system and on the transport protocols.

Some of them are:-

(a) Dynamic movement of forces between networks on ad-hoc basis.

(b) Taking maximal advantage of network resources is critical. Thus, bandwidth expensive (c)The system must not relay on a single point of failure of one connection to other network or networks.

(d)High PER.(Packet Error Ratio)

(d)Unstable connectivity

2.3 OPERATIONAL REQUIREMENTS:

The operational requirements are not fixed yet. However, some assumptions may be identified based on the targeted users and their operations. The users are military forces in a potentially hostile jamming scenario. The number of radios in one network is normally between 10 and 30. Several adjacent networks (domains) should be able to interact efficiently. The most important services are PTP(Point to Point) voice and low rate data communication for position tracking and messaging. In addition, background data transfer should be supported.

The military users are expected to utilise one-to-one data and voice communications (unicast) as well as multicasting within one or more multicast groups. Pre-emption, enabling high priority traffic to suspend or terminate lower priority traffic, should be included. Single users or groups of users should be able to bring their terminals into radio silence. The network should be able to operate in all types of terrain environments. Interoperability with ships and airborne platforms is expected to be important.

The handling of mobility is therefore a prerequisite, possibly including both terminal mobility and user mobility. Seamless handover between networks is currently not an issue. It is assumed that the wireless system is able to transport IP-traffic. Further it is assumed that standard interfaces, for example Ethernet, Bluetooth or USB are supported, enabling connection of various end-user devices.

2.4 APPLICATONS AND SERVICES:

The main objective of this section is to identify typical services and their characteristics and requirements. There have been some efforts in NATO to define common architectural elements for terrestrial wireless systems.

An NC3A report presents the operational view for wireless communications in the land

Information exchange services:

i)Voice/Video:

Real-time, some resilience to errors, unpredictable traffic patterns, group communication dominate over one-to-one communications

ii)Position tracking:

Small, regular messages with some timerelevance. This may include situational awareness functional services for combat forces.

iii)Targeting:

Timeliness, authenticity, robustness

iv)Core services:

E-mail, photographs, maps etc. Higher data quantity, lower timeliness requirements.

v)Functional services

Functional services for non-combat forces. This may include database access or replication. Timeliness and data quantities will be dependent on the specific service being utilised. The range of services clearly imposes strict requirements on the quality-of-service (QoS) implementation. In addition to the above mentioned services, it is foreseen that radio based combat identification (RBCI) will be incorporated.

vi)Voice

It is expected that voice traffic is distributed as multicast within a group, resembling the broadcast nature the users are accustomed to. The enhanced mixed-excitation linear predictive (MELPe) vocoder [3] is the narrowband voice codec assumed utilised internally in the ad-hoc network.

It operates at bit rates of 600, 1200, and 2400 bit/s. At 2400 bit/s MELPe samples the voice signal at 8 kHz and splits the samples into frames of 180 samples, which are then analysed and compressed to 54 bits. Hence the encoder outputs one 54 bits frame every 22.5 ms. In addition the encoder uses a look ahead making the algorithmic delay 42.625 ms or 341 samples. Measurements of voice traffic during disaster scenarios indicate that call holding times are lognormally distributed with mean duration significantly longer than the expected duration of TDMA time slots, see for example [4]. The average duration of voice spurts is

vii) Position tracking, text messaging and chat

Friendly force tracking is expected to be the most important data service, in addition to text messaging/chat. This service type will require an efficient broadcast/multicast distribution mechanism. In some cases one might want full broadcast of this information, possibly requiring multihop multicasting.

2.5 RADIO SYSTEMS:

- **PRR:**
  - Vehicle integrated personal role radio
  - Selex communications, Europe.
  - Provides communication between troops and supporting vehicles.
  - 2 – 4 MHz.
  - 500 m range.
  - DSSS modulation: DSSS multiplies the data to be transmitted with a noise signal which is much higher in frequency than original signal, there by spreading the enery into much wider band.
  - Provides resistence to deliberate and unintentional jamming.
  - Allows to share a single channel among multiple users.

1)**H4855:**

- For intra squad communication.
- 2.4 GHz
- 50 Watts power.
- 500 m range.

2)**PRC343B:**

- Vehicle to vehicle range of 3.5 Km.
- 2.4 GHz
- Data transfer rate – 38.4 Kbps
- 50 watts power
- AES 128-bit Encryption

- **CNR-9000HDR**:
    - Elbit systems
    - VHF/FM Vehicular mounted high data rate radio
    - 115Kbps
    - 25 KHz
    - Uses orthogonal frequency hopping. (OFDM/Frequency hopping)
    - Supports streaming video footage
    - Provides reistance to electronic counter measures.

- **PRC/VRC 9661:**
    - Aselsan radio, Turkey.
    - 2 to 30 MHz(HF)
    - 30 to 512(V/UHF)
    - 10 Watt (V/UHF),50 Watt(V/UHF), 100 Watt HF

- **VRC90:**
    - China's National Electronic Import and Export
    - VHF/FM Vehicular set
    - 30 to 88 MHz
    - 16 Kbps of data.
    - 23 Kg Weight.

- **FLEXNET4:**
    - By Thales communications.
    - High data rate mobile adhoc networking.
    - 500Kbps to 6 Mbps.

- **TRC4000:**
    - 64 Kbps/34 Mbps internet traffic.
    - Secure line of sight radio.
    - Armed forces of Australia, France and united kingdom uses.

- **MV300:**
    - Kongsberg of Norway.
    - Frequency hopping
    - 19.2Kbps.
    - 45 KHz
    - 0.5 to 50 Watts.

- **RC340 HCDR:**
    - By ITT Communications
    - Backbone for the British army's BOWMAN system.
    - 500 Kbps data.
    - 225 to 450 MHz.

- **RF7800B:**
    - By Harris Communications.
    - High Volume data capacity.
    - Operating over L Band.
    - Beyond Line of sight Communication.

MAHATMA GANDHI KCT CBE-6 CENTRAL LIBRARY
P 3519

- **PRC2100V**:
    - 75 Watts power.
    - An Embedded GPS Receiver included.
    - Frequency Hopping
    - Digital data and voice Encryption

2.6 ISSUES IN TACTICAL NETWORK:

In Tactical networks, there are physical limitations to the band. Lower frequency bands of higher frequency are able to carry more data. Trade-offs are made between the carrying capacity of the signals and its resiliency to attenuation. In addition to the problems of bandwidth, other issues of security, reliability, and networking overhead exist, complicating matters further.

In tactical situations, in particular, tracked vehicles are always under constraints for an efficient communication system unlike their civilian or commercial mobile radio system, where these do not have favourable environment or choice. Basically, military tactical radio communication systems suffer due to the following reasons:

a) Base station is always temporary and is required to move at a short notice and replay, which may not have favourable high exposed ground clearly necessitating non line-of-sight [NLOS] conditions working.

b) Quality of transmission/reception and equipment reliability are of paramount importance to the soldiers.

c) Modulation scheme should be user-friendly so that minimum noise, maximum usability with utmost protections for jamming sources and speech privacy are achieved. This is always a trade-off with respect to performance. Also, the tactical situation is highly dynamic and real scenario plays an important role with respect to screening effect, fading and atmospheric attenuation of radio signals, especially in HF radio sets.

At present the tactical network utilizes the VHF range (30MHz-88MHz) for voice and data communication over network.

2.7 EMERGING TRENDS TO COUNTER CHALLENGES:

The military establishment is currently transforming itself to fully benefit from advanced information networking technology. In the past two decades fundamental changes were introduced to the military infrastructure; new information systems were implemented, improving availability and management of information.

But the flow of information normally fails severely, as soon as forces start moving. Technical restrictions limited the integration of mobile systems to information "Islands". Without effective command and control systems, combat units had to be operated "the old way", relying on slow and unreliable voice communication, vulnerable relay stations, hand

Combat experience indicates that valuable information is generated at battalion level - battlefield intelligence, friendly forces status and location etc. A dangerous "fog of war" results when real-time data is not fed quickly enough through the command system, to update the "situational picture" at the higher echelons. These conditions are most susceptible to fratricide. Fortunately modern multimedia communications systems are now filing this gap with advanced, automated command and control capabilities which transform the military forces into more effective, cohesive, efficient and synchronized network-centric system.

Military Wireless Data Networks:

High speed wireless data networks are integrating communications between different command levels down to the divisions and brigades. To enable modern image-rich multimedia connectivity, substantial infrastructure enhancement is required, primarily in the introduction of computing and high-speed networking at the lower echelons, with the deployment of high speed, wireless data-communications backbone spanning throughout the theater of operation.

Such extensions can now reach battalions, with deployed line-of-sight terminals providing high-speed links. Data communications is required for all facets of military activities, including transfer of reports.

Tactical Mobile Broadband Networks:

To support the brigade level and above, these services rely on dedicated trunks for broadband connectivity. Such radios offer wireless connectivity at rates from 1 MB to 16 MB. Where transfer of images or video is required, higher data rates become imperative, links are being implemented with modern high speed digital networks. These services are provided by modern commercial networking systems, derived from commercial Wireless Local Area Networks (WLAN), cellular networks or broadband satellite links. Advanced, secured SDH connections provide an ultra-wideband channel for up to 155mbps. Such broadband satellite links and fiber-optics are widely used to link stationary or fixed command posts with terrestrial networks, but high-speed connectivity of mobile elements is still restricted.

Tactical Satellite Communications Networks:

With flexible operational services and compact ground terminals, Satellite Communications (SATCOM) services offer attractive solutions for military users in theater and on global links. Dedicated military satellite networks are augmented by commercial services, primarily Demand Assigned Multiple Access (DAMA) controlled networks that offer the user total control of the space link. When deployed in theater, SATCOM offers terrain independent communications, flexible networking and direct link to the final destinations – without reliance on radio relays.

Command and Control (C2) Systems for the Tactical Echelon:

Modern C4I systems are feeding huge amounts of information into the tactical operating center (TOC) where such information is processed, interpreted and displayed on maps and status reports. Such situational presentations are generated by computers, and displayed at the Command Posts (CP) on large screens or relayed to remote subscribers, via high speed networks. Unfortunately, such connectivity is not provided with existing tactical radios. Therefore, tactical commanders are usually disconnected form these vital information feeds when leaving the TOC to deploy with their command vehicles.

