ISBN : 978-81-953083-1-6

Power Optimized Reliable Routing to Enhance Work Capacity & Network Lifetime Over Real-Time MANETs

Author
Dr. T. K. Shaik Shavali

Publisher
ADITI PUBLICATION
Raipur (C.G.) India

Power Optimized Reliable Routing to Enhance Work Capacity and Network Lifetime over Real-time MANETs

Author
Dr. T. K. Shaik Shavali
Professor and Head,
Dept.of Computer Science and Engineering,
Lords Institute of Engineering and Technology,
Hyderabad, Telangana, India.

Publisher
Aditi Publication, Raipur, Chhattisgarh, INDIA

Power Optimized Reliable Routing to Enhance Work Capacity and Network Lifetime over Real-time MANETs

2021
Edition - **01**

Author

Dr. T. K. Shaik Shavali
Professor and Head,
Dept.of Computer Science and Engineering,
Lords Institute of Engineering and Technology,
Hyderabad, Telangana, India.

ISBN : **978-81-953083-1-6**

Price : Rs. **500/-**

Printed by
Yash Offest,
Lily Chowk, Purani Basti Raipur
Tahasil & District Raipur Chhattisgarh, India

Publisher :
Aditi Publication,
Near Ice factory, Opp Sakti Sound Service Gali,
Kushalpur, Raipur, Chhattisgarh, INDIA
+91 9425210308

About the book

This book contributes towards development of coding algorithm for reliable and robust routing scheme in adhoc networks. The objective of developing optimized routing scheme based on efficient power optimization and trust worthyness is been suggested. The problem of providing dynamic security over a distributed network is been analyzed. To present develop work this book is outlined into 8 chapters. Where chapter 1 provides a brief introduction towards the developed work. The problem focused for developing the proposed work is briefly outlined. The basic objective of developed work and the methodology outlined for developing a system is presented in this chapter. A basic literature survey on a proposed problem focusing on the past developments, contribution and limitations are studied. A summarized outline of the literature referred is outline in chapter2. Chapter 3 presents the basic operational description of current adhoc networks. The procedure of developing routings in MANETs is been presented. Towards a development of an optimized power routing scheme a routing intelligence protocol is proposed. The algorithmic description of the proposed protocol is outlined in chapter 4. The process of over scheduling and qualitative analysis of a proposed algorithm is presented in this chapter. Towards the development of robust routing scheme a trust worthy routing protocol is been suggested. Trustiness towards the routing is a major factor in providing reliability of developed routes for data forwarding. A modified Bayesian approach is proposed towards providing trustworthiness to developed route is proposed. The performance evaluation of suggested algorithm is outlined in chapter 5. The proposed approach of route optimization and scheduling scheme is been presented with the packet switching between multiple nodes. The effectiveness of switching scheme for high throughput is been proposed in chapter 6. The performance evaluation for the proposed methodology is presented in this chapter. The performance evaluations obtained for the developed approach are evaluated under different conditions. The performances obtained were evaluated under different conditions of network parameters, the observations made were presented in chapter 7. The book is presented with a summarized conclusion, and future scope in chapter 8. The references used for the development of proposed work is outlined at last.

INDEX

Chapter 01 Introduction

1.1. Overview

Wireless networking grows rapidly because of the human desires for mobility and for freedom from limitation, i.e., from physical connections to communication networks [1]. Recent advances in wireless technology have equipped portable computers, such as notebook computers and personal digital assistants with wireless interfaces that allow networked communication even while a user is mobile [2]. A particular kind of wireless network called mobile ad hoc networks is presently under development. A mobile ad hoc network is a self-organizing and rapidly deployable network in which neither a wired backbone nor a centralized control exists.

The network nodes communicate with one another over scarce wireless channels in a multi-hop fashion. The ad hoc network is adaptable to the highly dynamic topology resulted from the mobility of network nodes and the changing propagation conditions. These networks are used in emergency disaster rescue operation, tactical military communication and law enforcement. In these applications, where a fixed backbone is not available, a readily deployable wireless network is needed. Mobile ad hoc networks are also a good alternative in rural areas or third world countries where basic communication infrastructure is not well established. Another interesting application of mobile ad hoc networks is ubiquitous computing [3]. Intelligent devices are connected with one another via wireless links and are self-organized in such a way that a newly joined node can request service from local servers without any human intervention.

With the development of the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Some examples of possible uses include students using laptops to participate in an interactive lecture, business associates sharing information during a meeting, and emergency disaster relief personnel coordinating efforts after a hurricane or earthquake. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Because of the mobility of the nodes, the network topology may change rapidly and unpredictably.

The principle behind ad hoc networking is multi-hop relaying, which means that the other nodes transmit messages if the target node is not directly reachable. The absence of any central coordinator and base station makes it difficult to manage the network. Properties for the Adhoc network resources can be summarized as:

- **No fixed topology:** The network topology in an ad-hoc wireless network is highly dynamic due to the mobility of nodes. They may move in and out of the range of each other. The topology changes if one of those events happens, e.g. the route table and the multicast table [75] must be changed accordingly. This increases the difficulty to management the network.
- **Limited energy:** Mobile devices use generally battery power, which is exhaustible. In order to save the energy, some devices may be in sleepy mode. During this period they are possibly not reachable, or do not process traffic, or change to normal mode with latency. On one hand most wireless devices use spread spectrum communications, which need the receiving and decoding of the signal. These are expensive operations that consume much power. On the other hand some complex computations are also very expensive, for example modular exponentiation, which makes it difficult to implement the public key systems for ad hoc networks.

- **Limited processor:** Most mobile devices have cheap and slow processors, because fast processors cost much more and the size should be as smart as possible to make it easy to take. Hence it takes much time to operate some complex computations. The most PDAs have currently processors of several hundred MHz.
- **Limited storage capability and other resources:** Because of the size and cost restrictions, the most mobile devices are equipped with limited storage capability. For example, iPAQ hx4700 series of HP have only 192 MB memory. Due to the wireless technologies the network bandwidth is also limited. For example, some PDAs of HP are equipped with WLAN 802.11b, and Blue tooth 1.2.
- **Transient connectivity and availability:** Many nodes may not be reachable at some time so that they can save power.
- **Each node is a router:** The nodes out of the range of a fixed node can not be directly reached by this node. They can only be reached by packet forwarding of other nodes.
- **Shared physical medium:** Unlike wired networks, every device within the range can access the transmission medium.
- **Lack of central management:** Ad hoc networks can be established everywhere and every time. Generally there is no central management available, and we can also not assume that any information is shared.

Due to the lack of fixed infrastructure and limited resources, it will be much more complex to adapt protocols and other technologies from the infrastructure based networks.

1.2. Problem Statement

The limited resources in MANETs have made designing of an efficient and reliable routing strategy a very challenging problem. An intelligent routing strategy is required to efficiently use the limited resources while at the same time being adaptable to the changing network conditions such as: network size, traffic density and network partitioning. In parallel with this, the routing protocol may need to provide different levels of QoS to different types of applications and users. Nodes in MANETs often have limited energy supplies. Thus, to increase the network lifetime, a node should optimize its energy usage. In the communication system, the wireless interface between two nodes is the largest consumption of energy [10]. The wireless interface consumes energy not only during active communication but also during passive listening, when it is idle. Studies [4, 16] show that energy consumption while listening to data is only slightly less than it is while actually receiving data. Thus, in the case of moderate traffic load, idle time is the dominating factor in energy consumption.

The other major factor in Ad Hoc management is the node mislead. Although an efficient power management scheme is applied to a ad hoc network to a misleading node may result in the improper routing of packet which may extend to the complete collapsing of the network also. In mobile ad-hoc networks, where nodes act as both routers and terminals, the nodes have to cooperate to communicate. Cooperation at the network layer takes place at the level of routing, i.e. finding a path for a packet, and forwarding, i.e. relaying packets for other nodes. Mislead means aberration from normal routing and forwarding behavior. It arises for several reasons.

When a node is faulty, its erratic behavior can deviate from the protocol and thus produce non-intentional mislead. Intentional mislead aims at providing an advantage for the misleading node. An example for an advantage gained by mislead is power saved when a selfish node does not forward packets for other nodes. An advantage for a malicious node arises when mislead enables it to mount an attack. Without appropriate counter measures, the effects of mislead have been shown to dramatically decrease network performance.

Depending on the proportion of misleading nodes and their specific strategies, network throughput can be severely degraded, packet loss increases, nodes can be denied service, and the network can be partitioned. These detrimental effects of mislead can endanger the functioning of the entire network. Due to the issues such as shared physical medium, lack of central management, limited resources, no fixed and highly dynamic topology, ad hoc networks are much more vulnerable to security attacks which is one more major issue in current Adhoc networks. Hence it is very necessary to find security solutions, which are much more difficult to develop than in wired networks. As well as in wired networks, the major security goals of confidentiality, integrity, availability, authentication and non-repudiation should be satisfied. Hence overall for providing a efficient performance in adhoc network a reliable, secured and trusted routing scheme is to be developed so as to make the adhoc network a reliable wireless communication mode for next generation communication.

1.3. Motivation

With the focus of above stated problem outline this research was focused for the development of a routing protocol in Adhoc network for reliable and secured routing. A Robust Route Management (RRM) is proposed which provides an existing system to cope with mislead-route state. As a concrete instantiation of such an existing system, we chose mobile ad-hoc networks running Dynamic Source Routing (DSR) and applied RRM to it. The approach used in RRM is to detect misleading nodes and to render them harmless, regardless of the reason of their mislead, be it selfish, malicious, or faulty. The response to detected misleading nodes is to isolate them, so that mislead will not pay off but result in denied service and thus cannot continue. RRM detects misleading nodes by means of direct observation or second-hand information about several types of attacks, thus allowing nodes to route around misleading nodes and to isolate them. For the trustworthy nodes a power optimized routing scheme is been developed which provides the feature of topology management in Ad hoc networks for power saving routing. This routing protocol, called Power adaptive routing scheme (PAR) protocol is developing with the features of:

i) Allowing as many nodes as possible to turn their radio receivers off.

ii) Forwarding packets between any source and destination with minimally more delay than if all nodes were awake.

iii) Picking of backbone should be distributed, so that each node should make a local decision. To fulfill these requirements, each node in the network is scheduled to make periodic, local decisions on whether to sleep or stay awake and as a PAR node, participate in the forwarding backbone topology. Over this power optimized routing scheme a security issue is also proposed to make the adhoc routing completely reliable and secured. For the objective of providing security solution in adhoc network, a self-monitored key management that allows users to generate their key pairs, issue certificates, and perform authentication regardless of the network partitions and without any centralized services is proposed. A self organizing key management system that allows users to create, store, distribute and revoke their keys without the help of any trusted authority or fixed server is developed.

CHAPTER 02 LITERATURE SURVEY

2.1. Introduction

Mobile Adhoc Network [1 17 18 19] (MANET) is a collection of wireless mobile nodes which are dynamically forming a network without the use of any fixed infra-structure. Dynamic Source Routing (DSR) protocol and Adhoc On demand Distance Vector (AODV) protocol are popular on demand reactive routing protocols designed for MANET. The performance study of protocols [2] reveal that DSR is a self organizing and self-configuring protocol and is used for systems which have moderate mobility and lesser number of nodes. Adhoc On-Demand Distance Vector routing protocols [3,4] are highly efficient adapting quickly to the dynamic network link conditions with low processing and memory overhead, low network utilization and establish unicast routes to destinations. It is known that mobile nodes in network may move continuously leading to a volatile network topology with possibility of interconnections between them getting disconnected. Such situations create variable throughput and longer delay. To overcome this problem, either a method should be adopted to protocols getting changed from one another or go for an adaptive or one single universal protocol to meet all these conditions. Therefore, efficient routing in ad hoc networks is a crucial and challenging problem. In literature, protocols such as, SHARP— a hybrid adaptive [5] routing protocol, combined routing method [6], DSR over AODV (DOA) method [7] are reported.

Ad hoc networks, due to their quick and economically less demanding deployment, find applications in military operations, collaborative and distributed computing, emergency operations, wireless mesh networks, wireless sensor networks and hybrid networks[8].

The most comprehensive performance comparison of ad hoc multicast routing protocols uses the Uniform model, in which nodes move in a random direction with constant velocity and then bounce off the boundary of the simulated field [9]. Most other studies [10], [11], [12] use the Random Waypoint model, in which each node moves to a random destination, pauses for a specified period, and then chooses a new destination. A recent study shows that the average speed of a node using Random Waypoint decreases with time, and hence the results obtained using this model becomes unreliable as the simulation advances [13]. Classification and survey of existing mobility models are given in [14]. Since tactical network consist of mobile devices, the mobility models used has a decisive impact. In [15], the effect of mobility models on the performance of mobile ad hoc network using unicast routing protocol is discussed. The important framework [16] characterizes movement based on spatial dependence, relative speed, and other factors illustrates how these metrics impact unicast routing performance. Most of the studies in the literature are based on random way point mobility model and constant bit rate (CBR) traffic consisting of randomly chosen source–destination pairs as the traffic pattern.

2.2. Robust Routing and Misbehaving of Nodes

In this study, as an effective and practical metric of link quality, signal-to-interference plus noise ratio (SINR) is used because it takes interference and noise as well as signal strength into account. Note that SINR is measurable with no additional support at the receiver [20,21]. Furthermore, as nodes are fast moving, poor links are unpredictably increased. Actually, it is shown that the communication quality of mobile ad hoc networks is low and users can experience strong fluctuation in link quality in practical operation environments [22]. In particular, sending real-time multimedia over mobile ad hoc networks is more challenging because it is very sensitive for packet loss and the networks are error prone due to node mobility and weak links [23]. Accordingly, it is very important to include as many high-quality links as possible in a routing path. Also, the dynamic behavior of link quality should be taken into consideration in protocol design.

In the IEEE 802.11 MAC [24], broadcast packets are transmitted at the base data rate of 1 Mbps. Furthermore, as an effort, SINR based design of optimized link state routing was introduced for scenarios where VoIP (Voice over IP) traffic is carried over a static multihop networks [25].

A lot of routing protocols have been proposed for the (mobile) wireless ad hoc networks, which are followed one of two major strategies: proactive such as in DSDV [27] and OLSR [28] and reactive (on-demand) such as in AODV [29] and DSR [30]. These protocols were originally designed for single-rate networks, and thus have used a shortest path algorithm with minimum hop count metric to select paths. Min hop is a good metric in single rate networks where all links are equivalent. However, it does not perform well in the multi-rate wireless network because it does not utilize the higher link speed for data transmission.

The Ad hoc On demand Distance Vector (AODV) protocol [29] is one of the popular reactive routing protocol that discovers the path between the source and destination nodes dynamically. In AODV, when the source node wants to communicate with a destination node, it will broadcast a Route Request (RREQ) packet to the network. The neighboring nodes, which receive the RREQ packet, search for an existing route to the destination in its routing table. If there is a route already exist, the intermediate node replies with an unicast Route Reply (RREP) packet to the RREQ sender. Otherwise, it forwards the RREQ packet to its neighbors. By this way, the RREQ packet traverses hop by hop and reaches the destination. The destination node replies with an RREP to establish a new route by sending the packet traverses the same path in the reverse direction. When the source node receives multiple copies of RREP packets for the same RREQ packet, it selects the path with the minimum number of hops. The Hello and Route Error (RERR) packets is used to manage route failure and reconstruction. The design of AODV protocol is based on the simple packet radio model without the consideration of data transmission rate. The main problem of AODV is based on hop count, which can avoid to choose the highest data rate route.

The author in [31] introduced an approach for multi rate MANETs to improve traditional AODV routing protocol. The proposal based on the link cost which is simply provided by delay time for transfer a packet from MAC layer which is inherited from the conference version (published in the year 2004) of [26]. Nicolaos et. al. in [32] proposed routing metric for communication network using the new metric with connection probability approach. [32] also introduces the concept of link cost. However, they did not specify how to calculate the link cost for their routing metric. Also, the complexity of their proposal is very high because each node has to maintain the information of all other nodes in the network to calculate the routing metric based on the proposed probability models. Traditionally, the Automatic Rate Fallback (ARF) protocols originally developed in [33] is widely-adopted by the industries to determine the initial transmission rate. In ARF, the node first transmits packet to a particular destination at the highest data rate and it switches to the next available lower data rate when it does not receive two consecutive ACK frames and starts a timer after the switch. When the node receives 10 consecutive ACK frames successfully or the timer expires, it switches to the next higher data rate again and packets are always transmitted at the highest possible rate. In another paper, the Receiver Based Auto Rate (RBAR) protocol [34] allows the receiving node to select the rate. This is accomplished by using the SNR of the RTS packet to choose the most appropriate rate. The CTS packet is used to ACK that rate to the sender. The Opportunistic Auto Rate (OAR) protocol presented in [35] operates using the same receiver based approach. It allows high-rate multi-packet bursts to take advantage of the coherence times of good channel conditions. OAR uses the IEEE 802.11 mandated fragmentation field to hold the channel for an extended number of packet transmissions. In IEEE 802.11 each node has equal opportunity to send the same number of packets, so that the node transmitting at high speed actually does not gain high throughput if it shares the channel with some nodes at lower transmission rate. However in OAR, each node accesses the medium for the same amount of time, so the overall throughput will increase with the higher link rates. Therefore, both RBAR and OAR require modifications to the 802.11 standard but can increase the overall throughput. For multirate wireless ad hoc networks, Medium Time Metric is one of the well-known routing metrics.

2.3. Power Optimizing Mechanisms

In the research of network coding in unicast applications, one of the notable work is [36], which gives solutions to the following five problems: network coding for unicast applications, coping with bursty traffic and dynamic environments, broadcast with collision avoidance, low complexity encoding and decoding, and working properly with TCP.

Much attention has been paid on network coding, since it's proposed in [37]. The authors of [37] have shown that allowing intermediate nodes to process the information can increase the broadcast capacity, and intermediate nodes are required to perform combinations of the incoming packets. The basic idea is to allow and encourage mixing of data at intermediate network nodes.

In most research of network coding, much work has been done on multicast or broadcast applications [38-39, 40-41, 43, 44], with the target of reducing the total number of transmissions each forwarding node performs, and few work gives attention to unicast application [36, 42, 45]. Sachin Katti et al. [36] introduced a completely opportunistic approach called COPE to network coding. In COPE, every wireless node depends on local topology information and reception reports exchanged with its neighboring nodes to detect and exploit coding opportunities in real time. There are two components for every node to accomplish the task of network coding: opportunistic listening and opportunistic coding.

2.4. QoS Issues in Adhoc Networks

Charles J. Colbourn et al. [46] have proposed an alternate approach to collision resolution in a CSMA protocol and they introduce spatial backoff, the use of power control and they show that collision resolution using power backoff can be remarkably successful, outperforming IEEE 802.11 in both static and mobile ad hoc network scenarios.

Aran Bergman et al. [47] proposes the introduction of a novel utility function that reflects the tradeoff between the energy consumption induced by a MAC protocol and its throughput, thus representing the energy efficiency of the algorithm and they introduce a modification of the ‘‘0.487’’ algorithm that improves its energy effciency. Xiaojiang et al. [48] present a new routing protocol called multiclass (MC) routing, which is specifically designed for heterogeneous MANETs. Moreover, they also design a new medium access control (MAC) protocol for heterogeneous MANETs, which is more efficient than IEEE 802.11b. Vasudev Shah, et al. [49] develop a cross-layer framework to effectively address the link asymmetry problem at both the MAC and the routing layers and they perform extensive simulations to study the performance of their proposed framework in various settings, and show that the overall throughput in power heterogeneous networks is enhanced by as much as 25% over traditional layered approaches. Xiaojiang et al. [50] find a new routing protocol called Hybrid routing, which is specifically designed for hybrid MANETs. Javier Gomez et al. [51] show how routing protocols based on common-range transmission power limit the capacity available to mobile nodes and their results presented in their paper highlight the need to design future wireless network protocols (e.g., routing protocols) for wireless ad hoc and sensor networks based, not on common-range which is prevalent today, but on variablerange power control. Jungmin So et al. [52] proposes a medium access control (MAC) protocol for ad hoc wireless networks that utilizes multiple channels dynamically to improve performance.

Bright Chu [53] proposes a few schemes to determine the initial contention window size for a transmission based on the distance traveled by the flow and his Simulation results show that his approach achieves significant performance improvement. Alaa Muqattash et al. [54] propose a comprehensive solution for power control in mobile ad hoc networks (MANETs) and their solution emphasizes the interplay between the MAC and network layers, whereby the MAC layer indirectly influences the selection of the next-hop by properly adjusting the power of route request packets. Backoff strategiesfor multiple Access protocols have typically been analyzed by making statistical assumptions on the distribution of problem inputs. Although these analyses have provided valuable insights into the efficacy of various backoff strategies, they leave open the question as to which backoff algorithms perform best in the worst case or on inputs,such as bursty inputs, that are not covered by the statistical models. Michael A. Bender et al. [55] analyzes randomized backoff strategies using worstcase assumptions on the inputs. Nasipuri, A. et al. [56] describe a new carrier-sense multiple access (CSMA) protocol for multihop wireless networks. The CSMA protocol divides the available bandwidth into several channels and selects an idle channel randomly for packet transmission. It also employs a notion of “soft” channel reservation as it gives preference to the channel that was used for the last successful transmission. We show via simulations that this multichannel CSMA protocol provides a higher throughput compared to its single channel counterpart by reducing the packet loss due to collisions. Zhenyu Yang et al. [57] proposes a new multichannel MAC protocol called hop-reservation multiple access (HRMA) for wireless ad-hoc networks (multi-hop packet radio networks).HRMA is based on simple half-duplex, very slow frequency-hopping spread spectrum (FHSS) radios and takes advantage of the time synchronization necessary for frequency-hopping. HRMA allows a pair of communicating nodes to reserve a frequency hop using a reservation and handshake mechanism that guarantee collision-free data transmission in the presence of hidden terminals.

