DEVELOPMENT AND ANALYSIS OF ENERGY EFFICIENT INFRASTRUCTURE-LESS WIRELESS NETWORKS

A THESIS

Submitted in partial fulfilment of the requirements for the award of the degree of

DOCTOR OF PHILOSOPHY

in

PAPER TECHNOLOGY

by

SANDIP VIJAY

DEPARTMENT OF PAPER TECHNOLOGY
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE-247 667 (INDIA)

FEBRUARY, 2011

INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis entitled "**DEVELOPMENT AND ANALYSIS OF ENERGY EFFICIENT INFRASTRUCTURE-LESS WIRELESS NETWORKS**" in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy and submitted in the Department of Paper Technology, Indian Institute of Technology Roorkee, Roorkee is an authentic record of my own work carried out during a period from **July 2007 to Feb. 2011** under the supervision of Dr. S. C. Sharma, Associate Professor, Department of Paper Technology of the Indian Institute of Technology Roorkee, Roorkee.

The matter presented in this thesis has not been submitted by me for the award of any other degree of this or any other institute.

Sandip Vijay

(SANDIP VIJAY)

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

S Sharma

(S. C. Sharma)
Supervisor

Date: 17-02-2011

The Ph. D. Viva-Voce Examination of **Mr. Sandip Vijay**, Research Scholar, has been held on 01-11-2011

S Sharma 01/11/2011
Signature of Supervisor

1/11/11
(Chairman, SRC)

Signature of External Examiner

Sunil Kumar
(Head of the Department)
Chairman, विभागाध्यक्ष
कागज प्रौद्योगिकी विभाग
(भा०प्रौ०सं०रुड़की) सहारनपुर परिसर
सहारनपुर-247001

ACKNOWLEDGEMENT

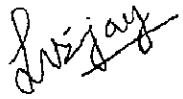
I feel expedient to express my profound indebtedness & deep sense of gratitude and sincere thanks to Dr. S.C. Sharma, Associate Professor, Electronics & Computer Discipline, DPT, Indian Institute of Technology, Roorkee, for their valuable guidance, inspiration, encouragement and whole hearted co-operation in understanding the relevant field and help in presenting this work. Their keen interest and efforts in planning the work in this form can not be expressed in words, as they devote their valuable time in discussions and in critical analysis of the work. I am highly obliged to them. It is a great opportunity to express my respect and gratitude to Dr. Mohan Lal, Assistant Professor, ICC, IIT Roorkee for all his valuable guidance, inspiring discussions, and overall motivation during my Ph.D. I would also like to thank Dr. S.C. Gupta (Emeritus Professor), for providing me with valuable suggestions and guidance during my study. I am extremely grateful to Dr. Satish Kumar, Professor and Head, DPT, IIT Roorkee, for providing necessary administrative help for carrying the work. The author is also thankful to Prof. M.C. Bansal (Ex-DRC Chairman), Prof. A.K. Ray (Ex-HoD) and Prof. A.K. Singh, Chairman, DRC, DPT, IIT Roorkee, whose co-operation and encouragement helped a great deal in this endeavor. I am also thankful to research colleague Mr. Vishal Gupta, Ms. Leena Arya, Dr. S. Quamar, Dr. A. K. Jain, Kumar Manoj, Parmanand, Santosh Kumar, and Dr. Amit Dixit for providing me necessary help to complete this work.

I would like to express my sincere thanks and regards to Dr. Chhaya Sharma, Asstt.Prof, DPT, IIT Roorkee, and her family for giving me morale support and inspiration from time to time.

It is my pleasant duty to acknowledge my thanks to all my well wishers, employees of D.P.T, (Since it is not possible to mention all the names), who support, and inspired me through their love and regards directly or indirectly. I am also thankful to management of Dehradun Institute of Technology, Dehradun for proving me necessary help and support to present this work. No words, no language is ever adequate to express my heartfelt veneration for my respected parents Shri Vijay Kumar Sinha, Smt.Usha Sinha, my brother Sachin Vijay, Nitin Vijay, and specially my wife Mrs. Amrita and my son Mr. Priyanshu, who's indebted sacrifice

and cheerful, enthusiastic, dedicated and unconditional efforts to engage myself in high pursuits.

Above all, I praise the almighty 'God' for his blessings.



Dated: Feb., 2011

(Sandip Vijay)

ABSTRACT

INTRODUCTION

An Infrastructure-less wireless network Viz. Ad-hoc and Sensor consists of independent mobile nodes, a processor, some memory, a wireless radio and a power source. The main standards for decentralized Infrastructure-less wireless networks are IEEE 802.11, Sensor Networks, Low Rate Wireless Personal Area Networks (IEEE 802.15.4), CAN and the Bluetooth (IEEE 802.15.1) specifications for short and medium-range wireless communications. Networking is to support efficient operation in decentralized Infrastructure-less wireless mobile network by incorporating routing functionality into independent mobile nodes. Packets are delivered to destination nodes as per the routing protocols. The energy can be saved at different layers like Physical layer, MAC (Medium Access Control) layer, LLC (Logical Link Control) layer, Network/ Transport layer and Operating System layer.

BACKGROUND OF THE PROBLEM

Several energy efficient/ power aware wireless Infrastructure-less networks routing protocol have been designed to support energy saving by power control. Most of them use a separate control channel, nodes have to be able to receive on the control channel while they are transmitting on the data channel and also transmit on data and control channels simultaneously and a node should be able to determine when probe responses from multiple senders collide. In spite of this, their spatial reuse is less than optimal. Thus there is a great need to identify the new energy efficient protocol for wireless Infrastructure-less networks. Initially the emphasis has been given to understand the different energy efficient routing protocol used at MAC layer and network layer.

Since each node in Infrastructure-less networks will be able to communicate directly with any other node that resides within its transmission range. For communicating with nodes that reside beyond this range, the node needs to use intermediate nodes to relay the messages hop by hop. Thus, there will be a great need for some cryptography scheme, which is suitable to protect us from plaintext attack, equation attack, conspiracy attack and impersonation attack. For clubbing any secure transmission and reception needs extra energy to be consumed. Because of node movement and changing wireless conditions, a wireless Infrastructure-less routing protocol must adapt cryptology technique, which results in more rapid topology change and unsecured transmission.

OBJECTIVE OF THE PRESENT RESEARCH WORK

The objective of the present research work is to analyze the existing energy efficient wireless Infrastructure-less network protocols/ algorithm reported in the literature to modified and developed the algorithm for energy efficient wireless Infrastructure-less network protocol. Further the author has developed and analyzed the cryptography algorithm for secure and attack preventive wireless Infrastructure-less networks. The present work is carried out as follows:

a) Analyze the existing popular energy efficient/ power aware routing algorithm.
b) Development of an optimal path-programming algorithm for decentralized Infrastructure-less wireless network.
c) Development of an energy efficient wireless Infrastructure-less networking (EEN) protocol.
d) Develop and analyze the cryptography algorithm for secure and attack preventive decentralized Infrastructure-less wireless network.
e) Conclusion and Scope for future work.

Analysis of existing popular and energy efficient/ power aware routing algorithm

Infrastructure-less wireless network consumes high-energy because of dynamic topology of network, to retrace of the network and frequent route failure. In the present work the existing power aware and energy efficient routing protocol has been analyzed. The approaches for energy consumption used by these protocols using MAC layer are PAMAS, the power saves in IEEE 802.11 ad-hoc mode, PCMA (Power control multiple access), AFECA, and SPAN (Network layer). The LEACH (Low Energy Ad Hoc Cluster-Head Network) is used both for MAC & Network Layer. The detail analysis has been provided in the thesis by comparing the protocols in terms of methodology, and bottleneck.

Development of an optimal path-programming algorithm for decentralized Infrastructure-less wireless network

This Chapter presents the basic theories of path programming and concepts of graph theory, then lays stress on the study of Dijkstra algorithm for the shortest path problem and describes the process of its realization in detail. Using the concept of graph theory and Dijkstra algorithm, a matrix for the crowded wireless Infrastructure-less network situation has

been created to search the shortest path from one node to any other nodes, the weight values has been find out for the optimal path programming to get the shortest path length.

Development of an energy efficient wireless Infrastructure-less networking (EEN) protocol.

The work reported in this chapter deals with the development of intelligent node for Energy Efficient Wireless Infrastructure-less Network Protocol (EEN), which is based on the few characteristics of SPAN and few of Improved PAMAS by including the allocation of source Id, maintaining list of backbone/ cluster-head and randomized characteristics. The developed algorithm (EEN) adaptively elects backbones / cluster-head from all nodes in the network, and rotates them in time using the essence of SPAN and backbones stay awake and performs multi-hop packet routing within the ad hoc network using Improved PAMAS. While keeping the other nodes remain in power-saving mode and periodically check if they should awaken and become a backbone. With EEN, each node uses a random back-off delay to decide whether to become a backbone (Using author addition of allocation of source ID and maintaining list of backbone / cluster-head). This delay is a function of the number of other nodes in the neighborhood that can be bridge using this node and the amount of energy it has remaining. To identify the unfaithful nodes in the particular geographic region and to control backbone, the author introduced a control mechanism (Using randomized characteristics) from the backbones, which must be fall in the middle of geographical area of complete network. The algorithm has been tested using NS2 for capacity, latency and energy savings and observed that for a practical scenario.

Analysis and development of cryptography algorithm for secure and attack preventive decentralized Infrastructure-less wireless network

This chapter has been divided into two sections. First part presents software model solution, namely *Generic Cryptology Algorithm (GCA),* is based on physical or logical node compromise detecting scheme, while incorporating global node position systems scheme for wireless Infrastructure-less networks. The GCA for wireless Infrastructure-less networks is developed to achieve ad-on security in terms of authentication, integrity, non-repudiation and confidentiality in Wireless Infrastructure-less Network for information interchange. For the development of GCA key management scheme is used for ad-on non-repudiation, availability, interoperability and efficient consumption require for overhead security protocol.

Adrain Perrig algorithm claims to have data confidentiality, two-party data authentication, and evidence of data freshness. It provides authenticated broadcast for severely resource-constrained environments for the networks. In addition to above parameters, the author has considered non-repudiation, availability, interoperability and efficient consumption, require

for overhead security protocol, and developed a GCA, for Wireless Infrastructure-less network. For developing GCA, the object class has been created to accept public key. The GCA public key object generates and distributes the attribute values for the "GCA parameters". Then finally the distribution algorithm for private key generation and decryption has been developed keeping in the view of low overhead for energy efficiency and wireless Infrastructure-less networking.

Now the second part of the chapter describes the Identity-based systems have the property that a user's public key can be easily calculated from his identity by a publicly available function. The bilinear pairing, especially Tate pairing, proved to be a high performance in cryptography. With the foundation of above two properties, the author has developed a new ID-Based (t,n) threshold signature scheme from Tate pairings. The developed scheme is proved secure that it can resist attacks including plaintext attack, recovery equation attack, conspiracy attack and impersonation attack for any wireless networks. The scheme is exceptionally suitable for wireless Infrastructure-less networking, since the Tate pairing and the scalar multiplications easily implemented in ad-hoc networking model. Furthermore, performance analysis has been carried out to check the suitability of ad-hoc environment.

Conclusion and scope for future work.

This chapter paving the way for finding the solution for secure characteristics of mobile devices networking that can use wireless networks almost anywhere and anytime by using one or more wireless networks technologies. These technologies enable the use of infrastructured networks and ad-hoc networks. This Chapters presents the future scope for infrastructure-less networks.

CONTENTS

LIST OF ACRONYMS

ACK	Acknowledgment
ALM	Application layer metrics
AODV	Ad hoc On-demand Distance Vector Routing
AP	Access point
ARQ	Automatic repeat request
ATM	*Asynchronous Transfer Mode*
BB	Black-Burst
BER	Bit error rate
BS	Base station
BSS	Basic Service Set
BWA	Broadband wireless access
BWCM	Bandwidth control management
CBR	Constant bit rate
CBWFQ	Class-based weighted fair queuing
CC	Channel Capacity
CDMA	Code division multiple access
CEDAR	*Core-Extraction Distributed Ad hoc Routing*
CQ	Custom queuing
CSMA/CA	Carrier sense multiple access/ collision avoidance
CTS	Clear-To-Send
CW	Contention window
DCF	Distributed Coordination Function

DIFS	Differentiation Inter Frame Spacing
DLC	Data link layer
DR	Data rate
DS	Distribution system
DSDV	Destination sequenced distance vector
DSR	Dynamic source routing
DSSS	Direct sequence spread spectrum
ESS	Extended service set
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
FEC	Forward error correction
FHSS	Frequency hopping spread spectrum
FIFO	First in first out
FQMM	Flexible QoS Model for MANET
GHz	Giga hertz
HCF	Hybrid coordination function
IAPP	Inter access point protocol
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical & Electronics Engineering
IETF	Internet Engineering Task Force
IF	Intermediate frequency
IMP	Inter-modulation products
IP	Internet Protocol

IR	Infra Red
ISM	Industrial, scientific, medical
LAN	Local Area Network
LLC	Logical link control
MAC	Medium Access Control
MACA/PR	Multiple Access Collision Avoidance with Piggyback Reservation
MANET	Mobile ad hoc network
Mbps	Mega bit per second
MHz	Mega hertz
MLM	MAC layer metrics
NLMs	Network layer metrics
NS-2	Network Simulator-2
OFDMA	Orthogonal Frequency Division Multiple Access
OPNET	Optimized Network Engineering Tools
OSI	Open system interconnection
OSI	Open system interconnection
PCF	Optional Point Coordination Function
PDA	Personal digital assistant
PHB	Per-hop forwarding behaviours
PHY	Physical layer
PKT	Packet
PLR	Packet loss ratio
PMP	Point-to-multipoint

PQ	Priority queuing
QoS	Quality of Service
RF	Radio frequency
RREP	Route reply
RREQ	Route request
RSVP	Resource Reservation Protocol
RT	Reservation table
RTP	Real-Time Protocol
RTS	Request-To-Send
SINR	Signal-to-interference plus noise power ratio
SS	Subscriber stations
STA	Stations
TCP	Transfer Control Protocol
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
UDP	User Datagram Protocol
UNII	Unlicensed National Information Infrastructure
WDS	Wireless Distribution System
WFQ	Weighted fair queuing
Wi-Fi	Wireless-Fidelity
WiMAX	Worldwide interoperability for microwave access
WLAN	Wireless Local Area Network
WRR	Weighted Round-Robin

LIST OF FIGURES

LIST OF TABLES

Glossary

Packet delivery ratio: Packet delivery ratio is the ratio of the number of data packets actually delivered to the destination to the number of data packets supposed to be received. This number presents the effectiveness of the protocol.

Average end-to-end delay: This indicates the end-to-end delay experienced by packets from source to destination. This includes the route discovery time, the queuing delay at node, the retransmission delay at the MAC layer and the propagation and transfer time in the wireless channel.

Throughput: This is average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per seconds (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

Retransmission: It is the resending of packets which have been either damaged or lost. It is a term that refers to one of the basic mechanisms used by protocols operating over a packet switched computer network to provide reliable communication (such as that provided by a reliable byte stream for example TCP)

Delay: It refers to a lapse of time.

Latency: Latency is a measure to time delay experienced in a system, the precise definition of which depends on the system and the time being measured.

Jitter: In computer networking, packet delay variation is the difference in end-to-end delay between selected packets in a flow with any lost packets being ignored. The effect is sometimes, incorrectly, referred to as jitter.

List of Publication Based on Work

REFERRED INTERNATIONAL/NATIONAL JOURNALS

1. **Vijay Sandip** , Sharma S. C. "A Secure Gateway Solution for Wireless Ad-Hoc Networks" ***International Journal of Computer Science and Applications (IJCSA)***, (ISSN:0972-9038), Vol.5 No.4, Pp: 26-44; December 31, 2008.

2. **Vijay Sandip,** Sharma S. C. "SV's Energy Efficient Network Design for Real Time Wireless Networks for Unmanned Blimp" ***IAENG - International Association of Engineers LS*** (ISBN:978-988-98671-9-5), WCE, London, U.K., Vol-36 III, Pp: 1745-1750, July 04, 2008.

3. **Vijay Sandip,** Sharma S. C. " Secure Cryptology Algorithm (SCA) for Wireless Ad-hoc Sensor Network" ***International Transactions on Computer Science and Engineering*** GESTS, USA, ISSN: 1738-6438, ISBN: 89-953729-5-8, Vol. 49, No. 1, Pp: 13-28, October 30, 2008.

4. **Vijay Sandip,** Sharma S. C. "A WSN for Distributed Fault Management in Power Systems" ***IAENG - International Association of Engineers LS*** (ISBN:978-988-98671-9-5), WCE, London, U.K., Vol-36 III, 2008, Pp: 1869-1874, July 04, 2008.

5. **Vijay Sandip,** Sharma S. C. "Computer Controlled Wireless Ad-hoc Networks for Blimp-SVEEN Application" ***International Journal of Intelligent Information Processing (IJIIP)***, ISSN:0973-3892; Vol.2, No.2,Pp: 133-144, December 01, 2008.

6. **Vijay Sandip,** Sharma S. C." The QPSK Modulated Signal Using the Improved ISI–JF Pulse for Digital Wireless Ad Hoc Communications" ***Annual Review of Communications***, International Engineering Consortium, USA, ISBN: 1-931695-92-X , ISBN: 978-1-931695923, Vol.61, Pp: 393-397, December 01, 2008.

7. **Vijay Sandip,** Sharma S. C. "Energy Efficient Parameters for Controlling Physical Layer of Mobile Ad-hoc Networks " ***International Transactions on Computer Science and Engineering*** GESTS, USA, ISSN: 1738-6438, ISBN: 89-953729-5-8, Vol. 49, No. 1,Pp: 13-28; October 30, 2008.

8. **Vijay Sandip,** Sharma S. C." SVEEN Model Design Application for Real Time Wireless Networks for Unmanned Machine" ***International Journal of Intelligent Information Processing (IJIIP)***, ISSN:0973-3892; Vol.2, No.2, Pp: 145-158,

December 01, 2008.

9. **Vijay Sandip,** Sharma S.C., "Energy Efficient Approach for Emergency Readiness Communications in Wireless Ad-hoc Networks" ***International Journal of Recent Trends in Computer Science,*** Academy Publisher, ACEEE, Finland, [ISBN 978-952-5726-04-6 (Print); ISBN 978-952-5726-05-3 (CD-ROM)], Vol.1(1), Pp:183-187;2009.

10. **Vijay Sandip**, Sharma S.C., "Research Reviews of IEEE 802.11 Wireless Ad-hoc Networks" ***International Journal of Recent Trends in Engineering,*** Academy Publisher, ACEEE, Finland, [ISBN 978-952-5726-04-6 (Print); ISBN 978-952-5726-05-3 (CD-ROM)], Vol.1 (2), Pp:233-235; 2009.

11. **Vijay Sandip**, Sharma S.C., "Optimal Secure Shortest Path Algorithm in Wireless Ad-hoc Networks under Complex Environment" ***Journal of Combinatronics Information and System Sciences,*** France, Vol. 21, No.3, Pp:34-40; 2009.

12. **Vijay Sandip**, Sharma S. C, "TSS based identity matrix for wireless Ad-hoc networks", ***Journal of Combinatronics Information and System Sciences***, France, Vol. 21, No.5, Pp:17-22;2009.

13. **Vijay Sandip**, Sharma S.C.,, "A secure identity based Threshold Signature Scheme Cryptography for Wireless Ad-hoc Computing" ***Journal of Scientific & Mathematical Research*** **, NASA**, USA Vol. 10, No.3,Pp: 13-19; 2010.

14. **Vijay Sandip**, Sharma S.C.,, " SVEEN: A Comparative Energy Efficient Ad Hoc Wireless Networks " ***IEEE Cad. Journal of Electrical & Computer Engineering***, IEEE Canada, under final Publication Review stage (Revised final manuscript submitted), (paper Id#2026), 2010.

PEER-REVIEWED INTERNATIONAL CONFERENCE

1. **Vijay Sandip** , Sharma S.C., "SVEEN: A Comparative Energy Efficient Ad Hoc Wireless Networks" Proceeding of International Conference on Intelligent Systems & Networks (ISN-2008), Kalawad, Y. Nagar, Pp:236-243 Feb. 22-24,2008

2. **Vijay Sandip** , Sharma S.C. "An Analysis Of Energy Efficient Communication In Ad-hoc WLAN's (802.11b)" Proceeding of ***IEEE Computer Society***, ICETET-2008 © IEEE, Nagpur, Pp: 140-144, July 16-18,2008,.

3. Sharma S.C., **Vijay Sandip**, Gupta Vishal "Fuzzy Model Approach for reduction of Path Loss" Proceeding of Fourth IEEE Conference on Wireless Communication and Sensor Networks (WCSN-2008), IIITA & DAVV, Indore, ***IEEE Press*** Catalog Number. CFP0875D, ISBN: 978-1-4244-3328-5, Library of Congress: 2008909475, Pp: 126-132; Dec. 27-29, 2008.
4. **Vijay Sandip** and Sharma S.C. "EEN: A Energy Efficient Multi-hop Ad Hoc Wireless Networks" Proceeding of ***IEEE Computer Society***, ICETET-2008 © IEEE, Nagpur, Pp: 145-151; July 16-18,2008.
5. **Vijay Sandip**, S. C. Sharma "A Power Saving Scheme For Wireless Sensor Networks" Proceeding of IEEE -**C**onference on **C**ommunication, **C**onvergence and **B**roadband **N**etworking (ICCBN), © ***IEEE Press***, Indian Institute of Science, Bangalore, Pp:17-24;17 - 20 J u l y 20 08.
6. **Vijay Sandip**, Sharma S. C. " Secure Routing Algorithm for Wireless Ad-hoc Sensor Networks" Proceeding of Advanced Computing and Communication Technologies (ICACCT-2008), Panipat, ISBN- 81-87433-68-X, Pp:688-693 Nov. 08-09, 2008.
7. **Vijay Sandip**, Sharma S. C., Gupta Vishal "Unrestricted Cipher Algorithm (UCA) for Energy Efficient Secure Wireless Ad-Hoc Sensor Network" Proceeding of Fourth IEEE Conference on Wireless Communication and Sensor Networks (WCSN-2008), IIITA & DAVV, Indore, ***IEEE Press*** Catalog Number. CFP0875D, ISBN: 978-1-4244-3328-5, Library of Congress: 2008909475, Pp: 274-279 Dec. 27-29, 2008.
8. **Vijay Sandip**, Sharma S.C. Threshold Signature Cryptography Scheme in Wireless Ad-Hoc Computing" ***Springer-Verlag Berlin Heidelberg***, , CCIS 40, Pp. 327–335, 2009 in Proc. of IC3 2009.
9. **Vijay Sandip**, , Sharma S.C. "Energy Efficient Approach for Emergency Readiness Communications in Wireless Ad-hoc Networks" ***IEEE Computer Society*** press for IEEE International Advanced Computing Conference 2009, Thapar University, Patiyala, (IACC'09) Pp:1248-1251. March 6-7, 2009.
10. **Vijay Sandip**, Sharma S.C., "OPSSP Algorithm in Wireless Ad-hoc Networks under Complex Environment", International Conference of Forum for Interdisciplinary Mathematics on Interdisciplinary Mathematical and Statistical Techniques, JUIT, Waknaghat, Pp:34-40; 2009.
11. **Vijay Sandip**, Kumar Santosh*, Sharma S. C "A WSN based Efficient Power Routing Protocol " Proceeding of Advanced Computing and Communication Technologies

(ICACCT-2008), Panipat, ISBN- 81-87433-68-X, Nov. 08-09, 2008, Pp:415-419.

12. **Vijay Sandip***, Sharma S. C., Gupta Vishal " SVEEN Model Design Application for Real Time Wireless Networks for Blimp Machine" Proceeding of Advanced Computing and Communication Technologies (ICACCT-2008), Panipat, ISBN- 81-87433-68-X, Nov. 08-09, 2008, Pp:445-449.

13. **Vijay Sandip***, Qamar S., Gupta Vishal, Sharma S. C. " Secure Routing Algorithm for Wireless Ad-hoc Sensor Networks" Proceeding of Advanced Computing and Communication Technologies (ICACCT-2008), Panipat, ISBN- 81-87433-68-X, Nov. 08-09, 2008, Pp:688-693.

14. Gupta Vishal*, **Vijay Sandip**, Sharma S.C.," Efficient Path Loss Prediction In Mobile Wireless Communication Network" MWON 2008 - ***International Conference on Mobile, Wireless and Optical Communications Networks***, Bangkok, Thailand, December 17-19, 2008, Pp: 1180-1183.

15. **Vijay Sandip**, Gupta Vishal, Sharma S.C. "Energy Efficient Approach for Emergency Readiness Communications in Wireless Ad-hoc Networks" Proc. Of ***IEEE Computer Society press*** for IEEE International Advanced Computing Conference 2009, Thapar University, Patiyala, (IACC'09) on March 6-7, 2009, Pp:1248-1251.

16. **Vijay Sandip**, Sharma S.C. Threshold Signature Cryptography Scheme in Wireless Ad-Hoc Computing" ***Springer-Verlag Berlin Heidelberg***, 2009 in Proc. of IC3 2009, CCIS 40, pp. 327–335.

PEER REVIEWED INTERNATIONAL/NATIONAL BOOK CHAPTERS

1. "Energy Efficient Parameters for Controlling Physical Layer of Mobile Ad-hoc Networks" by **Vijay Sandip**, Kumar Manoj, and S. C. Sharma in ***"Information Technology: Emerging Trends"*** 1st ed. New Delhi, Vitasta Publishing Pvt. Ltd. 2009. *(ISBN: 8189766406 KK-70675),*

   http://www.kkagencies.com/toc/70675.htm.

2. "SVEEN: Loss Rate Measurement in Ad-hoc Wireless Networks" by **Sandip Vijay,** Kumar Manoj, and S. C. Sharma in ***"Information Technology: Emerging Trends"*** 1st ed. New Delhi, Vitasta Publishing Pvt. Ltd. 2009. *(ISBN: 8189766406 KK-70675);* http://www.kkagencies.com/toc/70675.htm.

3 **Vijay Sandip**, Sharma S. C., "A Study on Secure Characteristics of Wireless Ad-hoc Networks" ***IGI Publication-Emerging Topics And Technologies In Information Systems,*** [ISBN 1605662224, 9781605662220]. By Miltiadis D. Lytras, Patricia Ordonez De Pablos Published by Idea Group Inc (IGI), *USA, Pp.115-136,* 2009.

HONORS' & BEST PAPER AWARD

2007: [***[Best Paper Award]*** National Conference on Emerging Technologies in Computer Science (ETCS-2007) held at MIET, Meerut, (AICTE- New Delhi) Sept. 2007.

2008: ***[Best Paper Award]*** Eighteenth International Conference of Forum for Interdisciplinary Mathematics on Interdisciplinary Mathematical and Statistical Techniques, JUIT, Waknaghat, 2009.

CHAPTER-1

INTRODUCTION

Chapter-1

INTRODUCTION

1.1 BACKGROUND & MOTIVATION

Mobile devices, such as laptop computers, Pocket PCs, cellular phones, etc., are now easily affordable, and are becoming more popular in everyday life [1,2]. At the same time, network connectivity options for mobile hosts have grown tremendously, as the support for wireless networking products based on radio and infrared has been greatly increased over the past few years. With the availability of mobile computing devices, mobile users have a natural tendency to share information between them. Often mobile users want to have a meeting, even though it is not planned in advance and there is no Internet connection available. For instance, there may be situations that employees find themselves together in a meeting room, or friends or business acquaintances may encounter each other in an airport terminal, or some scholars and researchers may meet in a hotel ballroom for a conference or workshop. In those situations, requiring each user to connect to a wide-area network to communicate with each other may not be convenient or practical because of the lack of Internet connectivity or because of the time or cost required for such a connection.

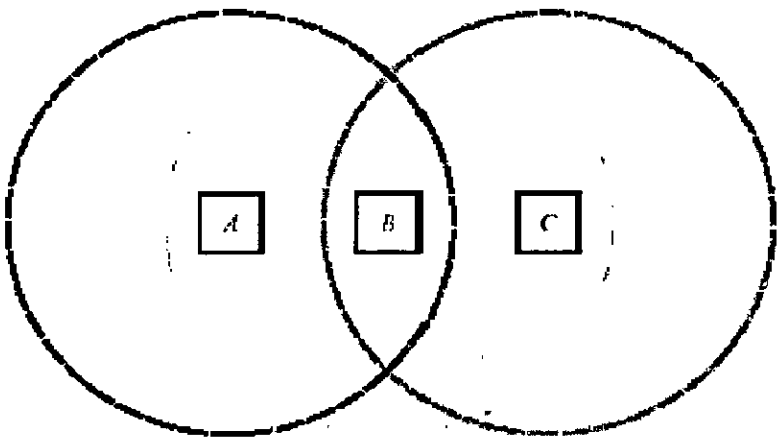


Fig. 1.1 An Infrastructure-less Networks with three wireless mobile hosts

Popularity of Infrastructure-less mobile devices along with the presence of Infrastructure-less networks has contributed to recent advances in the field of

mobile computing in wireless Infrastructure-less networks. Mobile Infrastructure-less networks have been mostly utilized in military environments. Pocket PCs communicate wirelessly with each other using the IEEE 802.11b technology without the use of an infrastructure. The recent advances in Infrastructure-less network technology now introduce the verity of new class of applications. Wireless Infrastructure-less networking is easy to configure in robust environment.

Several energy efficient/ power aware wireless Infrastructure-less networks routing protocol have been designed to support energy saving by power control. But most of them use a separate control channel, nodes have to be able to receive on the control channel while they are transmitting on the data channel and also transmit on data and control channels simultaneously and a node should be able to determine when probe responses from multiple senders collide. In spite of this, their spatial reuse is less than optimal. Thus there is a great need to identify the new energy efficient protocol for wireless Infrastructure-less networks. Since each node in Infrastructure-less networks will be able to communicate directly with any other node that resides within its transmission range [14, 16]. Infrastructure-less networks are not secure while communicating with nodes that reside beyond the range, the node needs to use intermediate nodes to relay the messages hop by hop for multi-hop communication. Thus, there are number of issues and challenges related to secure communication, so, there will be a great need for some cryptography scheme, which is suitable to protect us from plaintext attack, equation attack, conspiracy attack and impersonation attack.