Dismounted & Mobile Command and Control (C2) Systems:

Command and Control On the Move (C2OTM) applications enable commanders to receive data-intensive information via satellite-down linked feeds, on the move. Utilizing new generation satellite antennae, designed for mobile platforms, C2OTM introduces tactical commanders with new capabilities to deploy their command elements to the most critical points, without loosing contact with their tactical operations center (TOC). Initial C2OTM elements were already deployed in Iraq at the beginning of Operation Iraqi Freedom and more systems and variants are expected to be fielded in near future.

Mounted Battle Command On The Move (MBCOTM):

MBCOTM is another new concept enabling the commander to perform all command and control tasks while on the move. Although Command Vehicles which can operate independent of command posts(CPs) are well established in many armies, until recently these elements were not equipped with mobile data communications and therefore, could not fully modern C4I services. These systems are currently designed as "commander centric" maneuver, effects, intelligence, mobility, counter-mobility and survivability, NBC and air defence. Other tasks include monitoring and execution of fire support plans, tasking and re-tasking organisation etc.

Tactical Communication System (TCS):

The Indian Army too has adequately conceptualized the comn framework for the TBA and the systems are being inducted through TCS, CNR and satellite network program. Info systems for TBA, in the form of software applications, are also progressing in parallel through various Tactical C3I programs.

Though TCS covers all aspects of modern communication needs for TBA still, we need to consider catering for aerial communication nodes. These nodes though are going to be costly to handle but, will provide us with much needed mobility, flexibility in deployment and extended ranges in the critical hour of need. A Signals Aviation Unit comprising of Aircrafts, Helicopters and UAVs at theatre level, capable of supporting communication and EW needs of modern battle field within that theatre may be given a considerate thought. Western countries are working on this and in fact some are in advance stages of their trials.

CHAPTER 3

MANET

3.1 HISTORY:

The whole life-cycle of ad-hoc networks could be categorized into the first, second, and the third generation ad-hoc networks systems. Present ad-hoc networks systems are considered the third generation. The first generation goes back to 1972. At that time, they were called PRNET (Packet Radio Networks). The history of ad-hoc networks can be dated back to the DoD1-sponsored Packet Radio Network (PRNET) research for military purpose in 1970s, which evolved into the Survivable Adaptive Radio Networks (SURAN) program in the early 1980s [1]. In conjunction with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access), approaches for medium access control and a kind of distance-vector routing PRNET were used on a trial basis to provide different networking capabilities in a combat environment.

The second generation of ad-hoc networks emerged in 1980s, when the ad-hoc network systems were further enhanced and implemented as a part of the SURAN (Survivable Adaptive Radio Networks) program. This provided a packet-switched network to the mobile battlefield in an environment without infrastructure. This program proved to be beneficial in improving the radios' performance by making them smaller, cheaper, and resilient to electronic attacks. In the 1990s, the concept of commercial ad-hoc networks arrived with notebook computers and other viable communications equipment. At the same time, the idea of a collection of mobile nodes was proposed at several research conferences. Since mid 1990s, a lot of work has been done on the ad hoc standards.

Within the IETF, the MANET working group was born, and made effort to standardize routing protocols for ad hoc networks. Meanwhile, the IEEE 802.11 subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated hidden terminals, for building mobile ad hoc network prototypes out of notebooks and 802.11 PCMCIA cards. There are currently two kinds of mobile wireless networks. The first is known as *infrastructured* networks with fixed and wired gateways.

Typical applications of this type of "one-hop" wireless network include wireless local area networks (WLANs). The second type of mobile wireless network is the infrastructure. In such network, all nodes are dynamically and arbitrarily located, and are required to relay packets for other nodes in order to deliver data across the network.

3.2 BASICS

Mobile ad hoc networks (MANETS) due to its inherent capabilities of instant communication in most of the time and mission critical applications recently received a significant researchers attention.The main goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes which may be combined routers and hosts--they form the network routing infrastructure in an ad hoc fashion. However, only a few of them provide a guaranty which is an orthogonal to security critical challenge. Taking these factors into concern, the main vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links.

Considering this nature of MANETS, its environment consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)--herein simply referred to as "nodes"--which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. In the latter operational mode, it is typically envisioned to operate as a "stub" network connecting to a fixed internetwork. Stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network.

MANET nodes are equipped with wireless transmitters and receivers using antennas which may be unidirectional (broadcast), highly-directional (point-to-point), possibly steerable, or some combination thereof. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters [1]. In this paper we are describing the MANETS environment variations, challenges, capacity and some

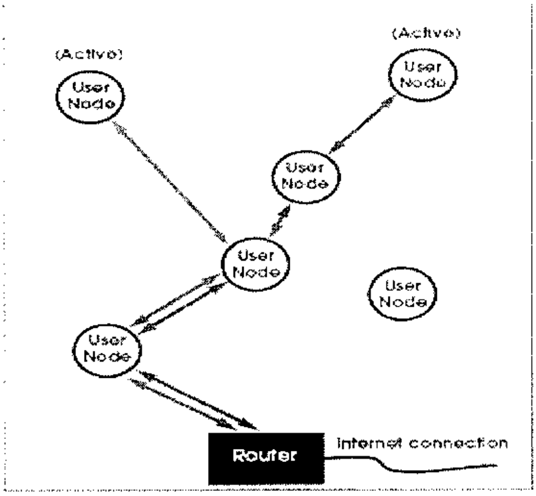


Figure 3.1 Basic Structure of MANET

3.3 ADHOC Vs WIRELESS NETWORK:

Ad hoc networks are new families of wireless networks. Advantages of ad hoc networks are,

1. No need to install base station.
2. Independence from central network administration.
3. Easier temporary setup.
4. Self-conFigureuring, nodes are also routers.
5. Self-healing through continuous re-conFigureuration.
6. Scalable - accommodates the addition of more nodes.
7. Flexible - able to access the internet from many different locations.
8. Well suited for free unlicensed spectrum.

While ad hoc networks are typically used where they have the greatest emphasis on its advantages, there are some limitations:

1. Each node must have full performance.
2. Throughput is affected by system loading.
3. Reliability requires a sufficient number of available nodes.
4. Large ad hoc networks can have excessive latency (time delay).

3.4 ENVIRONMENT VARIATIONS:

The different MANET environment variations [14] are listed as follows taking its dynamic topology in to consideration:

1. In MANETS all nodes have identical capabilities and responsibilities, which are termed as fully symmetric environment. A mobile ad hoc network (MANET) is a network comprising wireless mobile nodes that communicate with each other without centralized control or established infrastructure. These nodes which are within each other`s radio range can communicate directly, while distance nodes rely on their neighbouring nodes to forward packets. In MANETS every node can be a host or router. In MANET environment, nodes are free to join or leave the network at any point of time, resulting in a highly dynamic network environment compared to wired network [5].
2. The Asymmetric Capabilities in MANETS include transmission ranges and radios ranges which may differ. Battery life, speed of movement and processing capacity will be different at different nodes.
3. Asymmetric Responsibilities include that only some nodes may route packets in the network or some nodes may act as leaders for nearby nodes like cluster head.
4. Traffic characteristics may differ in different ad hoc networks like bit rate, timeliness constraints, reliability requirements, unicast or multicast or geocast, host-based addressing or content-based addressing or capability-based addressing.
5. MANETS may co-exist and also co-operate with an infrastructure based network.
6. Mobility patterns may be different like people sitting at an airport lounge, citywide taxi cabs,military movements and personal area networks. The performance of a mobile ad hoc network is dependent on the node mobility pattern as well as topology, data traffic patterns, and radio interference.
7. Mobility characteristics include speed, predictability, direction of movement, pattern of movement, uniformity of mobility characteristics among different nodes.

3.5 CAPACITY:

The different cases in which the throughput of the channel varies is a MANET is listed as follows:

Consider a single channel shared by n nodes in a network, then the throughput per node will be *(1/n)*, on average. Consider an IEEE 802.11a/g channel at 54 Mbps in a network with n nodes and no mobility considered, the throughput per node will be ***(O (1/sqrt (n))).***For a chain (linear) of ad hoc nodes in a network, the ideal capacity will be 1/4 of channel; simulation yields capacity of 1/7 of channel. Consider the case in which the packets are distributed to many intermediate nodes that relay packet to destination when destination comes nearby in a network. In such cases the throughput per node will be ***(O (1)).***Consider with multi-user coding in a network, then the throughput per node will be ***(O (1))*** .

Capacity of Fixed Ad Hoc Networks:

Let us consider ***n*** nodes in area ***A*** transmitting at ***W*** bits/sec using a fixed range(distance between a random pair of nodes is ***O (sqrt (n))***, then the bit-distance product that can be transported by the network per second is, ***(W sqrt (A n))***,[5] then the throughput per node is ***(W / sqrt (n)).***

Capacity of Mobile Ad Hoc Networks:

Let us assume random motion in a network, wherein any two nodes become neighbours once in a while and each node assumed sender for one *session,* and destination for another *session* and relay packets through at most one other node. Packet go from source to destination directly, when source and destinations are neighbours, or from source to a relay and the relay to destination, when each pair becomes neighbour respectively. In such a case the throughput of each session is ***O(1)***, which is independent of ***n***. Delay in packet delivery can be large if ***O(1)*** throughput is to be achieved and delay incurred waiting for the destination to arrive close to a relay or the sender.

3.6 CHALLENGES:

The following list of challenges shows the inefficiencies and limitations that have to be overcome in a MANET environment [14]:

1. Limited wireless transmission range: In wireless networks the radio band will be limited and hence data rates it can offer are much lesser than what a wired network can offer. This requires the routing protocols in wireless networks to use the bandwidth always in an optimal manner by keeping the overhead as low as possible. The limited transmission range also imposes a constraint on routing protocols in maintaining the

topological information. Especially in MANETS due to frequent changes in topology, maintaining the topological information at all nodes involves more control overhead which, in turn, results in more bandwidth wastage [6].

2.Time-varying wireless link characteristics: The wireless channel is susceptible to a variety of transmission impediments such as path loss, fading, interference and blockage. These factors resist the range, data rate, and the reliability of the wireless transmission. The extent to which these factors affect the transmission depends upon the environmental conditions and the mobility of the transmitter and receiver. Even the two different key constraints, Nyquist's and Shannon's theorems, that govern the ability to transmit information at different data rates can be considered [6].