Presently there is increasing interest in wireless ad hoc networks built from portable devices equipped with shortrange wireless network interfaces. Bacarreza Nogales, I.M. [58] analyze the behavior of connections using Bluetooth connectivity at the link layer and MAC protocol, with emphasis in the communication between mobile nodes. An efficient formation algorithm to build mobile ad-hoc networks is described. Ware, C. et al. [59] address issues with the performance of IEEE 802.11, when used in the adhoc mode, in the presence of hidden terminals. Results illustrating the strong dependence of channel capture behavior on the SNR observed on contending hidden connections are presented. The work has illustrated that in a hidden terminal scenario, the connection having the strongest SNR is able to capture the channel, despite the use of the RTS-CTS-DATA-ACK 4-way handshake designed to alleviate this problem. It is indicated that the near-far SNR problem may have a significant effect on the performance of an adhoc 802.11 network. The topology of wireless multihop ad hoc networks can be controlled by varying the transmission power of each node[60]. Wattenhofer, R. et al. propose a simple distributed algorithm where each node makes local decisions about its transmission power and these local decisions collectively guarantee global connectivity. Specifically, based on the directional information, a node grows it transmission power until it finds a neighbor node in every direction. The resulting network topology increases the network lifetime by reducing the transmission power and reduces traffic interference by having low node degrees. Moreover, we show that the routes in the multihop network are efficient in power consumption. Packet dynamic resource allocation (packet DRA) is a new medium access control (MAC) protocol that applies interference-adaptive DRA concepts to manage reuse in packet-switched networks. Sending and receiving stations use a short handshake to exchange interference-related information and publish it for 3rd parties so they can avoid interfering[61]. Whitehead, J.F. describe and execute, completely distributed, and compatible with both peer-to-peer and base-station-oriented networks. Smart antennas have gained significant importance in multihop wireless networks in recent years, because of their sophisticated signal processing capabilities that hold the potential for increased data rates and reliability[62].Karthikeyan Sundaresany,et al. have discussed the problems of communication in multi-hop wireless networks with smart antennas (specifically digital adaptive arrays). These smart antennas provide degrees of freedom (DOFs) that can be used to suppress co-existing communication links, thereby increasing spatial reuse in the network. The communication problem comprises of not just determining a channel access mechanism to be used by the communication links, but also involves the determination of the communication pattern (usage of DOFs) to be used by each node during channel access. They consider the problem of determining the communication pattern to be used by the nodes and formulate it combinatorially with the goal of optimizing network performance through interference minimization. Nie Nie and Cristina Comaniciu[63] propose an energy aware on demand routing protocol for CDMA mobile ad hoc networks, for which improvements in the energy consumption are realized by both introducing an energy based routing measure and by enhancing the physical layer performance using beam forming. Exploiting the cross-layer interactions between the network and the physical layer leads to a significant improvement in the energy efficiency compared with the traditional AODV protocol and ensures a faster response to system changes, and reduced overhead. An ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure[64]. Charles E. Perkins presents Ad hoc On Demand Distance Vector Routing in AODV a novel algorithm for the operation of such ad hoc networks. Each Mobile Host operates as a specialized router and routes are obtained as needed ie on demand with little or no reliance on periodic advertisements. The new routing algorithm is quite suitable for a dynamic self starting network as required by users wishing to utilize ad hoc networks. AODV provides loop free routes even while repairing broken links. Because the protocol does not require global periodic routing advertisements the demand on the overall bandwidth available to the mobile nodes is substantially less than in those protocols that do necessitate such advertisements.

T. Kullberg [65] presents the performance and scalability of the AODV protocol both in small and large networks. The amount of wireless communication devices has increased dramatically over the last few years. This has created new kinds of requirements to the technology as the growing number of users want to be able to communicate with each other anywhere and anytime without having to rely on any existing infrastructure or centralized access point. Adhoc network is composed of a collection of mobile nodes co-operating together to form such network. Every node in ad hoc network acts both as a host and a router, which eliminates the need for existing infrastructure. Adhoc On Demand Distance Vector Routing protocol (AODV) is one of the developed protocols that enable routing with continuously changing topologies. AODV is reactive which means that it builds routes only when they are first needed. It uses extensive flooding of messages when discovering routes but tries to increase the overall bandwidth available by minimizing the use of any periodic advertisements. The increasing popularity of these on-the-fly networks has arisen the question about the efficiency and accuracy of the routing protocols used.

Chapter 03 AD HOC Network – Structure & Operation

3.1. Overview

Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. There is no fixed infrastructure such as base stations for mobile switching. Nodes within each other's radio range communicate directly via wireless links while those, which are far apart; rely on other nodes to relay messages. Node mobility causes frequent changes in topology. The wireless nature of communication and lack of any security infrastructure raises several security problems. The following flowchart depicts the working of any general ad-hoc network.

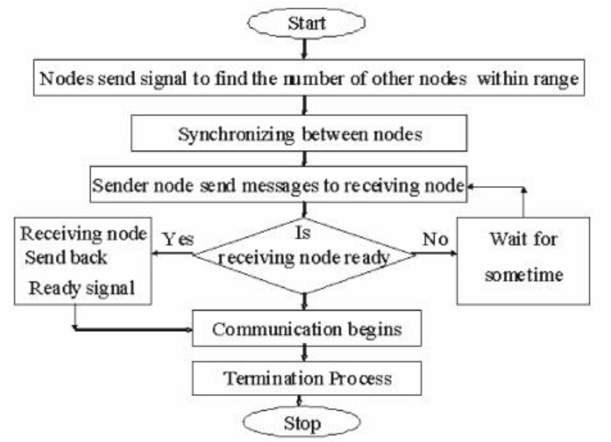

Start
Nodes send signal to find the number of other nodes within range
Synchronizing between nodes
Sender node send messages to receiving node
Is receiving node ready
Yes
No
Receiving node Send back Ready signal
Wait for sometime
Communication begins
Termination Process
Stop

Fig 2.1: Working of a general Ad-Hoc Network

The roots of ad hoc networking can be traced back as far as 1968, when work on the ALOHA network was initiated (the objective of this network was to connect educational facilities in Hawaii). Although fixed stations were employed, the ALOHA protocol lent itself to distributed channel access management and hence provided a basis for the subsequent development of distributed channel-access schemes that were suitable for ad hoc networking. The ALOHA protocol itself was a single-hop protocol that is, it did not inherently support routing. Instead every node had to be within reach of all other participating nodes. Inspired by the ALOHA network and the early development of fixed network packet switching, DARPA began work, in 1973, on the PRnet (packet radio network) a multihop network.2 In this context, multihopping means that nodes cooperated to relay traffic on behalf of one another to reach distant stations that would otherwise have been out of range. PRnet provided mechanisms for managing operation centrally as well as on a distributed basis. As an additional benefit, it was realized that multihopping techniques increased network capacity, since the spatial domain could be reused for concurrent but physically separate multihop sessions. Although many experimental packet radio networks were later developed, these wireless systems did not ever really take off in the consumer segment. When developing IEEE 802.11a standard for wireless local area networks (WLAN) the Institute of Electrical and Electronic Engineering (IEEE) replaced the term packet-radio network with ad hoc network. Packet-radio networks had come to be associated with the multihop networks of large-scale military or rescue operations, and by adopting a new name, the IEEE hoped to indicate an entirely new deployment scenario.

Today, our vision of ad hoc networking includes scenarios, where people carry devices that can network on an ad hoc basis. A users devices can both interconnect with one another and connect to local information points for example, to retrieve updates on flight departures, gate changes, and so on. The ad hoc devices can also relay traffic between devices that are out of range. The airport scenario thus contains a mixture of single and multiple radio hops. To put ad hoc networking in its right perspective, let us make some observations about wireless communication, beginning with present-day cellular systems, which rely heavily on infrastructure: coverage is provided by base stations, radio resources are managed from a central location, and services are integrated into the system. This lead to the good as well as predictable service of present-day cellular systems. The transport of traffic is not entirely dependent on the coverage provided by access points. Dependency on centrally administered coverage is further reduced when end-user terminals relay traffic in a multihop fashion between other terminals and the base station (cellular multihop).A similar approach applies to commercial or residential wireless local loop (WLL) multihop access systems, primarily conceived for Internet access (Figure 2, bottom left and middle). Fully decentralized radio, access, and routing technologies enabled by Blue tooth, IEEE 802.11 ad hoc mode, PRnet station less mode, mobile ad hoc network (MANET), and concepts such as the personal area network (PAN) or PAN-to-PAN communication fit more or less entirely into the ad hoc domain. The MANET initiative by the Internet Engineering Task Force (IETF) also aims to provide services via fixed infrastructure connected to the Internet.

Now coming to a mobile Ad Hoc network (MANET), it is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. This type of networks is suited for use in situations where a fixed infrastructure is not available, not trusted, too expensive or unreliable. A few examples include: a network of notebook computers or PDA’s in a conference or campus setting, rescue operations, temporary headquarters, industry etc. Mobile ad hoc networks (MANETs) are generating much interest both in academic and the telecommunication industries. The principal attractions of MANETs are related to the ease with which they can be deployed due to their infrastructure-less and decentralized nature. For example, unlike other wireless networks, MANETs do not require centralized infrastructures such as base stations, and they are arguably more robust due to their avoidance of single point of failures. Interestingly, the attributes that make MANETs attractive as a network paradigm are the same phenomena that compound the challenge of designing adequate security schemes for these innovative networks.

A very simple representation as below can be seen for an ad hoc network. The next figure shows the way communication is carried out in an ad hoc network.

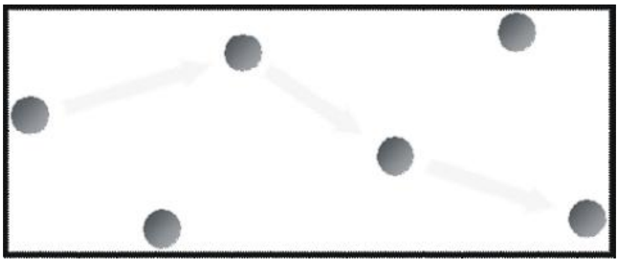


Fig 2.2: Basic Ad Hoc network architecture.

The message hops from one node to another. Every node acts as a switch and has routing capabilities.

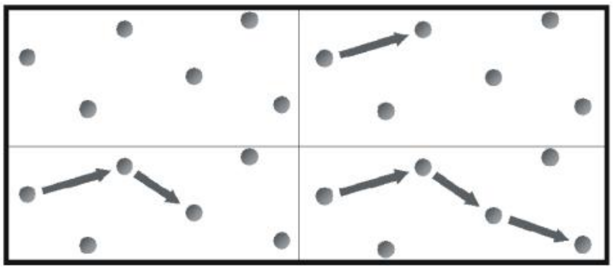


Fig 2.3: Ad Hoc communication

The message is propagating through the network usingintermediate nodes as switches. Therefore, each node must have routing capabilities.

3.2. Characteristics of Mobile ad-hoc Networks

It is important to acknowledge the properties or characteristics of mobile ad hoc networks (MANETs), since these properties have a significant impact on the design of security protocols for MANETs. Although these properties are detailed in various papers, security protocols that do not suit these characteristics are frequently published. The security implications of the characteristics are discussed where applicable.

3.3. Network Infrastructure

There is no fixed or pre-existing infrastructure in an ad hoc network: all network functionalit (routing, security, network management etc.) is performed by the nodes themselves. Due to the nodes' limited transmission range, data dissemination is achieved in a multihop fashion; nodes can therefore be considered as hosts and routers. Although the lack of infrastructure opens a new window of opportunity for attacks, the author believes the lack of infrastructure can help to ensure the survivability of the network in a very hostile environment. This holds true not only from a network security perspective, but also when the users of the network are under physical attack.

Ad hoc networks may be spontaneously formed with no a priori knowledge of the physical location and networking environment. MANETs' lack of infrastructure thus makes it suitable for various applications where conventional networks fall short

Some researchers have already addressed security issues in hybrid ad hoc networks (for Example. Hybrid ad hoc networks combine conventional network infrastructure with multi-hopping. This derivative of ad hoc networks will find useful application where fixed infrastructure can be extended through multi-hop networks or where the functionality (and performance) of multi-hop networks can be enhanced by relying on some infrastructure.

3.4. Network Topology

Nodes in ad hoc networks may be mobile resulting in a dynamic, weakly connected topology. Since node mobility is unrestricted, the topology may be unpredictable. The network will however demonstrate global mobility patterns, which may not be completely random. The topology is weakly connected due to transient, error-prone wireless connectivity. The users may therefore experience unavailability of essential security services. Node mobility and wireless connectivity allow nodes to spontaneously join and leave the network, which makes the network amorphous. Security services must be able to scale seamlessly with rapid changes in network density.

3.5. Self-Organization

MANETs cannot rely on any form of central administration or control; this is essential to avoid a single point of attack. Self-organized MANET cannot rely on any form of off-line trusted third party (TTP); the network can thus be initialized by a distributed on-line TTP. A pure or fully self-organized MANET does not rely on any form of TTP whatsoever, i.e. the on-line TTP is also eliminated. Nodes will therefore only have compatible devices with the same software installed. In the extreme case, the nodes will not even share a common set of security system parameters. The lack of a TTP may force the end-users to actively participate in the setup of security associations. A (fully)self-organized MANET has some inherent security implications:

- Fully self-organized MANETs are "open" in nature: similar to the internet, any user can join the network at random. Access control to applications will have to be provided at the application layer with a varying degree of user interaction.
- Each user will be its own authority domain, hence responsible for generating and distributing its own keying material. As pointed out by Douceur, any node can generate more than one identity when there is no off-line TTP. It is thus clear that it will be very difficult (if not impossible) to limit users to one and only one unique identity in a (fully) self-organized setting.
- The network will always be vulnerable to the active insider adversary.
- It will be difficult to hold malicious nodes accountable for

their actions, since they can always rejoin the network under a different (new) identity.

3.6. Limited Resources

Nodes have limited computational, memory and energy resources in contrast to their wired predecessors. Nodes are small hand-held devices (possibly "off-the-shelf" consumer electronics) that do not hinder user mobility. In an attempt to keep the cost of these devices low, a small CPU, accompanied by limited memory resources, normally powers them. As the devices are mobile they are battery operated. This often results in short on times and the possibility of power failure due to battery exhaustion, perhaps during execution of a network related function.

Devices may have limited bandwidth and transmission ranges. If it is assumed that advances in integrated circuit (IC) technology will keep on following Moore's law, computational and memory limitations will be alleviated in a matter of time. Bandwidth and transmission range (in the case of communication via radio transmissions) are unlikely to improve dramatically with respect to power consumption, as both are dependent on Shannon's law and thus limited. In order to achieve a higher bandwidth, a higher signal to- noise ratio (SNR) is required which in turn requires higher transmission power. Higher transmission power significantly depletes battery power, which is unlikely to improve significantly given the current rate of advancement in battery technology. A security protocol that fails to optimize node and network resources will simply not be adopted in practice.

3.7 Physical Security

Nodes are mobile and therefore cannot be locked up in a secure room or closet. These small hand-held devices are easily compromised by either being lost or stolen. It is therefore highly probable than an adversary can physically compromise one or more nodes and perform any number of tests and analysis. The adversary can also use the nodes to attack distributed network services, such as a distributed on-line certificate authority. Poor physical security is not as relevant in "open" MANETs: the adversaries do not have to physically capture nodes to become an insider or to perform analysis on the protocols. The poor physical security may result in serious problems in "closed", military type MANETs where physically compromised nodes can be used to launch active, insider attacks on the network.

3.8. Shared Physical Medium

The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted. Adversaries are therefore able to eavesdrop on communication and inject bogus messages into the network without limitation. The shared channel and the nodes' poor physical security again emphasize that security mechanisms must be able to deal with the worst-case active, insider adversary.

3.9. Distributed System

Considering the above properties, nodes in ad hoc networks have a symmetric relationship. This implies that they are all equal and therefore should equally distribute all of the responsibilities of providing network functions. This is not only for security reasons but to ensure reliable, available network services that places the same burden on the computational, memory and energy resources of all network participants .It is anticipated that a fair distributions of services will also help to alleviate selfishness.

3.10. Low-Power Devices

In many cases, the network nodes will be battery-driven, which will make the power budget tight for all the power-consuming components in a device. This will affect, for instance, CPU processing, memory size/usage, signal processing, and transceiver output/input power. The communication- related functions (basically the entire protocol stack below the applications) directly burden the application and services running in the device. Thus, the algorithms and mechanisms that implement the networking functions should be optimized for lean power consumption, so as to save capacity for the applications while still providing good communication performance. Besides achieving reasonable network connectivity, the introduction of multiple radio hops might also improve overall performance, given a constrained power budget. Today, however, this can only be realized at the price of more complex routing.

3.11. Typical ad hoc Network Functions

Typical functions of any ad hoc network include many issues like security, routing and more. They are discussed briefly in this section.

3.11.1 SECURITY : Obviously, security is a concern in an ad hoc network, in particular if multiple hops are employed. How can a user be certain that no one is eavesdropping on traffic via a for- warding node? Is the user at the other end really the person he claims to be? From a purely cryptographic point of view, ad hoc services do not imply many new problems. The requirements regarding authentication, confidentiality, and integrity or non-repudiation are the same as for many other public communication networks. However, in a wireless ad hoc network, trust is a central problem. Since we cannot trust the medium, our only choice is to use cryptography, which forces us to rely on the cryptographic keys used. Thus, the basic challenge is to create trusted relationships between keys without the aid of a trusted third-party certification. Since ad hoc networks are created spontaneously between entities that happen to be at the same physical location, there is no guarantee that every node holds the trusted public keys to other nodes or other parties will trust that they can present certificates that.

However, if we allow trust to be delegated between nodes, nodes that already have established trusted relationships could extend this privilege to other members of the group. The method described below can be used for distributing relationships of trust to an entire ad hoc network. The method is based on a public key approach and is exemplified by a small ad hoc network. We assume that connectivity exists between all the nodes in the network, and that it can be maintained by, say, a reactive ad hoc routing protocol. Initially, node A takes on the role of server node in the procedure of delegating trust. A triggers the procedure by flooding a start message into the network. Each node that receives this message floods the ad hoc network with a message containing the set of trusted public keys. A can then establish a map of trusted relations and identify them in the ad hoc network. In the example shown (Figure 2.2), three different groups (G1,G2, and G3) share a chain of trust. All the nodes in G2 share an indirect trusted relationship to A (through node C).

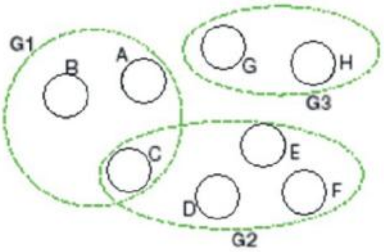


Fig2.2: Trust chain sharing in a network

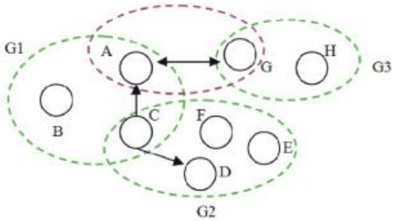


Fig 2.3: Trust chain relation between node G1 and G2

Node A can thus collect the signed keys it received from G2 via C (as illustrated in Figure 2.3). By contrast, the nodes in G3 do not have a trusted relationship to A. However, a trusted relationship between, say, node G in G3 and A can be created by manually exchanging trusted keys. Node A can now collect signed keys received from G3 via G (Figure 2.4). A can then flood the ad hoc network with all collected signed keys. This procedure creates trusted relationships between every node in G1, G2 and G3, and forms a new trust group, G1 (Figure 2.5). This example can be generalized into a protocol that handles the distribution of trust in an arbitrary ad hoc network.

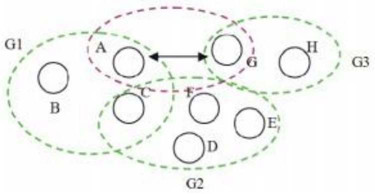


Fig 2.4: Node A collecting the keys from G3 via node G

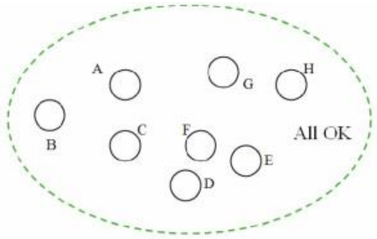


Fig 2.5: Ttrusted relation between nodes

3.11.2 Mobility Functions: In present-day cellular networks, node and user mobility are handled mainly by means of forwarding. Thus, when a user circulates outside his home network any calls directed to him will be forwarded to the visiting network via his home network. This same forwarding principle applies to mobile IP. A user, or actually the node with the IP interface, can also continue to use an IP address outside the sub network to which it belongs. A roaming node that enters a foreign network is associated with a c/o address provided by a foreign agent (FA). In the home network, a home agent (HA) establishes an IP tunnel to the FA using the c/o address. Any packet sent to the roaming nodes address is first sent to the home agent, which forwards it to the FA via the c/o address (tunneling). The FA then decapsulates the packet and sends it to the roaming node using the original (home) IP addresses. The actual routing in the fixed network is not affected by this tunneling method and can use traditional routing protocols such as open shortest path first (OSPF), the routing information protocol (RIP), and the border gateway protocol (BGP). This forwarding approach is appropriate in cases where only the nodes (terminals) at the very edges of (fixed) networks are moving. However, in an ad hoc network, this is not the case, since the nodes at the center of the network can also move or rather, the whole network is based on the idea of devices that serve both as routers and hosts at the same time. Hence, in an ad hoc network, mobility is handled directly by the routing algorithm. If a node moves, forcing traffic another way, the routing protocol takes care of the changes in the nodes routing table.

