University of Bedfordshire

Title An Energy-Aware and QOS Assured Wireless Multi-Hop Transmission Protocol

Name Yu Lin

AN ENERGY-AWARE AND QOS ASSURED WIRELESS MULTI-HOP TRANSMISSION PROTOCOL

By

Yu Lin

A thesis submitted in fulfillment of the requirements for the degree of Master of Science by research

May, 2011

Abstract

The Ad-hoc network is set up with multiple wireless devices without any pre-existing infrastructure. It usually supports best-effort traffic and occasionally some kinds of Quality of Service (QoS). However, there are some applications with real-time traffic requirements where deadlines must be met. To meet deadlines, the communication network has to support the timely delivery of inter-task messages. Furthermore, energy efficiency is a critical issue for battery-powered mobile devices in ad-hoc networks. Thus, A QoS guaranteed and energy-aware transmission scheme is one hot of research topics in the research area.

The MSc research work is based on the idea of Real-Time Wireless Multi-hop Protocol (RT-WMP). RT-WMP is a well known protocol originally used in the robots control area. It allows wireless real-time traffic in relatively small mobile ad-hoc networks using the low-cost commercial IEEE 802.11 technology. The proposed scheme is based on a token-passing approach and message exchange is priority based. The idea of energy-aware routing mechanism is based on the AODV protocol. This energy-saving mechanism is analysed and simulated in our study as an extension of the RT-WMP.

From the simulation results and analysis, it has been shown that adding energy-aware mechanism to RT-WMP is meaningful to optimise the performance of traffic on the network.

DECLARATION

I declare that this thesis is my own unaided work. It is being submitted for the degree of Master of Science by Research at the University of Bedfordshire.

It has not been submitted before for any degree or examination in any other university.

Name of candidate: Yu Lin

Signature: ____________________

Date: ____________________

ACKNOWLEDGMENT

I wish to thank to my supervisor Dr. Sijing Zhang of the Department of Computer Science and Technology, University of Bedfordshire, for his guidance and supervision of the research work and this dissertation.

Thanks are given to Xiao Guo and Tao Cao for their help with experiment, valuable suggestions and proof reading.

My thanks also go to my family, for their support and encouragement during the year of study.

TABLE OF CONTANT

TABLE OF FIGURES

LIST OF TABLES

Chapter 1. Introduction

Wireless communication between mobile users is becoming more popular than ever before. This is due to the recent technical development in laptop computers and wireless data communication devices. This has lead to lower price and higher data rates, which are the two main reasons why mobile computing continues to enjoy rapid growth.

There are mainly two distinct approaches for enabling wireless communication between two hosts. The first one is to let the existing cellular network infrastructure carry data as well as voice. The major problems with this approach include the problem of handoff, which tries to handle the situation when a connection should be smoothly handed over from one base station to another base station without noticeable delay or packet loss. Another problem is that networks based on the cellular infrastructure are limited to places where there exists such a cellular network infrastructure.

The second approach is to form an ad-hoc network among all users wanting to communicate with each others. This means that all users participating in the ad-hoc network must be willing to help forward data packets to make sure that the packet are delivered from source to destination. This form of networking is limited in range by the individual nodes transmission ranges and is typically smaller compared to the range of cellular system. This does not means that the cellular approach is better than the ad-hoc approach. Ad-hoc networks have several advantages compared to traditional cellular systems. These advantages include [2]:

- On demand setup
- Fault tolerance
- Unconstrained connectivity

Ad-hoc networks do not rely on any pre-established infrastructure and can therefore be deployed in place with no infrastructure. This is useful in disaster recovery situation and places with non-existing or damaged communication infrastructure where rapid deployment of a communication network is needed. Ad-hoc networks can also be used on conference where people participating in the conference can form a temporary network without engaging the service of any pre-existing network.

Ad-hoc networks usually support for best-effort traffic, and in some applications, such as multimedia, can offer some kind of Quality of Service (QoS) like, for example, minimum bandwidth guarantee, maximization throughput and timely delivery of data between the nodes. On the other hand, due to the limited battery power mobile device, transmitting the data in an energy saving model has became a hot-spot research topic. Our research motivation is to develop a novel priority based transmission scheme which can transmit data traffic over ad-hoc network in an energy-efficient manner with certain level of QoS guarantee.

The aim of this study is to develop an enhanced energy efficient transmission scheme based on the well known Real-time Wireless Multi-hop Protocol: RT-WMP

[1], and carry out a comparison evaluation of QoS and energy-efficiency performance of the proposed scheme with the RT-WMP.

In order to achieve the objections, the following tasks have been set in the original proposal:

- To review the published relevant studies which focus on the support to real-time traffic and energy efficient routing protocols over the ad-hoc network.
- To review the RT-WMP scheme and analysis its QoS performance.
- To develop an energy efficient approach based on AODV routing protocol.
- To apply the developed energy efficient approach on the optimization of RT-WMP scheme.
- To simulate the proposed scheme with related QoS performance parameters, and to compare the simulation result of the proposed scheme with RT-WMP scheme, in order to evaluate the performance of the proposed scheme.

This study has been carried out through literature review, comparative analysis and evaluation of an enhanced scheme which are aided by simulation experiments.

The rest of this thesis is organized as follows: Chapter 2 describes the relevant research in the areas of real-time communication the background knowledge of our proposed scheme and the main research areas in real-time traffic and energy efficient routing protocol over ad-hoc network. Chapter 3 introduces the relevant background knowledge of our thesis; Chapter 4 introduces the original RT-WMP protocol and gives an analysis of this scheme, finally, a proposed contribution of my thesis is given. Chapter 5 introduces a priority based wireless multi-hop protocol which based on the

RT-WMP protocol. In Chapter 6, an energy efficient routing scheme which based on the AODV protocol is proposed. Chapter 7 gives an experiment to verify the whole improved RT-WMP scheme and the original RT-WMP with an analysis of the results. Chapter 8 draws conclusions and discusses further work.

Chapter 2. Literature Review

2.2 The Priority Scheduling in Wireless Ad Hoc Network

Medium Access Control (MAC) protocols that aim to provide differentiated services should be able to meet requirements of traffic with different priority classes. If a high priority flow's traffic pattern satisfies the behavior described in the service agreement, its packets should be delivered in preference to other packets with lower priorities. On the other hand, flows with lower priorities should use as much bandwidth as possible after the transmission requirements of higher priority flows have been satisfied. In general, there are two directions in wireless MAC protocols to facilitate channel access privilege of high priority traffic: reservation based schemes and contention based schemes.

2.2.1 Reservation Based Schemes

Reservation based schemes usually make some assumptions about high priority traffic. For example, high priority traffic is assumed to be periodic with fixed arrival rate. For reservation based schemes, when resources are reserved but unused, they are often wasted.

A typical example of a reservation based MAC protocol is GAMA/PS [3]. GAMA-PS divides time into a sequence of cycles; each cycle begins with a contention period and ends with a "group-transmission" period. The group-transmission period is divided into a set of zero or more individual transmission periods, each for a station in the "transmission group". A station with data to send competes for membership in the "transmission group" during the contention period; also, by listening to the channel, a group member becomes aware of how many stations are in the group and of its own position within the group. In this case, members of the transmission group take turn transmitting data, and collision is avoided. However, a basic requirement for this protocol is that each station can hear the transmissions of other stations, which limits the use of the protocol to wireless LANs.

The MACA/PR protocol [4] extends the reservation based scheme to multi-hop networks. The first data packet of a high priority flow makes reservations along the route to the destination. Each station maintains a reservation table (RT) which keeps track of the transmitting and receiving "reserved windows" for neighbors within a two-hop neighborhood. Low priority sources are only allowed to fill in empty windows. In order for the reservation scheme to work, the size of high priority packets must be pre-specified for each connection, and the size of low priority packets must be bounded so as not to interfere with the reservation constraints.

2.2.2 Contention Based Scheme

Unlike the reservation based schemes, contention based schemes are probabilistic. Flow scheduling decision is made locally, and contention is resolved probabilistically. For example, "black burst" can be used to help high priority flows contend for the channel [5]. After channel becomes idle, a high priority flow has shorter waiting time before it transmits the "black burst", other low priority flows which have a longer waiting time will drop out of contention once they hear the "black burst" during their waiting time. This scheme thus provides a way for the high priority source stations in a wireless LAN to reserve the channel by occupying the channel with "black burst". Sobribo and Krisbnaknmar [6] further generalizes this scheme for using in ad hoc CSMA wireless network, in their work, it is assumed that there no hidden nodes in a wireless network. That is, each source station in such a network can always sense the possible interfering transmissions. However, this is not the case in most ad hoc networks. More often, "hidden terminals" do exist in ad hoc networks, and nodes cannot always sense each other's transmissions. Thus, the scheme in [6] cannot be applied to general ad hoc networks.

Several researchers propose some simple modifications to the IEEE 802.11 Distributed Coordination Function (DCF) to incorporate differentiated service. IEEE 802.11 DCF defines a collision avoidance mechanism to resolve contention among different stations willing to access the medium. Each station chooses a random number between zero and a given "Contention Window" as the back-off duration. There are two "waiting stages" in IEEE 802.11 before the station accesses the channel.

- The "inter-frame space" (IFS) stage.
- The back-off stage, whose duration is a random value between zero and the "Contention Window".

Various schemes [7], [8], [9] and [10] have been proposed to modify the back-off stage so that source stations with different priorities can use different "Contention Window" generation functions. For example, it is proposed in [7] that high priority source stations randomly choose the back-off interval from $[0, 2^{i+1}-1]$ and low priority source stations choose from $[2^{i+1}, 2^{i+2}-1]$, where i is the number of consecutive times a station attempts to send a packet. The setting of different values of *CWmin* and *CWmax* for different priority classes is proposed in [9]. It is proposed in [8] that instead of using the exponential factor after a collision, different priority classes use different exponential increase factors. Stations with lower priority increase their "Contention Window" much faster than the stations with higher priority. One drawback faced by [7], [9] and [8] is that high priority flows may possibly experience more collisions compared to their low priority counterparts in multi-hop networks. As a result, "high priority" flows cannot be ensured to have smaller "Contention Window", hence, the priority of channel access cannot be ensured either. In order to adapt better to multi-hop networks, it is proposed in [10], a packet's priority information is piggybacked in the RTS/CTS/Data/ACK frames. Based on overheard packets, each station maintains a scheduling table, which records priority information of flows that are within two hops neighborhood. The back-off duration is generated based on the scheduling table. However, this scheme suffers from incomplete scheduling table which is caused by collisions, location dependent errors, node mobility and partially overlapping transmission regions.

2.3 The QoS Routing Scheme in Ad Hoc Network

2.3.1 Routing scheme

Network routing in MANETs can be classified into three classes: *proactive, reactive, and hybrid.* Routing schemes use control messages to learn the network topology. Most proactive routing schemes use link state or distance vector routing algorithms.

Reactive Routing Protocols

Reactive routing is an on-demand routing scheme. Nodes learn about the network topology on an as-needed basis. Two of the better known reactive ad hoc routing protocols are Dynamic Source Routing (DSR) [11] and Ad hoc On-demand Distance Vector (AODV) [12].

Reactive routing protocols are characterized by two phases: *the route discovery phase* and *the route maintenance phase*. In the route discovery phase, nodes build their routing tables on demand. The sending node sends a route request for a packet in its sending queue for which it has no route information to the destination or whenever a node receives a packet not destined to it for which it has no route information to the destination. Nodes send route inquiries to neighbors and add an entry to a list of previously discovered routes. For example, in AODV, nodes along the route store the route information, while in DSR the initiating node stores the source route returned to it from the route reply. The route maintenance phase uses route error packets and acknowledgments to maintain routes. Each node that sends a packet gets an acknowledgment back. Acknowledgments are either received at the link layer as defined by the MAC protocol of IEEE 802.11, or as passive acknowledgment from the receiving node. If the receiving node fails to acknowledge the receipt of the packet, a route error is relayed back to the original sender which will result in the removal of the broken link from its cache and use an alternative route if available or initiate a new route discovery. Route discovery and route maintenance do consume bandwidth. Sholander, *et al.* [13] proposed that reactive routing is preferable over proactive in situations where route concentration, route activity, and the number of active routes per node are low and mobility is high.

Proactive Routing Protocols

- In proactive routing, nodes periodically monitor the network for changes in network topology. Therefore, every node in the network keeps an up-to-date copy of current network topology information by periodically broadcasting and receiving control packets. For instance, when a node receives a packet destined to another node, it knows how and where to forward the packet for final delivery of the packet. This relatively detailed information about the topology helps to improve the routing performance. However, this improvement in routing may come at a cost of increased overhead and a decrease in network capacity for data. Several proactive routing exist for MANETs. Two commonly referenced ones are Optimised Link State Routing (OLSR) [14] and Destination Sequenced Distance Vector Routing (DSDV) [15]. The way in which network topology information is gathered in proactive routing protocols is usually based on either of the above two commonly used routing algorithms, *link state* and *distance vector*.

- ***Link State Protocols***: In a link state protocol, each node keeps track of the changes that the network undergoes by keeping a map that reflects the state of all links in the network. Nodes use flooding, perhaps with some optimizations, to broadcast the link costs of their outgoing links to all neighboring nodes [15]. By exchanging link state, nodes learn the topology of the network. Each node creates a link-state packet that contains its identifier (ID), a list of its directly connected neighbors along with its cost to each one of them, a sequence number, and a time-to-live (TTL) value for the packet. These packets are broadcast whenever the TTL period expires or when the network topology changes. Link state routing is divided into two steps, flooding the network with link state information and the computation of routes based on link-state information using, typically, Dijkstra shortest path algorithm [15][16].
- ***Distance Vector Protocols:*** Distance vector protocols are based on the assumption that each node knows the distance (cost) to each of its immediate neighbors [15][16]. Thus, in distance vector protocols, all nodes create a list of distances to their immediate neighbors and distribute this list to their immediate neighbors. Initially, each node assigns a cost of one to each of its immediate neighbors and a cost of infinity to other nodes. Afterwards, the nodes exchange these lists with all of their immediate neighbors and start to replace the large costs with lower ones based on the received lists. Distance vector protocols suffer from several problems. The count-to infinity problem occurs when a node fails and, as

such, its neighbors keep increasing their cost to reach this node until they reach an infinite value [15]. Another problem with distance vector protocols is the slow convergence of routes throughout the network. By storing little information about links that are not directly connected to the node running the algorithm, distance vector protocols have lower complexity than link state protocols. In addition, the bandwidth requirement is also less [15].