3. Broadcast nature of the wireless medium: The broadcast nature of the radio channel, that is, transmissions made by a node are received by all nodes within its direct transmission range. When a node is receiving data, no other node in its neighbourhood, apart from the sender, should transmit. A node should get access to the shared medium only when its transmissions do not affect any on going session. Since multiple nodes may contend for the channel simultaneously, the possibility of packet collisions is quite high in wireless networks [6]. Even the network is susceptible to hidden terminal problem and broadcast storms [4]. The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver [6].

4. Packet losses due to transmission errors: Ad hoc wireless networks experiences a much higher packet loss due to factors such as high bit error rate (BER) in the wireless channel, increased collisions due to the presence of hidden terminals, presence of interference, location dependent contention, uni-directional links, frequent path breaks due to mobility of nodes, and the inherent fading properties of the wireless channel [6].

5. Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes. Therefore mobility management itself is very vast research topic in ad hoc networks.

6.Mobility-induced packet losses: Communication links in an ad hoc network are unstable such that running conventional protocols for MANETS over a high loss rate will suffer from severe performance degradation. However, with high error rate, it is very much difficult to

7. Battery constraints: This is one of the limited resources that form a major constraint for the nodes in an ad hoc network. Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device. By increasing the power and processing ability makes the nodes bulky and less portable. So only MANET nodes has to optimally use this resource.

8. Potentially frequent network partitions: The randomly moving nodes in an ad hoc network can lead to network partitions. In major cases, the intermediate nodes are the one which are highly affected by this partitioning.

9.Ease of snooping on wireless transmissions (security issues): The radio channel used for ad hoc networks is broadcast in nature and is shared by all the nodes in the network. Data transmitted by a node is received by all the nodes within its direct transmission range. So an attacker can easily snoop the data being transmitted in the network. Her the requirement of confidentiality can be violated if an adversary is also able to interpret the data gathered throughsnooping[6].

CHAPTER 4

SINGLE SOURCE BROADCASTING PROTOCOLS

Broadcasting is the process in which one node sends a packet to all other nodes in the network. Broadcasting is often necessary in MANET routing protocols. For example, many routing protocols such as Dynamic Source Routing (DSR), Ad Hoc On Demand Distance Vector (AODV) use broadcasting to establish routes. The broadcast is spontaneous. Any mobile host can issue a broadcast operation at any time. Several broadcasting algorithms are available. They are broadly classified into four types: simple flooding, probability based methods, area based methods and neighbor knowledge methods.

Simple flooding requires each node to rebroadcast all packets. Probability based methods use some basic understanding of the network topology to assign a probability to a node to rebroadcast. Area based methods assume nodes have common transmission distances; a node will rebroadcast only if the rebroadcast will reach sufficient additional coverage area. Neighbor knowledge methods maintain state on their neighborhood, via "Hello" packets, which is used in the decision to rebroadcast.

4.1 PROBLEMS INVOLVED:

Broadcasting the messages in an ad hoc network has following problems.

1)Redundant rebroadcasts:

When a mobile host decides to rebroadcast a broadcast message to its neighbors, all its neighbors already have the message.

2)Contention:

After a mobile host broadcasts a message, if many of its neighbors decide to rebroadcast the message, these transmissions (which are all from nearby hosts) may severely contend with each other.

3)Collision:

Because of the deficiency of back off mechanisms, the lack of proper acknowledgements and the absence of CD (Collision Detection) mechanisms, collisions are more likely to occur and cause more damage [8].

4.2 PROTOCOLS:

Existing broadcasting methods in mobile ad hoc networks are single source broadcasting algorithms in which only one source node can send the broadcast message to all the nodes in the network. Existing broadcasting algorithms are classified into following types.

Simple flooding

It starts with a source node broadcasting a packet to all its neighbors. Now each of the neighbors that receive this packet will rebroadcast the packet exactly once and this continues until all the nodes in the network have received the packet. The duplicate packets are not broadcasted again.

Demerit:

This technique is expensive and it results in collision.

Probablity based methods:

Probabilistic Scheme :

Source node broadcasts the packet to all its neighbors. Some neighbor nodes rebroadcast the packet. The selection is based on predetermined probability. When the probability is 100%, this scheme is same as simple flooding. This method is well suited for dense networks.

Counter Based Scheme:

Upon reception of a previously unseen packet, the node initiates a counter with a value of one and sets a RAD (Random Assessment Delay). During the RAD, the counter is incremented by one for each redundant packet received. If the counter is less than a threshold value when the RAD expires, the packet is rebroadcast. Otherwise, it is simply dropped.

Demerit :

For sparse networks, all the nodes might not receive the packets.

Area based methods:

In the area based method, the packet is re-broadcasted only if the node covers a additional area covered by the retransmission is low. If the receiving node is located at the boundary of the sender node's transmission distance, then a rebroadcast would reach significant additional area.

Distance-Based Scheme:

A node using the Distance-Based Scheme compares the distance between itself and each neighbor node that has previously rebroadcast a given packet. Upon reception of a previously unseen packet, a RAD (Random Assessment Delay) is initiated and redundant packets are cached. When the RAD expires, the source node location is examined to see if any node is closer than a threshold distance value. If true, the node doesn't rebroadcast [16].

Location-Based Scheme:

The Location-Based scheme uses a more precise estimation of expected additional coverage area in the decision to rebroadcast. In this method, each node must have the means to determine its own location, e.g., a Global Positioning System (GPS). Whenever a node originates or rebroadcasts a packet it adds its own location to the header of the packet. When a node initially receives a packet, it notes the location of the sender and calculates the additional coverage area obtainable were it to rebroadcast. If the additional area is less than a threshold value, the node will not rebroadcast. Otherwise, the node assigns a RAD before delivery. If the node receives a redundant packet during the RAD, it recalculates the additional coverage area and compares that value to the threshold. The area calculation and threshold comparison occur with all redundant broadcasts received until the packet reaches it's scheduled send time

Demerit:

Number of re-broadcasts made by the intermediate nodes is very high.

Neigbour knowledge methods:

Flooding with self pruning:

In this method each node will have knowledge of its neighbors and maintains neighbors list. A node that receives a broadcast packet compares its neighbour list to the sender's neighbour list. If the receiving node would not reach any additional nodes then it pruning. Existing algorithms are single source broadcasting algorithms. Only a single node transmits and it transmits only once to achieve reliable broadcast.

Scalable Broadcasting:

The Scalable Broadcasting requires that all nodes have knowledge of their neighbors within a two hop radius. This neighbor knowledge coupled with the identity of the node from which a packet is received allows a receiving node to determine if it would reach additional nodes by re-broadcasting. Suppose Node B receives a broadcast data packet from Node A. Since Node A is a neighbor, Node B knows all of its neighbors, common to Node A, that have also received Node A's transmission of the broadcast packet. If Node B has additional neighbors not reached by Node A's broadcast, Node B schedules the packet for delivery with a RAD. If Node B receives a redundant broadcast packet from another neighbor, Node B again determines if it can reach any new nodes by re-broadcasting. This process continues until either the RAD expires and the packet is sent, or the packet is dropped [7].

Dominant Pruning:

Dominant Pruning uses 2-hop neighbor knowledge, obtained via "Hello" packets, for routing decisions. Nodes inform neighbors to rebroadcast by including their address as part of a list in each broadcast packet header. When a node receives a broadcast packet it checks the header to see if its address is part of the list.

If so, it uses a Greedy Set Cover algorithm to determine which subset of neighbors should rebroadcast the packet, given knowledge of which neighbors have already been covered by the sender's broadcast. The Greedy Set Cover algorithm recursively chooses 1-hop neighbors which cover the most 2-hop neighbors and recalculates the cover set until all 2-hop neighbors are covered.

Demerit:

Routing overhead is high.

Existing broadcasting methods in mobile ad hoc networks are single source broadcasting algorithms in which only one source node can send the broadcast message to all the nodes in the network. The number of re-broadcasts made by the intermediate nodes is very high. This increases the delay latencies. Due to heavy traffic, routing overhead is high.

The proposed system is multi source reliable broadcasting which can broadcast the messages reliably from different sources to all the nodes in the network. The solution does not require the nodes to know the network size, its diameter and number of nodes in the network. The only information a node has its identity (IP Address) and its position. The algorithm takes into consideration node mobility and multiple nodes co-located at the same point. This algorithm delivers the messages within a bounded time. It minimizes the number of re-broadcasts made by the intermediate nodes. The algorithm reduces routing overhead by minimizing end to end delay.

CHAPTER 5

RELIABLE BROADCASTING PROTOCOL

The proposed system is multi source reliable broadcasting which can broadcast the messages reliably from different sources to all the nodes in the network. The solution does not require the nodes to know the network size, its diameter and number of nodes in the network. The only information a node has its identity and its position. On average, only a subset of nodes transmits and they transmit only once to achieve reliable broadcasting.

The algorithm calculates the relative position of the nodes with respect to the broadcasting source node. It propagates the message as far as possible to minimize the delay. The nodes that are farthest from the source node are scheduled to transmit first. The algorithm minimizes the number of transmissions made by the participating nodes. If a node that is scheduled to transmit a message in a round realizes that its transmission cannot propagate the message to any new node, it cancels its scheduled transmission. This minimizes the number of rebroadcasts made by the intermediate nodes and reduces the delay latency.

5.1 SYSTEM MODEL:

MANET is represented as a grid based graph where a vertex of the graph represents a node and there is a directed edge from node i to node j if node j is in the range of node i. Nodes are located at grid points and they know their own position [10],[11]. A node that has received the broadcast message is called a covered node and a node that has not yet received the broadcast message is called an uncovered node. Each node is equipped with a GPS receiver to know its own location.

5.2 PROTOCOL DESCRITION:

In order to reliably broadcast a message to all the nodes of the network, the scheduling algorithm considers the relative position of the nodes with respect to the Broadcast source. In every round, the covered node that is farthest from the source transmits. Algorithm also minimizes the number of transmissions by the participating nodes. If a node that is scheduled to transmit a message in a round realizes that its transmission cannot propagate the message to any new node, it will cancel its scheduled transmission.