1.2 ISSUES IN WIRELESS INFRASTRUCTURE-LESS NETWORKS

The flexibility and convenience of Infrastructure-less networks come at a price. The multi-hop nature and the lack of fixed infrastructure add the complexities and design constraints in Infrastructure-less networking [15]. Wireless Infrastructure-less networks has the following challenges:

- Limited wireless transmission range and channel capacity
- Broadcast nature of the wireless medium

- Packet losses due to transmission errors
- Mobility-induced route changes
- Mobility-induced packet losses
- Battery constraints
- Potentially frequent network partitions
- Ease of snooping on wireless transmissions (security hazard)
- Energy Saving

Limited wireless transmission range and channel capacity [15]

Wireless Infrastructure-less networks is used to obtain information from the surrounding areas and collected data is reported to the base station through wireless links. In certain scenarios ongoing transmissions within the network need to be concealed so that no information is leaked beyond a vulnerable area. Such a concealment effort necessitates transmit ranges of radios to be limited. However, limiting transmit ranges results in sub-optimal routing patterns within the network, which results in lower network lifetime. Due to their portability and their deployment in potentially harsh scenarios, nodes in Infrastructure-less networks are usually powered by batteries with finite capacity. It is always desirable to extend the lifetime of Infrastructure-less network nodes without sacrificing their functionality. Thus, the study of energy-efficient mechanisms is of significant importance. In wireless Infrastructure-less networks, the major energy consumption at each node is due to system operation, data processing, and wireless transmission and reception.

A packet radio network consists of a number of packet radio stations that communicate with each other. A packet radio network carries messages in packets like a wired packet network, but uses radio signals instead of wires to carry the packets between stations. Basically a station in a packet radio network includes radio transmitting and receiving equipment and a computer to perform packet routing and forwarding functions. In a multi-hop packet radio network each station participates cooperatively in forwarding traffic between other stations. Compared to wired networks, radio networks are much cheaper to install and provide a user a

chance of mobility. With multiple short hops link quality improves and stations can use less power or achieve better data rates. On the other hand, there are several differences in the access medium, as with radio signals propagation, interference, frequency band choices, and such things have to be considered more carefully. Also real support of mobility and power consumption are important issues, when considering radio transmission.

In theory multi hop wireless radio networks, also known as ad hoc networks provide more capacity than traditional radio networks.

Fig. 1.2 compares the theoretical scalability of multi hop wireless radio to the scalability of a point-to-multipoint radio. The capacity refers to the total capacity of the network. Multi hop wireless networks can in theory scale linearly with the amount of nodes, when multiple antennas are used in each node. This means in practice that the transmission speed available to each node remains constant. Even with single antennas the capacity grows in proportion to $\sqrt{N}$, where N is the number of nodes, leaving a capacity of $1/\sqrt{N}$ to each node [15]. With IEEE 802.11b WLAN the total capacity actually decreases according to Gupta, Gray and Kumar [16], due to sub optimal design of the MAC layer. The capacity comparison between PTM (Point- to-Multipoint) radio, BLAST – a multiple antenna ,ad Hoc theory using single antenna and IEEE802.11b ad Hoc has been compared in figure 1.2.

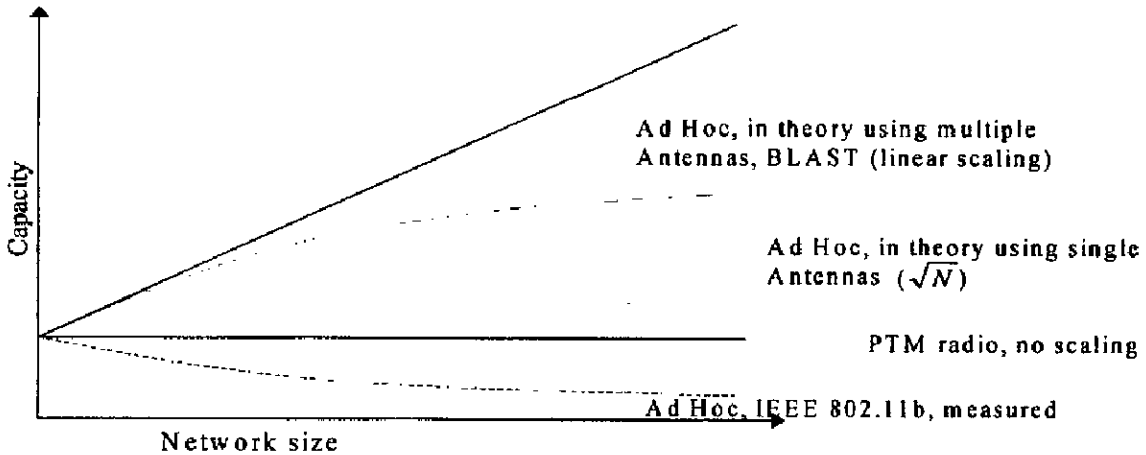


Fig. 1.2 Comparison of theoretical and real-life performance of ad hoc networks [15,16]

Broadcast nature of the wireless medium [15]

Wireless channels differ from their wire-line counterparts. The broadcast nature of the wireless medium has been studied from the point of view of channel capacity (described above), when security considerations become paramount, a whole new set of interesting and crucial issues need to be addressed regarding the broadcast medium. Specifically, the broadcast nature allows jammers to effectively disrupt wireless network communications with clever strategies that use minimal jammer resources. This denial of service can be made catastrophic by utilizing semantic information in the Medium Access Control layer. The broadcast nature also means that eavesdroppers can hear transmissions without much effort, raising privacy concerns. However, at the same time, the broadcast medium allows innovative security measures, such as a recently introduced, innovative, information-theoretically secure, key generation mechanism. This project is investigating denial-of-service at the MAC layer. An intelligent jammer could cleverly utilize the semantics of the data transmission, by interpreting the packet-on-the-air and deciding its relative importance, and carry out a jamming attack at the MAC-layer. In the context of CSMA/CA, the jammer could detect the transmission of valuable RTS control packets, and jam such crucial information-bearing packets, to prevent other users from accessing the channel. Due to the random back-off, this creates a cascade effect, which will waste a large bandwidth. We are investigating intelligent jamming attacks in the link layer, quantifying the loss of throughput caused, and designing protocols which are resistant to such attacks. The project is also investigating the topic of privacy and information-theoretic security in the presence of eavesdroppers. The approach uses multiple antennas and possibly other resources to degrade the eavesdropper's channel, while not affecting the channel of the legitimate receiver. This results in secure communication between the transmitter and the legitimate receiver.

Packet losses due to transmission errors [6]

Infrastructure-less 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].

Mobility-induced route changes [17]

The network topology in an Infrastructure-less 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 Infrastructure-less networks.

Mobility-induced packet losses [17]

Communication links in an Infrastructure-less networks are unstable such that running conventional protocols for MANETS, VANETS, WSN and ad hoc over a high loss rate will suffer from severe performance degradation. However, with high error rate, it is very much difficult to deliver a packet to its destination.

Battery constraints [18]

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 MANETS, VANETS, WSN and ad hoc nodes has to optimally use this resource.

Potentially frequent network partitions [7]

The randomly moving nodes in an Infrastructure-less networks can lead to network partitions. In major cases, the intermediate nodes are the one which are highly affected by this partitioning.

Ease of snooping on wireless transmissions (security hazard) [19]

The radio channel used for Infrastructure-less 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. Here the requirement of confidentiality can be violated if an adversary is also able to interpret the data gathered through snooping [6].

Energy Saving [1-12]

Based on the literature surveys [1-12], it is easy to find out the thrust area for saving energy as shown in figure 1.3 in wireless Infrastructure-less networks at the following cross layers:

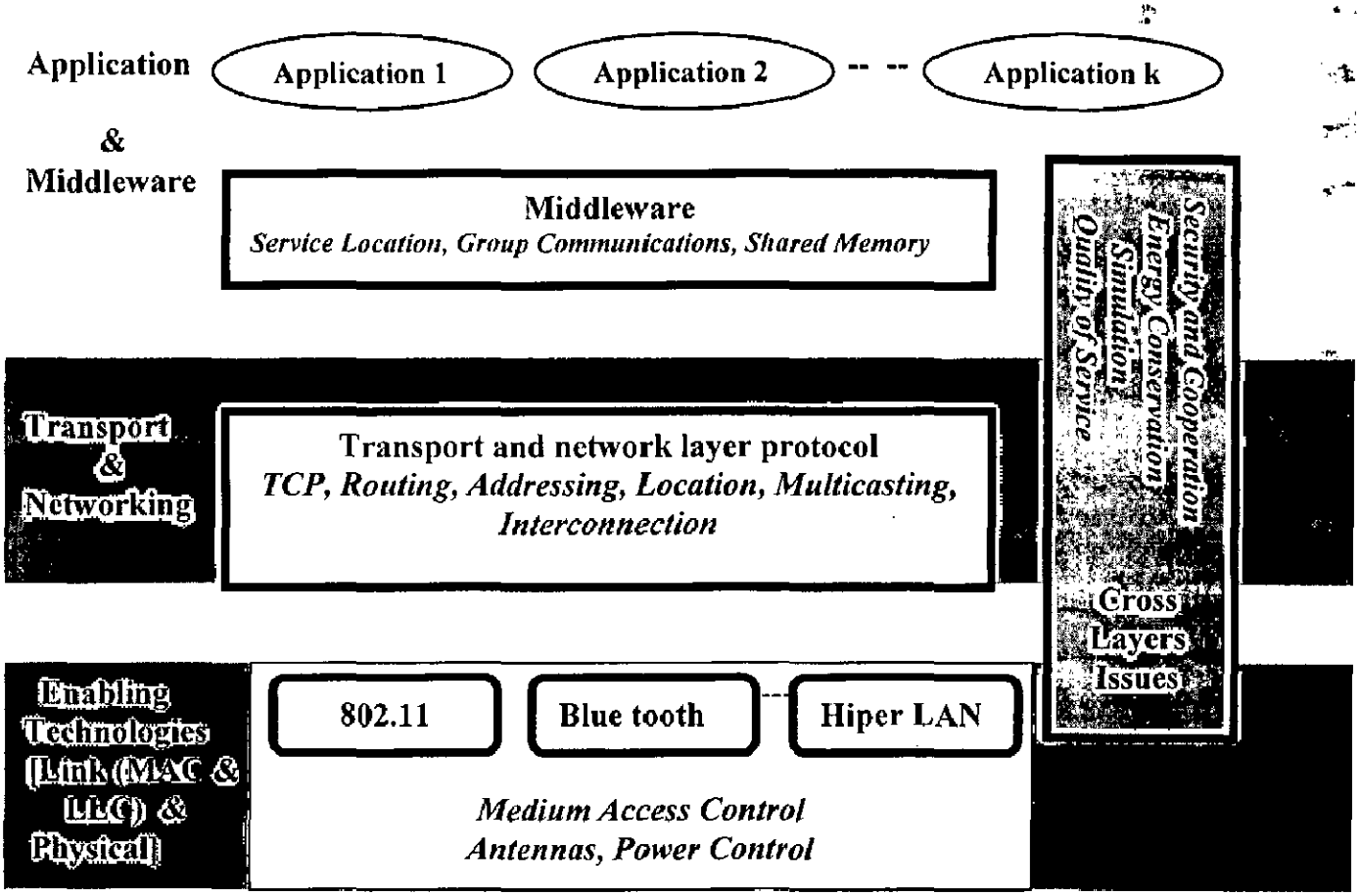


Fig. 1.3 Cross layer issues raising the section of energy conservation, QoS and security.

- *Physical layer* - At the lowest level an energy-efficient radio that has been used in various operating modes (like variable RF power and different sleep modes) such that it allows a dynamic power management. Energy can be saved by adapting suitable modulation techniques and basic error-correction schemes [11]. The bandwidth of a radio also influences its energy consumption [11].

- *Medium access layer* - In an energy-efficient MAC protocol the basic objective is to minimize the time the radio needs to be powered. Since the overhead introduced due to state transitions is also significant, minimizing the number of transitions also reduces energy consumption [3]. Scheduling data transfers in bulk, an inactive terminal is allowed to doze and power off the receiver. Due to this the network interface must be re-activated at a scheduled time. Transceiver unsuccessful actions due to collisions and errors should be avoided, and the protocol should adapt to the dynamic environment [1,2].

- *Logical link control layer* - Due to the dynamic nature of wireless networks, *adaptive error control* can give significant gains in effective bandwidth and energy efficiency. This avoids applying error-control overhead to connections that do not need it, and it allows to selectively matching the required *QoS* and the conditions of the radio link. Above these error-control adaptations, a slot scheduler in the base-station can also adapt its traffic scheduling to the error conditions of wireless connections of a mobile. The scheduler can try to avoid periods of bad error conditions by not scheduling non-time critical traffic during these periods [4]. *Flow control mechanisms* are needed to prevent buffer overflow, but also to discard stale packets. Depending on the service class and *QoS* of a connection, different flow control energy consumption. For instance, in a video application it is useless to transmit images that are already outdated.

- *Network/ Transport layer* - Errors on the wireless link can be propagated in the protocol stack. In the presence of a high packet error rate and network

protocols (such as TCP) may overreact to packet losses, mistaking them for congestion. TCP responds to all losses or drop by invoking congestion control and avoidance algorithms [5]. These measures result in unnecessary increases in energy consumption and deterioration of *QoS* [5,6]. The congestion control during packet errors. These schemes choose from a variety of mechanisms to improve end-to-end throughput, such as local retransmissions, split connections and forward error correction [8,9].

- *Operating system level* - Another way to avert the high cost (i.e. performance, energy consumption or money) of wireless network communication is to avoid use of the network when it is expensive by predicting future access and fetching necessary data when the network is cheap [10]. In the higher level protocols of a communication system caching and scheduling can be used to control the transmission of messages. The works in particular well when the computer system has the ability to use various networking infrastructures, with varying and multiple network connectivity and with different characteristics and costs [7].

To reduce the power consumption in infrastructure-less networks, there is great need to develop an energy efficient network which preserves the energy at different layers. However, it is not possible to incorporate energy efficient network design in more than one layer at a time. The present research work has given emphasis on the development of energy efficient network protocol above the MAC layer and below the network layer.

1.3 OBJECTIVE OF THE PRESENT RESEARCH WORK

The objective of the present research work is to analyze the existing energy efficient wireless Infrastructure-less network protocols/ algorithm reported in the literature and modified the algorithm for energy efficient wireless Infrastructure-less network protocols. Further, to develop and analyze the cryptography algorithm for

secure and attack preventive wireless Infrastructure-less networks. The present work is carried out as follows:

a) Analyze the existing popular energy efficient/ power aware routing algorithm.
b) Development of an optimal path-programming algorithm for decentralized Infrastructure-less wireless network.
c) Development of an energy efficient wireless Infrastructure-less networking (EILN) protocol.
d) Develop and analyze the cryptography algorithm for secure and attack preventive decentralized Infrastructure-less wireless network.
e) *Conclusion and Scope for future work.*

1.4 SIMULATION TOOLS USED FOR PRESENT WORK

The simulation part is an important work to design, develop and test the networks. It is available under Linux/ Cygwin (for window environment) , with a GPL license. The details of NS-2 are given below:

About Network Simulator: NS-2:

NS2 is a network simulator; built with C++ and TCL. It has been developed in the California University, by LBL, Xerox PARC, UCB, and USC/ISI through the VINT project supported by DARPA (Defense Advanced Research Project Agency, USA). Nowadays, this simulator is used around the world, because of the GPL license, and because it is a powerful simulator [11].

The simulator is composed of two parts:

i. The TCL code: it is used to communicate with the simulator, and permits to define different simulation parameters.
ii. The C++ code: it is the main part of the NS project, because it defines how the simulator has to behave

There are two kinds of interaction with the C++ code:

a) The first one is with TCL files, which can describe the initial conditions. It can also describe some events, like the change of speed for example.

b) The second one is the generation of events by the C++ code itself.

The C++ code produces some output files, which contain different types of results from the simulation.

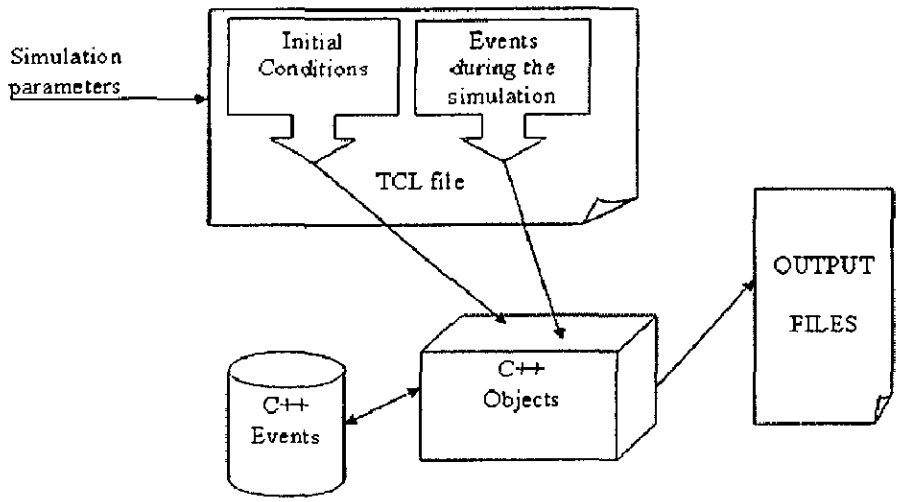


Fig. 1.4 NS2 Simulation Architecture

TCL: The Scenario Interface:

The main reason for using a TCL language in ns2 is because it is not useful to use only C++ code. In fact, by this mean, the user does not need to compile the simulator every time he wants to do a new simulation. The TCL language is interpreted by the C++ code in ns2, without being compiled.

To use a network simulator, we have to define two things:

a) How does the protocol behave? It is done by the C++ code, because it does not change for every simulation

b) What are the simulation parameters? It is done by the TCL code, because every simulation is different (number of nodes, positions, speeds, protocol used)

The TCL code allows the user to choose between fixed or wireless network, and among the different implemented protocols: DSDV, AODV, DSR, TORA (for wireless networks). The TCL file contains also information about nodes like position and speed, or information's about source and destination, the transmission rate, and a lot of other parameters.

The C++ Code:

Like C++, TCL is an object oriented language. The main purpose of the C++ code is to define how the simulator works, independently from the simulation

parameters, and the results depend only on different initial conditions. For instance, some C++ objects represent the different layers of the different nodes in the simulation. The simulation runs with a specific simulation time. Then, by sending packets, C++ objects creates some events: they want that one C++ object receives one packet at a time, by introducing a delay for example. But because NS-2 is a mono process program, there is a table, containing all the events and sorting them according to the time they occur. For the analysis point of view, we have used network simulation tool NS-2 [11].

1.5 ORGANIZATION OF THE THESIS

This thesis explores the secure and optimized energy efficient wireless Infrastructure-less networks that appeared in the literature and to explore the possibility of enhancements in the existing energy efficient wireless Infrastructure-less networking. This thesis analyzes the existing popular energy efficient/ power aware routing algorithm in chapter 2 to develop an optimal path programming algorithm for energy efficient for wireless Infrastructure-less networks described in chapter 3. It develops an energy efficient wireless Infrastructure-less networking (EILN) protocol and compares the developed protocol with popular existing protocols described in chapter 4. It also analyzes and developed the security aspects model algorithm in chapter 5 for secure and optimized energy efficient wireless Infrastructure-less networks and finally it find the Conclusion and Scope for future work.

CHAPTER-2

ANALYZE THE EXISTING POPULAR ENERGY EFFICIENT / POWER AWARE ROUTING ALGORITHM

Chapter -2

ANALYZE THE EXISTING POPULAR ENERGY EFFICIENT/ POWER AWARE ROUTING ALGORITHM

2.1 INTRODUCTION

The wireless networking environment presents formidable challenges to the study of broadcasting (one-to-all) and multicasting (one-to-many) problems, especially when energy-efficient operation is required. To address the specific problem of energy- efficient wireless infrastructure-less networks, the study of cross-layer communication approach is important. This section elaborates the similarities and differences between energy-limited and energy-efficient modes of operation, and illustrates the impact of these overlapping (and sometimes conflicting) considerations on network operation.

In energy efficient mode, Energy is a cost (e.g., to replace batteries) and Minimizing energy to achieve given communication goals is the main issue. In energy-constrained, Energy is a constraint means a node dies when its energy is depleted (i.e. Sensor networks, ad hoc networks in which batteries can't be recharged or replaced). Our goals are to maximize network's useful lifetime and to maximize quantity of data delivered to destinations. However, Optimizing energy efficiency does not guarantee good performance in energy-constrained applications.

Wireless connectivity with mobility support has become an important issue in the modern computing infrastructure. Especially, *mobile ad hoc networks* (MANETs) [20,21] attract a lot of attention with the advent of inexpensive wireless LAN solutions such as *IEEE 802.11*[22], *HIPERLAN* [23] and *Bluetooth* [24] technology. Since they do not need communication infrastructure in their basic forms and utilize the unlicensed *ISM (Industrial, Scientific, and Medical)* band, they are likely to be rapidly adopted. Applications of wireless infrastructure-less networks encompass various areas including home-area wireless networking, on-the-fly conferencing, disaster recovery, wireless sensor networks [25], and *GSM*

(Global System for Mobile Telecommunications) service extension covering dead spots [26]. Multicasting has been extensively studied [19] for wireless infrastructure-less networks because it is fundamental to many ad hoc network applications requiring close collaboration of the member nodes. A multicast packet is delivered to multiple receivers along a network structure such as a *tree* or *mesh,* which is constructed once a multicast group is formed. However, the network structure is fragile due to node mobility and, thus, some members may not be able to receive the multicast packet. In order to improve the *packet delivery ratio,* multicast protocols for wireless infrastructure-less networks usually employ control packets to refresh the network structure periodically. It has been shown that *mesh-based protocols* are more robust to mobility than *tree-based protocols* [27], due to many redundant paths between mobile nodes in the mesh. However, multicast mesh may perform worse in terms of energy efficiency because it uses costly broadcast-style communication involving more forwarding nodes than multicast trees. Another important aspect of energy efficiency is balanced energy consumption among all participating mobile nodes. In order to maximize the lifetime of a wireless infrastructure-less networks, care has to be taken not to unfairly burden any particular node with many packet-relaying operations. Node mobility also needs to be considered along with energy balancing. The rest of the chapter is organized as follows. Multicasting for wireless infrastructure-less networks is discussed in Section 2.2. Section 2.3 investigates research reviews on popular energy efficient multicast protocols for wireless infrastructure-less networks and analyzes energy efficiency assuming a static ad hoc network in a tabular form. Finally, concluding remarks are in Section 2.4.

2.2 MULTICAST PROTOCOLS FOR WIRELESS INFRASTRUCTURE-LESS NETWORKS

This section briefly overviews the literature survey on` multicast protocols targeting MANETs. They can be largely categorized into two types, *tree-based multicast* and *mesh-based multicast,* based on the multicast structure. Tree-based multicast is generally used in wired and infrastructured mobile networks (i.e., mobile networks

with base stations), as well as in MANETs. Depending on the number of trees per multicast group, tree-based multicast can be further classified as *per-source tree multicast* and *shared tree multicast.*

A new approach unique to MANETs is the *mesh-based multicast* [39-42]. A mesh is different from a tree since each node in a mesh can have multiple parents. Using a single mesh structure spanning all multicast group members, multiple paths exist and other paths are immediately available when the primary path is broken. This avoids frequent network reconfigurations, resulting in the minimization of disruption of ongoing multicast sessions and reduction of the overhead in implementing the protocol. However, care must be taken to avoid forwarding loops when multicast data are forwarded in a multicast mesh.

Tree-Based Multicast [30-37]

As mentioned earlier, there are two versions of tree-based multicast in a MANET: *per-source tree* and *shared tree multicast.* Per-source based tree is established and maintained for each multicast source node of a multicast group. The advantage is that each multicast packet is forwarded along the most efficient path from the source node to each and every multicast group member. However, this method incurs a lot of control overhead and cannot quickly adapt to the movements of the nodes in a MANET [31].

On the other hand, shared tree multicast is a more scalable approach than the per-source tree approach. Instead of building multiple trees for each multicast group, a single shared tree is used for all multicast source nodes. Multicast packets are distributed along this shared tree to all members of the multicast group. To establish a shared tree, a special node is designated as a *core node,* which is responsible for creating and maintaining the shared tree. Hence, a *core selection algorithm* is used [33]. The established shared tree can be either *unidirectional* or *bidirectional.*

In a unidirectional shared tree, multicast packets must be unicast to the core node, which is the root of the tree. From the core node, the multicast packets are distributed along the shared tree until they reach all the multicast group members.

However, in a bidirectional shared tree, multicast packets can enter the shared tree at any point, and they are distributed along all the branches of the shared tree. The shared tree approach has lower control overhead, but the path is not necessarily optimal, i.e., the path from a multicast source to a receiver is not necessarily the shortest. Furthermore, in a dynamic network, throughput can be deteriorated dramatically unless the core node and shared tree quickly adapt to the node mobility.

Figure 2.1 shows an example of a shared unidirectional tree multicast. The tree consists of a root node *(r)*, four intermediate forwarding nodes *(p, q, s,* and *t)*, seven receiver nodes of a multicast group (gray-colored nodes), and eleven tree links. In the shared tree scheme, receiver nodes periodically send *join requests* to the root node, and the root updates the multicast tree using the path information included in the join request messages [28].

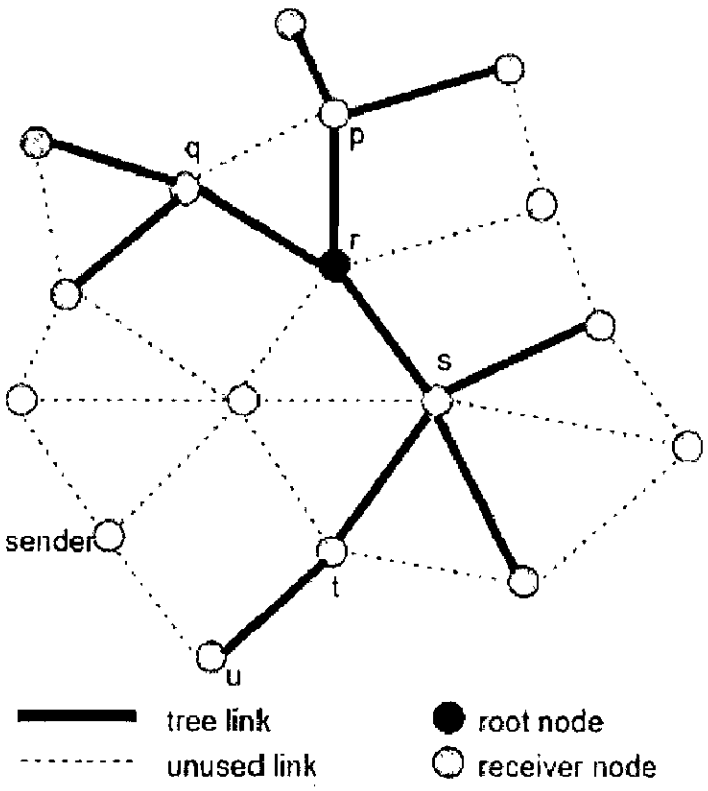


Fig. 2.1 An example of tree-based multicast

Joining a multicast group causes reports (i.e., join messages) to be periodically sent [29], while leaving a multicast group does not lead to any explicit action. The period must be carefully chosen to balance the overhead associated with tree

update and the delay caused by the tree not having timely updates when the nodes move [30]. Various tree-based multicast protocols have been proposed,[31-37] and here some representative ones are briefly reviewed:

• *Ad-hoc Multicast Routing Protocol (AMRoute)* [31] creates a bidirectional shared tree per multicast group. The tree contains only the group members, and multicast tunnels *(virtual links)* are assumed to exist between each pair of group members based on an underlying routing protocol. Therefore, the tree need not be reconstructed even though the network topology changes as long as routes between the group members exist.

• *Ad-hoc On-Demand Distance Vector Multicast Protocol (AODV)* [32] is another bidirectional shared tree multicast protocol. Here, if the sender does not belong to the multicast group, it first finds the nearest group member and lets it become a root for delivering the multicast packets.

• *Ad-hoc Multicast Routing protocol utilizing Increasing-idS (AMRIS)* [33] is a shared tree multicast approach. Each node has *multicast session member id (msm-id).* The msm-id provides each node with an indication of its "logical height" in the multicast delivery tree such that it increases as it radiates from the root of the delivery tree.

•*Lightweight Adaptive Multicast (LAM)* [34] builds a group-shared multicast routing tree centered at a preselected node called a *CORE.* LAM runs on top of *TORA (Temporally Ordered Routing)* protocol [35]; each node has information on its neighbors and the correct order of transmission path. Each member prepares a *JOIN* message containing the group id and the target *CORE* id, picks a neighbor with the lowest height as the receiver of the *JOIN* message, and sends the message. Since the *JOIN* message is supposed to travel along only a "downwards" path in the TORA DAG (directed acyclic graph) with respect to the target *CORE*, if a *JOIN* message is received over an upstream link, the tree is considered invalid and a valid one is constructed rooted at the *CORE.*

• In *Associativity-Based Multicasting Routing Protocol (ABAM)* [36], a multicast sender builds a per-source multicast tree with *i* messages sent by member receivers who received an *MBQ (multicast broadcast query)* message from the

sender. The multicast sender decides a stable multicast tree based primarily on association stability, which refers to spatial, temporal, connection, and power stability of a node with its neighbors, and it generates an *MC-SETUP* message to establish a multicast tree.

• Multicast Routing Protocol based on Zone Routing (MZR) [37] is another per-source tree approach, in which a multicast delivery tree is created using a concept called the zone routing mechanism. A proactive protocol runs inside each zone, maintaining an up-to-date zone routing table at each node. A reactive multicast tree is created for inter-zone routing.

Mesh-Based Multicast

Tree-based protocols may not perform well in the presence of highly mobile nodes because the multicast tree structure is fragile and needs to be readjusted frequently as the connectivity changes. Mesh-based multicast protocols have been proposed to address the problem by constructing a mesh structure with redundant links between mobile nodes. Figure 2.2 shows an example of mesh-based multicast for the MANET. Note that it includes three redundant links (marked in the figure) in addition to eleven tree links. As a result, even though the tree link from *s'* to *v'* is broken, node *v'* receives a multicast packet through the redundant link from *t'* to *v'*. Mesh-based protocols are more robust to mobility and thus allow better *packet delivery ratio*. Several [38-42] mesh-based multicast protocols have been reported in the literature, some of them are briefly described below :

•*Multicast Core-Extraction Distributed Ad hoc Routing (MCEDAR)*[38] is an extension to the *CEDAR routing protocol* [39], and it provides the robustness of mesh-based routing protocols while approximating the efficiency of tree-based protocols. As CEDAR extracts core nodes, MCEDAR extracts a sub-graph (called an *mgraph*) for each multicast group consisting only of core nodes as the routing infrastructure used for data forwarding.

•*Clustered Group Multicast (CGM)* [40] employs *advertising agents* to reduce traffic, which act as both a server and client for advertising join requests on behalf

of their local clients. Multicast backbone is also used to reduce the control overhead. By implementing CGM over the multicast infrastructure, the cluster-head works as an advertising agent if one or more subscribers are within its cluster, and the inter-cluster routing approach lets the number of nodes in the backbone be smaller.

•*Core-Assisted Mesh Protocol (CAMP)* [41] adopts the same basic architecture used in IP multicast. A node wishing to join a multicast mesh first consults a routing table to determine whether it has neighbors that are already members of the mesh. If so, the node announces its membership via a *CAMP UPDATE*. Otherwise, the node either propagates a *JOIN REQUEST* towards one of the multicast group "cores" or attempts to reach a member router by applying ring search of broadcast requests.

