TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

PULCHOWK CAMPUS

Thesis No.: IC062601

DYNAMIC-ADDRESS-ALLOCATION BASED ROUTING FOR SCALABILITY SUPPORT IN WIRELESS MESH NETWORKS

By

ACHYUTA NAND MISHRA

(062/MSI/R/601)

Thesis
Submitted to
Masters of Science in Information and Communication Engineering,
Department of Electronics and Computer Engineering

MARCH, 2010

DYNAMIC-ADDRESS-ALLOCATION BASED ROUTING FOR SCALABILITY SUPPORT IN WIRELESS MESH NETWORKS

By

Achyuta Nand Mishra

(062/MSI/R/601)

Thesis Supervisor

Sharad Kumar Ghimire

Asst. Professor

Institute of Engineering, Pulchowk, Campus

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Information and Communication Engineering

Department of Electronics and Computer Engineering

Institute of Engineering, Pulchowk Campus

Tribhuvan University

Lalitpur, Nepal

March, 2010

COPYRIGHT ©

Recommendation

The undersigned certify that they have read and recommended to the Department of Electronics and Computer Engineering for acceptance, a thesis entitled "**DYNAMIC-ADDRESS-ALLOCATION BASED ROUTING FOR SCALABILITY SUPPORT IN WIRELESS MESH NETWORKS"**, submitted by **Achyuta Nand Mishra** in partial fulfillment of the requirement for the award of the degree of "**Master of Science in Information and Communication Engineering**".

……………………………………

Sharad Kumar Ghimire

Asst. Professor

(Thesis Supervisor)

Department of Electronics and Computer Engineering

Institute of Engineering, Tribhuvan University,

Pulchowk Campus, Nepal

……………………………………

Om Bikram Thapa

(External Examiner)

Chief Technical Officer

Vianet Communication

Departmental Acceptance

The thesis entitled "**DYNAMIC-ADDRESS-ALLOCATION BASED ROUTING FOR SCALABILITY SUPPORT IN WIRELESS MESH NETWORKS** ", submitted by **Achyuta Nand Mishra** in partial fulfillment of the requirement for the award of the degree of "Master of Science in Information and Communication Engineering" has been accepted as a bonafide record of work independently carried out by him in the department.

Prof. Dr. Shashidhar Ram Joshi
Head of the Department
Department of Electronics and Computer Engineering,
Institute of Engineering,
Tribhuvan University,
Pulchowk, Nepal.

To my family

ACKNOWLEDGEMENTS

First of all, I would like to express my profound gratitude to Asst. Prof. Sharad Kumar Ghimire, my thesis supervisor and program coordinator of M.Sc. Information and Communication Engineering program, for his continuous help, support and inspirations during the thesis as well as during the whole of my study period in IOE.

I am grateful to my external examiner Mr. Om Bikram Thapa for his valuable time carefully reviewing my final thesis draft and providing useful suggestion.

I would like to thank Rajiv Nakarmi, faculty of computer science department in St. Xavier's College, for his keen interest, valuable suggestions and guidance during the whole period of thesis work.

My special thanks go to all staffs of the Department of Electronics and Computer Engineering and Information and Communication Engineering program of IOE and my friends for their cooperation during this study period.

Finally, I would like to dedicate this piece of work to my beloved parent who showed me the correct path of life.

Achyuta Nand Mishra
062/MSI/R/601

ABSTRACT

Ad hoc routing protocols cannot use efficiently because they don't scale well as the network size increases more than few hundred nodes. The existing protocols rely on flat and static addressing to keep track of each node individually. So, dynamic address allocation can be used to solve the problem of scalability. "Party" is recently proposed dynamic address allocation routing protocol, but it has not efficient mechanism for dynamic allocation of address in case of address in case of node failure and node movements.

Enhanced Mobile Party (EMP) is proposed to incorporate in party protocol to enhance it for dynamic address allocation in case of node failure and node movements. It provides better scalability as network size increases and as number of traffic flow increases. So, it can be better used for Wireless Mesh Network (WMN). With the help of Network Simulator (NS2) the performance of EMP is evaluated and compared with existing routing protocol AODV and DSDV. From simulation it is observed that EMP has better performance than AODV and DSDV in terms of signaling overhead as the network size and the number of traffic flow increases. In terms of packet delivery ratio, EMP performs better in static case and in case of mobility it provides PDR of more than 96.5%. External node and non-party can communicate with EMP which is more compatible and flexible in compared to exiting routing protocols, but EMP has high end to end delay.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

3G	3^{rd} Generation
AN	Anchor Node
AODV	On-Demand Distance Vector
BS	Base Station
BU	Binding Update
CBR	Constant Bit Rate
CI	Confidence Interval
CMU	Correspondent Mapping Update
CN	Correspondent Node
CoA	Care Of Address
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
EMP	Enhanced Mobile Party
ESS	Extended Service Set
ETX	Expected Transmission Count
GPS	Global Positioning System
GR	Gateway Router
HA	Home Agent
HIP	Host Identity Protocol
HNA	Host And Network Association
ID	Identity
IEEE	Institute Of Electrical And Electronics Engineers
IFQ	Interface Queue
IGR	Internet Gateway Router
INT	Institute National Des Telecommunications
IP	Internet Protocol
kbps	Kilo Bit Per Second

kmph	Kilo Meter Per Hour
L2	Layer 2
m	Meter
m/s	Meter Per Second
MA	Mapping Acknowledgement
MAC	Medium Access Protocol
MIPV6	Mobile IP Version 6
MN	Mobile Node
MR	Mesh Router
ms	Millisecond
MU	Mapping Update
NAT	Network Address Translation
NLOS	Non-Line-Of-Sight
NMN	Non-Party Mobile Node
No.	Number
NS	Network Simulator
OLSR	Optimized Link State Routing
OTCL	Object Tool Command Language
PA	Party Address
PDR	Packet Delivery Ratio
PMN	Party Mobile Node
PPN	Packet Processing Node
RA	Rendezvous Node
RAd	Routers Advertisements
RTT	Round Trip Time
RWP	Random Way Point
sec.	Second
SIP	Session Initiation Protocol
SON	Self-Organizing Network
TBRPF	Topology Broadcast Based On Reverse-Path Forwarding

TCL	Tool Command Language
Tid	Temporary Identity
UDP	User Datagram Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WIMAX	Worldwide Interoperability For Microwave Access
WLAN	Wireless Local Area Networks
WMAN	Wireless Metropolitan Area Network
WMN	Wireless Mesh Network
WPAN	Wireless Personal Area Networks

List of Symbols

$\in$	Belongs to (or is an Element of)
ρ	Intensity of The Arrival Process (Offered Traffic)
λ	Arrival Rate of Packets or Service Requests
μ	Service Completion Rate
γ	Input Net Mean Arrival Rate
B	Bandwidth in Bytes Per Second
D_i	Distance in Hops Between Two Nodes or No of hops the packet travels
$D_{i,Avg}$	Average Distance in Hops Between Two Nodes
K	Queue Length in Terms of Number of Packets
L	Latency of Wireless Link Between Nodes
$\log_a$	Logarithmic Function to the Base a
MA_{proc}	Time for Processing of the MA Message
MU_{proc}	Time for Processing of the MU Message
N	Total No of Nodes in Network
NP_{Avg}	Average Number of Packets Forwarded Per Session.
O(q)	of Order q
P	Size of Packet in Octet (Header + Payload + Overhead)
P_B	Blocking Probability
$(PDO)_{HO}$	Packet Delivery Overhead – due to Header Overhead
$(PDO)_{SO}$	Packet Delivery Overhead Due to Signaling Overhead
P_i^+	Additional Header Size (Excluding the Basic Party Header)
$P_{Loss,rate}$	Packet Loss Rate
P_O	Probability That There is No Packet in the Queue

P_{scale}	Number of Retransmission Plus One
RTT_{X-Y}	Round Trip Time Between Node X and Node Y
SP_i	Signaling Packet Size in Byte (Header + Payload)
t_a	Address Configuration Time
$T_{addconf}$	Time to Exchange Messages Between MPN and New Parent Node to Get a New Temporary Address.
t_d	Movement Detection Time
$T_{end-to-end}$	Packet Delivery Delay from Source to Destination
t_h	Total Handover Latency or Delay
T_{hello}	Average Time to Receive the HELLO Message from Neighbor
T_O	Average Total Overhead Per Packet
t_o	Mapping Update Completion Time
t_p	Additional Processing Delay (Mapping Table Lookup, Encapsulation or Header Modification Delay) at PPN.
t_r	Mapping Table Lookup Delay and or Processing Delay in Every Node
t_{reg}	Mapping Registration Time
$T_{rep,Tid}$	Time to Get Reply from Parent Node to MPN
$T_{req,Tid}$	Time to Send Request for Temporary Id from MPN to Parent Node
T_{table_update}	Time to Update the Neighbor Tables or Mapping Tables
V_{max}	Maximum Speed of Node

CHAPTER 1

INTRODUCTION

1.1 Background

Among the various wireless networks evolve in the next generation to provide better services, Wireless mesh networks (WMNs) are exciting key new technologies. WMNs are dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves (creating, in effect, an ad hoc network). This feature brings many advantages to WMNs such as low up-front cost, easy network maintenance, robustness, and reliable service coverage. Their promise of rapid deployment and re-configurability makes them suitable for important applications such as disaster recovery, homeland security, transient networks in convention centers, and hard-to-wire buildings such as museums, unfriendly terrains, and rural areas with high costs of network deployment. They can provide large coverage area, reduce “dead-zones” in wireless coverage, lower costs of backhaul connections for base-stations, and improve aggregate 3G, 802.11 cell throughput and help increasing end-user battery life.

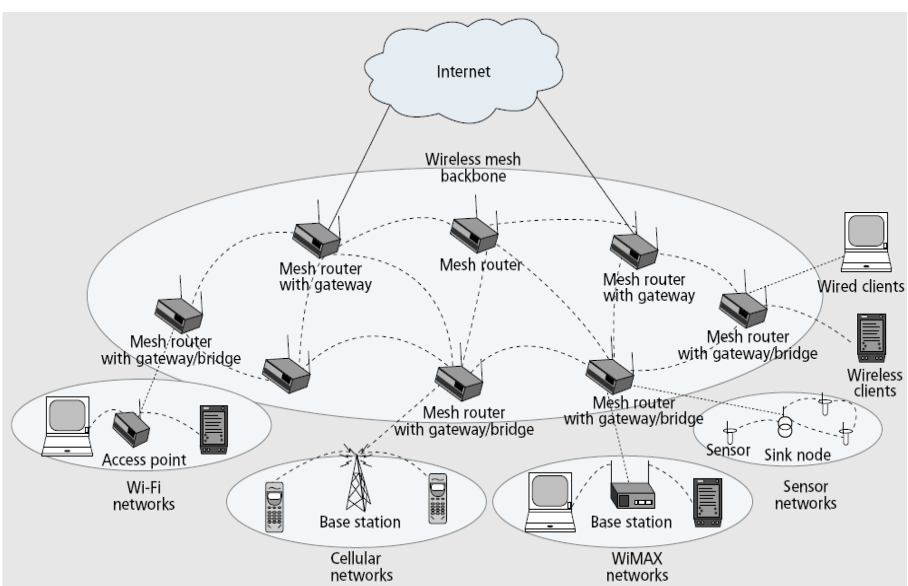

Fig. 1.1: Infrastructure or backbone Wireless Mesh Network (Adopted from [1])

Wireless mesh networks (WMNs) consist of mesh routers and mesh clients, where mesh routers have minimal mobility and form the backbone of WMNs. They provide network access for both mesh clients and conventional clients. The integration of WMNs with other networks and technologies such as the Internet, cellular, IEEE 802.11 (**Wi-Fi**, 2007), IEEE 802.15, IEEE 802.16 (**Wi-Fi**, 2007), sensor networks, etc., can be accomplished through the gateway and bridging functions in the mesh routers. Mesh clients can be either stationary or mobile, and can form a client mesh network among themselves and with mesh routers. WMNs can resolve the limitations and significantly improve the performance of ad hoc networks, wireless local area networks (WLANs), wireless personal area networks (WPANs), and wireless metropolitan area networks (WMANs) [1] and [2].

Due to potential applications of WMNs, large numbers of researchers have been attracted towards WMNs. Industrial standards groups are also actively working on new specifications for mesh networking.

WMNs have so many similarities with ad hoc networks, so deploying a WMN is not too difficult, because all the required components are already available in the form of ad hoc network routing protocols, IEEE 802.11 MAC protocol, wired equivalent privacy (WEP) security, etc. Several companies have already realized the potential of this technology and offer wireless mesh networking products. A few test beds have been established in university research labs. However, to make a WMN be all it can be, considerable research efforts are still needed. For example, the available MAC and routing protocols applied to WMNs do not have enough scalability; the throughput drops significantly as the number of nodes or hops in a WMN increases [3] and [1]. Some providers have developed mesh routers based on existing ad hoc routing protocols e.g. mesh routers of Fireside Networks are based on topology broadcast based on reverse-path forwarding (TBRPF) protocol, Microsoft mesh networks are built based on dynamic source routing (DSR), and many other companies are using ad hoc on-demand distance vector (AODV) routing, etc [2].

In any ad hoc network including WMNs nodes can be mobile and routing protocols must have capability to manage the nodes' mobility. Some solutions have been proposed for the mobility management in context of WMNs. In [4], authors propose to use the Mobile NAT solution within the context of mesh networks in order to achieve transparent mobility. Mobile NAT combines the Network address Translation functions with mobility operations executed by particular mobility agents. Whenever a MN is connected to a new relay (mesh router), this latter will NAT its packets and encapsulates them to the Anchor node. The Anchor node (AN) is the mesh network gateway that provides internet access. When the A receives the packets, it NATs them another time using its public address and forwards them to their final destination. Mapping rules are exchanged between AN and relays via signaling path via mobility agent. This latter is also responsible for detecting visiting node and guarantee their roaming or handoff transparently. The encapsulation achieved by the relays nodes hides the address destination of the packet which forces all intra-mesh network communications to go through the Anchor node. This slows down the transmission process.

[5] Use the link-state based routing protocol OLSR (Optimized Link state routing) for managing clients' mobility. Whenever a client associates with a new Mesh router (Access Point), the OLSR is triggered. It advertises the new location of the client by sending a HNA (Host and Network Association) message to the others mesh routers inside the mesh backbone. For keeping a permanent trace of the client, an IP-to-MAC address mapping table is required in each Mesh router. A major inconvenient of this solution is the scalability. Indeed, a huge amount of overhead is generated whenever the number of mobile clients increase or even the number of mesh routers increases.

Mobile IPv6 [6], the IETF standard for mobility management can also be used with mesh networks. The gateway of the mesh network or any other mesh router will achieve the functionality of the Home Agent. The idea is to register the current location of the Mobile node/Network with the HA. When a packet is sent by a Correspondent Node (CN) to the mobile node/network, it will be intercepted by the HA and then encapsulated to the Care of address (a temporary address configured at the visited network) of the Mobile node/Network. A signalling message called Binding update (BU) is used to register the CoA (prefix) of the mobile node (mobile network). However, MIPv6 is not suitable for micro-mobility as it generates high handoff latency. But these solutions are either proposed for specific topology or are not suitable due to lack of scalability support. So a robust solution is still lacking.

1.2 Statement of the problem

As discussed above the WMNs have a large number of potential applications e.g., broadband home networking, community and neighborhood networks, enterprise networking, building automation , disaster recovery, hard-to-wire buildings such as museums, unfriendly terrains, and rural areas with high costs of network deployment etc., as a result they are gaining significant attention and popularity [7]and [8]. With the capability of self-organization and self-configuration, WMNs can be deployed incrementally, one node at a time, as needed. As more nodes are installed, the reliability and connectivity for the users increase accordingly.

It is quite likely that the number of nodes and consequently number of hops will be large in WMNs as backbone mesh network will have traditional clients as well as mesh clients. So scalability of existing routing protocols for ad hoc network is a major issue and a new routing protocol which is scalable is needed. It is well known that the current ad hoc protocol suites do not scale to work efficiently in networks of more then a few hundred nodes [9]. The main reason behind this problem is the most of the current ad hoc routing architectures use static addressing and thus need to keep track of each node individually, creating a massive overhead problem as the network grows [10]. This problem of scalability can be solved by using the addressing scheme which indicates the location information. The problem with this location based addressing is that when connected to internet or other network, such address may not be unique. So the better solution is to use two addresses of node one globally unique static address and one dynamically allocated location based address for routing protocol. In their papers [9] and [10], the authors showed that the use of dynamic addressing can enable scalable routing in ad hoc networks. In this paper, each node has a unique permanent identifier and a transient routing address, which indicates its location in the network at any given time. The main challenge in such scheme is dynamic address allocation in the face of node mobility.

Sukkar G. A [11] have recently proposed a routing protocol called ‘Party’ based on dynamic addressing. Authors of this paper claim better performance of party over existing ad hoc routing protocols in terms of scalability. Party protocol is applicable to WMNs as it has scalability capability in terms of throughput and signaling overhead as the size of WMNs increases. However the authors have focused on the case of static nodes. They did not consider the case when nodes are moving and their dynamically allocated addresses are changing. But in real life some nodes are mobile in ad hoc network as well as in WMNs. Furthermore they did not consider the case that some nodes can fail suddenly. The assumptions that no node will fail is also not realistic. It is well known that in the protocols based on dynamic addressing, the main challenge is dynamic address allocation in the face of node mobility, but the authors has not mentioned effective schemes for this problem. Furthermore, if we use party protocol in WMNs, there must be some mechanism so that party-enabled nodes can communicate with non-party networks; otherwise our WMNs become isolated which is not acceptable.

Although party protocol is scalable and suitable for WMNs, it has to be enhanced to solve the problems and limitations mentioned above. Thus, it is very interesting to study and analyze party protocol (along with other existing ad hoc routing protocols) and further enhance it to make it suitable to our requirements for WMNs.

1.3 Objectives

The overall objective of this thesis is to analyze and propose mobility management mechanism for WMNs. The specific objectives are as follows:

1. To study in depth the concept of WMNs and state-of-the-art of network layer protocols for WMNs.

2. To study and analyze existing routing protocols (including Party protocol) relevant to WMNs in context of scalability. Finally select most suitable routing protocol.

3. To incorporate and enhance mobility management mechanisms in selected routing protocol to make it suitable for WMNs.

4. To evaluate the performance of proposed mobility management scheme in terms of packet delivery ratio (or throughput) and signaling overhead in context of WMNs.

1.4 Limitations and Assumptions

- Open source network simulator, NS 2 is used, although it is not well suited for the simulation scenario of large number of nodes.

- Only some relevant ad hoc routing protocols along with party protocol are studied.

1.5 Structure of the Report

The rest of the report is organized as follows. The chapter 2 gives the brief overview of literature related to this thesis works. First part of the chapter 2 deals with WMNs, its network architecture, characteristics, some factors influencing performance of WMN and state-of-the-art of network layer protocols for WMN. Second part of chapter 2 describes the party protocol and its working principle. The methodology used for this thesis is described in chapter 3, which describes the detail analysis of party protocols and then the proposed enhancements. The later part of chapter 3 also describes some simulation and performance evaluation parameters. Simulation scenarios and results of simulation are presented and discussed in chapter 4. Finally, the conclusions drawn from this thesis and some recommendations for future work are pointed out in chapter 5.

CHAPTER 2

LITERATURE REVIEW

This chapter gives an overview of the literature that is required for understanding the concept behind the research. The context of this thesis includes WMNs and Party Protocols. This chapter starts with the brief introduction of WMNs, their network architectures, characteristic features, critical factors that should be taken into consideration before designing a protocol for WMNs and state-of-art of the network layer protocols for WMNs. As the emphasis of this thesis is to provide mobility management in WMNs which should be scalable with increasing network size, we will discuss in detail about one such protocol called party which is better suited for scalability support.

2.1 Wireless Mesh Network (WMN)

A true Mesh Network is a network in which each node is connected to all the other nodes. That is each node can communicate with all other nodes directly. In true mesh network, the number of links increases exponentially with the increase in the number of nodes. For example, the number of links is 3 for 3 nodes, 6 for 4 nodes, 10 for 5 nodes, 14 for 6 nods and so on. So true mesh network is costly, complex and impractical. Generally partial mesh network is used in practical life. In partial mesh network each node is directly connected to only few neighbor nodes instead of all other nodes [8].

If the links between the nodes are wireless, then the mesh network is called Wireless Mesh Network (WMN). A WMN is dynamically self-organized and self-configured network which consists of 2 types of nodes: Mesh routers and Mesh clients. Mesh Routers are nodes having routing capability for gateway/repeater functions as conventional routers and additional routing functions to support mesh networking, while mesh Clients are nodes having necessary functions for mesh networking but can also work as router. Mesh routers have minimal mobility and form the backbone of WMNs. They provide network access for both mesh clients and conventional clients. The integration of WMNs with other networks and technologies such as the Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor networks, etc., can be accomplished through the gateway and bridging functions in the mesh routers. Mesh clients can be either stationary or mobile, and can form a client mesh network among themselves and with mesh routers. WMNs can resolve the limitations and significantly improve the performance of ad hoc networks, wireless local area networks (WLANs), wireless personal area networks (WPANs), and wireless metropolitan area networks (WMANs) [1] and [2].

WMN is a promising wireless technology for numerous applications, e.g., broadband home networking, community and neighborhood networks, enterprise networking, building automation, etc. Their promise of rapid deployment and re-configurability makes them suitable for important applications such as disaster recovery, homeland security, transient networks in convention centers, and hard-to-wire buildings such as museums, unfriendly terrains, and rural areas with high costs of network deployment. They can provide large coverage area, reduce "dead-zones" in wireless coverage, lower costs of backhaul connections for base-stations, and improve aggregate 3G, 802.11 cell throughputs and help increasing end-user battery life [8].

2.1.1 Network Architecture of WMNs

The architecture of WMNs can be classified into 3 types based on functionality of the nodes.

Infrastructure or Backbone WMNs (Infrastructure meshing):

This is the most commonly used architecture and used e.g. to build community and neighborhood networks. Mesh routers form a mesh of self-healing and self-configuring links among them. Various types of radio technologies can be used to build this mesh backbone. Some mesh routers with gateway functionality, can be connected to the Internet. This approach is also called infrastructure meshing and provides backbone for conventional clients and enables integration of WMNs with existing wireless networks, through gateway/bridge functionalities in mesh routers as shown in Fig. 1.1. Typically, two types of radios are used in the routers, i.e., for backbone communication and for user communication, respectively. The mesh backbone communication can be established using long-range communication techniques including directional antennas, WIMAX, etc.

Client WMNs (Client Meshing)

It is a peer-to-peer network among client devices as shown in Fig. 2.1 which are using the same radio technologies.