Control Slot

A single round with control and application slots is shown in the Figure 5.1. The only information required by the scheduling algorithm is for each node to be aware of all the other nodes that are within one grid distance from itself and their intended mobility for a round. In the first half of the control slot, all the nodes collocated at a grid point communicate with each other to learn their respective direction of movement for this round. This can be done reliably and deterministically by the CSMA/DCR (Carrier Sense Multiple Access with Deterministic Collision Resolution) protocol. This communication requires nodes to transmit using a very small range to avoid collisions with messages transmitted in neighboring grid points. After this communication, a node is aware of all the nodes collocated with itself and can determine if it has the smallest ID among the collocated nodes[12].

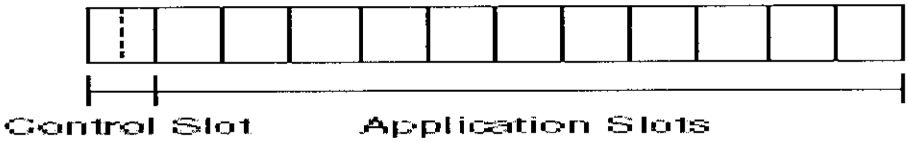


Figure 5.1. A round with control and application slots

The first half of the control slot consists of the source node and destination node addresses. The second half of the control slot is divided into three transmission phases: the node with the smallest ID at grid point i transmits in phase i mod 3 to convey the mobility information for all the nodes collocated at grid point i to the nodes at neighboring grid points. Hence, at the end of a control slot, a node has enough knowledge to determine the positions of other nodes that are one grid distance from it for the remaining slots of that round.

Application Slot

The source node starts the broadcast by transmitting in the first application slot of a round. The broadcast message carries the initial position of the source node as well as the this information to determine its grid segment and calculates its transmission schedule for the next round.

5.3 ALGORITHM:

In order to reliably broadcast a message to all the nodes of the network, the scheduling algorithm considers the relative position of the nodes with respect to the broadcast source. In every round, the covered node that is farthest from the source transmits. The algorithm minimizes the number of rebroadcasts made by the participating nodes. If a node that is scheduled to transmit a message in a round realizes that its transmission cannot propagate the message to any new node, it will cancel its scheduled transmission[11]. The grid segments relative to the source node are shown in the Figure 5.2. An unshaded circle represents an uncovered node and a shaded circle represents a covered node. A node with the thick circle is the one that transmits in that slot.

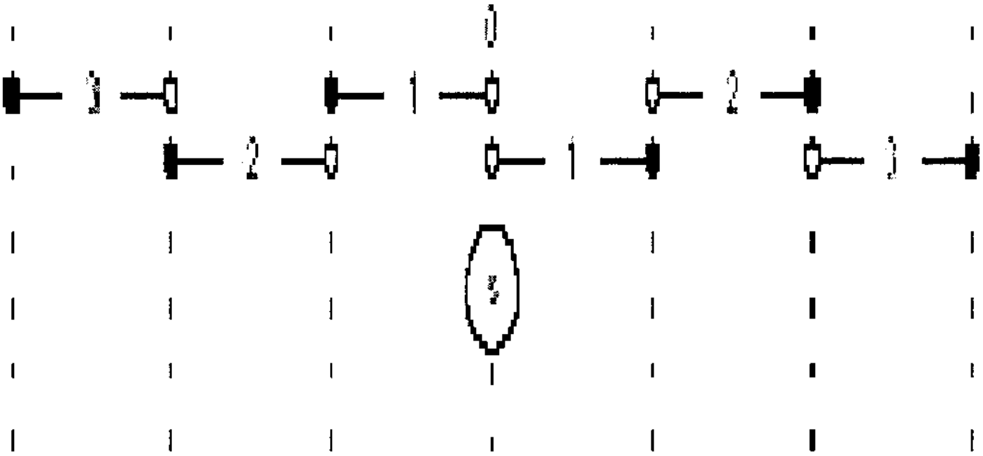


Figure 5.2. The grid segments

Let grid point p be the position of the source node at the beginning of the broadcast. Let 1, 2, 3, . . be the grid segments (p, p + 1), (p + 1, p + 2), (p + 2, p + 3), . . ., respectively, and let −1,−2,−3, . . . be the grid segments (p−1, p), (p−2, p− 1), (p−3, p−2), . . ., respectively. The source node and all the nodes collocated with the source node are in grid segment 0, which is a special grid segment consisting of a single point [11],[12].

The source node starts the broadcast by transmitting in the first application slot of a round. The broadcast message carries the initial position of the source node as well as the grid segment of the transmitting node. Upon receiving the broadcast message, a node uses next round. A node is not allowed to transmit in the same round it received a broadcast message. It can only transmit in the next round.

Whenever a node gets a new broadcast message it sets its counter equal to $R-|p1-p|+2$, where p1 is the grid segment of the receiving node and p is the grid segment of the transmitting node. When a node in segment p transmits, it covers all the nodes in segments $p, p \pm 1, p \pm 2, \ldots, p \pm R$, where $R > 1$ is the maximum communication range of each node. If a transmitting node is in grid segment p, then in the next round a receiving node from grid segment $p \pm (R + 1), p \pm R, p \pm (R - 1), \ldots, p \pm 1, p$ could transmit in slots $1, 2, 3, \ldots, R+1, R+2$, respectively. Whenever a node gets a new broadcast message it sets its counter equal to $R-|p-p1|+2$, where p is the grid segment of the receiving node and p1 is the grid segment of the transmitting node.

In the beginning of every application slot of the next round, each node decrements its counter by 1. If on decrementing, the counter reaches 0, the node is eligible to transmit in that slot. Let A be a node that is scheduled to transmit in a slot. Let node A be located in grid segment i and let there be another node B be located in grid segment j. On the right hand side of message propagation, if $i < j \leq i+R$ then node B has already transmitted in an earlier slot. In this case the transmission of node A is redundant and does not help to propagate the message any further. Hence, node A cancels its counter and does not transmit. Similarly, on the left hand side of message propagation, if $i > j \geq i - R$ then node B has already transmitted in an earlier slot and the transmission of node A is redundant. Hence, if a node whose counter is not yet 0 again receive the same broadcast message, it cancels the counter and does not transmit.

5.4. EXECUTION:

Execution of the reliable broadcasting algorithm when the nodes are mobile is shown in the Figure 5.4. Let A be a node got covered in the previous round. Let that node move from grid segment p1 to a neighboring grid segment p. If $|p| > |p1|$ then node A decrements its counter by 1, and if $|p| < |p1|$ then node A increments its counter by 1. This ensures that the rightmost and leftmost covered nodes have the smallest counter value [12]. When a node transmits, all the nodes collocated with the transmitting node and the transmitting node itself set their counter to $R-|p-p1|+2$, where p is the grid segment of the receiving node and p1 is the grid segment of the transmitting node, only if they have not already transmitted twice.

If a node is mobile then adjust the counter of that node depending on whether the node moves towards or away from the initial position of the source. When a node moves to a new grid segment then the counter is updated. Let A be a node that got covered in the previous round. Let node A move from grid segment p1 to a neighboring grid segment p. If |p| > |p1| then node A decrements its counter by 1, and if |p| < |p1| then node A increments its counter by 1. This ensures that the rightmost and leftmost covered nodes have the smallest counter value.

In every round the covered node that is farthest from the source node transmits. Whenever a node transmits a broadcast message, all the receiving nodes set a counter when they receive this message. The value of this counter depends on the position of the receiving node at the time it received the broadcast message. The counter value is inversely proportional to the absolute value of the grid segment number. Even if the nodes move, the counters are adjusted such that this property is preserved. Since these counters are decremented in every slot and the node whose counter is equal to 0 transmits, the nodes in the grid segment farthest from the source always get a chance to transmit first and their transmission never gets suppressed by the transmission of any other node [6],[7].

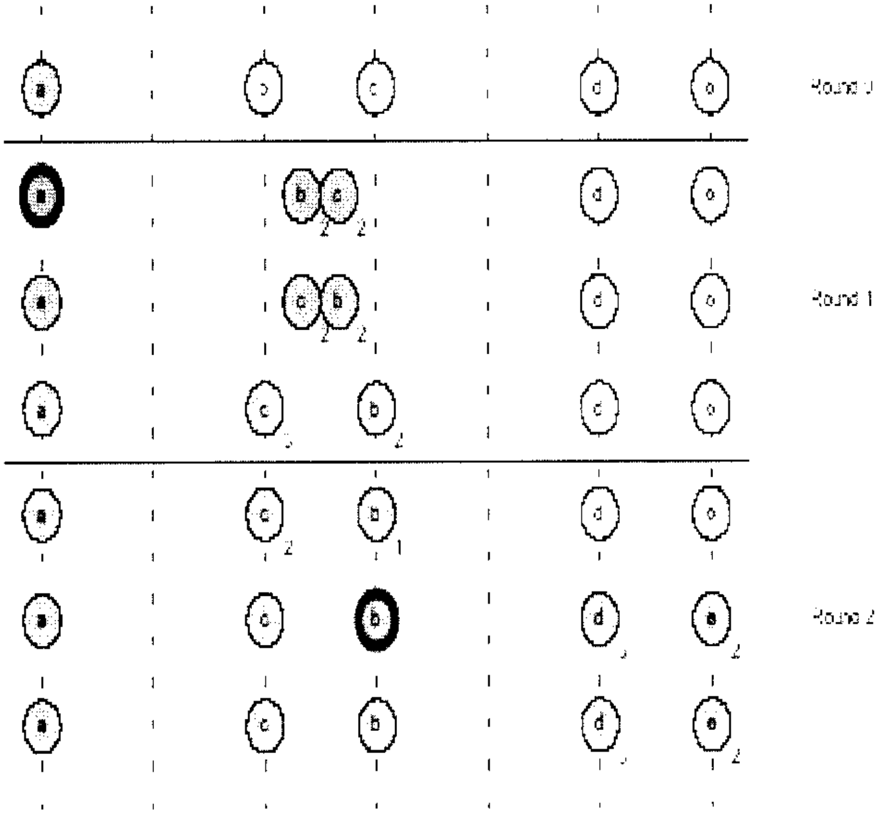


Figure 5.4 Execution of the algorithm

5.5. CSMA/DCR PROTOCOL:

Execution of CSMA/DCR protocol on a binary tree is shown in the Figure 5.5. Let n to be the total number of nodes in the network and let k be the maximum number of competing collocated nodes. All the n nodes construct an identical static binary tree with exactly n leaves representing the nodes identifiers. When a collision is detected, the nodes initiate a deterministic balanced tree search by recursively searching a sub tree with only one active leaf.