•*On-Demand Multicast Routing Protocol (ODMRP)* [42] employs on-demand routing techniques to avoid channel overhead and improve scalability. It uses the concept of *forwarding group*, a mesh of nodes responsible for forwarding multicast data on shortest paths between any pair of members. During the control message exchange between senders and group receivers (*JOIN REQUEST* and *JOIN TABLE*), a node realizes that it is part of the forwarding group when it is on the path from a receiver to the source.

•*Neighbor Supporting Multicast Protocol (NSMP)* [42] utilizes node locality to reduce the overhead of route failure recovery and mesh maintenance. A new source initially sends a *FLOOD REQ (FR)* packet containing an upstream node field. When an intermediate node receives it, it caches its upstream node and updates the field with its own address before forwarding it. When a receiver receives the *FR* packet, it sends an *REP* packet. The upstream node receives the *REP* packet and adds an entry for the group to its routing table, and the *REP* packet is forwarded eventually to the source node.

Both *tree-based multicast* and *mesh-based multicast* require to be an energy efficient multicast protocol to conserve the energy.

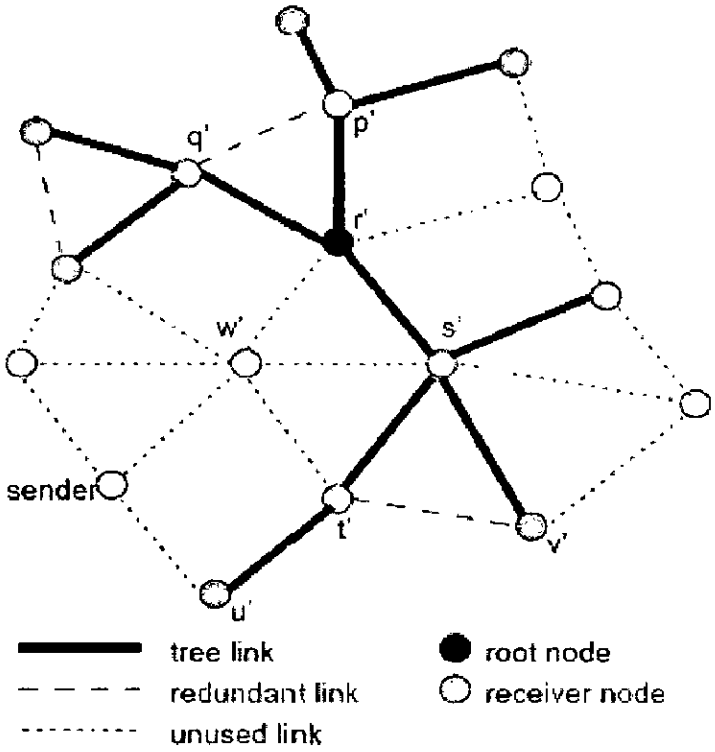


Fig. 2.2 An example of mesh-based multicast

Energy Efficient Multicast Protocols

Energy efficiency protocols have been emphasized to distinguish it from all other protocols. Two approaches have been proposed for energy efficient multicast in MANETs. The first is based on the assumption that the transmission power is controllable. Under this assumption, the problem of finding a tree with the least consumed power becomes a conventional optimization problem on a graph where the weighted link cost corresponds to the transmission power required for transmitting a packet between two nodes.

The second approach for energy efficiency comes from the difference of tree-based multicast [48] from mesh-based multicast. One general idea of the power-saving mechanism is to put a mobile node in sleep (low power) mode while it is not sending or receiving packets. Since every mobile node in the mesh must not sleep and must be ready to receive packets during the entire multicast session, it would consume more energy. Even though data transmission through a wireless medium is broadcast in nature, this does not necessarily mean that all neighbor nodes have

to receive the broadcast packets. Uncast transmission along the multicast tree is quite different from the intentional broadcast within the multicast mesh in that only the designated receiver needs to receive the transmitted data. A mobile node in tree-based protocols can safely put itself into a low power energy conserving sleep mode if it is not a designated receiver [49]. A connected dominating set S of a graph G is a connected sub graph of G such that every vertex u in G is either in S or adjacent to some v in S. Routing using connected dominating sets of a graph can reduce the search space for routes [45,46].

As mentioned in the introduction to this chapter, another important aspect of energy efficiency is balanced energy consumption among all participating mobile nodes. For example, consider a multicast tree shared by a number of multicast senders. In the shared tree, the root node of the tree consumes more battery energy and stops working earlier than other nodes. This affects the network connectivity and may lead to partitioning of the MANET and reduced network lifetime. A per-source tree-based multicast protocol alleviates this problem by using a separate tree per sender at the cost of increased tree management overhead [43,44]. Node mobility also needs to be considered along with energy balancing.

The next section presents the detail research review on energy efficient multicast protocols.

2.3 RESEARCH REVIEW ON ENERGY EFFICIENT MULTICAST PROTOCOLS

Das and Bharghavan [45] approximate the minimum connected dominating set of an ad hoc network, and route packets using nodes from that set. Wu et al. [46] propose a distributed algorithm for approximating connected dominating sets in an ad hoc network that also appears to preserve capacity. In a later paper, Wu and Gao [47] discuss power aware routing using the connected dominating sets. In GAF (Geographic Adaptive Fidelity) [77], nodes use geographic location information to divide the world into fixed square grids. The size of each grid stays constant, regardless of node density. Nodes within a grid switch between sleeping

and listening, with the guarantee that one node in each grid stays up to route packets.

In AFECA (Adaptive Fidelity Energy Conserving Algorithm) [48], each node maintains a count of the number of nodes within radio range, obtained by listening to transmissions on the channel. A node switches between sleeping and listening, with randomized sleep times proportional to the number of nearby nodes. The net effect is that the number of listening nodes is roughly constant, regardless of node density; as the density increases, more energy can be saved. AFECA's constants are chosen so that there is a high probability that the listening nodes form a connected graph, so that ad hoc forwarding works. An AFECA node does not know whether it is required to listen in order to maintain connectivity, so to be conservative AFECA tends to make nodes listen even when they could be asleep. The PAMAS power-saving medium access protocol [49,50] turns off a node's radio when it is overhearing a packet not addressed to it. This approach is suitable for radios in which processing a received packet is expensive compared to listening to an idle radio channel. Kravets and Krishnan [51] present a system in which mobile units wake up periodically and poll a base station for newly arrived packets. Like Stemm and Katz [52], they show that setting the on/off periods based on application hints reduces both power and delay. Span assumes the presence of an ad hoc polling mechanism such as that provided by 802.11, and could potentially work in concert with application hints; such hints would apply only to sleeping nodes, not backbones. Smith et al. [53] propose an ad hoc network that elects a virtual base station to buffer packets for local nodes. They do not, however, attempt to make sure that enough of these base stations are present to preserve connectivity in a multi-hop ad hoc network. Minimum-energy routing [54] saves power by choosing paths through a multi-hop ad hoc network that minimize the total transmit energy. Chang and Tassiulas [54] to maximize overall network lifetime by distributing energy consumption fairly have extended this approach. In this protocol, nodes adjust their transmission power levels and select routes to optimize performance. Ramanathan and Rosales-Hain describe distributed algorithms that vary transmission power and attempt to maintain connectedness

[55]. Rodoplu and Meng [56] give a distributed algorithm to produce minimum power routes by varying node transmission power. Wattenhofer et al. [57] describe a topology maintenance algorithm using similar underlying radio support, but their algorithm guarantees global connectedness using directional information. Heinzelman et al. [58], whose LEACH protocol selects rotating cluster-heads to collect local information and transmit it to a base station in a wireless sensor network, describe an alternative approach. Like LEACH, directed diffusion mechanism of Intanagonwiwat et al. [59] takes advantage of aspects of sensor networks, particularly the possibility of aggregating and compressing data that are not present in general-purpose networks.

In general, the basic idea that a path with many short hops is sometimes more energy-efficient than one with a few long hops could be applied to any ad hoc network with variable power radios and knowledge of positions. In preemptive routing [60], low received signal strength is used to predict when a link, and thus a route, will break. When signal strength becomes low, the routing protocol can preemptively select a new good route to the same destination, on the assumption that low signal strength indicates that the other end of the link will soon be out of range. New routes are selected so that all links have signal strength greater than some threshold. Low signal strengths are monitored for a period to ensure that random signal fades do not prematurely trigger a route change. Simulations with DSR [60] show that this technique decreases the number of broken routes, and generally decreases latency. Span adaptively elects "backbones" from all nodes in the network. Span backbones stay awake continuously and perform multi-hop packet routing within the ad hoc network, while other nodes remain in power-saving mode and periodically check if they should wake up and become a backbone.

Table 2.1 Bottleneck of Popular Energy Efficient/ Power saving wireless infrastructure-less networks

S.No.	Papers on Energy	Author/ Proposed by	Year of Pub.	Technique Used/ Available Information	Drawback(s)	Remarks (if any)

	Efficient Model					
1	**PAMAS** (Power aware multi access protocol)	S Singh et al. [49]	1998	The PAMAS power-saving medium access protocol turns off a node's radio when it is overhearing a packet not addressed to it. This approach is suitable for radios in which processing a received packet is expensive compared to listening to an idle radio channel. Choosing Beacon Period for *Improved* Response Time.	It uses a separate control channel, nodes have to be able to receive on the control channel while they are transmitting on the data channel and also transmit on data and control channels simultaneously and a node should be able to determine when probe responses from multiple senders collide.	+Use of Beacon Period-to improve response time.
2	**Improved PAMAS**	C. S. Raghwendra et al. [50]	1999	To avoid the probing, a node should switch off the interface for data channel, but not for the control channel (which carries RTS/CTS packets). Each sleeping node always know how long to sleep by watching the control channel.	This may not be useful when hardware is shared for the control and data channels. It may not be possible turn off much hardware due to the sharing.	+Control Channel (RTS/CTS packets) doesn't switch off.
3	Woesner et al, Jung et al., Tseng et al., Chen et at.	Woesner et al., [23] Jung et al., [46] Tseng et al.,[33] Chen et at. [54]	1998 2002 2002 2001	If each node uses the 802.11 power-save mechanism, each hop will require one beacon interval. This delay could be intolerable. If two hosts' ATIM windows do not overlap in time, they cannot exchange ATIM requests (synchronization problem). *If ATIM window is too*	If each node uses the 802.11 power-save mechanism, each hop will require one beacon interval. This delay could be intolerable. If two hosts' ATIM windows do not overlap in time, they cannot exchange ATIM requests *(synchronization*	+Based on ATIM Window

				large, reduction in energy consumption reduced. Energy consumed during ATIM window. If ATIM window is too small, not enough time to send ATIM request.	problem). If ATIM window is too large, reduction in energy consumption reduced. Energy consumed during ATIM window. If ATIM window is too small, not enough time to send ATIM request.	
4	**LEACH** (Low Energy Ad Hoc Cluster-Head Network)	Kravets and Krishnan [51]		Its mobile units wake up periodically and poll a base station for newly arrived packets.	Taekyoung kwon et al. shows that LEACH abruptly selects cluster-head in bad case scenario, where some nodes in the cluster are out of the radio range. LEACH media access consumes considerable high power consumption.	Periodically wake up by polling
5	**SPAN**	Balakrishnan et al. [61]	2001	It adaptively elects "coordinators" from all nodes in the network. Span coordinators stay awake continuously and perform multi-hop packet routing within the ad hoc network, while other nodes remain in power-saving mode and periodically check if they should wake up and become a coordinator.	Proposed algorithm is close to weak Wu/Li's concept of connected dominating sets (view: www.site.uottawa.ca/~ivan. Handbook of Sensor Networks: Algorithms and Architectures (I. Stojmenovic, ed.), Wiley, 2005, pp. 343-379.).	"coordinator" concept
6	Energy and rate based MAC protocol	Rajgopal Kannan et al. [62]	2003	In this paper the author propose an approach in which node duty cycles (i.e sleep and wake schedules) are based on their criticality.	This makes the problem of conserving energy at individual sensor nodes challenging. S-MAC and PAMAS are two MAC	+Using critical value for sleep and

	for wireless sensor networks			A distributed algorithm is used to find sets of winners and losers, who are then assigned appropriate slots in our TDMA based MAC protocol. They use the concept of of *energy-criticality* of a sensor node as a function of energies and traffic rates.	protocols which periodically put nodes (selected at random) to sleep in order to achieve energy savings.	wake period
7	A MAC Protocol to Reduce Sensor Network Energy Consumption Using a Wakeup Radio	Nitin H. Vaidya et al. [63]	2005	The author proposes a protocol for energy conservation. In addition, it allows sensors to control the amount of buffered packets since storage space is limited. To achieve this, a two-radio architecture is used which allows a sensor to "wakeup" a neighbor with a busy tone and send its packets for that destination.	This process is expensive because all neighbors must awake and listen to the primary channel to determine who the intended destination is. Therefore, triggered wakeups on the primary channel are proposed to avoid using the more costly wakeup procedure.	+new protocol for energy conservation – two radio architecture
8	**JAVeLEN** - An ultra-low energy ad hoc wireless network	J. Rediet al. [64]	2008	In this paper the period of time during which the network is operational depends on battery lifetime. The author has designed and simulated a novel design for a mobile ad hoc network with a low offered load (of approximately 1% average loading) that uses dramatically less (often 300 times or 99.7% less) power than industry standard protocols and yet achieves higher delivery reliability,		

				handles substantially greater node densities, supports mobility, and has the ability to perform well even under high offered loads.		
9	Energy Efficient Multicast Routing Protocol for MANET with Minimum Control Overhead	Pariza Kamboj and Ashok.K. Sharma [65]	2010	The algorithm uses the concept of small overlapped zones around each node for proactive topology maintenance with in the zone. To search for an existing multicast tree outside the zone, constrained directional forwarding is used which guarantees a good reduction in overhead in comparison to network wide flooding for search process.		

2.4 CONCLUSION

On the basis of above study it is observed that several energy efficient/ power aware wireless infrastructure-less networks routing protocol have been designed to support energy saving by power control and energy efficient. But most of them use a separate control channel, nodes have to be able to receive on the control channel while they are transmitting on the data channel and also transmit on data and control channels simultaneously, thus a node should be able to determine when probe responses from multiple senders collide. In spite of this, their spatial reuse is less than optimal. Thus there is a great need to identify the new energy efficient protocol for wireless infrastructure-less networks.

CHAPTER-3

DEVELOPMENT OF AN OPTIMAL PATH-PROGRAMMING ALGORITHM FOR DECENTRALIZED INFRASTRUCTURE-LESS WIRELESS NETWORK

Chapter 3.

DEVELOPMENT OF AN OPTIMAL PATH-PROGRAMMING ALGORITHM FOR DECENTRALIZED INFRASTRUCTURE-LESS WIRELESS NETWORK

3.1 INTRODUCTION

Path programming is a process that can help drivers to plan routes before or in traveling to achieve infrastructure-less node navigation. Several researchers uses neural net [66-68], genetic algorithm [69] and so on to resolve the path programming problem in complex environment for mobile infrastructure-less node navigation system and has made some achievements, but still exists a series of disadvantages in real-time ability and convergence velocity and so on. Path programming in complex environment hasn't been well resolved all the time. Aiming at this problem, the efforts has been made to develop a new modified optimal path programming algorithm which is based on the combined concepts of Dijkstra algorithm, Floyd algorithm and graph theory. The simulation results using NS-2 shows that the developed algorithm can curtail the optimal path programming time to a reasonable level.

Section 3.2 deals with the background and traditional shortest path finding concepts using graph theory, Dijkstra algorithm and Floyd algorithm. Section 3.3 describes the development steps for modified optimal path programming algorithm for shortest path. Section 3.4 discusses the operational scenario and comparative analysis of the traditional algorithm and modified algorithm and finally, 3.5 concludes.

3.2 BACKGROUND

The traditional path programming algorithms are generally based on the concepts of graph theory [70,71,72], Dijkstra algorithm [73], Floyd algorithm [74,75] etc. However case studies [70,74,75] shows that these algorithms are suitable for the particular situations or scenarios. The combination of these produces an effective solution to generalize the shortest path programming for infrastructure-less

wireless networks. The concept of graph theory, Dijkstra algorithm and Floyd algorithm are described in next steps:

3.2.1 Shortest Path using Graph Theory [70-72]

Graph theory is a science that studies the theory and algorithm related with graphs, whose application is very wide. In graph theory, If the beginning points, ending points and crossing points in a road traffic network are denoted as nodes, roads as the arcs connecting nodes, the properties such as road length and traveling time as road weight, the road network can be abstracted as digraph with weight, and problems related with it can be resolved by graph theory [70].

In order to explain the mathematical description and solution principle of the shortest path problem, some definitions and terminologies used in graph theory, Dijkstra algorithm and Floyd algorithm are described in next step:

Graph.

From the view of computer science, graph is a kind of data structure, which can be defined as:

$$G=(V,R)$$
$$V=\{x \mid x \in dataobject\}$$
$$R=\{VR\}$$
$$VR=\{<x,y> \mid P(x,y) \wedge (x,y \in V)\}$$

In graphs, the basic data element is vertex. V is the finite non-vacant gather of vertexes. VR is the gather of relations between any two vertexes.

Digraph and un-digraph.

If in a graph, when $<x,y> \in VR$, $<x,y>$ denotes an arc from x to y, where x is called tail or initial node and y is called head or terminal node, then the graph is called digraph. The un-digraph is the graph that when VR is symmetrical, namely it not only satisfied path programming $<x,y> \in VR$, but satisfied path programming $<y,x> \in VR$, and then replacing the two sequential couples with an un-sequential couple (x,y) called an edge from x to y.

Adjacency and relevancy.

It would be said that v, v' are adjacent or v, v' are adjoined if $(v, v') \in E$ in un-digraph $G = (V, \{E\})$, with (v, v') incident on v and v', or it can be said that (v, v') is correlated with v and v'. It would be said that v adjoins to v' and v' adjoins to self-vertex v and $< v, v' >$ is correlated with v and v' if $< v, v' > \in A$ in digraph $G = (V, \{A\})$.

Degree.

Degree of v, written as $TD(v)$, is the number of edges correlated with v in un-digraph or the number of arcs correlated with v in digraph, where the number of arcs headed with v is in-degree of v written as $ID(v)$, and the number of arc ended with v is out-degree of v written as $OD(v)$; Degree of v is equal to the sum of the two, namely $TD(v) = ID(v) + OD(v)$. For a graph with n vertexes and e edges or arcs, the degree of vertex i is written as $TD(i)$, then:

$$e = \frac{1}{2} \sum_{i=1}^{n} TD(v_i)$$

Sub-graph.

Supposing there are two graphs $G = (V, \{E\})$ *and* $G' = (V', \{E'\})$ with $V' \subseteq V$ *and* $E' \subseteq E$, then G' is the sub-graph of G.

Path.

In un-digraph $G = (V, \{E\})$, vertex sequence $(v_{i0} = v, v_{i1}, \Lambda, v_{in} = v')$ is called a path from v to v', where $(v_{ij-1}, v_{ij}) \in E, 1 \le j \le n, 1 \le i \le n-1$;.The path in digraph is directional, with vertex sequence satisfying $(v_{ij-1}, v_{ij}) \in E, 1 \le j \le n$. Number of edges or arcs in a path is the length of the path. A path in which the first vertex and the last vertex are the same is called a loop or a cycle, and the path whose vertexes in the sequence don't appeared repeatedly is called a simple path.

Connection.

It would be said that v and v' are connected if there exists a path from v to v' in un-digraph. The un-digraph where any two vertexes are connected is called connected graph. It would be said that v' is accessible relatively to v, if there exists a path from v to v' in digraph. v and v' are connected if there exist paths both from v *to* v' and from v' *to* v. The digraph, in which every couple of vertexes is connected, is a strong connected graph.

Weight and network.

The data related with an edge or arc, is called the weight of the edge or arc, it can be used to describe the distance or cost from one vertex to another. Graph with weight is network, where the vertex is called node.

3.2.2 Shortest Path using Dijkstra Algorithm [73]

In Dijkstra algorithm, when the optimizing standard in path programming is quantitated as the road's traveling cost, the optimal path programming summarized as the problem of searching an optimal path with minimum sum of traveling cost in a specific road network.

In a given digraph $G=(V,\{E\})$ with weight, where V is vertex gather including n vertexes, E is arc gather including m arcs, $<v,w>$ is an arc from v *to* w in E, and $c<v,w>$ is a un-negative weight value of $<v,w>$, supposing that $P_{st}=\{v_0=v_s,v_1\Lambda,v_n=v_t\}$ is a path from v_s *to* v_t in V, the sum of its weight value can be written as :

$$TW(P_{st})=\sum_{i=0}^{n-1}c(v_i,v_{i+1})$$

Searching a path with minimum sum of weight value from the appointed initial node to a terminal node in digraph with weight is called the shortest path problem. Regarding weight value as arc length property (distance), the target path is just the shortest path from the initial node to a terminal node.

It describes the single source shortest path problem, namely seeking the shortest path from v to any other vertex in G with the given digraph $G=(V,\{E\})$ with weight and source v.On this problem, Dijkstra put forward an algorithm that the shortest path is generated according to path length with an increasing order, the principles are as follows:

It sets an accessorial vector D, in which every component d_i denotes the length of the shortest path found currently from the source to every destination. Setting the initial state as: d_i is the weight value of arc if there exist arcs from v *to* v_i, otherwise, d_i is commanded as ∞. Apparently, the path with its length $d_j=\min_i\{d_i \mid v_i \in V\}$ is the one that starts from v and has the shortest length.

Supposing that S is the gather of destinations with the shortest length, it can be proved that the next shortest path (destination is x) is either $<v,x>$ or the path that just passes the destination in S and finally reaches x.Therefore, the length of the next secondary shortest length must be: $d_j=\min_i\{d_j \mid v_i \in S\}$, where d_i is either the weight value of $<v,v_i>$ or the sum of weight value of $d_k(v_k \in S)$ and $<v_k,v_i>$.

3.2.3 Shortest Paths using Floyd's Algorithm [74]

This algorithm is designed to find the least-expensive paths between all the vertices in a graph. It does this by operating on a matrix representing the costs of edges between vertices.

To understand Floyd's algorithm one must build a matrix, usually in a two-dimensional array. If there are n vertices in our graph, the matrix will be nx_n. Each row in the matrix represents a "starting" vertex in the graph while each column in the matrix represents an "ending" point in the graph. If there is an edge between a starting point i and ending point j in the graph, the cost of this edge is placed in position (i,j) of the matrix. If it deals with an undirected graph in which all edges are bi-directional, an entry is also made in position (j,i) of the matrix. If there is no edge directly linking two vertices, an infinite (or, in practice, very large) value is placed in

the (i,j) position of the matrix to specify that it is impossible to directly move from i to j.

For example, if it has a graph in which points 1 and 5 are connected by a bi-directional edge with a cost of 22 units, then the weight of the place is 22 for positions (1,5) and (5,1) of that matrix. Once it has set this matrix up, Floyd's algorithm used to compute the shortest distance between all points in the graph.

When this routine finishes the entries in all positions of the matrix represent the lowest-cost traversal between the row-vertex and column-vertex. If such a path is found, it becomes the value against which future indirect paths between these vertices are tested. In the end, each element of the matrix represents the lowest-cost traversal between the vertices it's row and column represent. Remember that if the graph is directed, so is the answer in (i,j) of the matrix; moreover, (i,j) may not be equal to (j,i) in a di-graph.

In Floyd algorithm, Floyd's algorithm works by looking for all non-direct paths between two vertices that have a less-expensive total cost than the best way yet found to move between said vertices.

The developed modified optimal path programming algorithm for shortest path is the combination of graph theory concepts, Dijkstra algorithm by using its accessorial vector using Di-graph and Floyd algorithm by using its costs of edges between vertices. The developed algorithm later compared with Dijkstra algorithm and Floyd algorithm. As it need not find the shortest route but the hypo-excellent route, which meet the parameter of error, so the searching time will not be long.

3.3 DEVELOPMENT STEPS FOR MODIFIED OPTIMAL PATH PROGRAMMING ALGORITHM FOR SHORTEST PATH

The basic structures for the modified optimal path programming algorithm for shortest path are as follows:

(i) Local Search for the path; The group of nodes searches for the start and target

node as a source and destination. As assuming a path search space, G = (V, W, C), where V is a set of nodes in the path tree, W is the weight representing the length of a pair of nodes, and C is the feature variable. A path search processing is as follows (as shown in figure 3.1):

a) Initialize V= empty;
b) Set Distance (v) = infinity;
c) Add u, a set of nodes in the path tree;
d) Generate weight list, Weight = distance (u) + length (u,v) + C;
e) Estimate weight, if Weight < distance (v), update v into u, else estimate neighborhood v of u;
f) Verdict all nodes in the path tree until the target node is reached.

(ii) Total number of path; Record the total number of paths between source node and target node.

(iii) Determine the length of each path; $d_j = \min_i\{d_i \mid v_i \in V-S\}$ and record the probability of each path, and record the flow that each path gets and so on. Using $P_i = \frac{e^{l(i)}}{\sum_{x=1}^{n-1} e^{l(x)}}$, Define the travel time as T(i), i=1,2,...n-1. In this step, the probability of each path will be calculated using T(i) and the module.

(iv) Modifying the length of the accessible shortest path from v_s to any other vertex v_k in the gather $V-S$. If $d_k > d_j + c_{jk}$, d_k would be modified as $d_k = d_j + c_{jk}$.

(v) Repeating step ii and step iii for $n-1$ times, the shortest path sequence with an increasing order and starting from the initial node to destination node in graph can be found out by analyzing is $u = v_i$?

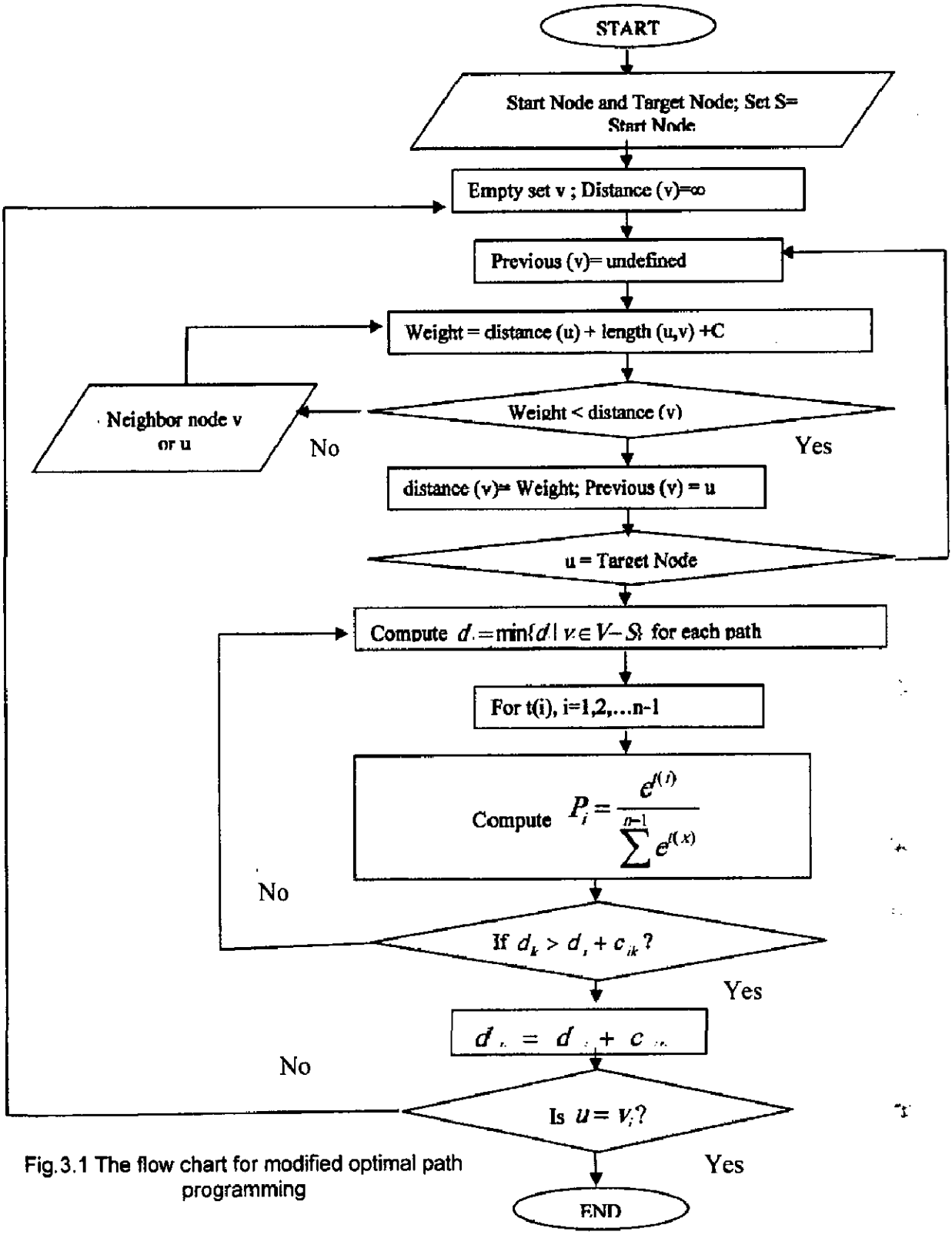


Fig.3.1 The flow chart for modified optimal path programming

3.4 OPERATIONAL SCENARIO AND COMPARATIVE ANALYSIS

In figure 3.2, the order to search the shortest path from node 1 to any other nodes, weight values between nodes and structures would be like the graph as follows:

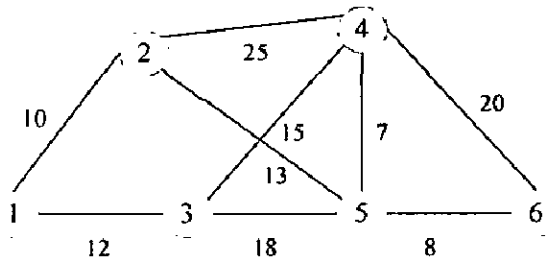


Fig.3.2 node weight value and structure analysis

According to the algorithm introduced above, an adjacency matrix C can be given:

$$C=\begin{bmatrix} c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} \\ c_{21} & c_{22} & c_{23} & c_{24} & c_{25} & c_{26} \\ c_{31} & c_{32} & c_{33} & c_{34} & c_{35} & c_{36} \\ c_{41} & c_{42} & c_{43} & c_{44} & c_{45} & c_{46} \\ c_{51} & c_{52} & c_{53} & c_{54} & c_{55} & c_{56} \\ c_{61} & c_{62} & c_{63} & c_{64} & c_{65} & c_{66} \end{bmatrix}=\begin{bmatrix} 0/1 & 10/2 & 12/3 & \infty/4 & \infty/5 & \infty/6 \\ 10/1 & 0/2 & \infty/3 & 25/4 & 13/5 & \infty/6 \\ 12/1 & \infty/2 & 0/3 & 15/4 & 18/5 & \infty/6 \\ \infty/1 & 25/2 & 15/3 & 0/4 & 7/5 & 20/6 \\ \infty/1 & 13/2 & 18/3 & 7/4 & 0/5 & 8/6 \\ \infty/1 & \infty/2 & \infty/3 & 20/4 & \infty/5 & 0/6 \end{bmatrix}$$