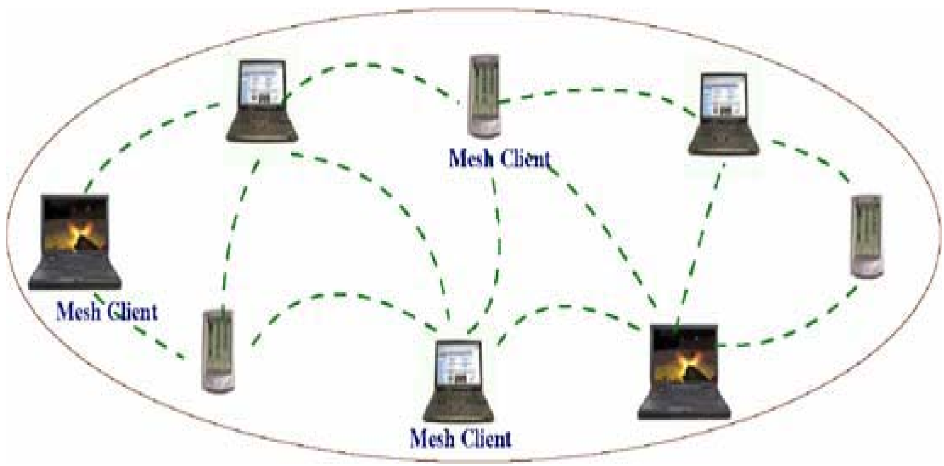

Fig. 2.1: Client WMNs (Adapted from [2])

The requirements on end-user devices is increased compared to infrastructure meshing since, in Client WMNs, the end-users must perform additional functions such as routing and self-configuration.

Hybrid WMNs:

The more practical architecture seems to be the case when Clients will form a peer-to-peer meshing among them and at the same time access the network through mesh router as shown in Fig. 2.2**.**

Fig.2. 2 : Hybrid WMNs (Adapted from [2])

2.1.2 Characteristics of WMNs:

The main characteristics of WMNs are listed below.

- ❖ WMNs Provide Multihop wireless communication which extend coverage range and also help to provide non-line-of-sight (NLOS) connectivity

- ❖ It has support for ad hoc networking and capability of self-forming, self-healing, and self-organization.

- Mobility dependence on the type of mesh nodes. Mesh Routers have minimal mobility, while Mesh Client can be stationary or mobile.

- WMNs support multiple types of network access. They support both backhaul accesses to the internet and peer-to-peer communication. They can integrate with different existing wireless networks like Wi-Fi, cellular, sensor, etc through gateway or bridge functionalities and provide services to end-users of these networks.

- Dependence of power-consumption constraints on the type of mesh nodes. Mesh Routers have no strict power constraints; Mesh Clients have strict constraint on power consumption and require power efficient protocols.

- Consists of wireless Infrastructure or backbone of mesh routers

- Reliability. Alternate route is available in case of one or few links failed.

- Scalability: As node can enter and leave mesh network, coverage area can extend by adding new nodes (Mesh Routers and clients)

2.1.3 Ad Hoc Network Vs WMNs

WMNs have many similarities with ad hoc networks, but they differ in the following respects.

- Ad Hoc Networks can be taken as Subset of WMNs, because Along with ad hoc networking technique WMNs requires some additional capabilities e. g. to form a mesh, so demanding more sophisticated algorithms.

- WMNs have wireless infrastructure or Backbone while ad hoc networks rely on end users. It provides large coverage, connectivity, and robustness in WMNs. Ad hoc may not be reliable as it depends on individual contributions of end-users. WMNs are more reliable.

- Integration: WMNs support integration of existing wireless networks such as Wi-Fi, WiMax, the Internet, cellular and sensor networks through gateway/bridge functionalities in the mesh routers

- Dedicated routing and configuration: In ad hoc end-user devices perform routing and configuration functionalities for all other nodes. But due to presence of Mesh Routers in WMNs, these load decreased significantly on end-users providing lower energy consumption and High-end application capabilities to end user devices.

- Mesh routers can use multiple radios– increasing capacity and performance of WMNs e.g. while routing and configuration are performed between mesh routers on one radio, the access to the network by end users can be carried out on a different radio. While in ad hoc networks only one radio is used for all accesses.

- Mobility: In ad hoc network, Routing; network configuration and deployment are more challenging as routing is provided using end-user devices; and network topology and connectivity depend on movement of users.

2.1.4 Critical Factors Influencing Network Performance

Before a network is designed, deployed, and operated, factors that critically influence its performance need to be considered. A detailed analysis of critical factors that influences the performance of WMNs can be found in [12] and [1]. Few important factors are as follows:

- Scalability: multi-hop networking, it is well known that communication protocols suffer from scalability issues, i.e., when the size of network increases, the network performance degrades significantly. Routing protocols may not be able to find a reliable routing path, transport protocols may loose connections, and MAC protocols may experience significant throughput reduction.

- Mesh connectivity: the MAC and routing protocol must support mesh connectivity. Network self-organization and topology control algorithms are generally needed.

Topology-aware MAC and routing protocols seems to be more suitable to improve the performance of WMNs.

- ❖ Compatibility and inter-operability with existing networks i.e. conventional clients is most important for the motivation of deploying WMNs.

- ❖ Ease of use: Protocols must be designed to enable the network to be as autonomous as possible, in the sense of power management, self organization, dynamic topology control, robust to temporary link failure, etc.

2.1.5 State of Art of Network layer protocols of WMNs

One of the limitations of WMNs is lack of standardization of protocols for different layers so far. But, due to potential applications of WMNs, large numbers of researchers have been attracted towards WMNs. Industrial standards groups are also actively working on new specifications for mesh networking. For example, IEEE 802.11 [15], IEEE 802.15 [16], and IEEE 802.16 [17] all have established sub-working groups to focus on new standards for WMNs and work is going on. The 802.11 working group in IEEE has started to produce the 802.11s standard for mesh networks. This group is called ESS Mesh Networking Task Group. 802.11s is the unapproved IEEE 802.11 amendment for Mesh Networking. It specifies an extension to the IEEE 802.11 MAC to solve the interoperability problem by defining an architecture and protocol that support both broadcast/multicast and unicast delivery using "radio-aware metrics over self-configuring multi-hop topologies." The standard is aimed for approval in 2008 [16] and [12].

The state of art of different layers' protocols, the open research issues are thoroughly described and analyzed in [12] and **[1]**. Here we talk briefly about the network layer protocols.

IP has been accepted as a network layer protocol for many wireless networks including WMNs as WMNs will be tightly integrated with the Internet. However, routing protocols for WMNs are different from those in wired networks and cellular networks. An interference aware routing protocol in multi-radio infrastructure mesh network is proposed in [18]. Routing based on a new metric, Weighted Cumulative Expected Transmission Time (WCETT), for multi-radio, multihop wireless mesh networks is proposed in [19]. As WMNs has similarities with ad hoc networks, routing protocols developed for ad hoc can be applied in WMNs. Some providers have developed mesh routers based on existing ad hoc routing protocols e.g. mesh routers of Fireside Networks are based on topology broadcast based on reverse-path forwarding (TBRPF) protocol, Microsoft mesh networks are built based on dynamic source routing (DSR), and many other companies are using ad hoc on-demand distance vector (AODV) routing, etc [2]. However, to make a WMN be all it can be, considerable research efforts are still needed. For example, the available MAC and routing protocols applied to WMNs do not have enough scalability; the throughput drops significantly as the number of nodes or hops in a WMN increases [1]. Furthermore WMNs differs from Ad hoc having minimal mobility of mesh routers, less power constraints for mesh routers, different performance metrics, etc. At the same time, in a WMN, nodes (mesh routers) in the backbone have minimal mobility and no constraint on power consumption, while mesh client nodes usually desire the support of mobility and a power efficient routing protocol. Such differences imply that the routing protocols designed for ad hoc networks are not appropriate for WMNs.

The routing protocols developed for wireless mesh networks must have the features like using multiple performance metrics-minimum-hop count, round trip time (RTT), expected transmission count (ETX), etc; fault tolerance with link failures; load balancing among different part of WMNs (e.g. using RTT metric); Scalability-Time for Setting up a routing path, overall throughput, end-to-end delay should be acceptable as network size increases; adaptive support of both mesh routers and clients, etc [18], [19] and [1]. Routing protocols of different categories have been proposed for WMNs like routing protocols with various performance metrics, multi-radio routing, multi-path routing for load balancing and fault tolerance, hierarchical routing, geographic routing, etc. But no protocol is perfect. According to [12] and [1], scalability is the most critical factor to be considered in WMNs. Hierarchical routing protocols can only partially solve this problem due to their complexity and difficulty of management. Geographic routing seems better in this aspect. But it relies on the existence of GPS or similar positioning technologies, which increases cost and complexity of WMNs. Moreover, the inquiry of destination position produces additional traffic load. Thus, developing new scalable routing protocols for WMNs is an interesting and challenging research area.

2.2 Routing Protocol Party

Party is a new routing protocol designed for wireless Self-Organizing Networks. It is intended to be applied in environments with large number of nodes where the scalability of the routing protocol plays an important role. Party's routing is unique and only depends on the current node's neighborhood. Routing tables are created on the basis of the first hop neighborhood only.

One of the most important components of the network layer is the routing protocol, the current ad hoc routing protocols and architectures work well only up to a few hundred nodes. Most of the current research in wireless Sons routing protocols focus more on performance and power consumption related issues in relatively small networks, and less on scalability. The main reason behind the lack of scalability is that these protocols rely on flat and static addressing. Party is a network layer solution in which routing is very simple and depends only on node's neighbors. Party is a distributed system without any centralized control, in which all nodes have identical responsibilities. Routing in party is hop by hop like in [20], but at the network layer. Each node has its own universal identifier (we can use as an identifier, the node's IP address or its MAC address) and is assigned a temporary address relative to its location in the network, thus the temporary address in this protocol is dynamically changed. With dynamic addressing, nodes change addresses as they move, so that their addresses have a topological meaning [11].

The party protocols can be explained in terms of its basic operations. The basic operations of party protocols are described below.

2.2.1 Address Allocation in Party

Party enables nodes to allocate addresses in a local way i.e. without the need to contact faraway nodes in the network, at any given time; each node manages a range of addresses including its own address. Node addresses are dynamically assigned depending on the node's current position in the network. More specifically, the addresses are organized as a tree. We call this the address tree, as shown in Fig. 2.3.

Let us assume that addresses are k digits decimal numbers, $a_{k-1} \ldots a_0$, the first node exist in the network take the address with all zeroes 00. . .0. We call it the root node. As nodes arrive in the neighborhood of this node (i.e. they are in the transmission range of it), they contact this node to obtain an address (call these nodes level 1 nodes). The root node control the first digit (leftmost digit) of the address, where it gives the first arriving node the address 100…0, the second arriving node 200…0 and so on up to 900…0. These nodes are called child of root node which is now parent of these node. These first level nodes control the second digit (from left) in the address, so when nodes connect to any of these nodes and ask for address, they fix the first digit same as in their own addresses and change the second digit according to node arriving sequence. For example if a node arrive and it is in the neighborhood of the node with address 100…0 and ask this node for an address, then node 100…0 will give it the address 110…0, the second node ask 100…0 for an address will take 120…0 as an address and so on (we call node 100…0 parent of nodes 110…0, 120…0,…, 190…0 and thus they are its children). These second level nodes take control of the third digit and so on. Fig. 2.3 shows an example of an address tree with three digits addresses. We call the last level nodes in the tree as leaves.

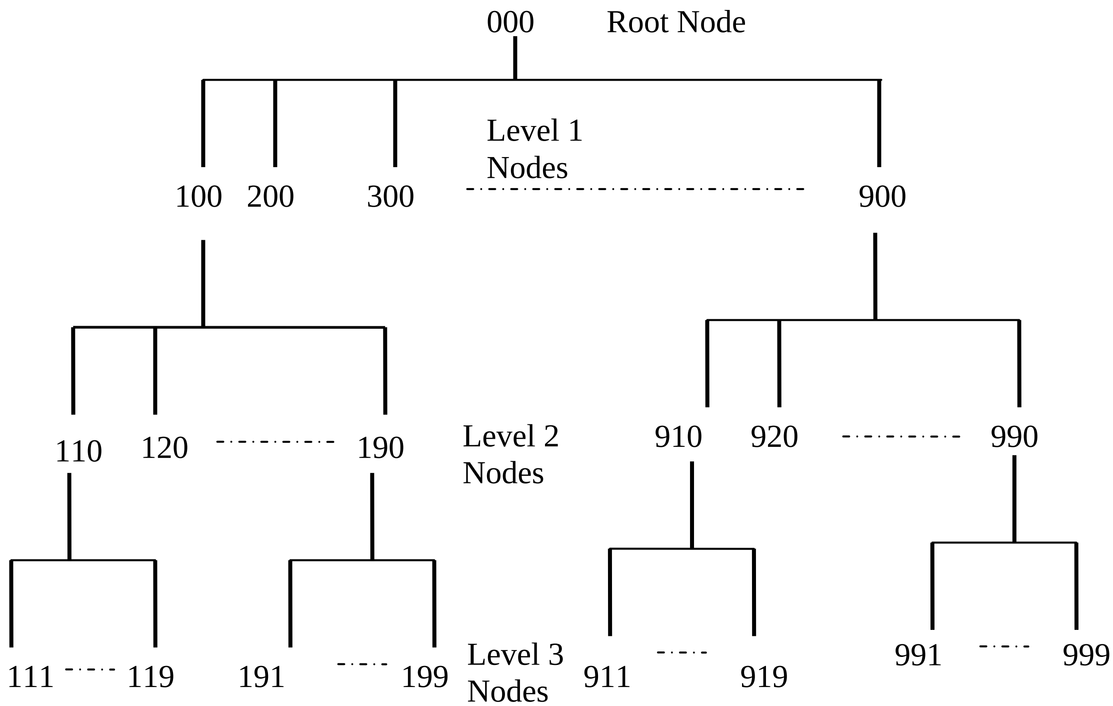

Fig. 2.3: Address tree with three digits decimal address space. (adopted from [11].)

2.2.2 Routing Procedure in Party

Address allocation algorithm in Party simplifies the routing procedure. Routing is performed in a hop by hop basis. Having obtained its temporary address Ri from one of its neighbors (we call this neighbor the parent neighbor Pi), the new node i also learns the temporary addresses of its immediate neighbors through the periodically exchanged hello messages. This neighborhood information will compose its routing table. In Party, a node routes a message by simply forwarding to the neighbor whose address is the closest to the

Searched temporary address of the destination until the messages reaches its target. In Party the message is forwarded to a node from the routing table that has a temporary address with longer shared prefix with the temporary address of the destination. If a node with a longer shared prefix matching can not find in the routing table, it simply forwards the message to the parent neighbor, and so on until the message reach its destination.

Fig. 2.4 shows an example of how the routing algorithm works, here node 10 with R_{10} = 211 wants to send message for the destination 11 with R_{11} = 121. Node 10 does not find any neighbOur node whose temporary address matches the first digit of destination temporary address, so it sends the message to its parent node 9. Due to same reason node 9 forwards the message to its parent node 4 and node 4 to its parent node 0. Now node 0 finds in its routing table that node 1 has a temporary address that matches the destination temporary address in the first digit, so it forwards the message to this neighbor, in its turn node 1 forwards this message to node 3 as temporary address of node 3 matches in first and second digits with temporary address of destination. Finally, this node forwards the message to node 11 which is the destination node. Similarly, the route to send message from node 10 to node 13 is shown in Fig. 2.4.

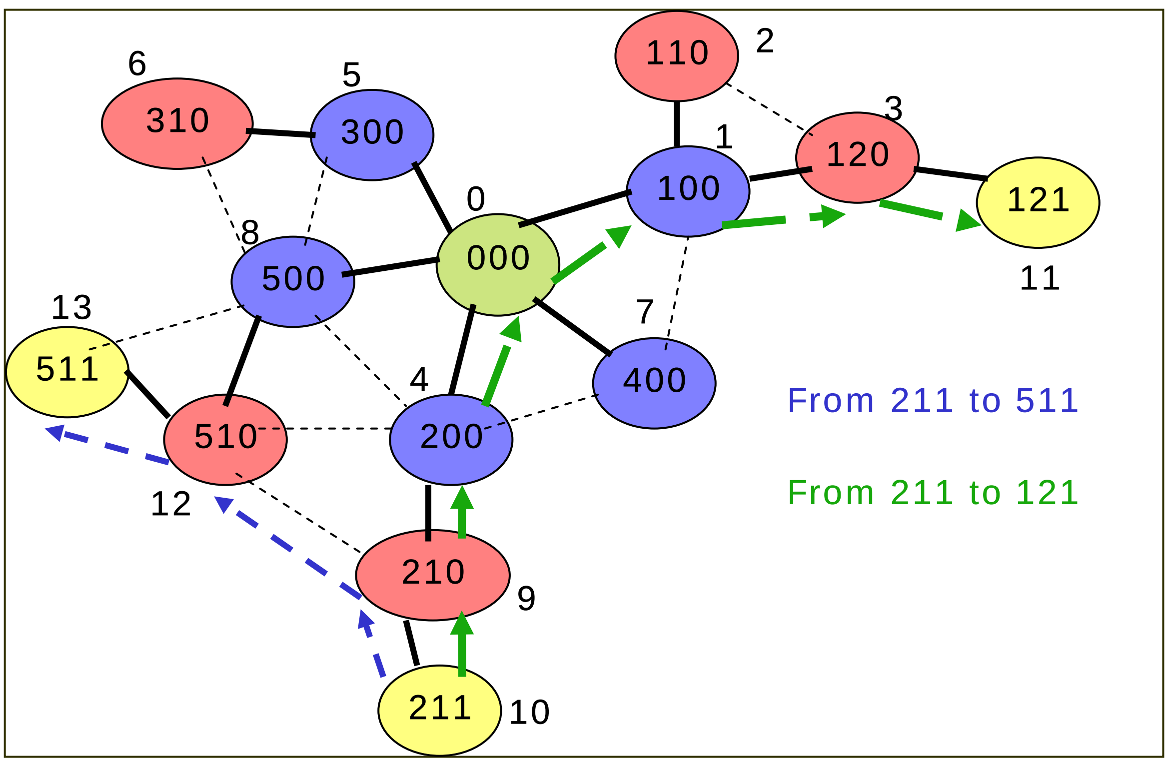

Fig. 2.4: Routing in Party. Solid Line Indicates Parent-Child; Dotted line Indicates Neighbor.

2.2.3 Address Registration Procedure

Since the address of the node is dynamically changing with node movement. After joining the network, the new node i with a temporary address R_i must identify the node which will be responsible for storing the mapping information (node ID, Current temporary address), this node is called the Rendez-vous node RA of node i. The operation of registering the temporary address in the corresponding Rendezvous node is mandatory for every arriving node. Every node in Party could be a Rendezvous node for one or more nodes in the Party network.

By using any well-known hash functions like SHA-1 [21] each node hashes its identifier, ID, and obtains an m-bit number. This number is then translated using certain function into a temporary address Rr, this address is used to find the rendezvous node of node *i* as follows. Node *i* forwards a *registration request* message using Rr as a destination address, by applying the routing procedure. This request will be forwarded until it reaches the node having temporary address that has the longest prefix matching with Rr. This node is the one responsible for storing the mapping information of node *i*; this mapping information will be refreshed periodically, as long as node *i* maintain its current position in the network. Also every node in the path to the rendezvous node will store this mapping in its cache for a certain period of time. This cached mapping is used to avoid the need to contact faraway nodes in the network for the mapping information of a node located in the vicinity of the source node. This will assure that the signalling overhead will be localized as possible.

2.2.4 Node Lookup Procedure

Since the ID of a node is not its address, Party provides a distributed node lookup service for looking up a temporary address given an identifier. Intuitively, each identifier is mapped through some function to a single address of the node (the rendezvous node) that currently holds that address is required to store the mapping and responding to requests for this mapping. In the lookup process the source node apply the globally known hash function on the destination node ID, so it well get a temporary address Rr, this temporary address is the one used to find the rendezvous node of the destination. To find the rendezvous node, the source forwards a *mapping request* message using Rr as a destination address, applying Party routing procedure, each time the message reaches a new node, this node will check its cache for a fresh mapping information, if it find this mapping, then it will respond with *mapping reply* message to the source node, otherwise it forwards the request to its neighbour whose address is the closest to the searched temporary address Rr. If no such cached information available in the path, then the request will be forwarded until it reaches the node with the longest prefix matching with Rr, this node is the rendezvous node of the destination. This rendezvous node will respond with the mapping information for the desired destination node. In the backward path from the rendezvous node to the source node, this mapping information will be cached for a certain time in each node on the path. This cached information is used in later *mapping requests* by other nodes for the same mapping information.

From the above description we can notice that Party protocol is decentralized, scalable, and independent of IP-like addressing limitations, also Party proposes an addressing structure and allocation that ease routing process. Where a small amount of information suffices to implement Party routing, *i.e.*, low signaling overhead is generated (only local neighborhood communication), thus the routing table size is $O(k)$, where k is the number of immediate neighbors of the node.

CHAPTER 3

METHODOLOGY

This chapter describes the comparative analysis of party protocols with existing protocols. As WMNs have many similarities with ad hoc networks, the existing routing protocols for ad hoc network seem suitable for WMNs. So for comparative study we choose one reactive existing ad hoc routing protocol AODV and one proactive existing protocol DSDV along with Party. Later part of this chapter describes my proposed enhancements to party protocol which can be divided into 2 phases. In first phase basic mobility supports are added to party for the communication within or outside the party network. We call the resulted enhanced party as Mobile Party. This does not include the mechanism of dynamic address allocation in case of node failure, node movement, etc. Second phase enhancement solves these problems of dynamic address allocation, after which we call mobile party as enhanced mobile party. Finally simulation variables and performance evaluation parameters are described.

3.1Analysis of the Party protocol

In this section, we will study some important features of party which inspire us to choose it as the routing protocol for WMNs. Although WMNs have some different characteristics, they have many similarities with ad hoc networks. Routing protocols for ad hoc networks, with some enhancements, seem to be suitable for WMNs. We considered three routing protocols for analysis as candidate for WMNs – Party, AODV and DSDV; analyzed and compared them for static case, theoretically and by simulation, and finally selected the party protocol for WMNs. The simulation result is same as described in section 4.1 because for static case party protocol and mobile party protocol have almost same performance. Some of the features of party protocols, which make it superior than others, are described below:

Scalability:

As mentioned before, Party is a scalable routing protocol; the scalability of this protocol comes from that it is a completely decentralized and self-organized system. Some factors that make the party scalable are as follows:

- ❖ **Size of the routing table - Smaller as well as almost Independent of Network Size and number of active flow:**

  In Party each node has a routing table of size O (q), where q is the number of immediate neighbors of the node. It should be noted that in party protocol routing table is just a neighbor table. In a classical proactive protocol the table size depends on the network size n; i.e. routing table size is O (n). In some reactive protocols like AODV, routing table size is also dependent on number of active flows.

- ❖ **Signaling traffic needed to implement and maintain the routing table.**

  In Party, routing table entries are the immediate neighbors and the signaling traffics needed are the periodic hello signals between neighbors that used to inform the neighborhood nodes that the node is still alive and still in its position and the mapping update to refresh the registration of temporary address. So, in party signaling is almost constant and independent on the number of active data flows. Classical ad hoc protocols, both proactive and reactive, require much more signaling messages and amount of signaling may depend on the number of data flows as well.