Hybrid Routing Protocols

Hybrid routing protocols combine the use of reactive and proactive routing protocols to obtain a better balance between the dynamic nature of MANETs and the routing overhead and to reduce the average end-to-end delay [17]. These protocols usually introduce a hierarchical structure to the MANET to reduce the number of control packet retransmissions during route discovery [18]. In hybrid routing protocols, each node maintains a set of nearby neighbors with which it will use a proactive routing scheme and a set of more distant nodes with which it will use a reactive routing scheme. The use of different routing strategies at different times at different locations is used in routing protocols such as the Zone Routing Protocol (ZRP) [19] [17].

2.3.2 QoS aware routing scheme

QoS aware routing is one of the most essential parts of the Quality of Service framework for wireless networks. Under QoS routing schemes, the data delivery routes are computed with the knowledge of availability of various resources in the network along with the QoS requirements of the corresponding flows. There are several issues to be considered during the design of the QoS based routing algorithms for multi-hop networks. These issues include:

- Metric selection (e.g., bandwidth, delay etc) and route computation;
- QoS state propagation and maintenance;
- Scalability;
- Domain of QoS such as reliability or timeliness (or both);

In certain types of wireless sensor networks, the QoS aware routing protocols have to deal with imprecise state information due to the frequent topology changes. Moreover a QoS aware routing scheme for multi-hop networks should also balance efficiency with adaptability while maintaining low control overhead in the system.

In recent years, several routing algorithms have been proposed to provide QoS in multi-hop networks. Some of these algorithms are briefly discussed below:

SPEED* [20]*:

This is a QoS aware soft real time routing protocol develop for Wireless Sensor Networks which helps ensures end to end QoS guarantees [20]. Three types of real time communication services are provided by this protocol. They are *real-time uni-cast*, *real- time area multicast* and *real time area any cast* [21]. With this protocol each node maintains information about its neighbors and utilizes geographic forwarding technique to find a path. It also tries to maintain a certain delivery speed for each packet in the network. SPEED maintains this speed by diverting the traffic at the network layer and regulating the traffic passed onto the MAC layer. The aim of these actions is to estimate end to end delay for the packets by dividing the distance to sink [20]. This is done before an admission decision is taken. SPEED can also provide congestion avoidance in the event of congestion in the network. SPEED has a routing module called "Stateless Geographic Nondeterministic Forwarding" (SNGF). It works with other four modules at the network layer.

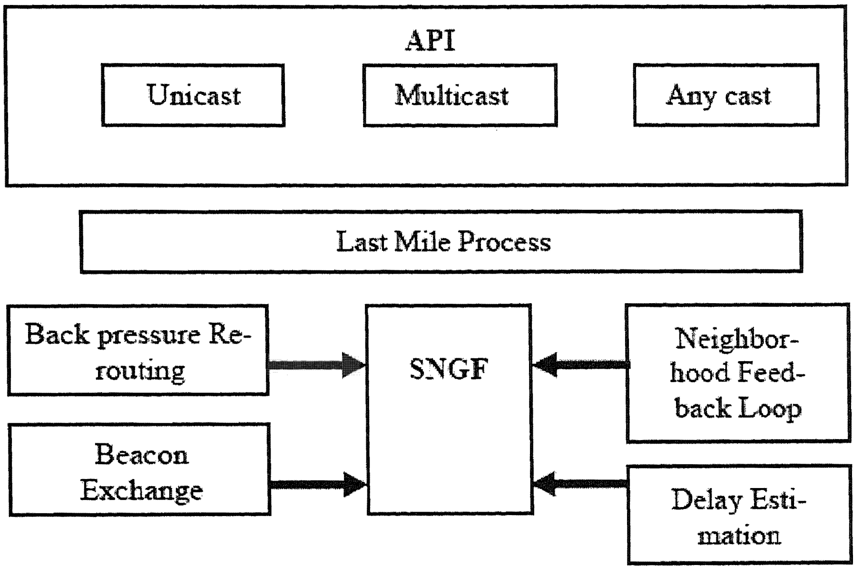


Fig 2.1 The procedure of SPEED which redrawn from [21]

The relationship of SNGF with other modules is shown in **Fig 2.1,** which is redrawn from [21]. The Backpressure Rerouting module works in collaboration with Neighborhood Feedback Loop (NFL) module and SNGF to reduce or divert traffic in the event of congestion. The Beacon Exchange module gathers information about the geographic location of its neighbor nodes to do geographic based routing by the SNGF module. Delay Estimation module is used to determine the occurrence of congestion in the network. It is done by calculating the elapsed time between the completion of a transmitted data packet and the reception of its corresponding acknowledgement packet. The Last Mile Process provides the required functions for implementing three communication services mentioned above.

Energy Aware Routing **[22]*:***

This protocol finds a least cost and energy efficient path that meets end to end delay during its connection [22]. The cost of a link is a function of a node's reserved energy, transmission energy, error rate and some other communication parameters. Imaging sensors are used to generate real time traffic. In this protocol a class based queuing model is used for the support of real time traffic and best effort traffic which classify the services for real time and non real time traffic.

A list of minimum cost paths is determined by this protocol using an extended version of Dijkstra's algorithms. A path is then selected from that list which satisfies the end to end delay requirement. The gateway sets an initial bandwidth ratio as the amount of bandwidth to be dedicated both to the non real time and real time traffic on a particular outgoing link.

Multi-Path Multi-Speed Protocol (MMSPEED) **[23]*:***

This protocol is an extension of SPEED [21] providing multi path multi speed transfer of packets across the network. The protocol spans over network layer and MAC layer and provides QoS support in terms of reliability and timeliness [23]. The protocol does probabilistic multi-path packet forwarding to meet various reliability requirements. It also provides multi network wide speed in such way that the various packets can choose the appropriate speed dynamically depending on the end to end deadlines. That is, packets can choose the best combination of service options depending on the reliability and timeliness requirements. This protocol also makes provision for end to end QoS with local decision at each intermediate node without doing path maintenance and end to end path discovery. The purpose of localized geographic forwarding is for scalability of larger sensor networks, adaptability to dynamic sensor networks and appropriateness to both periodic and non periodic traffic flows. To ensure end to end QoS provision results in a global sense, the concept of dynamic compensation is proposed which compensates inaccuracy of local decision in a global way as packets traverse toward the destination. Although packet forwarding decisions are made locally, packets can meet their end to end requirement with high probability. Although this protocol provides QoS support in timeliness and reliability domain, efficient power consumption has not been taken into account in the proposed protocol.

Mobile Object Tracking-Mobicast* [24]*:

This protocol deals with a multicast based routing protocol to track a mobile object dynamically [24]. It guides a mobile user to chase a mobile object accurately without flooding request to locate the mobile object. This protocol helps in saving power consumption of the sensor nodes, and as a result overall life time of the sensor network is increased. A mobile user is called source and the mobile object is called target. The sensor network helps the source detecting the target and keeping the tracked information of the target. To save energy, some of the senor nodes remain in active state while others are in sleeping state. The sensor that keeps the track information of the target acts as a beacon node. It waits for the source and guides the source in chasing the target. The source does not need to frequently send request packets to the present location of target in the course of chasing. The sensor also does not require to transmit the present location of the target when the source detects the target. When the source reaches the location of the beacon sensor, it makes a query asking about the present location of the target or the location of the next beacon sensor. This protocol uses face routing [25] based on the concept of Gabriel Graph [26] for tracking the target accurately. It also considers the moving direction and velocity of the target. The experimental results show that the protocol can save more energy than any of other flooding based protocols used in object tracking.

Directed Alternative Spanning Tree (DAST) [27]*:*

DAST Considers three important QoS parameters, namely *energy efficiency*, *network communication traffic* and *failure tolerance* (*i.e,* reliability) [27]. In this protocol a directed tree-based model is constructed to make data transmission more efficient. A Markov based communication state predicting mechanism is used to choose a reasonable parent, and packet transmission to double-parent is submitted with an alternative algorithm. Various nodes in the network are prioritized in order to decide different functions of nodes in WSN. It is worthy to mention that DAST enable data aggregation.

Real-Time Wireless Multi-hop Protocol (RT-WMP) [1]*:*

RT-WMP [1] is a protocol for MANETs, It works over the 802.11 protocol and supports real-time traffic. In fact, end-to-end message delay in RT-WMP has a bounded and known duration and the protocol also manages global static message priorities. Besides, RT-WMP supports multi-hop communications. The protocol has been designed to connect a relatively small group (10-20 units maximum) of mobile nodes. It is based on a token passing scheme and is designed to manage rapid topology changes through the exchange of a matrix containing link quality among nodes. RT-WMP has an error recovery mechanism that can recover from certain types of errors without jeopardizing real-time behavior. It was a technique for reincorporating lost nodes.

RT-WMP has been widely used in mobile robots communication. It also forms the base for our proposed scheme. Our main contribution is to add an energy saving mechanism in the original RT-WMP protocol.

2.4 Energy Conservation Scheme in Ad Hoc Network

A number of power saving techniques have been proposed to minimize power consumption in WLANs. While there are some schemes proposed for ad hoc WLANs, the majority of the proposed schemes are meant for infrastructure-based WLANs. These schemes can be categorized into physical, link (MAC), network, transport and application layer approaches or a mix of these approaches. Some of these schemes are adaptive, others are non-adaptive. The main of the proposed energy conserving approaches include:

1. Turning off the network interface card (NIC) when the node is not actively engaged in communication [28];

2. Adjusting the power level according to the packet size [29];
3. Partitioning the network into different clusters and allowing each cluster to use a different spreading code [30];
4. Using transmission scheduling and slot reservation instead of contention-based schemes [31]; and
5. Using adaptive transmission strategies instead of persistent ones [32][29][30].

In multi-hop ad hoc networks, a large amount of energy may be wasted in listening by non-intended receivers. Since a lot of mobile devices are battery powered, this energy waste exacerbates the energy problem. Consequently, a lot of research has been conducted to improve the energy capacity of batteries and to reduce power consumption. From a computer engineering standpoint, reducing energy consumption helps prolong the network life, which increases communication time as opposed to reducing interference and solving the near-far problem as in code-division multiple access (CDMA) based systems [33].

2.4.1 Techniques at the Physical Layer

Techniques used in energy minimization at the physical layer include miniaturizing circuit components, using efficient channel coding techniques, and improving amplifier characteristics of radio frequency (RF) circuits. Communication, in general, requires a lot of processing which consumes energy. Therefore, a protocol designed to minimize energy must balance energy minimization with the opposing goals of error-free communication.

Lahriri, *et al.* [34] describe a new battery-driven system-level power management scheme, communication-based power management (CBPM), which aims to improve battery efficiency. CBPM regulates the execution of the various system components. System components are of two categories: *bus masters* and *bus slaves*. Bus masters are components that are capable of initiating a communication transaction such as central processing units and digital signal processors. Slaves, on the other hand, are components that respond to transactions initiated by masters such as memories. This scheme may delay the execution of some system components and adapt the current discharge of the system to suit the battery's characteristics.

2.4.2 Techniques at the MAC Layer

A comparison of power-saving techniques at the MAC layer in IEEE 802.11 and ETSI HIPERLAN is presented by Woesner, *et al.* [68]. In ad hoc networks, collisions and packet retransmissions deplete battery power unnecessarily. Therefore, it is highly recommended to avoid packet retransmissions as much as possible. Mobility is an inherent characteristic of ad-hoc networks. As mobility increases, collisions increase and, therefore, packet retransmissions increase. A transceiver switching from the receive state to the transmit state consumes energy [31]. As a result, protocols that use slot assignments as a scheduling mechanism suffer a large overhead. Thus, to reduce the turnaround time (i.e., the time it takes to transition from a receive state to a transmit state and *vice versa*) and minimize energy, it is preferable to reserve several contiguous slots when transmitting or receiving data [31]. Another solution in minimizing power consumption at the physical layer is to turn off the transmit/receive radio when the node does not anticipate any communication with other nodes. This technique is mentioned by Raghavendra and Singh [28]. Sivalingam, *et al.* [35] propose a reservation based scheduling approach in which nodes broadcast their transmission time schedules so that they can go into standby mode and switch back to active mode when their transmit time comes.

The Energy Conserving Medium Access Control (EC-MAC) protocol [35] [36] was developed with an energy conservation goal in mind. It was developed for an infrastructure based wireless network where a single workstation serves mobile nodes within its coverage area. The authors argue that this protocol can be extended to an ad hoc network by allowing the mobiles to elect a coordinator to perform the base station functions. Others have also devised new MAC protocols that take into account energy constraints [37]. Careful reservation and scheduling of packets help to enhance the performance of the protocol and reduce collisions. This avoids retransmissions and, hence, reduces power consumption [35]. El Gamal, *et al.* [36] use an algorithm, MoveRight, to solve a convex problem based on the idea that, in many channel coding schemes, lowering transmission power and increasing the duration of transmission leads to a significant reduction in transmission energy. The Power Aware Multi-Access (PAMAS) protocol modifies the Multiple Access with Collision Avoidance protocol (MACA) described by Karn [39]. PAMAS is based on the premise that by allowing separate channels for control and data packets, nodes know when and for how long to turn off their transceivers. Simulation results from the study show that a power savings of up to 70 percent can be achieved for a fully connected network [39].

2.4.3 Techniques at the Link layer

Avoiding and delaying transmissions when channel conditions are poor improve energy minimization. Rao, Zorzi and Ramesh [40] found that by improving currently used error control scheme to cater to limited energy devices produces favorable results. Therefore, persistence is not preferable when energy is a constraint. Due to the dynamic nature of wireless links, error rates due to fading, attenuation and interference are highly variable. As stated by Zorzi, *et al.* [40], error control schemes such as automatic repeat request (ARQ) and forward error correction (FEC) waste network bandwidth and consume energy. When using these techniques in wireless environments, care should be taken so that packet retransmission and error correction do not overwhelm the wireless channel. Lettieri, *et al.* [41] describe an adaptive error control architecture that incorporates adaptive error control with forward error correction. This scheme changes the error control scheme according to the stream's channel conditions over time. In wireless networks, channel conditions along with traffic characteristics dictate the type of error control scheme used. Agrawal, *et al.* [42] study the effect of dynamic power control and forward error correction on power consumption. In their study, each node determines the minimal power and forward error correction required that satisfy the QOS constraint. In their technique, the signal is encoded twice with different transmission powers acting as boundaries for the upper and lower bound of transmission power.