Initializing accessorial vector D, $D=C \quad S=\phi$, where S is gather of destinations with the shortest length . Only the data of the first column are useful because what we need starts from v_1. For the first operation, it doesn't take v_1 into account, because the weight value from v_1 to the current node is zero. When $d_2=\min_j\{d_j \mid v_j \in V-S\}=10$, v_2 is the destination of the shortest path starting from v_1 currently. Commanding $S=\{v_2\}$ and modifying length of the accessible shortest path from v_1 to any other vertexes in the gather $V-S$, the data after modifying are:

1) The first operation

$$\begin{bmatrix} 0/1 & L \\ 10/1 & L \\ 12/1 & L \\ 35/1 & L \\ 23/1 & L \\ \infty/1 & L \end{bmatrix}$$

2) the second operation $S=\{v_2,v_3\}$

$$\begin{bmatrix} 0/1 & L \\ 10/1 & L \\ 12/1 & L \\ 27/1 & L \\ 23/1 & L \\ \infty/1 & L \end{bmatrix}$$

3) the third operation

4) the fourth operation

$S=\{v_2, v_3, v_5\}$

$$\begin{bmatrix} 0/1 & L \\ 10/1 & L \\ 12/1 & L \\ 27/1 & L \\ 23/1 & L \\ 31/1 & L \end{bmatrix}$$

$S=\{v_2, v_3, v_4, v_5\}$

$$\begin{bmatrix} 0/1 & L \\ 10/1 & L \\ 12/1 & L \\ 27/1 & L \\ 23/1 & L \\ 31/1 & L \end{bmatrix}$$

Up to now, the shortest paths from the source to all other nodes have been calculated:

v_1 *to* v_2 : □—□ path length 10

v_1 *to* v_3 : □—□ path length 12

v_1 *to* v_4 : □—□—□ path length 27

v_1 *to* v_5 : □—□—□ path length 23

v_1 *to* v_6 : □—□—□—□ path length 31

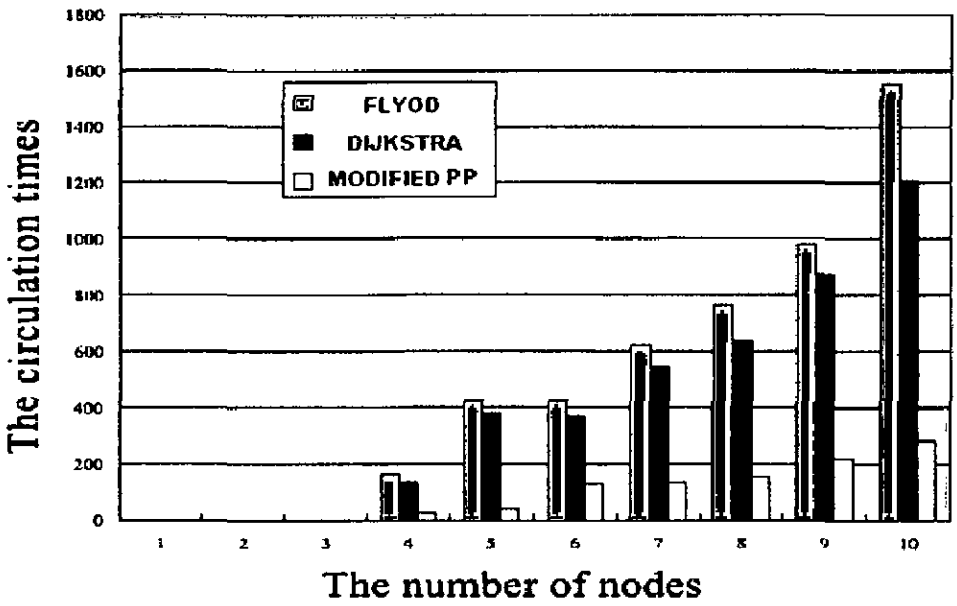


FIG. 3.3 time overhead comparison in Floyd, Dijkstra and modified path programming

Circulation time is an important parameter to evaluate an algorithm. The classical searching route algorithm (like graph theory, Dijkstra algorithm and Floyd algorithm) is more complex to find the shortest route, and takes much time, as show in figure 3.3. In the modified path programming algorithm, it combines the dynamical backup route mode and searching route mode. First of all, several backup routes from sample bank base are selected as substitute route. Commonly, the probability that all routes are saturation is very small. Therefore, most restoration route is obtained from the backup routes, and thus circulation time is very short. If the restoration route cannot be found in the backup route, searching the substitute with modified path programming is used. Here, O(N) is the circulation time overhead.

3.5 CONCLUSION

Combining Dijkstra and Floyd algorithm with the graph theory yields a modified path programming algorithm using hypo-excellent route in mobile infrastructure-less node navigation system under complex environment. The time complexity of Dijkstra is O (N^2), and the time complexity of Floyd is O (N^3). Although there is a certain statistical error to do statistics with circulation and judgment, it is shown that the Dijkstra is better than Floyd in time. With the increase in the number of nodes, the time complexity of Dijkstra is increased by N^2 and the time complexity of Floyd is increased by N^3. The time complexity of modified path programming algorithm is N, thus the circulation time increases linearly as the number of nodes.

CHAPTER-4

DEVELOPMENT OF AN ENERGY EFFICIENT WIRELESS INFRASTRUCTURE-LESS NETWORKING (EILN) PROTOCOL

Chapter-4

DEVELOPMENT OF AN ENERGY EFFICIENT WIRELESS INFRASTRUCTURE-LESS NETWORKING (EILN) PROTOCOL

4.1 INTRODUCTION & BACKGROUND

The energy efficiency of a wireless Infrastructure-less node is defined as the ratio of the amount of data delivered in one hop by the node to the total energy expended in multi-hop. Minimizing energy consumption is an important challenge in Multi-hop wireless Infrastructure-less networking. The previous study [In section 1.2] shows that efficient energy awareness needs to be adopted by the protocols at all the layers in the protocol stack, and has to be considered as one of the important design objectives for such Multi-hop wireless Infrastructure-less networking protocols. Quality of services also affects due to limited capabilities of wireless mobile nodes in terms of processing power, storage capacity, or energy efficiency.

Section 4.2 describes EILN's (Energy Efficient Infrastructure-less Network's) protocol development algorithms and its interactions with the link layer. This describes and evaluates EILN protocol. Section 4.3 presents simulated implementation of EILN on comparisons with other IEEE 802.11(like 802.11b, 802.11PSM) and SPAN using NS-2 network simulator. Section 4.4 presents performance results of several simulations. Finally, section 4.5 concludes.

4.2 STEPS FOR DESIGN OF NETWORK PROTOCOL

Considering the special properties of wireless infrastructure-less networks, when analyzing about any routing protocol, it is generally expected that there are the following properties, though all of these might not be possible to incorporate in a single solution [76]:

i) *Local adoption of topology:* A routing protocol for wireless infrastructure-less networks should be *distributed* in manner in order to increase its reliability. Where all nodes are mobile, it is unacceptable to have a routing protocol that requires a centralized entity. Each node should be intelligent enough to make local routing decisions using other collaborating nodes. A distributed but virtually centralized protocol might be a good idea.

ii) A unidirectional links is assumed for the route in routing protocol. Wireless medium may cause a wireless link to be opened in unidirectional only due to physical factors. It may not be possible to communicate bi-directionally. Thus a routing protocol must be designed considering unidirectional links.

iii) The routing protocol may be power-efficient. It should consider every possible measure to save power, as power is very important for small battery powered devices. To save power, the routing-related loads could be distributed among the participating nodes.

iv) *Selection of cluster-head:* It allows as many nodes as possible to turn their radio receivers off most of the time; since even an idle receive circuit consumes almost as much energy as an active transmitter.

v) *No central control:* On the other hand, it may forward packets between any source and destination with minimally more delay than if all nodes were awake. This implies that enough nodes must stay awake to form a connected backbone. The algorithm for picking this backbone should be distributed, requiring each node to make a local decision.

vi) Furthermore, the backbone formed by the awaken nodes provides the total capacity as the original network, since otherwise congestion may increase. This means that paths that could operate without interference in the original network should be represented in the backbone.

A good energy efficient network protocol cannot consider many assumptions about the link layer's facilities for sleeping; it works with any link-layer that provides for sleeping and periodic polling, including 802.11's infrastructure-less power saving mode. Finally, power saving inter-operate correctly with whatever routing system the infrastructure-less network uses. However, certain assumptions are required to

develop the infrastructure-less networks for simulation. As unless stated otherwise, fully symmetric environment is assumed implicitly means all nodes have identical capabilities and responsibilities.

Development of EILN protocol and its algorithm design consideration

To develop energy efficient infrastructure- less network protocol (EILN) algorithm the following design steps are taken:

a) *Local adoption of topology;* The collection of nodes ensure the formation of cluster. By calculating the distance between the present and next position and comparing it with threshold value, the members in the cluster maintain a "cluster member table", where it stores the destination cluster-head for each mobile node in the networks. Figure 4.1 shows the flowchart for local adoption of topology for each node.

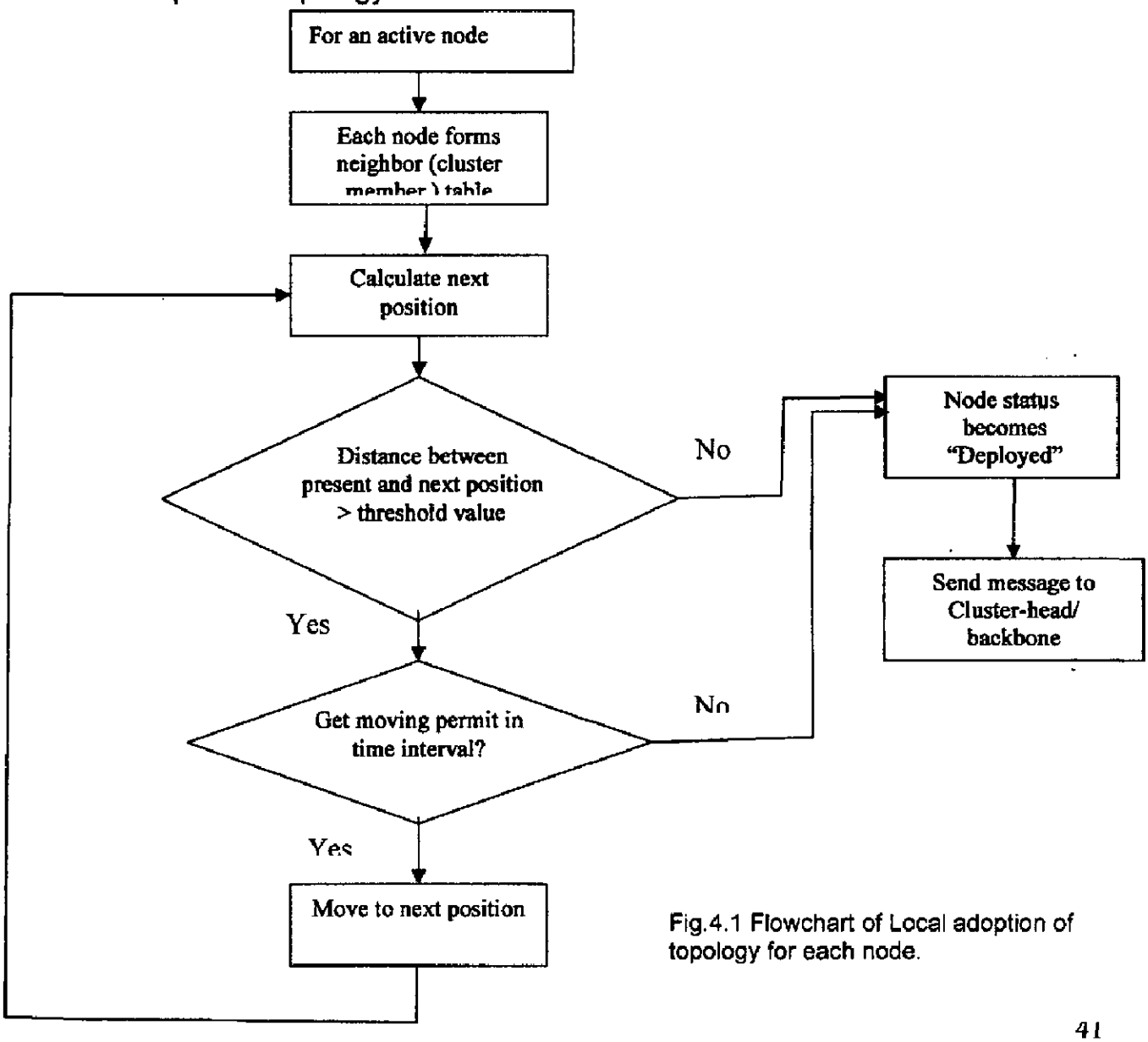


Fig.4.1 Flowchart of Local adoption of topology for each node.

b) *Selection of cluster-head*; By selecting the density of the nodes in the cluster and comparing it with the threshold for HD, it ensures that at least backbones are elected so that every node is in radio range of at least one backbone and one controller through gateway nodes. Figure 4.2 shows the process of electing cluster-heads.

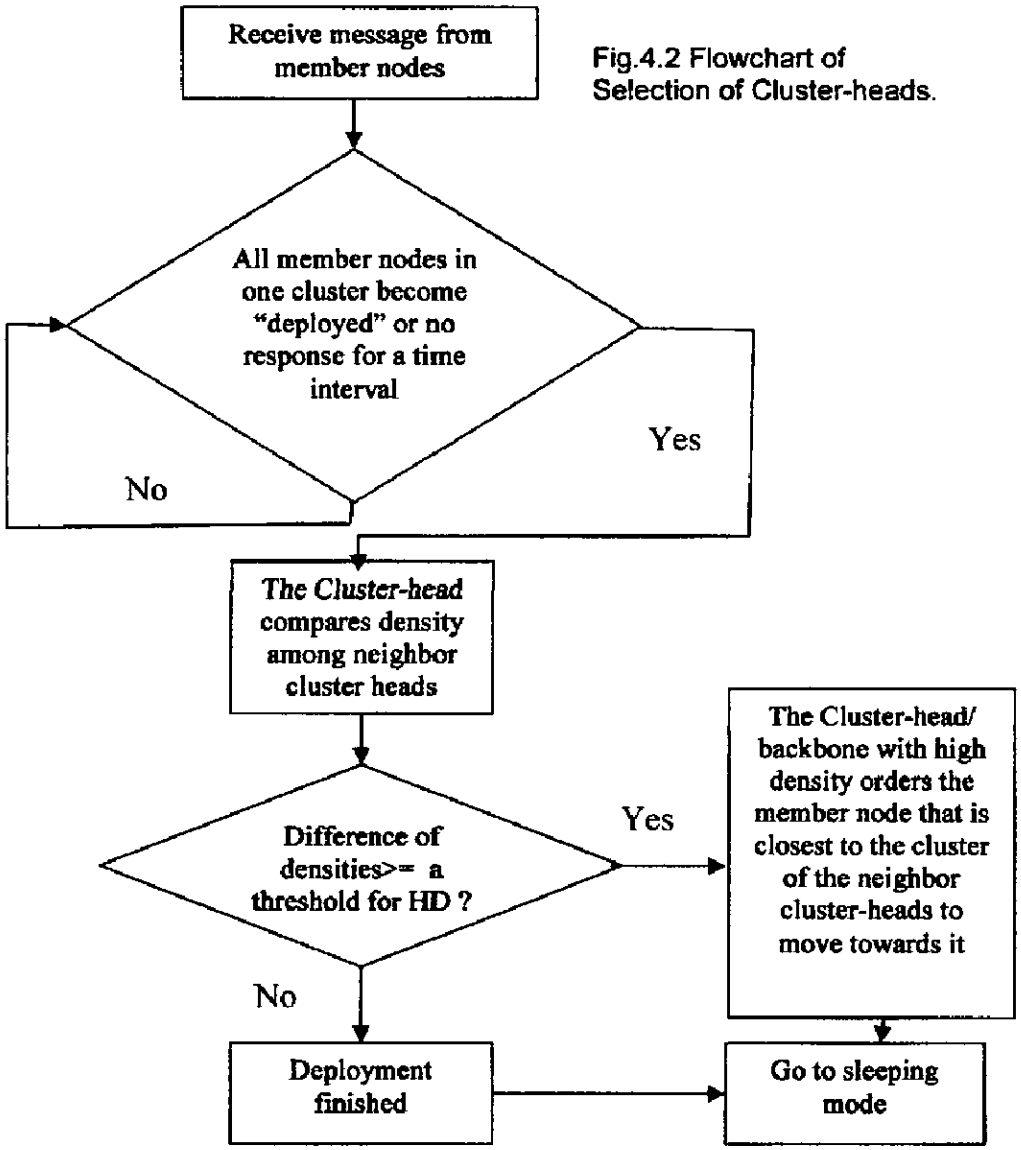


Fig.4.2 Flowchart of Selection of Cluster-heads.

c) *Distributed control and local routing (No central control)*; the algorithm is run in parallel in each and every node in the network i.e. each node only consults state stored in local routing tables during the election process. Figure 4.3 describes the distributed control and local routing of all the nodes.

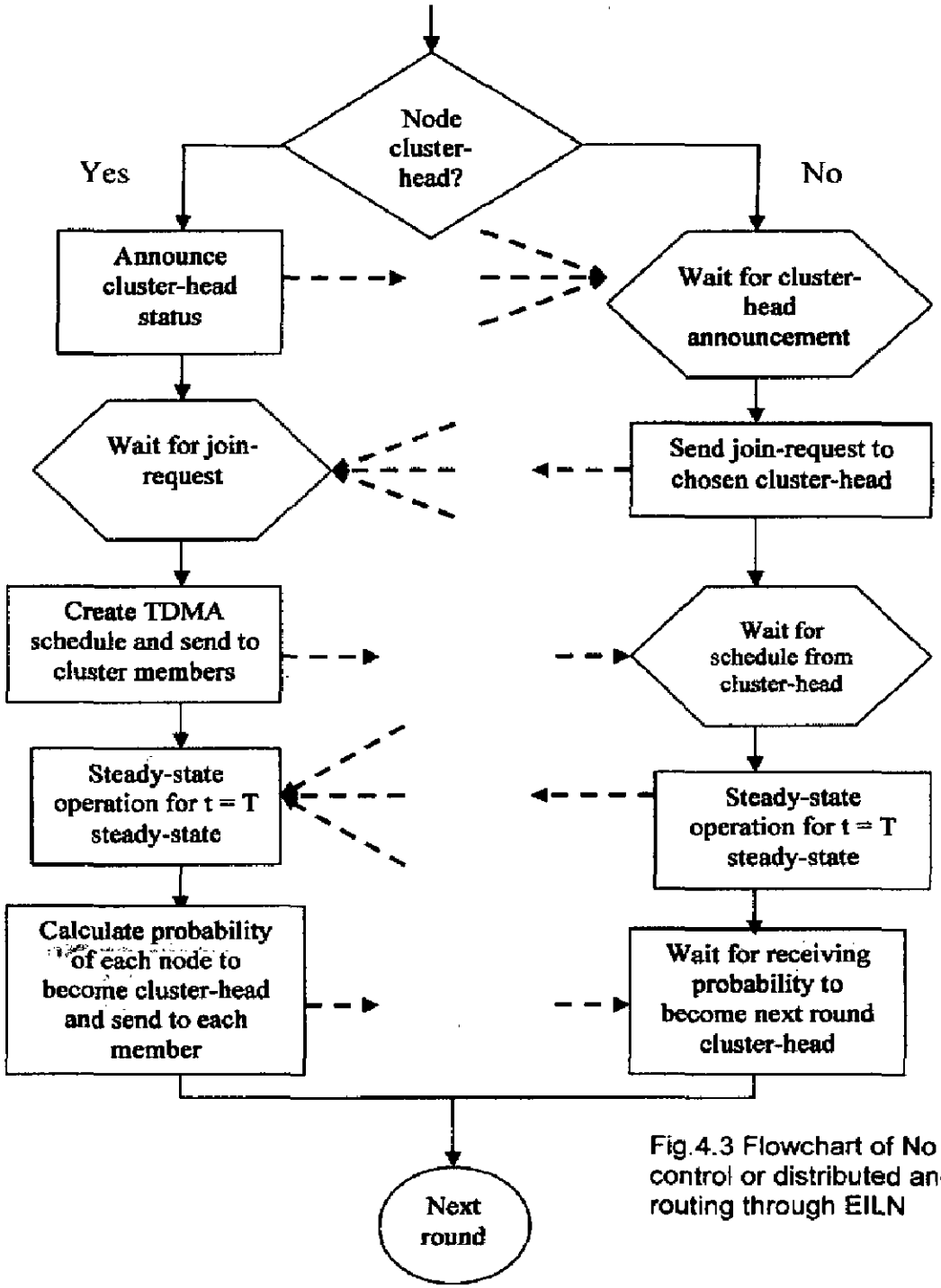


Fig.4.3 Flowchart of No central control or distributed and local routing through EILN

d) *Density of nodes in networks;* The algorithm is to efficiently handle large changes in the number of nodes in the cluster and density of nodes in the networks; it rotates the backbones in order to ensure that all nodes share the task of providing global connectivity roughly equally. For each networks the algorithm attempts to minimize the number of nodes elected as backbones, thereby increasing network lifetime, but without suffering a significant loss of capacity or an increase in latency [77].

e) *Selection of controller*: The flow sheet shown in figure 4.4 shows the algorithm for the selection of a controller by comparing the distance between the present and next path with the threshold value for central location in the approximated centralizes backbone node (centralized) to monitor non-faithful nodes and collection of IP tables using information collected from the backbones.

f) Finally, it connects the temporarily breakdown nodes containing buffer to select the path of data routing/broadcasting. EILN is Hybrid: each node periodically broadcasts HELLO messages and send ACK's that contain the node's status (i.e., whether or not the node is a backbone), its current connector, and its current neighbors. From these HELLO messages, each node constructs a list of the node's neighbors and backbones, and for each neighbor, a list of its neighbors and backbones.

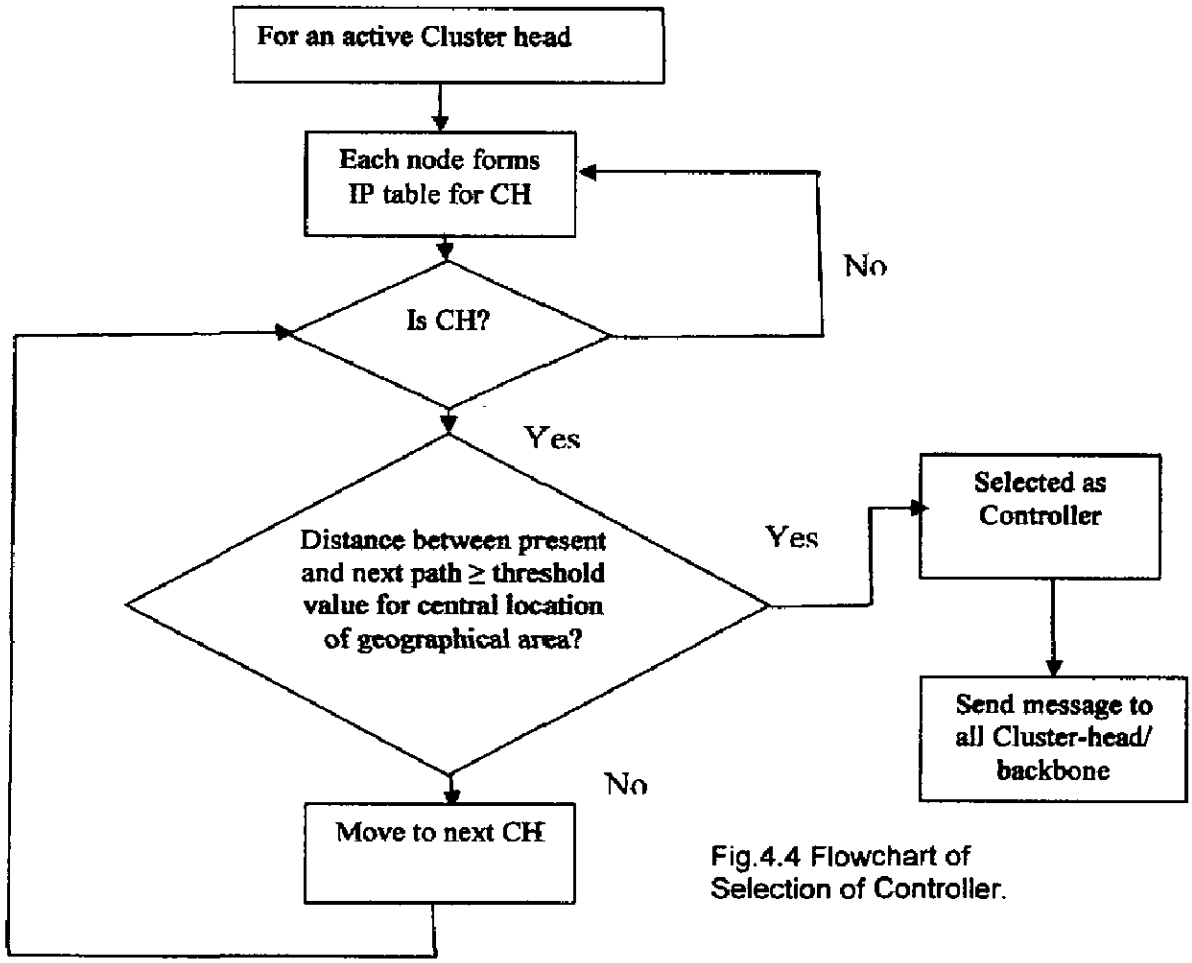


Fig.4.4 Flowchart of Selection of Controller.

As shown in figure 4.5, EILN runs above the link and MAC layers and interacts with the routing protocol. This structuring allows EILN to take advantage of power-saving features of the link layer protocol, while still being able to affect the routing process.

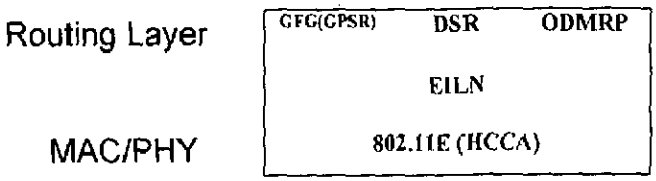


Fig.4.5 EILN is a protocol that operates below the routing layer and above the MAC and physical layers. EILN controls, coordinates and connects the routing layer, which takes advantage of any power saving features of the underlying MAC layer.

When developing the EILN, It was necessary to determine at what layer within the protocol hierarchy to implement infrastructure-less network routing? In the present EILN development have considered two different options: routing at the link layer (ISO layer 2) and routing at the network layer (ISO layer 3). Originally, it is opted to route in link layer and below the network layer for several reasons [RFC 4728]:

i) Pragmatically, running the EILN protocol at the link layer maximizes the number of mobile nodes that is participate in infrastructure-less networks. For example, the protocol can route equally well between IPv4 [RFC791], IPv6 [RFC2460] nodes.

ii) Technically, the developed EILN to be simple enough that it could be implemented directly in the firmware inside wireless network interface cards [20], well below the layer 3 software within a mobile node. Mobile nodes that would otherwise be unable to communicate with the base station due to factors such as distance, fading, or local interference sources could then reach the base station through their peers.

iii) Ultimately, however, it has been decided to specify and to implement [22] EILN as a layer 3 protocol, since this is the only layer at which it could realistically support nodes with multiple network interfaces of different types forming an infrastructure-less networks.

An EILN node switches state from time to time between being a backbone and being a non-backbone. A node includes its current state in its HELLO messages. In EILN, which uses local HELLO messages to propagate topology information, it does not depend on them for correctness: when HELLO messages are lost, EILN elects more backbones, but does not disconnect the backbone. Table 4.1(a,b) describes HELLO packet for EILN and algorithm for EILN node design. To accommodate for link sensing, neighborhood detection and selection signalling, as well as to accommodate for future extensions, an approach similar to the overall packet format is taken. HELLO message frame format is given below:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Reserved   |Node Position|  HELLO time    |  Willingness  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Link Code  |SID| Reserved    |       Link Message Size         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Neighbor Interface Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Neighbor Interface Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                               . . .                             :
:                                                                 :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Link Code  |SID| Reserved    |       Link Message Size         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Neighbor Interface Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Neighbor Interface Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Table 4.1 (a) HELLO message frame format

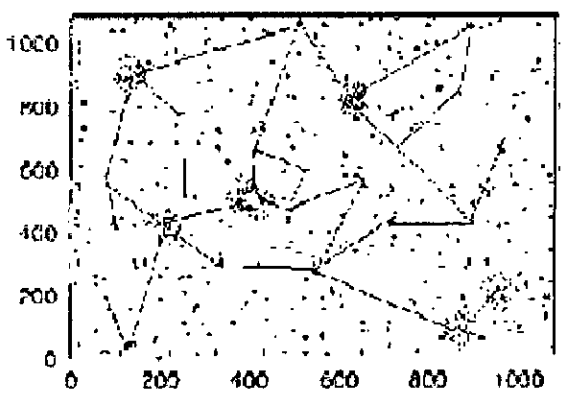


Fig.4.6 a scenario with 100 nodes, 19 backbone nodes, 1 Controller (with big GRAY dot) and a radio range of 250 m and area of 1000*1000 sq. meters.

Figure 4.6 shows the scenario of the election algorithm at a random point in time on a network of 100 nodes in a 1000 m * 1000 m area, where each radio has an isotropic circular range with a 50 m radius. Solid lines connect backbones that are within radio range of each other.

The algorithm presented in this chapter, *EILN*, fulfills the above requirements. Each node in the network running EILN makes symmetrical periodic, local decisions on whether to sleep or stay awake as a *backbone* and participate in the forwarding backbone topology. To preserve capacity, a node volunteers to be a backbone if it discovers, using information it gathered from local broadcast messages, that two of its neighbors cannot communicate with each other directly or through one or two existing backbones. The controller acts as centralized head, which updates the IP table from backbones. It is also a backbone, which is nearly in mid of the geographical network area. Figure 4.7 (a) describes the architecture of Span theory in which a connected backbone does not necessarily preserve capacity. In this connected topology Black nodes are Backbones. Solid and dotted lines connect nodes, which are within radio range of each other. Solid lines represent connection to and between backbones. Figure 4.7 (b) describes the architecture of EILN in which a connected/non-connected backbone preserve capacity using EILN. In this connected topology, Black nodes are Backbones and red is the controller. Solid and dotted lines connect nodes, which are within radio range of each other. Solid lines represent connection to and between backbones and all backbones are connected to red controller.