- ❖ **Cost of joining a new node: Low disturbance to existing nodes.**

  The arrival of a new node affects only a limited number of existing nodes (nodes that are in its direct transmission region). The number of neighbors and, consequently, the signaling overhead, depends only on the node’s transmission range and are independent of the total number of nodes in the system.

Communication cost:

The path establishment cost in Party is O (1), since the only thing that a source needs to establish a connection with a destination is destination's temporary address. This cost includes the cost to apply globally known hash function to the unique address (IP or MAC address) of destination to get temporary address of RA node and then to send lookup message to RA node to get the temporary address of destination. It can be shown that on average this look up message will travel just K +1/2 hops, where k is number of levels used in address tree. Any intermediate node in the way to RA node, can response to this message if it has fresh temporary address of destination in its cache.

Average Path Length, Number of nodes and Temporary Address Size:

After analyzing the party protocol, the average distance $D_{i,Avg}$, through which a packet, travels in party in terms of number of hops can be calculated as follows:

If the address tree is of the level K=2, then in worst case (e.g. from node 21 to node 12) the D_i is given as

$$D_{i,worst} = 2 * K = 4 \text{ (For K=2) hops}$$

At best (e.g. from node 21 to 51),

$$D_{i,best} = 1 \; hop$$

D_i can take any value from 1 to 4 (in general from 1 to 2*K). That is D_i = {1, 2, 3, 4} and in general Di = {1, 2, 2*K}. If the traffic generation between any 2 nodes are statistically independent and equiprobable, then

$$D_{i,Avg} = \frac{1}{4}(1+2+3+4) = 2.5\,hops$$

In general,

$$D_{i,Avg} = \frac{1}{2*K}(1+2+3+.......+2*K) = K + \frac{1}{2}\ hops \qquad \textbf{(3. 1)}$$

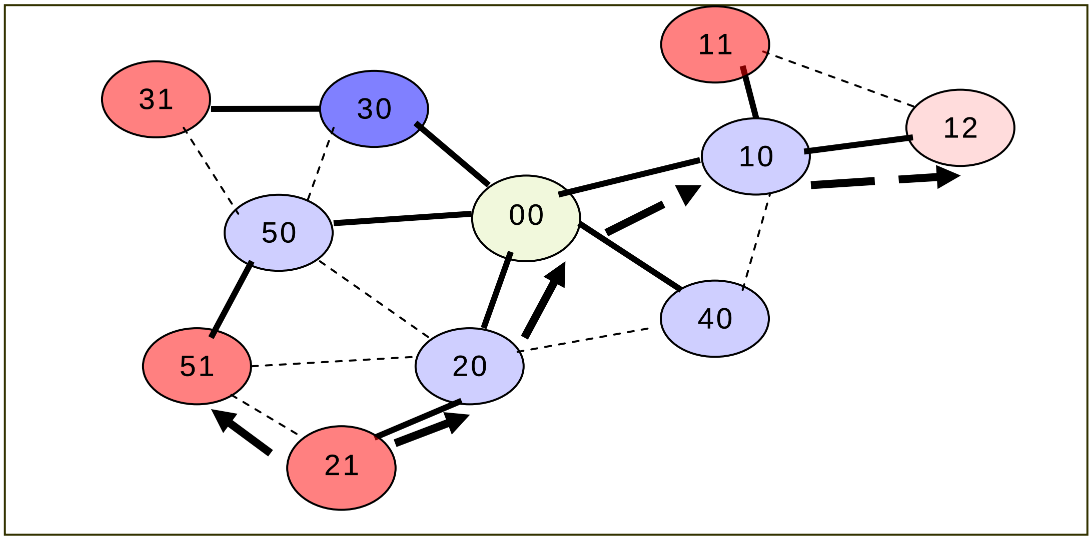

Fig. 3.1: Mesh Network with Three Digits (K=3) Decimal(R=9) Party Address

To estimate K

Let us suppose we use the addressing as XX…..X using K digits (Xs) where

$$X \in \{0, 1, 2, ..., r\}$$

Let N= total no of nodes in networks. Then we have to choose value of K satisfying

$$N = r^0 + r^0 * r^1 + r^2 + r^3 + ... + r^K$$

$$Or,\ \ N = \sum_{i=0}^{K} r^i$$

This is a geometric series, so using the formula 'Sum $=\frac{a(R^n-1)}{(R-1)}$', where a= first term = 1, R =common ratio = r, n= number of terms=K+1, we get

$$N = \frac{(r^{(K+1)}-1)}{(r-1)}$$

$$Or,\ K = [\log_r\{N(r-1)+1\}]-1 \qquad (0.2)$$

For r=9 (Fig. 2.3), we get

$$N = \frac{9^{(K+1)}-1}{9-1}$$

$$Or,\ N = \frac{9^{(K+1)}-1}{8}$$

$$Or,\ K = \lceil\ [\log_9(8N+1)]-1\ \rceil \qquad \mathbf{(0.3)}$$

So K should be

$$Or,\ K \geq \lceil\ [\log_9(8N+1)]-1\ \rceil \qquad \mathbf{(0.4)}$$

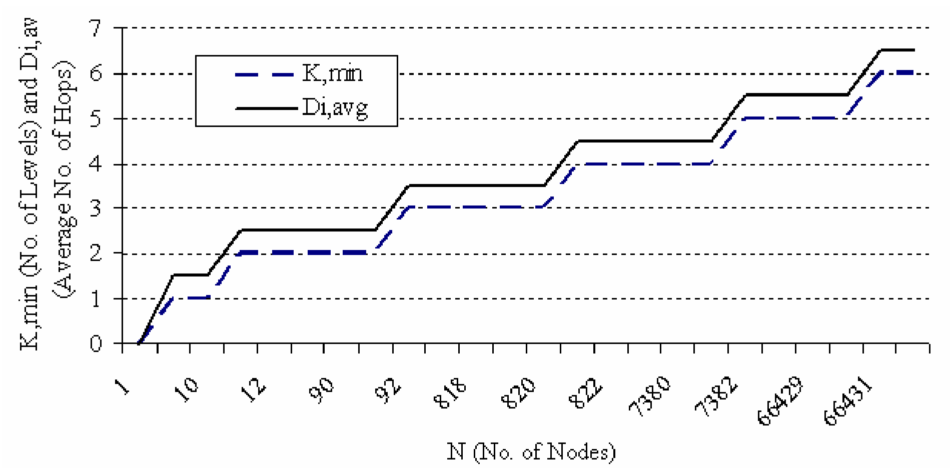

Fig. 3.2: Variation of number of digits or levels (K) and Average number of hops traveled (Di, avg) with the number of nodes (N) for decimal (r=9) address space.

Loop-free:

Another important property of Party protocol is that routing loops are impossible to occur. At any particular routing step, the packet is never routed to a node whose temporary address is farther from the destination's temporary address than the current address. The forwarding process will only greedily forward to a node whose temporary address is closer to the destination's address than the current node's address. When it fails to find such a node, it routes to its parent. Because the prefix of the parent's temporary address is also a prefix of the current node's address, it is no further from the destination address than the current node. Note that the parent cannot forward the packet back to the child; because the child's temporary address can be no closer to the destination than the parent's address.

3.1.1 Concluding Remarks about Party Protocol

From section 3.1and simulation results (the comparative simulation results are same as described in section 4.1. It should be noted that party and mobile party has same performance for static case if no nodes fails during the simulation time) it is clear that we choose party as routing protocols because of the following superiority of party protocol over other existing protocols:

- ❖ It is well scalable as the network size increases,
- ❖ Signaling traffic needed to implement and maintain the routing table is smaller and does not depend much on network size and number of active traffic flows.
- ❖ Increase in network size has less effect on throughput performance
- ❖ Communication cost is lesser
- ❖ Size of the routing table is smaller as well as almost Independent of Network Size and number of active flows.

- ❖ Disturbance on existing nodes is smaller when new node joins the network
- ❖ Average path length is k+0.5 where k is the number of digits used for temporary address.
- ❖ Routing is simple and based on prefix matching of Temporary address
- ❖ Temporary Address has some topological meaning
- ❖ It is a routing protocol for wireless Self-Organizing Network
- ❖ Party is a distributed system without any centralized control, in which all nodes have identical responsibilities.

For static cases, Party protocol is suitable. Party protocol is not optimized for mobility support. But in WMNs nodes may be moving. WMNs consist of two types of nodes- mesh router and mesh clients. Mesh routers have less or no mobility and it forms a backbone or infrastructure network of mesh router to which mesh clients and other existing networks Wi-Fi, cellular mobile, sensor networks, etc are connected. So if there is no mobility then party protocol will perform well. But we know that mesh clients are moving most of the time and in some scenario like military operation or disaster rescue, etc mesh routers are also mobile. Party protocol most has some mobility support mechanisms. Some of the limitations of the party protocol to use for WMNs are as follows.

- ❖ Interoperability: party is a new protocol. If a party enabled node of WMN needs to communicate with external node (i.e. node of other non-party network), how it can communicate. It must have some mechanism for such scenario, otherwise party enabled WMNs will be isolated from other existing networks.
- ❖ Let us suppose a node of party enabled WMN has started data session with another node CN (correspondent Node) within the same network. Now if the former node changes its temporary address due to movement or any other reason, then packets

will be lost as CN will continue to send packet assuming that former node still has the same temporary address. We must solve this problem.

- ❖ Consider a scenario in which a non-party node has already established a session with another node, CN which may be in party-enabled WMN or in some third network. Assume that the non-party node then moves in the coverage of party-enabled WMN. What will happen with the already establish session? Certainly, the session will break as the non-party node is not capable of supporting party protocol. Can we not find some mechanism to let the non-party node continue the session?

- ❖ The address allocation procedure of party has a serious drawback. If the upper level node moves and changes its address or fails, then it lets the entire preceding child parentless. For example if node with temporary address 100 is failed or changed its address due to its movement, then all the nodes whose temporary address starts with prefix 1 has to change its temporary address making the network unstable for some period, as shown in Fig. **3.3** . This situation can hamper the ongoing traffic flows, which is not acceptable. This is the most serious drawback of party protocol because in any ad hoc network or WMNs some nodes can fail or move frequently. This causes increased signaling overhead, instability of network, huge loss of packets as parent is one important node used in forwarding packets in party protocol. Without solving this problem party protocol can not be used as reliable and stable protocol.

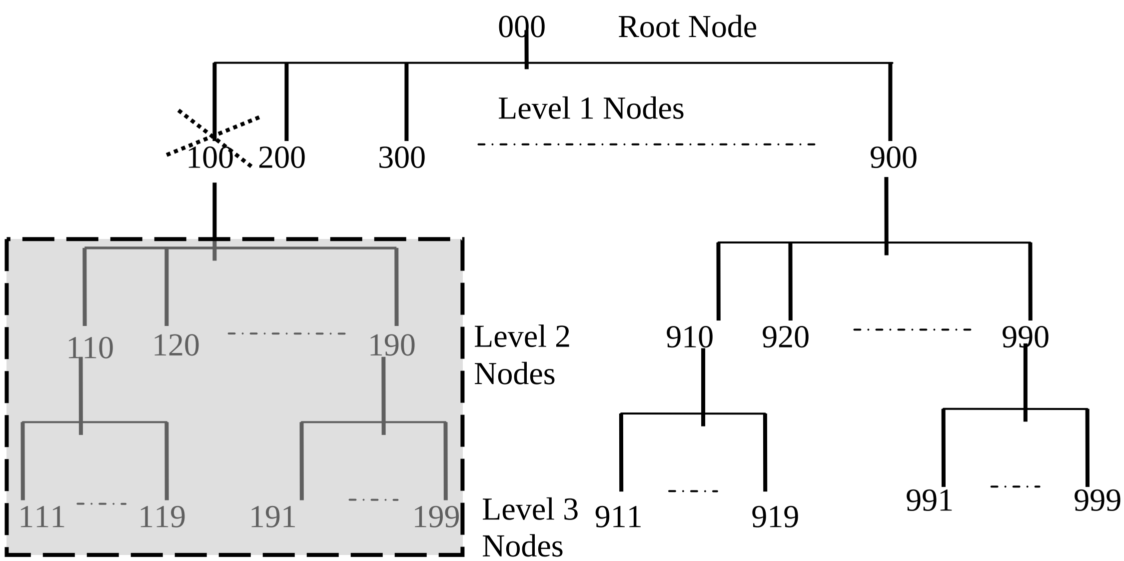

Fig. 3.3: Address Tree showing Effect of Node failure or Node Movement

3.2 Initial Enhancement of Party protocol: Mobile Party

After the detailed analysis and simulation we concluded, as discussed in **section 3.1,** that party protocols has some limitations to be used in case of mobile nodes. These limitations must be addressed i.e. party must be enhanced to make it suitable for mobility support. In this section we are proposing some mobility support enhancements to party protocols.

Nowadays users are also interested to have an access to the Internet and other ad hoc networks so that not to be isolated and limited to WMNs. Indeed, some works have trying to extended ad hoc networks by linking them to Internet Infrastructure via special nodes called “gateways”. In infrastructure mesh networks, gateway function is achieved by wireless routers named *mesh routers*. In addition to gateway/bridge function, mesh routers have additional routing functions to support mesh networking. Moreover, a mesh router can be equipped with multiple and different wireless interface technologies which improve the flexibility of mesh network. On the other side, mesh routers are well powered, self-configured and have minimal or sometimes no mobility which enhances the performance of packet forwarding and permits implementation of more advanced functions (DHCP, NAT …, etc.).

All mesh routers form a backbone (infrastructure) providing multi-hop communications between *mesh clients* and wired gateways providing Internet access. Some mesh routers are connected to the Internet infrastructure and then acts as gateways to the entire mesh network. This is completely transparent to *mesh clients* who view the mesh router as a conventional access router providing one hop access to the Internet. My overall system will look like as shown in Fig. 3.4.

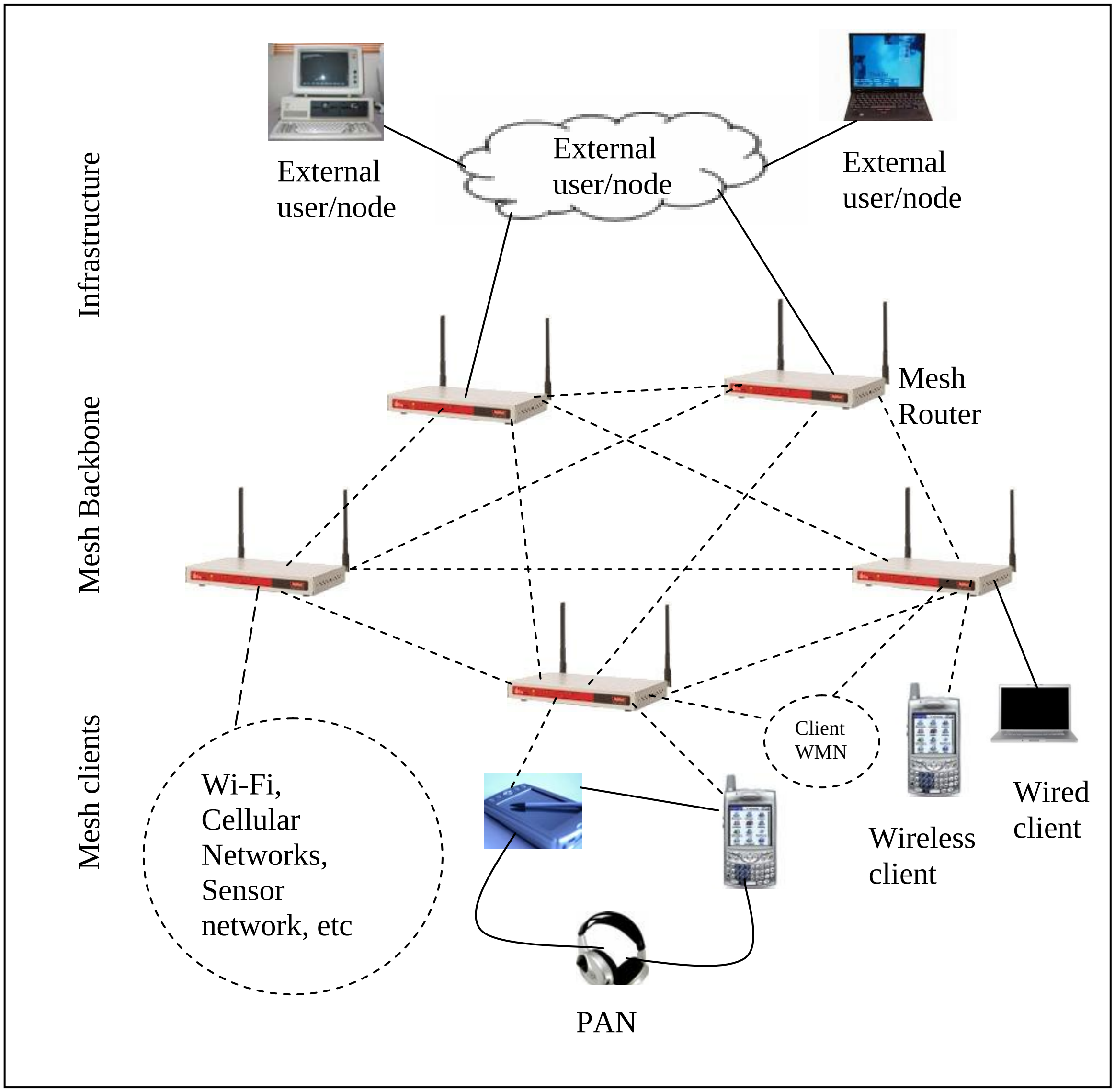

Fig. 3.4: Proposed System Model of Mesh Network

We are interested on studying the mobility management problem within the mesh network context. As already discussed in section 3.1, we use party protocol [11] to achieve mobility management in mesh network. We concluded in section 3.1 that party protocol is useful to overcome the drawbacks of mesh routing protocol in terms of scalability. My work can be divided in 2 parts. In first part we propose mobility management schemes assuming that party protocol has no any serious limitation in static case. But as we already mentioned in **section 3.1** party has a serious problem when an upper node fails or moves. In second part we propose schemes to solve that problem. Most of the existing proposed solutions focus on managing clients' mobility only inside the mesh network, my work takes into account three different scenarios of mobile communications as specified below:

- Mobile Communications inside the party-enabled mesh network
- Mobile Communications with external nodes (regarding to the mesh network).
- Mobile communications when a non Party-enabled node, which has already established a communication session with CN, visits party-enabled mesh network

By Mobile Communications, we mean communications where at least one participant is a mobile node. External node refers in this context to a node not belonging to the party enabled mesh network. Finally, a non-Party visiting mobile node is a mobile node that does not support the Party protocol and is visiting the party enabled mesh network.

One of major advantages of the Party protocol is scalability in case of wireless multi hop network. In mesh network this criteria has a great importance since many thousands of mobile users can be connected to the mesh backbone at the same time. Applying the Party protocol to the mesh network architecture as routing protocol shows better performance. However, additional functionalities must be included in the Party protocol to be able to manage users' mobility efficiently.

We propose three main schemes to guarantee this aim:

- Extending the periodic registration of temporary address to the CNs along with RA node. When a node will change its address, it will inform about it to CNs as well as RA.

- Integrating a default route notion for communications with external nodes – to support Communications with external nodes (regarding to the party enabled mesh network).

- A proxy function achieved by Access Mesh Router is introduced for non-Party nodes – to support Mobile communications when a non Party-enabled node, which has already established a communication session with CN, visits party-enabled mesh network

These are my enhancements proposed for Party protocol to manage users' mobility. After these enhancements to party protocol, we call the enhanced party as Mobile Party. We describe in details each type of Mobile communications scenarios in succeeding sections.

3.2.1 Communication inside the party-enabled mesh network

In this scenario we consider the case of mobile nodes communicating among themselves and belonging to the same WMN. Mobile nodes are Party-enabled nodes. When joining the mesh network and at each time it changes its address, a Party node will register its acquired address with its RA node as described in **section 2.2.3**. In addition, this registration request message will be also used to update the mobile node entry at the intermediate Mesh Routers' Mapping tables. This message is sent periodically by the Party node to its RA node. Moreover, each time the Party node will also send a registration update to its Correspondent Nodes. By achieving these mechanisms, the RA node and CNs has the guarantee that all stored registration entries are refreshed continually and updated. Then, each time the Party node moves and changes its location, the CNs will be updated and can forward the packet to the new Party node address.

In this case the communication between 2 communicating nodes is very simple and is as shown in Fig. **3.5**. Once the CN get the temporary address (Tid) of party mobile node (PMN), it continues to send packets to this temporary address. So it is necessary that whenever the PMN changes its temporary address, it must inform the CN about new Temporary address. This decreases the packet lost due to handover i.e. temporary address change. My proposed enhancement adds mapping update to CN periodically. This will certainly increase the signaling overhead slightly.

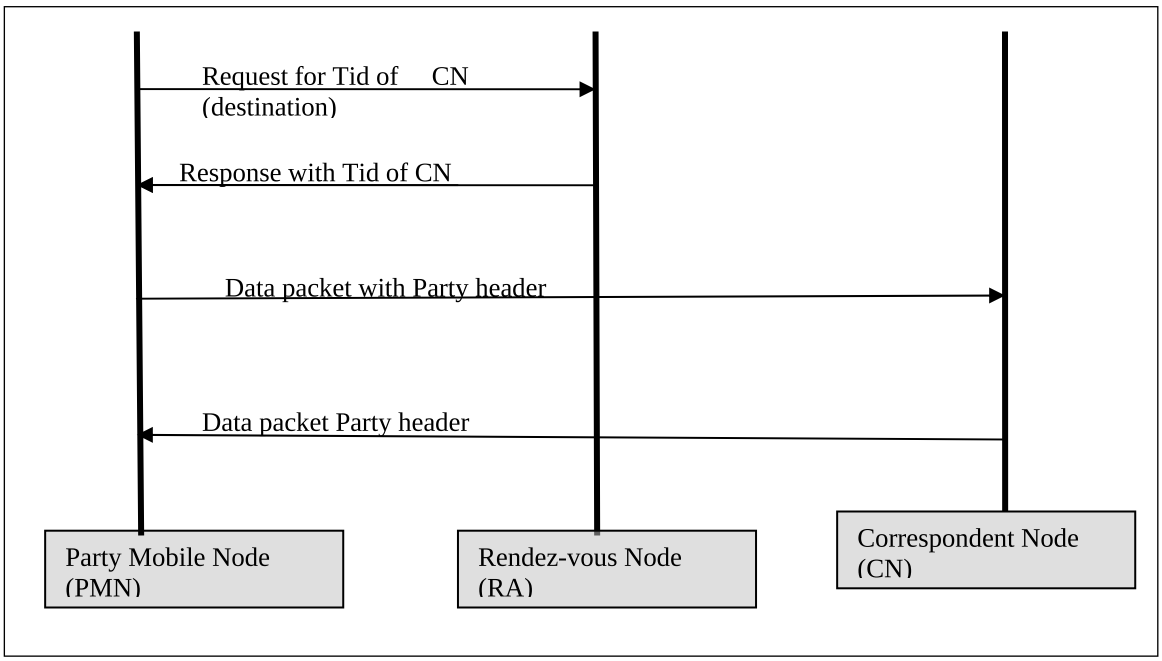

Fig. 3.5: Data transmission scenario in mesh party for communication Within the Party Network. Tid –temporary Identity or Temporary address

3.2.2 Communication with external node

In the Party protocol description, when a Party node wants to communicate with a node it will sent a Mapping request to the RA node to have the Party address of the correspondent node. However, what happens when the requested node is an external node? What is the external node's RA node address? What address will be returned? How the packet is routed to the external node?

