University of Windsor

Scholarship at UWindsor

Electronic Theses and Dissertations   Theses, Dissertations, and Major Papers

2006

Enhanced QoS for real-time multimedia delivery over the wireless link using RFID technology.

Mythili Enugula
University of Windsor

Follow this and additional works at: https://scholar.uwindsor.ca/etd

Enhanced QoS for Real-time Multimedia Delivery over the Wireless Link using RFID Technology

by

Mythili Enugula

A Thesis
Submitted to the Faculty of Graduate Studies and Research
through Computer Science
in Partial Fulfillment of the Requirements for
the Degree of Master of Science at the
University of Windsor

Windsor, Ontario, Canada

2006

© 2006 Mythili Enugula

Library and
Archives Canada

Bibliothèque et
Archives Canada

Published Heritage
Branch

Direction du
Patrimoine de l'édition

395 Wellington Street
Ottawa ON K1A 0N4
Canada

395, rue Wellington
Ottawa ON K1A 0N4
Canada

NOTICE:
The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:
L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

ABSTRACT

This thesis presents a Sensor Guided Wireless Adaptation Scheme (SGWAS) that works in a micromobility domain. SGWAS infers the reason of high packet loss in a real-time multimedia flow received by a mobile node in a wireless cell. Determining the reason of packet loss relies on information obtained from wireless sensors, specifically RFID devices scattered in the cell, to detect the location of the mobile node. If packet loss is due to wireless link congestion, then local rate adaptation is applied in the cell. However, if it is due to handoff or signal propagation effects, e.g. obstruction or attenuation, then rate adaptation is not performed. The source adapts its transmission rate if congestion occurs in the wired network.

SGWAS helps improve the quality of service and avoids unnecessary rate adaptation. Simulation results demonstrate that SGWAS identifies the reason of high packet loss and performs rate adaptation only when needed.

DEDICATION

To my parents who supported and encouraged me throughout the course of this thesis.

ACKNOWLEDGEMENTS

I would like to thank Dr. Randa El-Marakby for helping me write my thesis. She not only served as my supervisor but also encouraged and supported me all time in this research.

My special thanks to my husband, my parents and my sister whose love and support enabled me to complete this work.

v

TABLE OF CONTENTS

LIST OF TABLES

viii

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Recently, there has been an increasing demand for real-time multimedia applications over the wireless Internet. Applications like IP telephony and audio/video conferencing have been used over the wired Internet. They are different from traditional applications like e-mail, file transfer, etc... This chapter gives an overview of the real-time multimedia applications and the techniques used for the delivery of audio/video over the Internet. It also presents a brief introduction on wireless networks, mobility, and the problems in providing Quality of Service (QoS) to the applications over wireless networks.

1.1 Real-time Multimedia Applications

Real-time multimedia applications sending audio/video have different characteristics when compared to traditional network applications like e-mail, file transfer, etc... These multimedia applications have timing constraints and are highly delay-sensitive. The data received by the user is useful only when received with a certain quality. For example, highly interactive audio applications like Internet telephony can tolerate delays between 150 to 400 milliseconds [KR03]. But traditional network applications can tolerate more delay where completeness and integrity of data transferred is preferred.

Multimedia applications cannot tolerate significant packet loss. Packet loss might occur because of the overflow of the buffers in the routers on the path from sender to receiver. If the buffer is full, the arriving packets are discarded and they never reach their destination. Although many real-time multimedia applications are loss-tolerant, only 20% loss rate is tolerable by humans.

These applications usually require high bandwidth as they send large amount of data. Increase in the number of Internet users running real-time multimedia applications results in high traffic and thus creates congestion in the network. Congestion leads to the data quality degradation.

1

1.2 Real-time Transport Protocol (RTP)

The Real-time Transport Protocol (RTP) [SCF03] is being used by most of the real-time multimedia applications to deliver real-time audio and video over the Internet. RTP consists of two protocols: RTP Data Transfer Protocol for real-time data transmission; and RTP's Control Protocol (RTCP) for monitoring the Quality of Service (QoS) of the data received. RTCP provides feedback reports that are sent periodically by participants in the RTP session. The feedback reports summarize the quality of the data transmission in the multimedia session. The Receiver feedback Reports (RRs) issued by the receivers, include the fraction of packet loss, incurred in the current interval, which is used as an indicator of congestion. So, if there is a lot of packet loss in the current interval, then participants will assume there is congestion currently in the network. Then the sender can dynamically adapt the transmitting rate to suit the current network state. However, when running these applications on wireless networks, packet loss could be related to different causes other than congestion. This could be due to the wireless link characteristics like the low bandwidth of the wireless link, high bit-error rate, signal attenuation or obstruction or due to mobility.

1.3 Wireless Networks

In wireless networks, mobile nodes (e.g. laptop, palmtop, PDA) move from one network to another. This process is known as handoff. Such mobility leads to many problems like finding the current location of the mobile node and forwarding the data. Handoffs usually result in packet loss and delay which degrades the quality of real-time multimedia applications. During this process, the mobile node has to keep the same IP address to run the ongoing applications. To manage these mobility issues, Mobile IP [PER02] protocol was developed. It enables nodes to change their point of attachment to the Internet without changing their IP address. However, significant packet loss and delay occur when using Mobile IP for micromobility i.e. when the mobile node moves between multiple sub networks within a single network domain, such as a wide area network. To solve these problems, Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) micromobility approach [RVS02] was proposed. In this thesis,

2

we use this approach for data forwarding during handoff. This is a domain-based approach that supports mobility in wide-area wireless networks and helps in reducing delay and packet loss that occurs because of mobility and thus helps in improving the performance of multimedia applications.

1.4 Problem Description

When running multimedia applications over wireless cellular networks, packet loss occurs due to different causes other than congestion. That is to say, packet loss could be due to the low bandwidth of wireless link, signal attenuation or obstruction, or handoff. If packet loss occurs because of congestion, rate adaptation is performed to improve the quality of the transmission. However, if packet loss occurs due to wireless link problems, rate adaptation is not appropriate. So there is a need to identify the main reason of packet loss. In order to detect the reason of high packet loss, it is important to know the location of the mobile node. To know the location of the mobile node, Wireless Sensor Networks (WSNs) specifically Radio frequency ID (RFID) devices i.e. RFID tags and readers [AIM01] are used. RFIDs provide an efficient way to automatically detect, monitor, and control any object. This is done by a tag, which is embedded into any object and identifies the object. RFID readers read the information stored at tags that exist in their vicinity. This information is sent to an entity for processing through wireless link. Moreover, packet loss could occur because of changing weather conditions, e.g. raining, snowing, etc... Weather sensors can also play a role to sense the weather conditions in the cell where the mobile node is currently located.

1.5 Objective, Contributions and Significance

The main objective of this thesis is to help improve the QoS of the real-time multimedia delivery in wireless cellular networks. To achieve the objective, this thesis makes the following contributions:

- A scheme called, Sensor Guided Wireless Adaptation Scheme (SGWAS) has been designed.

3

- To the best of our knowledge it is the first time to use RFID devices to help improve the QoS of real-time multimedia delivery in wireless cellular networks.
- SGWAS identifies situations where local wireless rate adaptation or sender rate adaptation should be performed to alleviate congestion.
- SGWAS uses information sent by RFID devices to determine the location of the mobile node and thus detect if the mobile node is currently in the handoff region or is suffering from signal attenuation.
- SGWAS has been implemented in the Network Simulator (NS-2).

SGWAS helps improve the QoS of real-time multimedia delivery in wireless networks and avoids unnecessary rate adaptation. That is to say, if the mobile node is suffering from high packet loss because it is in the handoff region or it is far away from the base station, then the decrease in the transmission rate will not decrease the packet loss. Thus, in these cases rate adaptation is not performed and the quality of the real-time multimedia flow delivered to other receivers in the same session will not be affected.

1.6 Thesis Organization

This thesis is organized as follows. Chapter 2 provides some background on Real-time Transport Protocol (RTP) used for the delivery of real-time multimedia. Then, it gives an introduction on Wireless Sensor Networks and RFID devices which are used in the proposed scheme (SGWAS). Moreover, it describes the mobility management protocol used in the scheme. It discusses also the related work and compares the previous work with the proposed scheme. Chapter 3 explains SGWAS in details. It describes the problems to be solved by the scheme and solutions. Chapter 4 reviews the Network Simulator (NS-2) which is used in the simulation and explains also the wireless model and RTP features in NS-2. Chapter 5 describes the simulation topology, implementation details, experiments and results. Finally, chapter 6 presents the conclusions and recommendations. Appendix A defines terms used in this thesis. Appendix B lists the abbreviations used.

4

CHAPTER II

LITERATURE REVIEW

This chapter presents some background about the Real-time Transport Protocol (RTP), used in real-time multimedia transmission over the Internet, and its associated control protocol RTCP. Then, it introduces Wireless Sensor Networks (WSNs) and wireless RFID devices, which we use in our scheme. Furthermore, it presents the domain based micromobility approach called HAWAII [RVS02] that we use in our architecture. Finally, it explains some of the previous related work performed in this area and compares it with SGWAS.

2.1 Multimedia Delivery

Multimedia applications that send audio and video over the Internet have become very popular recently. Real-time multimedia applications require high Quality of Service (QoS) guarantees. QoS refers to the ability of an application to obtain the network service it requires for successful operation [FH98]. The main goal of the QoS is to provide applications with minimum bandwidth, low packet loss, and controlled delay and jitter. The QoS parameters affecting the delivery of real-time multimedia applications are packet loss rate, delay, jitter, and throughput [see Appendix A].

Real-time multimedia applications have different QoS requirements when compared to traditional network applications like FTP, email, etc.. Multimedia applications require high bandwidth because of their high data rates. If the minimum bandwidth requirement is not met, the quality degrades due to congestion. Unlike traditional applications, real-time multimedia applications cannot tolerate delay but can tolerate packet loss to some extent. Real-time multimedia applications require also the data to be played back in-order along with synchronization of audio and video flows. These applications can run in unicast mode, i.e. data flows from one sender to one receiver, or can run in multicast environment i.e. a data flow from a sender is sent to multiple receivers.

5

To handle these QoS requirements of real-time multimedia applications, the Real-time Transport Protocol (RTP) and its associated Real-time Control Protocol (RTCP) [SCF03] was proposed. In the next section, RTP/RTCP is explained in details.

2.2 RTP and RTCP Protocols

The Real-time Transport Protocol (RTP) provides end-to-end delivery services for real-time data such as audio and video. RTP supports data transfer over both unicast as well as multicast networks. Its services include payload type identification, sequence numbering, time stamping, and monitoring delivery of data. These services help in monitoring QoS and also handle timing and synchronization issues of real-time multimedia applications. RTP is integrated into the application. It runs usually on top of the network transport protocols, typically User Datagram Protocol (UDP) [POS80]. But RTP doesn't ensure timely delivery of data. Also, it doesn't guarantee delivery or prevent out-of-order packets. It does not assume a reliable underlying network and delivers packets in sequence. The sequence numbering in RTP packet header allows the receiver to reconstruct the packets. RTP consists of two protocols as shown in Figure 1.
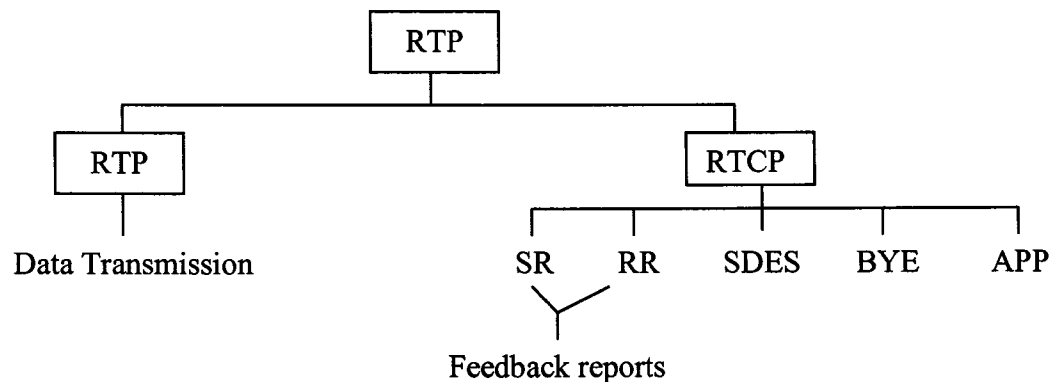
Figure 1: RTP and RTCP

- RTP Data Transfer Protocol for real-time multimedia transmission and
- RTCP Control Protocol for monitoring QoS and providing feedback information on the data received by the participants in a session [see

6

Appendix A]. It provides also minimum session control information about all participants in the session.