In many cases, inter working can be expected between ad hoc and fixed networks. Inter working would make it possible for a user on a trip who takes part in a laptop conference but wants mobility, to be reachable via the fixed IP network. Moreover, since the user wants to be reachable from the fixed network, mobile IP would be a convenient way of making him reachable through the fixed IP network. If the user is located several radio hops away from the access point, mobile IP and the ad hoc network routing protocol must inter work to provide connectivity between the traveling user and his unit peer node which is located in the fixed network or in another ad hoc network.

3.11.3 Routing: Each node in an ad hoc network participates in forming the network topology. As there are no dedicated routers, each node is on its own part responsible for routing packets between other nodes, too. Basically the routing infrastructure is yet similar to the one of Internet. There are many different routing protocols that provide information to forward packets to the next hop. In ad hoc network it would be necessary to manage topology changes, as all the nodes are required to run routing protocols. The routing protocols used in Internet are typically not applicable to ad hoc networks as such.

In general, mobility, dynamic topologies, and the constraints of power and bandwidth in ad hoc wireless networks have given the guidelines for routing protocol development. As nodes in a MANET usually have to deal with limited power resources, it is suitable to develop such protocols that need minimum amount of information exchanges, thus minimizing radio communication and also power consumption.

The Internet routing protocols are based on network broadcast, as is the case with common Open Shortest Path First (OSPF) protocol. OSPF is a link-state protocol, which means that the routing tables are sent to everyone. These traditional link-state protocols are not applicable for dynamic networks, because a considerable amount of bandwidth is needed to maintain network state. Instead of being link-state protocols, most of the routing protocols use distance vector algorithms, which send their routing tables only to neighbors.

The complexity of the Ad Hoc routing problem is reflected in the volume of research currently being conducted, no less than six different schemes are being researched. Basically there are two types of routing protocols:

Proactive Routing Protocols: Herein the nodes keep updating their routing tables by periodical messages. This can be seen in Optimized Link State Routing Protocol (OLSR) and the Topology Broadcast based on Reverse Path Forwarding Protocol (TBRPF).

Reactive or On Demand Routing Protocols: Here the routes are created only when they are needed. The application of this protocol can be seen in the Dynamic Source Routing Protocol (DSR) and the Ad-hoc On-demand Distance Vector Routing Protocol (AODV).

In today's world the most common ad-hoc protocols are the Ad-hoc On-demand Distance Vector routing protocol and the Destination-Sequenced Distance-Vector routing protocol and the Dynamic Source Routing. All these protocols are quite insecure because attackers can easily obtain information about the network topology. This is because in the AODV and DSR protocols, the route discovery packets are carried in clear text. Thus a malicious node can discover the network structure just by analyzing this kind of packets and may be able to determine the role of each node in the network. With all this information more serious attacks can be launched in order to disrupt network operations.

The Dynamic Source Routing (DSR) protocol is a purely reactive protocol. Every packet contains an ordered list of intermediate routing nodes, every node maintains a route cache, and if a route does not exist in the cache, a "route request" packet is broadcast and propagated along until it hits the destination, or a node which knows of the destination, upon which a reply packet is send to the requesting node. Intermediate nodes add their address along the way, and update their caches with eavesdropped routes. Routes are maintained by watching for lost packets, upon which another route discovery must be performed.

The Ad hoc On Demand Distance Vector (AODV) protocol, proposed by Perkins, blends elements of the DSR and DSDV protocols, using the DSR reactive route discovery and maintenance models, in combination with the sequence number and periodic update features of the DSDV protocol.

3.12. Applications of Mobile ad-hoc Networks

Ad hoc networking protocols allow building of self-configuring multi hop wireless networks. The concept in itself is generic and can be used in several application areas. Ad hoc networking is a critical enabling technology to some of the applications, such as sensor networks, where as others, e.g., fixed wireless broadband access networks can operate more efficiently using ad hoc networking protocols.

In general the use of ad hoc also known as mesh networking or multi hop wireless networking increases the spectral efficiency of communications, thus increasing the communications capacity of the network and allowing higher speeds for an individual user. At the same time use of multiple wireless hops decreases the power consumption required for sending data when compared to sending the data directly between communication end points, i.e., a mobile terminal and a wireless access point. The use of ad hoc protocols allows the networks to be self-configurable, decreasing the amount of configuration needed to set up a network. These theoretical characteristics make ad hoc networking a disruptive technology. However, in practice these advantages cannot be fully exploited due to limitations in radio technologies and routing protocols, but offer still notable benefits in certain application areas.

Also the requirements on networking differ depending on the application area. In mobile networking the computers, ad hoc network nodes, have limited computational and storage capabilities, and battery life is also limited. Spectral efficiency and communications overhead should be minimized for scalable and efficient operation. With fixed access, battery life is not an issue, but spectral efficiency and minimal communications overhead are critical for large-scale deployment. With vehicle networks the protocols need to be able to deal with very fast moving mobile nodes. The most challenging applications are in the military, where in addition to the above-mentioned challenges the adversary will try to disrupt and eavesdrop communications.

The application areas are overlapping, but have clearly separate markets. For example fixed broadband access technologies and mobile data services overlap to some degree, especially for portable access to the Internet. Still the two applications have at least for now separate markets, e.g., home and corporate Internet access for desktop computers using fiber, DSL and cable modems and on the other hand GPRS and the emerging 3G WAN and IEEE 802.11 LAN mobile data services. As speed for mobile data access increases, these two markets may merge to some degree at least for the corporate segment, in which the cost is not as big an issue, as in the residential segment.

Mobile data services can be seen to include also vehicular networks where computers in vehicles communicate with other vehicles and also with computers located in the Internet. However, the vehicle-to-vehicle communication distinguishes this application from normal mobile Internet access.

The figure below classifies potential applications of ad hoc networking based on the mobility of the nodes in the network and the size of the network. The technological challenges become more demanding as these parameters increase.

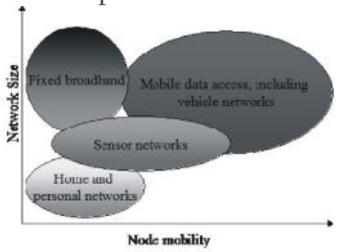

Network Size
Fixed broadband
Mobile data access, including vehicle networks
Sensor networks
Home and personal networks
Node mobility

Fig 2.6: Applications for ad hoc networking

In order to illustrate the concept of ad hoc network, the following application can be considered. The application is referred to as the ubiquitous flea market. An important characteristic of traditional flea markets is that they are only available on a certain day and time. Then, walking around takes time and energy, as one has to carefully scrutinize what is available. And finally, the different roles (buyer and seller) are clearly separated. The ubiquitous flea market is available wherever we are and at all time. It is available on many mobile devices and matches buyers and sellers present within a certain range, the latter being previously defined by the user. While walking, driving or flying, this ad hoc network can be used. scans its surroundings for possible peer sellers or buyers. It has to be noted that any user can be buyer and/or seller. When the application finds another mobile device that runs the same piece of software, it scans the shared items in order to find a matching one. If there is a match, the user is alerted and can then ask the peer to get in touch and make the physical transaction. All this, in a matter of simplification, is based on a shared and known taxonomy describing the items that can be bought and sold. The following user case diagram helps to have a better idea of the fundamental features of our ubiquitous flea market

3.12.1 Military Applications: The origin of networks that rely on no pre-existing infrastructure can be traced back to the early 1970s with the DARPA and PRNET projects where the initial focus was on military applications. The application of ad hoc networks in a military environment is particularly attractive because of their lack of infrastructure and self-organizing nature. Consider conventional networks that rely on infrastructure such as base stations: the infrastructure introduces points of vulnerability, which may be attacked, and, if eliminated, dismantle the operation of the entire network. In battlefield scenarios robust and guaranteed communication is essential with potentially fatal consequences if compromised. Ad hoc networks can continue to exist even in the event of nodes disappearing or becoming disconnected due to poor wireless connectivity, moving out of range, physical attack on users, broken nodes, battery depletion or physical node damage. Applications such as sensor networks positional communication systems and tactical ad hoc networks will continue to be one of the driving forces behind ad hoc network development.

3.12.2 Commercial Applications: Commercial applications of ad hoc networks may include deployment of connectivity in terrains where conventional networks, such as cellular networks, are not financially viable, cannot provide sufficient coverage or need bypassing. Private networks or personal area networks (for the purpose of teleconferencing, video conferencing, peer-to-peer communications, ad hoc meetings, or more generally, collaborative applications of all kinds) are possible applications of ad hoc networks. It is anticipated that these applications will gain momentum as soon as the flexibility and convenience of self-organized ad hoc networking is fully appreciated and protocols are implemented with commercially available products. Take for example cellular networks, what was once seen, as an impractical technology has now become a necessity.

Emergency situations caused by geopolitical instability, natural or man-made disaster could result in existing networking infrastructure being damaged or unreliable. For example, Hurricane Katrina struck New Orleans, Louisiana on August 29, 2005. The storm destroyed most of the fixed communication infrastructure as it blanketed approximately 90,000 square miles of the Unites States, a region almost as large as the United Kingdom. In order to launch an effective disaster relief operation, communications of the essence, even between a localized group of relief workers. “Open” MANETs will make it possible for relief workers from various countries to establish communication on the fly, therefore eliminating the time penalty in setting up and managing conventional, fixed infrastructure networks. Search and rescue missions could also be conducted in locations not allowing access to existing communication networks. Vehicular ad hoc networks allow vehicles traveling along a highway to exchange data for traffic congestion monitoring, inter vehicle communication and early warning of potential dangers ahead such as an accident, road obstruction or stationary vehicle. Several research projects have been initiated to deal with vehicular ad hoc networking.

3.12.4 Extending Cellularmobile Access Networks: Mobile ad hoc networking can be used for extending the coverage of a cellular mobile network. This allows mobile users to access the network even when they are outside the range of any base station. The use of multiple hops between a mobile node and a base station improves the signal quality, which either increases the data rate or decreases the required transmission power.

The cellular network in question can be, e.g., a CDMA or an IEEE 802.11 WLAN network. For example a user surfing the web in an Internet cafe with his laptop computer and a WLAN card could also provide access to other users outside the range of the cafeteria's WLAN access point.

The products and protocols developed for fixed broadband wireless access could possibly also be employed for mobile or at least portable Internet access. However, mobile use leads to a frequently changing network topology. Changes in the network topology pose challenges to any routing protocol used in the network. The amount of routing protocol related signaling makes large-scale flat mobile ad hoc networks impractical. To overcome this limitation, a clustered or hierarchical approach presented is needed. The fixed wireless network would then form the backbone network to which mobile nodes could attach through a small number of hops via other mobile nodes.

3.12.5 Personal Area Network: The concept of personal area networks is about interconnecting different devices used by a single person, e.g. a PDA, cellular phone, laptop etc. In this case the PDA or the laptop will connect with the cellular phone in an ad hoc fashion. The cellular phone can then as an example be used to access Internet. Another example could be when a person holding a PDA comes within communication range of a printer. If both the PDA and the printer were ad hoc enabled the PDA could automatically get access to the printing services.

3.12.6 Sensor Networks: Sensor networks are ad hoc networks consisting of communication enabled sensor nodes. Each such node contains one or more sensors, e.g. movement-, chemical- or heat sensors. When a sensor is activated it relays the obtained information trough the ad hoc network to some central processing node where further analysis and actions can be performed. Such sensor networks may consist of hundreds or thousands of sensors and can be used in both military and non-military applications, e.g. surveillance, environmental monitoring etc. Sensor networks differ significantly from the other types of ad hoc networks described in this section. The most significant difference is the small size, extremely limited power resources and processing power of the sensor nodes.

3.12.7 Collaborative Networking: This application of ad hoc networking may be the most intuitive. The simplest example is when a group of people are attending a meeting and need to share information between their laptops or PDAs. If these devices were ad hoc enabled they could dynamically set up a network consisting of the meeting participants and thus enable the sharing of the information.

Without ad hoc networking, a great deal of configuration and setup would be required to accomplish this task.

3.12.8 Disaster Area Networks: Ad hoc networking allows for the quick deployment of a communication network in areas where no fixed infrastructure is available or where the fixed infrastructure has been destroyed by natural disasters or other events. Thus such networks could be used to improve the communication among rescue workers and other personnel and thereby support the relief efforts.

3.13. Adhoc Routing-Approach

An ad-hoc network is a collection of wireless devices (or nodes) dynamically forming a network without using any pre-defined infrastructure. For example, soldiers relaying information for situational awareness on a battle field and personnel coordinating rescue relief operations after a disaster such as an earthquake. The goal of an ad-hoc network is to enable communication between any two wireless connected nodes in the network. Communication between nodes that are beyond direct communication range is enabled by using intermediate nodes in the network as forwarding agents.

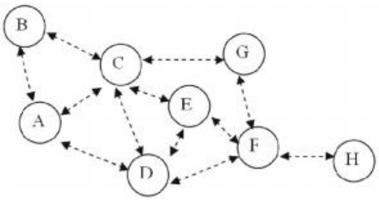


Fig2.1: A wireless Ad Hoc Network

In ad hoc networks, each node act as a router and the routes are mostly multi hop. Nodes in these network moves arbitrarily, thus network topology changes frequently, unpredictably, and may consist of unidirectional links as well as bi-directional links. Each node in these networks operates on constrained battery power, which eventually gets exhausted with time. Ad hoc networks are also more prone to security threats and misbehaving. All these limitations and constraints make Ad Hoc network research more challenging.

3.14. Properties of Mobile adhoc Networks

Mobile ad hoc networks exhibit properties different from fixed networks or infrastructure based wireless networks. These properties make it harder to implement security services or even exhibit vulnerabilities to different and additional security attacks:

- ➢ Unreliable wireless links are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping.
- ➢ Constraints in
  - ❖ Bandwidth is caused by the limits of the air interface with fading and noise.
  - ❖ Computing power in mobile devices require security mechanisms to be low in computation overhead.
  - ❖ battery power in mobile devices can lead to application specific trade-offs between security and longevity of the device
- ➢ Mobility/Dynamics make it hard to detect behavior anomalies such as advertising bogus routes since routes in this environment change frequently. It is difficult to employ mechanisms like firewalls, because the border between being inside or outside the network is blurred.
- ➢ Self-organization is a key property of ad hoc networks. They can not rely on central authorities and infrastructures. Therefore, trust management has to be distributed and adaptive [13]. On the bright side, self-organization leads to inherent better fault tolerance thanks to the absence of the potential bottleneck of centralized authorities.
- ➢ Latency is increased by the fact that in order to save battery power devices can decide to sleep and only wake up, when there is a message for them, which increases the reaction time of the device by the time it takes to wake up. Inherently the round-trip-time for packets is increased in wireless multi-

hop networks, rendering message exchange for security more expensive.

- Multiple paths are likely to be available given sufficient node density. [45] This property offers an advantage over infrastructure-based local area networks that can be exploited by diversity coding. This means that multiple copies of a packet or parts of it can be sent over different paths to increase the probability of a packet actually arriving at a destination unchanged.

3.15. Problem Issues in ad hoc Management

The major factor in Ad Hoc management is the node misbehavior. Although a efficient power management scheme is applied to an ad hoc network, a misbehaving node may result in the improper routing of packet which may extend to the complete collapsing of the network also. In mobile ad-hoc networks, where nodes act as both routers and terminals, the nodes have to cooperate to communicate. Cooperation at the network layer takes place at the level of routing, i.e. finding a path for a packet, and forwarding, relaying packets for other nodes. Misbehavior arises for several reasons such as, when a node is faulty; its erratic behavior can deviate from the protocol and thus produce non intentional misbehavior. Intentional misbehavior aims at providing an advantage for the misbehaving node. An example for an advantage gained by misbehavior is power saved when a selfish node does not forward packets for other nodes. Depending on the amount of misbehaving nodes and their specific strategies, network throughput can be severely degraded, packet loss increases, nodes can be denied service, and the network can be partitioned. These detrimental effects of misbehavior can endanger the functioning of the entire network.

3.16. Routing Protocols in ad hoc Networks

A number of routing protocols have been proposed for MANETs. These protocols can be classified into three different groups: global/proactive, on demand/ reactive and hybrid. In proactive routing protocols, the routes to all the destination (or parts of the network) are determined at the start up, and maintained by using a periodic route update process. In reactive protocols, routes are determined when they are required by the source using a route discovery process. Hybrid routing protocols combine the basic properties of the first two classes of protocols into one. That is, they are both reactive and proactive in nature. Each group has a number of different routing strategies, which employ a flat or a hierarchical routing structure.

3.17. Proactive Routing Protocols

In proactive routing protocols, each node maintains routing information to every other node (or nodes located in a specific part) in the network. The routing information is usually kept in a number of different tables. These tables are periodically updated and/or if the network topology changes. The difference between these protocols exists in the way the routing information is updated, detected and the type of information kept at each routing table. Furthermore, each routing protocol may maintain different number of tables.

A number of different PROACTIVE routing protocols are: Destination-sequenced distance vector (DSDV), Wireless routing protocol (WRP), Global state routing (GSR), Source-tree adaptive routing (STAR), Cluster-head gateway switch routing (CGSR), Optimized link state routing (OLSR) etc.

3.18. Reactive Routing Protocols

On-demand routing protocols were designed to reduce the overheads in proactive protocols by maintaining information for active routes only. This means that routes are determined and maintained for nodes that require sending data to particular destination. Route discovery usually occurs by flooding a route request packet through the network. When a node with a route to the destination (or the destination itself) is reached a route reply is sent back to the source node using link reversal if the route request has traveled through bi-directional links or by piggy-backing the route in a route reply packet via flooding. Reactive protocols can be classified into two categories: source routing and hop-by-hop routing. In Source routed on-demand protocols, each data packets carry the complete source to destination address. Therefore, each intermediate node forwards these packets according to the information kept in the header of each packet. This means that the intermediate nodes do not need to maintain up-to-date routing information for each active route in order to forward the packet towards the destination. Furthermore, nodes do not need to maintain neighbor connectivity through periodic beaconing messages. The major drawback with source routing protocols is that in large networks they do not perform well.

This is due to two main reasons; firstly as the number of intermediate nodes in each route grows, then so does the probability of route failure.. Secondly, as the number of intermediate nodes in each route grows, then the amount of overhead carried in each header of each data packet will grow as well. Therefore, in large networks with significant levels of multihoping and high levels of mobility, these protocols may not scale well. In hop-by-hop routing (also known as point-to-point routing) [8], each data packet only carries the destination address and the next hop address. Therefore, each intermediate node in the path to the destination uses its routing table to forward each data packet towards the destination. The advantage of this strategy is that routes are adaptable to the dynamically changing environment of MANETs, since each node can update its routing table when they receive fresher topology information and hence forward the data packets over fresher and better routes. Using fresher routes also means that fewer route recalculations are required during data transmission. The disadvantage of this strategy is that each intermediate node must store and maintain routing information for each active route and each node may require to be aware of their surrounding neighbors through the use of beaconing messages. A number of different reactive routing protocols have been proposed, they are: Ad hoc on-demand distance vector (AODV), Dynamic source routing (DSR), Temporally ordered routing algorithm (TORA), Associatively-based routing (ABR), Ant-colony-based routing algorithm (ARA), Cluster-based routing protocol (CBRP) etc.

3.19. Hybrid Pouting Protocols

Hybrid routing protocols are a new generation of protocol, which are both proactive and reactive in nature. These protocols are designed to increase scalability by allowing nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads. This is mostly achieved by proactively maintaining routes to near by nodes and determining routes to far away nodes using a route discovery strategy. Most hybrid protocols proposed to date are zone-based, which means that the network is partitioned or seen as a number of zones by each node. Others group nodes in to trees or clusters. A number of different hybrids routing protocol proposed for MANETs are: Zone routing protocol (ZRP), Zone-based hierarchical link state (ZHLS), Scalable location update routing protocol (SLURP), Distributed spanning trees based routing protocol (DST), distributed dynamic routing (DDR).

3.20. Dynamic Source Routing (DSR)

Misbehavior detection systems for mobile ad-hoc networks have mostly built on Dynamic Source Routing (DSR), monitoring node behavior with a watchdog component. DSR is a protocol developed for routing in mobile ad-hoc networks and was proposed for MANET by Broch, Johnson and Maltz [6]. In a nutshell, it works as follows: Nodes send out a route request message, all nodes that receive this message forward it to their neighbors and put themselves into the source route unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a reply message containing the full source route. It may send that reply along the source router in reverse order or issue a route request including the route to get back to the source, if the former is not possible due to asymmetric links. route reply messages can be triggered by route request messages or gratuitous. After receiving one or several routes, the source picks the best (by default the shortest), stores it, and sends messages along that path. In general, the better the route metrics (number of hops, delay, bandwidth or other criteria) and the sooner the REPLY arrived at the source (indication of a short path - the nodes are required to wait a time corresponding to the length of the route they can advertise before sending it in order to avoid a storm of replies), the higher preference is given to the route and the longer it will stay in the cache. In case of a link failure, the node that cannot forward the packet to the next node sends an error message toward the source. Routes that contain a failed link can be 'salvaged' by taking an alternate partial route that does not contain the bad link.