To resolve all these issues, we propose the following enhancements. As described in **section 2.2.4**, when a Party node wants to communicate with a node it will send a Mapping request packet to the RA node address given by the Hash function. The request packet will be then intercepted by the RA node having the nearest address to the given address. If there is no entry in the Mapping table corresponding to the external node address, this latter will answer with the Party address of one of the available gateways. To achieve this, each gateway has to broadcast a gateway advertisement message in the entire mesh network backbone including its identity and its Party address. When the party node receives the Mapping reply message, it sends the data packets to the gateway Party address as if it is the external node one. When the data packet reaches the gateway, this latter will remove the Party header. If the IP addressing inside the mesh network is private, the gateway will achieve a Packet Noting by setting the source address to its address otherwise (public) it sends the packet directly to the correspondent node.

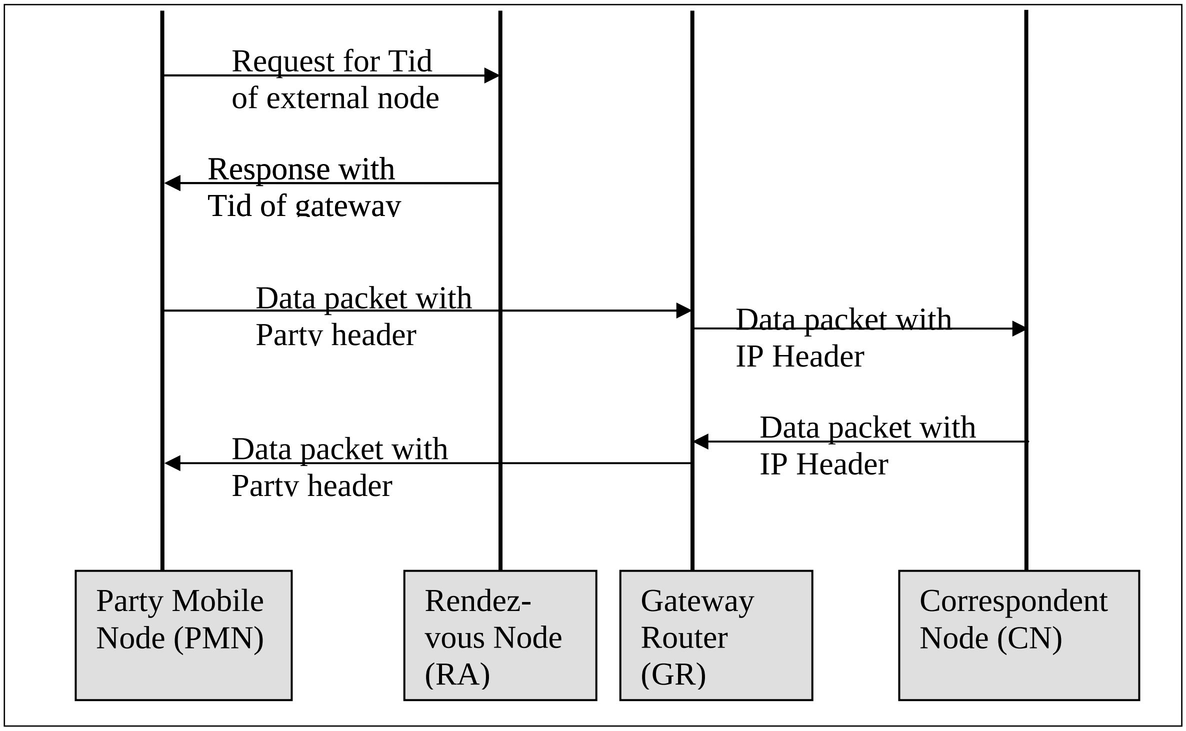

Fig. 3.6: Data transmission scenario in mesh party for communication with external node.

For incoming packets, they will be intercepted by the gateway. A Party header is added and the packet will be forwarded it to its final destination based on the available mapping entry for the sender node and the Nating policy in case of private address. After My enhancement the communication with external node (i.e. CN), would look like as shown in **Fig. 3.6.**

Due to My proposed enhancement signaling overhead will increase slightly during handover. Also gateways will broadcast a gateway advertisement message in the entire mesh network backbone including its identity and its Party address, increasing the signaling overhead.

3.2.3 Communication with Non-Party Mobile Node

This scenario happens when a non-Party node is visiting the mesh network and has already established communications with distant node. How this node can continue receiving and sending data via the mesh network access Router without any support to the Party protocol mechanisms? How we can provide transparency to visiting nodes with a minimum effect on communications performances in terms of handoff latency and end-to-end delay?

To achieve this, we divide the mobility management in two parts: macro-mobility and micro-mobility. By micro-mobility we mean the mobility achieved by the mobile inside the same mesh network (in terms of administrative authority). Macro-mobility happens when the non-Party node moves from one mesh network to another one.

We suppose that the visiting node has already a mobility management mechanism that guarantees a seamless communications when moving. This mechanism can be one of the well known protocols for mobility like Mobile IP, SIP [30], and HIP [31]. We suppose that the Mobile IPv6 [6] is the protocol used by the non-Party node to manage its mobility.

As long as the MIPv6 node is moving inside the mesh network, it will have the same CoA. This CoA is configured based on Routers Advertisements (RAd) sent by only Internet gateways on the infrastructure and broadcasted in the entire mesh network by the others mesh routers. For MIPv6-node location inside the mesh network (micro-mobility), it will be managed by the mesh router acting as a base station to this MIPv6 node. Indeed, this later will register a Mapping corresponding to the MIPv6 node identity (IP address) and its BS's Party address as MIPv6 node Party address. Packets sent by the MIPv6-node will be intercepted by its current mesh router and routed inside the mesh backbone as if they are generated by the mesh router. Then, this latter will add the Party header with its Party address as source address, request the Party address of the destination (a gateway or local node), find the next hop to the packets and forward the packet inside the mesh backbone. For incoming packets, they are intercepted by the gateway and forwarded to the mesh router to which the MIPv6 node is connected. This mesh router removes the Party header and sends the packet to the MIPv6 node. Whenever, the MIPv6 node is moving inside the mesh network there is no need to wait for binding update message to reach the HA since it keeps the same CoA.

For refreshing the MN location at the mesh routers level when it moves, the binding update message is used. Indeed, each Mesh router receiving the BU message will update the Mapping table entry corresponding to the source Identity (MN home address). By this mechanism, the cross-over mesh router at the intersection between the old and the new Path is updated and can forward packets to the right Party address. This will reduce considerably the handoff latency and provide a seamless communications. When the MIPv6 node moves to another mesh network (in terms of domain authority), its mobility is then managed by the MIPv6 protocol as it is a macro mobility issue.

The communication of visiting non-party mobile node with an external node CN will look like as shown in Fig. **3.7.**

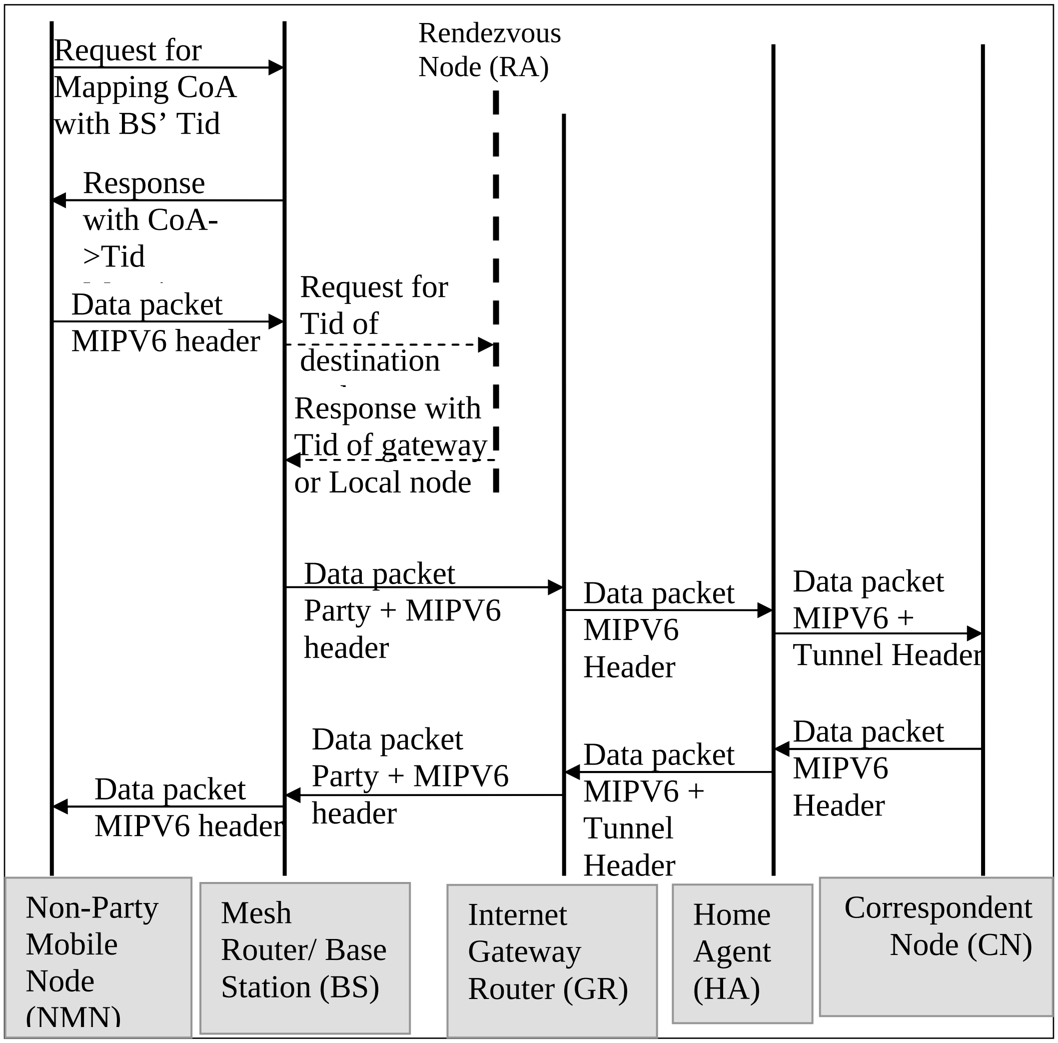

Fig. 3.7: Communication of Visiting Non-party Mobile Node with an External Node CN

The handover scenario i.e. the scenario when the non-party node changes the mesh router, called BS, will increase the signaling overhead slightly. Furthermore, Routers Advertisements (RAd) carrying information about available CoA is sent by only Internet gateways on the infrastructure and broadcasted in the entire mesh network by the others mesh routers periodically. This will also add the signaling overhead.

3.3 Proposed Enhanced Mobile Party (EMP)

In **section 3.2.1, 3.2.2, 3.2.3**, we proposed 3 schemes to support users' mobility under different scenarios. After these scenarios party-enabled mobile nodes can communicate either within themselves or with an external node. Furthermore a non-party node can visit party-enabled mesh network seamlessly. For Mobile party protocol and all the above schemes to work properly temporary address and parent node (Base station) play most important role. So far discussed party protocol and its enhancements does not have any robust mechanism to re-allocate the address or re-assign the parents, grand parent, and so on in the case when some parent or grand parent, … will change the address or fails suddenly.

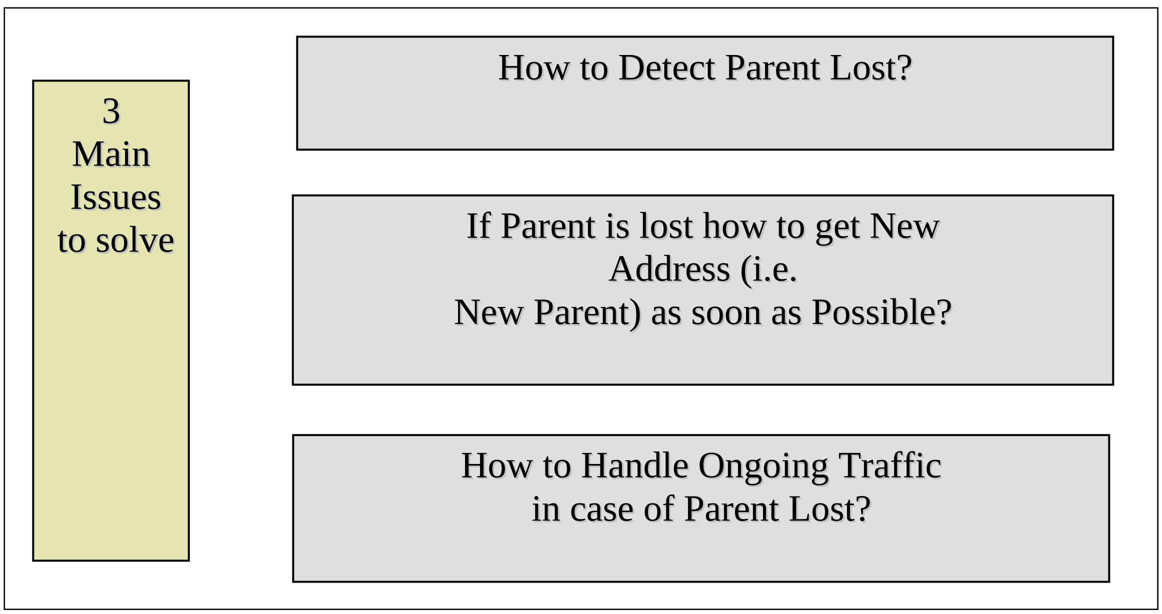

Fig. 3.8: Issues to solve in Mobile Party Protocol

As we already discussed in **section 3.1.1,** the address allocation procedure of party has a serious drawback. If the upper level node moves and changes its address or fails, then it lets the entire preceding child parentless. This is due to the fact that mobile does not have any robust mechanism for dynamic address allocation. The main issues to consider for this enhancement is how to detect that a node has lost the link with parent, how to get new address (i.e. new parent) as soon as possible if parent is lost and how to handle the ongoing traffic in the case of parent loss as shown in Fig. 3.8. The temporary address management algorithm in

Party and Mobile Party can be shown diagrammatically as shown in Fig. **3.9 and Fig. 3.10**. We can see that if any node loses its parent there is no mechanism to detect it, to select other parent and to reallocate address.

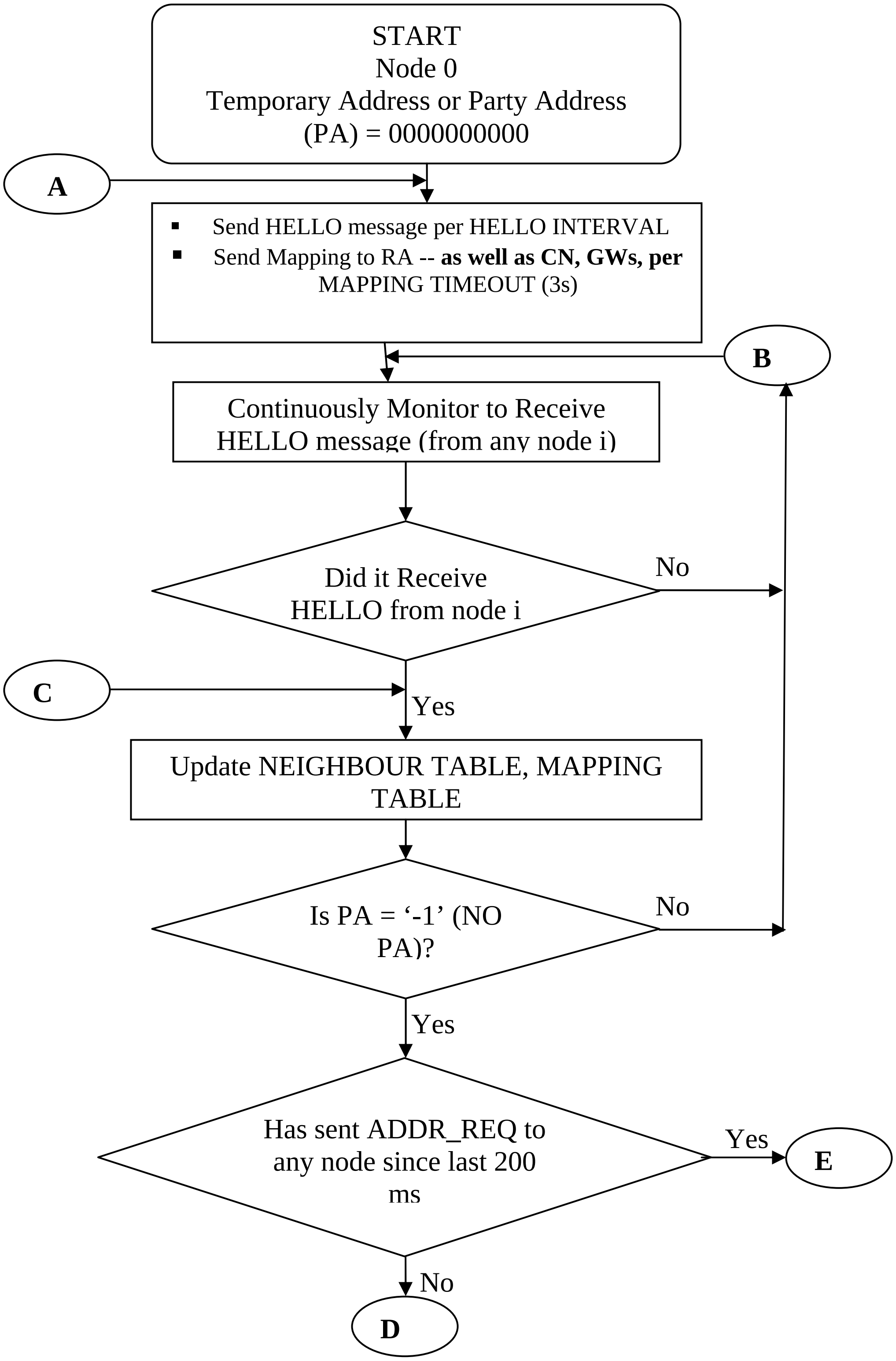

Fig. 3.9 : Temporary Address Allocation in Mobile Party or Party (PA = Party Address i.e. Temporary Address)

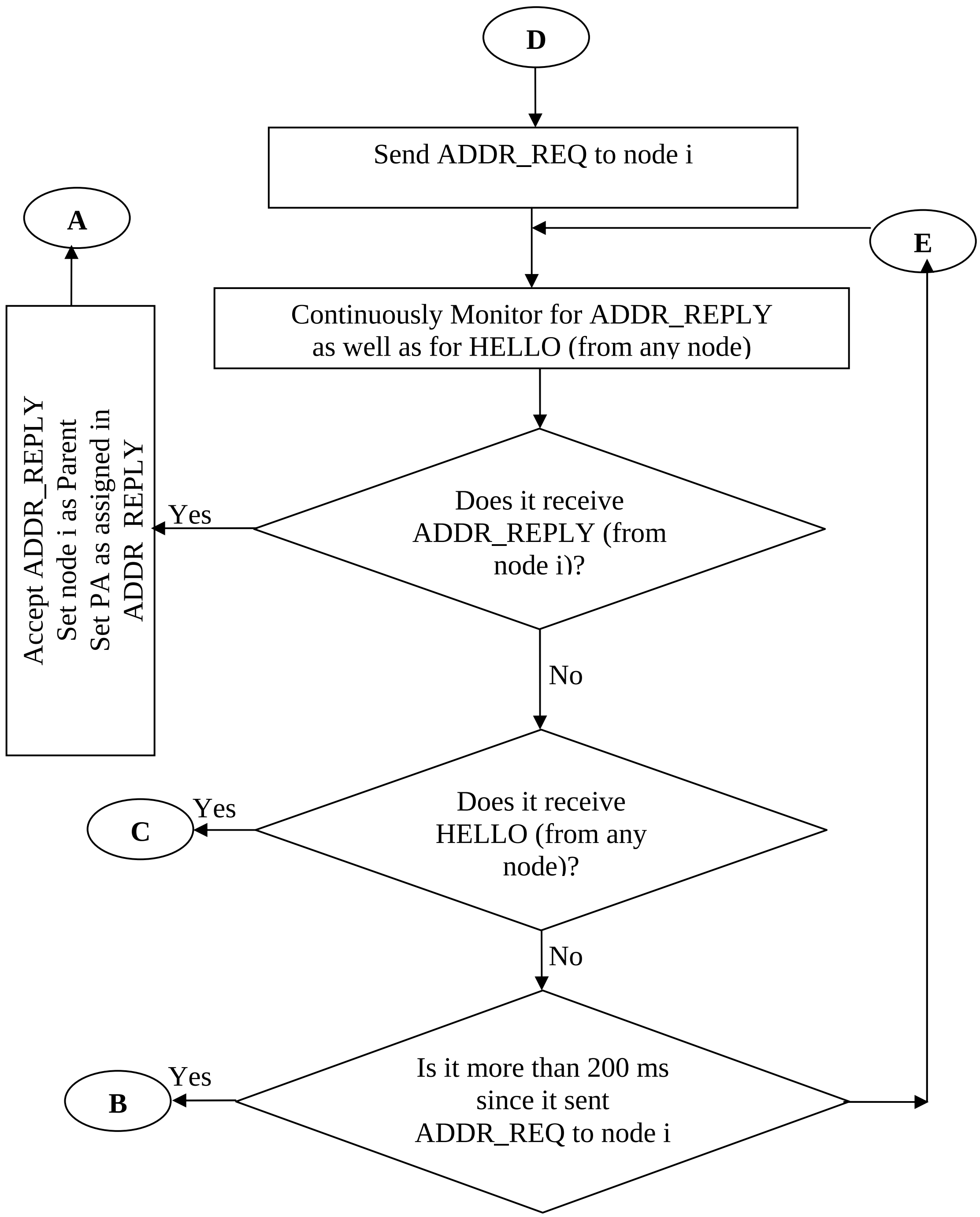

Fig. 3.10: Temporary Address Allocation in Mobile Party or Party (PA = Party Address i.e. Temporary Address) continued From Fig. 3.9.

The Fig. 3.11 shows the data packet transmission in party or mobile party. Packets will be dropped if parent is lost or moved out of range because while forwarding the packets to parent it does not take care whether the parent has moved or failed. In EMP we reduced this type of packet loss.