2.4.4 Techniques at the Network Layer

In wireless networks routing can be either through a base station, or access point, (as in the case of infrastructure wireless networks) or through the mobile nodes (as in the case of ad hoc networks). Routing in wireless networks must take into account node mobility and route management, and when energy-efficient routing is required, routing through nodes with ample energy is preferable when extending network life is the goal. Several schemes have been devised to minimize power usage [43] [44] [45] [46]. Singh, *et al.* [43] use power-aware metrics for route discovery in addition to using PAMAS as a MAC protocol for their study. They report an energy improvement from 40 percent to 70 percent. The algorithm which they use is based on lowest-cost, rather than shortest-hop, routing. Chang and Tassiulas [44] propose a routing algorithm that maximizes the battery life leading to a maximization of the network lifetime. It maximizes the network lifetime by balancing routing and energy consumption among nodes according to the battery's energy reserves. Another scheme is to use heuristics to adaptively adjust the transmit power whenever a topology change occurs, keeping in mind the connectivity of the network [47]. Banerjee and Misra [48] developed a transmission power adaptive algorithm that finds the minimum energy routing path. The authors also use analytical methods to find the optimum transmission energy on each individual path in a multi-hop wireless network.

In good channel conditions, more energy can be saved. Good channel conditions, generally, imply that packets can largely reach their destinations error free. This leads to fewer retransmissions and ultimately, to increased network life. Spyropoulos and Raghavendra [49] propose an energy-efficient routing and scheduling algorithm for use in nodes equipped with directional antennas. The authors argue that using omni-directional antennas leads to a large waste in energy since power is broadcast in all directions. Directional antennas can direct power toward the intended node. Wieselthier, *et al.* [50] propose a similar approach, but for connection-oriented multicast traffic. The authors argue that the network life can be extended by incorporating the node's residual energy into the cost function and equipping the nodes with directional antennas.

Feeney [51] has carried out simulations and experimental measurements of energy consumption on a per-packet basis for a Lucent WaveLan 2.4 GHz DSSS IEEE 802.11 wireless network interface card for two ad hoc routing protocols, DSR and AODV. The study measured the energy cost incurred at nodes that are in receiving range but are not destination nodes. The results indicate that the number of packets has a greater impact on energy consumption than packet size and that the power consumption cost of idle mode is high. Routing in wired networks relies on shortest paths and smallest delay. In wireless networks, the metrics differ since power limitation is a problem in mobile ad hoc networks. In this case routing through the closest node could hasten the death of that node. Therefore, other measures should be taken to alleviate this problem.

Singh, *et al.* [43] define five metrics for studying the performance of power-aware routing for uni-cast traffic: *energy consumed per packet*, *time to network partition*, *maximum node cost*, *variance in power levels across nodes*, and *cost per packet*. They study the effects of these metrics on end-to-end delay. Their results show that by using power-aware metrics instead of a shortest-hop metric, no extra delay is incurred.

Routing in MANETs requires the knowledge of node locations and the links costs between these nodes. This may leads to higher communication overhead. Stojmenovic and Lin [46] propose a loop-free localized routing algorithm. In this localized cost and power-cost routing algorithm, additional nodes are placed between the source and destination to make the transmission power linear. Thus, transmission power is in terms of d instead of d^{α}, where d is the distance between source and destination nodes and α is the propagation constant, where $\alpha \geq 2$. In localized power routing, nodes make decisions based on location, determined with Global Positioning System (GPS) devices, and distance from source to destination. For broadcast traffic, where intermediate nodes are required to retransmit the packet, Singh, *et al.* [52] show that channel allotment to nodes is important for power-efficient broadcast protocols. They also suggest that it is beneficial to spend some energy to gather topology information to determine the most energy-efficient broadcast tree. In another paper, Singh and Raghavendra [52] present a broadcast tree approach to share the cost of routing among all nodes in the system. In this case, a cost is associated with each node based on how much power the node has consumed. Priority in routing is given to nodes that have consumed lower amounts of power and nodes that have more neighbors. The study assumes that all nodes have only broadcast traffic. Packets from the same source may traverse different trees as the network topology changes. Wieselthier, *et al.* [53], combine routing decisions with transmission power levels. They describe an algorithm for determining a source-initiated minimum-energy tree for broadcast or multicast session requests. Their results show that the exploitation of routing and transmission power decisions provides greater energy savings than algorithms that are developed for link-based, wired networks.

Feeney [51] compared the Dynamic Source Routing (DSR) protocol with the Ad Hoc on Demand Distance Vector (AODV) routing protocol in terms of their energy consumption. The study takes into account the cost of sending and receiving packets, routing overhead and dropped packets. The study indicates that there is considerable energy being wasted on flooding the network with data packets and MAC control packets. In addition, receiving and discarding packets consume a substantial amount of power. The study also indicates that the cost of source routing headers in DSR is not significant, but operating the radio in promiscuous mode for routing and caching of routes wastes energy. The study also indicates that the generation of broadcast traffic in AODV results in high energy consumption.

2.4.5 Techniques at the Transport Layer

Several studies have been conducted to look at energy minimization at the transport layer. While TCP works well in wired networks, using the same version of

TCP for wireless links can lead to inefficiencies in terms of performance and energy use. The characteristics of wireless links are inherently different than wired ones. Therefore, applying standard TCP to wireless links, without modification, may not provide good performance for wireless networks.

Several schemes have been proposed to reduce the effects of TCP retransmissions due to factors other than congestion [54], [16], [56]. These schemes have been classified by Jones, *et al.* [31] into three groups: split connection protocols, link-layer protocols, and end-to-end protocols. The studies of Bakre *et al.*[54] , Balakrishnan *et al.*[16] and Gitlin *et al.*[55], show that these schemes provide better performance than standard TCP due to their adaptability to the dynamic nature of wireless links. Tsaoussidis, *et al.* [56] studied the energy versus throughput performance tradeoffs for different TCP variations. Their findings indicate that balancing energy consumption and throughput can be accomplished through the error control mechanism. Kravets and Krishnan [57] have designed and implemented a protocol that selectively chooses short periods of time to suspend communication and shut down the transceiver. The algorithm handles the queuing and the management of packets during this period.

2.4.6 Techniques at the Middleware and Application Layers

In an energy efficient system design, it is crucial to have the operating system and the applications that run on top of the operating system support the underlying power management mechanisms. Recent operating systems have incorporated the

Advanced Configuration Power Interface (ACPI) standard that can power down devices that have not been used for a certain period of time or even shut down the entire system after a certain period of inactivity [58]. Integrating power efficient features specific to wireless networks will certainly help increase the life of the network.

Chapter 3. Background Knowledge

3.1 Multi-hop Wireless Ad Hoc Networks

The conventional wireless mobile communication is usually supported by a wired fixed infrastructure (e.g. Cellular Networks). The mobile devices use single-hop wireless radio communication to access a base station that connects it to the wired infrastructure. In contrast, multi-hop wireless ad hoc networks do not depend on any fixed infrastructure. Instead, they can be deployed in an ad hoc manner, even in environments where no fixed infrastructure is available.

A multi-hop wireless ad hoc network consists of a number of wireless nodes that are typically limited in resources such as bandwidth, computation power, memory, and battery. The total set of ad hoc wireless links among neighboring nodes form a multi-hop network topology. Since nodes may be on and out, come and go, the ad hoc network topology is dynamic in nature. There are mainly two types of multi-hop wireless ad hoc networks: *mobile ad hoc networks* and *wireless sensor networks*. While these two types of networks target different types of applications, they share many common characteristics and issues.

A mobile ad hoc network (MANET) is formed by set of wireless devices that are capable of moving around freely and cooperate in relaying packets on behalf of one another. It does not require any fixed infrastructure or centralized administration. Instead, it is completely self-organizing and self-healing. MANETs have many potential applications in a variety of fields, like military tactical communication, disaster rescue and recovery, and collaborative group meetings.

Since MANET has no fixed infrastructure such as base stations, each mobile node acts as an end-system as well as a router. Two mobile nodes within the transmission range of each other can communicate directly via the ad hoc wireless link. A multi-hop route is needed when the destination is beyond the coverage of the sender. Hence routing is a key component of MANET performance. A number of routing protocols have been proposed for MANETs during the recent years [59]. Most of these routing protocols can be classified into two categories: *proactive protocols* and *reactive (on-demand) protocols*. In proactive approaches, each node will maintain routing information to all possible destinations irrespective of its usage. In on-demand approaches, a node performs route discovery and maintenance only when needed. Due to the nodal mobility and fast changing topology, on demand protocols generally outperform purely proactive protocols.

A wireless sensor network is formed by a number of wireless sensor nodes that are normally capable of sensing some physical process and transmitting data via wireless radio. Sensor nodes may be stationary, or capable of moving around, or a combination of both. Wireless sensor network is just one special type of sensor networks.

This dissertation is focused on several important issues in QoS provisioning in multi-hop wireless ad hoc networks. Such as enhanced routing, energy awareness, and end-to-end delay assurance.

3.2 Network Layer Model

The OSI network layer model consists of seven layers, each providing some functionalities. All these layers can work together to fulfill the wireless network goal:

- ***Physical Layer:*** Ensures that each bit reaches the next node correctly (e.g. using error control codes). This constitutes the hardware used for communication.
- ***Data Link Layer:*** Takes care of the sequencing of packets, and deals with issues like channel sharing in shared access environments.
- ***Network Layer:*** Ensures the routing of packets and their arrival at destination.
- ***Transport Layer:*** Ensures that the packets reach the correct process on the remote host.
- ***Session/Presentation Layers:*** Provides segmentation and Reassembly, and the user interface functions.
- ***Application Layer:*** Offers users the network-services via the communication protocols.

3.3 Quality of Service (QoS) Metrics

QoS is usually defined as a set of service requirements that needs to be met by the network while transporting a packet stream from a source to its destination. The network is expected to guarantee a set of measurable specified service attributes to the user in terms of end-to-end delay statistics, bandwidth, probability of packet loss, delay variance (jitter), etc. Energy efficiency and service coverage are two other QoS attributes that are more specific to wireless ad hoc networks due to the limited battery capacity of mobile devices.

3.4 Issues and Difficulties

Mobile multi-hop wireless networks differ from traditional wired Internet infrastructures. The differences introduce unique issues and difficulties for supporting QoS in the MANET environment. These issues include features and consequences. Examples of features include unpredictable link properties, node mobility, and limited battery life, whereas hidden and exposed terminal problems, route maintenance, and security can be categorized as consequences. These issues are itemized as follows.

Unpredictable link properties: Wireless media is very unpredictable. Packet collision is intrinsic to wireless network. Signal propagation faces difficulties such as signal fading, interference, and multipath cancellation. All these properties make measures such as bandwidth and delay of a wireless link unpredictable.

Node mobility: Mobility of the nodes creates a dynamic network topology. Links will be dynamically formed when two nodes come into the transmission range of each other and are torn down when they move out of range.

Limited battery life: Function of mobile devices generally depends on finite battery sources. Resource allocation for QoS provisioning must consider residual battery power and rate of battery consumption corresponding to resource utilization. Thus, all the techniques for QoS provisioning should be power-aware and power-efficient.

Hidden and Exposed Terminal Problems: In a MAC layer with the traditional carrier sense multiple access (CSMA) protocol, multi-hop packet relaying introduces the "hidden terminal" and "exposed terminal" problems. The hidden terminal problem happens when signals of two nodes say, Node A and B, which are out of each other's transmission ranges collide at a common receiver say, Node C. With the same nodal configuration, an exposed terminal problem will result from a scenario where Node B attempts to transmit data (to someone other than A or C) while Node C is transmitting to Node A. In such a case, Node B is exposed to the transmission range of Node C and thus defers its transmission even though it would not interfere with the reception at Node A.

Route maintenance: The dynamic nature of the network topology and the changing behavior of the communication medium make the precise maintenance of network state information very difficult. Thus, the routing algorithms in MANETs have to operate with inherently imprecise information. Furthermore, in ad hoc networking environments, nodes can join or leave at any time. The established routing paths may be broken even during the process of data transfer. Thus, the need arises for maintenance and reconstruction of routing paths with minimal overhead and delay. QoS-aware routing would require reservation of resources at the routers (intermediate nodes). However, with the changes in topology the intermediate nodes also change, and new paths are created. Thus, reservation maintenance with updates in the routing path becomes cumbersome.

3.5 Real-time Traffic *vs* Non-real-time Traffic

Real-time traffic requires QoS due to some essential differences between the non-real-time data and real-time data [60].

For the transmission of non-real-time data (also commonly termed as *elastic data*), timing is not a critical issue. As a result, the non-real-time network could work well without guarantee of timely delivery of data. However, non-real-time traffic usually has high requirement for data integrity. Retransmissions are used if there are some lost packets. Example of the applications requiring non-real-time data transmissions are Telnet, FTP, E-mail and web browsing. For real-time transmission like telephone, video conference, streaming video and audio, the basic requirement is to transmit packets to the destination on time. People cannot tolerate large delay for example on the phone. As a result, some QoS mechanisms are badly needed to ensure the required quality of the connection.

3.6 QoS in Difference Layers

QoS mechanisms can be implemented at different layers of the 7-layer communication model.

QoS considered in physical layer means the quality in terms of transmission performance. For example, through proper control of transmission power control both the stations that are near the sender and those far away from the sender should be able to hear the signal clearly with dynamically changed levels of transmission power. Power control is used both to ensure the quality of reception and to optimise the capacity.

QoS implemented in MAC layer is also important. It could provide high probability of access with low delay when stations with higher priority traffic want to access the wireless medium. For example, this can be achieved in wireless LANs by setting a shorter back off time based on IEEE 802.11e, as described in [61].

On the other hand, the MAC layer needs to discriminate the different priority packets and schedule the packets delivery according to the priority levels. The service differentiation should be completed in the packet queue through queue management and in the MAC layer through a MAC discriminator and priority classifier.