Chapter 04 MANETs Quality Metricls & Analysis

Minimizing energy consumption is the important challenge in mobile networking. Wireless network interface is often a device's single largest power consumer. Since the network interface may often be idle, turning the radio off when not in use could save this power. In practice, however, this approach is not straightforward. A node must arrange to turn its radio on not just to send packets, but also to receive packets addressed to it and to participate in any higher-level routing and control protocols. The requirement of cooperation between power saving and routing protocols is particularly acute in the case of multi-hop ad hoc wireless networks, where nodes must forward packets for each other.

4.1. Issues in Topology Management

The absence of a central infrastructure implies that an ad hoc network does not have an associated fixed topology. Indeed, an important task of an ad hoc network consisting of geographically dispersed nodes is to determine an appropriate topology over which high-level routing protocols are implemented. In this section, we consider topology management, the problem of determining an appropriate topology in an ad hoc network. Let V denote the collection of nodes and let G denote the graph on V in which there is an edge from node u to node v if and only if u can directly reach v. Let T denote the topology returned by the topology management algorithm.

The quality of the topology T can be evaluated according to several criteria, which are

1. Connectivity
2. power-efficiency
3. throughput
4. robustness to mobility.

In the remainder of this section, we elaborate on these measures.

4.1.1. Connectivity and Energy-Efficiency: Perhaps, the most basic requirement of topology is that it be connected. More precisely, we require that any two nodes that are connected in G are also connected in T. Since the topology T forms the underlying network for routing protocols, it is also desirable that there exist power-efficient paths between potential source-destination pairs.

We would like to provide connectivity and power-efficiency using a "simple" topology that is "easy" to maintain. While there is no single way to formalize "simplicity" and "”maintainability", some objective measures that influence these subjective goals are the size of the topology in terms of the power level of nodes in T, number of edges in T and the maximum degree of any node in T. What distinguishes the topology management problem in the mobile ad hoc setting from traditional network design is that we need to determine the topology in a completely distributed environment. Thus the every node in an ad hoc network should take decisions locally based on information obtained from neighbors.

4.1.2. Throughput: In addition to connectivity and energy-efficiency, we would like to have a topology with high capacity or throughput; that is, it must be feasible to route "about as much traffic" in the topology as any other topology, satisfying the desired constraints. The throughput-competitiveness of a topology depends on, among other factors, the level of interference inherent to the topology. Define the interference number of an edge e in T to be the maximum number of other edges in T that interfere with e. Define the interference number of the topology to be the maximum interference number of an edge in T. A plausible goal then is to seek a topology with a small interference number. The particular interference number achievable, however, depends on the relative positions of the ad hoc network nodes and their transmission radii. This leads to the following open problem in network design: Given a collection of ad hoc network nodes, design a connected topology that minimizes the interference number. It seems unlikely that the preceding optimization problem can be solved effectively by a local algorithm; nevertheless, a centralized algorithm for the problem may be of theoretical interest.

4.1.3. Robustness to Mobility: An additional challenge in the design of distributed topology management algorithms is to ensure some degree of robustness to the mobility of nodes. One measure of robustness of the topology is given but the maximum number of nodes that need to change their topology information as a result of a movement of a node. The number, which may be referred to as the adaptability of the topology management algorithm, depends on the size of the transmission neighborhood of the mobile node u, and the relative location of the nodes, Other than maintaining the topology, mobility also entails changes in the routing paths.

4.2 Topology Managemnt in Wireless ad-hoc Networks

The topology management in Ad hoc wireless networks is decided at every node

- Which node to turn on
- When the node to be turn on
- What should be the transmit power, So that network connectivity is maintained under the conditions of mobility.

Most of the algorithms proposed for Topology Management which are based on the first two points or the third point i.e. switching between active (transmit, receive or idle) to the transmission power. They are:

- Power On-off scheduling algorithms
- Power scheduling algorithms

In on-off management scheme, few nodes are having more power, which are called as cluster heads and gateways. These are selected distributively in such a way that each node in the Ad hoc wireless network is either cluster head or connected to cluster head. The gate way nodes are selected such that they forward packets between cluster heads. Here any node can send packets to any other node in the network through cluster heads and gateways. Thus the cluster heads and gateways form a virtual backbone to the rest of nodes. The packets destined to the nodes in the sleep mode can be buffered at its cluster head. When the node wakes up cluster head can deliver the packets to the node. The cluster node and gateway nodes are always in awake mode. Some proposed on off scheduling topology management schemes are Span (3) and TMPO (Topology Management by Priority Ordering) (4).

In the power scheduling topology management schemes, each node adjusts its transmission range in such a way that it has few neighbors. In this topology management scheme all nodes take part in the routing, it is called as flat topology management scheme. Few power scheduling topology management schemes are CBTM (Cone Based distributed Topology Management) (Rohl et al., 1997) and K_Neigh Protocol for symmetric topology control (Bao and Garcia-Luna-Aceves, 2003).

Span (3), a power saving technique for multi-hop ad hoc wireless networks that reduces energy consumption without significantly diminishing the capacity or connectivity of the network. Span builds on the observation that when a region of a shared-channel wireless network has a sufficient density of nodes, only a small number of them need be on at any time to forward traffic for active connections.

Span is a distributed, randomized algorithm where nodes make local decisions on whether to sleep, or to join a forwarding backbone as a coordinator. Each node bases its decision on an estimate of how many of its neighbors will benefit from it being awake, and the amount of energy available to it. In this algorithm coordinators rotate with time, demonstrating how localized node decisions lead to a connected, capacity-preserving global topology.

Improvement in system lifetime due to Span increases as the ratio of idle-to-sleep energy consumption increases. Here the system life time of 802.11 network in power saving mode with span is a factor of two better than with out. Span integrates nicely with 802.11- when run in conjunction with the 802.11 power saving mode, span improves communication latency, capacity and system lifetime.

But this algorithm implementation is extremely expensive. The implementation of the power saving technique periodically wakes up the nodes and makes them to listen to the advertisements and this will increase the cost. This warrants investigation into a more robust and efficient power saving technique in MAC layer that minimizes the amount of time each node spends in power saving mode.

TMPO (4) uses the neighbor-aware contention resolution (NCR) algorithm to provide fast convergence and load balancing with regard to the battery life and mobility of mobile nodes. Based on NCR, TMPO assigns randomized priorities to mobile stations, and elects a minimal dominating set (MDS) and the connected dominating set (CDS) of an ad hoc network according to these priorities. In doing so, TMPO requires only two-hop neighbor information for the MDS elections. The dynamic priorities assigned to nodes are derived from the node identifiers and their willingness to participate in the backbone formations. The willingness of a node is a function of the mobility and battery life of the node. The integrated consideration of mobility, battery life and deterministic node priorities makes TMPO one of the best performing heuristics for topology management in ad hoc networks.

In CBTM (Rohl et al., 1997), the topology of a wireless multihop network can be controlled by varying the transmission range at each node. This algorithm does not assume that nodes have GPS information available; rather it depends only on directional information. Roughly speaking, the basic idea of the algorithm is that a node u transmits with the minimum power p required to ensure that in every cone of degree d around u, there is some node that u can reach with power p, where d = 5pi/6 is a necessary and sufficient condition to guarantee that network connectivity is preserved. More precisely, if there is a path from s to t when every node communicates at maximum power then, if d < 5pi/6, there is still a path in the smallest symmetric graph G containing all edges (u,v) such that u can communicate with v using power p. On the other hand, if d > 5pi/6, connectivity is not necessarily preset

It has the disadvantages that eliminating edges may result in more congestion and, hence, worse throughput, even if it saves power in the short run. The right tradeoffs to make are very much application dependent. Therefore, an algorithm that adapts to the specific application setting is much needed. Reconfiguration in response to node mobility and failure consumes precious energy resources. Fast convergence of topology control is critical to keep the network functioning well.

K-Neigh Protocol (Bao and Garcia-Luna-Aceves, 2003): This approach is based on the principle of maintaining the number of physical neighbors of every node equal to or slightly below a specific value k. The proposed approach enforces symmetry on the resulting communication graph, thereby easing the operation of higher layer protocols. The value of k guarantees connectivity of the communication graph with high probability both theoretically and through simulation. K-Neigh, a fully distributed, asynchronous, and localized protocol that uses distance estimation, guarantees logarithmically bounded physical degree at every node, is the most efficient known protocol (requiring 2n messages in total, where n is the number of nodes in the network), and within strictly bounded time. But it fails when the nodes join the network at unpredictable times, and cannot deal with mobility.

Chapter 05 Mobile ad hoc Routing Intelligence protocol

5.1. Proposed Routing Protocol

In a mobile adhoc network discovering a route and its maintenance is of prime importance for maintaining the network performance for a longer time. To maintain the network performance a mobile adhoc routing intelligence (MARI) protocol is proposed. When the node awakens, it can retrieve these packets from the buffering MARI node. This scheme makes the routing simple, with minimum number of entries as only those entries in a node's routing table that correspond to currently active MIRA nodes can be used as valid next-hops.

5.2. Mobile adhoc Routing Intelligence Protocol

MARI nodes are the nodes such that all non-MARI nodes (nodes within the transmission range of that MARI node) are connected to any one of the MARI node and route packets for any other nodes with the help of Mobile Agents. The route consists of Source node, Corresponding MARI node, Gate way nodes and intermediate MARI and Gateway nodes and destination node.

For the operation of routes in the network a sleep cycle is used to maintain the power level. A Sleep cycle is defined as a period for the time period during which member nodes remain in the power efficient sleep mode and wake up once in fixed time duration in one beacon period.

We assume that each node periodically broadcasts a small packet "HELLO" message, which contains:

Node id

- It's Status (whether the node is MARI node, gateway, member or undecided)

- Its current power level
- Its current MARI node
- A wakeup counter wi
- Information about each neighbor i.e.:
    - Neighbor's id,
    - Its status,
    - Its MARI node.

Based on the HELLO message received from the neighbors, each node constructs a table, which contains the list of its neighbors, their MARI nodes, power level, wakeup counter and the information about their neighbors. A node switches form time to time between being a MARI node and being a member. A node becomes a gateway, if its MARI node chooses it as a gateway to route the packets between MARI nodes. A node is said to be kept in the undecided state, if it looses the connectivity with its MARI nodes due to mobility. The following sections describe the selection of MARI nodes, their withdrawal and the selection of gateways.

5.3. Mari Placement

MARI nodes along with gateways confirm a path in the virtual backbone, which is used for routing and there is demands for additional power for transmission, reception and processing of packets. Thus the MARI nodes should be selected in such a way that they have enough/higher power level.

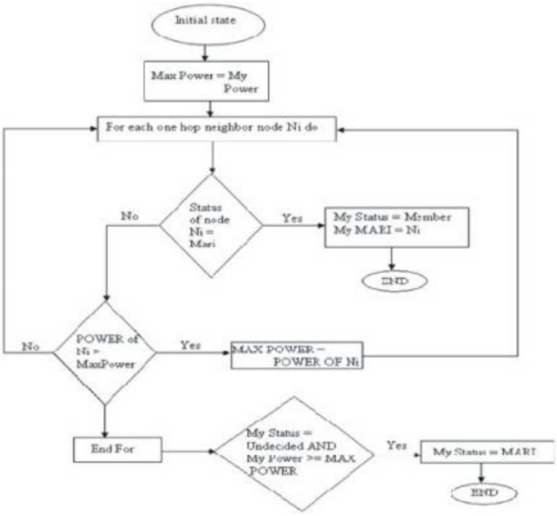
ALGORITHM 1: (MARI PLACEMENT, executed by undecided nodes)

```
MAXPOWER = My power
for Each one hop neighbor node Ni do
if Status of node Ni is MARI then
My status = member
My MARI = Ni
else
```

```
if Power of Ni > MAXPOWER then
MAXPOWER = POWER OF Ni
end if
end if
end for
if My status = undecided AND My power >=
MAXPOWER then
My status = RIMA
        end if
```

- Undecided nodes periodically checks if it has a maximum POWER level among its one hop neighbors which have not joined to any MARI node (i.e. undecided neighbors). If a node has maximum power level among such one hop neighbors, it becomes a MARI node and declares itself as a MARI node in the status field of next HELLO message and communicates to all its neighbors.
- If undecided node knows that its neighbor node has become MARI node from received HELLO message, it changes it's status to member. It declares its status as member and it's current MARI node in next HELLO message. If more than one neighbors of an undecided node became MARI, undecided node select its MARI node from which it has received the HELLO packet earlier
- There may be undecided nodes whose one hop neighbors with power level more than the undecided node chose to join MARI nodes, as the MARI nodes have more power level than its one hop neighbors. Such undecided nodes with maximum power level among one hop undecided neighbors declares themselves as MARI nodes in the next HELLO message.
- A MARI node prepares a list of its member nodes, which are joined to the MARI node, form the broadcast of HELLO messages received from one hop neighbors. This information

in the table is periodically changes as a new HELLO packet is received.



Flow Chart 1: Mari Placement

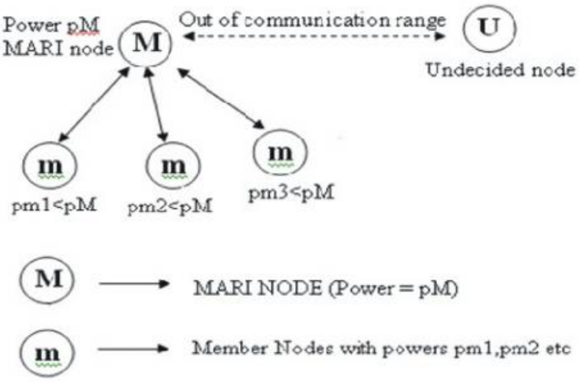


Fig 4.1: Illustration of MARI node selection in a Random Ad Hoc Network

5.4. Mari Node With Drawal

The MARI node will drain its energy more rapidly, as compared to member nodes. Before the MARI node loses its major part of its power, the responsibilities of the MARI node should be transferred to other node with sufficient power level. Also RIMA nodes should not be changed frequently which will increase the overhead.

- When a MARI node observes that its POWER level is gone below a threshold, it will withdraw its status of MARI node. The withdrawal of MARI node is declared to its member nodes in the next WAKEUP message as a undecided node. The threshold can be set to 80% of MARI level when the node decided to become a MARI node.
- When a gate way or member node comes to know that it can not contact its MARI node, it changes its status to undecided and starts MARI node placement procedure.

5.5. Gateway Selection

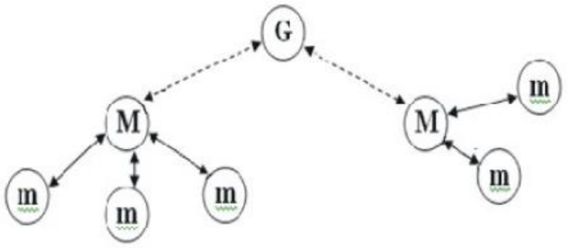
The maximum number of hops between any two close MARI nodes is two; hence gateways are required and are used to forward the packets between the MARI nodes. The gateway nodes must have sufficient amount of power, to transmit and receive the packets to and from the MARI nodes.

ALGORITHM 2: (Gateway Selection, executed my MARI nodes)

```
Transmit broadcast packet STAY-AWAKE
Wait for one beacon period
for Each RIMA node Ri within two hops do
If Ri has not decided gateway for this RIMA node then
If Ri is not neighbor of my existing gateways then Ri.
Gateway = My member which has maximum power among neighbors of Ri
else
Ri. Gateway = my existing gateway
end if
else
Ri. gateway = gateway of Ri for this node
```

```
    end if
    end for
```

- To determine the gateways, MARI nodes needs information in its two hop neighborhood. This information is obtained from the HELLO packets; it has received from its one hop neighbors. But as the member of different MARI nodes are not synchronized, they may miss the HELLO packets from members of different MARI nodes. MARI node periodically sends broadcast request packet STAY AWAKE to its members to put them in awake mode for at least one beacon period.
- MARI node finds out all the MARI nodes within two hops and MARI node selects its member as a gateway which has maximum power level, for each MARI node within two hops. Generally the gateway is taken such that it has more number of neighbors to ensure less number of gateways.
- If any MARI node within two hops have already declared their gateways, then there is no need to select gateway for such MARI node.
- The MARI node determine the validity of the gateway node i.e., power level periodically, if the power level is below the threshold level the MARI node starts the selection procedure for new gateway.



M – MARI Nodes, m – Member Nodes, G – Gateways

Fig 4.2: Gateway selection and flow in Ad Hoc Network

5.6. Scheduling of Sleep Cycle

We propose some additional POWER saving features to 802.11 CSMA/CA to make the MAC layer power efficient by using randomized wake up time for member nodes in ad hoc network. MARI nodes and Gateways continuously stay awake to forward packets of other nodes. Member nodes wake up a number of times in a beacon period T (see figure 4.2), and if they do not have to transmit or receive data, they goes to sleep again. There are number of sleep cycle periods (T1, T2), (T2, T3) … (Tn, T) in a beacon period. Member nodes wakes up once in a sleep cycle. All nodes stays awake during period (0, T1) called as broadcast window to exchange HELLO packets. Each node synchronizes its clock by using time stamp of HELLO message from MARI node. Each member node determines its wake up time from its node id and a wakeup counter wi given below (see algorithm 3):

ALGORITHM 3: (Sleep cycle scheduling, executed by all member nodes for each beacon Period)

```
Transmit HELLO packet at appropriate time in (T,T1)
For Each sleep cycle period (Tm, Tm+1), m = 1…n
do
    if there are no packets to transmit then
        Go to sleep mode until time tim
        Remain in wake up mode until time tim +t
        if Packet received at time in (tim, tim + t) then
            Remain in wake up mode until time + t
        end if
        if time < Tm+1 – T then
            Go to sleep mode until time Tm+1
        end if
    else
        Transmit the packet (s) at appropriate time(s)
        if tim – t<time < tim then
```

```
Remain in wake up mode until time tim+t for receiving
packets
end if
if time < Tim + t then
Remain in wake up mode until time + t
end if
end if
if time <Tm+1 – t then
Go to sleep mode until time Tm+1
end if
end if
end for
```

- During the initial period (0,T1) of the beacon period (0,T), all node remain awake, transmit broadcast messages, if any, and beacon messages so as to keep every node undated about one hop neighborhood. We call the period (0,T1) as broadcast window. Thus when a packet, other than HELLO and broadcast, comes at MAC layer for transmission during broadcast window, the packet can not be sent immediately. The packet has to be buffered at the MAC layer and it will be transmitted after the end of broad cast window
- At the end of broadcast window, i.e., at time T1, all member nodes go to sleep mode, if the node do not have any packets for transmission. Each member node with id I wakes up at time tim in mth sleep cycle. Node I calculates its wake up time tim for a pseudo-random number with its node id I and a wakeup counter wi as seed to the pseudo-random number generator. Wake up time of a node with id I in mth is given by tim.

$$tim = Tm + (Tm+1 – Tm) * Ran$$

Where Rand (I x wi) is pseudo-random number in (0, 1) with

I * wi as seed.

- This wake up time tim is also known to MARI node and one hop neighbors of node I as each node knows its one hop neighbor id and its wakeup counter wi from HELLO packet. All the nodes in ad hoc network have identical pseudo-random number generator. So when a MARI node or neighbor of node I wants to send packets to node I, it will send at time tim. After the node I receive packets, it goes to sleep again. So for MARI node and neighbors of node I, the packets have to be buffered at MAC layer until time tim. After a small time tim, if no packets are send to it, it goes to sleep again.
- If the node I wants to send packet to the MARI node, it senses the channel from the end of broadcast window or when arrives at MAC layer for transmission, until the channel is idle. The node I uses standard 802.11 back-off algorithm, if contention for channel occurs. When the channel is idle, it will send packets to the MARI node. Node I sleep after transmission is over and wakes up at time ti or T, whichever comes earlier.
- If the node k wants to send packets to its neighbor I other than its RIMA node, node k wakes up at time ti as node I wakes at time ti, and send packets to node I, if the channel is idle.
- After each sleep cycle (Tm, Tm+1) in beacon period, wakeup counter wi increased. If wi was not changed, the node k with wake up time tkm, little earlier than wake up time tim of node I will get more throughput than node I, as packets transmitted to node k will always overlap to the wake up period (tim, tim +T) of node I. Thus node k will get more throughput than node I. When the wakeup counter wi is increased after every sleep cycle (Tm,Tm+1) in beacon period T, wake up time of all nodes are redistributed in the time period (Tm,Tm+1) and all member nodes get fair share of throughput.

In the large ad hoc networks, traffic passing through the backbone nodes, i.e., MARI nodes and Gateway nodes is expected to be large as compared to local traffic between neighboring nodes. MARI nodes and Gateways do not have to wait for longer time for idle channel. Thus the overall delay for routing packets will be reduced. Whereas, if the packets are to be transmitted to the neighbors, sender has to wait until the wake up time of receiver. Thus the delay for local traffic is expected to be more.

On average each packet suffers delay slightly more than (Tm – Tm+1) /2 at last hop. To reduce this delay, the number of sleep cycles can be increased. This will reduce the delay at last hop, as sender has to wait for less amount of time to deliver the packet to receiver at last hop.