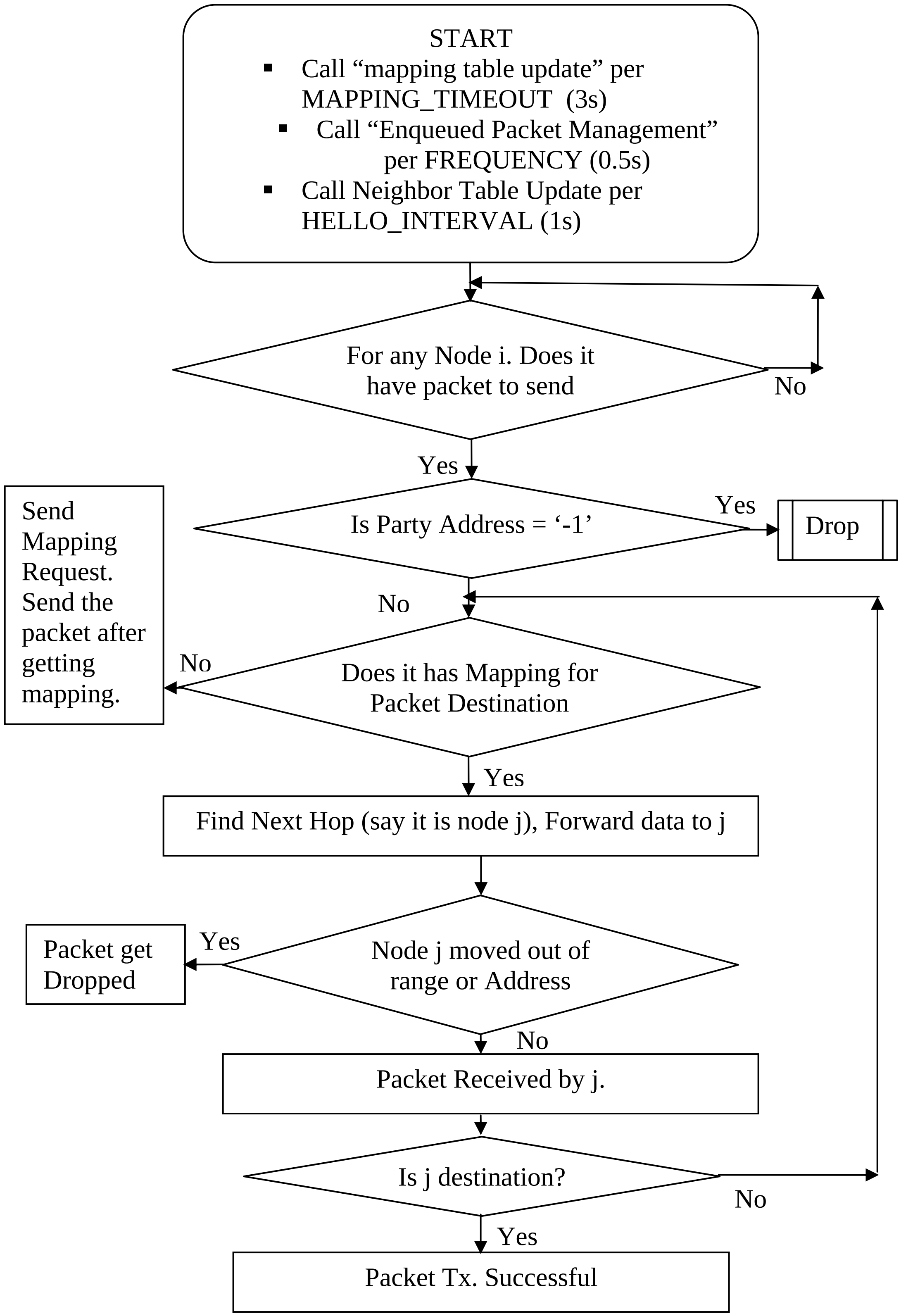

Fig. 3.11: Packet Transmission in Mobile party

EMP sets the status of parent lost = 1, when parent is either failed or moved out of range or changed its address. For the detection of parent lost, we implement layer 2 as well as layer 3 mechanisms. At layer 3 (network layer) mechanisms are

- If the child does not receive hello message from its parent since 3 HELLO Intervals, parent will be deleted from its neighbor table and parent lost flag will be set to 1.

- If child receives HELLO from its parent but temporary address of parent is changed, child will enter new address of parent in its neighbor table and set parent lost flag as 1.

At layer 2 the mechanism of parent lost detection is

- When MAC layer finds that the link between child and parent is lost, L2 trigger is evoked to set parent lost flag as 1.

When a child hear a HELLO from its parent and found that its parent has changed its address, then for the first try it will ask for new address to the same parent, after that to any node upon receiving HELLO from the later. In other cases of parent lost of a node, when it receives HELLO from any node, then it send address reconfiguration request to the later and upon getting new address, former will be child of later. In My proposed enhancement temporary address allocation is really a location based dynamic addressing.

The address allocation scheme of proposed enhanced party is as shown in Fig. 3.12 and Fig. 3.13. The data packet transmission in the enhanced party is as shown in the Fig. 3.14. If parent lost flag is set, all the packets for which next hop is parent are buffered. Upon getting new parent all packets in queue for which next hop is parent are forwarded.

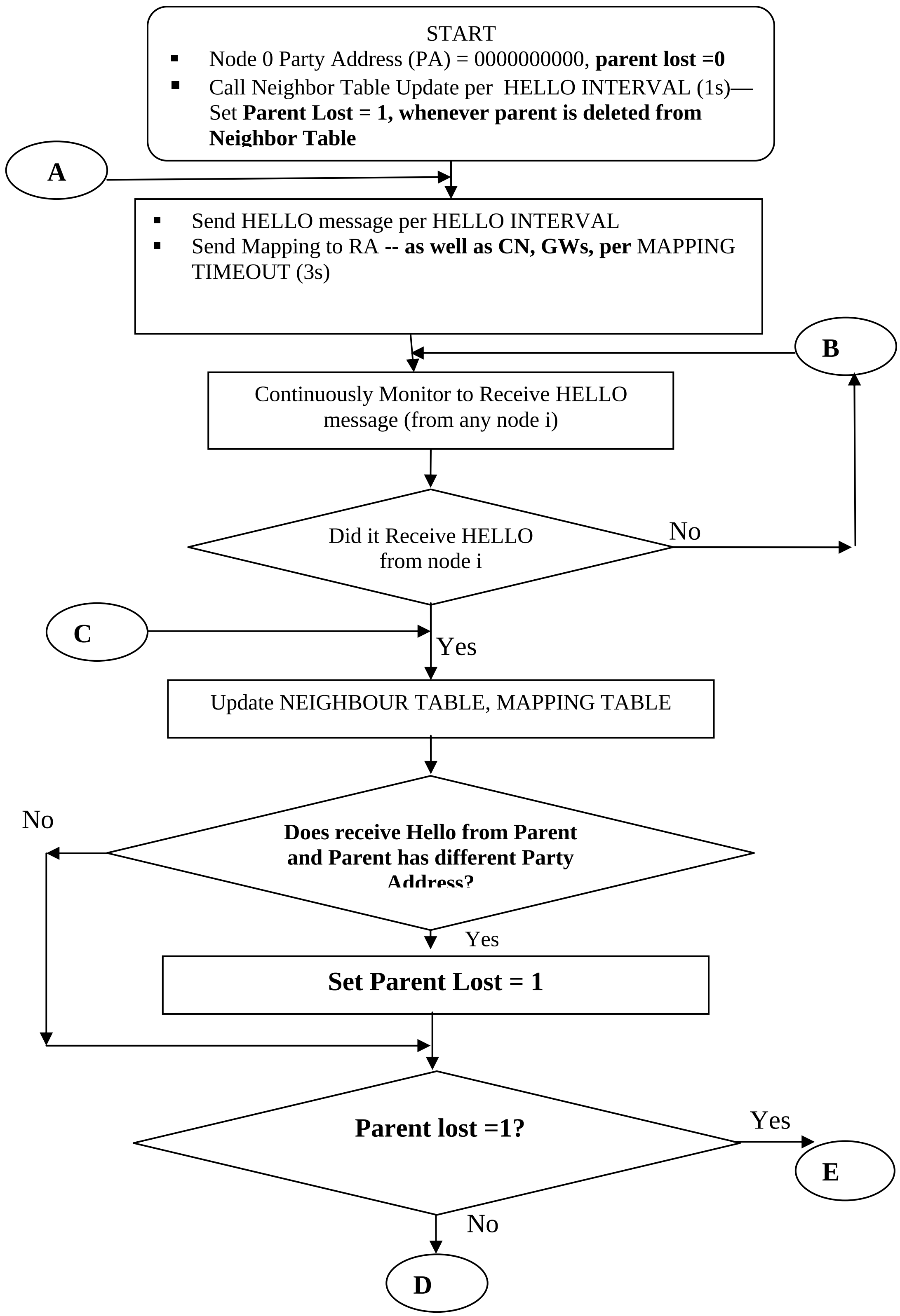

Fig. 3.12: Temporary Address Allocation in Proposed Enhanced Mobile Party

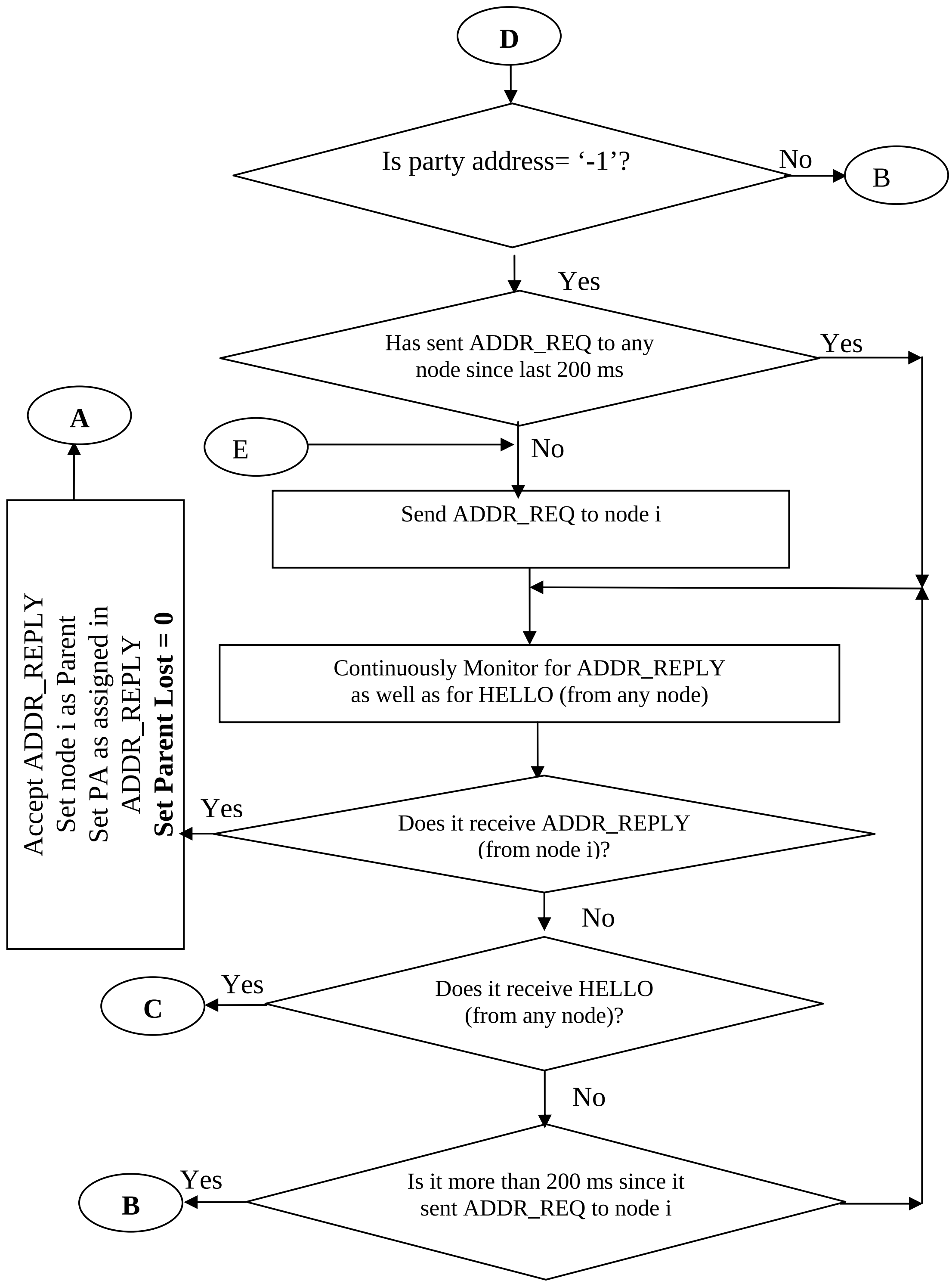

Fig. 3.13: Temporary Address Allocation in Proposed Enhanced Mobile Party continued from Fig. 3.12.

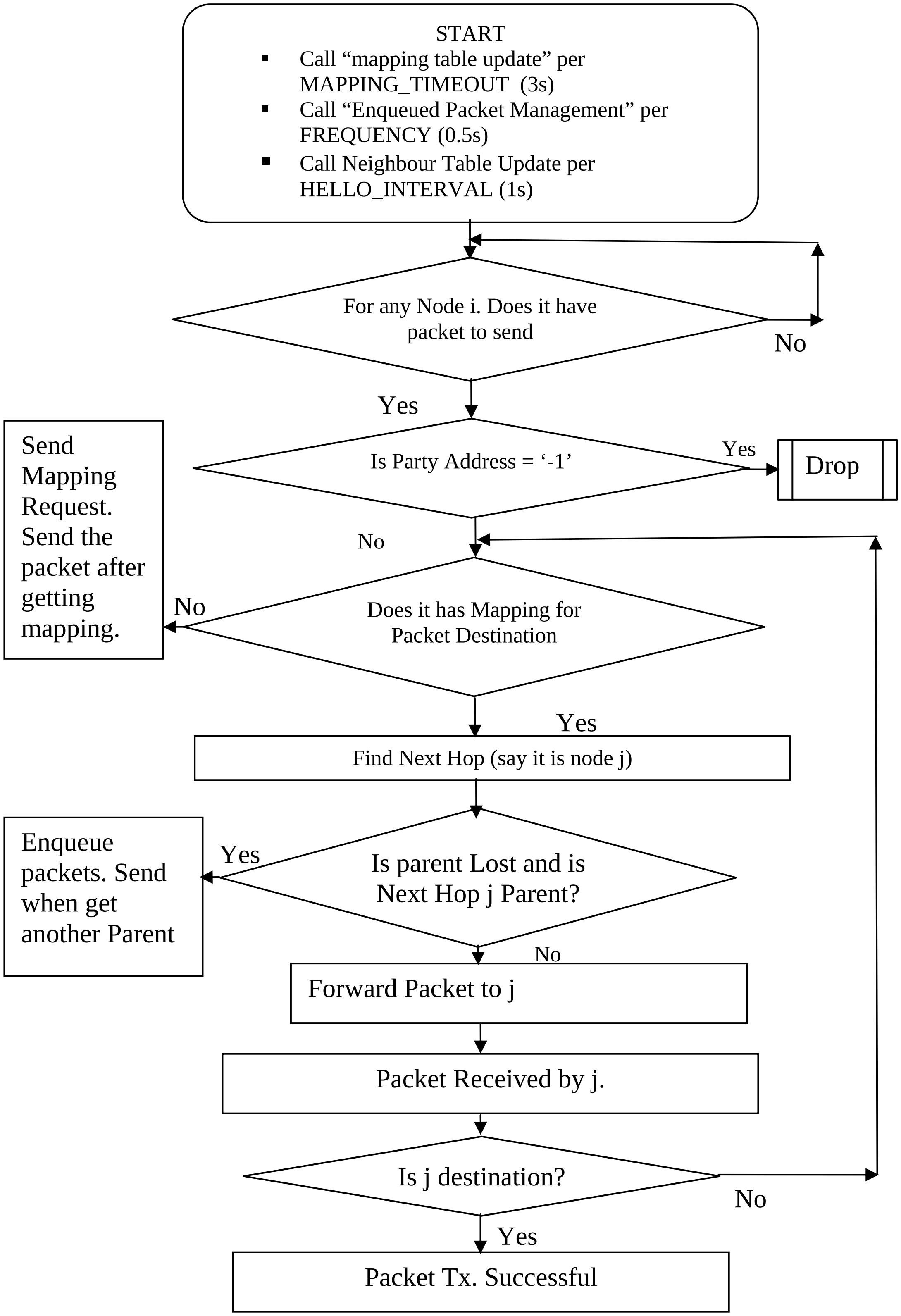

Fig. 3.14: Packet Transmission in Proposed Enhanced Mobile Party

3.4 Simulation variables and Performance Parameters

For the evaluation of proposed EMP, we used the Network Simulator -2 (NS-2). NS-2 is a free and open source network simulator widely used in research projects. Ns-2 is implemented in two programming languages: the core of the simulator is written in C++ and for configuring and running the simulations Tcl is used. The scope of the simulation is limited to analyze the performance of proposed EMP by network layer simulation.

3.4.1 Parameters of Evaluation

The main parameters of evaluation are Packet Delivery Ratio (PDR) or throughput, Signaling Overhead and end-to-end delay.

PDR is the ratio of the number of successfully received data packets at the destinations to the total number of packets sent in the network. Given total network load the throughput can be easily calculated by multiplying the network load by PDR. As one main purpose of routing protocol is to provide the route for packet transmission, PDR indicates one of the major performance parameters and it should be as high as possible. In network the useful traffic is data packet transmission, but for successful transmission of data signaling is needed although it is undesired traffic. So level of signaling traffic is one also one measure of performance. It should be lower is good routing protocols. It can be measured in different ways as number of packets per second or as percentage of total traffic in the network. The 3^{rd} important parameter of performance is end-to-end delay which is the time different between when a packet is sent in network by source node and when the same packet is received successfully at the destination. It includes propagation delay, congestion delay, delay in buffer, delay due to channel contention, etc. Some applications like voice services have strict constraint on end-to-end delay.

3.4.2 Simulation Parameters

Simulation results of Mobile Party and EMP protocol were compared with those of two routing protocols- a popular reactive routing protocol –AODV [22] and [24] and a popular proactive routing protocol –DSDV [23]. For all simulations, we used the standard values for the Lucent Wave LAN physical layer, and the IEEE 802.11 MAC layer standard with a transmission range of 250m.

In order to maintain a mostly connected topology the size of the simulation area was chosen to keep average node degree close to 28. For example square topology (X by Y) can be given as

$$X = Y = \sqrt{\frac{\pi * (250 * 250) * Number\ of\ Nodes}{Required\ Node\ Degree}} \quad \textbf{(0.5)}$$

For the traffic we use UDP/CBR flows, where we varied the rate and number of flows and kept the total offered load constant at 250 Kbit/s. For this we varied the Packet Interval (PI) depending on number of flows as given by

$$Packet\ Interval\ (PI) = \frac{Packet\ Size * 8}{1000 * Total\ Network\ Load\ in\ kbps} \quad \textbf{(0.6)}$$

The source and destination for all UDP flows are chosen randomly to make the simulation more realistic. For the motion of nodes we chose Random Way point (RWP) Model. *Random Way Point Model.* Random Waypoint (RWP) model is a commonly used model for mobility, in Ad Hoc networks. Each node moves along a zigzag line from one waypoint to the next. The waypoints are uniformly distributed over the given area. At the start of each leg a random velocity is drawn from the velocity distribution [0 to V_{max}, where V_{max} is maximum velocity specified explicitly in code by user].

In Mobile Party protocol we use decimal digits for the temporary addresses. The other Mobile Party's simulation parameters used in all simulations are show in Table 3.1.

Table 3.1: Default Values of Simulation Variables

Parameter	**Value**
Hello Message Rate	1sec.
Mapping Registration Refreshing Rate	3sec.
Party Signaling Packet Size	48 Bytes
Address Request Waiting Time	200ms
Mapping Entry Life Time	9sec.
Routing Table Entry (Neighbor) Life Time	4.5sec
Traffic Type	Constant Bit Rate (CBR)
Packet Size	625 Byte
Speed Variation	0m/s to 10 m/s (36 kmph)
Number Of Simulations For Each Variation	20 to 25 Times
Number Of Flows	10-500
Number Of Nodes	50-600
Transmission Range	250m

3.4.3 Simulation Scenarios

In this thesis my focus is on scalability of routing protocol while proposing the mobility management in WMN. So my proposed EMP must scale well when number of nodes or number of traffic flows increases. For the simulation we considered two scenarios – static and with node mobility. In both scenarios nodes are scattered randomly in unplanned way rather than a planned architecture forming an unplanned mesh architecture which is practically easier for deployment. But such architecture has some risk that network may have unusable low performance due to some users remains effectively disconnected [25]. We avoid this problem by increasing average node degree to 28.

3.5 Tools Used

During the thesis work following tools and software are used.

- NS 2 as simulator for all simulations
- C/C++ for writing code to implement proposed enhancement
- TCL/OTCL for simulation scripts
- Perl, and excel for analysis of log files
- Microsoft Word, Excel for the documentation and report writing

CHAPTER 4

SIMULATION RESULTS AND DISCUSSIONS

The simulation results for different scenarios are presented and analyzed in this chapter. The main parameters of evaluation are PDR (or throughput) and signaling overhead. In case of node mobility, end-to-end delay is also a major factor so it is also taken into consideration while comparing the proposed EMP with AODV, DSDV and mobile party which is the result of my first phase enhancement.

4.1 Scenario 1: static case

This scenario consists of only static nodes and better represents the backbone of mesh routers. Although mesh routers are generally placed manually, in worst case we can assume that they can be placed randomly. So, nodes are scattered randomly in a rectangular topology maintaining the average node degree of 28. We study the effect of increasing number of nodes and traffic flows on throughput and signaling overhead to ensure that my proposed EMP scale well compared to other existing routing protocols (proactive AODV and reactive DSDV). To study the effect of traffic flow counts, we varied the traffic flows from 10 to 500 keeping the number of nodes 200. Similarly during the variation of number of nodes, the number of flows is kept fixed at 100 UDP/CBR flows. The duration of simulations was set to 200 seconds, where the first 20 seconds are free of data traffic, allowing the initial address allocation to take place and for the network to organize itself.