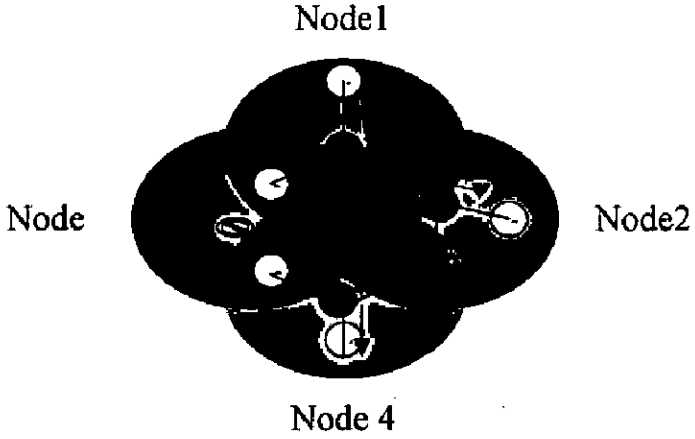


Fig.4.7(a) A Span Architecture

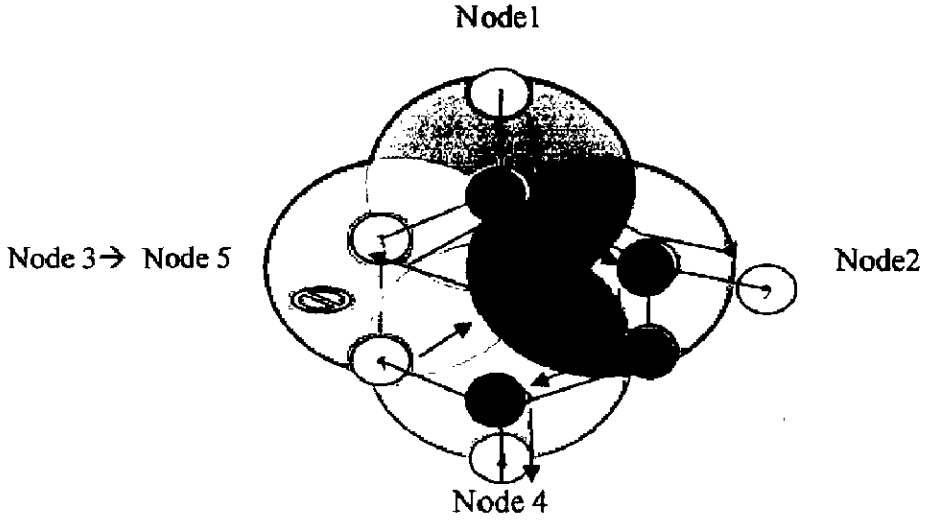


Fig.4.7 (b) An EILN Architecture

4.3 EILN IMPLEMENTATION

This section describes the implementation of developed EILN in terms of geographic forwarding, the 802.11E HCCA power saving mode (with our own improvements), and the energy model used in simulations.

EILN and geographic forwarding

The implementation uses a geographic forwarding algorithm. This implements geographic forwarding primarily because of its simplicity; EILN is used with other routing protocols as well.

EILNs election algorithm requires each node to advertise its backbones, its neighbors, and if it is a backbone, a tentative backbone, or a non-backbone. To reduce protocol overhead, we piggyback EILN HELLO information onto the broadcast updates required by geographic forwarding (see table 4.1b). Each node enters all the information it receives in broadcast updates into a *neighbor table*. Consequently, this neighbor table contains a list of neighbors and backbones, and for each neighbor, a list of its neighbors and backbones [76]. Geographic forwarding forwards packets using a greedy algorithm. The source node annotates each packet with the geographic location of the destination node. Upon receiving a packet for a node not in radio range, a backbone forwards the packet to a

neighboring backbone that is closest to the destination. If no such backbone exists, the packet has forwarded to a non-backbone that is closer to the destination. Otherwise, it is known that a packet has encountered a void, and so it has dropped.

The geographic forwarding algorithm in EILN implements MAC-layer failure feedback and interface queue traversal [56,57]. These mechanisms allow the routing layer to readily remove unresponsive nodes from its routing table and rescue packets using these nodes as the next hop.

TABLE 4.1 (b)
HELLO packet for EILN and geographic forwarding. Italized fields are EILN specific information

Source ID
Node position
Is backbone
Is Connector
Is tentative
Backbone list
Neighbor list

Controller and Backbone Selection algorithm

EILN selects just one controller to centrally monitor the backbones, within the backbones and keep the table of unfaithful nodes, which must be in the mid of geographical area of the network. The algorithm for the are as follows:

i) A node uses information from its neighbor table to determine if it should announce or withdraw itself as a coordinator. A non - coordinator node periodically calls check – announce - coordinator to determine if it should become a coordinator or not. Check - announce - coordinator first computes *C(connect pairs)*, the number of additional neighbor pairs that would be connected if the node becomes a coordinator, using connect-pair.

ii) If $C > 0$, the node computes *delay* by calculating the time require connecting and waits for *delay* seconds before recomputing C.

iii) If *C* continues to be greater than 0 after *delay* seconds, the node announces itself as a coordinator. connect-pair calculates the number of would-be connected neighbor pairs by iterating through the node's neighbors in

the neighbor table.

iv) A similar routine exists for checking if every pair of neighbor nodes can reach each other via one or two other neighbors. That routine is used by the withdraw algorithm.

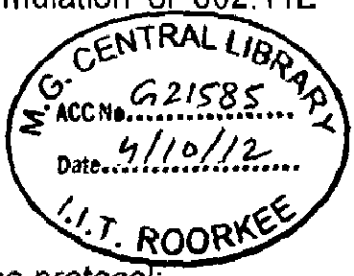
The EILN election algorithm may not react fast enough to elect new coordinators. In the worst case, nodes must wait until the old coordinator information has expired in the neighbor table before a new coordinator can be elected. Because geographic forwarding falls back to using non-coordinators to route packets if coordinators do not exist, a non-coordinator node announces itself as a coordinator if it has received a large number of packets to route in the recent past. If this coordinator turns out to be redundant, the coordinator withdraw algorithm select the node to withdraw itself as a coordinator soon after. Parameter & Setting of 802.11e (HCCA) ad-hoc power-saving mode are given in Table 4.2 below:

TABLE 4.2: 802.11E HCCA SETTINGS:

Transmit Rate: Auto (1, 2, 5.5, or 11 Mbps)
Channel: 2 (2417 MHz), Op. Frq.2.4GHz
Transmit Power :30 mW
Mode : Ad-hoc
Antenna :2.14 dBi rubber duck

EILN determines when to turn a node's radio on or off, but depends on the low level MAC layer to support power saving functions, such as buffering packets for sleeping nodes. The EILN implemented on top of the 802.11e MAC and physical layers with infrastructure-less power saving support [11]. 802.11e infrastructure-less power-saving mode uses periodic beacons to synchronize nodes in the network. Beacon packets contain timestamps that synchronize nodes' clocks. The HCCA ((HCF -Hybrid Coordinator Function) Controlled Channel Access) works a lot like the PCF. However, in contrast to PCF, in which the interval between two beacon frames is divided into two periods of CFP and CP, the HCCA allows for

CFPs being initiated at almost anytime during a CP. This kind of CFP is called a Controlled Access Phase (CAP) in 802.11e. The AP initiates a CAP, whenever it wants to send a frame to a station, or receive a frame from a station, in a contention free manner. In fact, the CFP is a CAP too. During a CAP, the Hybrid Coordinator (HC) -- which is also the AP -- controls the access to the medium. During the CP, all stations function in EDCA. The other difference with the PCF is that Traffic Class (TC) and Traffic Streams (TS) are defined. This means that the HC is not limited to per-station queuing and can provide a kind of per-session service. In addition, the HC can coordinate these streams or sessions in any fashion, it chooses (not just round robin). Moreover, the stations give info about the lengths of their queues for each Traffic Class (TC). The HC can use this info to give priority to one station over another, or better adjust its scheduling mechanism. Another difference is that stations are given a TXOP: they may send multiple packets in a row, for a given time period selected by the HC. During the CP, the HC allows stations to send data by sending CF-Poll frames.Using EILN on top of 802.11e infrastructure-less power saving mode improves routing throughput and packet delivery latency. Because backbones do not operate in power saving mode, packets routed between backbones do not need to be advertise or delayed. To further take advantage of the synergy between EILN and 802.11E power saving mode, we have made the following modifications to our simulation of 802.11E power saving mode.



ALGORITHM VERIFICATION METHODOLOGY STEPS:

a. Acquire needed information to model the protocol;
b. Create a detailed pseudo-code or finite state machine of the protocol;
c. Compare carefully all cases described in the protocol with the pseudo code and verify if they are consistent, if not repeat the previous steps;
d. Create a table with all kinds of packets and the nodes that can generate them (source, intermediate and destination node);
e. Specify the semantics of the packets to each node;
f. Divide the protocol into internal and external behaviors

(ii) Internal behavior: describes the message flows and behaviors for the node;

(iii) External behavior: describes the behaviors related to the node interactions;

(iv) Understand each aspect of the protocol; create an algorithm or an state machine representation to understand it better;

g. *Model the External vs. Internal interactions*

(i) The internal behavior should be modeled as if it was a routine call.

(ii) In this way the external behavior becomes independent of the internal behavior. Ideally, the external and internal behaviors should be independent;

h. *Start with a simple model and continuously increase the model complexity*

(i) For each error found

(ii) Verify whether the error is due to a protocol failure or a modeling failure;

(iii) Find a solution for the problem;

(iv) Model the solution;

(v) Test the solution;

(vi) Increase the model complexity;

i. Identify and isolate verified procedures to be used in other protocols.

4.4 PERFORMANCE EVALUATION

To measure the effectiveness of EILN, this section describes the simulation environment and results of EILN, with geographic forwarding, on several static and mobile topologies. The analysis carried out for static and mobile topologies are as follows:

a) Static Topology:

i) Cumulative distribution of per-link delivery rates on the network

ii) Packet delivery rate as a function of per-CBR-flow bit rate.

b) Mobility (Dynamic) Topology:

i) Packet loss rate as a function of pause time

ii) backbone density as a function of node density

iii) network performance in case of 50 bytes Vs. 1024 bytes

iv) Amount of energy saved in the EILN

v) Energy saving as function of *fup*

vi) Energy saving as a function of α

The Simulation parameters for the above are as follows:

No. of nodes taken	50, 120 or otherwise specified
Simulation area	1000 m * 1000 m
Bandwidth	2 Mbps
Radio range	250m
Data	CBR-128 Byte packets for static and 50 bytes Vs.1024 bytes for mobile
Simulation Time	400Secs
Mobility model	random waypoint motion model
Polling time	100msec.
Freq.	2.4Ghz
Transmit power	30mW

4.5 RESULTS & CONCLUSION

The proposed EILN is implemented using NS-2. The geographic forwarding algorithm, as described in section 4.3, routes packets from source to destination. EILN runs on top of the 802.11 MAC layer with power saving support.

4.5.1 Effects of Static:

The analysis carried out for static to find out Cumulative distribution of per-link delivery rates on the network and packet delivery rate as a function of per-CBR-flow bit rate.

(i) Figure 4.8 shows that the cumulative distribution of delivery rates across all links for each of the two packet sizes. The two directions between each node pair are considered as separate links. The fig.4.8 shows that about 50% of the links deliver no packets, while the best 20% of links deliver more than 95% of their packets. The delivery rates of the remaining 30% of links are approximately evenly distributed. Shortest-path routing works well if all links have similar characteristics, because a longer route won't provide better end-to-end performance.

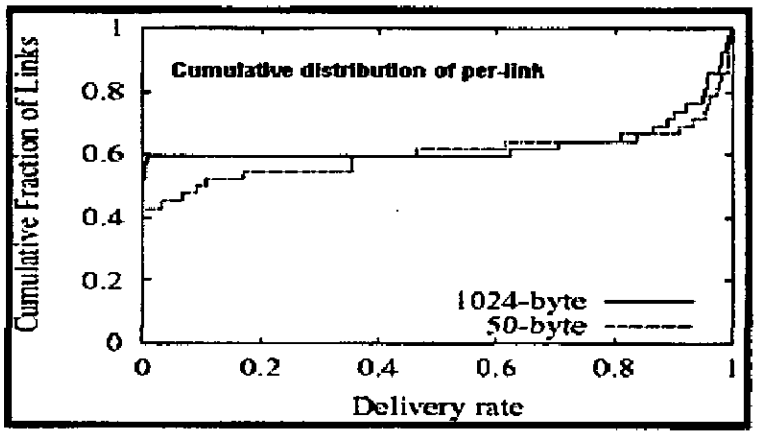


Fig.4.8 Cumulative distribution of per-link delivery rates on the network. Many links are of intermediate quality.

(ii) In this section, it compares the performance of EILN against both unmodified 802.11 MAC in power saving mode and unmodified 802.11 MAC not in power saving mode. For convenience, it will refer to them as EILN, 802.11 PSM, and 802.11. To evaluate EILN in different node densities, we simulate 120-node networks in square regions of different sizes. Nodes in our simulations use radios with a 2 Mbps bandwidth and 250 m nominal radio range. Twenty nodes send and receive traffic. Each of these nodes sends a CBR flow to another node, and each CBR flow send 128-byte packets. The result shows in figure 4.9 that each packet traverses six hops. Under higher traffic load, EILN delivers more packets than 802.11 PSM, but slightly less than 802.11B.

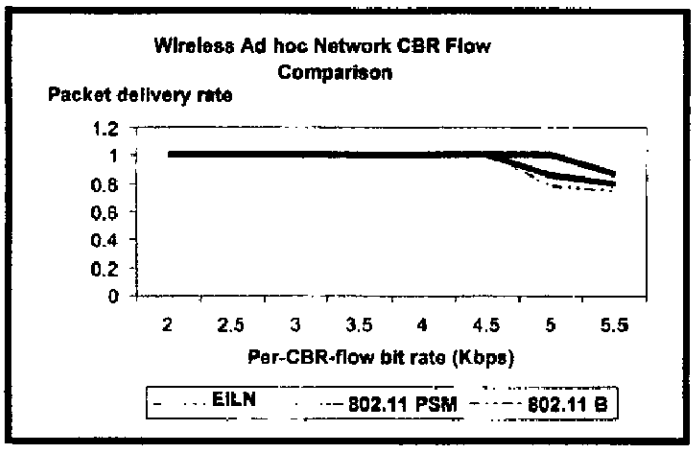


Fig.4.9 Packet delivery rate as a function of per-CBR-flow bit rate.

4.5.2 Effects of mobility:

The analysis carried out for mobile topologies for Packet loss rate as a function of pause time, backbone density as a function of node density, network performance

in case of 50 bytes Vs. 1024 bytes, Amount of energy saved in the EILN, Energy saving as function of *fup*, Energy saving as a function of *α are as follows:*

(i) Figure 4.10 shows the effects of mobility on packet loss rate. In these simulations, an area of 1000 m * 1000 m is used. Here, Mobility does not affect EILN very much, and Geographic forwarding with EILN delivers more packets than with 802.11 PSM and 802.11 because it encounters fewer voids.

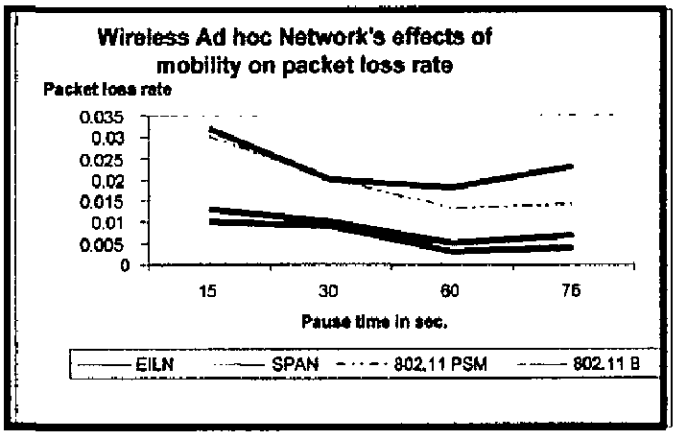


Fig.4.10 Packet loss rate as a function of pause time.

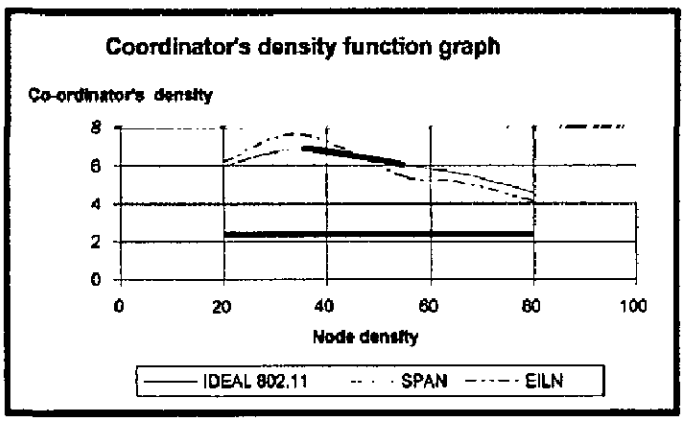


Fig. 4.11 Ideal and actual backbone density as a function of node density. The ideal curve represents an approximate lower bound on the number of Backbones needed. EILN elects more backbones than the ideal case Because of lower node density, backbone rotation, and announcement collision.

(ii) Nodes follow the random waypoint motion model, and the length of the pause time reflects the degree of mobility. The degree of mobility does not significantly affect routing with Span backbones. Span consistently performs better than both 802.11 PSM and 802.11. Most packet drops in these simulations are caused by temporary voids created by mobility. Because geographic forwarding with Span encounters fewer voids, its loss rate is lower. Figure 4.11 shows backbone density as a function of node density. For each node density, backbone density has computed from the average number of backbones elected by Span over 500 s of five mobile simulations.

(iii) A non-backbone node must stay up for the entire duration of the advertised traffic window (100 ms). Figure 4.12 shows the network performance in case mobility of nodes transmitted 50 bytes Vs. 1024 bytes packet as it shows almost similar performance then static topology.

(iv) Figure 4.13 shows the Per-node power usages. This yields that EILN provides significant amount of Savings over 802.11 PSM and 802.11.

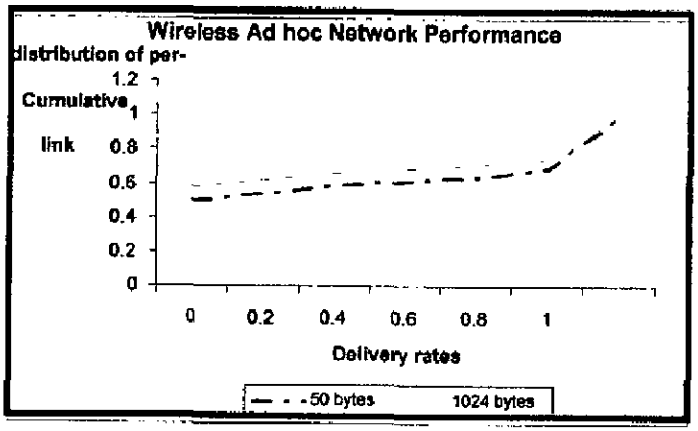


Fig. 4.12 shows the network performance in case of 50 bytes Vs. 1024 bytes.

(iv & v) This defines as the ratio of the power consumption of the radio in sleep mode to the power consumption of the radio in idle mode. Then, using *fidle*, the amount of energy savings can be estimate as

$$1 \div [F_{idle} + \alpha (1 - F_{idle})]$$

Note that because f_{idle} depends on *C/N* and that the backbone density stays the same for different node densities, the gain in energy savings also depends on the node density. Figure 4.14 plots equation as a function of α, substituting C_{ideal} and 0 as values for *C* and f_{up}. This figure shows that the amount of energy saving increases rapidly, as the value of α decreases. Our energy model uses α = 0.157 from measurements.

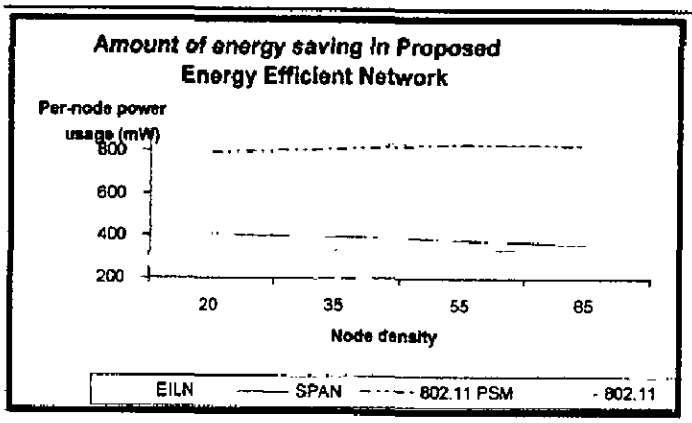


Fig. 4.13 Per-node power usage. EILN provides significant amount of Savings over 802.11 PSM and 802.11.

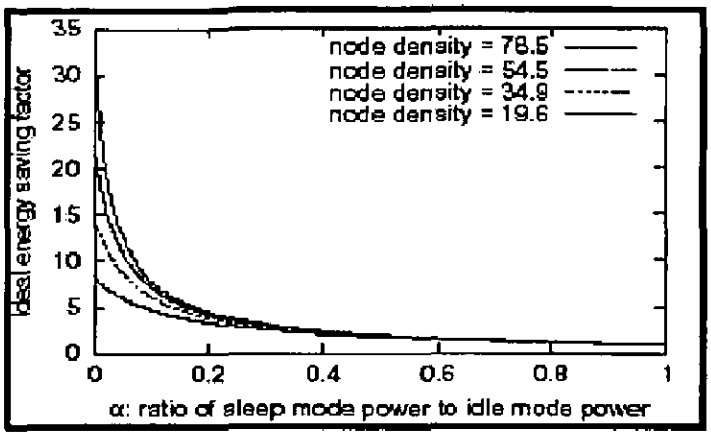


Fig.4.14 Energy saving as a function of $\alpha(\alpha=0.16)$, substituting Cideal and 0 as values for *C* and *fup*.

Figure 4.15 plots energy saving as a function of *fup*, using Cideal and 0.157 as values for *C* and α. This figure shows that as *fup* increases, the gain in energy savings decreases as well. These two figures explain why in figure 4.13, the gain in energy savings is a sub-linear function of node density. The numbers in the *fup* column are calculated using values from the "Idle time" column as *fidle*. We substitute *C/N* with numbers in the "Time as backbone" column divided by 500 s. This column suggests that EILN broadcast messages are expensive when density is high – the large number of broadcast messages per radio range keeps nodes awake for a longer period.

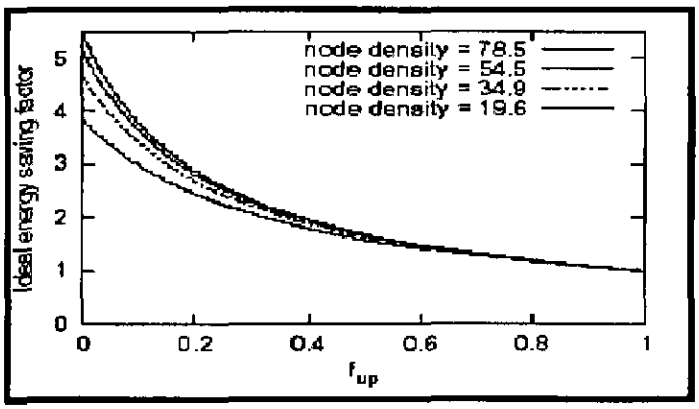


Fig.4.15 Energy saving as function of *fup* (*fup* is in between 0.185 to 0.263) , using Cideal and 0.157 as values for *C* and α.

This chapter presents *EILN*, a distributed as well as centralized coordination technique for multi-hop infrastructure-less wireless networks. EILN adaptively elects *backbones* from all nodes in the network, and rotates them in time. EILN backbones stay awake and perform multi-hop packet routing within the infrastructure-less network, while other nodes remain in power-saving mode and

periodically check if they should awaken and become a backbone. With EILN, each node uses a random back-off delay to decide whether to become a backbone. This delay is a function of the number of other nodes in the neighborhood that can be bridge using this node and the amount of energy it has remaining. To identify the unfaithful nodes in the particular geographic region and to control backbone, we introduced a controller from the backbones, which must be fall in the middle of geographical area of complete network. The amount of energy that EILN saves increases only slightly as density increases. This is largely because the current implementation of EILN uses the power saving features of 802.11, in which nodes periodically wake up and listen for traffic advertisements. Section 4.5 shows that this approach is extremely expensive. This warrants investigation into a more robust and efficient power saving MAC layer, one that minimizes the amount of time each node in power saving mode must stay up.

COMPARISON OF DEVELOPED EILN WITH OTHER PROTOCOLS (PRO's & CON'S)

Reported literature	***methodology***	***Comparison with EILN***
Das and Bharghavan [45]	Approximate the minimum connected dominating set of an ad hoc network, and route packets using nodes from that set.	The set of backbones elected by EILN, however, has the additional property of being capacity preserving. Consequently, the connected dominating set elected by EILN is likely to be larger than a minimal connected dominating set. For example, the black nodes in figure 4.6 form a minimal connected dominating set. However, EILNs election algorithm would additionally elect node 5 to be a backbone to preserve capacity.
Wu and Li [46]	A distributed algorithm for approximating connected dominating sets in an ad hoc network that also appears to	Their algorithm is similar to EILNs backbone election algorithm. EILN, however, elects fewer backbones because it actively prevents

	preserve capacity.	redundant backbones by using randomized slotting and damping.
Wu and Gao [47]	Power aware routing using the connected dominating sets.	
GAF [77] scheme of Xu et al.	Nodes use geographic location information to divide the world into fixed square grids. The size of each grid stays constant, regardless of node density. Nodes within a grid switch between sleeping and listening, with the guarantee that one node in each grid stays up to route packets.	Similar goals to EILN. EILN differs from GAF in two important ways. First, unlike GAF, EILN does not require that nodes know their geographic positions. Instead, EILN uses local broadcast messages to discover and react to changes in the network topology. Second, EILN integrates with 802.11 power saving mode nicely: no backbone nodes is still receive packets when operating in power saving mode.
AFECA [48]	each node maintains a count of the number of nodes within radio range, obtained by listening to transmissions on the channel. A node switches between sleeping and listening, with randomized sleep times proportional to the number of nearby nodes. The net effect is that the number of listening nodes is roughly constant, regardless of node density; as the density increases, more energy will be saved. AFECA's constants are chosen so that there is a high probability that the listening nodes form a connected graph, so that ad hoc forwarding works. An AFECA node does not know whether it is required to listen in order to maintain connectivity, so to be conservative AFECA tends to	EILN differs from AFECA in that, with high likelihood, EILN never keeps a node awake unless it is essential for connecting two of its neighbors. Furthermore, EILN explicitly attempts to preserve the same overall system capacity as the underlying network where all nodes are awake, which ensures that no increase in congestion occurs.

	make nodes listen even when they could be asleep.	
PAMAS power-saving medium access protocol [49,50]	Turns off a node's radio when it is overhearing a packet not addressed to it.	This approach is suitable for radios in which processing a received packet is expensive compared to listening to an idle radio channel.
Kravets and Krishnan [51]	A system in which mobile units wake up periodically and poll a base station for newly arrived packets.	EILN controls whether or not the receiver is powered on, rather than controlling the transmit power level. It also pays close attention to overall system capacity, in addition to maintaining connectivity.
Stemm and Katz [52]	Setting the on/off periods based on application hints reduces both power and delay.	
Smith et al. [53]	An ad hoc network that elects a virtual base station to buffer packets for local nodes. They do not, however, attempt to make sure that enough of these base stations are present to preserve connectivity in a multi-hop ad hoc network.	
Chang and Tassiulas [54].	Maximize overall network lifetime by distributing energy consumption fairly have extended this approach. In this protocol, nodes adjust their transmission power levels and select routes to optimize performance.	
Wattenhofer et al. [57]	A topology maintenance algorithm using similar underlying radio support, but their algorithm guarantees global connectedness using directional information.	

CHAPTER-5

ANALYZING AND DEVELOPMENT OF THE CRYPTOGRAPHY ALGORITHM FOR SECURE AND ATTACK PREVENTIVE DECENTRALIZED INFRASTRUCTURE-LESS WIRELESS NETWORK

CHAPTER-5

ANALYZING AND DEVELOPMENT OF THE CRYPTOGRAPHY ALGORITHM FOR SECURE AND ATTACK PREVENTIVE DECENTRALIZED INFRASTRUCTURE-LESS WIRELESS NETWORK

5.1 INTRODUCTION

Transformation of information from comprehensive form into an incomprehensible one and vice-versa is known as Cryptography, rendering it unreadable by interceptors or eavesdroppers without secret knowledge. Cryptography is the science of keeping message secure and cryptanalysis is an art and science of breaking cipher-text (the coded message or information). A wireless infrastructure-less network or nodes has no fixed infrastructure such as base stations or mobile switching centers. Deploying a secure protocol for wireless infrastructure-less network especially, Cryptology or Cryptography regarding mobile, decentralized nodes is always a challenge before us. Inserting the cryptography provides ad-on security, authentication, integrity, non-repudiation and confidentiality in wireless infrastructure-less network information interchange. However, implementing the cryptography for an infrastructure-less network to some infrastructure wireless network will now provide the gateway to think among the research communities. In pursuance of that, this chapter presents the idea for implementation of cryptography in the transport/network layers of wireless infrastructure-less network. However, the cryptography scheme can be extended in application (for SMTP, SNMP), session (for Internet based terminal session), transport (for TLS, SSL), network (for IPSec in IPV4 & IPV6), link / MAC (LLS) layers infrastructure-less based networks. It needs cryptography and cryptanalysis for authentication, integrity, non-repudiation, confidentiality/ secrecy, and availability. As cryptology begins to see wide application and acceptance, one thing is increasingly clear: if it is going to be as effective as the underlying technology allows it to be, there must be interoperable standards. Interoperability requires strict adherence to agreed-upon standards.

This chapter is broadly divided into two schemes. Scheme 1 deals with the development of Generic Cryptography Algorithm (GCA) for infrastructure-less networks and Scheme 2 deals with Mathematical Modeling of Combined Threshold & ID based cryptography.