- ***Queue Management:*** The aim of queue management is to schedule the different priority packets. Real-time data should have a higher priority to be sent to the channel compared with packets such as FTP and Email. Therefore, real-time data will be put in front of the non-real-time data in the packet queue. When the network is congested, the last packet in the packet queue will be dropped. Therefore, incorporating queue management will reduce the possibility that real-time packets are dropped in the packet queue when the network is congested. Thus, the delay of real-time application data packets can be reduced and the packet delivery ratio can be improved if appropriate queue management is implemented. Also, the packets whose delay has already exceeded the applications' requirement should be eliminated from the packet queue before transmission to save the battery power because transmission of these "out-off-date" packets will be useless to the receiver. If different flows go through the same host, it is easier to do the priority regulation in the packet queue than in the MAC layer.

- ***Priority Classifier and Packet Scheduler:*** To offer service differentiation in a distributed ad hoc network, real-time packets should be granted a higher priority to capture the channel. The priority classifier differentiates the different data packets that arrive from the packet queue and directs the packet scheduler to schedule the packet delivery based on the priority level of the current packet.

QoS implemented with the routing functions of the network layer aims to find a route which provides the required quality. The metrics which help choose the route are not only the number of needed hops along the route but also some other metrics like maximum delay and minimum data rate, as implemented in QAODV [62].

There are also other QoS frameworks, e.g. Stateless Wireless Ad Hoc Networks (SWAN) framework [63].

Chapter 4. The Analysis of Original RT-WMP Protocol

As mentioned in Section 3.2, the proposed scheme in our study is based on the idea of RT-WMP, which uses a priority based token-passing scheme. In this section, the original RT-WMP will be introduced first, followed by an analysis of its performance. A problem formulation will be given at the end of this section.

4.1 The Introduction of RT-WMP

4.1.1 RT-WMP Overview

RT-WMP protocol is a well known multi-hop transmission scheme proposed and implemented by Danilo Tardioli *et.al* [1] in 2007. It has been widely used in mobile robots control especially in robots visual signal transmission. There have been many studies based on the RT-WMP, which covered the areas of multi-cast communication [69], video transmission [70], and voice communication in underground environment [71].

4.1.2 Protocol Operation

The RT-WMP protocol works in three phases: *Priority Decision Phase (PDP)*, *Authorization Transmission Phase (ATP)*, and *Message Transmission Phase (MTP)*. The function of each phase is briefly described as follows:

- During the PDP, nodes reach a consensus over which of them holds the Most

Priority Message (MPM) among the network at that moment.

- In the ATP phase, an authorization to transmit is sent to the node which holds the highest priority message (MPM).
- Finally, in the MTP phase, the node which has the authorization to transmit will send the message to the destination node.

The protocol detail of PDP phase:

In order to find out and reach the consensus over which node holds the highest priority message, a token travels through all of the nodes in the network, in order to compare the message priority level of each node during the PDP phase. The node which initiates the PDP state that the highest priority message in its own queue is the MPM in the whole network and store this information in the token. Then it sends the token to another node, which checks the messages in its own queue. After the comparing, if the node fields that it holds a message with a higher priority level than the one carried by the token, it modifies the token data and continues the phase. The last node to receive the token, which knows which node in the network holds the MPM will close the PDP phase and initiates the ATP.

The protocol operation detail of ATP:

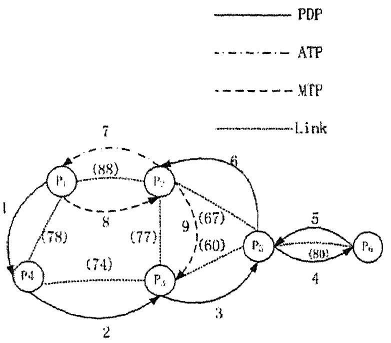
In the ATP phase, the node which initiates the PDP phase will calculate a path to the MPM holder using the topology information shared amongst the members of the network, and the routing algorithm is based on the Dijsktra's routing algorithm. The node which initiates the PDP will send an authorization message to the first node in the path, and the first node which selected by the routing algorithm will route this message to the second node in the path and so on, until the authorization reaches the MPM holder.

The protocol operation detail of MTP:

After the ATP procedure, the MPM holding node get the authorization message, and the MTP phase begins. MTP phase is quite similar to the proceeding one. The node that has received the authorization calculates the path to reach the destination, and sends the message to the first node of the path. The message follows the path and eventually reaches its destination. Phases repeat one after another. That is, when the MTP finishes, the node destination of the message initiates a new PDP and so on. When none of the nodes have a message to transmit, the authorization and message transmission phases are omitted, and the priority arbitration phase repeats continuously.

4.1.3 The Link Quality Matrix

In order to describe the topology of the network in PDP phase, the original RT-WMP defines an extension of the network connectivity graph (as defined in [10]) adding nonnegative values on the edges of the graph. These values are calculated as functions of the *radio signal* between pairs of nodes and are indicators of *link quality* between them. These values are represented in a matrix called the *Link Quality Matrix (LQM)*, which has widely been used in ad hoc routing scheme [11][12][13]. The elements of which describe the link quality between nodes (see Fig 4.1).



	P_1	P_2	P_3	P_4	P_5	P_6
P_1	-	88	0	79	0	0
P_2	88	-	77	0	67	0
P_3	0	77	-	74	60	0
P_4	79	0	74	-	0	0
P_4	0	67	60	0	-	0
P_4	0	0	0	0	80	-

Fig 4.1 The situation description by the network graph and the corresponding LQM [1]

Each column describes the links of a node with its neighbors. For example, from the LQM metrics, we know that the link quality value between Node P_1 and P_2 is 88. Nodes use this matrix to select which node to pass the token to and to take decisions on the best path to route a message from a source to a destination. All the nodes have a local copy of the LQM that is updated each time a frame is received. Besides, every node is responsible for updating its column of the LQM (both in the local copy and the shared copy) to inform the other nodes about local topology changes.

4.1.4 Error Handling in RT-WMP

RT-WMP has a set of error recovery mechanisms that can recover from errors such as transmission error and token duplication. The implicit acknowledge technique used, for example, dispenses with the necessity of monitor nodes to control the loss of the token. More details can be found in [1].

4.2 The Analysis of Original RT-WMP

From Section 4.1 we see that RT-WMP consists of two main procedures:

1) Most priority message selection by token passing scheme; and

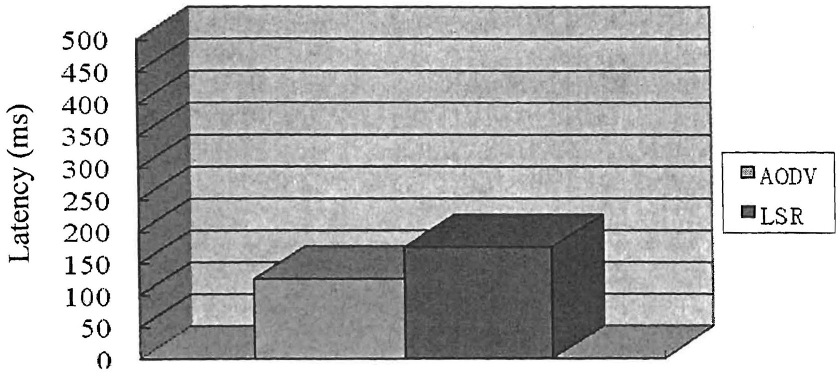
2) Routing procedure for important data (e.g, authorization messages or MPM messages);

In the data routing procedure, a shortest path routing scheme - Dijsktra's routing scheme is used in order to optimise the transmission delay aspect of QoS matrix. Dijsktra's routing scheme is a subset of the Link State Routing (LSR) protocol. In this protocol, the LQM matrix is held by each node and the token in order to help them to decide the most optimal routing path of data transmission. However, this routing method lacks of any energy saving mechanism, and thus restricts the application range in multi-hop networks (e.g, wireless sensor network). So what we do in this MSc research project is to develop a enhanced routing scheme in order to optimise the QoS performance, and on the other hand saving the energy by reducing power consumption in the data transmission procedure.

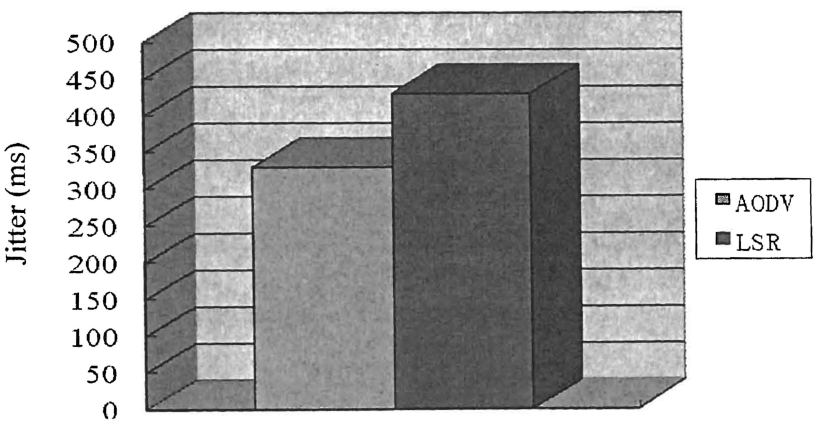
We put our focus on the AODV routing scheme which is a well known routing protocol widely used in ad hoc network area.

Karoly [64] has compared the QoS performance between Link State routing scheme and the well known AODV routing scheme.

The result has been illustrated in Fig 4.2. From this diagram, we learn that AODV shows a lower average latency of 125 ms. LSR protocol has much higher latency values. When comparing jitter, the reactive protocol AODV provide a lower delay jitter around 300 ms while the proactive protocol LSR suffers from higher jitter values of 400 ms, respectively.



(a)



(b)

Fig 4.2 Comparison of latency and jitter [64]

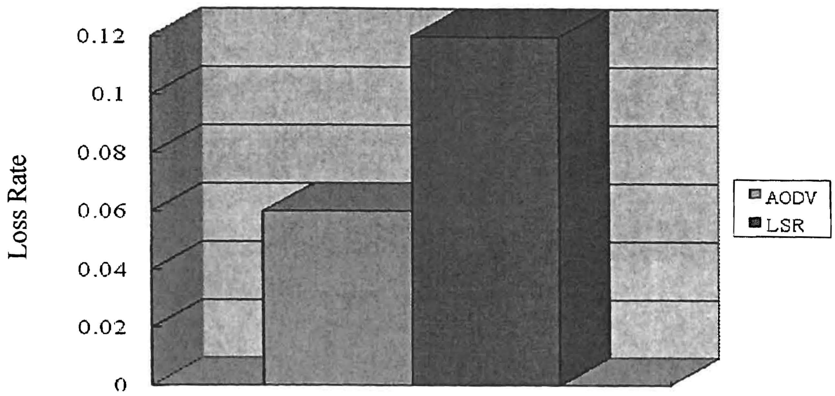


Fig 4.3 Comparison of Loss Rate [64]

Finally, the data loss rate about these protocols has been compared, as shown in Fig 4.3 The reactive protocol AODV shows a lower loss rate of 7 %, and the proactive protocol LSR has a loss rate of 13%, respectively, which is significantly higher than in case of the reactive protocol. The lower loss rate for the proactive protocol might be achieved by increasing the rate of periodic route advertisements to propagate link changes faster. Reactive protocols send more routing messages in case of broken links to discover a new route.

With regard to latency and jitter, AODV showed a better average performance while dijsktra's scheme produced much higher values in the range of some hundred milliseconds.

From above analysis, our research has been formulated as follows:

- Replacing the Dijsktra's algorithm by AODV scheme, and adding an energy aware mechanism in the routing procedure, in order to achieve a better QoS performance with more saving of energy.
- Implementing direct data transmission between the source node and the

destination node without a controller node, replacing the LQM matrix by a novel "routing path discover" method. In the original RT-WMP, the data transmission between the node which hold the MPM message and destination node is controlled by a third controller node which initiates the PDP phase.

Chapter 5. The Priority Based Wireless Multi-hop Scheme

5.1 Protocol Operations

In this section and the following chapter (Chapter 6), we will develop a modified priority based wireless multi-hop scheme based on original RT-WMP protocol. The main contributions of in this proposed scheme are listed below:

1) Replacing the three nodes interaction by direct transmission between two communication nodes. In the original RT-WMP protocol, there is an initiator to initiate the PDP procedure in order to find the MPM message and then control the follow-up transmission process from the MPM holder to the destination node. In our proposed scheme, a source node can directly collect the most priority message on demand from the other nodes in the network without the "controller", as shown in Fig 5.1

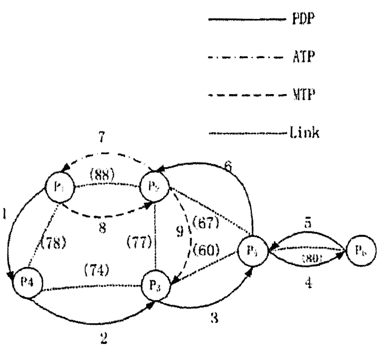
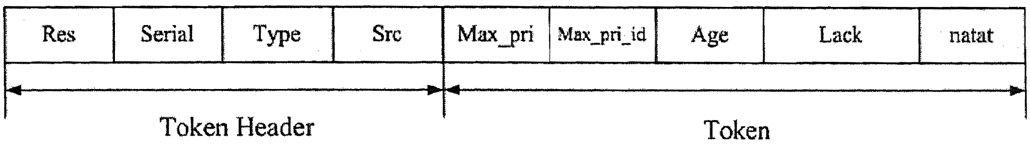


Fig 5.1 The network structure of proposed scheme [1]

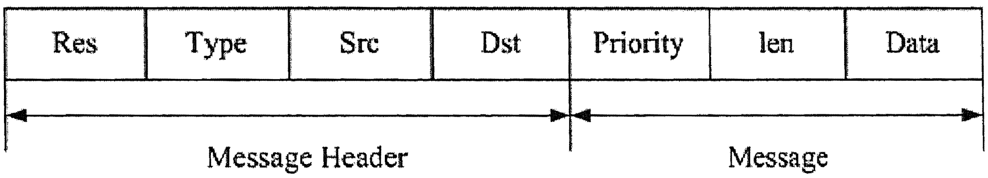
2) Proposing an AODV based energy saving routing scheme (as detailed in Chapter 6) which replaces the Dijsktra's routing scheme in order to make a preferring QoS guarantee.