4.1.1 Signaling Overhead:

Fig. 4.1 shows the effect of number of active flows on the average routing signaling overhead, keeping the network size fixed at 200 nodes. In the following experiments we use 10 decimal digits for Mobile Party temporary address and in each simulation run we make sure that each node in the network takes a temporary address. Here we compare Mobile Party signaling overhead with that of AODV, and DSDV. We normalized the packet size for each protocol to that of AODV. The results show that Mobile party protocol has a lower overhead compared to the other routing protocols. AODV overhead has an approximately linear relationship with flow count, because for each new traffic flow, AODV broadcast the route request message to get the fresh or new route to the destination creating a huge signaling. The overhead of DSDV is unaffected by this parameter due to its proactive route establishment approach. Although Mobile Party is considered as a reactive routing protocol, its overhead does not affected much by the flow count; this is due to the fact that in party

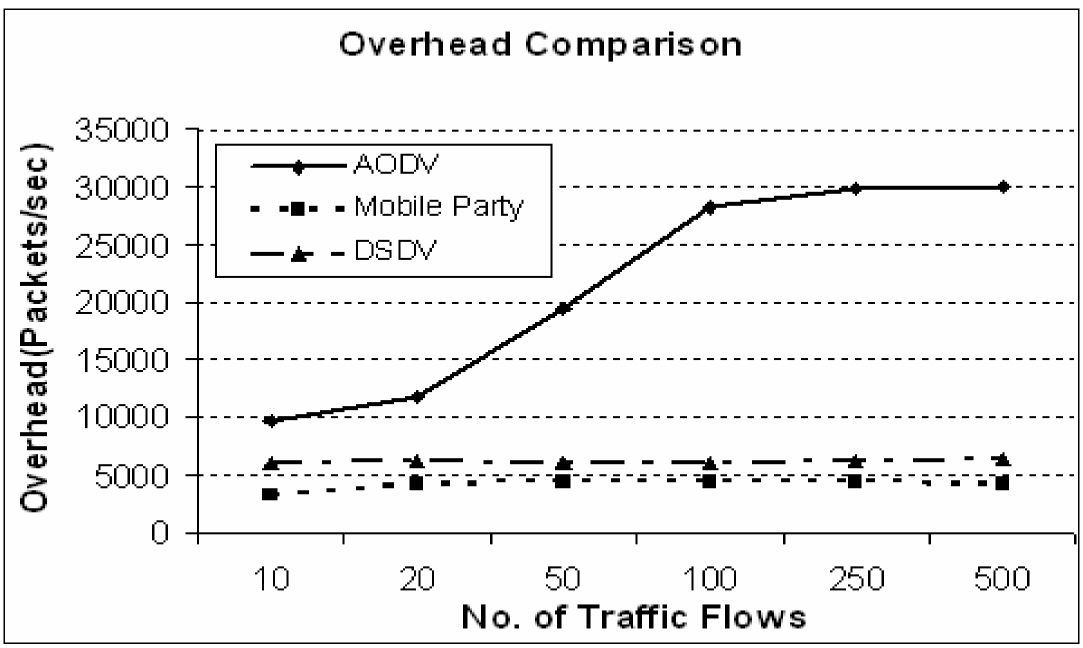

Fig. 4.1 : Overhead vs. Flow Count: UDP/CBR flows, 200 Nodes.

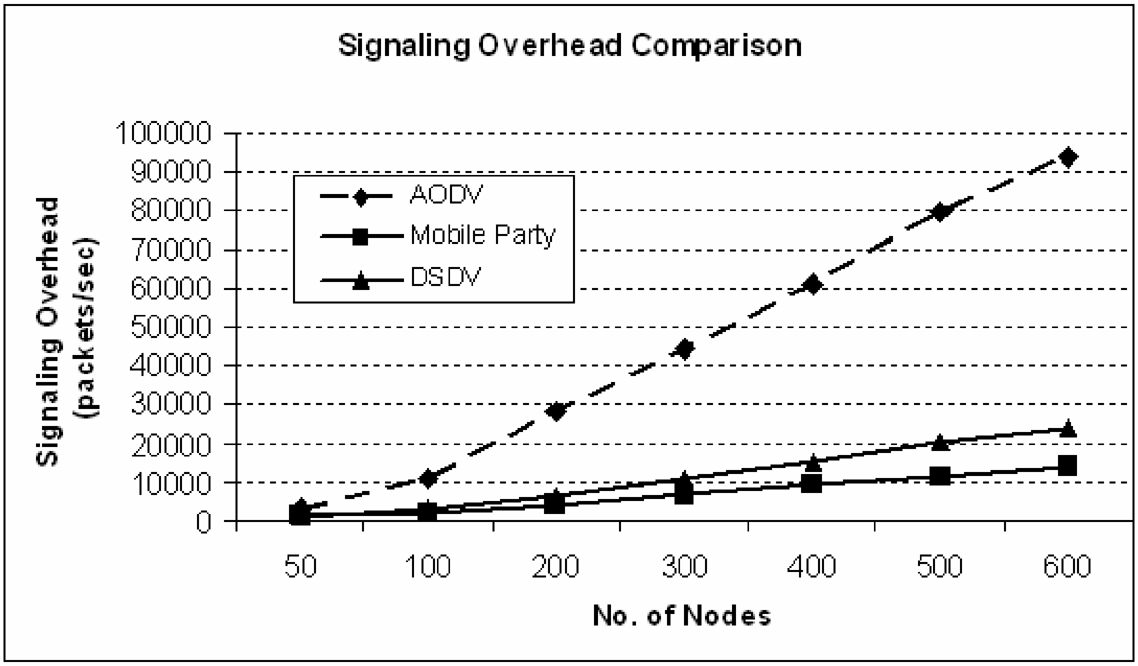

Fig. 4.2: Overhead vs. Network Size: 100 UDP/CBR flows.

Route is determined by temporary address of destination and overhead is needed just to get the temporary address of destination by mapping lookup procedure where no flooding is needed. This mapping lookup is needed only if there is no temporary address of destination already in the source's mapping table. With the variation of number of active traffic flows Mobile party shows the best performance.

Fig. 4.2 shows the effect of network size on the routing signaling overhead, maintaining the number of flows equal to 100. We can see that Party maintains a relatively low overhead compared to the other protocols. We can observe also that its overhead grows linearly by a low rate with the network size. This slight increase in signaling overhead in mobile party is due to the fact that there are periodic hello messages and temporary Id registration messages which depend on the number of nodes in the networks.

4.1.2 Throughput:

For a protocol to be scalable it is necessary that the average throughput of the network should remain good even when the size of network increases or when the number of active flows increases. To study the effect of number of active flows on the throughput, we run the simulation, using a varying number of UDP/CBR flows, keeping the number of nodes fixed at 200 and also the total load fixed as 250 kbps. From Fig. 4.3 it is clear that DSDV and Mobile Party remain largely unaffected as the number of flows increases. But in case of AODV, as the number of flows increases, its linearly increasing overhead slows down its initial performance advantage. A slight decrease in throughput is expected for all protocols, as inter-flow interference will increase with increasing number of flows.

To analyze the idea of protocol scalability with respect to network size, we studied the throughput achieved under varying network size, keeping the number of active flows fixed at 100. When connection end-points are chosen randomly and uniformly, it is natural for any protocol to see reduced throughput with increasing network size, due to increasing average path length, and increasing routing protocol overhead. As seen in Fig. 4.4, Mobile Party throughput is higher than that for the other protocols, due to its small overhead, thus it seems to be suitable for large networks.

The comparison results of overhead and throughput emphasizes the superiority of scalability of mobile Party protocol for static mesh backbone and hence it seems better suited for WMNs. In WMNs the mesh routers have low or no mobility, so this result shows that Mobile party protocol is well suited for backbone WMNs. But in some cases like in military operation, disaster rescue, etc mesh routers are mobile. More over mesh clients have mobility in most of the cases. Mobile Party protocol must perform better in these cases also. For these cases Mobile party protocol is needed to be enhanced.

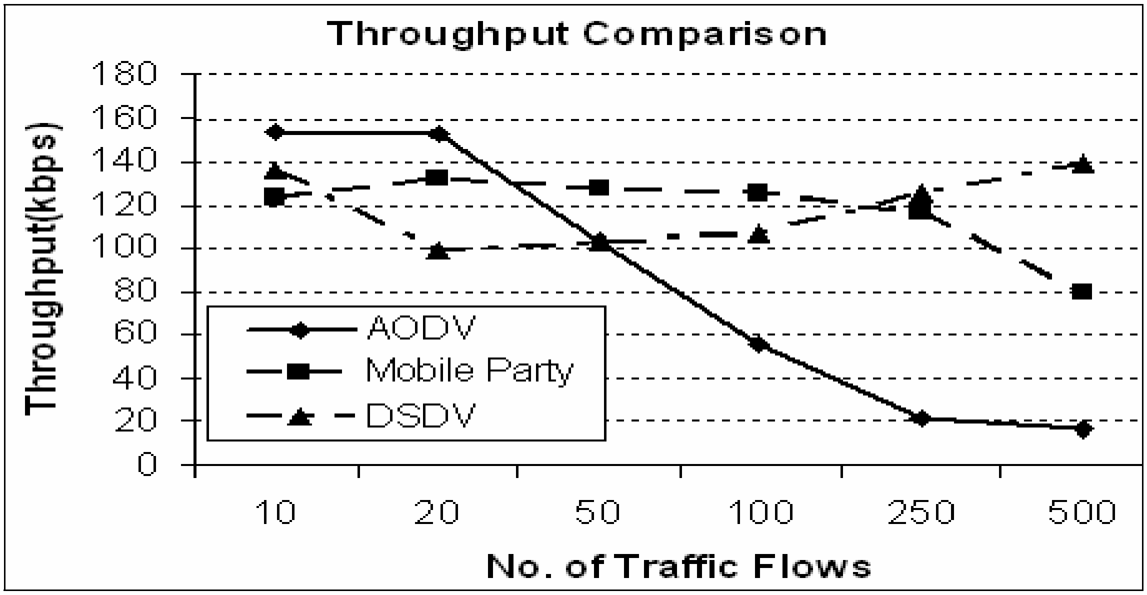

Fig. 4.3: Throughput vs. Flow Count: UDP/CBR flows, 200 Nodes.

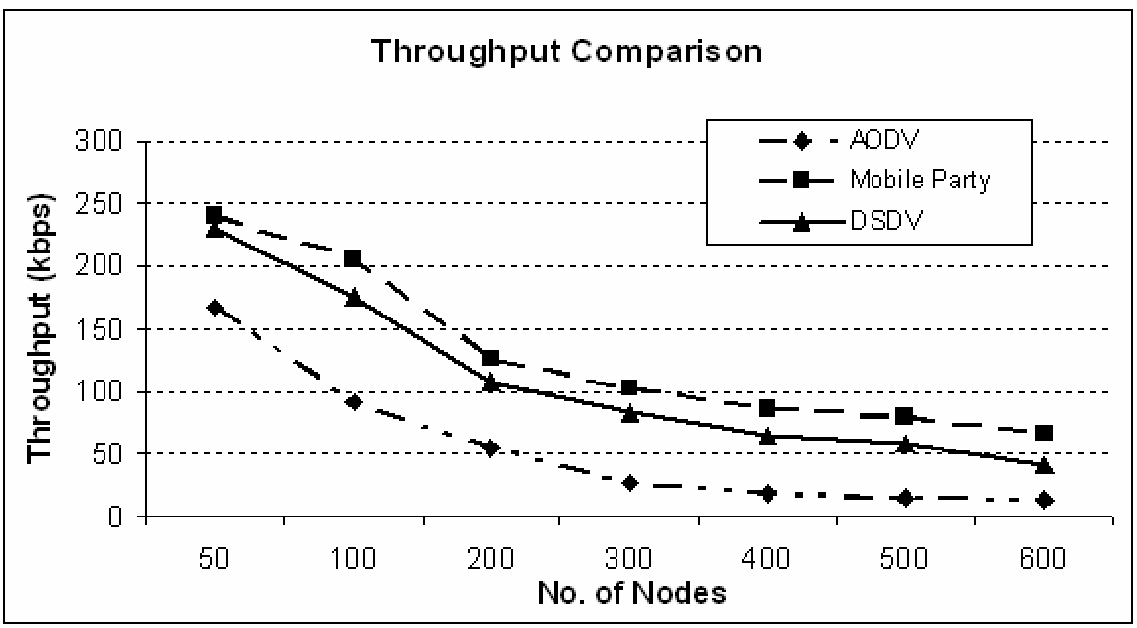

Fig. 4.4: Throughput vs. Network Size: 100 UDP/CBR flows.

4.2 Simulation Scenario 2: with Node Mobility

The proposed Enhanced Mobile Party (EMP) is to solve the problem of dynamic and instant location based addressing in mobile party in a case when a node loses its parent or its parent's temporary address changes. This situation arises when child or parent moves away from each other, parent node suddenly fails, parent changes its own temporary address etc. In fixed mesh backbone such situations are not more likely. The situation will more frequently occur in mesh-client or infrastructure mesh backbone with ad-hoc topology. So to better evaluate my enhancement we chose the worst case scenario of ad-hoc topology in which fifty nodes are scattered randomly in an area of 590m * 590m. Randomly chosen 70% of nodes are moving without any pause. Motion pattern is generated using random way point model. Maximum speed is varied from 0m/s to 10m/s (36 kmph). Number of simultaneous traffic-flows is varied from 10 to 50 keeping total network load fixed at 250 kbps. The source-destination for each traffic flow is chosen randomly. For the traffic we use UDP/CBR flows. The duration of NS2 simulation was set to 80 sec while traffic starts from 20 sec. The other parameters are as shown in Table 3.1.

The performance parameters considered for performance evaluation include Packet Delivery Ratio (PDR), end-to-end delay, Signaling overhead as the percentage of total network traffic and signaling packets per second.

4.2.1 Analysis of Packet delivery ratio (PDR) and Signaling Overhead for enhanced mobile party

In this case, the routing protocol used is EMP proposed in this thesis. The variation of PDR and signaling overhead with number of traffic flows, keeping the total load fixed as 250 kbps and maximum speed fixed as 5 m/s, is shown in Fig. 4.5. The variation for 95% Confidence Interval (CI) is also shown in the Fig. The variation of less than 2% from mean for 95% CI validates the good reliability of simulation results.

The general trend found is that PDR remains constant (around 97.15 %) for low number of traffic flows (up to 20). After that it decreases slightly with increase in number of flows and reaches up to 95.61% for 50 flows. The expected reason for slight decrease in PDR is the increase in inter-flow interference with the increase in number of flows, because for 50 flows in a network of 50 nodes, on average each node, is receiving as well as transmitting one traffic flow all the time, along with receiving and generating periodic and non-periodic signaling messages. Another reason for inter-flow interference might be the fact that in My approach source and destination of each traffic flow will exchange the mapping update to each other per mapping timeout until the period of transmission; creating extra 2 * (number of flows) periodic mapping update flows.

The PDR of higher than 95% in the case when all the nodes are receiving and transmitting data packets can be considered as very good value.

Signaling traffic as a percentage of total traffic (signaling traffic + data traffic) is almost constant with slight increase with the increase in number of flows. The constant amount of signaling overhead is generated by periodic signaling messages (hello message, temporary Id registration, etc). The signaling due to mapping request for destination's temporary Id and periodic update exchange between source and destination as described above depends on the number of traffic flows creating slight increase in signaling traffic.

The signaling traffic is almost independent of number of flows (about 1% variation for the increase of traffic flows from 10 to 50). The data traffic shown in Fig. 4.1 is just 100 minus signaling traffic. So its nature is obviously same as signaling traffic curve.

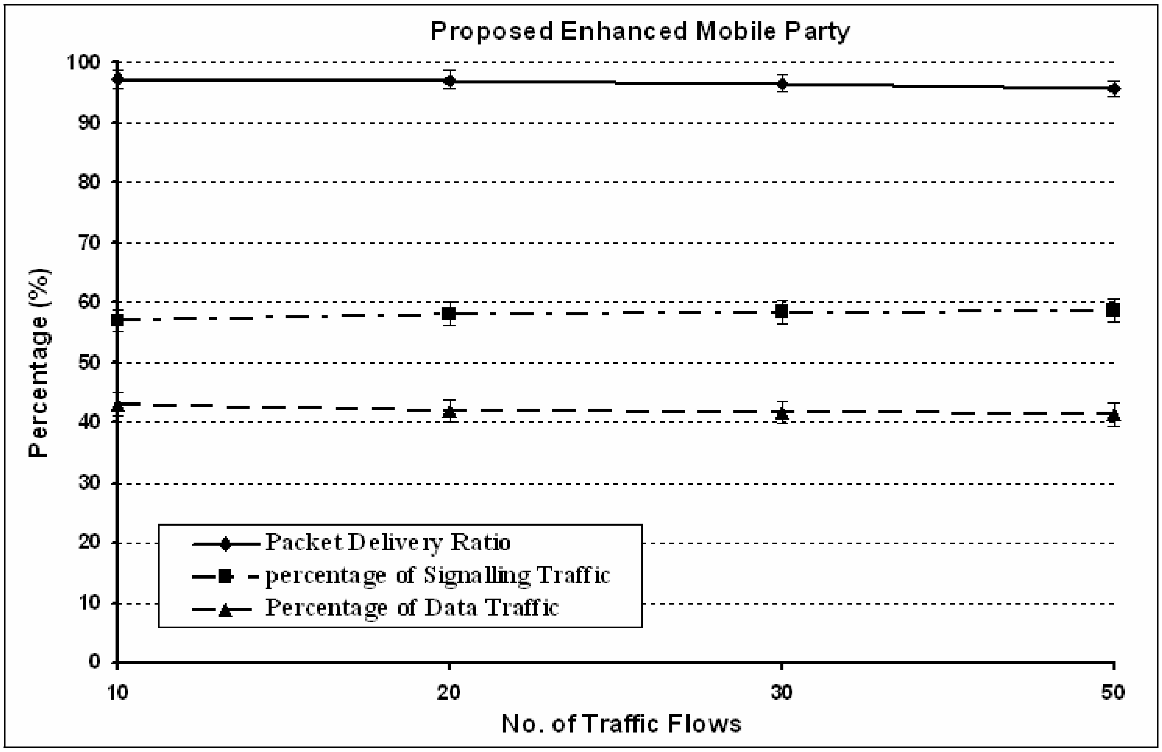

Fig. 4.5: PDR and Signaling Overhead versus No. of Traffic Flows for Proposed EMP

The variation of PDR and signaling with the speed of nodes keeping traffic flows at 30 flows is shown in Fig. 4.6

The PDR is constant and above 96.5% for the speed of up to 5m/s (18km/hr). But it decreases when the speed of node reaches around 10 m/s (36 km/hr) falling up to 92%. At higher speed the packet loss increases as the nodes start to change the address more frequently causing more and more data packets to put in queue. Most of the losses were found to be due to MAC layer dropping and IFQ dropping during simulations. Actually, 802.11 MAC is not well suitable for WMN, particularly when node density is high [6]. The IFQ dropping was found to increase with the increase in speed which is obvious as more packets have to be kept in queue during parent lost and address transition period.

In My addressing approach, the effect of motion of node, not only depends on speed but also on position (level) of node in address tree (Fig. 2.4). If some higher level of node (nodes towards root level) moves it affect a large part of network causing more packet drops as well as more signaling overhead, while motion of nodes towards leaves create less effect to network and causes less packet loss as well as less signaling overhead.

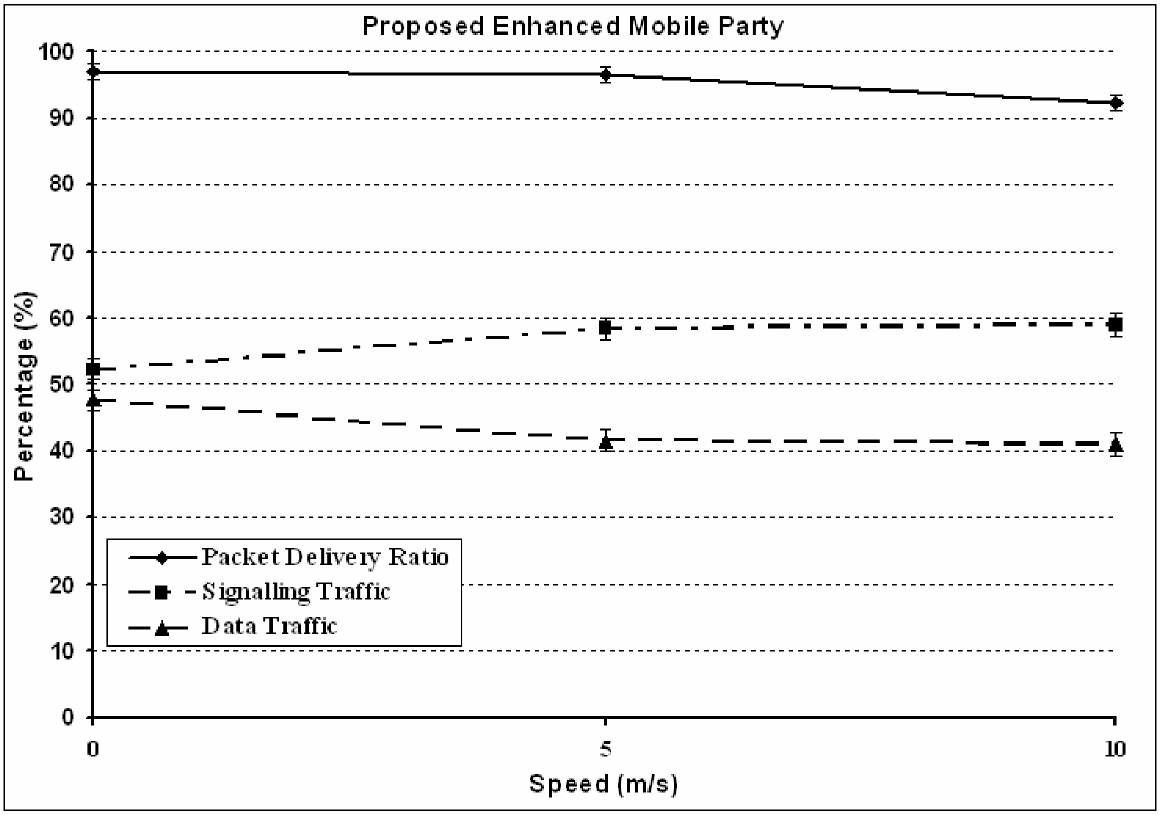

Fig. 4.6: PDR and Signaling Overhead versus Speed of Nodes for Proposed EMP

The signaling overhead increases with the increase in speed which is obviously due to increase in signaling for address reallocation. The signaling overhead increases by 10 % for the speed variation from 0 m/s to 10 m/s (36 kmph). But it increases by less than 3% for speed up to 5 m/s (18 kmph). With the increase in speed more and more child-parent will move out of range requiring large number of address reallocation. Each address reallocation generates extra signaling as "Address request", "Address reply", mapping update to RA node and Correspondent Nodes (CNs).

From the above analysis, it is clear that my proposed EMP performs very good up to the speed of around 5 m/s (18 kmph) regarding PDR as well as increment in signaling overhead. It should be noted that for mesh network the maximum speed of interest is less than 5 m/s. So for the mobility scenario of mesh network my proposed EMP can guarantee a PDR of more than 96.5% with the increase of signaling less than 3% compared to static case of Mobile Party.

4.2.2 Analysis of End-to-end Delay for Proposed EMP:

The variation of end-to-end delay with number of traffic flows keeping maximum speed fixed as 5 m/s is shown in Fig. 4.7.

The end-to-end delay is constant for lower no of traffic flows but increases with no of flows beyond 20 flows. The average value of end-to-end delay is high, although most of the time its value was found to be low during the simulations. We can see from the graph that median value of end-to-end delay is quite low (around 0.042 sec). The higher average value is due to the fact that some sample values of simulation are quite high (around 0.7 sec to 0.9 sec) compared to most of the sample values (which are around 0.01 sec to 0.045 sec).