5.2 RELATED WORK

The literature review broadly classified the nature of wireless networks in three categories:

i. Wireless infrastructure-based cryptography

ii. Wireless sensor network (WSN) cryptography

iii. Wireless infrastructure-less (Ad hoc) cryptography

However, the research community roughly distinguishes infrastructure-less and wireless infrastructure-less networks into two categories. On the one side there are the systems researchers who build real infrastructure-less on wireless infrastructure-less networks and on other side simulation based infrastructure-less nodes are the key research interest. Thus, WSN and Infrastructure-less cryptography scheme are broadly classified into one category. Quoting of the latest reference of white paper site "Wireless infrastructure-less network applications require wireless infrastructure-less networking techniques."[Latest Technology , Friday, September 4, 2009]. Based on the various literature surveys [78-87] the above wireless networks are broadly categorized into two sections:

i. Physical or logical attack detecting schemes

ii. Global node positioning schemes

5.2.1 Wireless infrastructure-based cryptography:

Physical or logical attack detecting schemes:

Most attack detecting schemes use neighbors' cooperative technique to detect malicious nodes. G. Wang et al. in [78] has proposed a distributed cooperative failure detecting mechanism to let the neighbors of a faulty node cooperate to detect the failure. To achieve neighbors' communication efficiency, G. Wang et al.

developed a Tree-based Propagation-Collection (TPC) protocols to collect the information from all neighbors of the suspect with low delay, low message complexity, and low energy consumption. S. Marti et al. [79] have proposed the Watchdog, which also uses neighbors to identify misbehaving nodes. M. Ding et al. [80] reported another localized approach to detect the faulty nodes by using neighbors' data and processing them with the statistical method. Threshold approaches is a special type of neighbors' cooperative approach, proposed by B. Krishnamachari et al. [81]. Recently, Liu et al. [82] introduced a new neighbors' cooperative approach to detect insider attacks. The nice feature of their algorithm is that it requires no prior knowledge about normal or malicious nodes, which is important considering the dynamic attacking behaviors. Further, their algorithm can be employed to inspect any aspects of networking activities, with the multiple attributes evaluated simultaneously. A number of software's based code testing schemes has been proposed by A. Seshadri et al. [83], which rely on optimal program code and exact time measurements. Some hardware-based code testing schemes have been proposed by R. Sailer et al.[84], which are based on public-key cryptography. This approach is not suitable for WSN's because it require extensive computational power, as well as the transmission of large messages. Krauss et al. [85] assumes that some cluster nodes posses much more resources than the majority of clusters and are equipped with a Trusted Platform Module in the hybrid WSN's.

Global Node Positioning scheme:

In some location systems, several infrastructure-less have a position system such as GPS to locate their positions. This type of infrastructure-less is known as beacon node. These location systems use location information from these beacon nodes to construct the whole location system by utilizing ultrasound and time-of-flight techniques. A mechanism for position verification, called Verifiable Multilateration (VM), proposed by S. Capkun et al. [86], is based on Distance bounding techniques proposed by S. Brands et al. [87] that can prevent compromised nodes from reducing the measured distance. VM use the distance

bound measurements from three or more reference points (verifiers) to verify the position of the claimant.

In 2005 Yang pointed out that Novikov and Kiselev scheme is insecure against the man-in-middle attack. Awasthi showed another evidence of man-in-middle attack, but did not suggest any improvement.

5.2.2. Wireless infrastructure-less Sensor network (WSN) cryptography and Wireless infrastructure-less (Ad hoc) cryptography

Physical or logical attack detecting schemes:

A. Seshadari et al. [83] assumes that the attacker's hardware devices were not present in the node network for the duration of the repair process, which is different from many application scenarios.

H. Song et al. [88] provide a method to detect node compromise by comparing the previous position of nodes with current position. The main idea of their mechanism is based on the assumption that a node compromise often consists of three stages: physically obtaining and compromising the nodes, redeploying the compromised nodes, and compromised nodes launching attacks after their rejoining the network.

In some applications an attacker may not be able to precisely deploy the compromised nodes back into their original positions. Their mechanism can detect compromise events, when compromised nodes change positions or identities. Their mechanism can detect compromised nodes when attackers use the physically capturing and reprogramming method. But it cannot detect compromise nodes when attacks use soft attacks.

Global Node Positioning scheme:

L. Lazos et al. [89] propose a range overlapping method instead of using the expensive distance estimation method. Its main idea is as follows: each locator transmits different beacons with individual coordinates and coverage sector areas. After receiving enough sector information from different locators, the infrastructure-less estimates its location as the center of gravity of the overlapping region of the

sectors that include it. Due to adversaries' attacks, the beacon nodes or normal nodes maybe compromised.

Some location systems estimate location by combining deployment knowledge and probability theory without beacons node. Fang et al. [90] propose integrated pre-deployment knowledge of infrastructure-lesss and the Maximum Likelihood Estimation method to estimate the infrastructure-lesss' locations. M. Tatebayashi et al. [91] propose the Key distribution Protocol (KDP) for resource-starved devices for mobile environment. Park et al. [92] point out weaknesses and improvements. M. Beller and Y. Yacobi [93] further develop key agreement and authentication protocols. C. Boyd and A. Mathuria [94] survey the previous work on key distribution and authentication for resource-starved devices in mobile environments. The majority of these approaches rely on asymmetric cryptography. P. Bergstrom et al. [95] consider the problem of secure remote control of resource-starved devices in a home.

A security protocol for infrastructure-less networks SPINS proposed by Adrain Perrig et al. [96] claims to have two secure building blocks: SNEP and μTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA provides authenticated broadcast for severely resource-constrained environments. The major drawbacks of SPINS are repudiation, non-availability, non-interoperability and high-energy consumption require for overhead security protocol.

GCA (Generic Cryptography algorithm) a asymmetric cryptography scheme, removes all the major drawbacks of the SPINS.

Key distribution Protocol (KDP) is developed for resource-starved devices in a mobile environment [97]. Park et al. [92] point out weaknesses and improvements. Beller and Yacobi [93] further develop key agreement and authentication protocols. Boyd and Mathuria [94] survey the previous work on key distribution and authentication for resource-starved devices in mobile environments. The majority of these approaches rely on asymmetric cryptography. Bergstrom et al. [95]

consider the problem of secure remote control of resource-starved devices in a home.

In Scheme 2, Shamir et al. [98] introduced the concept of identity-based (ID-based) systems to simplify key management procedures of CA-based Public Key Infrastructure (PKI). Since then, several ID-based signature schemes have been proposed [99-101]. ID-based systems can be a good alternative for CA-based systems from the viewpoint of efficiency and convenience. ID-based systems have a property that a user's public key can be easily calculated from his identity by a publicly available function, while a trusted Key Generation Center (KGC) can calculate his private key. They enable any pair of users to communicate securely without exchanging public key certificates, without keeping a public key directory, and without using online service of a third party, as long as a trusted KGC issues a private key to each user when he first joins the network.

Ever since threshold signature was first proposed by Desmedt and Frankel [102], several threshold signature schemes [103-107] from bilinear pairings have been proposed. A. Boldyreva et al. [103] proposed a robust and proactive threshold signature scheme, which works in any Gap Diffie-Hellman (GDH) group. Baek and Zheng [104] formalized the concept of identity-based threshold signature and gave the first provably secure scheme. Chen proposed an ID-based threshold signature scheme without a trusted KGC. Cheng et al. [106] proposed an ID-based signature from m-torsion groups of super-singular elliptic curves or hyper-elliptic curves. It is proved that the time of Tate pairing operations is a half of that of Weil pairings [107].

The present analysis has been carried out on development of GCA (Generic Cryptography Algorithm) and development steps for id-based (t,n) threshold signature scheme from Tate pairings. Scheme 1 describes the details of GCA and scheme 2 describes the threshold signature scheme from Tate pairings.

5.3 STEPS FOR DEVELOPMENT OF CRYPTOGRAPHY ALGORITHM

GCA Node Description

Generic Cryptology Algorithm's prototype node will consists of nodes, which are tiny, self-contained, battery-powered computers with radio links, which enable them to communicate and exchange data with one another, and to self-organize into infrastructure-less networks. The hardware and software description of prototype GCA nodes is described in tabular form in Table 5.1. Motes/ nodes form the building blocks of wireless infrastructure-less and infrastructure-less networks, developed by collaborative efforts of University of California Berkeley and the Intel Research Berkeley laboratory.

CPU	16,32,64-bit; 4-866MHz
Storage	8-64KB instruction flash 512 bytes-1GB RAM 512 bytes-1GB EEPROM
OS	Tiny-OS (for infrastructure-less only)
OS code space	3500 bytes (for infrastructure-less only)
Routing Protocol	AODV, DSDV, DSR, TORA (for infrastructure-less nodes) LEACH (for wireless infrastructure-less nodes)

Table 5.1: Characteristics of prototype GCA nodes

However, distributed programming abstractions, like Remote Procedure Calls (RPC), the Distributed Object Model (DOM), or Distributed Shared Memory (DSM) have traditionally simplified and enabled the implementation of complex distributed systems. Figure 5.1 describes the secure on-demand route discovery protocol without GCA.

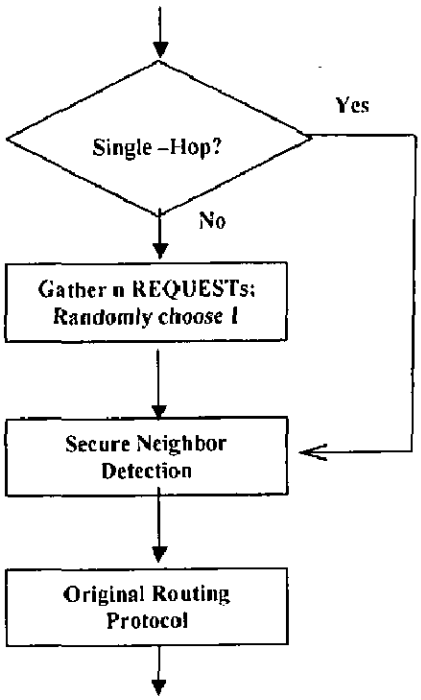


Fig. 5.1 Secure on-demand route discovery protocol without GCA

GCA mechanism provide protocol description in Figure 5.2, in which node send the message to its parent node (PROBE: a→b : probe_prt). If parent hears the message then it gives a reply message, which tells if it could contact Backbone/ Cluster head(BACK_Y: p→a: connected || hopes). If the reply message is not sent then the node broadcasts a request message to neighbour node (RQST: a→ NEIGHBOURS: request_parent). Any neighbour nodes who can connect to the radio range of Backbone/ Cluster head send reply message to the node which contains the ID of parent node (RPLY: c→a : connected || c_hopes || c.parent).

For the developed GCA for wireless infrastructure-less infrastructure-less network requires basic set of mechanism to support Cryptology for mobile infrastructure-less nodes, includes the following:

- *GC Key Generation*
- GC Key Derivation

The above mechanism is briefly described in sub-section Key Management and agreement for GCA.

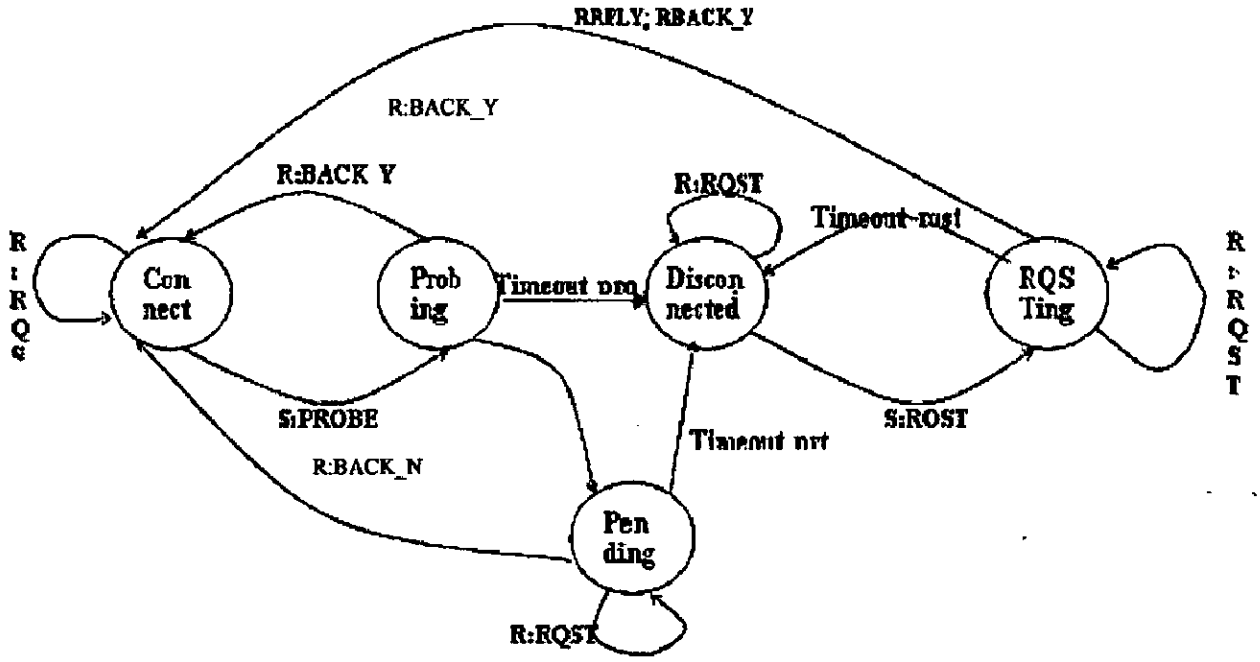


Fig.5.2 GCA protocol description with finite state machine (FSM)

Key Management and agreement for GCA

For security, key management is very important and complex, especially in symmetric cryptography structures. Many current key management proposals, such as [20-23], do not consider the node compromise distribution. They imply the probability of node compromise to be the same for every node. However, when their security system is deployed in a different environment from their supposition, the security performance will decrease greatly. Figure 5.3 describes the Symmetric Cipher historic Model for secure network.

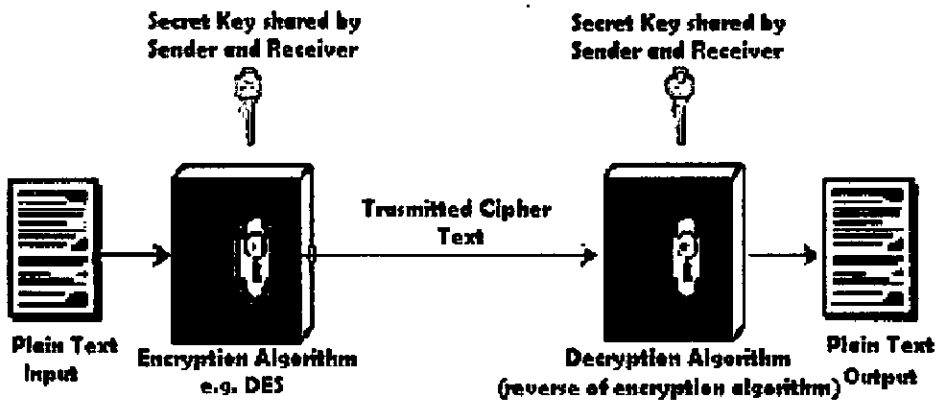


Fig.5.3 Symmetric Cipher historic Model for secure network

Key management security requires topology-specific and efficient key management system. Nodes must have to make a mutual agreement on a shared secret or exchanged public keys. Like in more dynamic environments the exchange of encryption keys may be addressed on-demand. In less dynamic environments, the keys are mutually agreed proactively or configured manually. Private keys are stored in the nodes confidentially to encrypt with the system key with proper hardware protection (smart cards). The infrastructure-less keying mechanism agreement is shown in Figure 5.4, which consists of ancestor sets and the arrow shows the distribution management.

The security scheme proposed by H. Chan et al. [108] requires q common keys (q is a constant, $q \geq 1$) to establish secure communications between a pair of nodes. In their scheme, q is equal in each area. When this schemes is deployed in a gradient based environment, the security performance will decrease because: the system has the same ability to tolerate or defend against node compromise in all areas, but adversaries attack the system with different strengths on different areas; thus making the system unable to provide enough security in some areas, and able to provides more security than needed in other areas. Of course, by increasing q to get enough security everywhere, but it will consume more resources. It looks difficult to get a high security performance with a low overhead; however, when it applies to a node compromise distribution model to this security mechanism, it conclude that this is the key in solving this issue. For example, if q to follow the same distribution as the node compromise distribution model, i.e.,, where (x, y) is the coordinates of node, the system may resolve the issue. In the modified security scheme GCA, the ratio between the strength of preventions and attacks can be kept the same in every area. In gradient-based application schemes [109, 110], uses threshold property λ (when the number of compromised nodes is less than the threshold λ, the probability that any nodes other than these compromised nodes are affected is close to zero), they need more resources to implement this desirable threshold, when they are deployed in a gradient-based application environment. Similarly, it also apply λ to follow the same distribution as

the node compromise model of the given application environment to ease the issue.

Besides improving the key pre-distribution step of key management, it can also apply our developed models to infrastructure-less network for node management, re-keying frequency, etc. with the similar modification method in order to improve system performance and security.

Wireless Infrastructure-less Network Key Mechanism

The infrastructure-less networks keying mechanisms are consist of:

i. ID-based cryptography

- Master public key/secret key is generated by private-key generation service (PKG)

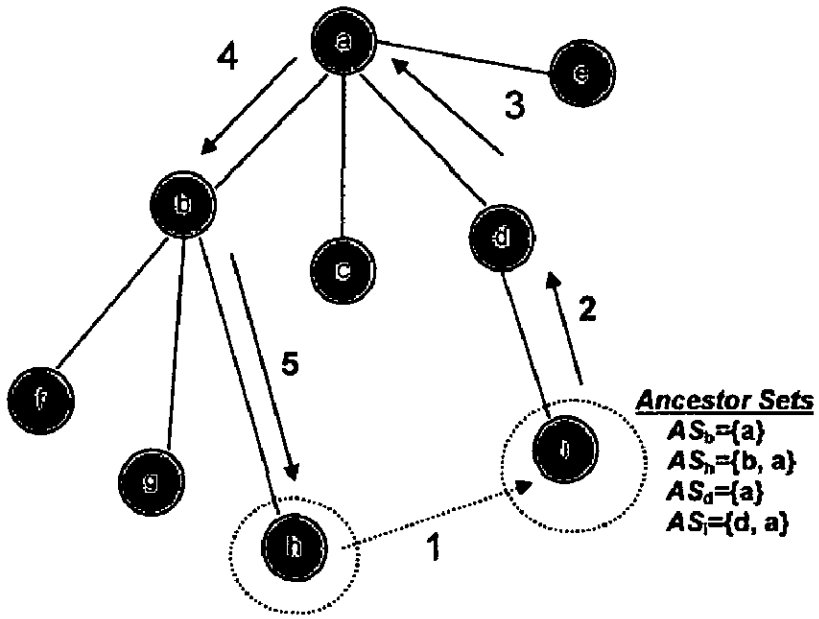


Fig. 5.4 Infrastructure-less keying mechanism agreement

- Master keys known to everyone
- Arbitrary identities are public keys
- Identity: "A1"
- Public key: "Master-Public-Key | A1"

- Private keys should be delivered to nodes by PKG

ii. ID-based encryption schemes

- *Setup*: input a security parameter, return master public/secret keys
- *Extract*: input master secret key and identity, return the personal secret key corresponding to identity
- *Encrypt*: input master public key, the identity of the recipient and message, return cipher-text
- *Decrypt*: input master public key, cipher-text and a personal secret key, return plaintext

iii. Threshold cryptography

- Allows operations to be "split" among multiple users
- In *t*-out-of-*n* threshold scheme, any set of *t* users can compute function while any set of *t*-1 users cannot
- If adversary compromises even *t*-1 users, he cannot perform crypto operation
- Honest user who needs to perform crypto operation should contact *t* of users
- Secure against Byzantine adversaries exist for $t < n/2$, secure against passive adversaries can support $t < n$

5.4 DEVELOPMENT OF INFRASTRUCTURE-LESS NETWORK MECHANISM

In the present analysis the emphasis has been given to develop a GCA infrastructure-less node for generating secure network mechanism.The GC_PRIME and GC_BASE attribute values are collectively the "Generic Cryptology parameters". Figure 5.5 gives clear picture of implementation of *GC_KEY_GEN* and *GC_KEY_DERV*. Figure 5.5 describes the Generic Cryptology Infrastructure-less networking mechanism for Secure Data Transfer.

Depending on the token, there may be limits on the length of the key components.

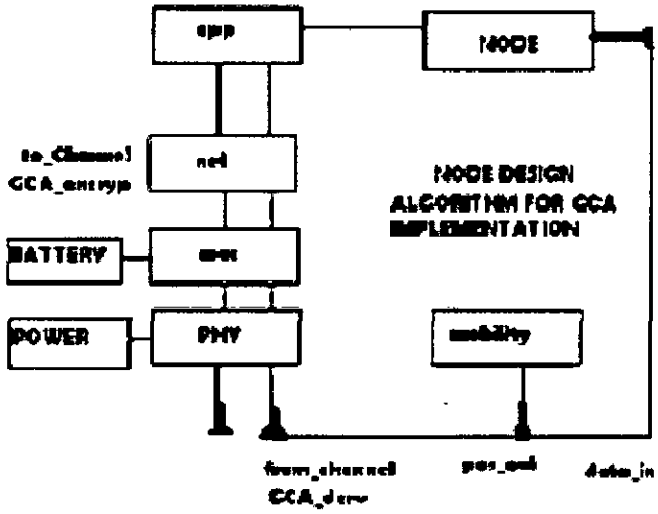


Fig. 5.5 A Generic Cryptology Infrastructure-less networking mechanism for Secure Data Transfer

The following program for creating a Generic Cryptology public key object in the infrastructure-less networks:

GCA INFRASTRUCTURE-LESS NODE

```
component AdhocNode : public TypeII
{
public:
   CBR app;
   net_component <app_packet_t> net;
   MEDIA <net_medium>phy/mac;
   MAC80211 <net_packet_t*> mac;
   // A transceiver that can transmit and receive at the same time (of course
   // a collision would occur in such cases)
   DuplexTransceiver < mac_packet_t > phy;
// Transceiver –2.14 dBi Rubber duck antenna
// Transmit Rate: Auto (1, 2, 5.5, or 11 Mbps), Channel: 2 (2417 MHz), Op.
Frq.2.4GHz
// Transmit Power :30 mW
   // Linear battery
   SimpleBattery battery;
   // PowerManagers manage the battery
```

```
    PowerManager pm;
    // nodes are mobile
    mobile mob;
    // the queue used between network and mac
    FIFOACK3<net_packet_t*,ether_addr_t,unsigned int> queue;
//.....
    // GCA class object described underneath
        GC_OBJECT_CLASS class = GCO_PUBLIC_KEY;
// generation of public key
        GC_KEY_TYPE keyType = GCK_DH;
        GC_UTF8CHAR label[ ] = "A Generic Cryptology public key object";
        GC_BYTE prime[ ] = {...};
        GC_BYTE base[ ] = {...};
        GC_BYTE value[ ] = {...};
        GC_BBOOL true = TRUE;
        GC_ATTRIBUTE template[ ] = {
        {GCA_CLASS, &class, sizeof(class)},
// data confidentiality, two-party data authentication, and evidence of data
freshness
        {GCA_KEY_TYPE, & keyType, sizeof(keyType)},
        {GCA_TOKEN, &true, sizeof(true)},
        {GCA_LABEL, label, sizeof(label)-1},
        {GCA_PRIME, prime, sizeof(prime)},
        {GCA_BASE, base, sizeof(base)},
        {GCA_VALUE, value, sizeof(value)}
            {GCA_ CONVERT, operatable value, sizeof(ope_value)}
          };
// availability, interoperability
    double MaxX, MaxY;  // coordinate boundaries
    ether_addr_t MyEtherAddr; // the ethernet address of this node
    int ID; // the identifier
```

```
// non-repudiation
   virtual ~AdhocNode();
   void Start();
   void Stop();
   void Setup();
```

GCA public key objects

GCA public key objects (object class GCO_PUBLIC_KEY, key type GCK_KEA) hold GCA public keys.

Attribute Data type Meaning

GCA_PRIME Big integer Prime *p* (512 to 1024 bits, in steps of 64 bits)

GCA_SUBPRIME Big integer Subprime *q* (160 bits)

GCA_BASE Big integer Base *g* (512 to 1024 bits, in steps of 64 bits)

GCA_VALUE Big integer Public value *y*

The GCA_PRIME, GCA_SUBPRIME and GCA_BASE attribute values are collectively the "GCA parameters". The following is a sample template for creating a GCA public key object:

```
GC_OBJECT_CLASS class = GCO_PUBLIC_KEY;
GC_KEY_TYPE keyType = GCK_GCA;
GC_UTF8CHAR label[ ] = "A GCA public key object";
GC_BYTE prime[ ] = {...};
GC_BYTE subprime[ ] = {...};
GC_BYTE base[ ] = {...};
GC_BYTE value[ ] = {...};
GC_BBOOL true = TRUE;
GC_ATTRIBUTE template[ ] = {
```

{GCA_CLASS, &class, sizeof(class)},

{GCA_KEY_TYPE, &keyType, sizeof(keyType)},

{GCA_TOKEN, &true, sizeof(true)},

{GCA_LABEL, label, sizeof(label)-1},

{GCA_PRIME, prime, sizeof(prime)},

{GCA_SUBPRIME, subprime, sizeof(subprime)},

{GCA_BASE, base, sizeof(base)},

{GCA_VALUE, value, sizeof(value)}

{GCA_ CONVERT, operatable value, sizeof(ope_value)}

};

Private Key objects

Private Key objects (object class GCO_PRIVATE_KEY) hold private keys. List of common private key attributes are presented in Table 5.2.

Table 5.2: Common Private Key Attributes

Attribute	Data Type	Meaning
GCA_SUBJECT	Byte array	DER-encoding of certificate subject name (default empty)
GCA_SENSETIVE	GC_BBOOL TRUE	If key is sensitive
GCA_SECONDARY_AUTH	GC_BBOOL	TRUE is the key requires a secondary authentication to take place before its use it allowed. (default FALSE)
GCA_AUTH_PIN_FLAGS	GC_FLAGS	Mask indicating the current state of the secondary authentication PIN. If GCA_SECONDARY_AUTH is FALSE, then this attribute is zero.
GCA_DECRYPT	GC_BBOOL	TRUE if key supports decryption
GCA_SIGN	GC_BBOOL	TRUE if key supports signatures where the signature is an appendix to the data
GCA_SIGN_RECOVER	GC_BBOOL	TRUE if key supports signatures where the data can be

		recovered from the signature
GCA_UNWRAP	GC_BBOOL	TRUE if key supports unwrapping (*i.e.*, can be used to unwrap other keys)
GCA_EXTRACTABLE	GC_BBOOL	TRUE if key is extractable
GCA_ALWAYS_SENSITIVE	GC_BBOOL	TRUE if key has *always* had the GCA_SENSITIVE attribute set to TRUE
GCA_NEVER_EXTRACTABLE	GC_BBOOL	TRUE if key has *never* had the GCA_EXTRACTABLE attribute set to TRUE

Brief description of proposed GCA private key objects

The different attributes used in the GCA as in Table 5.2 are briefly described for ready reference. When an object is created, the GCA_SENSITIVE attribute may be changed, but only to the value TRUE. Similarly, after an object is created, the GCA_EXTRACTABLE attribute may be changed, but only to the value FALSE. Attempts to make other changes to the values of these attributes should return the error code GCR_ATTRIBUTE_READ_ONLY.

If the GCA_SENSITIVE attribute is TRUE, or if the GCA_EXTRACTABLE attribute is FALSE, then certain attributes of the private key cannot be revealed in plaintext outside the token. Which attributes these are is specified for each type of private key in the attribute table in the section describing that type of key.

If the GCA_SECONDARY_AUTH attribute is TRUE, then the GCA implementation will associate the new private key object with a PIN that is gathered using a mechanism that is transparent to the GCA client. The new PIN must be presented to the token each time the key is used for a cryptographic operation. If GCA_SECONDARY_AUTH is TRUE, then GCA_EXTRACTABLE must be FALSE and GCA_PRIVATE must be TRUE. Attempts to copy private keys with GCA_SECONDARY_AUTH set to TRUE in a manner that would violate the above conditions must fail. An application can determine whether the setting the GCA_SECONDARY_AUTH attribute to TRUE is supported by checking to see if

the GCF_SECONDARY_AUTHENTICATION flag is set in the GC_TOKEN_INFO flags.

The GCA_AUTH_PIN_FLAGS attribute indicates the current state of the secondary authentication PIN. This value is only valid if the GCA_SECONDARY_AUTH attribute is TRUE. The valid flags for this attribute are GCF_USER_PIN_COUNT_LOW, GCF_USER_PIN_FINAL_TRY, GCF_USER_PIN_LOGCED, and GCF_USER_PIN_TO_BE_CHANGED defined for the GC_TOKEN_INFO *flags* field. GCF_USER_PIN_COUNT_LOW and GCF_USER_PIN_FINAL_TRY may always be set to FALSE if the token does not support the functionality or will not reveal the information because of its security policy. Finally, the GCF_USER_PIN_TO_BE_CHANGED flag may always be FALSE if the token does not support the functionality.