Intially, all nodes may transmit a message. Suppose that a collision happens in the first slot. Then, in the second slot, only the nodes whose identifiers belong to the left sub tree are allowed to transmit. If the transmission succeeds, then nodes whose identifiers belong to the right sub tree are allowed to transmit [8].

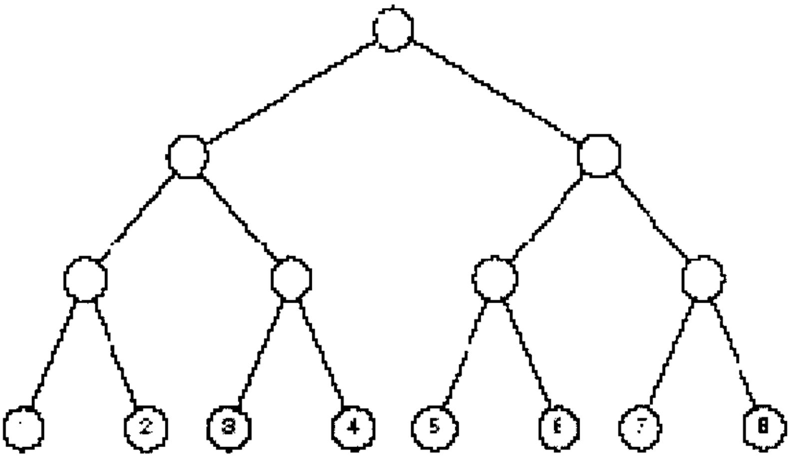


Figure 5.5. CSMA/DCR execution on a binary tree

State of a channel during the execution of the protocol CSMA/DCR [9] is shown in the Table 1.

The active nodes that have a message to transmit are represented as dark circles. In the first slot, nodes 3, 4, 6 and 8 transmit and cause a collision (denoted by C). In the second slot, only nodes belonging to the left sub tree transmit, namely nodes 3 and 4, which results again in a collided channel. In the next slot, the protocol allows only nodes 1 and 2 to transmit. Since none of them have a message to send, the slot is empty (denoted by E). Then,

TABLE 1.

THE STATE OF THE CHANNEL DURING CSMA/DCR EXECUTION

C - Collision, E - Empty channel, T - Transmission.

Slots								
1	2	3	4	5	6	7	8	9
C	C	E	C	T	T	C	T	T
3	3		3	3	4	6	6	8
4	4		4			8		
6								
8								

The CSMA/DCR protocol is used in the first half of the control slot. Nodes transmit with a very small range during this time. Hence, if one node at grid point i detects a collision due to the broadcast of nodes collocated at grid point i, all the nodes at the same grid point also detect that collision. This means that the hidden terminal problem does not occur with this schema.

In multi source reliable broadcasting algorithm, multiple sources can initiate the broadcasts at a time. The algorithm takes into consideration node mobility and multiple nodes co-located at the same point. This algorithm delivers the messages within a bounded time. It minimizes the number of re-broadcasts made by the intermediate nodes. The algorithm reduces routing overhead by minimizing end to end delay.

CHAPTER 6

IMPLEMENTATION DETAILS

The proposed algorithm is implemented in ns-2. Network Simulator is an object-oriented, discrete, event-driven network simulator developed at the OC Berkley and ISC ISI as part of the VINT project. In the recent years, its functionality has grown to include wireless and ad hoc networks as well. It allows simulation scripts to be written in a script like programming language OTCL. It provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks.

The simulator is open source, allowing everyone to make changes to the existing code, besides adding new protocols and functionalities to it. The usage of OTCL for simulation scenario scripts allows the user to change parameters of a simulation without having to recompile any source code. It is also possible to let ns-2 generate a special trace file that can be used by NAM (Network Animator), a visualization tool that is a part of the simulator distribution.

6.1 BASICS NETWORK SIMULATOR:

The ns-2 architecture is shown in the Figure 6.1.

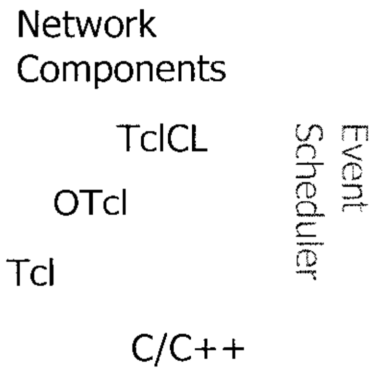


Figure 6.1 ns-2 Architecture

OTcl (object variant of TCL) and C++ share class hierarchy. TclCL is a glue library that makes it easy to share functions and variables. C/C++ is used for detailed implementations of protocols. TCL scripting is the front-end interpreter for ns-2 used for constructing commands and conFigureuration interfaces.

6.2 NETWORK SIMULATOR ELEMENTS:

- Create the event scheduler
- Turn on tracing
- Create network
- Setup routing
- Insert errors
- Create transport connection
- Transmit application-level data

6.3 NETWORK SIMULATOR FUNCTIONALITIES:

1. Wired network
    - i Routing DV, LS, PIM-SM
    - ii Transportation: TCP and UDP
    - iii Traffic sources: web, ftp, telnet
    - iv Queuing disciplines: drop-tail, RED, FQ, SFQ, DRR
    - v Emulation
2. Wireless network
    - i Ad hoc routing and mobile IP
    - ii Directed diffusion, sensor-MAC
3. Tracing, visualization, various utilities

6.4 IMPLEMENTTATION AND SIMULATION STEPS:

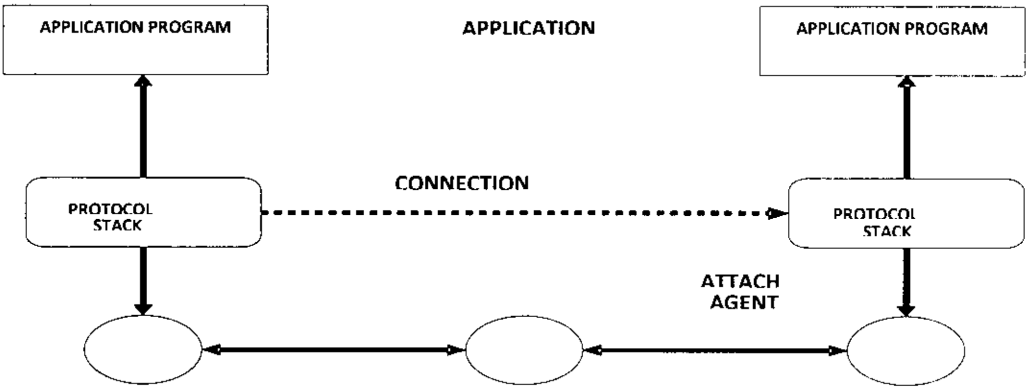


Figure 6.2 Steps in ns2

Implementation steps in ns-2 are shown in the Figure 4.2. Implementation consists of 4 steps:

- Implementing the protocol by adding a combination of C++ and OTCL (Object-Oriented Tool Command Language)
- code to ns-2's source base;
- Describing the simulation in an OTCL script;
- Running the simulation and analyzing the generated trace files.

Network simulator source code is split between C++ for its core engine and OTCL, an object oriented version of TCL for configuration and simulation scripts. The combination of the two languages offers an interesting compromise between performance and ease of use. Implementing a new protocol in ns-2 typically requires adding C++ code for the protocol's functionality, as well as updating key ns-2 OTCL configuration files in order for ns-2 to recognize the new protocol and its default parameters. The C++ code describes which parameters and methods are to be made available for OTCL scripting. An agent in ns-2 terminology represents an endpoint where network packets are constructed, processed or consumed. Such an Agent was implemented at the Application layer for the broadcast source, and the simulation trace was collected at the MAC layer.

6.5 CREATING AN WIRELESS ENVIRONMENT:

The following OTcl code fragment creates a wireless environment.

set mnode [$opt(rp)-create-mobile-node $id] where $opt(rp) defines "dsdv", "aodv", "tora" or "dsr" and id is the index for the mobilenode.

```
$node set X_ <x1>

$node set Y_ <y1>

$node set Z_ <z1>

set ns [new Simulator]

$ns at $time $node setdest <x2> <y2> <speed>

$mobilenode start

set topo [new Topography]

$topo load_flatgrid $opt(x) $opt(y)
```

where opt(x) and opt(y) are the boundaries used in simulation.

```
set rng [new RNG]
```

The simulator supports simulation of protocols, routing, and broadcasting over wireless networks. When compared with other simulators, ns-2 would provide better accuracy, speed and ease of use. It is used in wired and wireless environment. Hence, the proposed algorithm is effectively implemented in ns-2. Graphs are generated from the produced results to evaluate and analyze the performance of the system.

CHAPTER 7

EXPERIMENTATION AND RESULTS

The performances of flooding, probability based broadcasting and reliable broadcasting for single and multi sources are analyzed. The simulations are performed using ns2.

The NAM (Network Animators) instances of initial and final phases of Single and Multi source reliable broadcasting algorithms are shown in Figure 7.1 ,7.2, 7.3 and 7.4. The Gold nodes are the source nodes which initiate the broadcasting. Red nodes receive the broadcast message and forward it to the neighboring nodes. Blue nodes receive the message but will not forward it.

The performance metrics to be observed are:

Packet delivery ratio is the number of data packets received by the destination nodes divided by the number of data packets transmitted by the source nodes.

Normalized routing load is the ratio between the number of routing packets sent by all the nodes for route maintenance and discovery and the number of data packets delivered to the destination nodes.

graphs are generated to compare various Broadcasting algorithms based on the above two metrics.