2.2.1 RTP data transfer protocol

The RTP data transfer protocol is used for real-time multimedia transmission. The sender sends chunks of data called packets and each RTP packet consists of a header and payload. The header consists of several main fields, e.g. payload type, sequence number, timestamp, synchronization source identifier (SSRC).

The **payload type** field identifies the format of the RTP payload and determines its interpretation by the application.

The **sequence number** increments by one for each RTP data packet sent and may be used by the receiver to detect packet loss and restore the packet sequence.

The **timestamp** reflects the sampling instant of the first octet in the RTP data packet. This sampling instant is derived from a clock that increments linearly. This is useful for synchronization and jitter calculations.

The **SSRC** field uniquely identifies the synchronization source within the same RTP session. This identifier is chosen randomly so that all the sources within a RTP session have different SSRC identifier. This helps also in identifying the data sender within a group of participants in a session.

A RTP packet is sent to a UDP socket and is encapsulated as a UDP packet. Then, the packet is forwarded to the IP layer and is encapsulated as an IP datagram. This encapsulation is done by the end systems. Routers do not have any knowledge on the RTP packet carried in the IP datagram.

As mentioned earlier, RTP packets can be sent over both unicast and multicast networks. In a multimedia session, for example, in a videoconference session, audio and

7

video are carried in separate sessions. A participant may be involved in multiple RTP sessions at the same time. Each participant distinguishes multiple sessions using different pairs of destination transport addresses, where each pair includes a network address plus a pair of ports for RTP and RTCP. In multicast, all the participants in a session use the same destination transport address pair. Whereas in unicast, the destination transport address pairs are different for the sender and the receiver. In unicast case, the receiver receives data from the sender using same pair of ports for RTP and RTCP or may be different pairs.

2.2.2 Real-time control protocol (RTCP)

The Real-time Control Protocol (RTCP) transmits periodically control information to all participants in a session. Its functions include QoS monitoring, source identification and RTCP bandwidth scaling.

QoS monitoring

This is the main function of RTCP. RTCP provide feedback information summarizing the quality of multimedia data received. Using this feedback information, the data sender can assess the current state of the network to adjust its transmission rate or change the encoding to alleviate congestion in the network and to improve QoS. The participants may also use this feedback information to identify problems and evaluate if those problems are local or global. The feedback information can also be sent to a network service provider, which is not involved in the session and can act as a third-party monitor to diagnose network problems.

Source identification

RTCP Source DEScription (SDES) packets contain an identifier called canonical name (CNAME) for an RTP source. Receivers require the CNAME to keep track of each participant in case if the synchronization source identifier (SSRC) is changed due to conflicts. The CNAME is used also for synchronization of audio and video data received.

8

RTCP bandwidth scaling

RTCP packets are sent periodically to all participants in a session. But, the rate at which the control packets are sent has to be controlled with the increase in the number of participants in order for RTCP to scale up to a large number of participants. RTCP attempts to limit its control traffic to 5% of the session bandwidth. RTCP gives 75% of this bandwidth to receivers and remaining 25% to the senders. To reduce the traffic, RTCP modifies the transmission rate as a function of the number of participants in the session. This number is obtained by having each participant send its control packets to all the others in a session, so that each participant can independently keep track of the number of participants. Each participant determines also the RTCP packet transmission period by calculating the average RTCP packet size and dividing by the allocated transmission rate.

RTCP Packets

RTCP defines five types of RTCP packets, namely SR (Sender Report), RR (Receiver Report), SDES (Source DEScription items), BYE and APP (Application defined). The participant who issues a SR packet is a data sender who is also a receiver, while a participant who issues a RR packet is only a receiver. These two types of packets contain reception statistics summarizing the quality of the transmission. SDES packets contain information about the source. BYE must be the last packet in the communication which signals the leaving of the participant. The APP packets are for experimental use.

Sender and Receiver Reports

SRs and RRs are the most important feedback reports. The participants that are active senders and also receivers send SRs. The participants who are only receivers send RRs. Both SRs and RRs contain reception report blocks, one for each of the data sources sending RTP data. A source could be a MIC or a camera, for example. Each block consists of the following fields:

- The SSRC_n identifier is the nth identifier of the source of the information in the block.

9

- The Fraction lost is the fraction of RTP data packets lost in the interval [see Appendix A] between sending this feedback report and the previous one. The interval is the time difference between sending the current RTCP feedback report and the previous one from the same node. The fraction of packet loss is computed as the number of packets lost divided by the number of packets expected [SCF03].

- Cumulative number of packets lost is the total number of RTP data packets from SSRC_n that are lost since the beginning of reception.

- Interarrival jitter is the estimate of the statistical variance of the RTP data packet interarrival time.

- Delay since last SR (DLSR) is the delay between receiving the last SR packet from source SSRC_n and sending this reception report block.

The SR provides more statistics summarizing the data transmission from the sender, e.g. timestamps, number of RTP data packets, and the number of payload octets transmitted. Timestamps are used for the reconstruction and the synchronization of the data packets sent by the sender.

SDES – Source Description Packet

The packet provides identification information of all participants in the session. It contains items like CNAME, EMAIL, PHONE, etc... to describe the sources. CNAME is the canonical name of the source used as an identifier of the source. CNAME is used to keep track of each participant in case if the synchronization source identifier (SSRC) is changed due to conflicts.

BYE and APP Packets

The BYE packet indicates that one or more sources are no longer active. The APP packet is intended for experimental use as new applications and new features are developed.

The feedback information given by the RTCP reports is useful for both data senders and receivers and also for third-party monitors. The information conveyed by these reports help in analyzing the current network state and thus helps in designing new

10

schemes and algorithms for improving QoS and congestion control. The SGWAS scheme proposed in this thesis uses RTCP RRs to collect the feedback information and determine the current network state. In our work, we have modified the RTP to send the RTCP RRs unicast to the sink. We use the fraction lost field of RR i.e. the fraction of packet loss incurred in the current interval to identify network state. Since the packet loss rate reported in RTCP RRs reflects the current network state, this information can be used for to perform adaptation and improve the QoS of the real-time multimedia application.

2.2.3 Sender adaptation

When running real-time multimedia applications over wired/wireless networks, the desired QoS may not be achieved because of the frequent changes in network state. This might be due to change in the availability of network resources because of different network conditions and congestion. An efficient way to improve the QoS of a real-time multimedia application in such conditions is to perform adaptation.

A common example of adaptation is of a sender adapting its transmission rate dynamically based on the feedback received form the receiver. This feedback reflects the current network state. But if the available bandwidth is too low, then rate adaptation cannot guarantee a minimum quality. Some other ways of performing adaptation are change audio/video encoding, change the color of frames in case of video transmission, or change the frame size.

Several rate-adaptation algorithms [BT94] [BDS96] [EH97] are proposed for improving the QoS of real-time multimedia applications. In our scheme, we use the algorithm proposed in [EH97] to solve the congestion problem. In this algorithm, rate adaptation is performed by the sender. The sender uses the fraction of packet loss sent in RTCP RRs to identify the current network state. On one hand, if the packet loss reported in RRs is more than a certain threshold, the sender identifies that the network is congested and decreases its transmission rate by a fixed fraction. This helps in transmitting less number of packets and thus reduces network congestion as the bandwidth requirements of the sender are decreased. On the other hand, if the packet loss becomes less than a certain threshold, the rate is increased by a fixed fraction and more packets are transmitted.

11

2.3 Wireless Sensor Networks

As mentioned in section 1.2, when running real-time multimedia application over wireless networks, packet loss could be due to signal attenuation or handoff other than congestion. To differentiate wireless link losses from congestion, there is a need to identify the location of the mobile node. To know the location of the mobile node, we use Wireless Sensor Networks (WSNs) specifically Radio frequency ID (RFID) devices, i.e. RFID tags and readers [AIM01]. This subsection introduces the concept of wireless sensors and RFID devices.

Recent technological advances have led to the development of small, inexpensive and low power sensor nodes that are capable of wireless communication. These sensor nodes perform sensing, data processing, and communicating tasks. Large collections of such nodes coordinate and perform large sensing tasks. Such collections of sensor nodes that perform a specific sensing task are known as Wireless Sensor Networks (WSN). Sensors have a variety of applications namely, environmental monitoring, military surveillance, healthcare, industrial purposes, motion monitoring, disaster management etc... Sensor nodes can be randomly deployed in any environment like in a remote geographic location or in a physical structure like a machine, vehicle, bridge or building. An example for a sensor could be a weather sensor that can be used to monitor the weather conditions and report any changes (sunny, raining, snowing, etc...). Another example can be the Radio Frequency Identification (RFID) device that could act as a sensor (see subsection 2.3.3). In our scheme, we use wireless sensors, specifically RFID devices to detect the location of mobile node and determine the main reason of packet loss when transmitting audio/video data between mobile nodes. In the remaining part of this chapter, we present the applications of sensor networks, WSN architecture and protocol stack and describe RFID devices and their applications in detail.

2.3.1 Wireless sensor network applications

Sensors have a variety of applications namely, environmental monitoring, military surveillance, healthcare, industrial purposes, motion monitoring, disaster management

12

etc... Sensors are of different types: visual, infrared, acoustic and radar, thermal, etc.. The new concept called motes or smart dust sensors has become very famous recently [PK00]. A mote usually consists of a small, low-cost and low-power computer that acts like a sensor. For example, motes can be used for military purposes to gather information on battlefields or even to monitor the strength of bridges or buildings. Another important application is sensors for medicine and science. Oxygen sensors can be used for metabolic rate measurement and glucose sensors for monitoring glucose for diabetic patients [SGW01]. Coming to environmental applications, sensors can monitor temperature, pressure humidity, etc.. Oceanographic sensors are used for monitoring under water environment against the threat of biological or chemical contamination. Commercial applications include wireless automatic meter reading, which is very cost-effective of gathering consumption data (electricity, gas, water) to the billing system. Sensors can also be used to control heat, ventilation and air conditioning in commercial buildings.

2.3.2 WSN architecture and protocol stack

A sensor node usually consists of four components: a sensing unit, processing unit, transceiver unit, and a power unit [AVA02]. A sensing unit consists of a sensor, which produces analog signals, and an analog to digital converter, which converts the analog signals to digital signals before sending the signals to the processing unit. The processing unit manages the procedures that enable the sensor node to collaborate with other nodes to carry out the sensing tasks. The transceiver, which is an optical or radio frequency device, connects the sensor node to the network. The power unit is the main component of a sensor node, which provides little power because of its small size. Since a sensor node has limited energy and processing capability, a large number of sensor nodes have to be deployed in a wide region. This helps in increasing the accuracy of the data reported by the sensor nodes.

Sensor nodes are present in a field where they sense, collect data, and route this data to the sink. Sink is a sensor node with more energy and processing capabilities than other sensor nodes. Figure 2 shows the data flow from sensors to the sink in a WSN. First, the sink requests specific data by sending queries to the sensors. The sensors sense

13

an event, e.g. moving vehicle, and send the collected data to the sink. This data is routed hop-by-hop through the sensor nodes until it reaches the sink. The sensor nodes communicate through wireless links that can be formed by radio, infrared, or optical media. Then, the sink sends this data to a task manager node (not shown in the figure), which in turn sends it to the end user. The sink communicates with the user through network services, such as Internet services. The data is sent from the sensors to the sink using multi-hop communication.
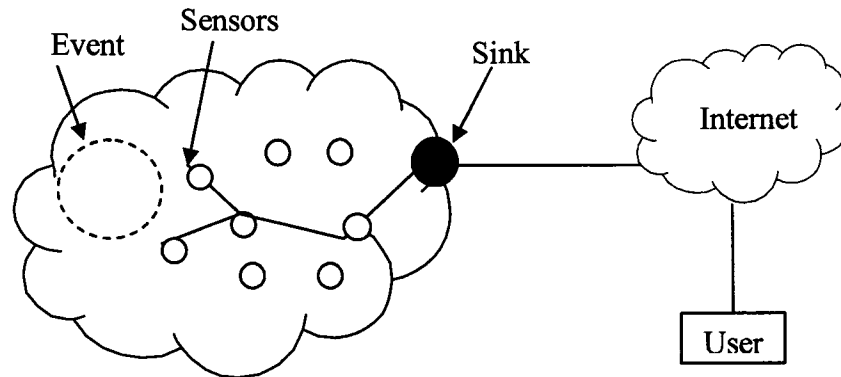
Figure 2: Wireless Sensor Network

The sink and sensors have a 5-layer protocol stack [AVA02]: application layer, transport layer, network layer, data link layer, and physical layer. Based on the type of sensing task, different types of application software can be built and used in the application layer. The transport layer helps in maintaining the flow of data depending on the requirement of the sensor application. For example, the transport layer may provide an error control mechanism for the data delivered between a sensor and the sink based on the reliability requirement of the application layer. It may use also congestion control mechanisms to regulate the amount of traffic injected into the network.