5.5 RESULTS AND RESPONSES WITH & WITHOUT GCA:

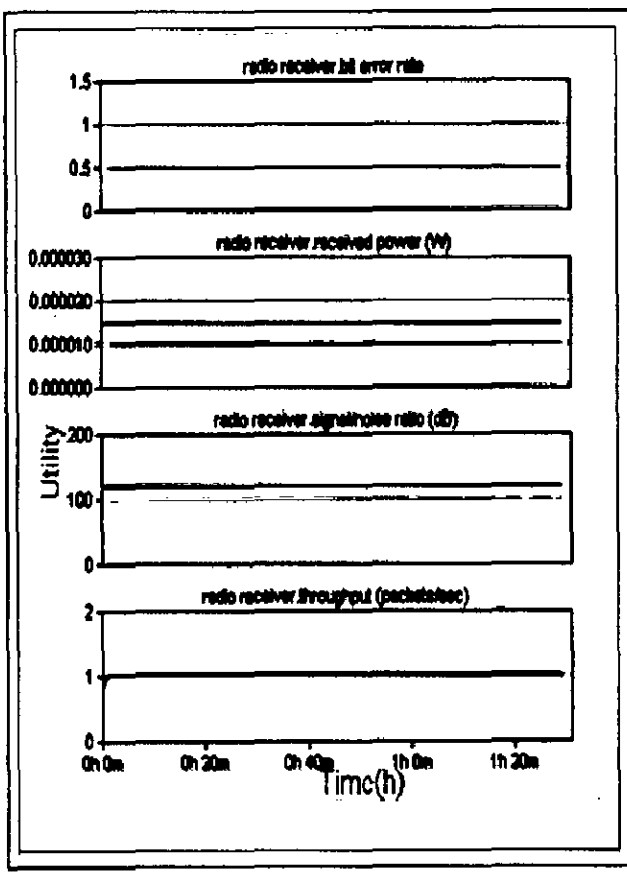


Fig.5.6 Response success rate of detection (without GCA)

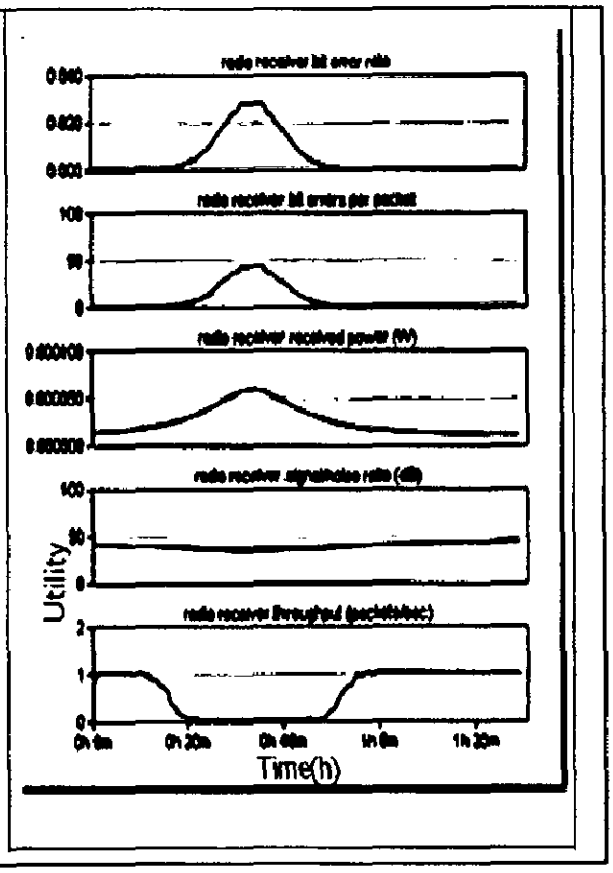


Fig. 5.7Response success rate of detection (with GCA)

5.6 TATE PAIRING (See Appendix 1)

Let E be an elliptic curve over a finite F_q. We write O_E for the point at infinity on E. Let l be a positive integer, which is co-prime to q. In most applications l is a prime and $l \mid \#E(F_q)$. Let k be a positive integer such that the field F_{q^k} contains the lth roots of unity (in other words, $l \mid (q^k - 1)$). Let $G = E(F_{q^k})$ and write $G[l]$ for the subgroup of points of order l and G/lG for the quotient group (which is also a group of exponent l). Then the Tate pairing is a mapping:

$$t : G[l] \times G/lG \to F_{q^k}^* / (F_{q^k}^*)^l$$

The Tate pairing satisfies the *Bilinear, Non-degeneracy and Well-defined* properties. (See Appendix 2)

5.7 DEVELOPMENT STEPS FOR ID-BASED (t,n) THRESHOLD SIGNATURE SCHEME FROM TATE PAIRINGS

In this section, it will present a new group-oriented threshold signature scheme. It consists of four algorithms: *System setup, Private Key extraction, Signature generation and signature verification*. The ID-based (t,n) threshold signature is described as follows:

(1)*System setup*: Let P is the generator of G. Our ID-based signature scheme is based on G. The trust KGC randomly chooses $a_0, a_1, a_2, \cdots, a_{t-1} \in Z_q^*$, $P_{pub} = a_0 P$. It constructs a polynomial of degree $t-1$:

$$f(x) = (a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}) \bmod q .$$

For $i = 1,2,\cdots,n$, $1 \le j \le t$, it computes and publishes $P_{pub}^{(i_j)} = f(ID)P$, where ID is the public identifier of each P_{i_j}. Before requesting his private share, each player

can check that $\sum_{j=1}^{t} L_{i_j} P_{pub}^{(i_j)} = P_{pub}$ for any subset $B=\{P_{i_1}, P_{i_2}, \Lambda\ P_{i_t}\}$ of the player set $A=\{P_1, P_2, \Lambda\ P_n\}$, where L_{i_j} denotes the Lagrange coefficient [3]:

$$L_{i_j} = \prod_{k=1, k\neq j}^{t} \frac{0 - ID_{i_k}}{ID_{i_j} - ID_{i_k}} \bmod q.$$

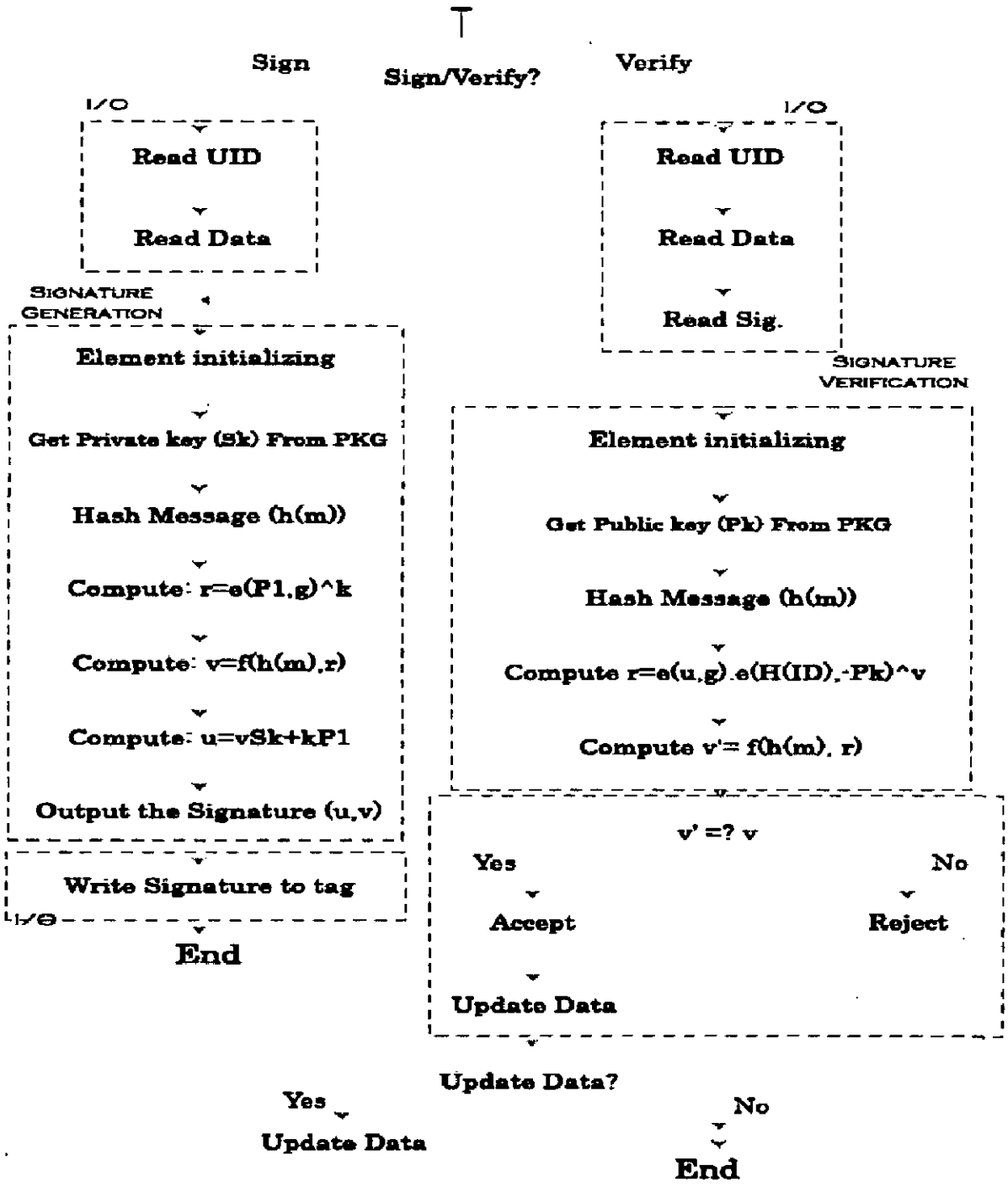


Fig. 5.8 Flow Chart for Signature Scheme from Tate Pairing

(2) *Private key extraction and distribution [4]*: The group secret key of P_i can be set by $f(0) = a_0$ and the corresponding group public key $Y_i = f(0)P \bmod l = a_0 P \bmod l$. For the purpose of security, the KGC defines two one-way hash functions $H : \{0,1\}^* \rightarrow G^*$ and $H' : \{0,1\}^* \rightarrow Z_q^*$ and makes it public. Given an identity ID, the KGC plays the role of the trusted dealer. It computes a secret key publishes $S_{ID}^{(i_j)} = f(ID)Q_{ID}$ for each player P_{i_j}, where $Q_{ID} = H(ID)$ is the public key associated with the public identifier ID of P_{i_j}. P_{i_j} accepts $S_{ID}^{(i_j)}$ as his private key if $t(P, S_{ID}^{(i_j)}) = t(P_{pub}^{(i_j)}, Q_{ID})$; otherwise, he shows his complains to the KGC. In summary, the parameters are those listed in Table 5.3.

Table 5.3. The parameters of the proposed scheme

Participants	Secret Parameters	Public Parameters
KGC	$f(x)$	G , P , $P_{pub}^{(i_j)}$, P_{pub} , H , H'
Signer	$S_{ID}^{(i_j)}$	ID , Q_{ID}
Signer group	$f(0)$	Y_i

(3) *Partial signature generation* [98]: It assumes that $B = \{P_{i_1}, P_{i_2}, \cdots P_{i_t}\}$ is the set of the t players designated to join the signing. Each player $P_{i_j} (1 \le j \le t)$ randomly chooses $k_j \in Z_q^*$ computes two values u_j and r_j as

$u_j = k_j P_{pub} \bmod l$,

$r_j = k_j Y_i \bmod l$.

Then each P_{i_j} transmits (u_j, r_j) to the other $(t-1)$ signers via a secure channel.

Upon receiving all (u_j, r_j), each P_{i_j} computes u, r and v as follows:

$$u = \sum_{j=1}^{t} u_j \bmod l, \qquad (1)$$

$$r = \sum_{j=1}^{t} r_j \bmod l, \qquad (2)$$

$$h = H'(u, r, M), \qquad (3)$$

$$v_j = L_{i_j}(P_{pub}^{(i_j)} + hS_{ID}^{(i_j)}) \bmod q. \qquad (4)$$

The partial signature on message M given by player P_{i_j} is $\sigma_j = (u_j, v_j)$.

(4) *Threshold signature generation* [104-106]: Anyone in $B = \{P_{i_1}, P_{i_2}, \cdots P_{i_t}\}$ can be designated to reconstruct the partial signature. After having received the partial signatures, the designated player (DP) first verifies the validity of each partial signature. σ_j is accepted if $t(v_j, P) = t(P + hQ_{ID}, P_{pub}^{(i_j)})^{l_{i_j}}$. Without lose of generality, it assumes that the partial signatures are all valid. DP computes $u = \sum_{j=1}^{t} u_j$ and $v = \sum_{j=1}^{t} v_j$. Then $\sigma = (u, v)$ is the signature on message M.

(5)*Threshold signature verification* [106]: After receiving $\sigma = (u, v)$, the verifier computes $h = H'(M, u)$ and accepts the signature if

$$t(v, P) = t(P + hQ_{ID}, P_{pub}). \qquad (5)$$

***Correctness of the partial signature*:**

$$t(v_j, P) = t(L_{i_j}(P_{pub}^{(i_j)} + hS_{ID}^{(i_j)}), P)$$

$$= t(L_{i_j} P_{pub}^{(i_j)}, P)\, t(L_{i_j} hS_{ID}^{(i_j)}, P)$$

$$= t(L_{i_j} f(ID_{i_j})P, P)\, t(L_{i_j} hf(ID_{i_j})Q_{ID}, P)$$

$$= t(L_{i_j} P, f(ID_{i_j})P)t(L_{i_j} hQ_{ID}, f(ID_{i_j})P)$$

$$= t(L_{i_j} P, P_{pub}^{(i_j)})t(L_{i_j} hQ_{ID}, P_{pub}^{(i_j)})$$

$$= t(L_{i_j} P + L_{i_j} hQ_{ID}, P_{pub}^{(i_j)})$$

$$= t(P + hQ_{ID}, P_{pub}^{(i_j)})^{L_{i_j}}$$

Correctness of the threshold signature:

$$v = \sum_{j=1}^{t} v_j = \sum_{j=1}^{t} (L_{i_j} (P_{pub}^{(i_j)} + hS_{ID}^{(i_j)}))$$

$$= \sum_{j=1}^{t} L_{i_j} P_{pub}^{(i_j)} + \sum_{j=1}^{t} L_{i_j} hS_{ID}^{(i_j)}$$

$$= P_{pub} + hQ_{ID} \sum_{j=1}^{t} L_{i_j} f(ID_{i_j})$$

$$t(v, P) = t(P_{pub} + hQ_{ID} \sum_{j=1}^{t} L_{i_j} f(ID_{i_j}), P)$$

$$= t(P_{pub}, P)t(hQ_{ID} \sum_{j=1}^{t} L_{i_j} f(ID_{i_j}), P)$$

$$= t(P_{pub}, P)t(hQ_{ID}, \sum_{j=1}^{t} L_{i_j} f(ID_{i_j})P)$$

$$= t(P_{pub}, P)t(hQ_{ID}, \sum_{j=1}^{t} L_{i_j} P_{pub}^{(i_j)})$$

$$= t(P_{pub}, P)t(hQ_{ID}, P_{pub})$$

$$= t(P + hQ_{ID}, P_{pub})$$

5.8 SECURITY ANALYSIS OF DEVELOPED THRESHOLD SCHEME

The security of the proposed scheme is based on the well-known difficulty of computing the one-way hash function and the cryptographic assumption of discrete logarithms. In the following paragraphs, it considers some attacks against

our proposed scheme. It demonstrates that our scheme can successfully withstand those attacks.

(i) Plaintext attacks

An adversary tries to expose a signer's secret key $S_{ID}^{(i)}$ from the corresponding public key Q_{ID}. However, it is as difficult as breaking the discrete logarithms to obtain the user's secret key from the associated public key, the hardness of which depends on the hardness assumption of the discrete logarithm problem (DLP) in $E(F_q)[l]$ [11]. Similarly, assume that the adversary attempts to get P_i's group secret key $f(0)$ from their corresponding group public key $Y_i = f(0)P \bmod l$. The adversary will also have to face the intractability of the same problems as, deriving P_i's group secret key.

(ii) Recovery equation attacks

An intruder tries to derive the signer's secret key $S_{ID}^{(i_j)}$ from the individual signature v_j by Equation (4). Given a message M and a signature v_j, it is difficult to determine $S_{ID}^{(i_j)}$ because Equation (4) has two unknown parameters. The values $S_{ID}^{(i_j)}$ are kept secret and the commitment values u and r are only known to the signers. Moreover, if one message with its related signature is added, the number of unknown parameters is also increased by one. The number of secret parameters is always greater than the number of equations available. Consequently, the intruder cannot succeed in recovering the equation and breaking the scheme.

(iii) Conspiracy attacks

Any $(t-1)$ or less signers in B attempt to reconstruct the secret polynomial $f(x)$ to reveal the other signers' secret keys $S_{ID}^{(i_k)}$ and the group secret key $f(0)$. By using the Lagrange interpolating polynomial, with the knowledge of t or more signers' secret parameters $f(ID)$, the $(t-1)$th degree polynomial $f(x)$ can be uniquely determined as

$$f(x) = \sum_{j=1}^{t} f(ID_{i_j}) \prod_{k=1, k \neq j}^{t} \frac{x - ID_{i_k}}{ID_{i_j} - ID_{i_k}}$$

Therefore, any $(t-1)$ or less malicious signers cannot conspire to derive the secret polynomial $f(x)$. Then, they cannot obtain any other signer's secret key and the group secret key. Thus conspiracy attacks can be successful.

(iv) Impersonation attacks

Now let's discuss some possible impersonation attacks as below:

(a) An adversary attempts to impersonate a signer P_{i_j}. However, she/he cannot create a valid individual signature (u_j, r_j) to satisfy Equation (4) because of the lack of the secret key $S_{ID}^{(i_k)}$.

(b) An adversary tries to forge a valid threshold signature (u, v) of chosen message M to satisfy Equation (5). First, the adversary has to randomly choose u and r and find v to satisfy Equation (5), which is as difficult as solving discrete logarithms. In another similar approach, given u, v, finding r to satisfy Equation (5) is as difficult as solving the one-way hash function and the discrete logarithms. Therefore, the adversary cannot successfully forge the valid threshold signature.

(c)An adversary tries to collect a preciously valid threshold signature (u, v)' on the message M and the associated value r to forge the signature of an arbitrary message M'[12]. First, the adversary selects a random $k_j' \in Z_q^*$ and calculates two values u' and r' as follows:

$u_j' = k_j' P_{pub} \bmod l$,

$r_j' = k_j' Y_i \bmod l$.

Then she/he computes

$$u_j' = u_j H'(u, r, M)^{-1} H'(u', r', M') \bmod l \quad (6)$$

$v_j' = v_j H'(u, r, M)^{-1} H'(u', r', M') \bmod q$.

Finally, the adversary sends the signature (u', v') for the message M' to verifiers. The validity of the threshold signature can be checked by Equation (5). Since

$$t(v', P) = t(P + H'(u', r', M')Q_{ID}, P_{pub})$$

The threshold signature (u', v') is valid for the message M'. However, it is hardly possible for the adversary to determine the value u' that satisfies Equation (6). Hence, the proposed scheme is secure against the impersonation attacks.

5.9 PERFORMANCE ANALYSIS

For developing GCA, each node is made intelligent as described in section 5.3, then object class has been created to accept public key. The GCA public key object generates and distributes the attribute values for the "GCA parameters". Then finally the distribution algorithm for private key generation and decryption has been developed keeping in the view of low overhead for energy efficiency and wireless infrastructure-less networking. The performance of the network has been analyzed after the implementation of GCA shown in figure 5.7.

In the scheme 2, a new ID-Based (t, n) Threshold Signature Scheme from the Tate pairing has been developed. According to our discussions, none of the possible attacks including plaintext attack, equation attack, conspiracy attack and impersonation attack can break our scheme. Performance analysis shows that it is more efficient and is more applicable to systems where signatures are sent over a finite bandwidth channel and with low capability equipment. It is believed that 1024-b RSA and 160-b elliptic curve cryptosystem are offering more or less the same level of security [13]. In this case, if our scheme pre-computes (u_j, r_j), the timing of signing will be much shorter for two scalar multiplication operations reduced. On the other hand, our scheme uses the Tate pairing instead of Weil pairing because the Weil pairing takes longer than twice the running time of the Tate pairing for the cryptographic applications. Obviously, our scheme has high performance.

5.10 CONCLUSION

In Scheme 1, work reported is based on the work carried by Adrain Perrig et al. [96]. It claims to have data confidentiality, two-party data authentication, and evidence of data freshness. It provides authenticated broadcast for severely resource-constrained environments for infrastructure-less networks. It consider non-repudiation, availability, interoperability and energy efficient consumption, require for overhead security protocol, in addition to above parameters and developed a GCA, for Wireless infrastructure-less infrastructure -less network. The simulated responses shows that success rate of the detections described above.

In scheme 2, the performance of partial signature is determined by those dominant cost operations. One of dominant operations in our scheme is scalar multiplication. Another dominant operation is the Tate pairing defined in section 5.6. Comparing with scalar multiplication or the Tate pairing, point addition and hash functions can be ignored. Performance estimations of our partial signature with reference to those corresponding popular signature schemes are shown in Table 5.4.

Table 5.4 Performance Comparison

	PARTIAL SIGNING	**PARTIAL SIGNATURE VERIFICATION**	**SIGNATURE VERIFICATION**
Baek and Zheng's scheme[7]	1 Weil pairing 1 scalar multiplication	2 Weil pairing 2t+1 integer exponentiations 2t+1 scalar multiplications	2 Weil pairings 1 integer exponentiation 1 scalar multiplication

Cheng and Liu's [9]	4 scalar multiplications	3 Weil pairings 3 scalar multiplications	2 Weil pairings 1 scalar multiplication
Developed scheme	**5 scalar multiplications**	**2 Tate pairings** **2 scalar multiplications**	**2 Tate pairings** **1 scalar multiplication**

CHAPTER-6

CONCLUSION AND SCOPE FOR FUTURE WORK

Chapter-6

CONCLUSION AND SCOPE FOR FUTURE WORK

6.1 INTRODUCTION

This chapter reviewed the future scope for secure characteristics of energy efficient mobile devices that can use wireless Infrastructure-less networks (ad-hoc) almost anywhere and anytime by using one or more wireless network technologies. Currently, most computers communicate with each other by using wired networks. Wired networking is well suited for stationary computers, but it is not appropriate for mobile devices. These technologies enable the use of infrastructured networks (3Generation Partnership Protocol) and Infrastructure-less networks. The summary of the work done has been described below.

6.2 BACKGROUND AND SUMMARY OF THE WORK

6.2.1 Summary of existing popular energy efficient/ power aware routing algorithm

On the basis of literature study [49-65] it is observed that:

(i) Several energy efficient/ power aware wireless infrastructure-less networks routing protocol have been designed to support energy saving by power control and energy efficient.

(ii) Most of the energy efficient/ power [49-62] use a separate control channel, nodes have to be able to receive on the control channel while they are transmitting on the data channel and also transmit on data and control channels simultaneously and a node should be able to determine when probe responses from multiple senders collide. In spite of this, their spatial reuse is less than optimal.

(iii) a node in an ad hoc network has to relay (and, hence route) messages for other nodes in the same network.

(iv) At the MAC layer and above, this is often done by selectively putting the receiver into a sleep mode, or by using a transmitter with variable output power.

(v) Recently, much work has been done with energy-aware routing protocols and applications, especially with the idea of vertical layer integration.

6.2.2 Summary of optimal path programming algorithm for energy efficient for wireless Infrastructure-less networks

(i) Combining Dijkstra and Floyd algorithm with the graph theory yields a modified path programming algorithm using hypo-excellent route in mobile infrastructure-less node navigation system under complex environment.

(ii) The time complexity of Dijkstra is O (N^2), and the time complexity of Floyd is O (N^3). Although there is a certain statistical error to do statistics with circulation and judgment, it is shown that the Dijkstra is better than Floyd in time.

(iii) With the increase in the number of nodes, the time complexity of Dijkstra is increased by N^2 and the time complexity of Floyd is increased by N^3. The time complexity of modified path programming algorithm is N, thus the circulation time increases linearly as the number of nodes.

6.2.3 Summary of developed energy efficient wireless Infrastructure-less networking (EILN) protocol

(i) The protocol has been analyzed in static and dynamic (mobility) scenario.

(ii) The result of static topology for cumulative distribution of delivery rates across all links for each of the two packet sizes shows that about 50% of the links deliver no packets, while the best 20% of links deliver more than 95% of their packets. The delivery rates of the remaining 30% of links are approximately evenly distributed.

(iii) The result of static topology for Packet delivery rate as a function of per-CBR-flow bit rate under higher traffic load, EILN delivers more packets than 802.11 PSM, but slightly less than 802.11B.

(iv) The result of dynamic (mobility) topology for Packet loss rate as a function of pause time shows that mobility does not affect EILN very much, and Geographic forwarding with EILN delivers more packets than with 802.11 PSM and 802.11 because it encounters fewer voids.

(v) The result of dynamic (mobility) topology for backbone density as a function of node density shows that the degree of mobility does not significantly affect routing with EILN backbones. EILN consistently performs better than 802.11 PSM, SPAN and 802.11.

(vi) The result of dynamic (mobility) topology for cumulative distribution of delivery rates across all links for each of the two packet sizes shows that it is similar to static topology result.

(vii) The result of dynamic (mobility) topology for energy saving as function of fup shows that EILN broadcast messages are expensive when density is high means the large number of broadcast messages per radio range keeps nodes awake for a longer period.

6.2.4 Summary of developed security aspects model algorithm

(i) Work reported in scheme 1 is based on the work carried by Adrain Perrig et al. [96]. It claims to have data confidentiality, two-party data authentication, and evidence of data freshness. It provides authenticated broadcast for severely resource-constrained environments for infrastructure-less networks.

(ii) The developed GCA considers non-repudiation, availability, interoperability and energy efficient consumption, require for overhead security protocol, in addition to above parameters.

(iii) The simulated response shows that success rate of the detections.

(iv) The developed scheme 2 is a five scalar multiplication partial signing scheme.

(v) The partial signature verification has been done using two Tata pairing and two scalar multiplications.

(vi) The signature verification has been done using two Tata pairing and one scalar multiplication.

6.3 SCOPE FOR FUTURE WORK

The future of Infrastructure-less networks really appealing, given the vision of "anytime, anywhere" communications. Before those imagined scenarios come true, huge amount of work is to be done in both research and implementation. At present, the general trend is toward mesh architecture and large scale. New applications call for both bandwidth and capacity, which implies the need for a higher frequency and better spatial spectral reuse. Propagation, spectral reuse, and energy issues support a shift away from a single long wireless link (as in cellular) to a mesh of short links (as in ad hoc networks). Research on "multi-hop mesh-based" architecture showed it a promising solution to the implementation of ad hoc networks. As the evolvement goes on, especially the need of dense deployment such as battlefield and sensor networks, the nodes in ad hoc networks will be smaller, cheaper, more capable, and come in all forms. Large scale ad hoc networks are another hot issue in the near future which can be already foreseen.

Ad hoc networks have indeed the potential to change how we see the communication and networking world today, from the indoor ad hoc networks that can connect smart appliances to the Internet, to the ultimate "anytime, anywhere" communications. In all, although the widespread deployment of Infrastructure-less networks is still year away, the research in this field will continue being very active and imaginative. Wireless Infrastructure-less networks will use mobile routers to provide Internet connectivity to mobile ad-hoc users. A mobile router will also allow mobility of an ad wireless Infrastructure-less network, where mobile users may use an Internet access within an ad-hoc network domain. Recently, organizations have begun to see potential for such dynamic networks. Mobile ad-hoc networks are of increasing interest for a distributed set of applications, such as distributed collaborative computing, distributed sensing networks, potential fourth generation wireless systems, and response to incidents that destroyed the existing communication structure.

There is current and future need for dynamic wireless Infrastructure-less networks networking technology. The emerging field of mobile computing, with its current focus on mobile IP operation, will expend gradually. In the future, mobile computing will require highly-adaptive networking technology to manage multi-hop clusters that can operate autonomously and possibly be able to attach at some point to the bigger network.

Appendix 1

The Tate Pairing

Elliptic Curves

$E(F_q) : y^2 = x^3+Ax+B$

Elliptic curves are considered interesting primarily as an alternative group structure, with certain advantages when it comes to the implementation of common cryptographic protocols. The main advantage is that much smaller keys can be used, as there is no known polynomial-time algorithm for the discrete logarithm problem for the great majority of such curves. Given a point **P** on a curve ***E*** defined over a finite field F_q where $q = p^m$ (where p is a large prime) this is the problem of determining *a* given *a***P**. In most circumstances the points on such a curve form a simple cyclic group. Each point on the curve has an *order*. This is the smallest positive integer r such that $r\mathbf{P} = \mathbf{O}$, where **O** is the identity point of the group, the so-called point at infinity. The number of points on the curve, the order of the curve, is referred to as $\#E$. Every valid r divides $\#E$. We also need to know the important relationship $\#E = q+1-t$, where t is the *trace of the Frobenius*, and t is relatively small - a constant for each curve. We note also the "twisted" curve

$E^t(F_q) : y^2 = x^3+ d^2Ax+ d^3B$

Where d is any Quadratic Non Residue mod q. This curve has $\#E^t = q+1+t$ *points on it.*

So far so good. A rather boring cyclic group.

The Embedding Degree

However something rather magical happens when a curve with the same equation is considered over the field F_qk for a certain value of k. The group structure undergoes a strange blossoming, and takes on a new, more exotic character. The smallest value of k for which this happens is referred to as the *embedding degree.* For a random curve the embedding degree will be very large. However it can be as small as k=1, and it is not in fact difficult to find curves for any positive value of k. Here for simplicity we concentrate on the particular case k=2 and q=p a prime. In the field F_p2 (called the *quadratic extension* field) elements are represented as

(a,b) which is $a+ib$ where i is the "square root" of a QNR. If p = 3 mod 4 one can conveniently choose the QNR as p-1.

A k=2 curve $\boldsymbol{E}(F_p)$ has $p+1-t$ points on it. Call this set of points **S**. It contains a subgroup of points of prime order r and a representative of these is a point **P**. The same curve over $\boldsymbol{E}(F_p2)$ will have $\#\boldsymbol{E}(F_p2) = (p+1-t)(p+1+t)$ points on it, as a consequence of Weil's Theorem. For a k=2 curve r exactly divides both $p+1$ and $(p+1-t)$, and hence necessarily r divides t. And r^2 divides $\#\boldsymbol{E}$.

An example will be useful. The curve is

$\boldsymbol{E}(F_{131}) : y^2 = x^3-3x+8$

with p =131, r =11, t=22, **P**(123,100), $\#\boldsymbol{E}$=110. There are points on the curve of order 110, and the group is cyclic. There is a subgroup of order r. The curve is not supersingular.

The twisted curve is

$\boldsymbol{E}^t(F_{131}) : y^2 = x^3-3x-8$

And $\#\boldsymbol{E}^t$ = 154.

This same curve taken over the extension field $\boldsymbol{E}(F_p2)$ has 16940=154.110 points on it. And there are no points on the curve of this order - it is not cyclic. We represent a point on this curve as $\mathbf{Q}[x,y] = \mathbf{Q}[(a,b),(c,d)]$

Group Structure

There are a couple of ways of considering all these points. But first some notation. The complete set of curve points is called $\boldsymbol{G}$, of order $\#\boldsymbol{E}$. The set of all points that are transformed to **O** by multiplication by r ("killed by r") is called $\boldsymbol{G}[r]$. These are the r-torsion points. Since r is prime, this is all the points of order r plus **O**. There are r^2 such points, and these r^2 points can be organised as r+1 distinct cyclic subgroups of order r - they all share **O**. Note that one of these subgroups is $\boldsymbol{S}[r]$ and consists of all those r-torsion points from the original curve $\boldsymbol{E}(F_p)$ - points of the form $\mathbf{Q}[(a,0),(c,0)]$, which are of course on both curves.

Let $h = \#\boldsymbol{E}/r^2$. Then a random point on the curve can be mapped to a point in one of these sub-groups of order r by multiplying it by this co-factor h. For simplicity we assume that r does not divide h.

For our example curve r=11 and h=140.

The set of distinct points generated by multiplying every element of ***G*** by *r* is called ***rG***. The number of elements in ***rG*** is *h*. This is called a *coset*.

Consider the partitioning of the ***#E*** points into distinct *cosets*. This can be done by adding a random point **R** to every element of ***rG***. There are exactly r^2 such distinct cosets, each with *h* elements.

The original coset ***rG*** is the unique coset that contains **O**. Every coset contains exactly one *r*-torsion point. Elements of these cosets are **not** all of the same order. They do **not** form a group.

The quotient group ***G/rG*** is the group formed of all these cosets.

Finally - the Tate Pairing

The Tate Pairing operates on a pair of points, **P** of prime order *r* (a member of ***G[r]***) and a point **Q** which is a representative member of one of the cosets. It is denoted $e_r(\mathbf{P},\mathbf{Q})$. It evaluates as an element of the finite field F_p2 of order *r* - observe that *r* divides p^2-1. Its value is the same irrespective of which element of a particular coset is chosen. Recall that each coset has exactly one *r*-torsion point. For convenience we will choose **P** to be a member of ***S[r]*** - as it also lies on $\boldsymbol{E}(F_p)$, this makes the Tate Pairing calculation much faster.