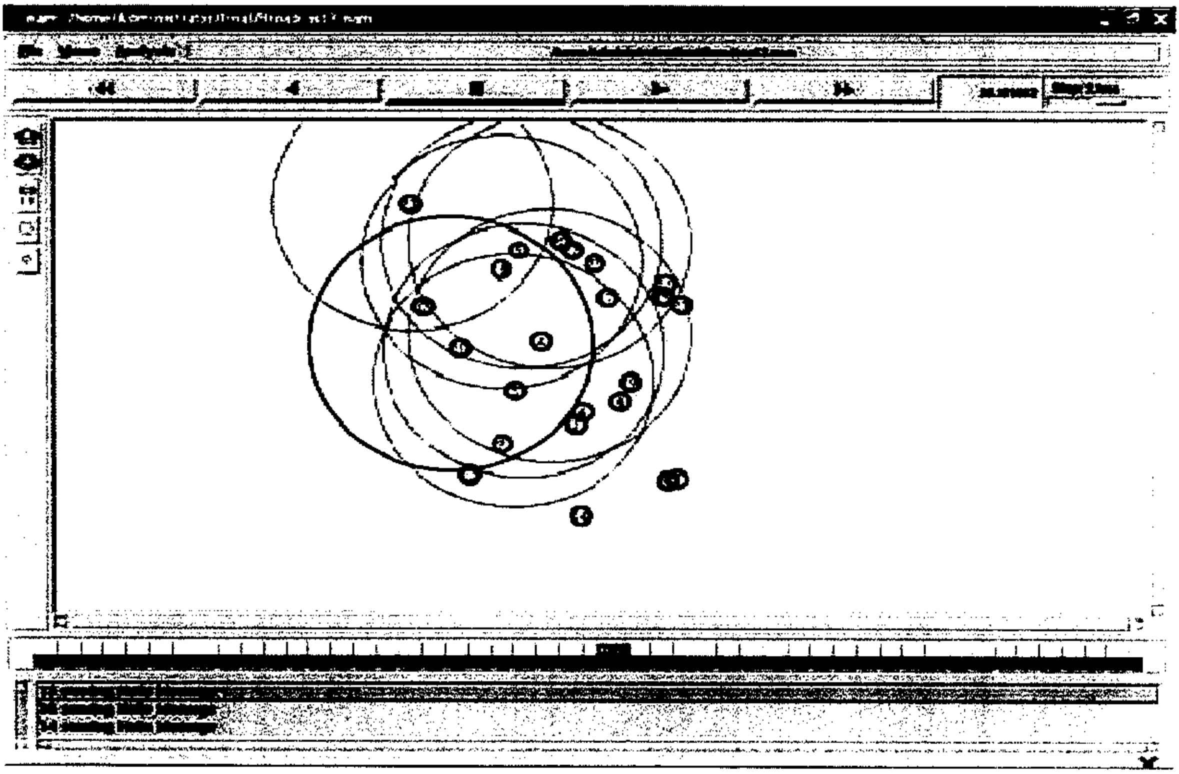
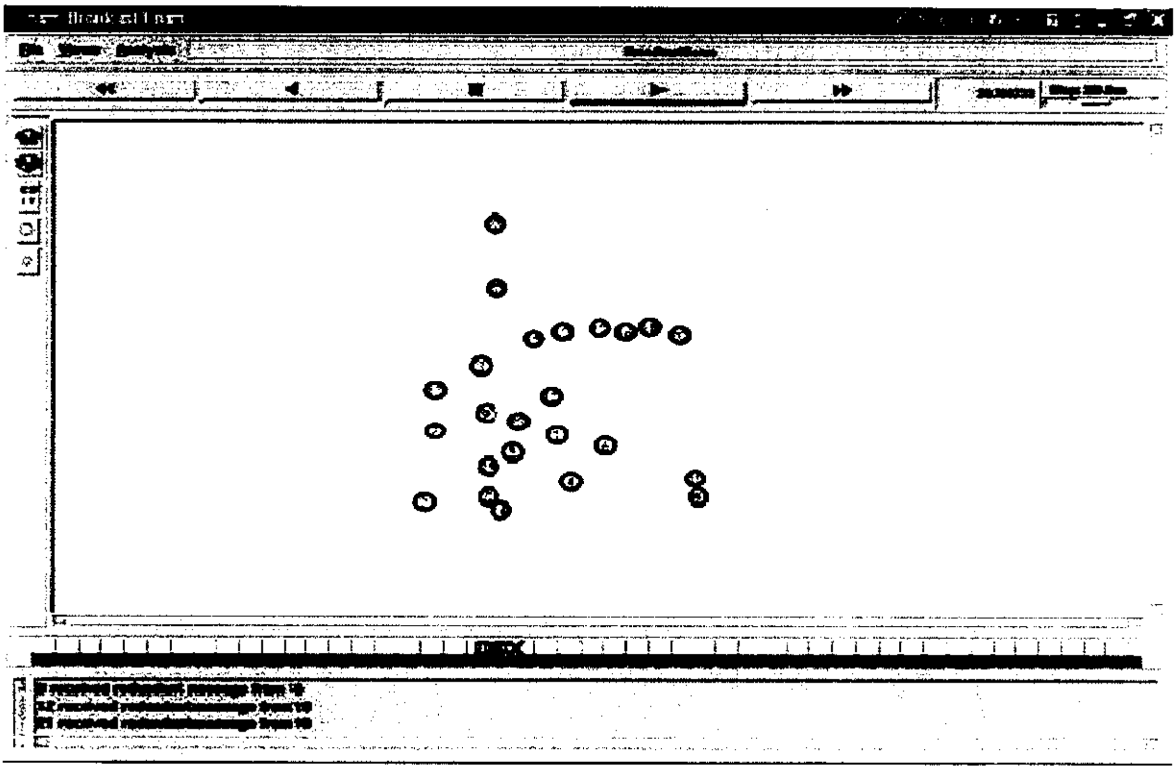
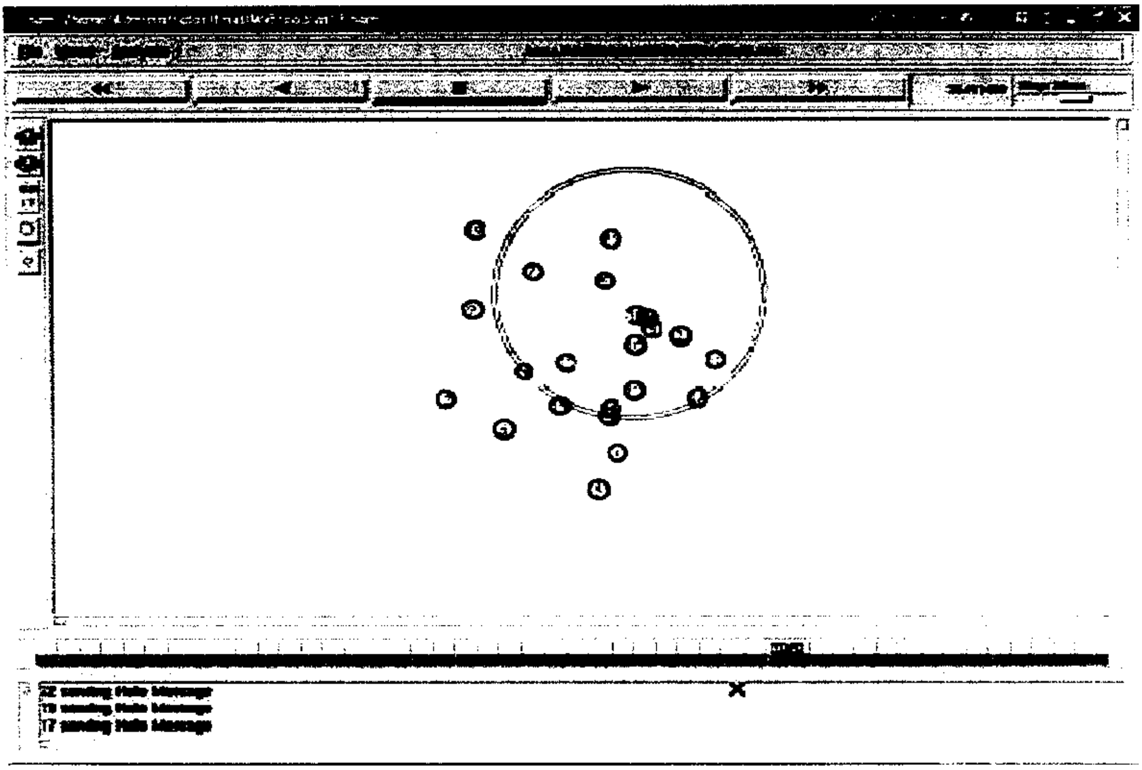


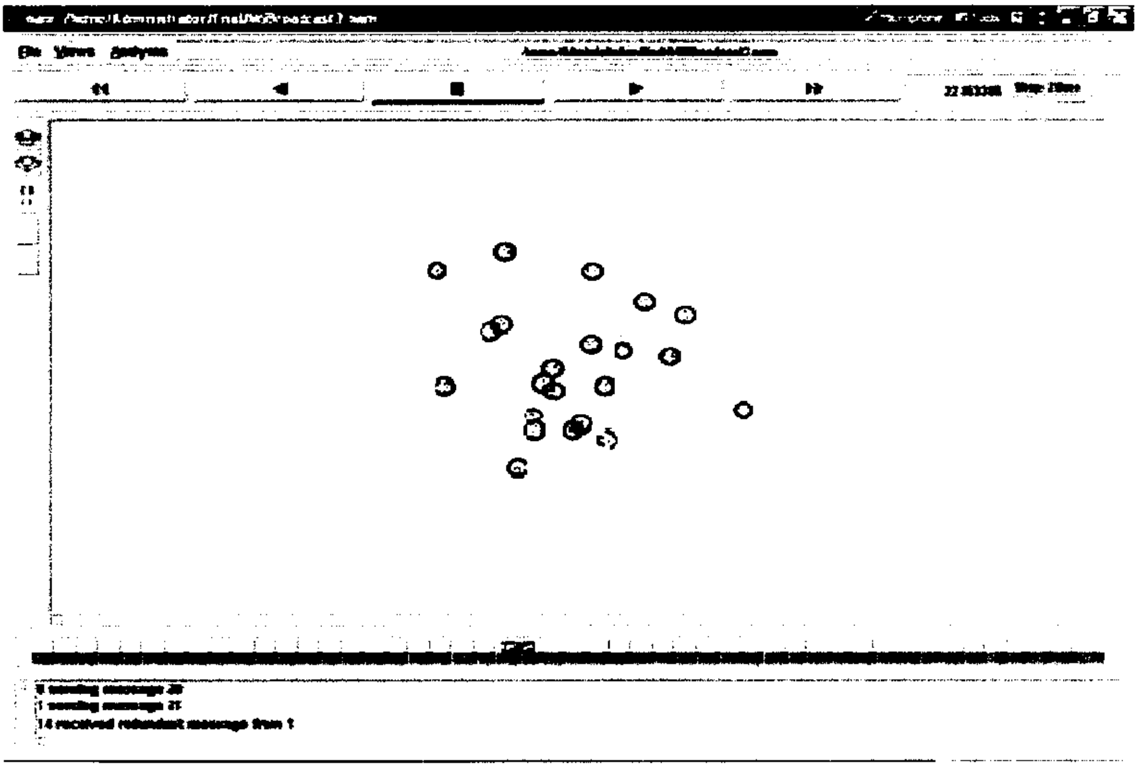
Figure 7.1: Initial Phase of Single Source Reliable Broadcasting Algorithm





```
22 sending Hello Message
19 sending Hello Message
17 sending Hello Message
```