The network layer takes care of routing the data forwarded by the transport layer. Flooding is an old technique that can be used for routing in sensor networks. In flooding, each node receiving a data or management packet repeats it by broadcasting, until it reaches its destination or minimum number of hops is reached. In our scheme (SGWAS), we use flooding protocol for routing of data packets between sensors and sink. Other routing protocols for sensor networks include Sensor Protocols for Information via

14

Negotiation (SPIN), Directed Diffusion [IGE00], Low-Energy Adaptive Clustering Hierarchy (LEACH) [HCB00], etc..

The data link layer must be power-aware. It handles multiplexing/demultiplexing of data, data frame detection, medium access, and error control. The physical layer converts mainly the bit streams into signals that can be communicated across the wireless link. This layer is responsible also for frequency selection and generation, modulation, signal detection, and data encryption. Sensor nodes also have power, mobility and task management planes to monitor the power, movement, and task assignment among the sensor nodes.

2.3.3 Radio frequency identification (RFID)

RFID technology [SAB04] is becoming more popular because of its applications at home, manufacturing, vehicle tracking, etc... RFID devices provide an efficient way to automatically detect, monitor and control any object. In our SGWAS scheme, we use RFID devices to help identify the location of mobile node. This is achieved by the two components of RFID devices, namely RFID tag and RFID reader, as shown in Figure 3. RFID tags are comprised of small integrated circuit for storing information and an antenna used for communication. Tags can be embedded into any object and can store the identification of that object. Tags are of two types, passive and active. Passive tags do not have batteries and instead use the energy from the received signal to send its stored information. Active tags are powered by an internal battery. RFID readers read the information stored at the RFID tags that exist within their vicinity. A RFID reader has also an antenna to communicate the information. It sends the information received from the nearby tags, via wired or wireless links, to a central database for processing [CRK05].

15
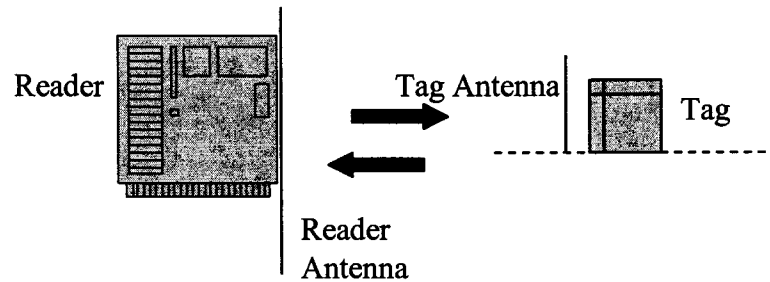
Figure 3: RFID device Components

RFID tags consist of small memory for storing the identification of an object. The memory can be Read-Only Memory (ROM), Random Access Memory (RAM), or non-volatile programmable memory depending on the type and sophistication of the tag. Tags with ROM are invariably low capacity devices programmed at source, usually with an identification number. Tags with non-volatile programmable memory are user programmable and also allow the user to change data stored in a tag.

2.3.4 RFID applications

RFID devices have many applications in home, manufacturing, vehicle tracking etc... In case of vehicle tracking, an RFID tag may be attached to a license plate of a vehicle and this helps in automatic and reliable identification of the vehicle. Another interesting application is to place a tag on the dashboard of a car. A deployed infrastructure of RFID readers can then localize the vehicle carrying RFID tag and thus send information about nearest restaurants, hospital, bank or even weather, and traffic information [KRO05]. Even for security purposes, the Police can use RFIDs for detecting the prisoners or even preventing unauthorized access to the confidential locality. RFID Tags can be also inserted underneath the skin of animals for animal tracking. They come also in screw-shaped to identify trees, wooden items, or credit-card shapes for use in access applications.

16

2.4 Micromobility in Wireless Network Domain

This subsection gives a brief introduction to wireless networks and describes the protocols used for mobility management in wireless networks.

In the past decade there has been a rapid growth in the use of wireless devices for Internet access. Examples of these wireless devices include laptops, PDAs, palmtops, cellular phones etc. Wireless networks consist of these devices and are known as mobile hosts. A mobile host connects to a base station or other hosts through a wireless communication link. The base station transmits data to and from the mobile hosts. These base stations are in turn connected to large networks like the Internet. If a host is connected to a base station it means that it is within the wireless communication distance of the base station. The region that is covered by a base station is called a cell. Examples of base stations include cell towers in cellular networks and access points in wireless Local Area Networks (LANs).

When the mobile host (mobile node) moves from one base station range to another, it changes its point of attachment, i.e. it changes the base station with which it is associated. This process is known as Handoff (see Appendix A). Such mobility poses many challenges like finding the current location of the host and forwarding data. Handoffs often result in data loss as the data may not be forwarded to the new location of the mobile host and it may introduce large variations in packet (data) delivery times. Running multimedia applications that require minimum bandwidth, low delay, and low packet loss during frequent handoffs is very challenging.

2.4.1 Mobile IP

During the process of handoff, the mobile node has to keep the same IP address to run the ongoing applications. Mobile IP is the protocol, which enables nodes to change their point of attachment to the Internet without changing their IP address [PER02]. The Mobile Node (MN) is assigned a fixed IP address in its home network and the Home Agent (HA) of that network maintains a list of all mobile nodes registered. During handoff, when the mobile node moves to a foreign network, the Foreign Agent (FA) of the foreign network assists the mobile node by creating a temporary address called Care-

17

of-Address to identify the mobile node's current new location. The mobile node discovers the Foreign Agent/Home Agent either by the agent advertisements received from them or by soliciting the Foreign Agent/Home Agent. The mobile node registers the care-of-address with its home agent and thus informs its home agent about its current location. A Correspondent Node (CN) is the one trying to communicate (send/receive data) to/from the mobile node. Figure 4 shows the routing of packets from the correspondent node to the mobile node when away from home. The following steps summarize the routing of packets from the correspondent node to the mobile node.
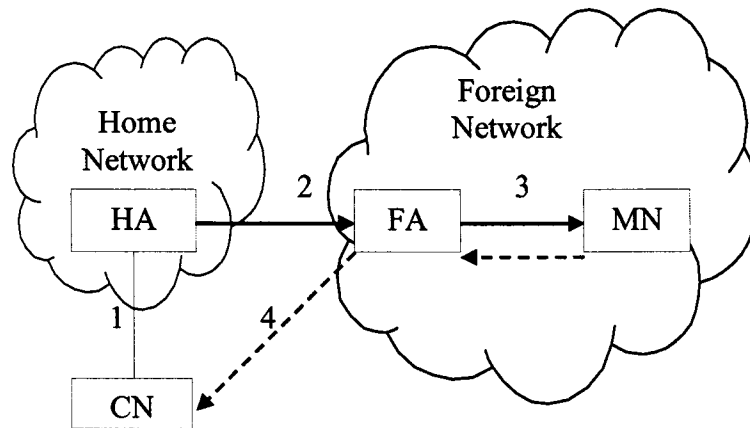
Figure 4: Routing of packets in Mobile IP

1. Packets sent to the MN by the CN (using fixed IP address) arrive at the Home Network.

2. The HA intercepts these packets, encapsulates them (to address them to the care-of-address) and tunnels them to the care-of-address maintained at the FA.

3. These packets arrive at the FA and are then decapsulated i.e. FA extracts the original data packet. Then, the decapsulated packet is sent to the MN.

4. The packets sent by the MN to the CN are directly sent without reaching the home network. MN knows the CN's address from the source address field of the packet received from CN. Thus, it can send the packets directly to CN using the address of CN.

2.4.2 Micromobility

Several problems appear when applying Mobile IP for micromobility i.e. movement between multiple sub networks (i.e. cells) within a single network domain[1]. One problem is triangle routing, where packets addressed to the mobile node are first routed to the home agent and then to the foreign network even if a more efficient route exists between the correspondent (data sender) node and the mobile node. Another problem exists because the mobile node has to register its care-of-address with its home agent every time it moves from one foreign network[2] to another. This results in a lot of control overhead under frequent mobility. Moreover, packet loss also occurs during the handoff, i.e. moving from one network to another, as the mobile node does not receive data until after its care-of-address is registered with the home agent. Thus, Mobile IP tunnelling mechanism introduces network overhead in terms of increased delay and lots of packet loss, which is not suitable for multimedia applications.

To address the frequent mobility problems within a domain, e.g. wide area wireless network, micromobility protocols like Cellular IP [VAL99] and HAWAII [RVS02] were developed. In the HAWAII approach, the network is divided into a hierarchy of domains and each domain in turn consists of a group of cells. For each cell there is a base station. Figure 5 shows a micromobility domain. The gateway in the domain is called the domain root router. When the mobile node first enters the foreign domain, the new care-of-address is registered with the home agent. As long as the mobile node is moving within the domain, the home agent is unaware of this mobility. The care-of-address also remains unchanged while moving within the domain. Messages are sent to the domain root router, which forwards the destined packets to the mobile node using dynamically established paths. Whereas in Mobile IP, the care-of-address changes when the mobile node moves from one cell to another.

---

[1] Example of a domain can be a wide area network.

[2] Example of a foreign network can be a local area network.

19
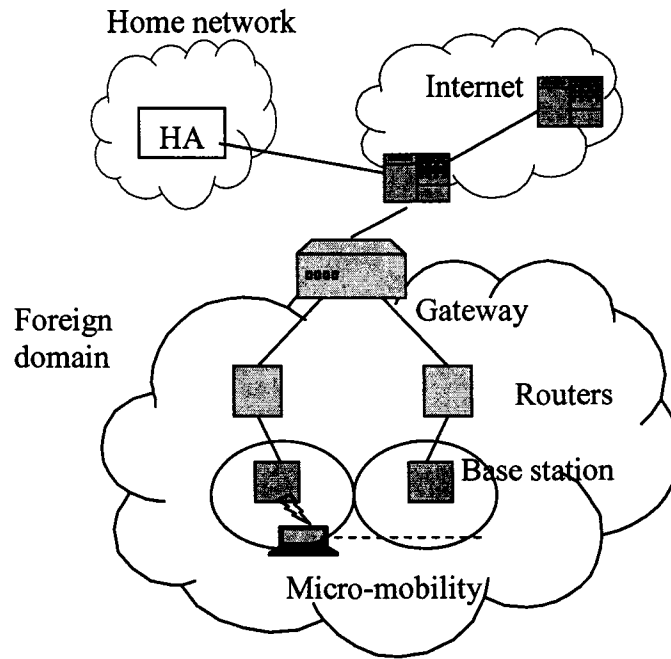
Figure 5: Micromobility Domain

In the HAWAII approach, there are three types of messages for path setup: powerup, update, and refresh. When a mobile node enters a domain, it first sends a powerup message. This message helps in establishing host-specific routes for that mobile node in the domain root router and in the intermediate routers. During powerup, the paths have to be setup and this is achieved by path update messages. Figure 6 shows the flow of path setup messages. To setup a path, the mobile node first sends an update message to its current base station by setting the destination field to be the domain root router. After the base station receives this message, it adds an entry for the mobile node by setting the outgoing interface and forwards it to the next hop router, Router 1. Router 1 performs the same operation and forwards it to the domain root router. Then, the domain root router adds an entry for the mobile node and sends an acknowledgement (ACK) back to the mobile node. The packets are sent to the mobile node using this path.