5.1.1 Frame Definition

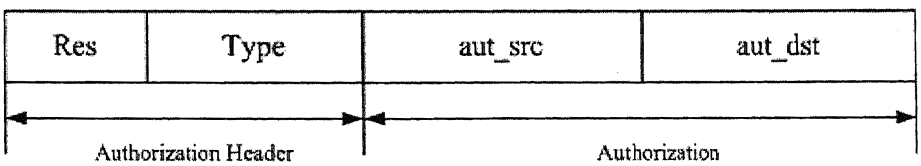
Before we introduce the details of various phases, we will first introduce 3 types of frames defined in the scheme: *token, message and authorization.*



(a) The token frame



(b) The message frame



(c) The authorization frame

Fig 5.2 Frames description of the protocol.

Fig 5.2 presents the frames which are exchanged amongst the nodes. The token frame (as shown in (a) of Fig 5.2) has a *Token Header* and a *Token format*. In the *Token Header* field, the first byte (*res*) is reserved for communication between the network interface card (NIC) driver and the protocol process. The *Serial* field contains the serial number of the frame, which is useful for the error recovery mechanism (The detail of the error recovery mechanism see the section 5.3). The *Type* field identifies the type of the frame (i.e., identifying the *token, authorization, message* and *drop*). The *Src* and *Dst* fields contain information about the source and the destination of the frame. In fact, in the proposed scheme, nodes are identified through a natural number between 0 and n−1 called IP address where n being the fixed number of the nodes in the network. When a node needs to send a frame (of any type), it fills the Src/aut_src (in a *token*, *message* or *authorization* frame) and Dst/aut_dst (in a message or authorization frame) fields of the frame with its IP address and the IP address of the destination node, and then broadcasts the frame. Since the radio channel is shared, all the neighbors of the sender hear the frame but only the destination processes it. The token frame adds the Max_pri and Max_pri_id fields that carry the MPM priority level and the MPM holder IP address. The *Age* field is used to find the oldest message amongst messages with the same priority level. The *Lack* field is used for belated acknowledgement of the sender (see Section 5.2). Finally, the *nstat* field is an array of n bytes. The value nstat[i] represents the status of the p_i node which can be either *unreached*, *reached*, *lost* or *searched*. The authorization frame adds the *aut_dst* and *aut_src* fields which carry the address as of the destination node and the source of the authorization to the common header. The message header holds the IP address of the source and of the messages destination. The *priority* and *len* fields hold the priority and the length of the data carried by the frame as well. The field *data* contains the payload of the frame, which can have a length between 0 and MTU bytes.

5.2 Phases of The Protocol

The discussion in this subsection is under the assumption that:

1) The network is fully connected.

2) In 5.2, we presuppose that the communication among the nodes is error free.

3) As the same to [1], the system architecture considered in this thesis consists of a set S of n mobile nodes $S = \{P_0 ....P_{n-1}\}$ which can communicate over a wireless link. All the nodes use a single shared radio channel to exchange messages. We call the subset of nodes that can hear the transmission of the neighbors of node P_i. Each node has two priority queues: one for transmission and the other for reception. Each message exchanged between nodes is identified by a priority level in the range of 0~127, where 127 is the highest priority value. Messages with the same priority are stored in FIFO order. When an application needs to transmit a message to another node, it puts the message into the transmission queue. The proposed scheme process takes the message from that queue and transmits it through the network to the destination node. The latter pushes the message into the reception queue and the destination application can finally pop the message from that queue.

5.2.1 Priority Decision Phase (PDP)

The first phase of the scheme is the priority decision phase. When there is a node initiates this phase, for example when the node P_k initiates the PDP phase, P_k will initiate a traffic between itself and the Most Priority Message (MPM) holder.

First of all, it will generate a token with a *nstat[i]* field in its frame. When the token was generated, it will sets the *nstat[i]* to *unreached.* For all *i,* under $\forall i < [0, n-1] : i \neq k$. The value *nstat[k]* will be set instead to *reached.* These mean that in the current PDP, none of the nodes have been reached by the token except the node P_k.

Secondly, the token will check the priority level of highest priority message in its transmission queue and sets the *Max_pri* and *Max_pri_id* fields with this highest priority message value and its ID address respectively. The *Age* field is filled with the value for the maximum amount of time this message can wait in the queue. This way, the P_k node is selected as the MPM holder. Then, it analysees the Received Signal Strength indicator (RSSI) which is provided by the 802.11 protocol (In order to obtain the RSSI, the physical sub-layer measures the energy observed at the antenna being used to receive the current frame. Normally, 802.11 device provides this value to the device driver) [60], in order to know which node P_{bl} shares the best link quality with the node P_k. (P_{bl} is the node which holds the best link quality with the P_k.) After the selection of the receiving node, the P_k node will send the token to it. When P_{bl} receives the token, it sets the *nstat[bl]* to *reached,* It subsequently increases the value of the age field of the token and compares it with the priority level of the highest priority message in its own queue. If it holds a higher priority message, it modifies the *Max_pri* and *Max_pri_id* fields. If it holds a message with the same priority, however, it checks the *Age* field of the token, and updates the token as well. Subsequently, it chooses the node with which it shares the best link quality amongst the set of nodes not yet reached, and sends the token to it. The process is repeated until all the nodes have been reached by the token (i.e. *nstat[i]=reached*). The last node to receive the token knows the MPM holder's identity (which is contained in the *Max_pri_id* field) and is responsible for sending it the authorization. The node ends the PDP and initiates the Authorization Transmission Phase (ATP).

5.2.2 Authorization Transmission Phase (ATP):

First of all, the node (which proposed destination node) that starts the ATP calculates a path to reach the destination node. To do this, it applies an energy efficient routing protocol (which will be introduced in Chapter 5) to return a path to the destination as a set of nodes denotes as $P = \{P_{p1}......P_{pm}\}$. Then the node creates an authorization, fills the *aut_dest* and *aut_src* fields with the MPM holder address and its own address respectively, and sends the authorization to the first node of the path. When P_{p1} receives the authorization, it looks at the *aut_dest* field. If this filed contains its address, it ends the ATP and initiates the Message Transmission Phase (MTP). Otherwise, it passes the authorization to the next node on the route path, which in our study is P_{p2}. The node repeats the process just explained, routing the message to the next member of the path, leaving the *aut_dest* field unchanged.

5.2.3 Message Transmission Phase (MTP):

When the MPM holder receives the authorization to transmit, it takes the highest priority message out from its transmission queue, creates a new *message* frame and places the data into the *message* field. It fills the *src* and *dest* fields with its address and with the destination address, and calculates the path to the destination, just like the procedure in the ATP. Then it fills the priority and *len* field with the message priority and data length, and sends it to the first node of the selected path. When the node in the routing path receives the message, it checks *msg_dest* field. If it contains its address (i.e. if it is the destination node) it stores the message into the reception queue, and starts a new PDP. Otherwise, it repeats the computation of the path and repeats the process just explained, routing the message to the next member of the path with the *msg_dest* field left unchanged. An explicit acknowledgement is not included because it would create too much overhead. However, if the message reaches the destination node, the destine node introduces its IP address in the *lack* field of the new token before initiating the new PDP. During this PDP, the token will reach the sender of the previous message, who can check if the message has been delivered or not by looking at the *Lack* field.

5.3 Error Handling Mechanism

When the token travels through the network, the error may occur because of the node failure, token loss and token duplication. In the following subsections, we will discuss these error situations and the error handling mechanisms.

5.3.1 Node Failures and Token Loss

While the token traveling between two nodes, the receiving node may be in a failure, in this case, the receiving node will fail to receive the token.

To handle this problem, CTS message is used to acknowledge the sender node. It is request for transmission RTS to transmit when the sender wishes to pass the token to the receiving node, it will send a RTS (Ready to Send) message to the receiving node. The receiving node will reply with a CTS (Clear to Send) message in order to acknowledge the sender after it received the RTS successfully. When the sender receives the CTS, it will send the token to the receiving node. On the other hand, if the sender did not hear the CTS message within certain time limit, specified by: *tim_lim,* it will re-transmit the RTS message, If at this time sender also did not hear the CTS within *tim_lim* either, the sender will give up to send the token to this proposed node.

5.3.2 Token Duplication

There also has a situation in which the receiving node received the token successful and sent an ACK message to the sender, but the sender did not hear the ACK within *tim_lim* (i.e. the ACK being lost on its way to the sender and receiving node), and the sender will re-transmit the token to the receiving node. On the other words, there will be two tokens in the network at that moment. In order to handle this problem we introduce the *serial* field in the token. Before each transmission of the token, the sender increments this value, save it locally, and then transmit the token.

However, when a node receives a token with its serial number no larger than the highest serial that has been transmitted, it discards the token and informs the sender by sending a *drop* frame to it.

Chapter 6. An Energy Efficient Routing Scheme

In order to route the authorization and high priority messages in the ATP and MTP phases, a shortest path routing scheme is needed in the proposed protocol. As we have mentioned above, minimizing the energy consumption is a key research topic in the area of ad-hoc networking because of the limitation of battery supply in mobile devices. In the original RT-WMP protocol, the data routing in the ATP and MTP phases is based on the Dijsktra's routing scheme. However, this scheme has not get any energy-saving mechanism, and this shortcoming limits its application in wireless networks especially in mobile ad-hoc networks. This project aims to find a proper method to route the data from source node to destination in an energy efficient manner.

In this chapter, we propose an energy efficient algorithm which is implementable under current well-known routing protocol AODV [12]. This energy efficient extension is a metric based algorithm, which, introduced in Chapter 2 and inspirited from the work of [43][66], integrates the runtime battery capacity and the estimated real propagation power loss, obtained from the sensing the received signal power. So it independent of location information and terrain-based, permitting power loss by terrain profiles such as large building blocks. Optimised cost functions are derived to combine the available information into one routing metric, which is optimised into two ways: Local optimization among neighbors and global optimization between end-to-end nodes.

6.1 Energy Consumption Model for Routing Algorithm

Routing path selection based on the shortest path is usually not energy efficiency concerned. (i.e. Dijsktra's routing scheme which is used in RT-WMP.) When we add an energy saving mechanism in the original RT-WMP's routing scheme, there has different metrics are considered and an appropriate weight is assigned to each link. Between two end to end nodes, there usually exists more than one route can be selected. For a given set of potential relay nodes, there will be relatively energy-optimal routes that can achieve the least cost based on the nodes' battery capacity and propagation loss of links. Fig 6.1 shows a simple multi-hop network, with the relay nodes set K between the source and destination nodes. We can find an energy efficient route $A \rightarrow B \rightarrow C$.

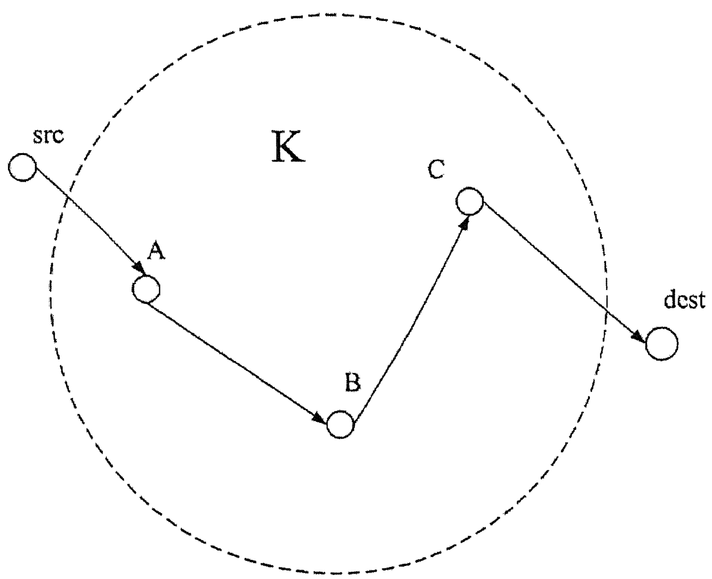


Fig 6.1 A multi-hop ad hoc

In the routing path selection, links with less propagation power loss and nodes with higher residual battery capacity are preferred. Thus the problem is simplified to minimize the power consumed during transmission and maximize the battery capacity of the next node to be used. The solution from [67] is to minimizes:

$$\frac{p(i)}{g(i)} \quad i \in K \tag{1}$$

for the local (immediate next hop) optimization.

$$\text{and} \qquad \sum_{i \in K} \frac{p(i)}{g(i)} \quad i \in R \tag{2}$$

for the global (all end-to-end hops) optimization.

We define the *g(i)* the residual battery capacity of the i^{th} node, and *p(i)* as the power cost per packet from node *i*-1 to node *i* (Joules per second per packet). Thus selecting the optimal routing path implies the selection of the link which has the minimum $\frac{p(i)}{g(i)}$ or $\sum_{i \in K} \frac{p(i)}{g(i)}$.

The residual battery capacity is the amount of remaining energy in the battery while the transmitter is consuming the power. It is assumed that each node can read its own residual battery capacity. The immediate next hop optimization can also be expressed as [67]:

$$\frac{p(i)}{g(i)} = [p_{loss}(i-1,i) + p_{rx}(i) + p_c(i)] \cdot f(i) \tag{3}$$

Where we define $f(i) = \frac{1}{g(i)}$, and $P_{loss}(i-1,i)$ represents the sum of the power loss of the link between node *i*-1 and *i* ; the $p_{rx}(i)$ represents the power cost to receive the packet at the *i*th node; and $p_c(i)$ represents the power cost for routing message to maintain this connection.

Because the minimum threshold of receiving power of the receiver is constant for all receivers, the $p_{rx}(i)$ can be express as a constant number demoted as p_{rx}. Besides that, since the routing message for route discovery and maintenance is the same for all nodes for on demand routing protocols, we can also consider $p_c(i)$ as a constant number p_c. Hence, both control and data packets are considered to consume energy according to their packets size. So the above (3) can be re-writen as:

$$\frac{p(i)}{g(i)} = f(i)\Box p_{loss}(i-1,i) + (p_{rx} + p_c)\Box f(i) \tag{4}$$

This algorithm is independent of location information. The value of propagation loss is obtained by calculating the difference between transmitting power and receiving power, which is determined by exchanging local routing control message, such as HELLO message in AODV.

From the above introduction, we see that in order to get a minimum value of $\frac{p(i)}{g(i)}$, we only need to know the values of $P_{loss}(i-1,i)$ and $f(i)$. With these two values, we can calculate the value of $\frac{p(i)}{g(i)}$ using the expression (4).