However the Tate pairing can evaluate as 1. This will occur if **P** *is a multiple of* **Q**, which will be the case if **Q** is chosen from a coset whose *r*-torsion point is also a member of ***S[r]***. For a randomly chosen **Q** and for large *r* this is extremely unlikely - the odds are 1/*r*.

The Tate Pairing is *non-degenerate* as for any given **P** not equal to **O**, we can always find a **Q** such that $e_r(\mathbf{P},\mathbf{Q})$ is not 1. Also $e_r(\mathbf{P},\mathbf{P})=1$ for **P** in ***S[r]*** (and $k > 1$).

However probably the most important property of the Tate pairing is *bilinearity*

$$e_r(a\mathbf{P},b\mathbf{Q}) = e_r(\mathbf{P},\mathbf{Q})^{ab}$$

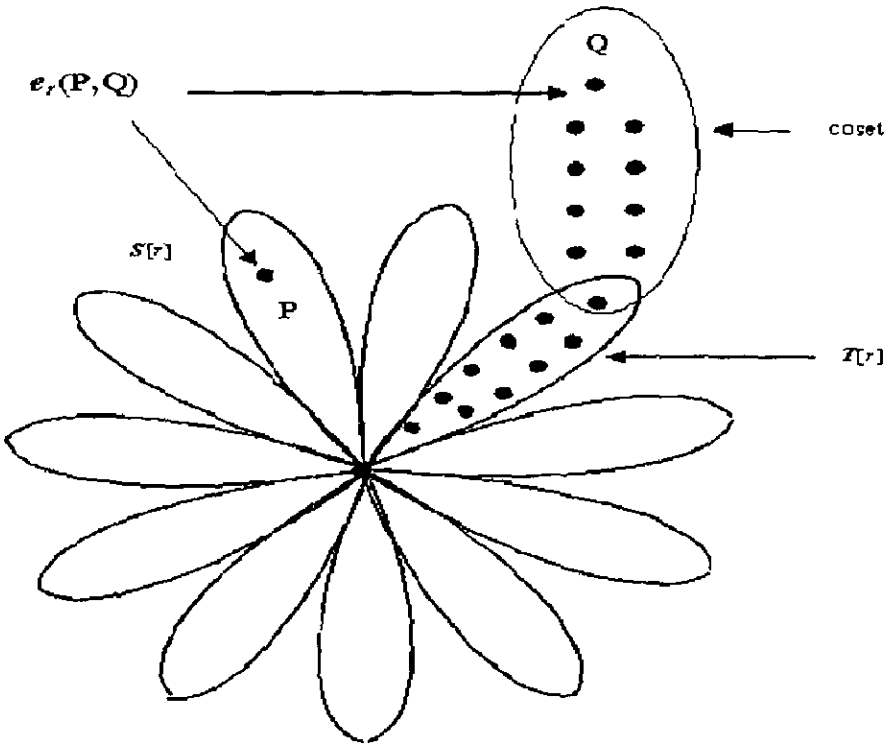
Note that **P** must be of order *r*, but **Q** need not be.

Which coset to choose **Q** from? There are computational advantages in choosing points of the form $\mathbf{Q}[(a,0),(0,d)]$. Call the set of points of this form ***T***. It is not difficult to see that if there are $p+1-t$ points of the form $\mathbf{Q}[(a,0),(c,0)]$ then there will be

$p+1+t$ points of the form $\mathbf{Q}[(a,0),(0,d)]$. Substitute all $a<p$ for x in the curve equation. Then if the RHS is a QR the point is $\mathbf{Q}[(a,0),(\pm c,0)]$, otherwise its $\mathbf{Q}[(a,0),(0,\pm d)]$. There will always be a subgroup of order r, consisting of points of this form. **Q** can therefore be chosen as an element of $\boldsymbol{T}$. Note that points of this form stay in this form under point multiplication, so such a **Q** will be in a coset supported by an element of $\boldsymbol{T}[r]$.

But wait. There are also $p+1+t$ points on the twisted curve. Is there a connection between the group of points of the form $\mathbf{Q}[(a,0),(0,d)]$ and the group of points on the "twisted" curve? Yes there is - they are *isomorphic*. For every point of the form $\mathbf{Q}[(a,0),(0,d)]$ on the curve defined over the quadratic extension field F_p2, there is a point $Q(-a,d)$ on the twisted curve defined over F_p. This is convenient as it means that multiplication of such points can be done on the twisted curve using regular $\boldsymbol{E}(F_p)$ methods.

A diagram might help. The point-at-infinity is in the centre. Twelve subgroups of order 11 radiate out from it. Each of the points in each subgroup support a coset. The point-at-infinity supports the co-set $r\boldsymbol{G}$.

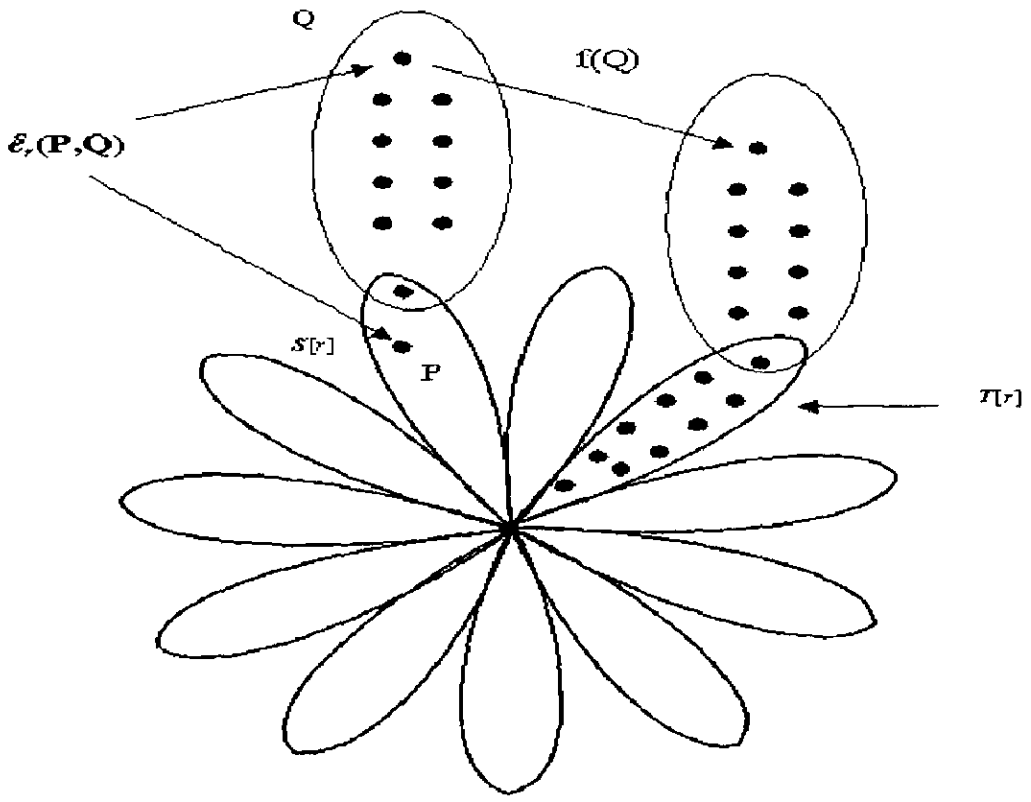


An alternative idea is to use a *super-singular* curve. For example

$\boldsymbol{E}(F_p) : y^2 = x^3+x$

with p =131, r =11, t=0, **P**(6,22), #E=132. There are points on the curve of order 132, and the group is cyclic. There is a subgroup of order r.

This same curve taken over the extension field $E(F_p 2)$ has 17424 (=132.132) points on it. As before there are no points on the curve of this order - it is not cyclic. In this case the sets S and T are of the same order. But more than that - every point in S can be mapped directly to a point in T of the same order via the *automorphism* $f(x,y) = (-x,0),(0,y)$. For every point $\mathbf{Q}[(a,0),(c,0)]$ in S, there is a point $\mathbf{Q}[(-a,0),(0,c)]$ in T. This allows the introduction of the alternative function $\hat{e}_r(\mathbf{P},\mathbf{Q}) = e_r(\mathbf{P},f(\mathbf{Q}))$, where **P** is a member of $S[r]$ and **Q** is a member of S. Note that $\hat{e}_r(\mathbf{P},\mathbf{P})$ is not 1.



What about all those other subgroups of order r ? In fact they are of little interest. Any general point $\mathbf{P}[x,y] = \mathbf{P}[(a,b),(c,d)]$ of order r on the curve can be written as the sum of a point from S and a point from T using the *Trace Map*.

$\mathbf{P}[x,y] = \mathbf{P}_S + \mathbf{P}_T$

Where $\mathbf{P}_S = Trace(\mathbf{P})/k$, and $\mathbf{P}_T = \mathbf{P} - \mathbf{P}_S$

In our case $\mathbf{P}_S = ((a+ib,c+id)+(a-ib,c-id))/2$ (an elliptic curve point addition followed by elliptic curve point division by 2)

For a general point $\mathbf{P}[x,y] = \mathbf{P}[(a,b),(c,d)]$ of order r, $e_r(\mathbf{P},\mathbf{P}) = e_r(\mathbf{P}_S,\mathbf{P}_T)$. $e_r(\mathbf{P}_T,\mathbf{P}_S)$ which is NOT equal to 1.

Appendix 2

The Tate pairing satisfies the following properties:

a. ***Bilinearity***:

$\forall P, P_1, P_2 \in G[l] \square \forall Q, Q_1, Q_2 \in G / lG$,

$t(P_1 + P_2, Q) = t(P_1, Q)t(P_2, Q)$

and $t(P, Q_1 + Q_2) = t(P, Q_1)t(P, Q_2)$

$\forall a, b \in Z_q$, we have

$t(aP, bQ) = t(bP, aQ) = t(P, Q)^{ab}$

b. ***Non-degeneracy***:

If $t(P, Q) = 1 \quad \forall Q \in G[l]$, then $P = O_E$. Conversely, for each $P \neq O_E \quad \exists Q \in G[l]$ so that $t(P, Q) \neq 1$

c. ***Well-defined***:

$(O_E, Q) \in (F_{q^k}^*)^l$ for all $Q \in G$ and $(P, Q) \in (F_{q^k}^*)^l$ for all $P \in G[l], Q \in lG$

REFERENCES

1. Aspinwall, Jim, "Installing, troubleshooting and repairing wireless networks" McGraw-Hill, USA, pp: 17-22, 2003.
2. IETF-Working-Group, "MANET: Mobile Ad-hoc Networks," www.ietf.org/html.charters/manet-charter.html.
3. Paul Havinga & Gerard J.M. Smit, "Energy-Efficient Adaptive Wireless Network Design" IEEE Symposium on Computers and Communications, pp: 1530-1346, 2006.
4. Paul Havinga, Gerard J.M. Smit, Martinus Bos, "Energy efficient wireless ATM design. Resource Management" Wireless Networking, Springer US, pp.26-33. 2000.
5. Ben Abdallah Abderazek, and Masahiro Sowa . "Advanced Power Management Techniques For Mobile Communication Systems" International Journal of Computer Research, Volume 14, Number 1/2, pp. 109–128, 2007.
6. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries ."Security Considerations for Voice Over IP Systems. C o m p u t e r S e c u r i t y ", NIST Special Publication 800-58. 2005.
7. Paul J.M. Havinga, Gerard J.M. Smit. "Energy-efficient wireless networking for multimedia Applications." Wireless Communications and Mobile Computing, Wiley, pp.165-184. 2001.
8. K.Srinivas, A.A.Chari "Updated Congestion Control Algorithm for TCP Throughput improvement in Wired and Wireless Network" Global Journal of Computer Science and Technology, USA Vol. 9 Issue 5 (Ver 2.0), pp. 25-29. January 2010.
9. Philippe Jacquet, Paul Muhlethaler and Amir Qayyum, "Optimized Link State Routing Protocol", Internet draft, draft-ietf-manet-olsr-00.txt, November 1998.
10. Havinga P.J.M., Smit G.J.M. "Design techniques for low power systems. Journal of Systems Architecture" Vol. 46, Iss.1, a previous version appeared as CTIT Technical report, Enschede, the Netherlands. pp 97-32. 2000.
11. Marc Greis' *Tutorial* for the UCB/LBNL/VINT Network Simulator "ns" Website: www.isi.edu/nsnam/ns/tutorial/
12. Internet Engineering Task Force (IETF) Mobile Ad Hoc Networks (MANET) Working Group Charter, http://www.ietf.org/html.charters/manet-charter.html, 2000.

13. Jubin, J. and Tornow, J., "Packet radio network protocols Analysis for QoS", Proceedings of the IEEE, 37, pp 33–39, 1989.
14. Kamerman, A. and Monteban, L.," Medium Access Control in Wireless LAN for the Unlicensed Band", Bell Labs Technical Journal, pp. 27–33, Summer 1996.
15. Shepard, T. J. "Decentralized Channel Management in Scalable Multihop Spread-Spectrum Packet Radio Networks" Ph.D. Thesis, Massachusetts Institute of Technology. 1995.
16. Gupta, P. Gray, R. & Kumar, P. R. "An Experimental Scaling Law for Ad Hoc Networks" University of Illinois at Urbana-Champaign, 2001.
17. Pottie, G. and Kaiser, W., "Wireless Integrated Network Sensors", Communications of the ACM, pp. 51–58, May 2000.
18. Park, V. and Corson, M., "A Performance Comparison of the Temporally-Ordered Routing Algorithm and Ideal Link-State Routing", IEEE Symposium on Computer and Communications, July 1998.
19. Perkins, C., Ed., Ad Hoc Networking, Addison-Wesley, Reading, MA, 2001.
20. Internet Engineering Task Force (IETF) Mobile Ad Hoc Networks (MANET) Working Group Charter, http://www.ietf.org/html.charters/manet-charter.html, 2000.
21. Jubin, J. and Tornow, J., "The DARPA packet radio network protocols", Proceedings of the IEEE, Vol. 75, pp. 21–32, 1987.
22. Kamerman, A. and Monteban, L., "WaveLAN-II: A High-Performance Wireless LAN for the Unlicensed Band", Bell Labs Technical Journal, pp. 118–133, Summer 1997.
23. Woesner, H., Ebert, J., Schlager, M., and Wolisz, A., "Power-Saving Mechanisms in Emerging Standards for Wireless LANs: The MAC Level Perspective", IEEE Personal Communications, pp. 40–48, June 1998.
24. Complete Bluetooth Tutorial, http://infotooth.tripod.com/tutorial/complete.htm, 2000.
25. Pottie, G. and Kaiser, W., "Wireless Network for Sensors management" Communications of the ACM, pp. 19–28, May 2002.
26. Aggelou, G. and Tafazolli, R., "On the Relaying Capability of Next-Generation GSM Cellular Networks" IEEE Personal Communications, pp. 40–47, Feb. 2001.

27. Lee, S., S u, W., Hsu, J., Gerla, M., and Bagrodia, R., "A Performance Comparison Study of Ad Hoc Wireless Multicast Protocols", IEEE Infocom 2000, Tel Aviv,Vol. 2, pp. 565–574, Mar. 2000.

28. Chiang, C., Gerla, M., and Zhang, L., "Adaptive Shared Tree Multicast in Mobile Wireless Networks" IEEE Global Telecomm. Conference (GlobeCom 1998), vol. 3, pp. 1817–1822, Nov. 1998.

29. Lee, S., S u, W., Hsu, J., and Bagrodia, R., "Analysis and Performance Comparison Study of Wireless Ad Hoc Multicast Protocols", IEEE Infocom, Tel Aviv, vol. 2, pp. 565–574, Mar. 2000.

30. Varshney, U . and Chatterjee, S., "Architectural Issues to IP Multicasting over Wireless and Mobile Networks", IEEE Wireless Communications and Networking Conference (WCNC '99), vol. 1, pp. 41–45, Sep. 1999.

31. Bommaiah, E., Liu, M., McAuley, A., and Talpade, R., "AMRoute: Ad-hoc Multicast Routing Protocol", Internet-Draft, draft-talpade-manet-amroute-00.txt, Aug. 1998.

32. Royer, E. an d Perkins, C., "Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol", MobiCom '99, Seattle, WA, pp. 207–218, Aug. 1999.

33. Wu, C., Tay , Y., and Toh, C., "Ad Hoc Multicast Routing Protocol Utilizing Increasing id-numberS (AMRIS) Functional Specification", Internet-Draft, draft-ietf-manet-amris-spec-00.txt, Nov. 1998.

34. Ji, L. and Corson, M., "A Lightweight Adaptive Multicast Algorithm", IEEE Global Telecomm. Conference (GlobeCom 1998), vol. 2, pp. 1036–1042,1998.

35. Park, V. and Corson, M., "Temporally-Ordered Routing Algorithm for MANET", IEEE Symposium on Computer and Communications, July 1998.

36. Toh, C., Guichal, G., and Bunchua, S., "ABAM: On-demand Associatively-based Multicast Routing for Ad Hoc Mobile Networks", IEEE Vehicular Technology Conference (VTC Fall 2000), vol. 3,pp. 987–993, 2000.

37. Devarap alli, V. and Sidhu, D., "MZR: A Multicast Protocol for Mobile Ad Hoc Networks", IEEE International Conference on Communications, Helsinki, Finland, 2001, vol. 3, pp. 886–891.

38. Sinha, P., Sivakumar, R., and Bharghavan, V.," MCEDAR: Multicast Core

Extraction Distributed Ad-hoc Routing", IEEE Wireless Communications and Networking Conference (WCNC '99), 1999.

39. Sinha, P., Sivakumar, R., and Bharghavan, V., "Core Extraction Distributed Ad Hoc Routing (CEDAR) Specification", Internet Draft draft-ietf-manet-cedar-spec-00.txt, Sep. 1998.
40. Lin, C. and Chao, S., A Multicast Routing Protocol for Multihop Wireless Networks, IEEE Global Telecomm. Conference (GlobeCom 1999), pp. 235–239, 1999.
41. Garcia-Luna-Aceves, J. and Madruga, E., "The core assisted mesh protocol, IEEE Journal on Selected Areas in Communications", 17, pp. 1380–1394, Aug. 1999.
42. Lee, S., Gerla, M., and Chiang, C., "On-Demand Multicast Routing Protocol", IEEE Wireless Communications and Networking Conference (WCNC '99), pp. 1298–1302, 1999.
43. Wieselthier , J., Nguyen, G., and Ephremides, A., "Algorithms for Energy-Efficient Multicasting in Ad Hoc Wireless Networks", Military Communication Conference (MILCOM 1999), Atlantic City, NJ, vol. 2, pp. 1414–1418, Nov. 1999.
44. Wieselthier , J., Nguyen, G., and Ephremides, A., On the Construction of Energy-Efficient Broadcast and Multic ast Trees in Wireless Networks, IEEE Infocom 2000, Tel Aviv, vol. 2, pp. 585–594, Mar. 2000.
45. B. Das and V. Bharghavan, "Routing in ad-hoc networks using minimum connected dominating sets", Proceedings of the IEEE International Conference on Communications (ICC'97), June 1997.
46. J. Wu, F. Dai, M. Gao, and I. Stojmenovic, "On calculating power aware connected dominating sets for efficient routing in ad hoc wireless networks", IEEE/KICS Journal of Communication Networks, Vol. 4, No. 1, pp. 59-70, March 2002.
47. Wu, J. and Gao M. "On Calculating Power Aware Connected Dominant Set For Efficient Routing In Ad Hoc Wireless Networks" Proceedings of International conference on parallel processing, Sept. 2001.
48. Spiewla Jacek K. "Dynamic Routing Protocols and Energy Efficient Communication in Mobile Ad Hoc Networks", www.ece.mtu.edu/ee/faculty/cchigan /ee4272/projects/Spring03-paper1.pdf
49. C. Raghavendra and S. Singh, "PAMAS: Power Aware Multi-Access Protocol with

Signaling for ad hoc networks", ACM Computer Communication Review, pp. 5–26, July 1998.

50. Χ. Σ. Ραγηαωενδρα, Στεπανεκ □Power-Aware Broadcasting in Mobile Ad Hoc Networks", 1999.

51. R. Kravets and P. Krishnan, "Application-driven power management for mobile communication", Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Dallas, TX ,October 1998.

52. M. Stemm, R. Katz, and S. Seshan. "A Network Measurement Architecture for Adaptive Applications". Proceedings of IEEE Infocom 2000, March 2000.

53. W. Mangione-Smith, P.S. Ghang, S. Nazareth, P. Lettieri, W. Boring and R. Jain, "A low power architecture for wireless multimedia systems: Lessons learned from building a power hog", International Symposium on Low Power Electronics and Design Digest of Technical Papers, Monterey, CA , August 1996.

54. J. Chang and L. Tassiulas, "Energy conserving routing in wireless ad hoc networks", Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Network (MobiCom), Dallas, TX (August 1998).

55. R. Ramanathan and R. Rosales-Hain, "Topology control of multi-hop wireless networks using transmit power adjustment", Proceedings of IEEE INFOCOM, Tel Aviv, Israel , March 2000.

56. V. Rodoplu and T.H. Meng, "Minimum energy mobile wireless networks", Proceedings of the IEEE International Conference on Communications(ICC), Vol. 3, Atlanta, GA , pp. 1633–69, June 1998.

57. F. Kuhn, R. Wattenhofer, and A. Zollinger. "Ad-hoc networks beyond unit disk graphs". Proceedings of the 2003. http://citeseer.ist.psu.edu/kuhn03adhoc.html

58. W.R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy efficient communication protocols for wireless micro-sensor networks", Proceedings of the Hawaaian International Conference on Systems Science, January 2000.

59. C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking

(MobiCom), Boston, MA, August 2000.

60. L. Feeney and M. Nilsson, "Investigating the energy consumption of a wireless network interface in an ad hoc networking environment", Proceedings of IEEE INFOCOM, Anchorage, AK , 2001.
61. H. Balakrishnan, Chen, jimson, "Span: An Energy Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks", ACM Wireless Networks Journal, Volume 8, Number 5, pp.17-24, September, 2001.
62. R. Kanan et.al, "Energy and rate based MAC protocol for wireless sensor networks", ACM SIGMOD, Volume 32 Issue 4, ACM New York, NY, USA, pp. 73-79, December 2003.
63. Nitin H. Vaidya et al., "A MAC Protocol to Reduce Sensor Network Energy Consumption Using a Wakeup Radio", IEEE Transection on Mobile Computing, Vol. 4(3), pp. 228 – 242, 2005.
64. J. Redi et al., "JAVeLEN - An ultra-low energy ad hoc wireless network", Ad Hoc Networks, Elsevier, 6. pp.108–126, 2008.
65. Pariza Kamboj and Ashok.K.Sharma , "Energy Efficient Multicast Routing Protocol for MANET with Minimum Control Overhead", International Journal of Computer Applications 8(7), pp:1–11, 2010.
66. L. Bodin, B. L. Golden, A. Assad, and M. Ball, " Routing and scheduling of vehicles and crews: The state of the art" Comput. Oper. Res. , vol. 10 pp. 63 - 211, 1983.
67. A. Ephremides and S. Verdu, "Control and optimization methods in communication network problems" IEEE Trans. Automat. Contr. vol. 34 pp. 930 - 942, 1989.
68. S. Jun and K. G. Shin, "Shortest path planning in distributed workspace using dominance relation" IEEE Trans. Robot. Automat. vol. 7 pp. 342 - 350, 1991.
69. E. L. Lawler, "Combinatorial Optimization" Networks and Matroids, pp. 59 - 108, 1976. :Holt, Rinehart, and Winston
70. Professor Jonathan Gross and Yellen, "The Handbook of Graph Theory", Columbia University, CRC Press, pp. 233-314 , 2003.
71. Daniel Sanders ,"Graph Theory and Its Applications", Columbia University, CRC Press, pp. 211-437, 2007.

72. Professor Jonathan Gross and Tuckker, "Topological Graph Theory", Columbia University, CRC Press, pp. 17-194, 2001.

73. Dijkstra, Edsger; Thomas J. Misa, Editor . "An Interview with Edsger W. Dijkstra". Communications of the ACM, Vol. 53 (8), pp. 41–47, 2010.

74. Floyd, Robert W. "Algorithm 97: Shortest Path". Communications of the ACM, Vol. 5 (6): pp. 18-345, June 1962.

75. Floyd, Robert W. "A general framework for solving path problems in directed graphs", pp. 570–576.

76. T. Nantagopal, T. Kim, X. Gao, and V. Bharghavan. Achieving MAC layer fairness in wireless packet networks. In Proceedings of ACM MOBICOM, Boston, MA, August 2000.

77. Y. Xu, J. Heidemann, D. Estrin, Geography-informed Energy Conservation for Ad-hoc Routing," In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 70-84, 2001.

78. G. Wang, W. Zhang, and G. Cao, "On Supporting Distributed Collaboration in Sensor Networks," in IEEE Military Communications Conference. vol. 2, pp. 752-757, 2003.

79. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in the 6th annual international conference on Mobile computing and networking Boston, Massachusetts, USA, pp. 255 – 265,2000.

80. M. Ding, D. Chen, K. Xing, and X. Cheng, "Localized Fault-Tolerant Event Boundary Detection in Sensor Networks," in IEEE INFOCOM. vol. 2, pp. 902- 913, 2005.

81. B. Krishnamachari and S. Iyengar, "Distributed Bayesian Algorithms for Fault-Tolerant Event Region Detection in Wireless Sensor Networks," IEEE Transactions on Computers, vol. 53, pp. 241- 250, 2004.

82. F. Liu, X. Cheng, and D. Chen, "Insider Attacker Detection in Wireless Sensor Networks," in IEEE INFOCOM Anchorage, AK, USA, pp. 1937-1945, 2007.

83. A. Seshadri, M. Luk, A. Perrig, L. v. Doorn, and P. Khosla, "SCUBA: Secure Code Update By Attestation in Sensor Networks," in the 5th ACM workshop on Wireless security, pp. 85-94,2006.

84. R. Sailer, X. Zhang, T. Jaeger, and L. v. Doorn, "Design and implementation of a TCG-based integrity measurement architecture," in the 13th USENIX Security Symposium. vol. 13 IBM T. J.Watson Research Center, 2004.

85. C. Krauss, F. Stumpf, and C. Eckert, "Detecting Node Compromise in Hybrid Wireless Sensor Networks Using Attestation Techniques," in Security and Privacy in Ad-hoc and Sensor Networks. vol. 4572/2007: Springer Berlin / Heidelberg, 2007.

86. S. Capkun and J.-P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in INFOCOM vol. 3, pp. 1917- 1928, 2005.

87. S. Brands and D. Chaum, "Distance-bounding protocols," in Advances in Cryptology – EUROCRYPT '93: Workshop on the Theory and Application of Cryptographic Techniques. vol. 765/1994: Springer Berlin / Heidelberg, pp. 344–359, 1994.

88. H. Song, L. Xie, S. Zhu, and G. Cao, "Sensor node compromise detection: the location perspective," International conference on Wireless communications and mobile computing Honolulu, Hawaii, USA, pp. 242 - 247, 2007.

89. L. Lazos and R. Poovendran, "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks," in the 3rd ACM workshop on Wireless security Philadelphia, PA, USA pp. 21 – 30,2004.

90 L. Fang, W. Du, and P. Ning, "A Beacon-Less Location Discovery Scheme for Wireless Sensor Networks," in IEEE INFOCOM, 2005.

91 M. Tatebayashi, N. Matsuzaki and D.B.J. Newman, "Key distribution protocol for digital mobile communication systems" Advances in Cryptology - Crypto89', Lecture Notes in Computer Science, Vol. 435, pp. 324-334, 1989.

92 C. Park, K. Kurosawa, T. Okamoto and S. Tsujii, "On key distribution and authentication in mobile radio networks" Advances in Cryptology -EuroCrypt93', Lecture Notes in Computer Science, Vol. 765 pp. 461-465, 1993.

93 M. Beller and Y. Yacobi, "Fully-edged two-way public key authentication and key agreement for low-cost terminals" Electronics Letters 29(11) Pp.:999-1001, 1993.

94 C. Boyd and A. Mathuria, "Key establishment protocols for secure mobile communications: A selective survey" Australasian Conference on Information Security and Privacy Pp. 344 -355, 1998.

95 P. Bergstrom, K. Driscoll and J. Kimball, "Making home automation

communications secure", IEEE Computer 34(10) Pp: 50-56, 2001.

96 Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victorwen and David E. Culler "SPINS: Security Protocols for Sensor Networks" Wireless Networks, Kluwer Academic Publishers. Netherlands, Pp: 521-534 , 2002.

97 E. Shi and A. Perrig, "Designing Secure Sensor Networks," in Wireless Communication Magazine. vol. 11, 2004, pp. 38-43.

98 A. Shamir, "Identity-based cryptosystems and signature schemes"[C]// *Advance in Crypto'84. LNCS 196.* Springer-Verlag, 1985: 47-53.

99 S. Tsuji and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem"[J], *IEEE Journal of Selected Areas in Communications*, 7(4): 467-473,1989.

100 D. Boneh and M. Franklin, "Identity Based Encryption from the Weil Pairing" Advance in Crypto'01, LNCS 2139, Springer-Verlag,: pp. 213-229. 2001.

101 X. Yi, "An identity-based signature scheme from the Weil pairing" IEEE Communications Letters, 7(2): 76-78,2003.

102 Y. Desmedt and Y. Frankel, "Shared Generation of Authenticators and Signatures" Advances in Cryptology-Crypto'91, LNCS 576, Springer-Verlag,: 457-469, 1992.

103 A. Boldyreva, "Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signatures Scheme" Public Key Cryptography-PKC'03, LNCS 2567, Springer-Verlag,: pp. 31-46,2003.

104 J. Baek and Y.L. Zheng, "Identity-Based Threshold Signature Scheme from the Bilinear Pairings" ITCC'04, IEEE Computer Society,: pp.124-128.2004.

105 X.F. Chen, F.G. Zhang, D.M. Konidala, and K. Kim, "New ID-Based Threshold Signature Scheme from Bilinear Pairings" Indocrypt'04, LNCS 3348, Springer-Verlag,: pp.371-383, 2004.

106 X.G. Cheng, J.M. Liu and X.M. Wang, "An Identity-Based Signature and Its Threshold Version" Advanced Information Networking and Applications-*AINA'05*, IEEE Computer Society,: 973-977, 2005.

107 Steven D. Galbraith, Keith Harrison, and David Soldera, "Implementing the Tate Pairing, Algorithmic Number Theory" 5th International Symposium (ANTS-V), *LNCS 2369*, Springer -Verlag,: 324~337, 2002.

108 H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in IEEE Symposium on Security and Privacy Berkeley, California, 2003, pp. 197- 213.

109 W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," ACM Transactions on Information and System Security (TISSEC), vol. 8, pp. 228 - 258, 2005.

110 D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," ACM Transactions on Information and System Security (TISSEC), vol. 8, pp. 41 - 77, 2005.