When, the mobile node moves to a new base station, it sends a path setup message to the old base station. The old base station performs a routing table lookup for the new base station and determines the interface and the next hop router. Then it adds the entry for the mobile node and forwards message to next hop router and so on. After it reaches the domain root router, it adds forwarding entries that result in new packets being

20

diverted to the mobile node at the new base station and forwards the message to the new base station. Then, the new base station adds the forwarding entry and sends an ACK to the mobile node. The path state maintained in routers is soft state. The mobile node sends periodic path refresh messages to the current base station to update forwarding entries. If the base station doesn't receive the refresh messages, the entries will be removed. The messages are again forwarded to the domain root router by base station and intermediate routers.
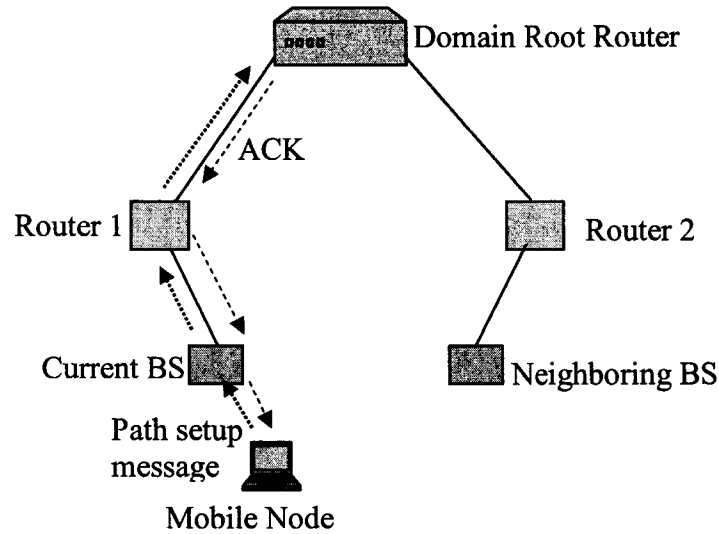
Figure 6: Flow of Path setup messages

Thus, the HAWAII approach, which is a domain-based approach that supports mobility in wide area wireless networks, helps in reducing service disruption during handoffs compared to Mobile IP. It enhances scalability by reducing the control messages sent to the home agent while the node is moving within the domain. This improves the performance of real-time multimedia applications within a wide area domain when compared to the Mobile IP scheme. However, because of path establishments during the process of handoff and because of wireless link characteristics like low bandwidth, high bit-error rate, and signal propagation effects, significant packet loss can still occur.

21

2.5 Comparison of SGWAS and Related Work

In the past few years, some work has been done for improving the QoS for real-time multimedia applications over wireless networks. This subsection explains some of the previous work and compares it with our scheme.

In [YY00], Youngseok et al proposed the Gateway-based Rate Control Algorithm (GRCA) for solving the congestion problem over wireless links for RTP-based applications. The GRCA focuses mainly on providing fast rate adaptation and fair sharing of the link bandwidth among all the RTP flows. This algorithm is implemented at the gateway, which lies at the intersection of the wired and wireless network because this algorithm deals with congestion in the wireless link only. The gateway or a base station acts as a RTP mixer [see Appendix A] and receives the RTCP receiver reports (RR) from the mobile node (receiver). Then, it performs rate control based on the feedback information received from the RTCP RRs sent by the mobile node. The mobile node (receiver) calculates the smoothed Inter-Packet Gap (IPG) value whenever it receives an RTP data packet and reports this value in the profile-specific extensions field of RTCP RRs. Smoothed IPG value for the ith received RTP packet is computed using the following equation:

$$\text{Smoothed\_IPG}_i = \alpha \, . \, \text{Smoothed\_IPG}_{i-1} + (1 - \alpha). \, \text{Sample\_IPG}, \, (0 <= \alpha <= 1)$$

Sample_IPG is the inter-arrival time between (i-1) and (i) RTP packet and Smoothed_IPG$_{i-1}$ is the previous smoothed IPG. This equation uses the exponential weighted average function to calculate the smoothed IPG. This smoothed IPG value represents the current network state. When the gateway receives an RTCP RR, it compares the smoothed IPG value with the congestion threshold. If the value is more than the congestion threshold, it decreases its RTP packet sending rate multiplicatively and tries to recover from the congested state. But, if the smoothed IPG value is less than the congestion threshold, it will increase its RTP sending rate additively until it reaches the maximum bandwidth for the RTP session. To handle handoffs and frequent session creations, the RTCP at the mobile node (receiver) is modified to send RTCP RRs more often when an event, such as handoff occurs. Thus, using the feedback reports sent on

22

occurrence of an event, the sender can adjust its rate more frequently just after an event occurs.

This algorithm focuses mainly on packet loss due to local wireless congestion but does not consider other wireless link problems like signal attenuation or obstruction. But our scheme (SGWAS) identifies the main reason of performance degradation like local wireless link congestion, signal attenuation or obstruction, handoff, etc... based on the information obtained from RFID sensors. In order to consider handoffs during simulation, GRCA adds and drops RTP sessions [see Appendix A]. This way of considering handoffs is vague. During handoff, it is not necessary that a mobile node joins a new session or drops from a session. Moreover, a mobile node can drop from a session even if it is not moving in the handoff region. But, in our SGWAS simulation (see subsection 5.3.1), the mobile node moves from the range of one base station to another during handoff. Also, SGWAS identifies the reason of high packet loss during handoff. Apart from this, our scheme identifies also the reason of packet loss if congestion occurs in the wired region. In our scheme, the base station present at the wired/wireless intersection intercepts the RTP data packets and uses packet sequence number to identify the packet loss in the wired region before the packets are forwarded to the wireless cell.

GRCA uses the smoothed IPG value reported in RTCP RRs to determine the current network state and these RRs are sent to the gateway. Whereas, our scheme uses the fraction of packet loss sent in RTCP RRs to determine the current network state. We believe that packet loss is more accurate than the estimated smoothed IPG. In our scheme, RTCP RRs are sent to the sink and the sink determines the main reason of packet loss. Furthermore, in GRCA, the mobile host and the gateway use Mobile IP to handle IP-mobility. Whereas, in our scheme, we use the HAWAII micromobility protocol to handle mobility because Mobile IP provides minimum support for QoS.

Yoshimura et al [YO02] proposed a QoS control architecture for mobile multimedia streaming that uses RTP monitoring agent to report the QoS information about data transmission to the sender. The monitoring agent lies at the intersection of wired/wireless network. This architecture distinguishes between wireless link bit errors and wired network congestion so that the data sender can perform appropriate QoS

23

control based on received feedback information. The feedback information regarding the current network state is provided to the sender by the RTP monitoring agent. In other words, the RTP monitoring agent sends the feedback reports to the sender indicating if there is congestion in the wired network. If the reports received from the monitoring agent report high packet loss, then the sender performs rate adaptation to alleviate the congestion in the wired network. But, the sender receives also the feedback reports from the mobile node. Then, the sender compares the reports received from the monitoring agent and those received from the mobile node and estimates the packet loss due to wireless link bit errors (P_{radio}) using the following equation:

$$P_{radio} = (P_{client} - P_{agent}) / (1 - P_{agent})$$

Where P_{client} is the packet loss reported by the mobile node and P_{agent} is the packet loss reported by the RTP monitoring agent. To handle the problem of wireless link bit errors, two alternative ways were proposed to make the data flows more robust against packet loss. One way is to change the encoding of the data flows. For example, in MPEG the interval of I-frames can be altered to change the encoding of video flows. Another alternative way is that the sender can increase the transmission frequency of Forward Error Control (FEC) packets that helps in increasing the robustness of the data flows against packet loss. For example, when a FEC packet is generated from N data packets, the FEC packet can recover at least one lost packet as long as N-1 data packets are correctly received.

This approach distinguishes only between wireless link bit errors and wired network congestion but doesn't consider other wireless link problems like handoff. The feedback reports are sent to the sender by both monitoring agent and the mobile node and this helps in differentiating between the wired losses and wireless link bit errors. Whereas, in our scheme we modified the RTCP to send the feedback reports to the sink. The sink receives also messages from RFID reader devices scattered in the cell and deduces the location of the mobile node. Thus, the sink can identify the main reason of packet loss like signal obstruction or attenuation, handoff, local wireless congestion etc... We identify also if the packet loss is due to the congestion in the wired network. In this approach, always the sender adapts the rate of the data transmission even if high packet

24

loss is due to bit error rate at the wireless cell. In case of multicast, if a participant in one cell reports high packet loss, the sender decreases the transmission rate to alleviate the congestion for that participant. But this might affect other participants of the same multicast session, present in a different cell, who are not currently experiencing high packet loss. However, in SGWAS, if high packet loss is due to wireless link congestion, the sender does not adapt. The base station of the cell reduces only the forwarding rate of the RTP flow incurring high packet loss. Thus, it doesn't decrease the rate of the RTP flow, sent to other participants of the same session, present in another cell.

In [CY02], an enhanced RTP monitoring agent, called streaming agent is proposed to improve the quality of the streaming media and the adaptiveness of the media server (data sender). The streaming agent lies also at the intersection of the wired/wireless network and sends timely feedback reports and statistical feedback reports to the sender. The timely feedback reports are positive/negative acknowledgements (ACKs, NAKs) that tell the sender which packets have or have not arrived correctly and on-time at the streaming agent. The statistical feedback reports are the RTCP RRs that contain statistical information like packet loss rate and jitter. These statistical feedback reports are sent to the sender by the streaming agent and the mobile node. By comparing the reports sent by the streaming agent and the mobile node, the sender can determine whether the packet loss is due to wired network congestion or wireless link problems. In contrast to these statistical feedback reports, timely feedback reports are sent more frequently and contain packet acknowledgements. These timely feedback reports sent by the streaming agent are useful when wired network is congested because they report packet drops using NAKs more quickly. Then, the sender performs adaptation by changing the encoding of the data flows to alleviate congestion in the wired network.

In this approach, the timely feedback reports sent by the streaming agent can help only in wired network congestion control and cannot handle wireless network congestion. Even though it uses statistical feedback reports to identify wireless losses, it still cannot identify the reason of packet loss in case of handoff. Whereas, our scheme uses RFID devices to help detect the main reason packet loss, i.e. handoff, signal attenuation or obstruction, or local wireless congestion. In this approach, the sender always adapts to

25

alleviate congestion in the wireless network. In case of multicast, if rate adaptation is performed to decrease the packet loss incurred by a participant present in a wireless cell, then other participants present in other wireless cells get affected. Our scheme handles this problem, by performing rate adaptation at the base station instead of the sender, only in case of local wireless congestion. The base station decreases the forwarding rate of the flow that is incurring high packet loss. Thus, the rate of the RTP flow, sent to other participants of same session present in other cell, doesn't decrease.

Brown et al [BS96] proposed data bandwidth reduction techniques to adapt real-time multimedia applications in a wireless network. Here, the RTP data bandwidth reduction is accomplished by the gateway, present at the border of the wired/wireless network. The gateway acts like an RTP mixer [see Appendix A] and intercepts the RTP data packets and recodes them to a lower rate. It discards also the data packets. For example, in MPEG-1, the gateway might discard P or B frames and keep the I frames intact. In this approach, the gateway reduces also the bandwidth assigned for control RTCP reports because the control rate may overload the wireless link in case of multicast.

This algorithm focuses only on reducing the data and control bandwidth to provide good QoS but doesn't consider the handoff case. Furthermore, reducing data and control bandwidth during handoff or signal attenuation does not help improve the quality of the transmission. Our scheme uses RFID sensors to detect the problems like handoff, signal attenuation, and obstruction. Rate control is performed only when the quality of the transmission degrades due to congestion.

2.6 Summary

In this chapter, we explained different technologies and protocols related to the real-time multimedia delivery over the wireless networks. Our proposed scheme (SGWAS) uses RTP/RTCP protocols and wireless RFID devices in a micromobility domain to enhance QoS of real-time multimedia applications transmitted over the Internet.

26

This chapter discusses also the related work in context of improving the QoS of multimedia applications over the wireless networks. The main objective of our scheme (SGWAS) is to identify the main reason of packet loss i.e., handoff, signal attenuation, congestion in wireless link or in wired network and also perform proper QoS control to improve the quality of the real-time multimedia transmission. This scheme uses the information obtained from RFID sensors to help detect the main reason of packet loss. To the best of our knowledge, it is the first time to use RFID sensors to improve the QoS for real-time multimedia transmission.