This algorithm can optimise either locally for each hop or globally for end-to-end route between a source-destination pair. Similarly, for global optimization, summing function (4) along multi-hop routes can be expressed as:

$$\sum_{i\in K}\frac{p(i)}{g(i)} = \sum_{i\in K} p_{loss}(i-1,i)\Box f(i) + (p_{rx} + p_c)\Box f(i) \tag{5}$$

For the global optimization, the data source will know through the global cost function (5) the summation of the costs for all possible routes and can then decide which route to choose. While for local optimization, each intermediate node will choose locally a different next hop to forward data for energy efficiency from the local cost function (4). The goal of global optimization is to achieve less transmission delay by routing data with fewer hops. Thus, a preferred routing path can be selected from local optimization result and global optimization result. The local optimization procedure is to determine which path is more energy efficient; and the global optimization procedure is to determine which path offers better timely delivery.

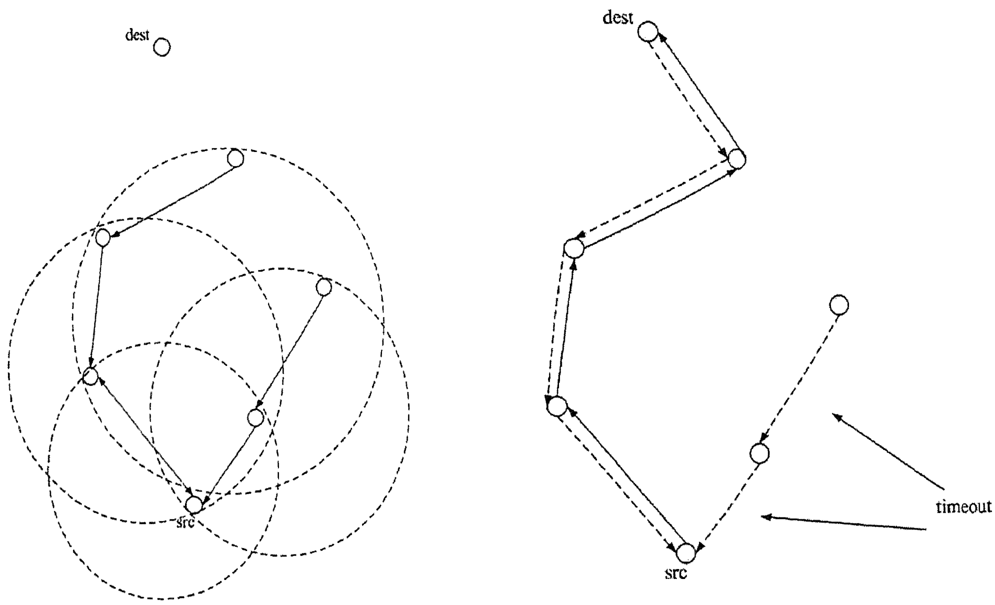
6.2 AODV Routing Protocol

6.2.1 Protocol Overview

Ad hoc On Demand Distance Vector (AODV) [12] is a source initiated, reactive protocol. It discovers and maintains routes only if and when necessary. Route discovery works as follows:

When the source requires a path to a particular destination, it broadcasts a route request (RREQ) packet in the ad hoc network. Nodes receiving RREQ record a *reverse* route back towards the source, using the node from which the RREQ was received as the next-hop, and then re-broadcasts the RREQ. If the same RREQ is received more than once (via different routes), it is ignored. This way the RREQ packets are flooded to every node in the connected part of the network.

When the RREQ packet reaches the destination, it sends a route reply (RREP) packet back to the source, using the reverse route. If an intermediate node has an up-to-date route to the destination, a special message called gratuitous route reply (G-RREP) is uni-cast to the destination, notifying it that the source has route request and then a bi-direction route is formed. By then, both the data source and destination have routes to each other, and all the intermediate nodes have routes to the source and destination. As the RREP packet follows the path back to the source, the corresponding *forward* route is created at each intermediate node towards the destination [see Figure 6.2 (a) & (b)]. Once the RREP packet reaches the source, data traffic can now flow along this forward route. In the AODV, source node will choose the shortest path if there are multi-routes discovered (with several routes replies).



(a) Reverse Path Formation (b) Forward Path Formation

Fig 6.2 Reverse and forward route formation in AODV

To prevent routing loops, AODV maintains a sequence number on each node. Any routing information transmitted on routing packets or maintained on a node is tagged with the last known sequence number for the destination of the route. AODV protocol guarantees the invariant that the destination sequence numbers in the routing table entries on the nodes along a valid route are always monotonically increasing. Other than preventing loops, sequence numbers also ensure freshness of routes. Given a choice of multiple routes, the one with a newer sequence number is always chosen.

An important feature of AODV is maintenance of timer based states in each node, regarding utilization of individual routes. A route is "expired" if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating a set of neighboring nodes that use that entry to route data packets. These nodes are notified with route error (RERR) packets when the next hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. This RERR is thus propagated to each source routing traffic through the failed link, causing the route discovery process to be reinitiated if routes are still needed.

6.2.2 Message Format of AODV

In this sub-section, we will introduce the "HELLO" message format of AODV (RREQ and RREP) as used in this study. Other message formats can be found in [12].

Route Request (RREQ) Message Format

As shown in Figure 6.3, in this format, a 32-bit value is separated into three parts, and every part has 10-bits:

J: Join flag; reserved for multicast.

R: Repair flag; reserved for multicast.

G: Gratuitous RREP flag; indicates whether a gratuitous RREP should be uni-cast to the node specified in the Destination IP Address field.

D: Destination only flag; indicates only the destination may respond to this RREQ.

U: Unknown sequence number; indicates the destination.

Reserved: Sent as 0; ignored on reception.

Hop Count: The number of hops from the Originator IP Address to the node handling the request.

RREQ ID: A sequence number uniquely identifying the particular RREQ when taken in conjunction with the source node's IP address.

Destination IP Address: The IP address of the destination for which a route is desired.

Destination Sequence Number: The latest sequence number received in the past by the originator for any route towards the destination.

Source node IP Address: The IP address of the node which originated the Route Request.

Originator Sequence Number: The current sequence number to be used in the route entry pointing towards the originator of the route request.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |J|R|G|D|U|   Reserved          |   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            RREQ ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Source node IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Source node Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig 6.3 HELLO RREQ message format

Route Reply (RREP) Message Format:

As shown in Figure 6.4, in this format, a 32-bit value is separated into three parts. The main functional fields are defined as follows:

R: Repair flag; used for multicast.

A: Acknowledgment required.

Reserved: Sent as 0; ignored on reception.

Prefix Size: If nonzero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination.

Lifetime: The time in milliseconds for which nodes receiving the RREP consider the route to be valid.

Other parts of the message header format are the same as RREQ.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |R|A|   Reserved      |Prefix Sz|   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination IP address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Source node IP address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Lifetime                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig 6.4 HELLO RREP message format

We have discussed the AODV routing protocol and its HELLO message format definition on above, and we will introduce an energy efficient routing scheme which based on the AODV routing protocol.

6.3 Energy-Aware Routing Scheme Based on AODV

In order to find an energy efficient routing path from the source node to the destination node, an "energy recording" field is added in RREQ message and "an energy losing" field is adding in RREP message. We also assume that each mobile device has the capability of reading the energy related fields. From these information, we can calculate the energy loss through the message broadcasting between two nodes.

1) Modified HELLO Message:

HELLO message is broadcast only to neighbors one hop to maintain updated local connections. Energy information is embedded in it so that neighbor nodes can have updated knowledge of the energy conditions of each other. To guarantee bi-directional links, the RREQ message is used as the HELLO message, and neighbor nodes receiving it will reply with a RREP to acknowledge this link.

The following slight modifications to the AODV specification [12] are made in this study:

*a) **HELLO RREQ format:***

A *"Source Battery Function Value f(s)"* was added in the HELLO RREQ header format. As shown in Fig 6.5, this value is a 32-bit long value, and is calculated from the current residual battery capacity. The message length and all other fields are kept unchanged.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |J|R|G|D|U|   Reserved          |   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            RREQ ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Source node IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Source node Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                Source Battery Function Value f(s)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig 6.5 Enhanced HELLO message format

b) HELLO RREP format:

A "Power Loss Level" was added in the HELLO RREP format. As shown in Fig. 6.6, this 32-bit long field is used to show the power lost for a specific link. The node that receives HELLO RREQ obtains the source battery function value *f(s)* and can also obtain the received signal power from the radio receiver. The power loss can be calculated by subtracting the received signal power from the transmission power as follows:

$$p_{loss}(i-1,i) = p_{tx}(i-1) - p_{rsp}(i) \; p_{loss}(i-1,i) = p_{tx}(i-1) - p_{rsp}(i);$$

Where the value $p_{tx}(i-1)$ is the transmission power of node *i-1* and value $p_{rsp}(i)$ is the receiving RREQ signal power in node *i*.

The local optimization value will be calculated from the cost function based on the information of $p_{loss}(i-1,i)$ and *f(s)*, and calculate the value:

$$\text{Cost } (i\text{-}1 \rightarrow i) = \frac{p(i)}{g(i)}$$

Which from the function (4), and added the result value to the local cost table. Then a RREP with energy information is uni-cast to the HELLO source which can then calculate the power loss and construct a new entry in its local cost table (as shown in Table 1). This way, each node will have a local cost table with the cost to its neighbors.

Table 1 Local Cost tables constructed by HELLO message

Node	A	B	C	D
Local cost table	Cost(A→B)	Cost(B→A) Cost(B→C)	Cost(C→B) Cost(C→D)	Cost(D→C)

From Table 1 we can see that each node holds two local cost values (except the source node A and destination node D). For example, Node B holds the local cost value for transmission of the RREQ message from node A to node B [Cost (B→A)] and the local cost value for transmission of the RREP message from node C to node B [Cost (B→C)].

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |R|A|    Reserved     |Prefix Sz|   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination IP address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Source node IP address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Lifetime                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                        Power Loss Level
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig 6.6 Enhanced RREP message format

2) Modification of RREQ/RREP for Global (end-to-end) Optimization:

Global cost information travels along the full path when a route is being setup, and the end-to-end cost can be calculated and updated hop-by-hop from the global cost function (5), carried by a new 32-bit cost field in RREQ/RREP message. The backward global cost table is constructed during the route request, while the forward global cost table is formed during the route reply. Table 2 shows this process with an example discussed below.

As shown in Fig 6.3, we assume that there is a routing request from the node A to node D. Node A will initiates a RREQ message and broadcast it to the neighbor nodes. The neighbor nodes of node A will calculate an optimal routing path from node A to D.

The source initializes a RREQ with the global cost zero, and the nodes receiving it will find in their local cost table, the local cost from themselves to the RREQ forwarder (indexed by IP address), and add this cost to the global cost in this RREQ. Then every time the RREQ is broadcast, each receiver will add the cost from itself to the previous forwarder to the global cost, called backward global cost formation (from relay nodes to the source).

For example, as shown in Fig 6.3, a RREQ is traveled from node A to node D. Node A initiates the RREQ and it does not have any RREQ & G-RREP message to receive, so its global cost is 0. Node B receives the RREQ from A and it calculates the local cost value of A to B: Cost(B→A). Its forwarder is just Node A, so there is just one value Cost(B→A) in the global table of node B. Node B also adds this value to the RREQ message as its global cost value. The RREQ message travels on to the node C. When the C receives the RREQ, it will calculate the local cost value of B to C as well. Because Node B is the forwarder for Node C, and Node A is also a forwarder for Node B, the global cost value of node C and be calculated as:

$$\mathrm{Cost}(C \rightarrow A) = \mathrm{Cost}(C \rightarrow B) + \mathrm{Cost}(B \rightarrow A);$$

On completion of the calculation, Node C will add this value on its global cost table and will also update the global cost value field in the RREQ message.

Similarly, the global cost value of Node D from Node A can be calculated by adding the local cost value of C to D onto the global cost value of node C, as follows:

$$\text{Cost}(D \rightarrow A) = \text{Cost}(D \rightarrow C) + \text{Cost}(C \rightarrow A);$$

When a RREP is generated by an intermediate node for this route discovery, the global cost is initialized to the cost from this node to the destination. Each node that receives this RREP will update the global cost field in the message by summing the value in this RREP with the local cost value from itself to the previous RREP forwarder. Then along the way the RREP is forwarded back to the source, all the relay nodes will update the global cost entry pointing to the destination in their global cost table, called forward global cost formation.

If a G-RREP is uni-cast to the destination, the global cost field is initialized with the value in the RREQ (the cost of this node to the source). When G-RREP is relayed to the destination, each relay node will also update its global cost field by summing the value in this G-RREP with the local cost from this node to the G-RREP forwarder. So the relay node will have the global cost to the source. This is still part of the backward global cost formation. After the whole process, the source knows the cost to the destination and vice versa, and all the intermediate nodes know the cost to both the source and destination. Global cost is kept valid until the route is outdated. For the simple scenario of Fig 6.7, the local and the global optimization algorithms are described in table 1 and table 2 respectively.