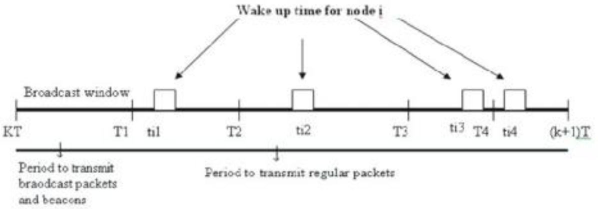

Wake up time for node i
Broadcast window
KT
T1
ti1
T2
ti2
T3
ti3
T4
ti4
(k+1)T
Period to transmit braodcast packets and beacons
Period to transmit regular packets

Fig 4.3: Illustrating Beacon Period

5.7. Routing Over Virtual Backbone

To measure the effectiveness of the Topology Management scheme, we have designed a mobile agent based routing protocol. The routing protocol is on demand i.e. route is found only when route to the destination is required. This routing protocol is executed only on MARI nodes, which have the routing intelligence. Whereas, gateways only forward the packets between MARI nodes using field of the packet. If a MARI node has to send packet to other MARI node, it sends the packet to gateway with address of other MARI node in field. Thus the routing is between MARI node to MARI node and gateways act as relay between MARI nodes. (See algorithm 4):

Algorithm 4: (Routing over virtual backbone)

```
if Forward mobile agent received then
    if Destination D is neighbor then
        Inform node D about route request
        Wait for acknowledgement
        if Acknowledgement received then
            Waif for time Tw
            Send the reverse mobile agent along path with highest accumulated congestion metric
        end if
    else
        Send forward mobile agent to all MARI nodes within two hops
    end if
end if
if Reverse mobile agent received then
    if Source S is neighbor then
        Update the routing table
        Inform node S about established path
    else
        Update the routing table
        Send the reverse mobile agent along the reverse path
    end if
end if
```

- Member or gateway node S, which needs route to destination D, sends request for route to its MARI node Rs.
- MARI node Rs. checks, if the destination D is the neighbor. If destination D is not neighbor of MARI node, then MARI node sends mobile agent to MARI nodes within two hops through gateways. For any MARI node Ri, which receive the mobile agent, if destination D is not the neighbor of Ri, then mobile agent migrates to the neighboring MARI nodes.

- While migrating mobile agent collects the information about congestion metric and the path followed by mobile agent. If the mobile agent, with same id is received more than once, then all subsequent mobile agents same id are rejected.

- If the destination D is neighbor of MARI node RD, RD informs D about route request from node S. If node D accepts route request, it acknowledges to MARI NODE rd.

- MARI node RD waits for time Tw for mobile agents coming from various paths. After time Tw, MARI node RD selects the path over which accumulated congestion metric is minimum. RD sends reverse mobile agent on selected path along with the accumulated congestion metric and path information received from forward mobile agent. Reverse mobile agent follows the path which was followed by the forward mobile agent.

- The reverse mobile agent updates the routing table of the MARI nodes along the path. When reverse mobile agent reaches the MARI nodes Rs, it updates the routing table and informs node S about path establishment. Now node S can send packet over the established path.

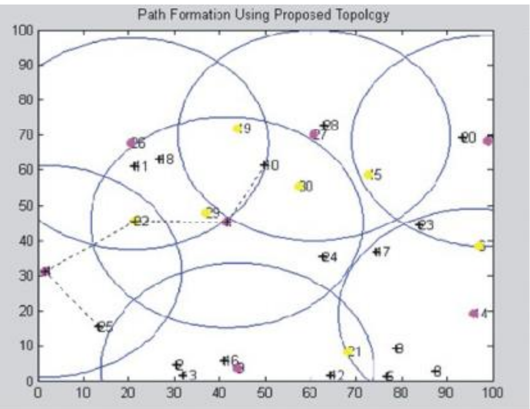


Fig 4.4: creation of a cluster network with probable member, head and gateway nodes

5.8. Load Distribution

One part of ad hoc network may be congested and other part of network may have free resources. This will increase the packet delivery latency. Throughput and packet delivery ratio also will be badly affected. To distribute the load evenly in the network, we have devised a congestion metric which is used for route selection as described above. This congestion metric is based on the amount of time MARI node sees free channel for the past T seconds.

This congestion metric is given by

$$Fm= fmt + (1-a) fm$$

Where fmt is fraction of time channel is free during past T seconds and 'a' is weighing factor in (0, 1).

For congested MARI nodes this congestion metric will be more, as the channel will be more busy and for free MARI node this will be less, as the channel will be more free.

5.9. Performance Evaluation

To evaluate the Topology Management scheme, we simulate 30-node networks in square region of 100m x 100m. Nodes in our simulations use radius with a 2 Mbps bandwidth and 30 m nominal radio range. Twenty nodes send and receive traffic. Each of these nodes send a CBR traffic to another node.

5.10. Power Consumption

We have used the energy consumption model of (3), which is obtained from measurements on the Cabletron Roam about 802.11 DS High Rate network interface card (NIC) operating at 2 Mbps. Power consumption in various modes such as Tx (transmit), Rx (receive), Idle and sleeping.

Tx	Rx	Idle	Sleeping
1400mW	1000mW	830mW	130mW

Table 4.1: Power consumption in various modes

5.11. Fraction of Nodes in Forwarding Backbone

Fig 4.5 shows the fraction of nodes that are part of virtual forwarding backbone (i.e. MARI and gateway nodes) as node density increases. It can be observed that as node density increases, fraction of forwarding nodes goes on decreasing. Thus more number of nodes are member nodes, which are in power efficient sleep state most off the time.

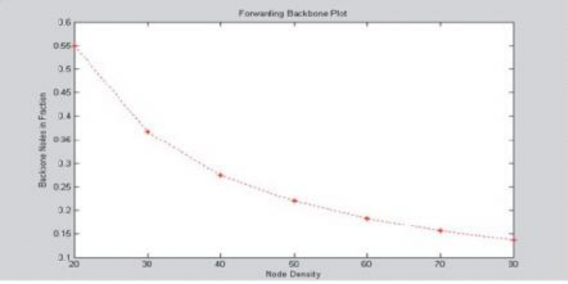


Fig4.5: Fraction of nodes that are part of virtual forwarding backbone (MARI and gateway nodes) as node density increases

5.12. Node Lifetime

Fig 4.6 shows fraction of nodes remaining in the network as a function of simulation time. If the energy of a node falls below certain threshold, the node is marked as dead. Figure shows that Topology Management scheme increases the life time of node more than factor of two.

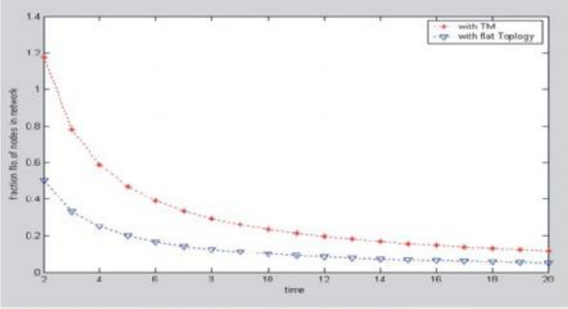


Fig 4.6: Node Life Time

5.13.Comparing Beacone and Non-Beacon Topologie

The amount of data transmitted and the node life of the member nodes can be increased by implementing the concept of beacon period.

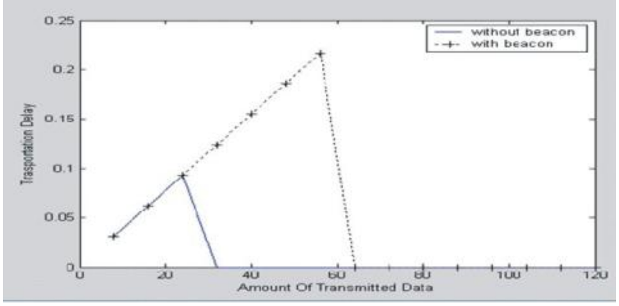


Fig 4.7: offered load v/s transportation delay plot

The proposed protocol provides a simplified approach to the performance improvement of a mobile adhoc network. This protocol when implemented on the network scenario as presented above outperformed the flat topology approach. This approach is focused on improving the routing method based on the individual node power consumption. The power though saved in this manner may be dissipated under misbehavior operations in adhoc network. Hence prediction and removal of misbehaving nodes on such a node in the network is of prime importance. A method for the prediction and removal of misbehavior in the network is suggested.

Chapter 06 Robust Trust-Worth Routing Protocol

6.1. Overview

Mobile ad hoc networks (MANETs) rely on the cooperation of all the articipating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. But supporting a MANET is a cost-intensive activity for a mobile node. Detecting routes and forwarding packets consumes local CPU time, memory, network-bandwidth, and most important the energy. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data.

There are two approaches of dealing with selfish nodes. The first approach tries to give a motivation for participating in the network function. The authors suggest to introduce a virtual currency called Nuglets that is earned by relaying foreign traffic and spent by sending own traffic. The major drawback of this approach is the demand for trusted hardware to secure the currency. There are arguments that tamper-resistant devices in general might be next to impossible to be realized. A similar approach without the need of tamper proof hardware has been suggested by Zhong. There exist also other unresolved problems with virtual currencies, like e.g. nodes may starve at the edge of the network because no one needs them for forwarding etc. Most of the existing work in this field concentrates on the second approach: detecting and excluding misbehaving nodes.

The first to propose a solution to the problem of selfish (or as they call it "misbehaving") nodes in an ad hoc network were Marti, Giuli, Lai and Baker. Their system uses a watchdog that monitors the neighboring nodes to check if they actually relay the data the way they should do. Then a component called path rater will try to prevent paths which contain such misbehaving nodes. As they indicate their detection mechanism has a number of severe drawbacks. Relying only on overhearing transmissions in promiscuous mode may fail due to a number of reasons. In case of sensor failure, nodes may be falsely accused of misbehavior. The second drawback is that selfish nodes profit from being recognized as misbehaving. The paths in the network are then routed around them, but there is no exclusion from service.

A wireless or mobile ad hoc network (MANET) is formed by a group of wireless nodes, which agree to forward packets for each other. One assumption made by most ad hoc routing protocols is that every node is trustworthy and cooperative. In other words, if a node claims it can reach another node by a certain path or distance, the claim is trusted. If a node reports a link break, the link will no longer be used. Although such an assumption can simplify the design and implementation of ad hoc routing protocols, it does make ad hoc networks vulnerable to various types of denial of service (DoS) attacks. One class of DoS attacks is malicious packet dropping. A malicious node can silently drop some or all of the data packets sent to it for further forwarding even when no congestion occurs.

Malicious packet dropping attack presents a new threat to wireless ad hoc networks since they lack physical protection and strong access control mechanism. An adversary can easily join the network or capture a mobile node and then starts to disrupt network communication by silently dropping packets. It is also a threat to the Internet since the various software vulnerabilities would allow attackers to gain remote control of routers on the Internet. If malicious packet dropping attack is used along with other attacking techniques, such as shorter distance fraud, it can create more powerful attacks (i.e., black hole) which may completely disrupt network communication.

Current network protocols do not have the capability to detect the malicious packet dropping attack. Network congestion control mechanisms do not apply here since packets are not dropped due to congestion. Link layer acknowledgment, such as IEEE 802.11 MAC protocol, can detect link layer break, but cannot detect forwarding level break. Although upper layer acknowledgment, such as TCP ACK, allows for detecting end-to end communication break, it can be inefficient and it does not indicate the node at which the communication breaks. Moreover such mechanism is not available in connectionless transport layer protocols, such as UDP. Therefore, it is important to develop mechanisms to render networks the robustness for resisting the malicious packet dropping attack.

6.2. Properties of Misbehavior in ad hoc Network

We found the following ways of attacking DSR, targeting availability, integrity, confidentiality, non-repudiation, authentication, access control or any combination thereof:

1. **Incorrect forwarding:** acknowledge ROUTE REQUEST, send new request or do not forward at all. This works only until upper layers find out.
2. **Bogus routing information or traffic attraction:** reply to ROUTE REQUEST, also gratuitous, to advertise a non-existent or wrong route.
3. Salvage a route that is not broken. If the salvage bit is not set, it will look like the source is still the original one.
4. Choose a very short reply time, so the route will be prioritized and stay in the cache longer.
5. Set good metrics of bogus routes for priority and remaining time in the cache.
6. Manipulate flow metrics for the same reason.
7. Do not send error messages in order to prevent other nodes from looking for alternative routes.
8. Use bogus routes to attract traffic to intercept packets and gather information.

9. Use promiscuous mode to listen in on traffic destined for another node.
10. Cause a denial-of-service attack caused by overload by sending route updates at short intervals.

6.3. Detection of Attacks in DSR

With the exception of the promiscuous listening in 9), all of the attacks listed above correspond to observable events the monitor component in each node can detect either at once or at the latest when they happen repeatedly:

1. **Forwarding:** this can be detected by passive acknowledgement, i.e. keeping a copy of a packet until having confirmed correct forwarding by listening to the transmission of the next hop node.
2. **Bogus routing:** a strong indication would be when an intermediate node sees itself advertised on a route it does not have. As a last resort, if a node cannot tell whether a route is real or bogus, it can at least detect the lack of forwarding as in 1). Unusually increased frequency of route advertising can be detected as in 10).
3. **Salvaging:** indicated by the reception of a salvaged packet without having received a link error message first.
4. **Reply time too short:** can be detected by comparing reply time to actual route length.
5. **Metrics of bogus routes too good:** detectable by comparing metrics to actual quality.
6. **Lack of error messages:** indicated in the case when a node receives a link error message from its own link layer but no explicit error message by other nodes in the range.
7. **Route updates too frequent:** detectable by keeping timestamp of last update to compare.

6.4. Grudging nodes in DSR

The suggested scheme works as an extension to a routing protocol. In this example, normal DSR information flow (ROUTE REQUEST, ROUTE REPLY messages) as explained takes place. Once non-cooperative behavior has been detected and exceeds threshold values, an ALARM message is sent. 5.1 through 5.5 show the flow of messages and data from route discovery to the detection of malicious behavior and subsequent rerouting.

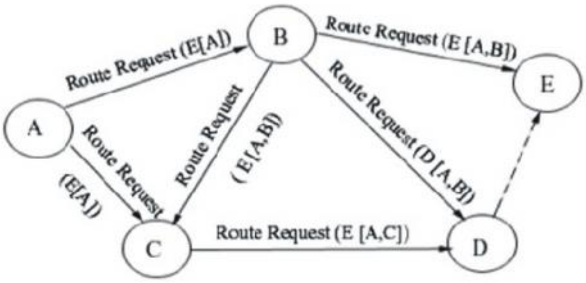


Fig 5.1: Route request from node A to E

In more detail: Fig 5.1 shows DSR route discovery for a path from node A to node E. Every node forwards the request to its neighbors unless it has already received the same route request or has a path cache entry for the desired destination.

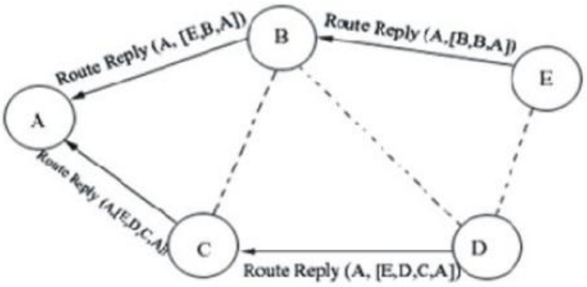


Fig 5.2: Route Reply to node A

Fig 5.2 shows the reply messages of the destination node itself, node E, and from node D, which has a path to E. The reply message contains the reversed source route to the destination and is sent to the source. In the case of unidirectional links, or if generally the route can not be reversed, node E would send the reply along a path to A that it has in its route cache. If there is no path to A in the route cache, E has to perform a route discovery itself to get to A. In this route request, the already found path from A to E is included.

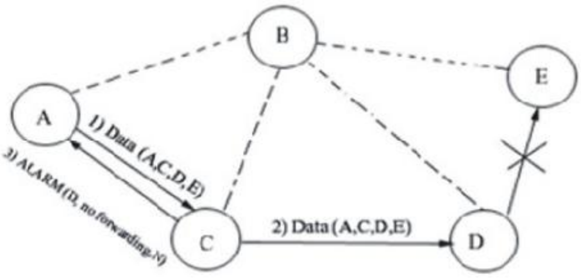


Fig 5.3: Data flow and alarm message

In Fig 5.3 data flow is from node A to node E via node C and D. In this case, node A has chosen this route according to some metrics and preferred it over the route via B. During the data flow, node C detects that node D does not behave correctly. In this example, node D does not forward the data destined for node E. After the occurrence of the bad behavior of node D was observed by node C for a number exceeding a threshold, node C triggers an ALARM message to be sent to the source, node A.

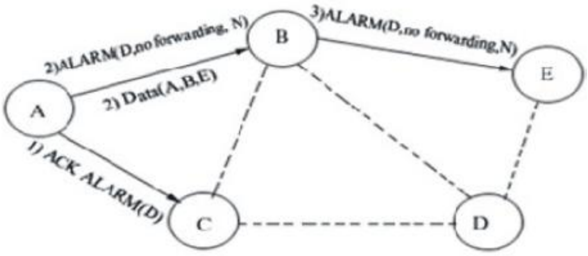


Fig 5.4: Data flow through alternate path

Upon reception of the ALARM message as shown in Fig5.4, node A acknowledges the message to the reporting node C and decides to use the alternate path via node B to send the data to the destination node E.

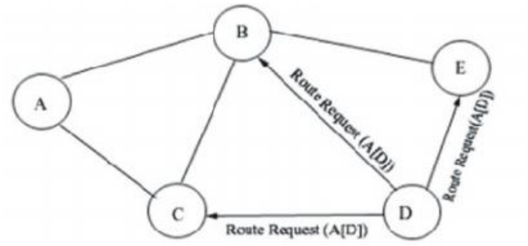
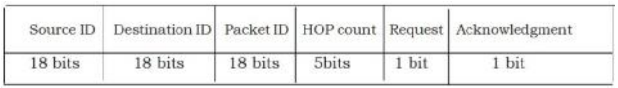


Fig 5.5: Isolation of Node D

Now if node D sends a Route request to the neighboring nodes as shown in fig5.5, all the nodes do not forward the packet and thus isolates node.

6.5. Management Scheme

6.5.1. Route Establishment: Every node generates a route request packet as structured (shown in figure 5.6) and broadcast to each neighboring node as shown in figure 5.7 with source and destination id to establish a route when it enters in to a network. The structure of the packet is given as;



Source ID	Destination ID	Packet ID	HOP count	Request	Acknowledgment
18 bits	18 bits	18 bits	5bits	1 bit	1 bit

Fig 5.6: Route Request packet format

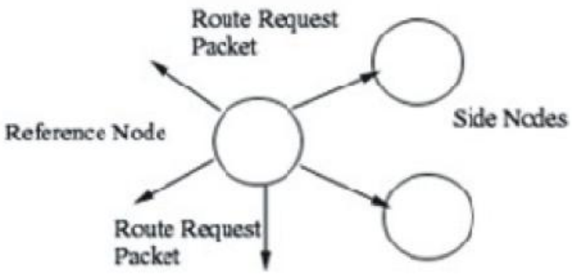


Fig 5.7: Route request by reference node

In RMP protocol each node monitor their neighborhood and detect several kinds of misbehavior by means of an enhanced passive acknowledgment mechanism designed.

This means that every time a node sends a packet, it listens to overhear whether the next-hop node on the route forwards the packet correctly. Consider the following scenario as depicted in Fig 5.8

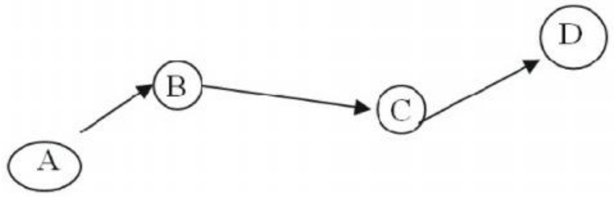


Fig 5.8: Packet forwarding between nodes

Node A sends packets via nodes B and C to the destination D. For every packet, nodes keep track of the behavior of the next-hop node and remember whether it has forwarded the packet correctly. A stores ratings about B, B about C, etc., which is called as first-hand information, since the ratings are derived from direct observation. Suppose that C misbehaves by dropping the packet instead of forwarding it, as shown in Figure 5.9. B's rating of C then becomes bad. Since A is not in range with C, it cannot directly observe its behavior and thus cannot find out about C's misbehavior.

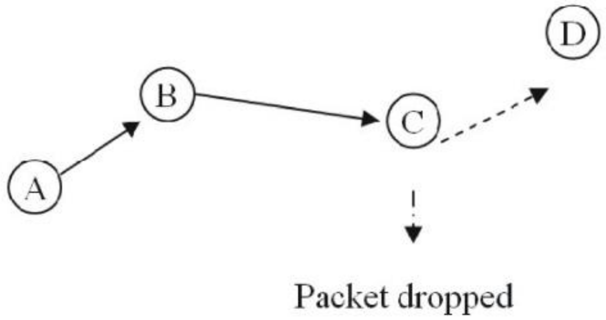


Fig 5.9: Packet dropping at node C

In this project this problem is solved by allowing the use of second-hand information as follows: In addition to keeping track of direct observation, nodes publish their first-hand information from time to time by local broadcasts to exchange information with other nodes. This information is termed as second-hand information. A thus receives information from its neighbor B about node C. Again, since A has no first-hand information about C, it can only find out about C's misbehavior by second-hand information. There is, however, a problem since second-hand information can be false. A node could for instance make false accusations about another node.