27

CHAPTER III

SENSOR GUIDED WIRELESS ADAPTATION SCHEME (SGWAS)

This chapter explains our scheme in detail. It describes the problems to be solved by our scheme, its design, and some important concepts related to it.

3.1 Overview of SGWAS

Sensor Guided Wireless Adaptation Scheme (SGWAS) works in a micromobility domain and helps detect the main reasons of packet loss incurred by the mobile device (e.g. car, laptop, mobile phone, PDA, etc...) in the wireless cell. Determining the reason for packet loss relies on the information obtained from the wireless sensors, specifically, RFID tags and readers. The RFID devices help detect the location of the mobile node within the cell. If packet loss is due to the low bandwidth of the wireless link that can cause local wireless link congestion, then transmission rate adaptation is performed in the cell. If packet loss is due to mobility or signal propagation effects like attenuation or obstruction, then the mobile node is informed about the reason for its currently experienced packet loss or the base station is informed to change its transmission to improve the quality of transmission. Rate adaptation is not performed during handoff or signal attenuation. Thus, we use additional information from wireless sensors to guide adaptation and to detect the reasons of packet loss.

SGWAS works in a micromobility domain using the HAWAII approach [RVS02] as shown in figure 7. In this figure, there is a domain, which consists of two cells. Each cell has a Base Station (BS) that is connected to an intermediate router to the Gateway of the domain (Domain Root Router) that connects to the rest of the Internet. The Sender present in a different domain sends RTP data to the mobile node. Mobile node receives the RTP data via the BS of the cell they are currently located in. Stationary Radio Frequency ID (RFID) reader devices that read RFID tags are located on light poles that are scattered in the cell covered by the BS of this cell. These RFID reader devices operate using the energy emitted from the light poles and have no energy constraints. Weather

28

sensors are also placed in each cell to sense the weather conditions. All these sensors together form a WSN that covers the range of base station.
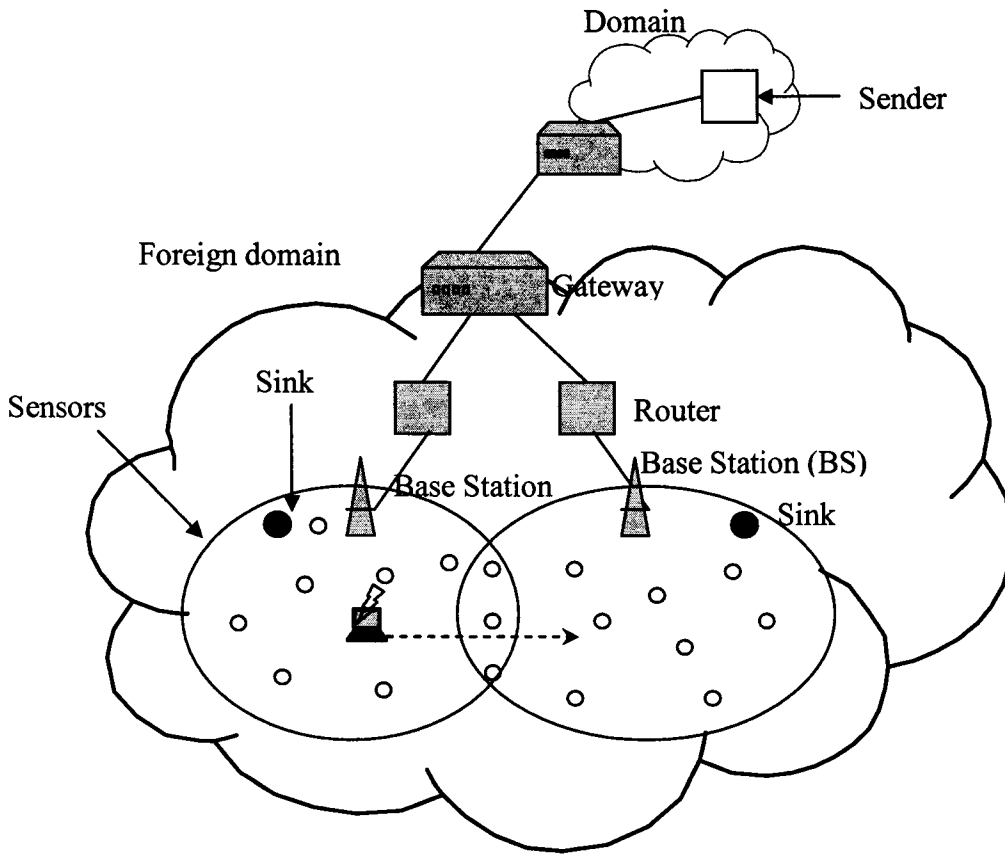
Figure 7: Sensor Guided Wireless Adaptation Scheme in a micromobility domain

In this scheme, we assume that sender is present in the wired region and the base stations are stationary. We assume also that there is one sink for each wireless cell covered by a base station (BS). The sink has an IP address [ZK03] and a dual protocol stack. It communicates with the sensors, the BS, and the mobile nodes in the cell. It also knows the location of the stationary RFID devices located on the light poles. It receives data from the stationary sensors as well as RTCP reports from the mobile nodes within the cell. In SGWAS, we modified RTP/RTCP where the mobile node sends (unicasts) RTCP RR feedback reports periodically to the sink. We have also added some RTCP application specific messages used in communication between several entities. We use the fraction of packet loss sent in the RTCP RR as the main indicator of the QoS of the data transmission incurred in the current interval. This packet loss rate is calculated by

29

the receiver and sent to the sink. It indicates the recent quality of the data received by the receiver. If the loss rate is large, then the quality is bad, and vice versa.

3.2 Description of SGWAS

A mobile device, e.g. car, laptop, mobile phone, PDA, that is a participant in a RTP session receives RTP audio/video data from the data sender. The mobile node sends (unicasts) periodically RTCP Receiver feedback Reports (RRs) to the sink. These RRs include fraction of packet loss incurred in the current interval. In a wired network, packet loss was used to detect if there is congestion in the network. However, when running multimedia applications over wireless networks, packet loss could be attributed to different causes other than congestion. That is to say, packet loss could be due to low bandwidth of the wireless link, handoff, signal propagation effects, e.g. attenuation, or obstruction. So, if there is significant packet loss reported in the most recent RR feedback received by the sink, then this reported packet loss could be due to factors other than congestion.

Determining the reason of packet loss relies on information obtained from wireless sensors, specifically RFID devices. These RFID devices help detect the location of the mobile node within the cell. We assume a RFID tag is attached to each mobile node. The RFID tags are used to store information like identity of an item or a vehicle, location, good in transit, etc... In our scheme, the MAC address [Appendix A] of the mobile node is stored on the RFID tag [KDJ04]. MAC addresses of the mobile nodes are unique. Stationary RFID reader devices with antennas, placed on the light poles scattered in the cell, broadcast beacon messages periodically that can reach any mobile node in their vicinity and within their range. Each RFID reader has a unique ID. The RFID tag attached to a mobile node in the vicinity of RFID reader(s) receives the beacon messages and replies with its address. Note that the address of the RFID tag is the same as the MAC address of the mobile node. The stationary RFID devices send the reply to the sink along with their unique IDs.

30
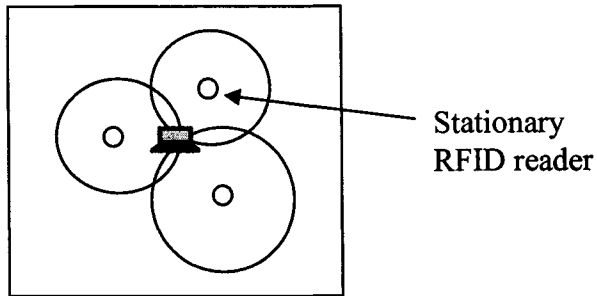
Figure 8: Position Computation of mobile node

The sink receives the periodic RR feedback messages from the mobile node, which includes its IP address. The MAC address can be obtained from the IP address. The sink receives also the messages from the stationary RFID devices carrying the MAC address of the mobile node that is moving within their range. It knows the location of these stationary RFID devices. By matching the data sent by the RFID devices and the MAC address of the mobile node sending the RR, it will be able to detect the location of this specific mobile node and thus infers the reason for packet loss, as explained below.

Any of the stationary RFID devices detecting the mobile node within its range, will calculate the round trip time starting from the time it sends the beacon message that triggered the reply from the mobile node to the actual time of arrival of the reply. The RFID device sends the computed round trip time to the sink along with the MAC address of the mobile node. Consequently, the sink can estimate the distance between the RFID device and the mobile node. If there are three or more RFID devices, which inform the sink that they detected the mobile node at approximately the same time, the sink can pin point the location of the mobile node using a localization algorithm as illustrated in figure 8 [LR05]. However, if the number of RFID devices detecting the mobile node is less than three, then the sink can estimate approximately the location of the mobile node.

3.2.1 Problem identification and actions taken

The sink has a geographical map of the area covered by the base station. It can infer if the packet loss is due to local wireless link congestion, signal propagation effects, or handoff, as follows:

31

- If the RR feedback shows significant packet loss but the signal path was obstructed by an obstacle such as a mountain or a cement building, then the sink will know that packet loss occurred because of the signal obstruction and not because of congestion. Obviously, obstacles, e.g. mountains and high buildings, are stationary. It is possible to use spatial data mining techniques [RT05] to deduce an association between packet loss and locations. This can be done during an initial stage, when the sink collects spatial data and the packet loss associated with that spatial data. Spatial data mining algorithms can then be applied to identify certain areas that suffer from high packet loss due to stationary obstacles.

- If the distance between the BS relaying the RTP data flow and the mobile node receiving this data is large, the cause of packet loss could be due to signal attenuation. Ideally, signal strength is inversely proportional to the square of the distance. Practically, it has been shown [RAP01] that the drop in signal strength can be proportional to the fourth power of the distance.

- If the weather sensor senses a bad weather (e.g. raining, snowing, etc...), then it reports to the sink which then sends a RTCP application specific message to the mobile nodes in its region informing them about the reason of current packet loss which is the bad weather.

- If the mobile node is in the process of handoff, then packet loss is due to its movement from one cell to another. As shown in figure 7, stationary sensor nodes that lie within the intersection of the two cells can detect that the mobile node is currently located in the handoff region. These sensor nodes send to the sink the information required to identify the location of the mobile node. Then, the sink identifies the location of the mobile node and infers that the mobile node is in the process of handoff.

- If none of the previous conditions exist and current packet loss is not due to congestion in the wired network, as will be explained later, then the sink infers that

32

current packet loss is due to low bandwidth of the wireless link that result in local wireless link congestion.

After detecting the main reason of packet loss, the sink informs the BS to take the appropriate action, as follows:

• If the current packet loss is due to local congestion in the wireless link, then the BS, which is RTP-aware, can decrease the transmission rate of the RTP flow that is received by the mobile node to help alleviate congestion. Note that if a BS adjusts its transmission rate dynamically, the transmission rate of the other base stations will not be affected.

• If packet loss occurs because the distance between the BS and the receiving mobile node is large, then the sink can send to the BS to increase its transmission power or to adjust the directivity or direction of its antenna.

• If packet loss occurs due to handoff, the sink sends an RTCP application specific message to the mobile node to inform it that the current packet loss experienced by the mobile node is due to handoff.

• If packet loss occurs because the signal to the mobile node is obstructed by an obstacle, then the sink searches for another node, if it exists, that is a participant in the same RTP session and that doesn't suffer from high packet loss. The sink sends to this node an application specific message to forward the RTP data packets it receives to the mobile node experiencing this problem. Note that this relaying node has to be in a location free of obstacles and not in the handoff region.

Thus, in case of packet loss due to handoff or signal propagation affects like attenuation or obstruction, rate adaptation is not performed and the quality of the real-time multimedia flow delivered to other receivers in the same session will not be affected.

As mentioned earlier, the mobile nodes send RR feedback messages periodically to the sink. These RRs contain the Synchronization Source (SSRC) of the sender of the

33

RTP flow and the related reception statistics like packet loss rate computed when that RTP flow is received. The RRs contain also a profile-specific extensions field that we use to send the session identification to the sink. The sink stores this information in a table and thus can distinguish between different RTP sessions. The SSRC, which is unique among all participants in a RTP session, is used to distinguish different flows within a session. Using this information, the sink can identify the RTP flow, which is incurring packet loss, and also the mobile node(s) in the cell receiving that flow. The sink tries to locate another node not suffering from significant packet loss and in the same RTP session. This relay node has to be in a location to forward the RTP packets to the mobile node having this type of problems. To determine this, the sink uses again the information stored in the table, i.e. session identification. If it finds such a node, it sends an application-specific message to that node to send the RTP data it receives to the mobile node incurring high packet loss.