Figure 7.3: Initial Phase of Multi Source Reliable Broadcasting Algorithm



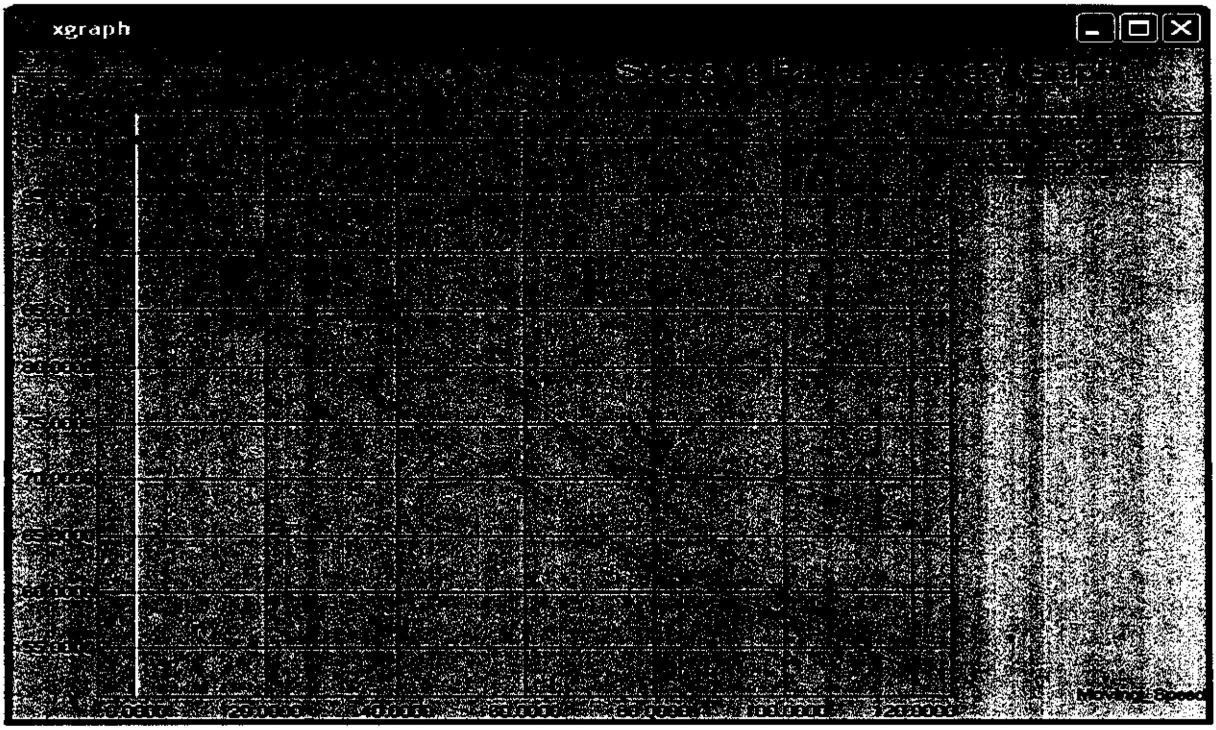
```
[illegible] sending message [illegible]
1 sending message 21
14 received redundant message from 1
```

Graphs are generated to compare various Broadcasting algorithms based on the above two metrics.

Each point in the plot is an average of over ten simulation runs. Simulation results based on different threshold values are presented to verify and compare the effectiveness of these algorithms.

The comparisons of packet delivery ratio for various single and multi source broadcasting algorithms are shown in the Figure 7.5 and 7.6. In general, data packet delivery ratio will decrease with increase in node speed because it is very difficult to find a stable route to the destination. When compared with other broadcasting algorithms reliable broadcasting algorithm maximizes the packet delivery ratio because number of re-broadcasts made by the intermediate nodes is very less.

The comparisons of normalized routing load for various single and multi source broadcasting algorithms are shown in the Figure 7.7 and 7.8. Normalized routing load will increase with increase in node speed because of heavy traffic. When compared with other broadcasting algorithms reliable broadcasting algorithm minimizes the routing overhead.



Figureure 7.5: Speed vs. Packet Delivery Ratio for various Single Source Broadcasting Algorithm

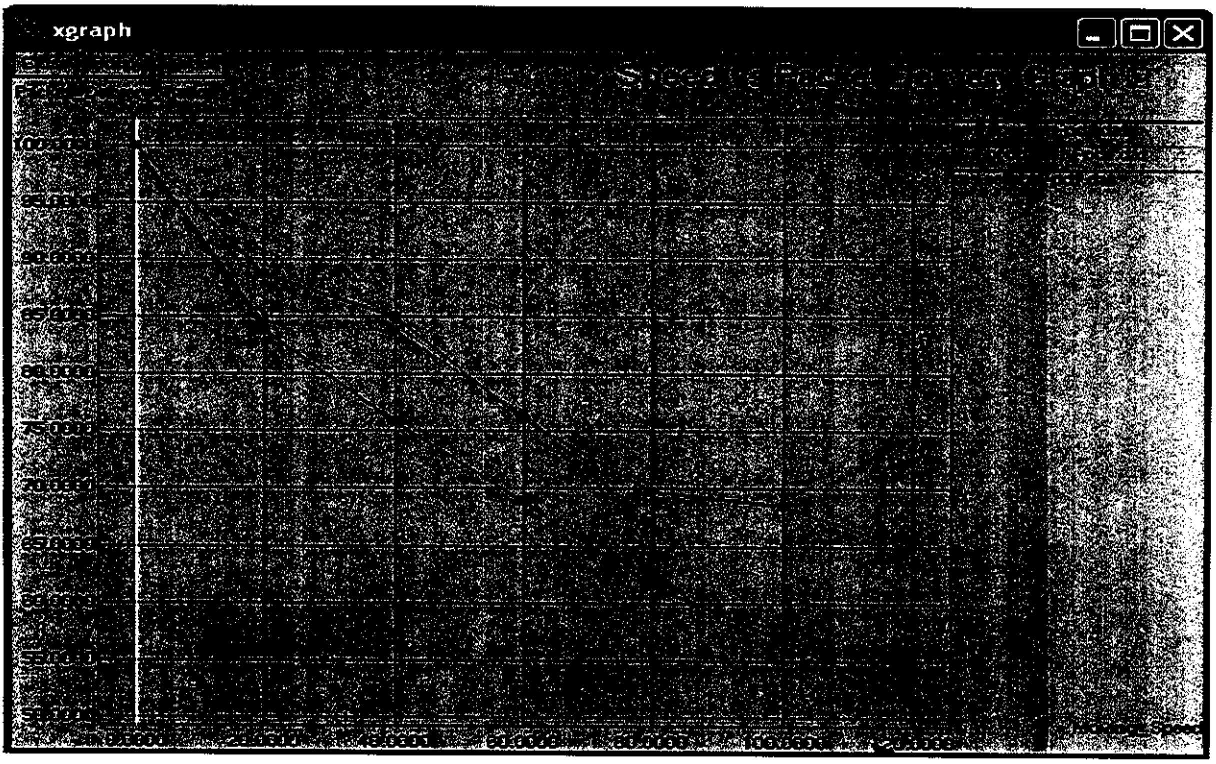


Figure 7.6: Speed vs. Packet Delivery Ratio for various Multi Source Broadcasting Algorithms

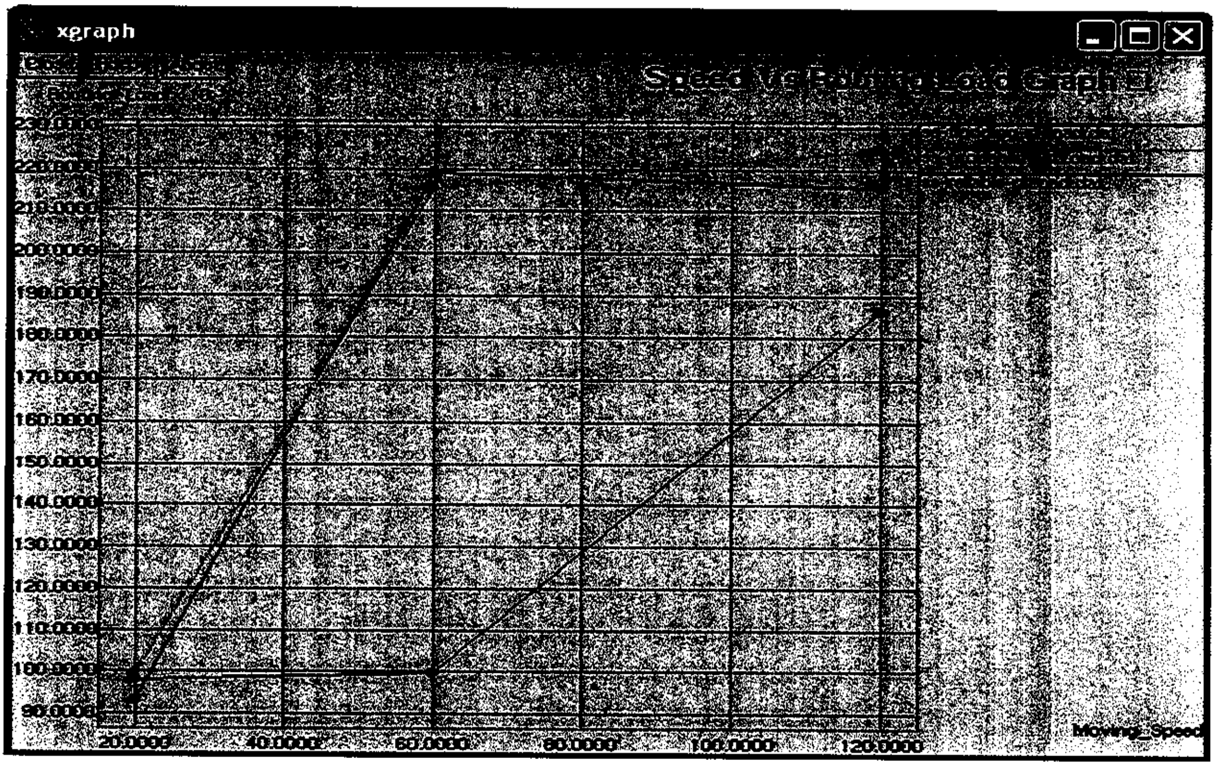


Figure 7.7: Speed vs. Normalized Routing Load for various Single Source Broadcasting Algorithms