In this project a combination of two mechanisms is used to cope with spurious second-hand information. First, we only consider second-hand information that is not incompatible, i.e. that does not deviate too much from the reputation rating. Our motivation behind this is, that when second-hand information deviates substantially from the rating a node has built over time using previously received second-hand information from several sources and potentially its own first-hand information, it is more likely to be false. Second, even when second-hand information is compatible, we only allow it to slightly influence the reputation rating. We modified Bayesian model merging to implement these mechanisms.

Nodes use the reputation ratings they keep about other nodes to classify them. This classification provides a basis for decision-making about providing or accepting routing information, accepting a node as part of a route, and taking part in a route originated by some other node. Nodes classify other nodes as misbehaving if their reputation rating is worse than their threshold for misbehavior tolerance. Once a node classifies another as misbehaving, it isolates it from the network by not using it for routing in forwarding and in turn not allowing to be used by it.

6.6. Passive Acknoledgment (Pack)

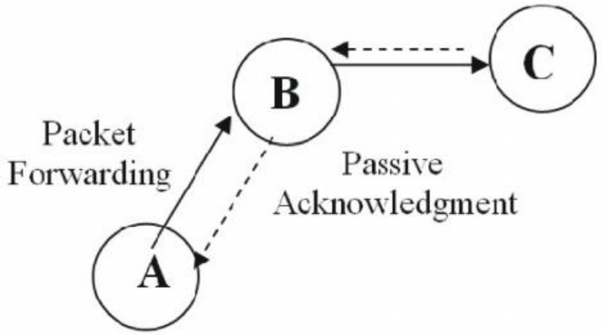


Fig 5.10: Passive Acknowledgment process.

During packet forwarding every node is responsible confirming that the packet was received by the next hop. There are three ways to get this acknowledgment:

- Link-layer acknowledgment: this is supplied by the MAC layer.
- Passive acknowledgment: this confirmation comes indirectly by overhearing the next node forward the packet
- Network-layer acknowledgment: this is when nodes explicitly request a DSR acknowledgment from the next hop.

Passive acknowledgment means that instead of waiting for an explicit acknowledgment for each packet by the next-hop node on the route, a node assumes the correct reception the packet when it overhears the next-hop node forwarding the packet. PACK can be used for Route Maintenance when originating or forwarding a packet along any hop other than the last hop. PACK cannot be used with the last hop since it will never retransmit a packet destined to itself. PACK needs two conditions to be applied: nodes have their network interfaces in promiscuous mode, and network links operate bi-directional. PACK works as follows: The bi-directionality of the link-layer (IEEE 802.11b), makes a node is to find out whether the next node forwards its packet if both nodes are still in the range of one another. This is possible because the node receives the packet in promiscuous mode when the next node forwards it. When a node receives a packet to be forwarded to a node other than last hop, the node sends the packet without requesting a network-layer acknowledgment (ACK).

If it does not overhear the packet forwarded, it means that the next hop either did not forward it or that it did forward it but it was not overheard because the next-hop node moved out of range just after receiving the packet to be forwarded. With the PACK retransmission mechanism, the node waiting for the PACK resends the packet without network-layer ACK request. After a certain number of trials, a network-layer ACK request must be used instead of PACK for all remaining attempts for that packet. If it does not get acknowledged, it emits a route error claiming that the next node is unreachable.

When a node receives a new packet, it considers it as a PACK if the following checks succeed:

- Source address, destination address, protocol identification and fragment offset fields in the IP header of the two packets must match.
- If either packet contains a DSR Source Route header, both packets must contain one, and the value in the Segments Left field (it indicates the number of hops remaining until the destination) in the DSR Source Route header of the new packet must be less than that in the first packet.

In this project the simple passive acknowledgment is used not only for an indication of correct reception at the next hop, but also to detect if nodes fail to forward packets. The enhanced the passive acknowledgment mechanism is used to detect several kinds of misbehavior. ie to compare packets to detect the illegitimate modification of header fields and the fabrication of messages. With this modified passive acknowledgment mechanism, nodes make inferences from all messages overheard and classify behavior as normal or misbehaving at each observation. Since the packets sent are logged in a queue waiting to be acknowledged by PACK, it is straightforward to check some additional fields to detect misbehavior in the flow of packets. The fact that PACK cannot be used for the last hop, as explained above, has no influence on the misbehavior detection capability since the destination has no incentive to drop its own packets and no route tampering can be done.

The DSR draft fields must checked in order to consider that the packet received is a PACK. By checking the four fields of the IP header, packet can be identified uniquely so that it can be assured that the overheard one retransmission of the packet is what was forwarded. Next, the DSR draft requires that if both packets have a source route option, then the segments left value in the overheard packet must be less than in the logged packet. This last check assures that the overheard packet is fresher than the logged one.

In order to implement enhanced PACK to detect some attacks or events, every packet is completely checked for changes when overheard. The following fields are checked and log if one of them changes:

- **IP header:** The TTL value must be decremented by only one.
- **Route reply option(s):** All fields.
- **Route error option(s):** All fields.
- **Source route option:** If the Salvage value is unchanged, all fields except Segs Left (we only check that this value decreases). If the Salvage flag changed, we only check Type, Last Hop External, First Hop External and Segs Left (must have decreased).
- **Forged route error:** a node can detect it, if the unreachable address in the route error option is its own.

6.7. Monitoring by Enhanced Passicve Acknowledgement

When a RMP node, say node i joins a mobile ad-hoc network running DSR, its path cache is empty and it has no first-information, trust, or reputation ratings about others. When it has a packet to send, it first sends out a route request, and after receiving route replies according to DSR, it chooses the shortest path and puts it in its route cache. Let node j be the next-hop node on the source route to the destination. Node I then sends its packet to node j.

After sending the packet to node i, node j puts packet information into the queue for passive acknowledgment (PACK) and sets a PACK timer. Every time i overhear a packet, it checks whether it matches an entry in the PACK table.

6.8. Modified Bayesian Approach

6.8.1 Gathering First-Hand Information : Node i overhears j forward the packet to the next hop on the route, say node k. It compares the overheard packet with the information in the PACK queue and verifies, that the changes are legitimate. It thus infers correct reception of the packet by j and the attempt of j to forward it to k. Node i interprets this as normal behavior by j and removes the packet from the PACK queue. To reflect this observation of j, node i creates a first-hand information rating for j, which we call F i,j.

6.8.2. Updating First-Hand Information: The first-hand information record Fi,j has the form (α, β). It represents the parameters of the Beta distribution assumed by node i in its Bayesian view of node j's behavior as an actor in the network. Initially, it is set to (1,1).

The standard Bayesian method gives the same weight to each observation, regardless of its time of occurrence. We want to give less weight to evidence received in the past to allow for reputation fading. We therefore developed a modified Bayesian update approach by introducing a moving weighted average as follows.

Node i just made one individual observation about j. Let S=1 if this observation is qualified as misbehavior by RMP, and S=0 otherwise. The update is

$$\alpha: = u\alpha+s$$

$$\beta := u\ \beta +(1-s)$$

The weight u is a discount factor for past experiences, which serves as the fading mechanism.

In our case, node i classified the behavior of node j as normal, since it overheard the packet re-transmission and detected no illegitimate changes, therefore

F i,j=Fi,j (uá, u â+1)

In addition, during inactivity periods, we periodically decay the values of α, β as follows.

Whenever the inactivity time expires, we let

$$\alpha: = u\alpha$$

$$\beta:= u\ \beta$$

This is to allow for redemption even in the absence of observations. Node i thus periodically discounts the parameters of Fi,j.

6.8.3. Updating Reputation Ratings: When node i updates its first-hand information Fi,j, it also updates its reputation ratingFor j, namely Ri,j in the same way.

The reputation rating Ri,j is also defined by two numbers, (α’, β’). Initially, it is set to (1,1) . It is updated on two types of events: (1) when first-hand observation is updated (2) when a reputation rating published by some other node is copied. Here we discuss the first case.

So far, node i has made one first-hand observation of node j. Since it made a positive experience with node j, it changes

$$R_{i,j}=R_{i,j}(u\alpha', u\,\hat{a}'+1).$$

If the update to the first-hand information is due to inactivity, the formula is

$$\alpha' := u\alpha'$$

$$\beta' := u\beta'$$

6.8.4. Using Trust: To speed up detection, nodes can also use trust to accept second-hand information even if it is incompatible. Assume node i receives the reported first-hand information $F_{k,j}$ from node k. .

If $T_{i,k}$ is high enough, it will accept $F_{k,j}$ to slightly modify its own $R_{i,j}$ even if it fails the deviation test. Node i updates $T_{i,j}$ in any case. If passed the k deviation test, δ will be increased, otherwise γ.

6.8.5. Classifying Nodes: Every time node i updates its ratings about j, it checks whether it is still within the boundaries of its misbehavior tolerance. This is done to provide a basis for decisions about how to treat j. Node i thus classifies j as normal, if $R_{i,j}$ is smaller than t, as misbehaved otherwise.

6.8.6. Sending Packets, Detecting Misbehavior: For each packet node i sends, it keeps the same procedure of storing the information in he PACK queue and setting the PACK timer. When the PACK timer goes off, it means that node i did not overhear the retransmission of the packet by the next hop j. In this case, node i interprets this as an instance of misbehavior by node j and updates its firsthand information and reputation rating about node j, such that

$$F_{i,j} = F_{i,j}(u\alpha'+1, u\,\beta') \text{ and}$$

$$R_{i,j}(\alpha', \beta') := R_{i,j}(u\alpha'+1, u\,\beta').$$

The PACK timer going off is only one case of a misbehavior indication, another one is when node i detects an illegitimate modification of the packet when it overhears the retransmission by j. When there are no packets being sent, node i updates F i,j and R i,j using the decay factor u.

6.8.7. Managing Paths: When i classifies j as misbehaving, it deletes all routes containing node j from its path cache. If it still has packets to send and there is an alternate path that does not include j, node i proceeds to send packets over that path, otherwise it sends out a new route request. In addition, node i puts node j on its list of misbehaving nodes and increases its reputation tolerance threshold r.

Assume now that node j wants the services of node i for forwarding a packet node. Originating from j or providing a route for j. Node i deny service to j in order to retaliate and isolate it.

In our approach, we do not punish nodes that are categorized as untrustworthy but merely restrict their influence. The reasons for this are that testimonial inaccuracy can not be proved beyond doubt, deviations can arise because nodes discover misbehavior before others do, and punishment discourages the publication of ratings.

6.9. Proposed Monitoring Architecture

The tasks RMP carries out are, to gather information to classify first-hand experience, to exchange this information and to consider the second-hand information thus received, to update the belief about the behavior of others, which is called the reputation rating, taking into account both first and second-hand information, to classify other nodes based on the reputation rating, and to adapt one's own behavior according to that classification. RMP consists of several components that fulfill these tasks. The architecture of the protocol is as shown in figure 5.11

The components of the protocols are:

- Monitor, Reputation System
- Path Manager, Trust Manager

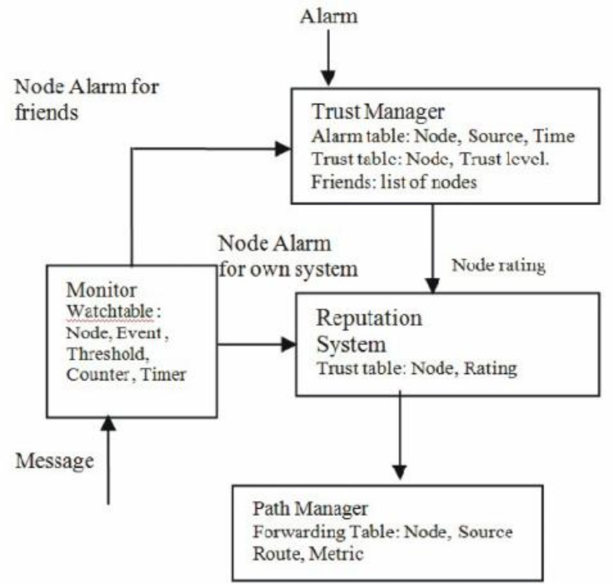


Fig 5.11: RMP Architecture within each Node

As shown in Fig 4.1 The Monitor, the Reputation System, the Path Manager, and the Trust Manager are the components that are present in every node and they are described in detail subsequently:

6.9.1. The Monitor (Neighborhood Watch): In a networking environment, the nodes most likely to detect non-compliant 'criminal' behavior are the nodes in the vicinity of the criminal and in some case the source and the destination, if they detect unusual behavior or do not get proper responses. The latter is not always the case, for instance in the case of replay. One approach to protocol enforcement and detection of damaging behavior (intrusion, misuse of cooperation incentives, denial of service, etc.) suggested here is the equivalent of a 'neighborhood watch', where nodes locally look for deviating nodes. The neighbors of the neighborhood watch can detect deviances by the next node on the source route by either listening to the transmission of the next node or by observing route protocol behavior. By keeping a copy of a packet while listening to the transmission of the next node, any content change can also be detected. In this paper we focused on the detection of observable routing and forwarding misbehavior in DSR as listed in section 5.2. In general, the following types of misbehavior can be indicated:

- no forwarding (of control messages nor data),
- unusual traffic attraction (advertises many very good routes or advertises routes very fast, so they are deemed good routes),
- route salvaging (i.e. rerouting to avoid a broken link),although no error has been observed,
- lack of error messages, although an error has been observed,
- unusually frequent route updates,
- silent route change (tampering with the message header of either control or data packets).

As a component within each node, the monitor registers these deviations of normal behavior. As soon as a given bad behavior occurs, the reputation system is called.

6.9.2. The Trust Manager: In an ad hoc environment, trust management has to be distributed and adaptive [2]. This component deals with incoming and outgoing ALARM messages. ALARM messages are sent by the trust manager of a node to warn others of malicious nodes. Incoming ALARMS originate from outside friends, whereas the node itself generates outgoing ALARMS after having experienced, observed or been reported malicious behavior.

The following functions are performed by the trust manager:

- Trust function to calculate trust levels, o Trust table entries management for trust level administration,
- Forwarding of ALARM messages,
- Filtering of incoming ALARM messages according to the trust level of the reporting node.
- The trust manager consists of the following components:
- Alarm table containing information about received alarms,
- Trust table managing trust levels for nodes,
- Friends list containing all friends a node sends alarms to.
- The trust manager administers a table of friends, i.e. nodes that are candidates to receive ALARM messages from a given node, and how much they are trusted. Trust is important when making a decision about the following issues:
- providing or accepting routing information,
- accepting a node as part of a route,
- taking part in a route originated by some other node.

6.9.3. The Reputation System (Node Rating): In order to avoid centralized rating, local rating lists and/or black lists are maintained at each node and potentially exchanged with friends. The nodes can include black sheep in the route request to be avoided for routing, which also alarms nodes on the way. Nodes can look up senders in the black list containing the nodes with bad rating before forwarding anything for them. The problem of how to distinguish alleged from proven malicious nodes and thus how to avoid false accusations can be lessened by timeout and subsequent recovery or revocation lists of nodes that have behaved well for a specified period of time. Another problem is scalability and how to avoid blown-up lists, which can also be addressed by timeouts. The reputation system in this protocol manages a table consisting of entries for nodes and their rating. The rating is changed only when there is enough evidence for malicious behavior that is significant for a node and that has occurred a number of times exceeding a threshold to rule out coincidences. The rating is then changed according to a rate function that assigns different weights to the type of behavior detection:

- Own experience: greatest weight,
- Observations: smaller weight,
- Reported experience: weight function according to PGP trust.

Once the weight has been determined, the entry of the node that misbehaved is changed accordingly. If the rating of a node in the table has deteriorated so much as to fall out of a tolerable range, the path manager is called for action. Bearing in mind that malicious behavior will hopefully be the exception and not the rule, the reputation system is built on negative experience rather than positive impressions.

6.9.4. The Path Manager: Once a node i classifies another node j as misbehaving, i isolates j from communications by not using j for routing and forwarding and by not allowing j to use i. This isolation has three purposes. The first is to reduce the effect of misbehavior by depriving the misbehaving node of the opportunity to participate in the network. The second purpose is to serve as an incentive to behave well in order not to be denied service. Finally, the third purpose is to obtain better service by not using misbehaving nodes on the path. The path manager performs the following functions:

- Path re-ranking according to security metric,
- Deletion of paths containing malicious nodes,
- Action on receiving a request for a route from a malicious node (e.g. ignore, do not send any reply),

- Action on receiving request for a route containing a malicious node in the source route (e.g. also ignore, alert the source).

The dynamic behavior of RMP is as follows [2]. Nodes monitor their neighbors and change the reputation accordingly. If they have reason to believe that a node misbehaves, i.e. when the reputation rating is bad, they take action in terms of their own routing and forwarding. They thus route around suspected misbehaved nodes. Depending on the rating and the availability of paths to the destination, the routes containing the misbehaved node are either re-ranked or deleted from the path cache. Future requests by the badly rated node are ignored. In addition, once a node has detected a misbehaved node, it informs other nodes by sending an ALARM message.

When a node receives such an ALARM either directly or by promiscuously listening to the network, it evaluates how trustworthy the ALARM is based on the source of the ALARM and the accumulated ALARM messages about the node in question. It can then decide whether to take action against the misbehaving node. Note that simply not forwarding is just one of the possible types of misbehavior in mobile ad-hoc networks. Several others, mostly concerned with routing rather that forwarding have been suggested, such as black hole routing, gray hole routing, worm hole routing. Other kinds of misbehavior aim at draining energy, such as the sleep deprivation attack. RMP is not restricted to handling any particular kind of misbehavior but can handle any attack that is observable. Even if the observation cannot precisely be attributed to an attack but is the result of another circumstance in the network such as a collision, RMP can make use of it. If it is a rare accident, it will anyhow not influence the reputation rating significantly, and if it happens more often, it means the observed node has difficulties performing its tasks.

6.10. Context Diagram For RPM

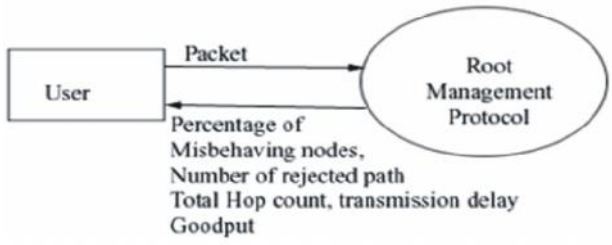


Fig 5.12: Context Diagram for Route Management Protocol (RPM)

Every node uses RMP Process for the transferring of packets to route around the malicious nodes and to evaluate the performance in terms of Percentage of Misbehaving nodes, numbers of rejected path, Total Hop count, transmission delay and Good put.

6.11. Level 1 DFD For Route Management Protocol

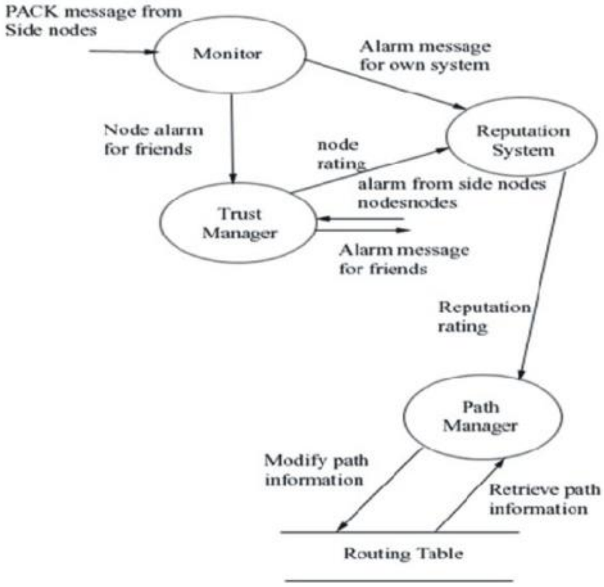


Fig 5.13: Level 1 DFD for Route Management Protocol

The monitor process receives PACK message & observes the behavior of neighboring nodes, sends alarm to trust management process and Reputation system process if the node misbehaves. The Trust Manager process in turn sends this alarm to friend nodes, and if it receives alarm massages, it evaluates the node rating and sends to the reputation system. The reputation system process evaluates the reputation rating and sends to the path manager. The path manager process modifies the path information based on the reputation rating.

6.11.1. Level 2 DFD For Trust Manager:

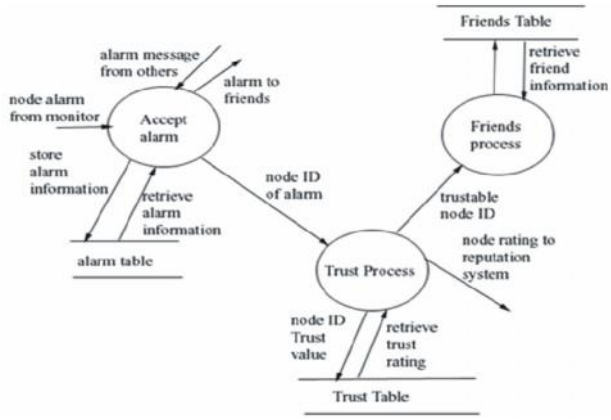


Figure 5.14: Level 2 DFD For Trust Manager

Accept alarm process receives the alarm messages from monitor and nodes and stores in the alarm table and it retrieves the node ID of alarm received to the Trust process. It also sends alarms to the friend nodes. The trust process retrieves the Trust rating from Trust table and sends the node rating to the path Manager process.