- Packet loss might occur also because of congestion in the wired region. To alleviate congestion, rate control mechanisms can be used by the data sender [BT94, BDS96, EH97], assuming the sender is located in the wired network. There is a need to distinguish between network congestion in the wired part and degradation of quality in the wireless link. To solve this problem, the sender is informed about the packet loss only if it is because of congestion in the wired region. The base station present in each cell is RTP-aware and detects the congestion in the wired network. That is to say, the base station forwards the RTP data sent by a data sender to the mobile node(s) in the cell, it can intercept the RTP data packets and detect packet loss. This can be done using the sequence number field in RTP packet header. When the base station detects a high packet loss in a RTP flow, it asks the mobile node to send the RR feedback to the data sender, which can then reduce its transmission rate to alleviate congestion in the wired network.

3.3 Summary

This chapter gives an overview of the SGWAS scheme. Then, it describes the scheme in details, assumptions, problems solved by the scheme, and actions taken.

34

CHAPTER IV

NETWORK SIMULATOR

This chapter gives a brief introduction to the Network Simulator (NS) [GRE00] [FV99], the Wireless model, Wireless Sensor model, and RTP implementation in NS. It explains also the contributed modules of RTP and the Wireless model in NS.

4.1 NS Overview

NS [FV99] is a discrete event simulator for networking research. NS provides support for simulation of various protocols like TCP [POS81], UDP [POS80], different routing techniques, and multicast protocols over wired and wireless networks.

NS is an object-oriented simulator, written in C++, which uses OTcl as the interpreter. The simulator supports two hierarchies, namely, C++ or compiled hierarchy and OTcl or interpreted hierarchy, which are closely related to each other. There is also a one-to-one correspondence between the class in interpreted hierarchy and the one in compiled hierarchy.

NS uses two programming languages, C++ and OTcl. C++ is used for the detailed protocol implementation because it runs fast but takes more time to change. It is basically used to create packet headers, manipulate bytes, and implement detailed algorithms.

On the other hand, OTcl is used for simulation configuration e.g., setup topology and change simulation parameters, because it is easy change and runs slower than C++. Tclcl provides links to make objects and variables appear on both languages.

4.2 Wireless Model in NS

The basic wireless model in NS was developed by the CMU/Monarch group [CMU01]. This model includes the mobile node, routing mechanisms, and network components that are used to construct the network stack for a mobile node.

The mobile node is the basic node object with functionalities like movement, ability to transmit and receive on a channel. This helps in creating mobile, wireless

35

simulation environment. The mobile node moves in a three-dimensional topology and has three co-ordinates, X, Y and Z whose values change with movement of the mobile node.

The network stack for a mobile node consists of a link layer (LL), an Address Resolution Protocol (ARP) module connected to the LL, an InterFace priority Queue (IFQ), a media access control layer (MAC), a network interface (netIF), all connected to the channel.

The link layer for the mobile node has an ARP module connected to it for converting IP address to the MAC addresses. IFQ gives priority to routing protocol packets, inserting them at the head of the queue. It also supports running a filter over all packets in the queue and removes those with a specified destination address. Coming to the MAC layer, the 802.11 MAC protocol and time division multiple access (TDMA) MAC are implemented in the wireless model. The network interface serves as a hardware interface, which is used by mobile node to access the channel.

Four different types of routing methods are defined in the wireless model in NS:

- Destination-Sequenced Distance Vector (DSDV)

- Dynamic Source Routing (DSR)

- Temporally-Ordered Routing Algorithm (TORA)

- Ad Hoc On Demand Vector (AODV)

To perform simulations using both wired and wireless nodes, certain extensions have been added to the wireless model. This extension is called wired-cum-wireless. In wired-cum-wireless scenarios, data is exchanged between wired and wireless nodes. To exchange data, both the wired and wireless domains have to be connected. To do this, a Base Station (BS) node was created that acts like a gateway between wired and wireless domain. It delivers packets into and out of the wireless domain. To forward the packets to the mobile node, hierarchical routing is required. In this routing, each wireless domain along with its base station is assigned a unique domain address. All packets destined to a wireless node would reach the base station attached to the domain of that wireless node, which would eventually hand the packets over to the destination (mobile node). Mobile nodes route packets, destined to outside their (wireless) domain, to their base station node.

36

4.3 Contributed Modules to the Wireless Model

Other than the routing mechanisms mentioned above, NO Ad-hoc Routing Agent (NOAH) [WID00] was contributed to NS wireless model. NOAH is a wireless routing agent only supports direct communication between base stations and mobile nodes.

The Columbia IP Micro-Mobility Suite (CIMS) [CG01] has been added as an extension to the wireless model. This module supports the implementation of the micro mobility protocols like Cellular IP, HAWAII, and Hierarchical Mobile IP. CIMS uses NOAH as the routing agent for routing data packets between the base station and the mobile nodes.

4.4 Sensor Simulation in NS

NS supports the simulation of sensors and also provides support for simulation of routing protocols like flooding and directed diffusion (see section 2.3.2). Flooding is old technique that can be used for routing in sensor networks. We use flooding protocol for routing of data packets between the sensors and the sink in our SGWAS scheme. We have also added additional functionality messages to this flooding protocol for sending requests and responses between sensors and sink.

4.5 RTP Simulation in NS

The RTP implementation in NS consists of different classes for RTPAgent, RTCPAgent and RTPSession.

RTPAgent performs the functionalities of RTP data protocol such as sending RTP packets, Sender Reports. RTCPAgent performs the functionalities of RTP Control Protocol (RTCP) such as sending control information e.g. RTCP Receiver Reports (RRs). The class RTPSession creates the RTP session and also determines the interval of sending RRs from the same participant.

But the RTP/RTCP implementation in NS is incomplete, as it does not provide any implementation for RTCP reports. We used contributed code by El-Marakby [EL01], which provides functionalities like RTCP report packet structure, RTCP SRs and RTCP RRs. In our scheme, we modified RTP/RTCP to send the RTCP RRs unicast to the sink.

37

We even added this functionality to NS. Thus, these functionalities are necessary for our scheme and also help in enhancing the functionality of RTP.

4.6 Summary

Network Simulator provides support for simulation of wired and wireless networks, sensor networks, and also RTP/RTCP for running real-time multimedia applications. We used these functionalities to simulate our scheme. We have also added some additional features to RTP module and sensors module of NS thus making NS suitable to simulate our scheme.

38

CHAPTER V

SIMULATIONS

This section explains the simulation topology and parameters, implementation details, different experiments, and results.

5.1 Simulation Environment

We performed some experiments to evaluate our scheme. We used NS-2 [FV99], a network simulator tool, to simulate a real-time multimedia application that uses RTP/RTCP and works using the HAWAII micromobility approach. The Simulation topology is shown in Figure 9. Our real-time multimedia application runs in source S1. It sends data packets of size 210 bytes each at a rate of 256Kbps to the mobile node MN2. The mobile nodes, MN1 and MN2, are placed in the range of base station BS1, while MN3 is in the range of base station BS2.
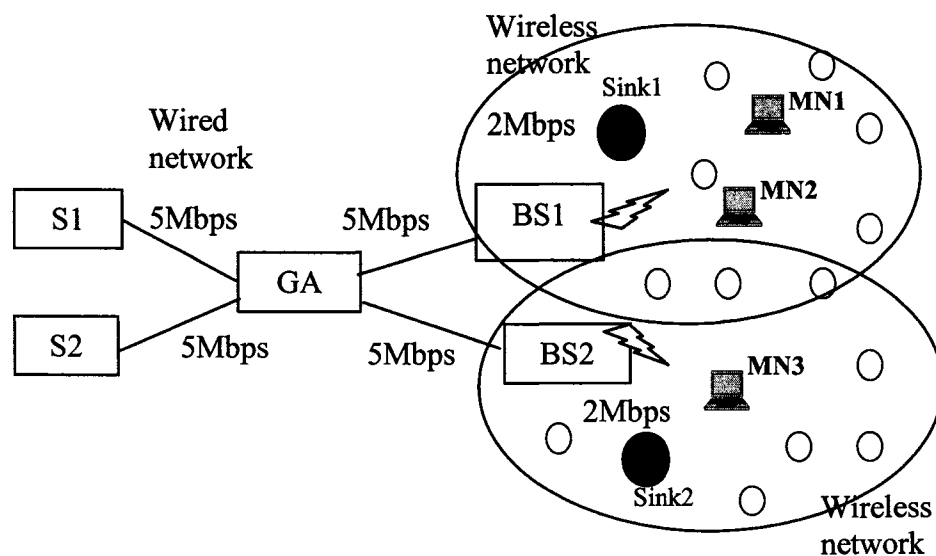

Figure 9: Simulation Topology

Sink1 is placed in the region of BS1, while sink2 is in the region of BS2. The coverage area of each base station is set to 250m. The bandwidth of each individual link between wired nodes S1, GA and S2, GA is set to 5Mbps. The bandwidth of each link

39

between GA, BS1 and GA, BS2 is also set to 5Mbps. The wireless link bandwidth (bottleneck link) between each base station and the mobile nodes in its cell is set to 2Mbps. All the nodes in the simulation are placed in a 600x600 field.

Initially, at 1.2s S1 starts sending RTP data. S1 sends interfering UDP flows to MN1 at 2.2s and S2 sends UDP traffic to MN3 at 2.4s. Both the UDP flows stop at 15s. Once the node MN2 receives the data, it sends RTCP RRs to sink1, which contains the packet loss rate incurred in the current interval. To identify the location of a mobile node, sensors are placed in the range of each base station. We placed 10 sensors in the region covered by each base station. Sensors identify the mobile node moving in their range and send the information required to identify the location of that mobile node to the sink. We used flooding protocol for routing of data between the sensors and the sink. Using the information sent by the sensors, the sink identifies the current location of the mobile node. Then, the sink checks the packet loss rate of the mobile node and based on its location, the sink identifies the reason of high packet loss e.g. handoff, signal attenuation or local wireless congestion.

If high packet loss is due to handoff, then the sink sends an application specific message to the mobile node to inform it that the packet loss is due to handoff. If high packet loss is due to signal attenuation, i.e. increase in the distance between the base station and mobile node, then the sink informs the base station to increase its transmission power or change the direction of the antenna. If high packet loss is due to local wireless congestion, then the sink sends an application specific message to the base station, which performs rate adaptation to improve the QoS of the transmission. If the packet loss is due to wired congestion, then the base station sends a message to the mobile node asking it to send the RRs to the sender. Then, the sender performs rate adaptation to improve the QoS of the transmission.

We performed several simulations to detect the main reason of high packet loss in case of handoff and signal attenuation. We have also conducted experiments for testing the rate adaptation performed by the base station during local wireless link congestion and adaptation performed by the sender during congestion in wired network. In the next subsections, we will describe the implementation details and different simulation experiments.

40

5.2 Implementation

We used the Network Simulator NS-2 (version 2.28) [FV99] installed on Windows XP operating system for the implementation of our scheme. NS uses two programming languages, C++ and Tcl. We used C++ to implement new agents and functions used in the simulation. Tcl is used for setting up the topology and configuring the simulation parameters. In the remaining part of this section, we will describe the various steps involved in our implementation.

5.2.1 Configuring the network topology

In the present work, wired nodes, wireless nodes, and wireless sensors were created. First, the wired nodes were configured and then were connected to each other by creating links. Each link between the wired nodes is configured by assigning parameters like bandwidth and delay. Coming to wireless nodes, each node is configured by assigning different parameters like channel type, link layer type, interface queue type and length, MAC type and the routing protocol. To manage the mobility issues of the nodes, micromobility protocol is used in our simulations. We added the micromobility functionality to NS-2 using Columbia IP Micro-Mobility Suite (CIMS) [CG01]. But this approach requires NOAH routing agent for communicating data packets between the mobile nodes. So we added NOAH routing agent to NS-2 using the patch from [WID00].