The reason of quite high value of end to end delay in some cases can be described as follows. In My proposed EMP, data packets with next hop as parent is kept in queue in case of parent loss and will be forwarded only after getting new address (i.e. new parent). There might be the case at some instant that a node will loose the parent and no one of its neighbors has address space left to allocate to it instantly. As a result the node will get address after some delay, not sure after what period (although the probability of such case is very low). As the packet traverses multiple hops before reaching the destination, there is some chance that same packet can suffer from above worst case more than one time, resulting in very high end-to-end delay. This situation increases with increase in traffic flow as well as speed, resulting in high average end-to-end delay.

In My simulation, we are choosing source-destination pair randomly and 70% of nodes are moving. For different traffic flows, there may be different scenarios like source-destination both are static; source-destination both are moving; one of them, either source or destination, is moving; intermediate nodes may be static or moving; etc. These situations decide the end-to-end delay. That’s why end-to-end delay is found to be varying.

The variation of end-to-end delay with speed of nodes, keeping traffic flow count fixed as 30 flows is shown in Fig. 4.8.

The delay increases sharply from static case to mobile case which is indicated by the higher slope of curve from speed of 0 m/s to 5 m/s. After that end-to-end delay increases with increase in speed but with smaller slope. The high increase in delay at transition from static case to mobile case is due to the fact that in mobile case we introduce the mechanism to put the packets in queue in the case of parent lost.

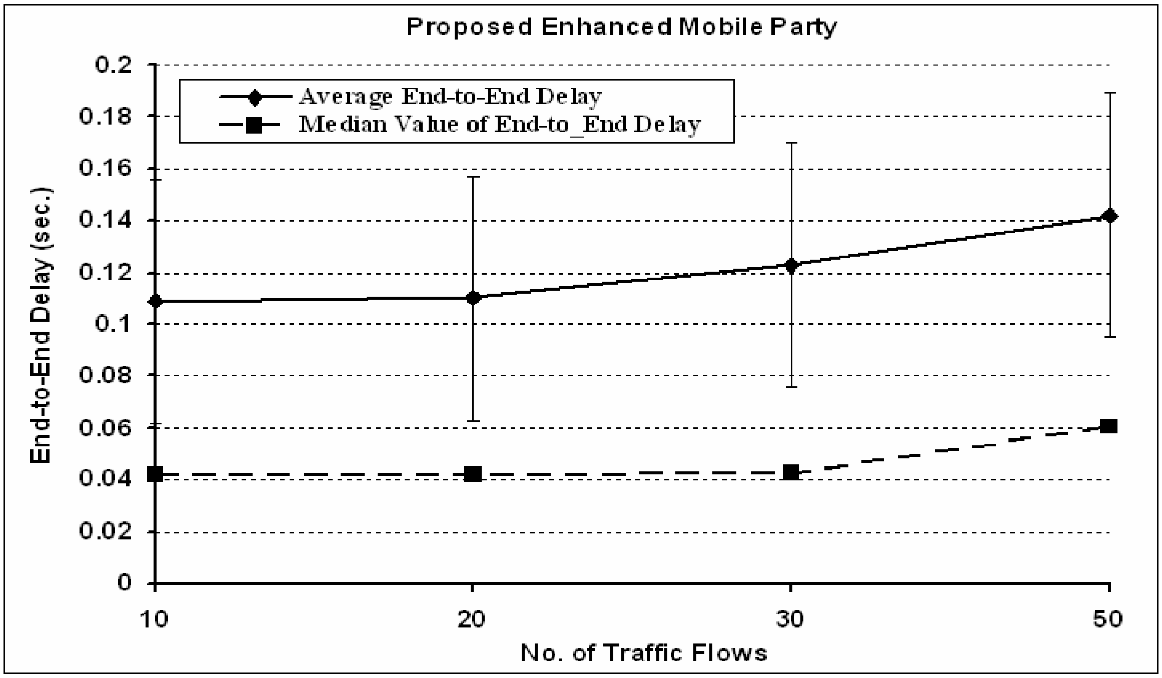

Fig. 4.7: End-to-End Delay versus No. of Traffic Flows for Proposed EMP

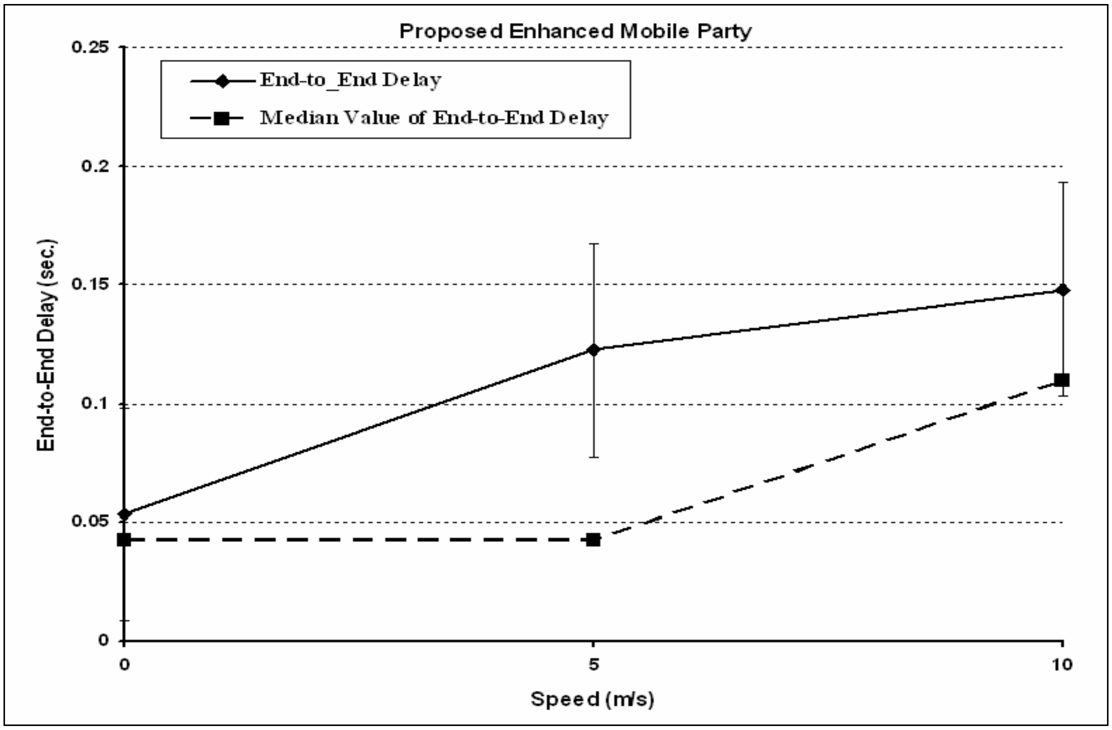

Fig. 4.8: End-to-End Delay versus Speed of Nodes for Proposed EMP

It should be noted that the average end-to-end delay can be reduced by allowing intermediate node to drop the packets in queue after some time in case of parent loss, but it will increase the packet loss slightly. We have to compromise between delay and loss.

4.2.3 Comparative analysis of PDR for different routing protocols

The comparative graphs showing the PDR for four routing protocols (proposed EMP, AODV, mobile party and DSDV) are shown in Fig. 4.9 and Fig. 4.10. The range for 95% confidence interval is also depicted in the graph to validate the reliability of simulation results.

Fig. 4.9 compares the PDR performance of these four protocols for different number of traffic flows, keeping maximum speed fixed at 5 m/s. PDR is highest for AODV; proposed EMP being nearer to AODV. But the PDR for mobile party is lowest; DSDV is close to mobile party being slightly better than it. The reason is that DSDV is a proactive protocol and not well suited for mobile case as it requires large pause time for routing update to converge. The cause of high packet loss in Mobile party is that it has no mechanism of tracking the mobility of node (i.e. although routing is based on location based temporary address, there is no mechanism of reallocation of this temporary address based on changed location dynamically).

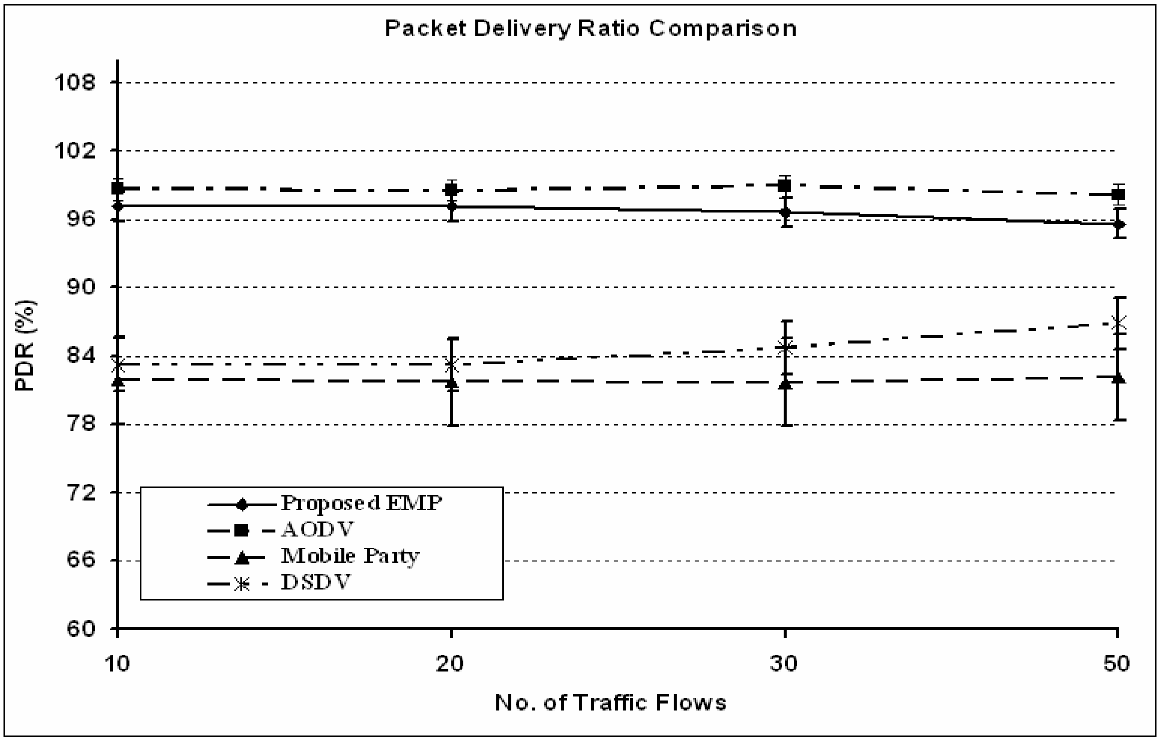

Fig. 4.9: Comparison of PDR versus No. of Traffic Flows with Different Routing Protocols

After the proposed enhancement to mobile party, an average improvement of about 15% can be seen in PDR performance which is remarkable.

Fig. 4.10 shows the variation of PDR of different protocols with respect to speed of nodes keeping number of flows fixed at 30 flows. For static case, all four routing protocols have almost similar performance converging around 97-98% PDR, but diverging more and more with increase in speed. The general trend is decrease in PDR with increase in speed. AODV has best performance with higher speed while proposed EMP being close to it. DSDV and mobile party have worse performance. The higher loss in DSDV is due to the fact that routing table takes large time to converge and packets are lost mainly due to stale routing entries when nodes are mobile without large pause time.

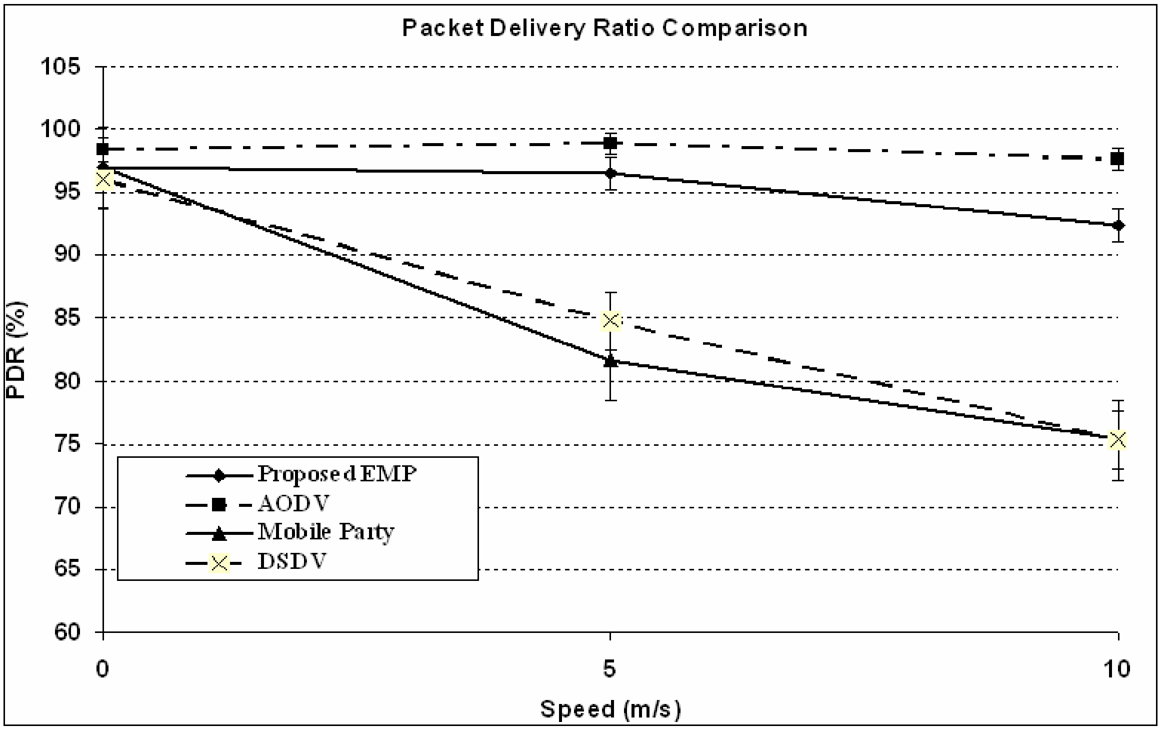

Fig. 4.10: Comparison of PDR versus Speed of Nodes with Different Routing Protocols

4.2.4 Comparative Analysis of Signaling Overhead for Different Routing Protocols

Fig. 4.11, Fig. 4.12, Fig. 4.13 and Fig. 4.14 show the comparative signaling overhead performance of four routing protocols under consideration with the variation of number of traffic flows and speed of the node.

From Fig. 4.11, it is clear that AODV generates the highest number of signaling packets per second and it increases almost linearly with the number of traffic flows. DSDV has the lowest value; Mobile Party and Proposed EMP being in between. In the later three, the signaling packets remains almost same, only slight increase is noted. In AODV route discovery (includes broadcasting route request, generating route reply) starts for each new destination and route error message is likely to sent to more number of nodes if the number of flows is higher. This is the cause for linearly increase in signaling in AODV.

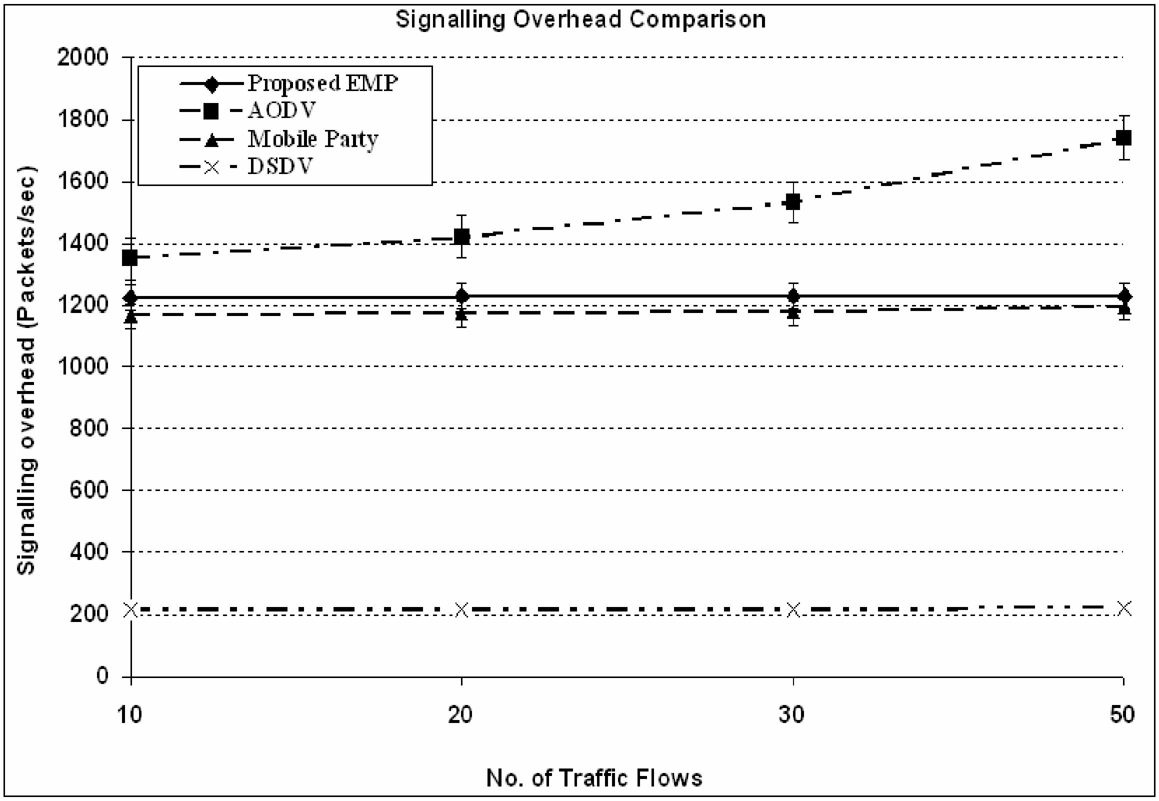

Fig. 4.11: Comparison of Signaling Overhead versus No. of Traffic Flows with Different Routing Protocols

As shown in Fig. 4.12, the signaling packets per second, increases almost linearly with speed of nodes in AODV, due to route error message and new route discovery process overhead generated in case of any route failure. In case of proposed EMP, the signaling packets per second increases first and soon gets saturated. The slight increase in signaling packets at beginning is due to address reconfiguration, new address registration and mapping updates.

In DSDV the number of signaling packets increase very slightly with speed and it apparently seems to have least signaling overhead. But this is not the fact. In DSDV, the number of incremental update increases only slightly, but the size of incremental update packet increases linearly with the speed of nodes and in worst case most of the incremental updates will be replaced by the full dump updates, in which all entries of routing table is transmitted. This is because in DSDV when the size of the incremental update packet reaches a limit, it is replaced by full dump update. That's why although the number of signaling packets generated is less in DSDV, the overall signaling overhead traffic is higher than Mobile party and Proposed EMP as shown in Fig. 4.13 and Fig. 4.14.

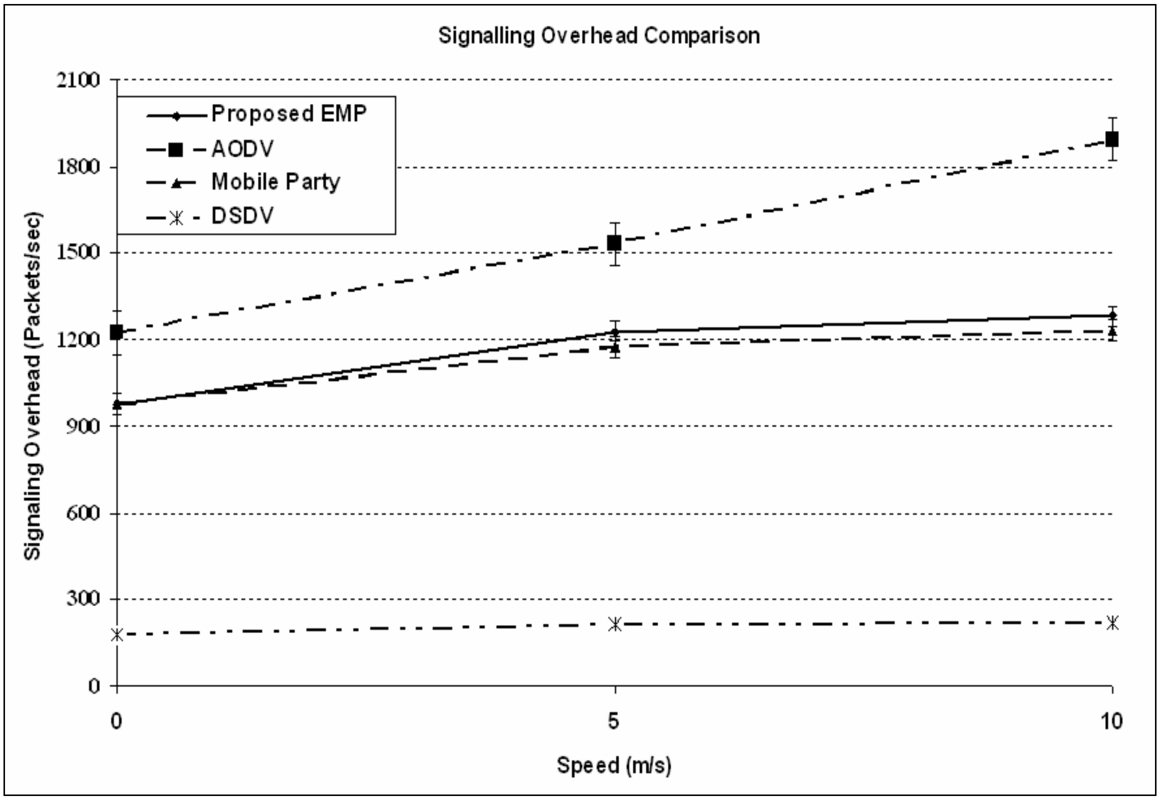

Fig. 4.12: Comparison of Signaling Overhead versus Speed of Nodes with Different Routing Protocols

Fig. 4.13 and Fig. 4.14 compares the signaling overhead as percentage of total traffic (signaling traffic + data traffic). AODV is worst with linear increase with speed as well as with number of traffic flows; proposed EMP is best; Mobile Party and DSDV being in between. Although number of signaling packets generated is slightly more, proposed EMP wins mobile party because in Mobile party more packets are lost after traveling few hops creating less data traffic in network in terms of byte-hops. So as Data traffic amount decreases but signaling amount remains same, in terms of percentage of total traffic, signaling traffic in mobile party is more than that of EMP. The proposed EMP seems best suited in terms of signaling overhead and can maintain scalability in large wireless mesh networks.