6.12. Level 2 DFD For Reputation System and Path Manager

The weight process receives the input from the Monitor process, Trust manager process, and calculates a weight and sends the reputation information to the Rating function process, which in turn calculates the reputation rating and sends to the path Manager process, The Path Manager process compares the reputation rating with the tolerable range and either changes the ranking of the path or deletes the path from the routing table.

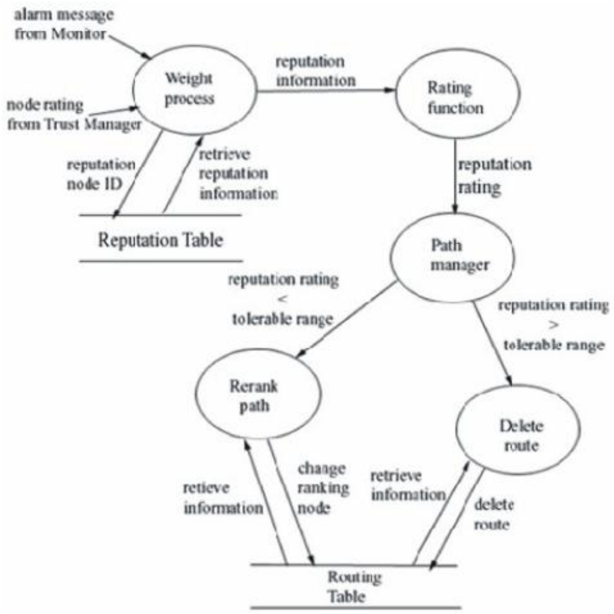


Figure 5.15: Level 2 DFD For Reputation System And Path Manager

This project is implemented using 5 modules, they are:

1. network creation
2. Evaluating a path between source and destination
3. Finding node as a friend or malicious
4. Isolation of malicious node based on Bayesian Approach
5. The Network Performance Evaluation

The above said modules are explained subsequently.

6.13. Network Creation

For the creations of the network for simulation, an area of 280*300 units is chosen. The nodes are randomly created by allocating their coordinates and with random BW and ID allocated. These nodes are plotted over a scale is randomly chosen with a destination. This module then implements a DSR protocol where a packet is generated from the source with a structure explained in section two. This packet is forwarded to their neighboring nodes maintaining a node list during forwarding the packets and return back an acknowledge from the destination from the same node as maintained in the list once the destination is reached.

The module carries out this operation for all randomly distributed nodes to extract all possible paths from source to destination. Based on the number of Hops in the path the shortest path is chosen for analysis.

6.14. Evaluating a Path Between Source and Destination

For the source chosen, the packets generated rate transferred over the shortest path and observed whether a destination is reached or not. This module gives an option for selecting a particular node as regular or misbehaving based on which the reputation of each node is evaluated.

6.15 Finding a Friend or Malicious NODE

Based on the PACK received from the next node in the path, the HOP count field and the TTL field are compared with the same fields of the packet in PACK queue to determine whether the next node has forwarded the packet or not.

If these fields are found randomly modified, the node will be processed for misbehaving else will be declared as a friend. During misbehaving evaluation this module reads few network parameters as r,t,a’,b’,g,J for deciding the node property and trustworthiness.

This module evaluates the node performance and decides to retain the node in path or isolates based on modified Bayesian approach. The modified Bayesian approach is presented in section 5.12.this module reads the network parameter from previous module.

A power optimized routing scheme with trust worthy routes were observed to be efficient in providing a longer node life with higher quality metrics as observed in above simulations. These routings are the best optimal paths in adhoc network but the issue of data switching is still a major challenge in such a routing scheme. The data switching issue is focused to be overcome by a mobile switching scheme as outlined in following chapter.

Chapter 07 Robust Switching Scheme for Mobile ADHOC Network

In the near future, a large number of Mobile Stations (MSs) will be equipped with multiple radio interfaces for wireless access to the Internet. A multi-mode MS with multiple air interfaces (cellular interface, Bluetooth, IEEE 802.11 and IEEE 802.16 etc) and different data rates will be able to access cellular Base Stations (BSs), WLAN or WMAN Access Points (APs). In this scenario, the integration of multi-hop ad hoc communications with infrastructure based (or single-hop) wireless networks, such as wireless WANs (e.g., 2.5G, 3G, and 4G), wireless LAN (e.g., IEEE 802.11 a/b/e/g and HiperLAn/2) and wireless MANs (e.g., IEEE 802.16), is fundamental to improving the coverage and performance of the integrated network. In addition, multi-hop communications can be used to increase the utilization and capacity of a BS by decreasing the co-channel interference via lowering the transmission power either of the BS or of the MSs . Also, the integration can be useful in achieving load-balancing by forwarding part of the traffic from an overloaded cell to a free neighboring cell. From the protocol stack perspective, the network layer is the lowest possible layer where the convergence of heterogeneous wireless systems can be developed. Furthermore, the desire to extend the great success of the Internet Protocol (IP) from the wired world to wireless leads to an all-IP vision. So far, the IP is the best integration technology for heterogeneous networks and there is currently no foreseeable alternative to the IP. To allow for seamless handoff to take place in IP-based heterogeneous networks, the IP must support users' mobility. In an effort to do that, the Internet Engineering Task Force (IETF) has developed the mobile IP standard to support mobility in IP-based networks. In recent years, there has been a considerable amount of works that address the mobile IP-based handoff problem in heterogeneous networks. Since data packets could be lost during the latency period, mobile IP-based handoff may not meet the quality-of-service (QoS) requirements for real time voice applications. Even though, mobile IP describes a scheme to recover the lost packets from the old foreign agent to the new one, this process takes some time as the signal experiences a random delay when it travels through the network. This makes the latency even longer. For non-real time services, this additional delay will not create a major problem. However, for real time services, this will dramatically degrade the QoS requirements. This problem can be solved if multicasting is employed. In this case, data packets are sent to the neighboring foreign agents as soon as the Received Signal Strength (RSS) of the mobile host goes below a certain threshold level. When this occurs, the data packets are stored in the buffer at the new foreign agent, and in the process, the latency can be reduced.

In this paper, we consider a multicasting scheme to solve the handoff latency problem in heterogeneous networks. The proposed handoff technique offers two main advantages:

i. It reduces the handoff latency in hybrid networks,

ii. Recovers lost packets during the handoff process which increases the system throughput.

7.1 Mobile IP and Handoffs

First, second- and third-generation mobile systems depended on the employment of the radio spectrum that was either unlicensed (available for public use) or licensed for use by a very small number of service providers and network operators in each region. Differences in bandwidth and coverage areas have led to the necessity of developing multi-network interface devices (terminals) that are capable of using the variety of different network services provided.

7.1.1. Mobile IP: Mobile IP is an Internet protocol, defined by the Internet Engineering Task Force (IETF) that allows users keep the same IP address, and stay connected to the Internet while roaming between networks. The key feature of Mobile IP design is that all required functionalities for processing and managing mobility information are embedded in well-defined entities, the Home Agent (HA), Foreign Agent (FA), and Mobile Nodes (MNs). When a MN moves from its Home Network (HN) to a Foreign Network (FN), the correct delivery of packets to its current point of attachment depends on the MN's IP address, which changes at every new point of attachment. Therefore, in order to guarantee packets delivery to the MN, Mobile IP allows the MN to use two IP addresses: The Home address, which is static and assigned to the MN at the home network; and the Care-of-Address (CoA), which represents the current location of the MN. One of the main problems that face the implementation of the original Mobile IP is the Triangle Routing Problem. When a CN sends traffic to the MN, the traffic gets first to the HA, which encapsulates this traffic and tunnels it to the FA. The FA de-tunnels the traffic and delivers it to the MN. The route taken by this traffic is triangular in nature, and the most extreme case of routing can be observed when the CN and the MN are in the same subnet.

In mobile IP, two network entities are defined to support users mobility namely; the home agent and the foreign agent. These two agents periodically send advertisement messages to their corresponding networks (i.e., home and foreign networks) to acknowledge the mobile of its present location. Based on these advertisement messages, and the present location of the mobile host, the mobile host decides whether it belongs to its home network or to a new foreign network. If the mobile host discovers that it has migrated to a new foreign network, it sends a registration request to the corresponding new foreign agent to obtain a care-of-address. Also the foreign agent registers the new address (i.e., new location) with the mobile host home agent. After this process, any data packets that are received at the mobile's home network will be encapsulated with a new IP address and tunneled to the new foreign agent to which the mobile host resides. The foreign agent (at the other end of the tunnel) takes care of the de-encapsulation of the arriving data packets, and then forwards them to the mobile host using the new IP address. In the same way, if the mobile host transmits data packets to its correspondent host, it uses the foreign agent for the tunneling process to forward these data packets to the home agent for subsequent transmission to the correspondent host.

7.1.2. Classification of Handoffs: In principle, each mobile terminal (node) is, at all times, within range of at least one network access point, also known as a base station. The area serviced by each base station is identified as its cell. The dimensions and profile of every cell depend on the network type, size of the base stations, and transmission and reception power of each base station. Usually, cells of the same network type are adjacent to each other and overlap in such a way that, for the majority of time, any mobile device is within the coverage area of more than one base station. Cells of heterogeneous networks, on the other hand, are overlaid within each other. Therefore, the key issue for a mobile host is to reach a decision from time to time as to which base station of which network will handle the signal transmissions to and from a specific host and handoff the signal transmission if necessary. We classify handoffs based on several factors as shown in Fig. 1. No longer is the network type the only handoff classification factor. Many more factors constitute categorization of handoffs including the administrative domains involved, number of connections and frequencies engaged. The following are categorization factors along with the handoff classifications that are based on them.

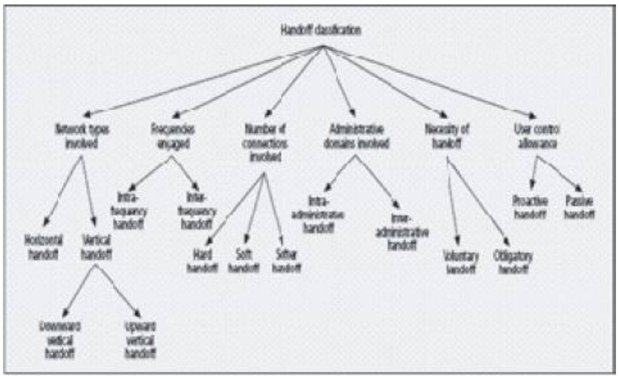


Figure 6.1: Hierarichal Classification of Handoff

Handoffs can be classified as either horizontal or vertical. This depends on whether a handoff takes place between a single type of network interface or a variety of different network interfaces.

7.1.3. Horizontal Handoff: The handoff process of a mobile terminal between access points supporting the same network technology. For example, the changeover of signal transmission (as the mobile terminal moves around) from an IEEE 802.11b base station to a geographically neighboring IEEE 802.11b base station is considered as a horizontal handoff process.

7.1.4. Vertical Handoff: The handoff process of a mobile terminal among access points supporting different network technologies. For example, the changeover of signal transmission from an IEEE 802.11b base station to an overlaid cellular network is considered a vertical handoff process.

7.2. System Architecture

The proposed interconnection architecture using mobile IP is shown in Fig. 6.2 the following are the network parameters and assumptions used in our handoff technique:

1. The home agent (HA), the foreign agents (FAs) and the correspondent host (CH) are interconnected through Internet
2. FAs are connected to the Internet through a wireless or a wired medium with large bandwidth.
3. The CH can be a fixed or mobile host.

The time taken to switch from the home agent of the mobile user to the new foreign agent is known as the mobile IP handoff latency. In addition to this handoff latency if the mobile host enters into a new foreign agent (from another foreign agent) during the tunneling process between the home agent and the old foreign agent, and before registering with the new foreign agent, data packets destined to the mobile host will be lost. These packets will then be retransmitted leading to an increase in the overall system delay.

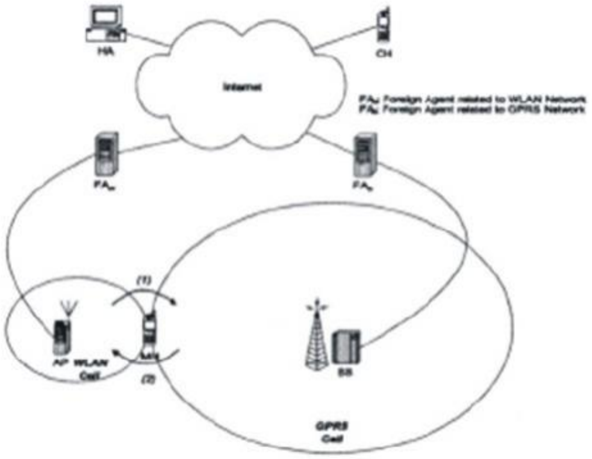

HA
CH
Internet
FA$_W$: Foreign Agent related to WLAN Network
FA$_G$: Foreign Agent related to GPRS Network
FA$_W$
FA$_G$
(1)
AP WLAN Cell
MH
(2)
BS
GPRS Cell

Figure 6.2: Proposed IP-based handoff architecture.

In delay-sensitive applications, handoff latency can cause serious degradation in the quality of the underlying application. As a result of the frequent handoffs, this handoff latency becomes a major problem if the coverage area of the sub-networks gets smaller. Recent works on the existing problems of the handoff latency of mobile IP based networks and possible solutions can be found in.

7.3. Proposed Improvement in Latency

7.3.1. Improvement in Registration Time: The improvement in Registration Time is achieved by starting to forward data packets after a small fixed delay (termed as the 'Fixed Registration Delay') following the Registration Request from the MH to the new FA through the new AP/ BS. That is, data packets will not wait for the registration process to be completed. Given the fact that the new FA has data packets stored in its buffer, it can start sending these packets to the MH immediately after receiving the Registration Request from the MH. This, in turn, will reduce the total handoff latency and the requirement of large buffer capacity at the FA. To improve the probability of packet loss during the handoff process, we propose a simple modification to the standard mobile IP. In that, the new FA can directly send the Binding Update to the CH instead of sending it to the HA. This of course requires the CH to be notified earlier about the new point of attachment of the MH. This modification is shown to assist in reducing the number of data packets forwarded to the old FA, which in turn reduces the probability of packet loss during the handoff process.

7.3.2. Improvement in Packet Reception Time: The main contributor to the Packet Reception Time is the time required for transmitting the data packets to the MH. This time is mainly dependent on the packet size and the transmission data rate. For low data rate applications, such as voice communications, the transmission takes a significant amount of time. In this case, the Packet Reception Time will have a significant effect on the overall handoff latency. In our scheme, the network will adjust the packet size according to the application data rate. Therefore, the packet size will be small (or large) depending on the transmission data rate of the underlying application.

Note that the use of smaller packet size has an impact on the amount of packet lost. A smaller packet size results in a short packet transmission time. Hence, the duration of which packet loss occurs also gets smaller [3]. Since our focus is on the handoff latency and not on the system throughput, we have not considered the effect of packet loss here. For more details on the system throughput and probability of packet loss, the reader is referred to. Even though the proposed adaptive packet size technique may lead to a large reduction in the handoff latency, lowering the packet size will have an impact on the associated transmission are accompanied with a considerably large header size. However using header compression techniques, this problem can be greatly eliminated. Results have been for the handoffs in a network model to observe the distribution of handoff latency using the standard mobile IP multicasting technique compared to our proposed multicasting technique.

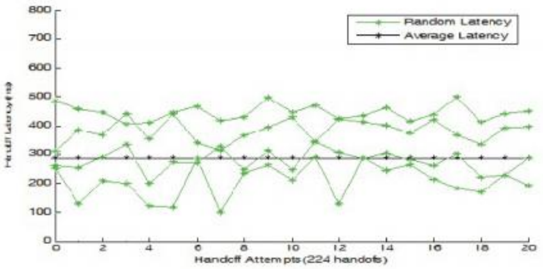


Figure 6.3: Handoff latency distribution using the standard multicasting mobile IP with 224 random handoffs.

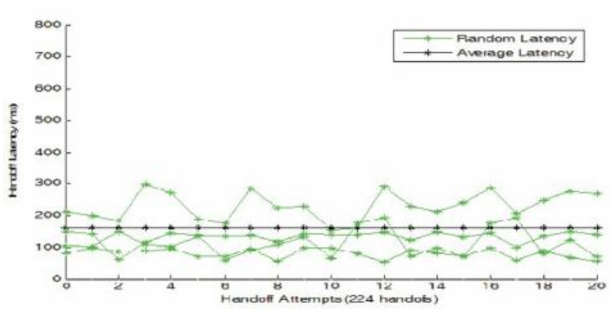


Figure 6.4: Handoff latency distribution using the proposed improvement.

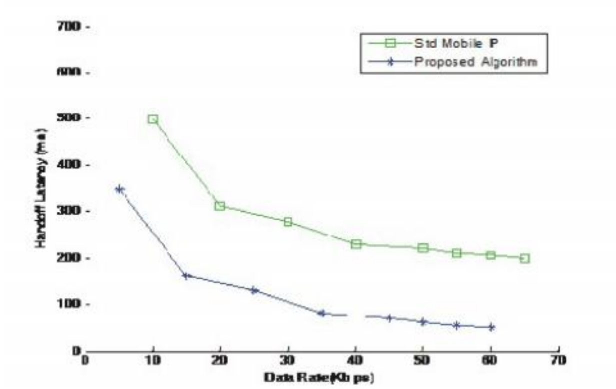


Figure 6.5: Comparison of handoff latency for different data rates. Standard mobile IP versus proposed algorithm.

Chapter 08 Performance Evaluation-Adhoc Network

For the develop protocol the performance were evaluated with the following network parameter.

Distribution	Random
Number of Nodes	17
Region	280 x 300 units
Communication Range	80 units
Mobility	Static
MAC:	802.11
Packet Size	61 bits
Weight (w)	0.1
Trustworthy Threshold (t)	0.75
Node status threshold (r)	0.5

Table 7.1: Network Parameters

8.1. Considered Network for Simulation

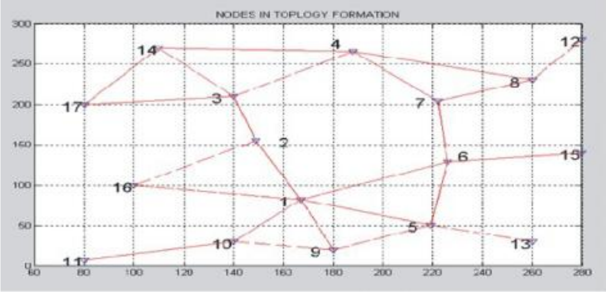


Fig 7.2: A randomly distributed network considered for simulation

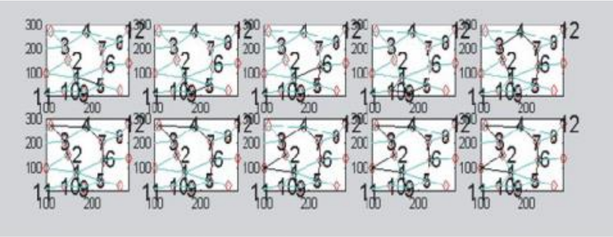


Fig7.3: Possible paths from source to Destination with 1 hop link

Few quality factors were observed for the developed network the obtained quality metrics were observed and the performances were as obtained.

8.2. Delay Performance

Fig 7.4 shows average delay as the number of sleep cycles in a beacon periods are increased. As can be seen, delay goes on decreasing as number of sleep cycles per beacon period is increased. This is because, to deliver packet at the last hop, RIMA node has to wait for less amount of time, if number of sleep cycle per beacon period is more. It can also be seen that with load distribution delay has been reduced. For more number of sleep cycle per beacon period, average delay drops.

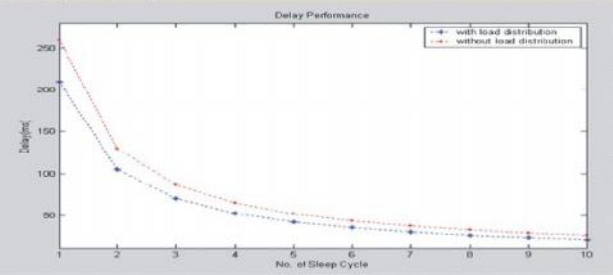


Fig7.4: Average delay for CBR traffic

8.3. Overhead Messages Per Node

Fig 7.5 shows the comparison of overhead messages of topology management scheme and routing as the number of nodes increase. Number of overhead messages per node per second decrease as number of nodes increase. Also it can been seen that overhead messages per node per second with Topology Management scheme is less as compared with flat topology.

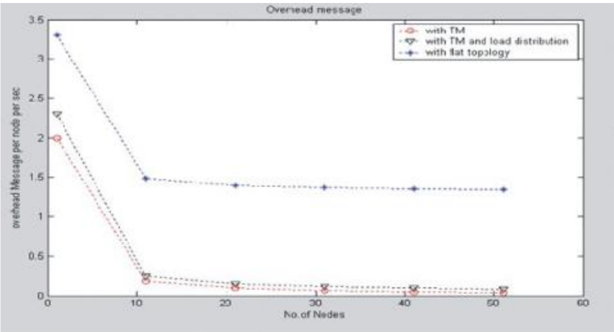


Fig 7.5: Overhead messages per node per second

8.4. Power Consumption

Fig 7.6 shows the average power consumption, as node density increases. It can be noticed that as node density increases, average power consumption per node is much less in Topology Management scheme, as compared to flat Topology network. For more node density, there are less number of MARI and gateway nodes, which are awake all the time and large number of member nodes are in power efficient mode, most of the time.