Then, the wireless sensors were configured. In the simulation, each sensor node is configured with the parameters: link layer type, range, and frequency. Flooding protocol is used as the routing protocol for the sensor nodes. We added two messages, HELLO and DATA_MN to this routing protocol. The HELLO message is broadcasted to the sensors by the sink. When the sensors receive this message, they check if that node is the sink and stores the address of the sink. The other message, DATA_MN, is sent by the sensors when sending data packets to the sink. This message is sent when the sensors sense the mobile node is in their range. Sensors broadcast this message to their neighbouring sensor nodes in the local cell who then forward to their neighbours. This process is repeated until the message reaches the sink.

41

5.2.2 Sending RTCP RRs and location information of the mobile node to the sink

As mentioned in the subsection 5.1, when the mobile node receives RTP data, it sends RTCP RRs to the sink, which contain the packet loss rate incurred by the mobile node in the current interval as well as the Synchronization Source (SSRC) of the data sender of the RTP flow. In our simulations, we modified the RTP/RTCP to send the RRs unicast to the sink. Moreover, we added session identification (sid) (see subsection 2.2.1) to the profile-specific extension field of the RR to identify the RTP session. We created a table called Pktloss to store the session identification, SSRC of the RTP flow, and packet loss rate along with the mobile node ID (MAC address). This table is updated when a new RR arrives at the sink, to keep track of the most current packet loss of each RTP flow in the RTP session.

At the same time, the RFID sensors, placed in the cell, send the information required to identify the location of the mobile node to the sink. To implement this module, we created a class RTPMonitor and added a function called send_mn_packet() to send the location information of the mobile node. When the RFID sensor, senses a mobile node in its vicinity, it calls the function send_mn_packet() and broadcasts a message to other sensors. This function sends a message of type DATA_MN (see subsection 5.2.1) which includes the location co-ordinates, i.e. X and Y co-ordinates of the mobile node. When another sensor, receives the message of type DATA_MN, it forwards it to another sensor node until it arrives at the sink. We created another table called location at the sink to store the X and Y co-ordinates of the mobile node along with the mobile node ID (MAC address). This table is updated on receiving a DATA_MN message from sensors to keep track of the most recent location of the mobile node.

5.2.3 Determining the reason of high packet loss

After the sink receives the RRs from the mobile node and identifies the location of the mobile node, it checks the packet loss rate and the location information to determine the reason of high packet loss, e.g. handoff, signal attenuation or local wireless link congestion. We added another function recv_rr() for the checking. This function uses

42

the packet loss rates stored in the table called Pktloss and the location information stored in the table called location for this checking.

We set the packet loss threshold to 0.15, which is a tolerable limit by human beings for audio flows [KR03]. For comparing the location information, we need to know the handoff region co-ordinates. Here the range of base station was set to 250m. Then, we set the values of handoff region co-ordinates, i.e. X and Y co-ordinates as follows: (80, 260), (100, 290), (250, 170) and (220, 140). To determine the reason of high packet loss, the sink compares the current location co-ordinates with the above mentioned handoff region co-ordinates. If the packet loss incurred is greater than the threshold and mobile node is in the handoff region, then the reason for packet loss is handoff.

If the reason of high packet loss is due to signal attenuation, then the sink calculates the distance between the base station and the mobile node and compares it with the range (radius) of the base station. After the sink identifies the location of the mobile node, it uses the X, Y co-ordinates of the mobile node's current location and the X, Y co-ordinates of the base station and calculates the distance between the base station and the mobile node (r) using the following equation:

$$r^2 = (x\text{-}h)^2 + (y\text{-}k)^2$$ (where x, y are the X, Y co-ordinates of the location of the mobile node and h, k are the X, Y co-ordinates of the base station). Then, the sink compares the calculated distance with the radius (range) of the base station. If the distance is approximately close to the base station range or greater than the base station range and the packet loss incurred by the mobile node is greater than the threshold, then the reason of high packet loss incurred is signal attenuation.

If the sink identifies that the mobile node is neither in the handoff location nor far away from the base station, but packet loss is greater than threshold then, the reason for packet loss is local wireless congestion.

In wired/wireless networks, high packet loss might occur also due to congestion in the wired network. In our scheme, the base station present at the intersection of wired/wireless network detects if there is significant packet loss in the wired region. To detect packet loss, we added a function called bs_loss(). This function intercepts the RTP

43

packets sent to the mobile node and uses the sequence number in the RTP header to detect the packet loss.

5.2.4 Taking appropriate action

After the sink determines, the main reason of packet loss, it takes appropriate action described below.

If the high packet loss is due to handoff, the sink sends an application specific message to the mobile node to inform it that the current packet loss occurred because the mobile node is in the handoff region. To send this message, a function sendpkt() is added. This function sends an application specific message to the mobile node that includes the session identification (sid) and the SSRC of the RTP flow, which is currently incurring packet loss. The sid and SSRC are used to identify which flow is incurring packet loss at the mobile node due to handoff.

If the major packet loss is due to local wireless congestion, the sink sends a message to the base station of the cell where mobile node exists. When the base station, which is RTP-aware, receives this message, it performs transmission rate adaptation to alleviate congestion. We added another function rate_adap() to send a message to the base station. This function sends a message, which includes sid and SSRC of the RTP flow, which is currently incurring packet loss. After receiving this message, the base station checks the sid and SSRC of the RTP flow and identifies the flow that is incurring packet loss. It then reduces the transmission rate of that flow.

To perform the rate adaptation, we added a class rateinfo. We implemented the algorithm developed in [EH97] to perform rate adaptation. The following steps summarize the algorithm developed in [EH97].

if (packetLoss > threshold)

       currentRate=max (alpha*currentRate, minRate)

else

       currentRate=min (beta*currentRate, originalRate)

44

If the packet loss incurred is more than the threshold[3], the sending rate is decreased. Note that the rate cannot decrease below the *minRate*. If the packet loss incurred is less than threshold, the sending rate is increased, not to exceed the *originalRate*. The rate is changed dynamically within a limit between the *minRate* and *originalRate*. The *originalRate* is the initial rate used by the data sender of the RTP flow at the beginning of the transmission. The *currentRate* is initially set equal to the *originalRate*. In our experiments, we set the *originalRate* of the RTP flow to 256Kbps, *minRate* to 50Kbps, and threshold to 0.15. The value of alpha is set to 0.9 and the value of beta is set to 1.2.

As mentioned in subsection 2.4, the base station forwards the data sent by the sender to the mobile node. In SGWAS, the base station decreases the rate of transmission to alleviate congestion in the local wireless region. But, the data sender sends the data at the originalRate. So, when the base station decreases its sending rate, packet loss might occur at the base station because the sender is sending data at the originalRate. In order to handle this problem, we created a buffer at the base station to store the packets sent by the sender. Thus, when the base station decreases the sending rate, the packets sent by the sender are stored in the buffer, which are then forwarded to the mobile node.

If high packet loss is due to wired network congestion, then the base station sends a message to the mobile node to inform it to send the RRs to the sender. To send this, we added a function called sendmsg(). This function sends a message called BS_RATE containing the session identification of the RTP flow to the mobile node. After receiving this message, the mobile node sends the RRs to the sender. When the sender receives RRs, it checks the packet loss reported. If the packet loss is greater than threshold, it performs rate adaptation to decrease the packet loss and thus alleviates congestion. The sender uses the adaptive algorithm [EH97] implemented in class rateinfo to perform rate adaptation.

---

[3] The sender could send the packet loss threshold value to the base station in the profile-specific extensions field of RTCP sender report.

<u>5.2.5 Recording data and generating graphs</u>

The final step in implementation is to record the data for the entire simulation and generate the graphs. We recorded the history of packet loss rates, location co-ordinates of the mobile node, and also the sending rates during rate adaptation. Then, we plot the graphs according to the recorded data. These graphs show the packet loss rates of the mobile node during handoff, signal attenuation, and also during rate adaptation. Moreover, the sending rates of the RTP flow during rate adaptation are shown in the graphs.

<u>5.3 Simulation Experiments</u>

This subsection explains the simulation experiments in details. These experiments test and compare SGWAS, which is implemented in a real-time multimedia application, under the following scenarios:

- Handoff
- Local wireless link congestion
- Signal attenuation
- Wired network congestion

<u>5.3.1 Handoff region</u>

In this scenario, at 1.2s, S1 sends RTP data to MN2, which is in the range of BS1. After receiving the data, MN2 sends RTCP RRs to sink1. At the same time, the sensors present in the range of MN2, send the information required to identify the location of MN2 to sink1. Now, sink1 knows the location of MN2 and the packet loss rate incurred by MN2. At 2.2s, S1 sends interfering UDP traffic to MN1 at a high rate (550Kbps). At 2.4s, S2 sends UDP traffic to MN3 at a low rate (64Kbps). Both stop at 15.0s. Initially the packet loss rate of MN2 ranges from 0 to 0.01 when there is no interfering traffic (see Figure 10). The values in Figure 10 show the packet loss reported in different RRs, which are received by the sink, since the beginning of transmission. This figure shows only the handoff problem. It doesn't show the other causes of high packet loss. That is to say, this

46

figure doesn't show what happens if MN2 is experiencing high packet loss due to signal attenuation, local wireless congestion, or congestion in the wired region. The RR received at 2.48s reports 0 packet loss and the RR received at 3.15s reports a very low packet loss (0.01). Then, at 3.48s the packet loss rate increases to 0.196 because of the buffer overflow at BS1 due to interfering traffic sent to MN1 at a rate of 550Kbps. MN1 lies in the range of BS1.
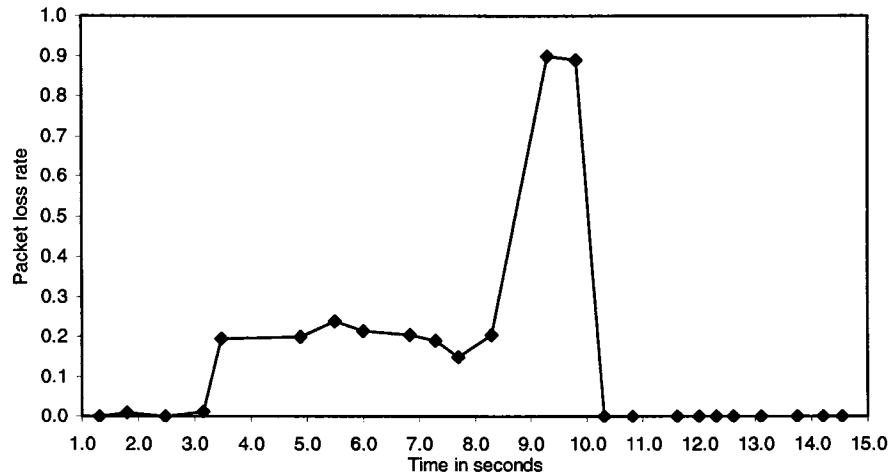
Figure 10: Packet loss rate of the RTP flow versus Time during handoff

Time	Location (x,y)	Packet loss rate
3.48s	150,150	0.196
6.18s	150,150	0.23
9.3s	169,180	0.9
9.8s	177,190	0.89
10.29s	191,213	0
10.8s	197,222	0

Handoff region co-ordinates

Table 1: Packet loss rate and location of the node at sink

After 6s, MN2 starts to move towards BS2 with a speed of 20ms. It reaches the handoff region at 9.3s and its packet loss increases to 0.9. At 9.82s, it leaves the handoff region and moves in the range of BS2. The RR received at 10.3s reports zero packet loss.

47

The packet loss rate of MN2 remains zero for the rest of the simulation because the UDP traffic is being sent at a low rate (64Kbps) from S2 to MN3, which lies in the range of BS2.

Table 1 shows the values of location, i.e. x, y co-ordinates of MN2 along with packet loss experienced by MN2 during handoff. Moreover, it also shows the values before and after the handoff phase. In Table 1, the values of the location of the mobile node at different times 9.3s and 9.8s show the co-ordinates of MN2 when it is in the handoff region. Notice that the packet loss rate of MN2 when moving in the handoff region is high i.e. 0.9 and 0.89. Since the sink knows the handoff region co-ordinates (see subsection 5.2.3), it identifies that the packet loss incurred by MN2 at the locations (169,180) and (177,190) is due to handoff. Then, the sink sends an application specific message to MN2 to inform it that the reason for current high packet loss is handoff.

The first message is received by MN2 at 9.32s. At 9.8s, when the sink receives another RR reporting a high packet loss, it identifies that MN2 is still moving in the handoff region. MN2 receives another message at 9.83s informing it that current high packet loss is due to handoff.