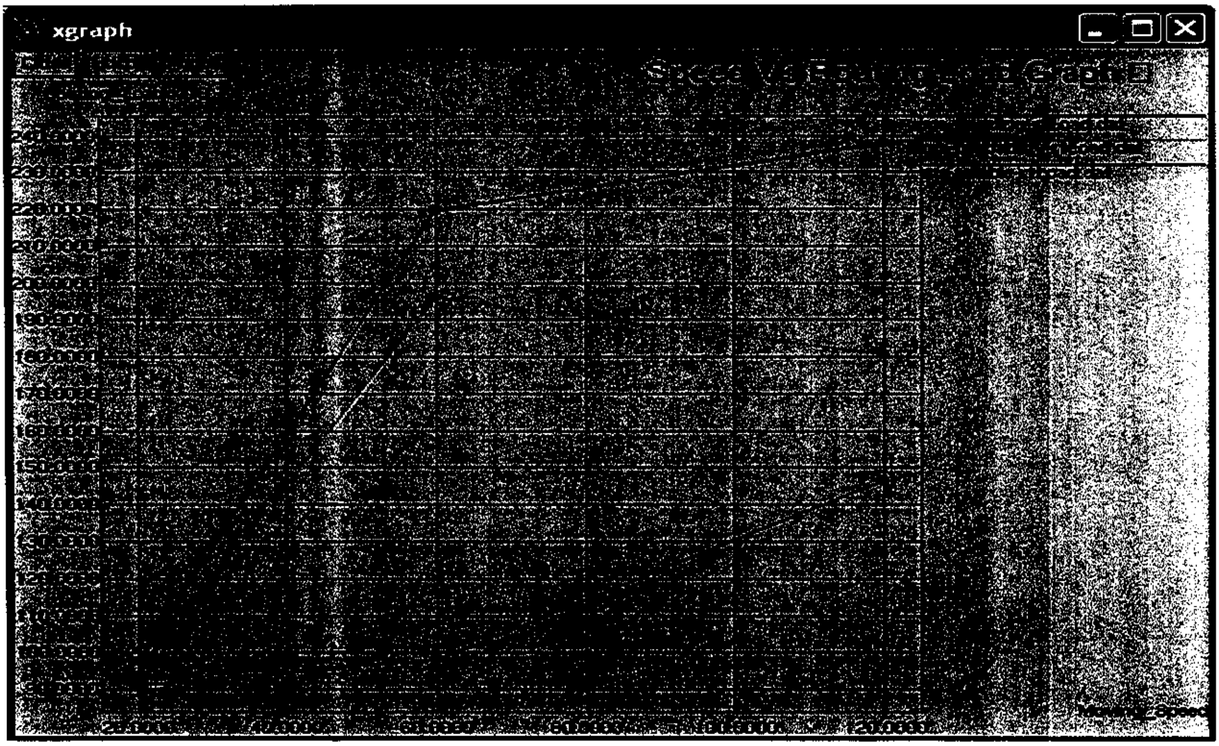


Figure 7.8: Speed vs. Normalized Routing Load for various Multi Source Broadcasting Algorithms

CHAPTER 8

CONCLUSION AND FUTURE SCOPE

A suitable communication system for the battle field is proposed and implemented which maximizes the packet delivery ratio and minimizes the network overload. The system consists of a reliable broadcasting protocol for a battle area.The algorithm calculates the relative position of the nodes with respect to the broadcasting source node. The nodes that are farthest from the source node are scheduled to transmit first. If a node that is scheduled to transmit a message in a round realizes that its transmission cannot propagate the message to any new node, it will cancel its scheduled transmission.When compared with other broadcasting algorithms this algorithm would reduce routing load overhead and maximize packet delivery ratio, since only less number of control packets are sent to the destination and the number of rebroadcasts made by the intermediate nodes is very less respectively.

For future work, the algorithm can be extended to work under error-prone conditions, i.e., location errors, imperfect time synchronization, and message losses.

BIBLIOGRAPHY

[1] Broch,J. Maltz,D.A. Johnson,D.B. Hu,Y. Jetcheva,J. (1998)A Performance Comparison of Multi-Hop Wireless Ad Hoc network Routing Protocols, Proc. Of MobiCom'98.

[2] Briesemeister,L. Sch¨afers,L. and Hommel,G.(2000)"Disseminating messages among highly mobile hosts based on inter-vehicle communication," in *IEEE Intelligent Vehicle Symposium*, pp. 522–527.

[3] Fujimoto, H. Wu. R. Guensler, R. and Hunter, M. (2004)"MDDV: A mobility centric data dissemination algorithm for vehicular networks," in VANET '04: Proceedings of the first ACM workshop on Vehicular Ad Hoc Networks, 47–56.

[4] Grossglauser,M. and Tse,D. (2002)"Mobility increases the capacity of ad hoc wireless networks",IEEE/ACM Transactions on Networking, Vol. 10, No. 4.

[5] Gupta ,P. and Kumar, P.R. (2005)"The capacity of wireless networks," IEEE Transactions on Information Theory, Vol. 51, No. 3, pp. 834-847.

[6] Gupta,P.Kumar, P.R. (2000)"Capacity of Wireless Networks", IEEE Transactions on Information Theory, Vol. 46, No. 2.

[7] Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, and Robert Morris,(2001)" Capacity of Ad Hoc Wireless Networks", In proceedings of IEEE Infocom.

[8] Krishna Moorthy Sivalingam,(2003) "Tutorial on Mobile Ad Hoc Networks".

[9] Korkmaz, G. Ekici,E. Ozg¨uner.F. and Ozg¨uner,U.(2004)"Urban multihop broadcast protocol for inter-vehicle communication systems," in VANET '04: Proceedings of the first ACM workshop on Vehicular Ad Hoc Networks,, pp. 76–85.

[10]Kranakis . E. Krizanc, D. and Pelc, A. (2001) 'Fault-tolerant broadcasting in radio networks' Journal of Algorithms, vol. 39, pp. 47–67.

[11]Liao, W.-H. Sheu J.-P. and Tseng Y.-C. (2000) 'GRID: A fully location aware routing protocol for mobile ad hoc networks' Telecommunication Systems, vol. 18, no. 1–3, pp. 37–60.

[12]Liao, W.H. Tseng Y.C. Lo K.L. and Sheu J.P. (2000) 'GeoGRID: A geocasting protocol for mobile ad hoc networks bases on GRID' Journal of Internet Technology, vol. 1, pp. 23–32.

[13]Prakash, R. Schiper A. Mohsin M. Cavin D. and Sasson Y. (2004) 'A lower bound for broadcasting in mobile ad hoc networks' Ecole Polytechnique Federale de Lausanne, Switzerland, Tech. Rep. IC/2004/37.

[14] Siva Ram Murthy,C. and Manoj, B.S.(2007) "Ad Hoc Wireless Networks, Architectures and ProtocoL,Second Edition, Low price Edition, Pearson Education.

[15] Special Issue on Wireless Ad Hoc Networks,(1999), IEEE Journal on Selected Areas in Communications.

[16] Scoy, F. L. V and Brooks, J.A. "Broadcasting multiple messages in a grid," Discrete Applied Mathematics,vol.53,1994

[17] Tan Guang. Jarvis Stephen, A. Xue James Hammond, W.J. and Simon D. (2007) 'Distributed Broadcast Scheduling in Mobile Ad Hoc Networks with Unknown Topologies' Parallel and Distributed Processing Symposium, IPDPS 2007 IEEE International, pp. 1 - 7

[18] Wei Lou. and Jie Toward. (2007) 'Toward Broadcast Reliability in Mobile Ad Hoc Networks with Double Coverage' Mobile Computing, IEEE Transactions on mobile computing, Volume 6, Issue 2, pp. 148-163

[19] Yang, X. Liu, J. Zhao, F. and Vaidya, N. H. (2004) 'A vehicle-to-vehicle communication protocol for cooperative collision warning' in Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04), pp. 114–423.

KUMARAGURU COLLEGE OF TECHNOLOGY

(An Autonomous Institution Affiliated to Anna University of Technology, Coimbatore)

COIMBATORE - 641049, TAMIL NADU, INDIA.

CERTIFICATE

CITEL 2011

This is to certify that ~~Mr.~~/Ms. S. SATHIYAPRIYAH, ME (COMMUNICATION SYSTEMS)

ARAGURU COLLEGE OF TECHNOLOGY, COIMBATORE has ~~attended~~ / presented a paper

Identification of a suitable Communication System for a Battle field in

nagement System.

3rd National Conference on **COMMUNICATION, INFORMATION AND TELEMATICS**

EL 2011) on 3rd & 4th March 2011, organized by the Department of Electronics and

mmunication Engineering, Kumaraguru College of Technology, Coimbatore.

3311

eswari Mariappan
HOD - ECE

Dr. S. Ramachandran
Principal

Dr. J. Shanmugam
Director