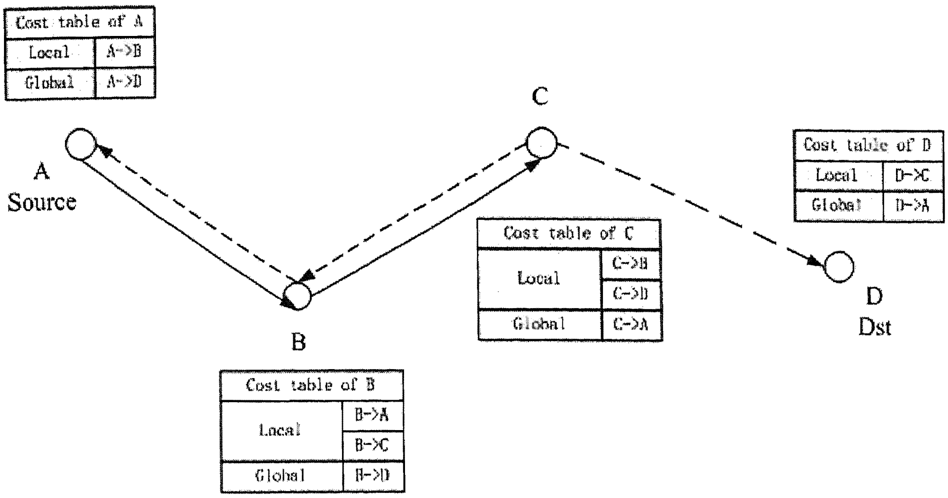


Fig 6.7 Route discovery mechanism in a four nodes system

Table 2 Global cost table updated during route discovery

	Node	Action	RREQ&G-RREP Cost Table	Global Cost Table
Backward	A	A-B broadcast RREQ	0	0
Global cost	B	B-C broadcast RREQ	Cost (B→A)	0
(D->A)	C	C-D Uni-cast G-RREP	Cost(B→A)+Cost(C→B) =Cost(C→A)	Cost(C→A)
Table	D	Receiver G-RREP, update global cost table (D->A)	Cost(C→A)+Cost(D→C) =Cost(D→A)	Cost(D→A)
Forward	C	C-B Uni-cast RREP	Cost(C→D)	Cost(C→A)
Global cost	B	B-A Forward RREP	Cost(C→D)+Cost(B→C) =Cost(B→D)	Cost(B→D)
(A->D) Table	A	Receiver RREP, update global cost table (A->D)	Cost(B→D)+Cost(A→B) =Cost(A→D)	Cost(A→D)

Chapter 7. Simulation and Analysis

In this section, a simulation of an enhanced scheme proposed in this study will be discussed. OpNet Modeler has been used as the simulator in our study. The parameters which we simulated in this study are *end to end delay* and *the dead time of nodes* under our proposed scheme. The whole simulation will be held under the static nodes environment. That is, the mobility of the nodes will not be discussed in our study.

The network architecture is modeled by the OpNet Modeler using the layering and modeling function. Each layer decomposes the complex system into three main sub-layer systems, and every sub-layer system carries out several mission functions. Each sub-layer system contains several models, and each model will do the smaller missions which contained in the mission of the network architecture.

Network Model Layer: Node Model Layer and the Processing Model Layer are the three main layers of OpNet Modeler modeling.

The rest of this Chapter is organized as follows: In 7.1 we will introduce the Adaptive Low-battery Alert Mechanism. In 7.2 we will introduce the simulation environment modeling which contains the Network Model and Node model. In 7.3, the static network simulation which focuses on the nodes dead lifetime will be introduced. Finally, the end-to-end delay performance will be simulated.

7.1 Adaptive Low-battery Alert Mechanism

The existing on-demand routing protocols including AODV have a problem of overusing existing routes. Once a valid route is setup, before it becomes outdated, the source will not bother to discover newer and more efficient routes although there may be better route available. The worst case is that under heavy load, if the network topology is not changing fast, the route discovered first will be overused and the nodes along this route will be drained out of energy rather quickly. To overcome this problem, we propose an adaptive low-battery alert mechanism has been used to enforce new route update when relay nodes are drained below certain low-battery alert level, for example, 50% or 40% of the new battery capacity. To avoid excessive link breakage, this low battery alert level is adjusted dynamically at an appropriate low level. The first node that reaches its alert level will initialize a special route error (RERR) message for route update. Every time the alert level is reached, this alert level will be decreased by a small amount, called alert adjustment step, which reflects the willingness of a node to relay a data packet. The alert level is decreased uniformly, for example, 1% or 5% of the new battery capacity (actually, only crude measures of residual battery are practical). If a new efficient route is discovered, the routing protocol will use the new route, else the old route is used until a newly adjusted alert level is reached.

In the implementation with AODV, a special route error (RERR) message with local route repair function is generated when the alert level is reached, signaling that there are recoverable errors in the route. In AODV RERR message, when the 'N' bit is set to '1', whoever receives this RERR will not delete the current route entry, and just disable it to wait for the repairing of this route. The source will try to find a newer route if this RERR is received. Due to the new route update, there may be delay or even loss of data packets, and therefore a little decrease of the network throughput may happen.

7.2 Simulation Environment Configurations

In order to compare the simulation result of the proposed scheme with those of the original RT-WMP protocol, we use the same set of simulation parameters configured for simulation of RT-WMP as [1]. That is, we will simulate our proposed scheme under the same simulation environment as RT-WMP.

A. Network model

All the simulations are based on 5 fixed nodes being placed into a network of $1200 \times 500m^2$ as shown in Fig 7.1 . In this network architecture, there contains a source node which needs to receive the priority packets from destination node, and node 1~node 3 are all the relay nodes in this network.

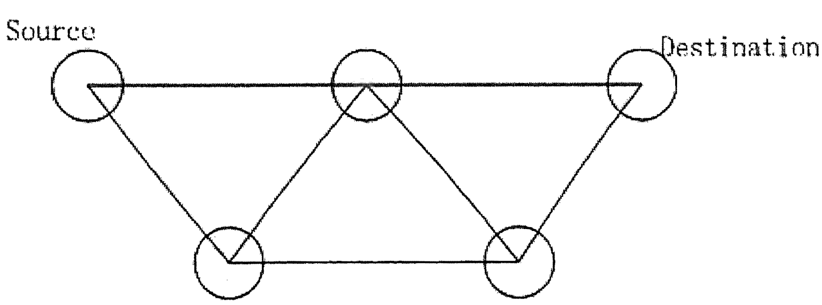


Fig 7.1 The network architecture of simulation

B. Node model

Each of the 5 nodes is uniquely identified by its user ID. In order to compare the lifetime of the proposed routing scheme with Dijsktra's scheme, the source model generates packets according to an inter-arrival exponential distribution. This inter-arrival time can be chosen as a Constant bit rate (CBR), in our study, this value we chosen as 4K bits per 0.25-0.1 seconds. The low-battery adjusting step is set at 1% of total power.

The IEEE802.11 peer-to-peer (ad-hoc) mode at 1Mbps data rate is chosen for the MAC model, and the free space propagation model is used for the channel model.

We use the same energy consumption model for the wireless interface as that adopted in [65]. In particular, we use the following typical values from the specification of the 2.4GHz DSSS Lucent IEEE 802.11 WaveLAN PC card [65].

Table 3 Energy related parameters of Lucent IEEE 802.11 WaveLAN PC card

Voltage supply	5 Volt
Transmitting	300mA
Receiving	250mA

From these values, given a packet length in bits, power consumption can be calculated. For instant, to transmit a packet of 4K bits including AODV header plus 224-bits IEEE 802.11 MAC header [65], from these values the energy consumption can be calculated as:

Energy Consumption = $5V \times 300mA \times (4 \times 1024+224)bits \div 10^6 bps=6.48 \times 10^{-3}J$.

When the Dijsktra's scheme is simulated, the energy consumption model for 802.11 b [65] can be adopted. The total battery capacity is assumed as 1mA • Hr.

7.3 Simulation results and analysis

The first dead lifetime has been used as a metric for performance evaluate: *First dead lifetime* is defined as the time when the first node on the route to destination dies (drained out of battery). Since there is no network topology change, the transmission route will fail when there is a node on this route reaches its dead life time.

We have simulated our proposed scheme and Dijsktra based routing scheme respectively using OpNet, and obtained the relationship between first dead lifetime improvement percentage value and Low-battery Alert Level value as shown in Fig 7.2.

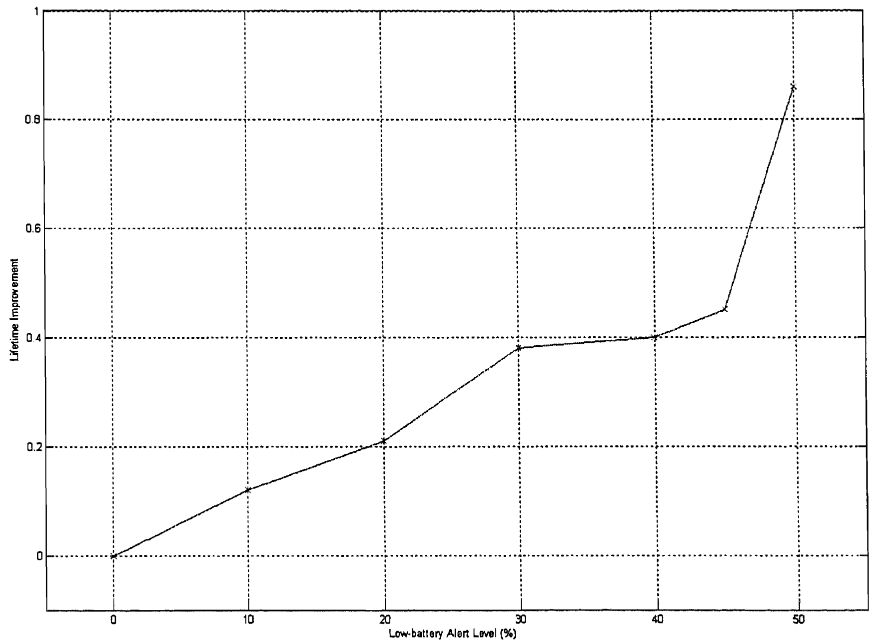


Fig 7.2 The lifetime improvement (Under packet generation interval 0.25 seconds).

Fig 7.2 shows the improvement of first-dead lifetime using our proposed scheme when compared with the Dijsktra's scheme, with different low battery alert levels, from 0% to 50%. From this figure we can see that when the low-battery alert mechanism is disabled (with its level set to 0%), our scheme show the same performance as the dijsktra's scheme, and as the Low-battery Alert Level value grows, the improvement percentage for the first-dead lifetime improvement keeps increased steadily (and sharply from 45% to 50%), this results shows that the low-battery alert mechanism may affect heavily in energy consumption of routing scheme. When the Low-battery alert value is set to 0%, there is no difference between our energy efficient AODV routing scheme and Dijsktra's routing scheme, because when the battery is exhausted in a routing path, there is no use to select the other one. When the Low-battery alert value is set to 50%, the increment between the energy efficient AODV routing scheme and Dijsktra's routing scheme reaches its maximum value.

The second experiment we have done is to measure the delay suffered by messages according to their priorities when the data message are transmitted under the RT-WMP protocol and energy efficient RT-WMP scheme which we have proposed in Chapter 6. To do this, we performed the same experiment as the RT-WMP in [1], which is in a five node network (as the same in Fig 7.1), Saturated traffic was generated in all of the nodes. Each node had a transmission priority queue for 20 messages and the messages generated had a random priority in a range between 0 and 31.

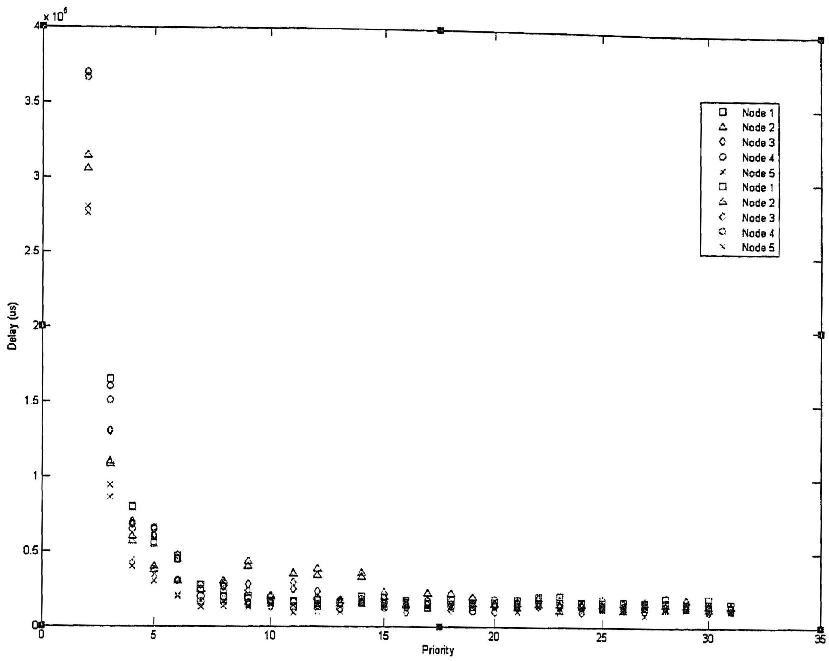


Fig 7.3 The relationship between the message priority and transmission delay

As shown in Fig 7.3, the blue points represent the delay suffered under original RT-WMP protocol and the red points represent the delay suffered under the energy efficient RT-WMP protocol. From this figure we can see that under these two protocols the lower priority messages may suffer longer delay. The most important is the energy saving mechanism did not show a significant impact on the real-time transmission a lot. It is mainly due to the facts that the Dijsktra's routing scheme is based on the idea of selecting a shortest transmission path and that the energy efficient RT-WMP is based on the minimum energy consumption path. However, a path with the minimum number of hops is selected as the minimum energy consumption path. So it is easy to understand why the proposed scheme did not affect the transmission delay a lot.

Chapter 8. Conclusions and Future Work

8.1 Conclusions

The aim of this research is to develop an AODV-based energy efficient routing scheme in order to improve RT-WMP by overcoming the protocol's energy costing problem. The original RT-WMP protocol is widely used in ad hoc real-time traffic area. However, it dose not have any energy saving mechanism to improve the network's lifetime. AODV is a well known routing protocol, and it has a better QoS performance than Dijsktra's routing scheme which was used in RT-WMP, but again this protocol dose not have any integrated energy-aware transmission mechanism.

An enhanced AODV scheme is proposed in this study in order to transmit the data in an energy efficient way. The following contributions have been made in the proposed MSc research:

- An energy efficient routing scheme has been proposed, based on our evaluation and performance analysis of the original RT-WMP protocol.
- A error handling mechanism has been proposed in this study in order to handle the problem of token loss and data frame loss.
- A simulation aided evaluation of our proposed energy efficient RT-WMP protocol in comparison with the original RT-WMP protocol.

8.2 Further work

Although the proposed energy efficient RT-WMP has shown some better performance than original RT-WMP, several extensions can be made for further improvement of the proposed solution. For example:

- Our proposed scheme is based on the static model. That is, we have not considered the mobility issue. Nowadays, mobile ad-hoc network has become a hot-spot research topic in wireless network area. Thus how to add a mobility model is part of our future work.
- In our study, we have only considered how to optimise energy consumption through appropriate routing the network layer. However, the MAC layer is also a critical layer which affects the energy consumption. Thus, how to develop an efficient, a cross layer method to optimise the energy consumption becomes another important topic area of our future studies.