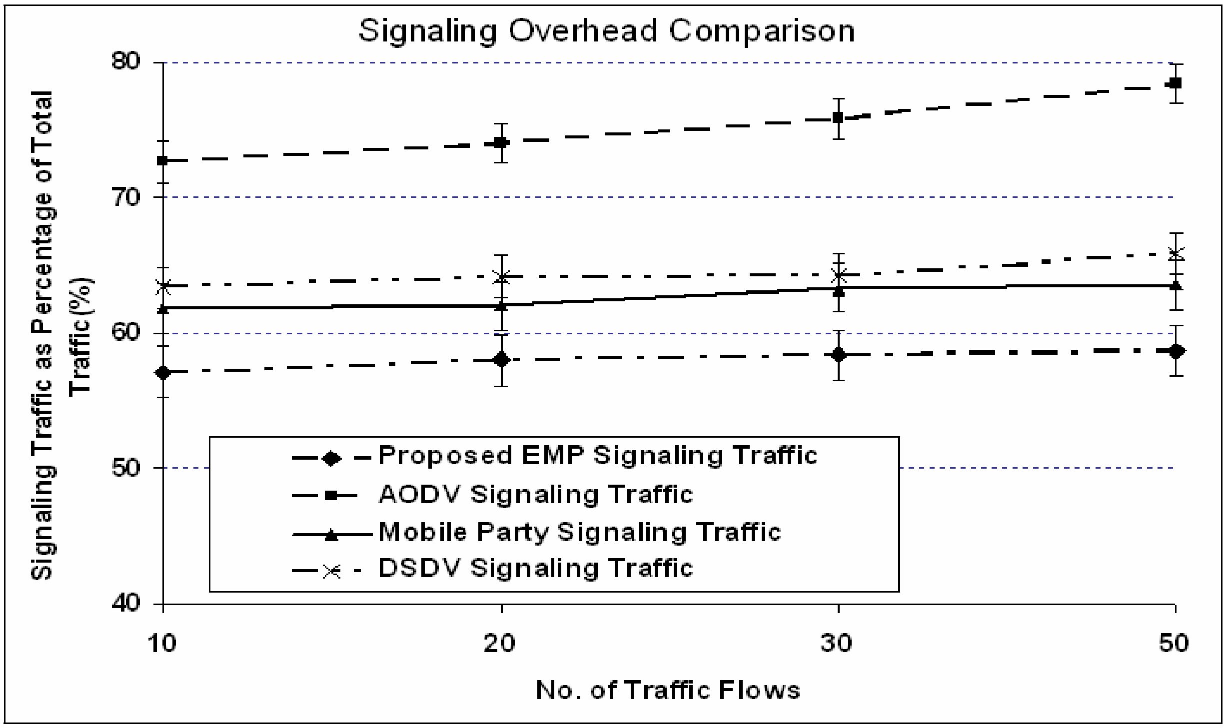

Fig. 4.13: Comparison of Signaling Overhead versus No. of Traffic Flows with Different Routing Protocols

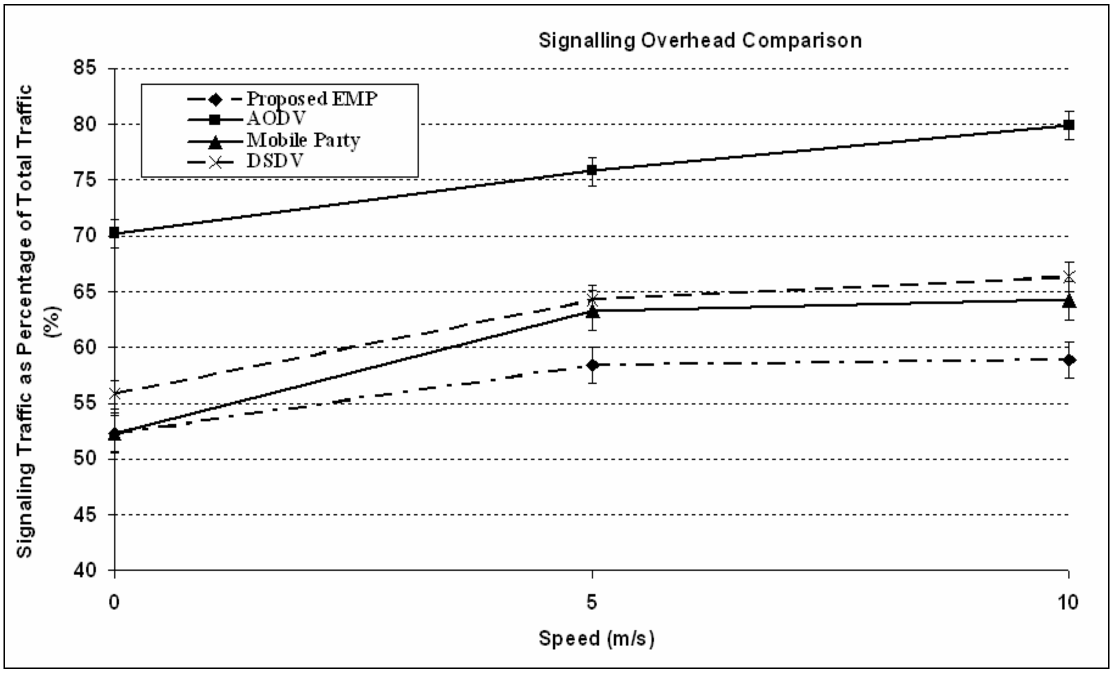

Fig. 4.14: Comparison of Signaling Overhead versus Speed of Nodes with Different Routing Protocols

4.2.5 Comparative Analysis of End-to-End Delay

The graphs showing the comparative End-to-End delay with respect to number of traffic flows and speed of nodes are respectively shown in Fig. 4.15 and Fig. 4.16.

With respect to no. of traffic flows, the general trend is that end-to-end delay increases with the number of flows as inter-flow interference is likely to increase. Proposed EMP and AODV has worse value because packets are kept in queue in case of parent lost and no mapping entry for destination in EMP and in case of no fresh and active route in AODV. DSDV, being proactive protocol, has the best performance as the route is generally available (although it may be the stale entry). Mobile party has less delay as packets are kept in queue only in case of having no mapping of destination.

The trend of end-to-end delay is found to be the same as described in above paragraph with respect to speed of nodes. DSDV is best; Proposed EMP and AODV are worse; mobile party being in between. For lower speed EMP wins AODV, but as speed increases the AODV has less delay than EMP. The reason is that when a node moves from transmission range of one node to another node, AODV just need to start new route discovery for that node. But in case of EMP, the node should first get the new address; register the address to RA; then only it can be tracked. That's why at higher speed when such address reallocation is higher, the end-to-end delay is higher in EMP.

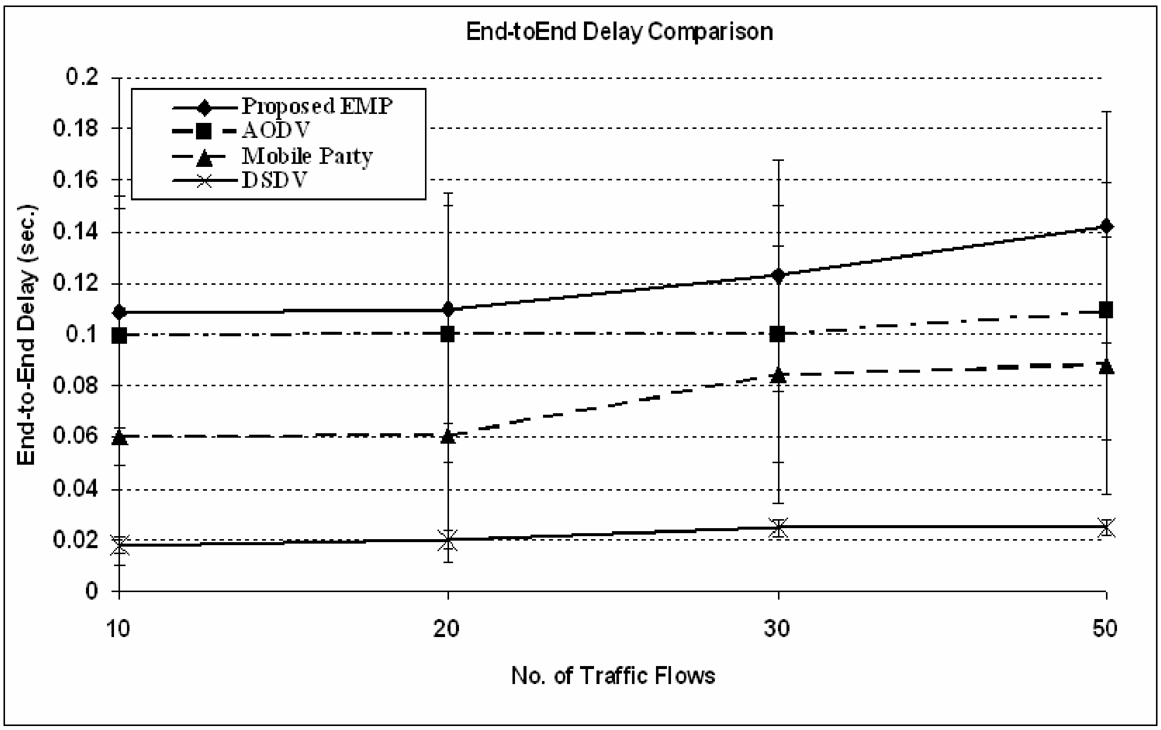

Fig. 4.15: Comparison of End-to-End Delay versus No. of Traffic Flows with Different Routing Protocols

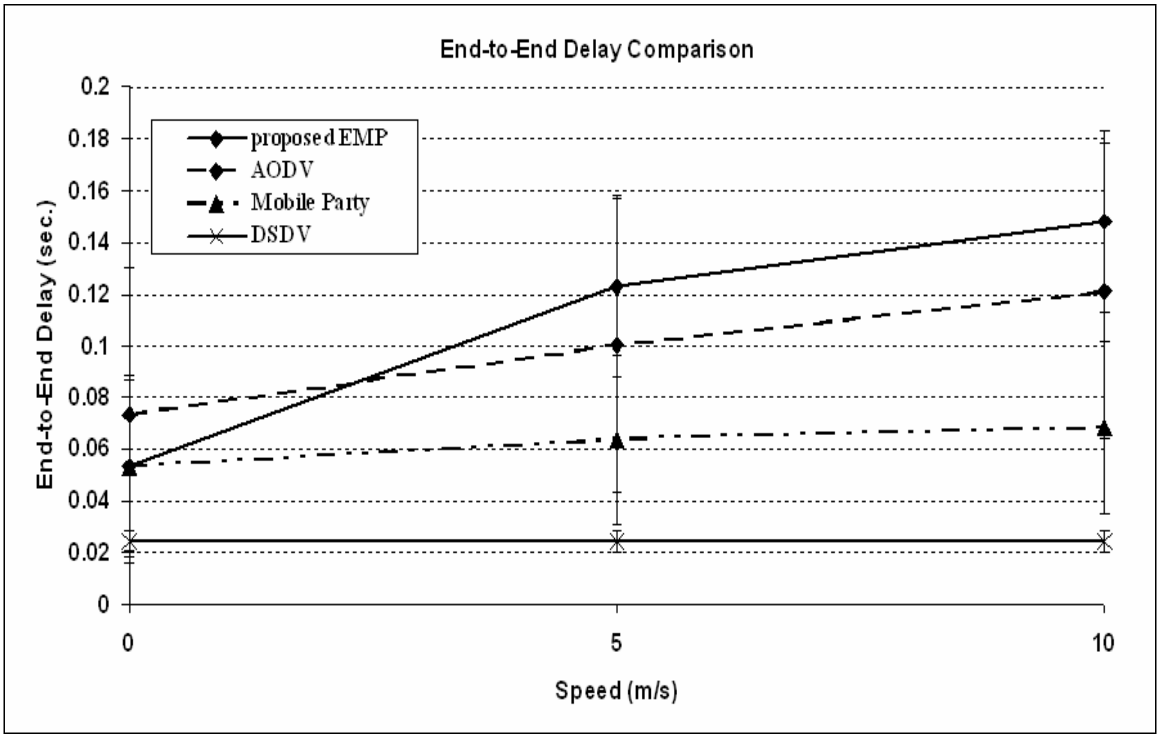

Fig.4. 16: Comparison of End-to-End Delay versus Speed of Nodes with Different Routing Protocols

In conclusion, proposed EMP is better affordable for wireless mesh network where scalability is main issue and the mobility is lesser (maximum speed is generally less than 5 m/s (18 km/hour)). For the mobility range of our interest (i.e. less than 5 m/s), EMP provides:

- A PDR improvement of about 15% compared to Mobile Party (PDR for EMP is about 96.5%; PDR for Mobile Party about 81.5%). PDR of EMP is comparable with AODV.

- Lowest signaling traffic overhead- about 17 % less than that of AODV (for EMP: about 58% and for AODV: about 75%). For the mobility support the signaling overhead added is less than 3% compared to static case of Mobile party (for EMP with mobility signaling overhead is about 58.38 % and for Mobile Party static case it is about 55.81 %).

- End-to-end delay comparable with AODV. Delay can be further decreased by allowing intermediate nodes to drop the packets in queue after certain time. This will increase the drop slightly.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

The overall objective and contribution of the thesis is to provide scalability support in WMNs using the dynamic address allocation based routing approach as the network size increases. The general objectives are to study the scalable routing protocol 'party' which uses dynamic address allocation, to enhance and make it suitable for WMN in the case of node mobility and to evaluate the performance of proposed enhanced mobile party compared to existing routing protocols. My work and results fulfill the objectives of the thesis. Additionally, the code written for the simulation of EMP is also a part of contribution to the development of party protocol.

General conclusion is that routing based on dynamic address allocation, in which address is based on current location, is a promising approach to solve the problem of scalability in large WMNs and other ad hoc networks.

The Signaling overhead in proposed EMP is found to be least compared to existing routing protocols (AODV, DSDV) and is almost independent of the network size and number of traffic flows because in EMP the signaling needed to maintain the routing table is mostly limited to just immediate neighbors. This provides the scalability to the proposed EMP. In terms of throughput the proposed EMP is found to scale well. In the case of smaller network with higher node speed, AODV is found to be better in terms of PDR, but due to linearly increasing signaling overhead with network size and number of traffic count, performance of AODV degraded sharply as network size increases beyond 50 nodes. The cost paid for better scalability in the proposed EMP is the increase in end-to-end delay. The end-to-end delay is found to be highest in EMP, although it is comparable with AODV.

The result of this thesis proved that the EMP proposed in this thesis is better affordable for WMN where scalability is main issue and mobility of the nodes is generally less than 5m/s (18 kmph). The work carried out during this thesis also reveals the promising fact that routing based on dynamic address allocation (like proposed EMP) can solve the problem of scalability in large ad hoc networks. It will help to motivate the researchers towards promising research field of dynamic address allocation to solve the problem of scalability in general ad hoc networks.

In EMP, notion of default gateway is introduced so that node of EMP network can communicate with the external nodes (non-EMP nodes). Similarly another mechanism is introduced to support roaming of non-EMP nodes in EMP network. So using EMP in WMN or any other ad hoc network avoids the network being isolated from other networks.

Regarding the implementation and deployment of proposed EMP in real systems, the system is quite feasible and not complex. The proposed EMP supports the use of IP based applications because the EMP routing is introduced between IP and MAC layers in the protocol stack, thereby hiding the dynamically allocated routing address from the higher layers and preserving the compatibility. Access to other network resources is handled by the gateway nodes connected to the internet. Several EMP networks can be connected using the way of an overlay network of gateways that tunnel through the internet. Further more as specified above the notion of default gateway and mechanism for supporting roaming of non-EMP nodes make the proposed EMP more flexible and compatible with other networks.

5.2 Recommendations for Future Work

In proposed EMP, when a node loses its parent, all the data packets whose next hop is parent, is kept in queue until it gets another parent. Due to this, end-to-end delay is high. To make EMP more suitable for delay sensitive applications, end-to-end delay can be decreased considerably by allowing intermediate nodes to drop the packets in queue after certain time. This will increase the drop slightly. Some other alternatives are that in the case of parent lost, intermediate node can forward the data in queue whose next hop is parent, to grandparent, if it is within the transmission range. Further work is needed to reduce the delay maintaining higher PDR.

My simulation results are focused on small size networks for mobility case. My plan is to evaluate EMP for larger networks with higher speed which is a future work.

In EMP we are using prefix based routing, not the shortest path. So the path stretch which is defined as the routing path length over shortest path length is found to be 30-70 % higher. Future study can be made to decrease this value. This will contribute to reduce the end-to-end delay as well.

In EMP routing is completely loop free for static case, but in the case of node mobility no guarantees can be made for loop free routing as routing is done based on temporary addresses and nodes can change address while a packet is in flight. Future study can be done in this area to guarantee the loop free routing in all the case.

REFERENCES

[1] Akyildiz, I.F., Wang, X., Wang, W., *Wireless mesh networks: a survey*, Science Direct, Computer Networks, (2005), Available online on http://www.sciencedirect.com/

[2] Akyildiz, I.F., Wang, X., *A survey on wireless mesh networks*, IEEE, Communication Magazine, Volume 43,Issue 9, pages S23-S30, September., (2005).

[3] Mittal, K. and Belding, E.M., *RTSS/CTSS: mitigation of exposed terminals in static 802.11-based mesh networks*, 2nd IEEE Workshop on Wireless Mesh Networks, Wi Mesh 2006.Page(s):3 - 12, Digital Object Identifier 10.1109/WIMESH.2006.288617, 2006.

[4] Buddhikot, M., Hari, A., Singh, K. and Miller, S., *MobileNAT: A New Technique for Mobility Across Heterogeneous Address Spaces*, Mobile Networks and Applications, Volume 10, Number 3, pp. 289-302(14), Publisher: Springer, January 2005.

[5] Nava, V., Kashyap, A. and Das, S.R., *Design and Evaluation of iMesh: an Infrastructure-mode Wireless Mesh Network*, Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM 2005, pages 164-170, June 2005.

[6] Johnson, D., Perkins, C., Marko, J., *Mobility Support in IPv6*, IETF RFC 3775, Network Working Group, June 2004.

[7] Mesh Networking Forum, *Building the business case for implementation of wireless mesh networks*, Mesh Networking Forum 2004, San Francisco, CA, October 2004.

[8] Held, G., *Wireless Mesh Networks*, Auerbach Publications, Taylor and Francis group, USA, 2005.

[9] Eriksson, J., Faloutsos, M. and Krishnamurthy, S. *Scalable Ad Hoc Routing: The Case for Dynamic Addressing*, INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, volume 2, pages 1108-1119, march 2004

[10] Eriksson, J., Faloutsos, M. and Krishnamurthy S.V., *DART: Dynamic Address Routing for Scalable Ad Hoc and Mesh Networks* ,IEEE/ACM Transactions on Networking, Vol. 15, Issue 1., pp. 119-132, February 2007.

[11] Sukkar G. A., Afifi H., Senouci S. M., *Party: Pastry-Like Multi-hop Routing Protocol for Wireless Self-Organizing Networks*, Mobile Computing and Wireless Communications International Conference, Amman, Jordan, Organized by Mosharaka For Researches and Studies, Technically Co-Sponsored By IEEE Communications Society, September 2006.

[12] Faccin, S. M., Wijting, C., Kneckt, J. and Damle, A., *MESH WLAN NETWORKS: CONCEPT AND SYSTEM DESIGN* ,IEEE Wireless Communications, Volume 13, Issue 2,pages 10-17, April 2006

[13] Ju, H. J. and Rubin, I., *Backbone Topology Synthesis for Multiradio Mesh Networks*, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, Issue 11, Page(s): 2116 - 2126 Digital Object Identifier 10.1109/JSAC.2006.881611, November 2006.

[14] Krishnamurthy, L.,Conner, S.,Yarvis, M.,Chhabra,J., Ellison, C., Brabenac, C.and Tsui, E., *Meeting the demands of the digital home with high-speed multi-hop wireless networ*ks, Intel Technology Journal, Vol. 06, Issue 04, ISSN 1535-766X, pages: 57–68, November 2002

[15] IEEE 802.11s, *Status of Project IEEE 802.11s*, IEEE, ESS Mesh Networking Task Group, January 2007 website: http://www.ieee802.org/11/Reports/tgs_update.htm

[16] IEEE 802.15, *IEEE 802.15 Working Group for WPAN*, march 2007, Available at Web site of IEEE , http://www.ieee802.org/15/,

[17] IEEE 802.16, *The IEEE 802.16 Working Group on Broadband Wireless Access Standards*, Retrieved on March 2007, Available at website of IEEE, http://www.ieee802.org/16/

[18] Subramanian, A.P., Buddhikot, M.M., Miller, S., *Interference aware routing in multi-radio wireless mesh networks*, 2nd IEEE Workshop on Wireless mesh Networks,WiMesh 2006, Pages 55 -63, Digital Object Identifier 10.1109/WIMESH.2006.288620, 2006

[19] Draves, R., Padhye, J. and Zill, B., *Routing in multi-radio, multi-hop wireless mesh networks*, International Conference on Mobile Computing and Networking Proceedings of the 10th annual international conference on Mobile computing and networking, Philadelphia, PA, USA, Pages: 114 - 128, ISBN: 1-58113-868-7, Publisher: ACM press New York, 2004.

[20] Rowstron, A. and Druschel, P., *Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems*, In Proceedings of the 18th IFIP (International Federation for Information Processing)/ACM, International Conference on Distributed Systems Platforms (Middleware 2001). Heidelberg, Germany, November 2001.

[21] SHA, *FIPS 180-1*, *Secure Hash Standard*. U.S. Department of commerce/NIST, National Technical Information Service, Springfield, Apr. 1995.

[22] Perkins, C., Belding-Royer, E., Das, S., *Ad hoc On-Demand Distance Vector (AODV) Routing* IETF RFC 3561, Network Working Group, IETF, July 2003.

[23] Perkins, C. E., Bhagwat, P., *Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers*, ACM SIGCOMM Computer Communication Review archive, volume 24, Issue 4, pages 234-244, October 1994.

[24] Perkins C. E., Royer, E.M., *Ad-hoc On-Demand Distance Vector Routing*, available at http://ieeexplore.ieee.org/iel4/6056/16183/00749281.pdf

[25] Bicket, J.,Aguayo, D., Biswas, S., and Morris, R., *Architecture and Evaluation of an Unplanned 802.11b Mesh Network*, International Conference on Mobile Computing and Networking, Proceedings of the 11th annual international conference on Mobile computing and networking, Cologne, Germany, Pages: 31 - 42, ISBN:1-59593-020-5, September 2005.

[26] Clausen, T. and Jacquet, P., *Optimized link state routing protocol (OLSR)*, IETF RFC 3626, October 2003.

[27] Dunmore, M. and Pagtzis, T., *Contributors: Martin Dunmore, Theo Pagtzis, Mobile IPv6 Handovers: Performance Analysis and Evaluation*, Project 6NET, Project Number: IST-2001-32603, version 1.1, Deliverable Number: 32603/ULANC/DS/4.1.1/A1, May 2004.

[28] Sukkar G. A., et. al., *Performance Evaluation of Party Protocol*. To be submitted for Publication. INT, Evry , France, 2007.

[29] Wi-Fi Alliance, Official Site of Wi-Fi Alliance, http://www.wi-fi.org/

[30] Rosenberg J.et. al, SIP: *Session Initiation Protocol*, IETF RFC 3261,Network Working Group, June 2002

[31] Satish Chandra Jha**,** *Dynamic-Address-ALLocation based routing for scalability support in WIRELESS****.*** *MESH NETWORKs***,** Aug. 2008