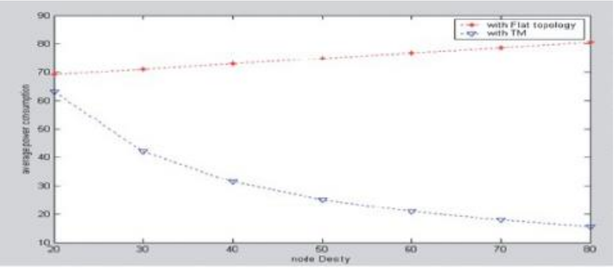


Fig 7.6: Average power consumption as node density increases

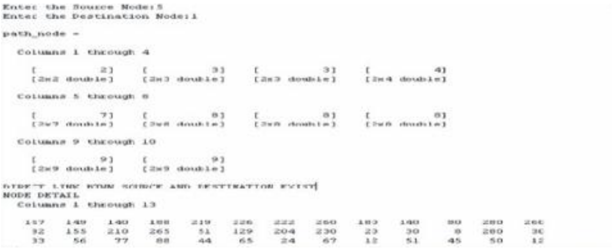
8.5. The Network Performance Evaluation

This module simulates the network for various combinations with misbehaving varying from 0 to maximum limit. This module evaluates transmitting delay, excess HOP count, good put and number of rejected paths to decide the efficiency of RMP for randomly distributed Ad-hoc network.

The developed system is evaluated over different case studies with various communication conditions, the observing parameters were evaluated with variable path from source to destinations. The obtained observations were illustrated below,

CASE I:

SHORTEST PATH, 1 HOP (Direct Link Between Source And Destination)



```
Enter the Source Node:5
Enter the Destination Node:1

path_node =

  Columns 1 through 4

    [           2]    [           3]    [           3]    [           4]
    [2x2 double]    [2x3 double]    [2x3 double]    [2x4 double]

  Columns 5 through 8

    [           7]    [           8]    [           8]    [           8]
    [2x7 double]    [2x8 double]    [2x8 double]    [2x8 double]

  Columns 9 through 10

    [           9]    [           9]
    [2x9 double]    [2x9 double]

DIRECT LINK BTWN SOURCE AND DESTINATION EXIST
NODE DETAIL
  Columns 1 through 13

   157   149   140   188   219   226   222   260   183   140    80   280   26
    92   155   210   265    51   129   204   230    23    30     8   280   3
    33    56    77    88    44    65    24    67    12    51    45    50   12
```

Fig 7.7: Output of Direct link between source and destination

CASE II:

SHORTEST PATH, MORE THAN 1 HOP (with Intermediate Nodes Between Source And Destination)

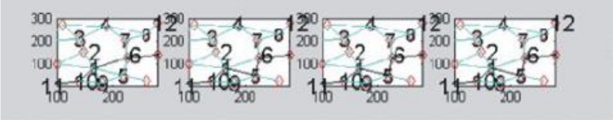
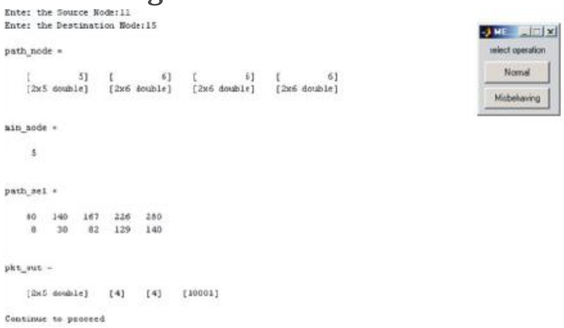


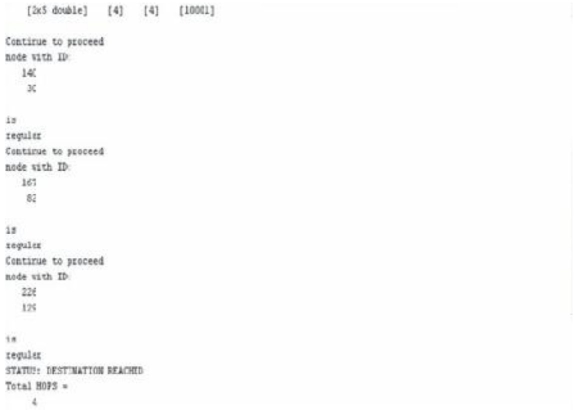
Fig 7.8: Paths from source to destination with more than one hope

a. With Regular Nodes



```
Enter the Source Node:11
Enter the Destination Node:15

path_node =

    [          5]    [          6]    [          6]    [          6]
    [2x5 double]    [2x6 double]    [2x6 double]    [2x6 double]


min_node =

     5


path_sel =

    80   140   167   226   280
     8    30    82   129   140


pkt_out =

    [2x5 double]    [4]    [4]    [10001]

Continue to proceed
```

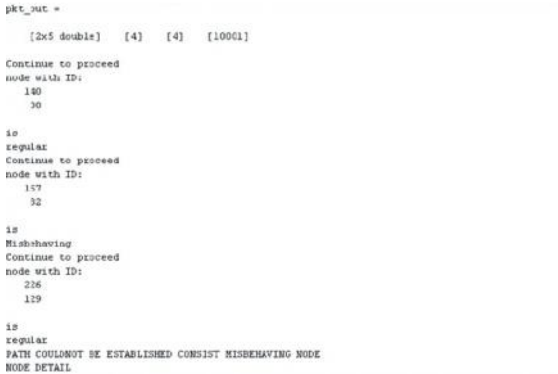
Fig 7.9: Output of shortest path consisting of regular nodes



```
    [2x5 double]    [4]    [4]    [10001]

Continue to proceed
node with ID:
   140
    30

is
regular
Continue to proceed
node with ID:
   167
    82

is
regular
Continue to proceed
node with ID:
   226
   129

is
regular
STATUS: DESTINATION REACHED
Total HOPS =
     4
```

Fig 7.10: Details of data flow with regular nodes

b. With Malicious nodes

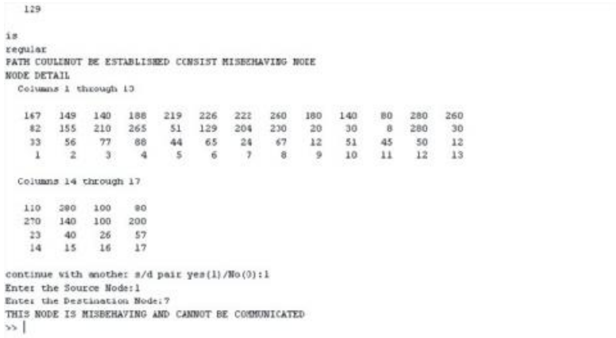


```
pkt_out =

    [2x5 double]    [4]    [4]    [10001]

Continue to proceed
node with ID:
   140
    30

is
regular
Continue to proceed
node with ID:
   157
    32

is
Misbehaving
Continue to proceed
node with ID:
   226
   129

is
regular
PATH COULDNOT BE ESTABLISHED CONSIST MISBEHAVING NODE
NODE DETAIL
```

Fig7.11: outputs off shortest path consisting of malicious nodes

CASE III

MALICIOUS NODE AS SOURCE



```
   129

is
regular
PATH COULDNOT BE ESTABLISHED CONSIST MISBEHAVING NODE
NODE DETAIL
  Columns 1 through 13

   167   149   140   188   219   226   222   260   180   140    80   280   260
    82   155   210   265    51   129   204   230    20    30     8   280    30
    33    56    77    88    44    65    24    67    12    51    45    50    12
     1     2     3     4     5     6     7     8     9    10    11    12    13

  Columns 14 through 17

   110   280   100    80
   270   140   100   200
    23    40    26    57
    14    15    16    17

continue with another s/d pair yes(1)/No(0):1
Enter the Source Node:1
Enter the Destination Node:7
THIS NODE IS MISBEHAVING AND CANNOT BE COMMUNICATED
>> |
```

Fig 7.12: Output with malicious node as source

8.6. Analysis

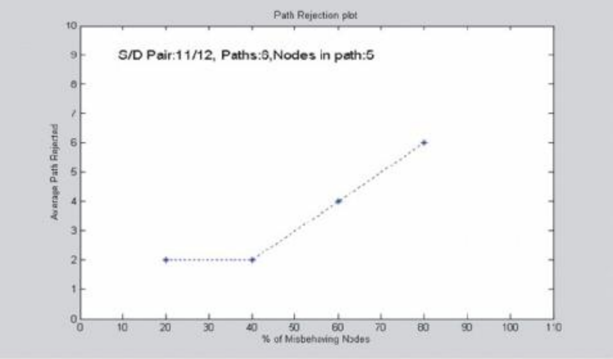


Fig 7.13: Average path rejections wrt. Misbehaving nodes

The average rejected paths increases if percentage of malicious nodes increases but with the use of RMP average paths rejected remains constant even if the percentage ;of malicious nodes increases to 40%.

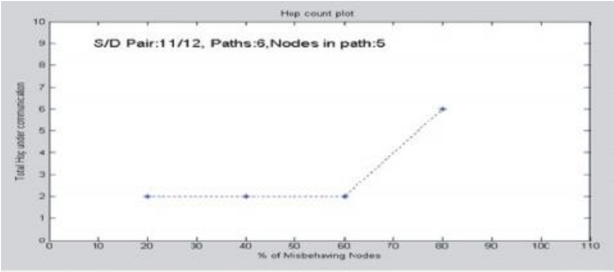


Fig7.14: Total Hops under communication wrt. Percentage of misbehavior plot

The number of rejected path from the source to destination increases as percentage of misbehaving nodes increases hence the number of hop counts required for communication also increases. The total hop counts for communication remains constant with the use of RMP (Route Management protocol) even if percentage of malicious nodes increases to 60%.

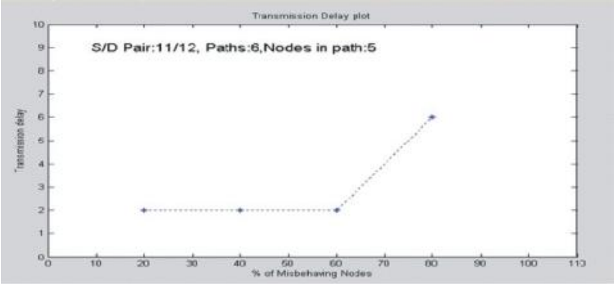


Fig7.15: Transmission Delay versus % Misbehavior plot

The packet transmission delay increases with the increase in percentage of malicious nodes but with use of RMP (Route Management Protocol) the transmission delay remains constant even if the percentage of malicious nodes increases to 60%

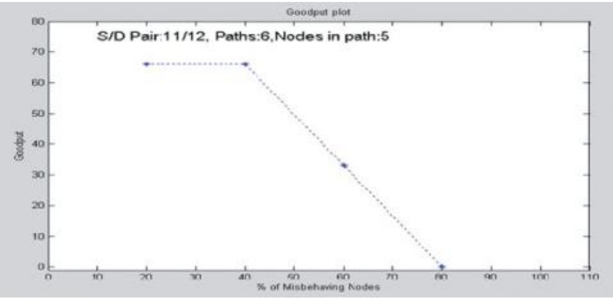


Fig 7.16: Goodput plot for the network

Observation

% Misbehaving Nodes	20%	40%	60%	80%
No. of Rejected path	2	2	4	6
Total Hops under communication	2	2	2	6
Transmission delay in seconds	2	2	2	6
% Goodput	66.67	66.67	33.33	0

The performances were illustrated for the suggested keying mechanism and the performance for obtained robust routings were as shown below. The performance criterion for the evaluation of the suggested method remains the same with variable route lengths, the delay performance and the repository updation factor.

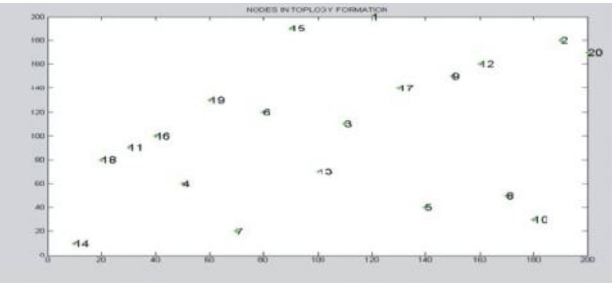


Fig:7.17: keying mechanism for roust rout

Case 1:

With No Add-on nodes

Generated load: one byte

Source node:18

Destination node:12

Route taken for communication from source to destination:

18→4→ 6→17→12

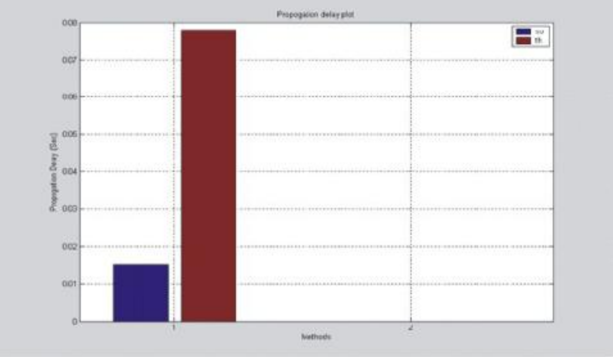


Fig 7.18 : Propagation delay plot

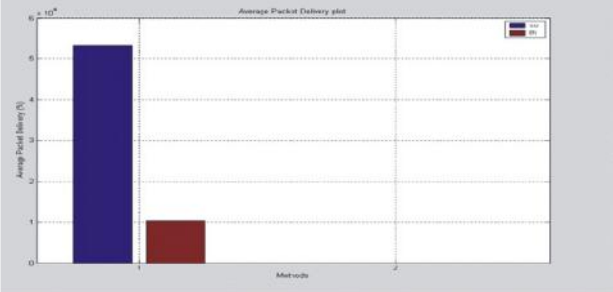


Fig 7.19: Average Packet Delivery plot

Case 2

Generated load: one byte

Source node:14

Destination node:20

With No Add-on nodes

Route taken for communication from source to destination:

14→4→ 6→3→9→20

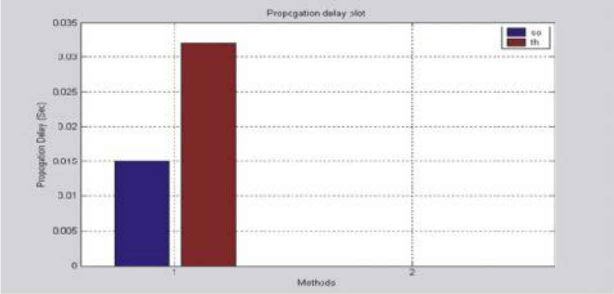


Fig 7.20: Propagation delay plot

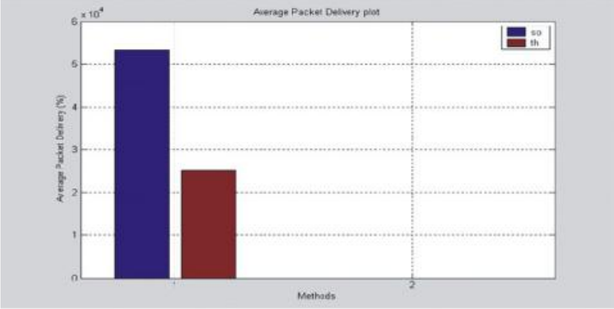


Fig 7.21: Average Packet Delivery plot

Case 3

Source node:14

Destination node:20

Generated load : four bytes

With no add on nodes

Route taken for communication from source to destination:

14→4→ 6→3→9→ 20

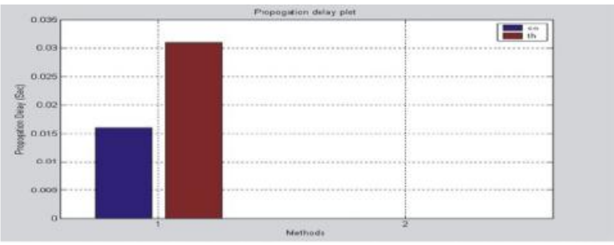


Fig 7.22: Propagation delay plot

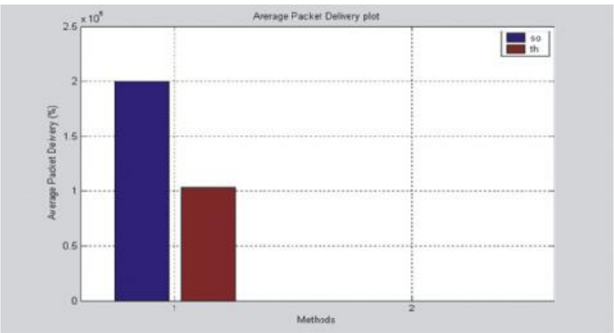


Fig 7.23: Average Packet Delivery plot

Case 4

Source node:14

Destination node:20

Generated load : four bytes

With 2 add on nodes

Route taken for communication from source to destination:

14→4→ 6→3→9→ 20

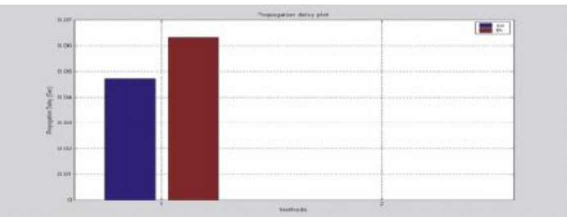


Fig 7.24: Propagation delay plot

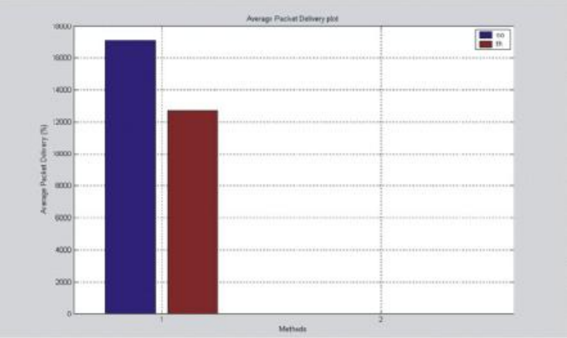


Fig 7.25: Average packet delivery plot

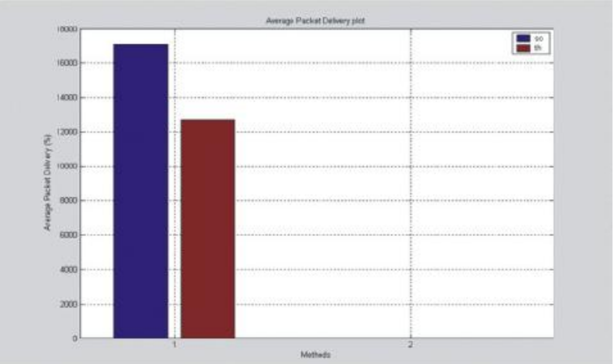


Fig 7.25: Average Packet Delivery plot

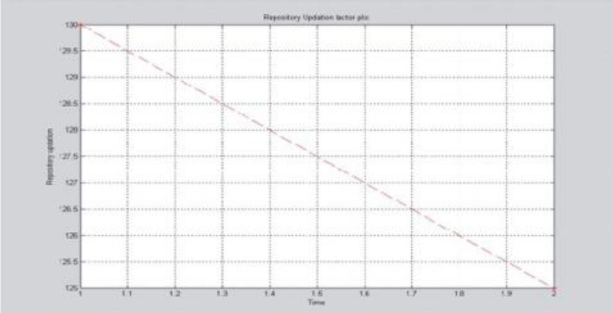


Fig 7.26: Repository Updation plot

Summary

In this work, the problem of key management in mobile adhoc networks is addressed. A fully self-monitored key management system for mobile adhoc networks is developed and it is observed that two users in a mobile ad hoc network can perform key authentication based only on their local information, even if security is performed in a self-monitored way, it is shown that with a simple local repository construction algorithm and a small communication overhead, the system achieves high performance on a wide range of certificate graphs; (iv) it is also shown that nodes can have mobility to facilitate authentication and to detect inconsistent and false certificates. An important feature of this scheme is that key authentication is still possible even when the network is partitioned and nodes can communicate with only a subset of other nodes. In this method the involvement of all the nodes are required only when their key pairs are created and for issuing and revoking certificates; all other operations including certificate exchange and construction of certificate repositories are self monitored. it is concluded that node with RMP can sustain the network with efficient data transmission for 50% of misbehaving node. The proposed approaches are evaluated under various network scenarios and are found to be effective in their qualitative performance of operation. In the presented work the need of security authentication and reliability is been focused, the problems coming in providing such services and their suggestive remedies are been focused and presented. the overall observation illustrates that the suggested approach can give a better performance for reliable, secure and robust routing scheme for wireless adhoc network compared to their conventional counterpart.

The proposed work is been focused on providing reliable, secure and resource effective protocol scheme for wireless adhoc network communication. the work could be extended on testing its feasibility and application on other format of network such as

heterogeneous network and hybrid network. the objective can also be tested and improved for providing various mode of synchronous and asynchronous communication in adhoc network.

About author

Dr. T. K. Shaik Shavali

Dr. T. K. Shaik Shavali is Head of the Department and Professor in Computer Science and Engineering in Lords Institute of Engineering and Technology, Hyderabad, completed his Ph.D from Sri Krishna Devaraya University (SKU), Ananthapuramu. A.P. He has 21 years experience in teaching and 9 years in Industry and has 20 publications in International Journals and 3 patents.

9 788195 308316

₹ 500

ADITI PUBLICATION

Near Ice Factory, Opp. Shakti Sound, Service Gali, Kushalpur, Raipur (C.G.)
Mob. 91 94252 10308, E-mail:shodhsamagam1@gmail.com, www.shodhsamagam.com