References

[1] D. Tardioli and J. L. Villarroel, "Real time communications over 802.11: RT-WMP," in Mobile Ad-Hoc and Sensor Systems, 2007.

[2] C.Siva Ram Nurthy and B.S. Manoj. "Ad hoc wireless networks Architectures and Protocols", Prentice Hall, 2004.

[3] Andrew. Muir and J.J. Garcia-Luna-Aceves. "An Efficient Packet Sensing MAC Protocol for Wireless Networks". ACM Journal on Mobile Networks and Applications, 3(2):221–234, August 1998.

[4] Chunhung Richard Lin and Mario Gerla. "Real-time support in multi-hop wireless networks". Wireless Networks, 5:125–135, 1999.

[5] J.L.Sobrinho and A.S.Krishnakumar. "Real-time traffic over the IEEE 802.11 medium access control layer". Bell Labs Technical Journal, pages 172–187, Autumn 1996.

[6] J.L.Sobrinho and A.S.Krishnakumar. "Quality-of-Service in Ad Hoc Carrier Sense Multiple Access Wireless Networks". IEEE Journal on Selected Areas in Communications, 17(8), August 1999.

[7] Dr-Jiunn Deng and Ruay-Shiung Chang. "A Priority Scheme for IEEE 802.11 DCF Access Method". IEICE Trans. Commun, E82-B(1), January 1999.

[8] Imad Aad and Claude Castelluccia. "Differentiation mechanisms for IEEE 802.11". IEEE INFOCOM, April 2001.

[9] Michael Barry and Andrew T. Campbell and Andras Veres. "Distributed Control Algorithms for Service Differentiation in Wireless Packet Networks". IEEE INFOCOM, April 2001.

[10] V.Kanodia and C.Li and A.Sabharwal and B.Sadeghi and E.Knightly. "Distributed Multi-Hop Scheduling and Medium Access with Delay and Throughput Constraints". MOBICOM, August 2001.

[11] D. A. M. D. B. Johnson and Y.-C. Hu. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)". draft-ietf-manet-09.txt, 2003.

[12] E. M. B.-R. C. E. Perkins and S. R. Das. "Ad Hoc On-demand Distance Vector (AODV) Routing". Internet draft, draft-ietf-manet-aodv-12.txt, RFC3561 (Mobile Ad Hoc Networking Group), Nov., 2002.

[13] P. C. P. Sholander, A. Yankopolus and S. S. Tabrizi. "Experimental Comparison Of Hybrid and Proactive MANET Routing Protocols". MILCOM, 2002.

[14] P. M. P. Jacquet and A. Qayyam. "Optimised Link State Routing Protocol, draft-ietf-manetolsr-06.txt". IETF MANET Internet draft, RFC3626, 2002.

[15] C. Perkins. "Ad hoc Networking". Addison-Wesley, 2001.

[16] K. Ross and J. Kurose. "Computer Networking". Addison Wesley Longman Inc, 2001.

[17] B. H. A. Nasipuri, R. Burleson and J. Roberts. "Performance of Hybrid Routing Protocols for Mobile Ad Hoc Networks". Proceedings of the IEEE International Conference on Computer Communication and Networks (ICCCN2001), pages 296–302, 2001.

[18] M. Abolhasan and T. Wysocki. "Displacement-based Route Strategies for Proactive Routing Protocols in Mobile Ad Hoc Networks". Workshop on the Internet, Telecommunications and Signal Processing(WITSP03), 2003.

[19] R. Pearlman and Z. J. Hass. "Zone Routing Protocol for Ad Hoc Networks". Internet Draft, draft-ietf-manet-zrp-02.txt, 1999. http://www.ietf.org.

[20] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks," *Ad Hoc Networks*, Vol. 3, 2005, pp. 325-349.

[21] T. He, *et al.*, "SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks," *Proceedings of International Conference on Distributed Computing Systems*, Providence, RI, 19-22 May 2003, pp. 46-55.

[22] K. Akkaya and M. Younis, "An Energy-Aware Qos Routing Protocol for Wireless Sensor Networks," *Proceedings of the IEEE Workshop on Mobile and Wireless Net works* (*MWN* 2003), Providence, RI, May 2003.

[23] Emad Felemban, Chang-Gun Lee, and Eylem Ekici, "MMSPEED: Multipath Multi-SPEED Protocol for QoS Guarantee of Reliability and Timeliness in Wireless Sensor Networks", IEEE Transaction on mobile computing, Vol. 5, no. 6, June 2006, pp. 710-715.

[24] H. W. Tsai, *et al.*, "Mobile Object Tracking in Wireless Sensor Networks," *Journal of Computer Communications*, Vol. 30, No. 8, March 2007.

[25] Q. Huang, S. Bhattacharya, C. Lu and G. Roman, "FAR: Face-Aware Routing for Mobicast in Large-Scale Sensor Networks," *ACM Transactions on Sensor Networks*, Vol.1, No. 2, 2005, pp. 240-271.

[26] K. R. Gabriel, R. R. Sokal, "A New Statistical Approach to Geographic Variation Analysis," *Systematic Zoology*, Vol. 18, No. 3, 1969, pp. 259-270.

[27] P. Ji, *et al.*, "DAST: A QoS-Aware Routing Protocol for Wireless Sensor Networks," *Proceeding of International Conferences on Embedded Software and Systems Symposia*, Sichuan, 29-31 July 2008, pp. 259-264.

[28] C. Raghavendra and S. Singh. "PAMAS- Power Aware Multi-access Protocol with Signaling for Ad Hoc Networks". ACM SIGCOMM Computer Communication Review, pages 5–26, 1999.

[29] E. W. J.-P. Ebert, B. Stremmel and A. Woliz. "An Energy-efficient Power Control Approach for WLANs". Journal of Communications and Networks (JCN), 2(3):197– 206, 2000.

[30] T. J. Kwon and M. Gerla. "Clustering with Power Control". 2:1424–1428, 1999.

[31] P. A. C. E. Jones, K. M. Sivalingam and J.-C. Cheng. "A Survey of Energy Efficient Network Protocols for Wireless Networks". ACM Wireless Networks, 7(4):343–358, 2001.

[32] P. B. R. Wattenhofer, L. Li and Y.-M. Wang. "Distributed Topology Control for Power Efficient Operation in Multi-hop Wireless Ad Hoc Networks". IEEE INFOCOM 2001, pages 1388–1397, 2001.

[33] M. Gerla. "Clustering and Routing in Large Ad Hoc Wireless Nets", 1998.

[34] A. R. K. Lahiri and S. Dey. "Communication Architecture Based Power Management for Battery Efficient System Design". Annual ACM IEEE Design

Automation Conference, Proceedings of the 39th Conference on Design Automation, New Orleans, Louisiana, pages 691–696, 2002.

[35] P. A. K. M. Sivalingam, J.-C. Chen and M. Srivastava. "Design and Analysis of Low-Power Access Protocols for Wireless and Mobile ATM Networks". ACM Wireless Networks, pages 73–87, 2000.

[36] P. A. Chen J.-C., K. Sivalingam and S. Kishore. "A Comparison of MAC Protocols for Wireless Local Networks Based on Battery Power Consumption". IEEE INFOCOM, Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, 1:150–157, 1998.

[37] D. E. W. Ye and J. Heidemann. "An Energy-efficient MAC Protocol for Wireless Sensor Networks". INFOCOM 2002 IEEE Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, 3, 2002.

[38] B. P. E. U.-B. A. El Gamal, C. Nair and S. Zahedi. "Energy-efficient Scheduling of Packet Transmissions over Wireless Networks". IEEE INFOCOM, IEEE Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, 3(2002):1773–1782, 2002.

[39] P. Krishnan and R. Kravets. "Application-driven Power Management for Mobile Communication". ACM Wireless Networks, 6:263–277, 2000.

[40] R. R. Rao and M. Zorzi. "Error Control and Energy Consumption in Communications for Nomadic Computing". IEEE Transactions on Computers, 46(3):279–289, 1997.

[41] C. F. P. Lettieri and M. B. Srivastava. "Low Power Error Control for Wireless Links". International Conference on Mobile Computing and Networking, Proceedings

of the 3rd annual ACM IEEE International Conference on Mobile Computing and Networking, pages 139–150, 1997.

[42] J. S. P. Agrawal, B. Narendran and S. Yajnik. "An Adaptive Power Control and Coding Scheme for Mobile Radio Systems". Proceedings of IEEE Personal Communications Conference, pages 283–288, 1996.

[43] M. W. S. Singh and C. S. Raghavendra. "Power-Aware Routing in Mobile Ad Hoc Networks". International Conference on Mobile Computing and Networking, Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pages 181–190, 1998.

[44] L. Tassiulas and J. H. Chang. "Energy Conserving Routing in Wireless Ad-Hoc Networks". The IEEE Conference on Computer Communications INFOCOM, pages 22–31, 2000.

[45] J. H. Ryu and D. H. Cho. "A New Routing Scheme Concerning Power-Saving in Mobile Ad Hoc Networks". Proceedings of the IEEE International Conference on Communications, 3:1719–1722, 2000.

[46] L. Xu and I. Stojmenovic. "Power-Aware Localized Routing in Wireless Networks". IEEE Transactions on Parallel and Distributed Systems, 12(11):1122–1133, 2000.

[47] R. Ramanathan and R. Rosales-Hain. "Topology Control of Multi-hop Wireless Networks Using Transmit Power Adjustment". INFOCOM, Proceedings of the Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, 2:404–413, 2000.

[48] S. Banerjee and A. Misra. "Adapting Transmission Power for Optimal Energy

Reliable Multi-hop Wireless Communication". Wireless Optimization Workshop (WiOpt'03), 2003.

[49] A. Spyropoulos and C. S. Raghavendra. "Energy Efficient Communications in Ad Hoc Networks using Directional Antennas". The IEEE Conference on Computer Communications INFOCOM, pages 220–228, 2002.

[50] G. N. J. Wieselthier and A. Ephremides. "Energy-Limited Wireless Networking with Directional Antennas: the Case of Session Based Multicasting". IEEE Conference on Computer Communications INFOCOM, 2002.

[51] L. M. Feeney. "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks". Mobile Networks and Applications, 6(3):239–249, 2001.

[52] S. S. J. Stepanek and C. Raghavendra. "Power-Aware Broadcasting in Mobile Ad Hoc Networks". Proceedings of IEEE PIMRC, 1999.

[53] G. D. N. J. Wieselthier and A. Ephremides. "On the Construction of Energy-Efficient Broadcast and Multicast Trees". IEEE Conference on Computer Communications INFOCOM, pages 585–594, 2000.

[54] A. Bakre and B. R. Badrinath. "I-TCP: Indirect TCP for Mobile Hosts". Proceedings of the 15th International Conference on Distributed Computing Systems, pages 136–143, 1995. 185

[55] T.F.L.K.K.S.E. Ayanoglu, S. Paul and R. D. Gitlin. "AIRMAIL: A Link-Layer Protocol for Wireless Networks". ACM Wireless Networks, 1(1):47–60, 1995.

[56] H. B. K. Pentikousis, V. Tsaoussidis and X. Ge. "Energy / Throughput Tradeoffs

of TCP Error Control Strategies". Proceedings of the 5th IEEE Symposium on Computers and Communications (ISCC), 2000.

[57] P. Krishnan and R. Kravets. "Application-driven Power Management for Mobile Communication". ACM Wireless Networks, 6:263–277, 2000.

[58] I. Corporation. "ACPI-Frequently Asked Questions". http://www.intel.com/technology/iapc/acpi/faq.htm.

[59] C.Siva Ram Nurthy and B.S. Manoj .Ad hoc wireless networks Architectures and Protocols,. Prentice Hall, 2004.

[60] QoS relevant lecture slides from Helsinki University of Technology: http://keskus.hut.fi/opetus/s382121/s05/Slides, visited 2006-07-22

[61] A.Lindgren. A.Almoquist, and O.Schelen, "Evolution of Quality of Service Scheme for IEEE 802.11", In Proc. Of IEEE LCN 2001, November 2001.

[62] X. Gu, K. Nahrstedt, R. N. Chang, and C. Ward. "QoS Assured Service Composition in Managed Service Overlay Networks". Proc. of IEEE 23nd International Conference on Distributed Computing Systems (ICDCS 2003), Providence, RI, May 2003.

[63] Gahng-Seop Ahn, Andrew T.Campbell, Andras Veres and Li-Hsiang Sun, "SWAN: Service Differentiation in Stateless Wireless Ad Hoc Networks", In Proc. IEEE INFOCOM'2002, New York, New York, June 2002.

[64] K. Farkas, D. Budke, B. Plattner, O. Wellnitz, and L. Wolf, "QoS Extensions to Mobile Ad Hoc Routing Supporting Real-Time Applications," presented at 4th ACS/IEEE International Conference on Computer Systems and Applications

(AICCSA-06), Dubai-UAE, 2006.

[65] B. O'Hara and A. Petrick, "The IEEE 802.11 Handbook: A Designer's Companion," IEEE Press, January 1999.

[66] C. K. Toh, "Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks," IEEE communication Magazine. 2001.

[67] Carla F. Chiasserini, Pavan Nuggehalli and Vikram Srinivasan, "Energy-Efficient Communication Protocols," Proceedings of 39th Design Automation Post-Conference (DAC) 2002, June 2002.

[68] M.S.H.Woesner, J.-P. Ebert and A. Wolisz. "Power-Saving Mechanisms in Emerging Standards for Wireless LANs: the MAC Level Perspective". IEEE Personal Communication, 5(June):40–48, 1998.

[69] Danilo Tardioli and Jose Luis Villarroel. Adding multicast capabilities to wireless multi-hop token-passing protocols: Extending the rt-wmp. In *14th IEEE International Conference on Emerging Technologies and Factory Automation*, 2009.

[70] R. P. Moreno, D. Tardioli, and J. Salcedo, "Distributed Implementation of Discrete Event Control Systems based on Petri nets," in *IEEE Int. Symposium on Ind. Electronics*, June 2008, pp. 1738–1745.

[71] S. Yarkan, S. Guzelgoz, H. Arslan, and R. Murphy, "Underground mine communications: A survey," Communications Surveys & Tutorials, IEEE, vol. 11, no. 3, pp. 125–142, Quarter 2009.