These results show that the sink detects that the reason of high packet loss is due to handoff using the information sent by the sensors and RRs sent by the mobile node. It then sends an application specific message to the mobile node to inform it the reason for the current high packet loss.

5.3.2 Local rate adaptation in the wireless cell

In wireless networks, because of the low bandwidth of the wireless link that can cause congestion in the wireless region, high packet loss occurs. To handle the congestion problem and improve QoS of the transmission, rate adaptation is performed. But, there is a need to differentiate between the case when high packet loss occurs due to local wireless congestion and the case when high packet loss occurs due to handoff or signal attenuation. In this subsection, we present the simulation of SGWAS, which performs local rate adaptation only during wireless link congestion. When the mobile node is in the handoff region, rate adaptation is not performed but the mobile node is

48

informed that reason of current high packet loss is due to handoff. Other works in this area [BS96] [YO02] [CY02] perform rate adaptation during handoff. Moreover, we added an experiment to show what happens if rate adaptation is performed during handoff which we do not do.

In our experiment, at 1.2s, S1 sends RTP data to the mobile node MN2. The interfering UDP flow sent from S1 to MN1 starts at 2.2s and the UDP flow sent from S2 to MN3 starts at 2.4s. Both UDP flows stop at 15s. MN2 sends RTCP RRs to sink1. Sink1 receives also the information required to identify the location of the mobile node from RFID sensors. When sink1 notices packet loss rate is greater than threshold[4] and identifies that MN2 is in the range of BS1 and not in the handoff region and not far away from BS1, it sends an RTCP application specific message to the base station BS1. Then, BS1 performs rate adaptation of the RTP flow experiencing local major packet loss. Figure 11 shows the transmission rate of the RTP flow sent to MN2 versus time and figure 12 shows the packet loss, incurred by the mobile node and reported to the sink in RRs, versus time. Figure 11 and 12 show the rate adaptation performed locally at BS1 in case of local wireless congestion.

In our experiments, the sender S1 sends RTP data at a rate of 256kbps and BS1 forwards data at a rate of 256Kbps. At the very beginning, MN2 reports very low packet loss in the RTP flow. At 3.48s, sink1 receives an RR with loss rate 0.19 (see Figure 12). The packet loss increases because of buffer overflow at BS1 due to the amount of RTP and UDP traffic BS1 is forwarding. Then, sink1 checks the location of MN2. It deduces that the local high packet loss incurred us due to wireless link congestion because MN2 is not in the handoff region and not far away from BS1. Sink1 sends an application specific message to BS1. Then, BS1 reduces its forwarding rate of the RTP flow to 230Kbps (see Figure 11) since the packet loss is greater than threshold (0.15). Then the packet loss rate reduces to 0.123 at 4.89s because of the decreased forwarding rate at BS1. Then, BS1 increases its forwarding rate to 256Kbps, as the packet loss incurred is less than the threshold. At 5.5s, packet loss is reduced further to 0.12. At 6.18s, sink1 notices a packet

---

[4] In our experiments, we set the packet loss threshold to 0.15, which is tolerable by human beings for audio flows [KR03].

49

loss rate of 0.23, which is greater than threshold and sends an application specific message to BS1. Then, BS1 reduces its rate to 230 Kbps. At 7.27s, there is still high packet loss (0.2). Since this is greater than threshold, the sink sends again an application specific message to BS1 and BS1 reduces its forwarding rate of the RTP flow to 207Kbps. The packet loss goes below the threshold at 7.8s and the forwarding rate of the RTP flow is increased to 248Kbps. At 8.43s, the packet loss reported (0.14) is still less than threshold, so the rate is increased to 256Kbps.
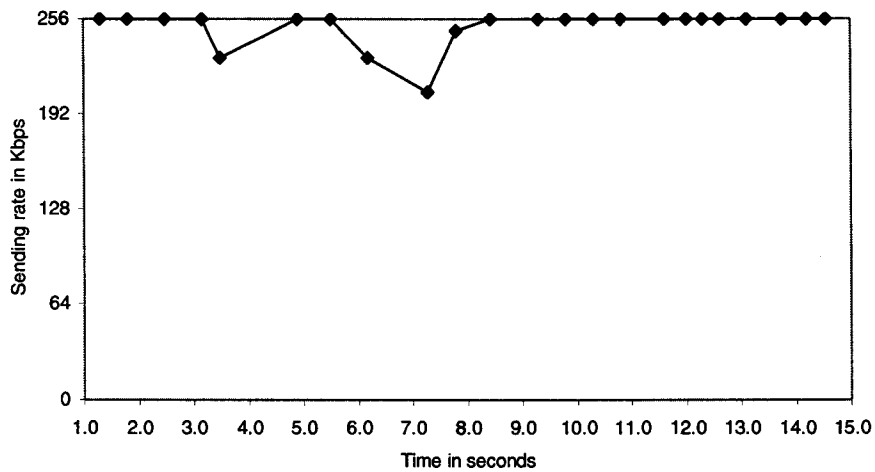

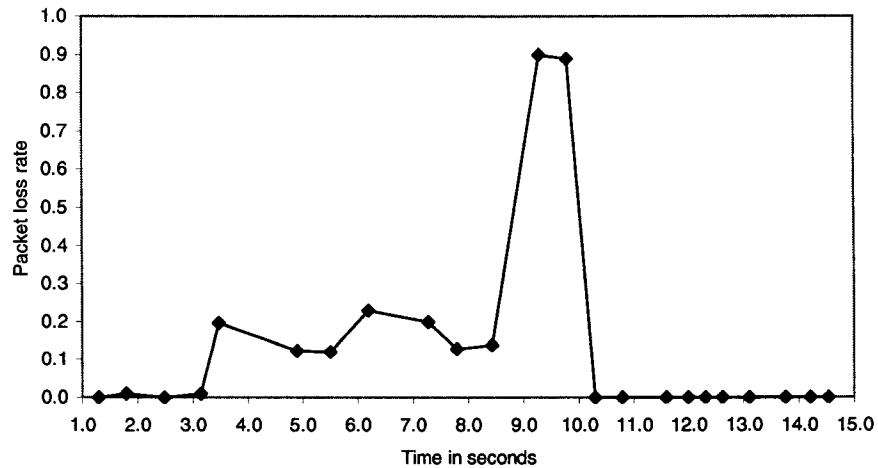**Figure 11: Local rate adaptation versus time in case of wireless link congestion**

Figure 12: Packet loss of the RTP flow versus time in case of local rate adaptation

After 6s, MN2 starts to move towards BS2 with a speed of 20ms. At 9.3s, it reaches the handoff region (see Figure 12). During this time, the sink notices that the

50

packet loss (0.9) incurred by MN2 is high and checks the location of MN2. Since the sink knows the handoff region co-ordinates (see subsection 5.2.3), it deduces that the packet loss is due to handoff and thus sends an application specific message to MN2 informing it that the packet loss is due to handoff. Hence, the base station doesn't perform rate adaptation during the interval, 9.3s to 9.8s. In figure 11, the forwarding rate of the BS1 is 256kbps is same as original rate during handoff because rate adaptation is not performed by BS1.

In the next experiment, we describe the transmission rate adaptation performed during handoff, which is not implemented in SGWAS. Other related works in this area [BS96] [YO02] [CY02] perform rate adaptation during handoff. Figure 13 shows the transmission rate of the RTP flow versus time if rate adaptation is performed during handoff.
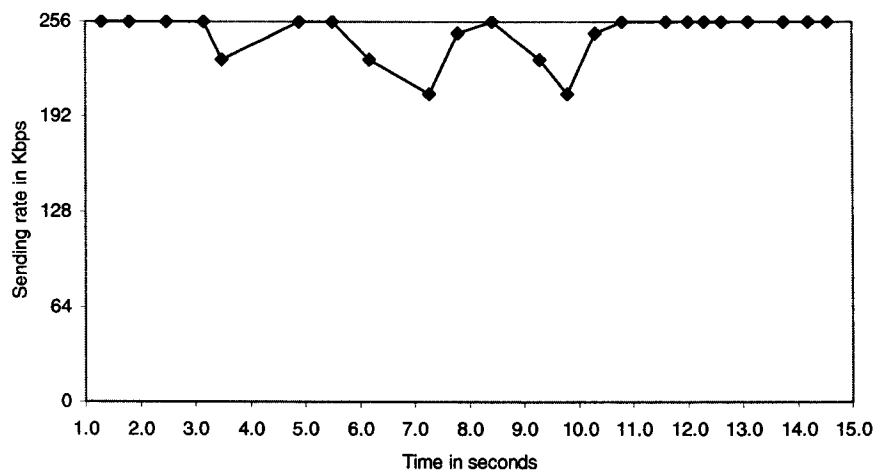
Figure 13: Rate adaptation during handoff (not implemented in SGWAS)

In this scenario, at 6s, MN2 starts to move towards BS2 with a speed of 20ms. At 9.3s, MN2 reaches the handoff region and packet loss rate reported increases to 0.9. The base station thinks that high packet loss occurred because of local congestion in the wireless cell and then reduces the forwarding rate of the RTP flow to 230 Kbps (see Figure 13). The next RR reports high packet loss rate of 0.89 at 9.8s. The base station still thinks that this high packet loss is due to congestion and reduces the forwarding rate of the RTP flow further to 207Kbps. But, actually MN2 is still in the handoff region at 9.8s. At 9.82s, MN2 leaves the handoff region and moves in the range of BS2. At 10.3s, the

51

packet loss rate decreases to zero since MN2 has reached the range of BS2. Thus, we see that decreasing the forwarding rate of RTP flow at 9.3s and 9.8s, when MN2 moves in the handoff region, will not decrease the packet loss in the RTP flow and thus will not improve the quality.

So, from the above simulation, we see that rate adaptation does not improve the QoS during handoff. In case of multicast, if a participant is experiencing high packet loss, then the rate is decreased to alleviate the congestion for this participant. So, if rate adaptation is performed for a mobile node during handoff, the quality of the data flows sent to other participants in the session gets affected. In other words, other participants suffer greatly because one mobile node is in the handoff region. Our scheme (SGWAS) solves this problem by adapting the forwarding rate of the RTP flow that is incurring high packet loss, at the base station only if there is local wireless congestion. In SGWAS, in case of handoff, the sink informs the mobile node that the reason of current high packet loss is handoff (see subsection 5.3.1).

These results show that our scheme (SGWAS) differentiates between the packet loss due to congestion in the wireless link and the packet loss due to handoff. The base station performs rate adaptation only if packet loss is due to local wireless congestion.

5.3.3 Signal attenuation

We conducted simulations to show the case of high packet loss during signal attenuation. In this scenario, we use different ranges for the base stations BS1 and BS2: 250m, 100m, and 40m. This is to test signal attenuation for different ranges. These experiments show that using different base station ranges, the distance between the base station and the mobile node, experiencing high packet loss because of signal attenuation, changes. But, SGWAS could identify the reason of high packet loss during signal attenuation using different ranges for the base station.

In our first experiment, we set the range of the base station to 250m. Initially, MN2 is stationary at location (20,30) and packet loss rate of the RTP flow received by MN2 is 0. At 2.2s, S1 sends interfering UDP traffic to MN1 at a rate of 350Kbps and at

52

2.4s, S2 sends UDP packets to MN3 at a rate of 64Kbps. The total simulation time for this scenario is 25s.

At the beginning, there is no packet loss in the RTP flow received by MN2 because the interfering UDP traffic is sent at low rate (350Kbps) to MN1 which lies in the range of BS1 as node MN2. After 6s, MN2 starts to move towards location (270,50) with a speed of 20ms. At 19.95s, MN2 reports high packet loss rate (0.78) to the sink (see Figure 14). When the sink receives an RR with high packet loss rate (0.78), it checks the location of MN2 (265,49) and calculates the distance between BS1 and MN2 (see subsection 5.2.3). The distance is 245m. Then, the sink finds out that the distance is close to the radius (range) of BS1 which is 250m. It detects that the reason of packet loss is due to signal attenuation. Then, at 20s, MN2 starts to move back towards (20, 30). At 20.4s, the packet loss incurred by MN2 changes to 0.69. Again, the sink checks the location of MN2 (264, 49) and finds that the distance between BS1 and MN2 (244m) is close to the range of BS1. Hence, the sink infers that current high packet loss is due to signal attenuation.
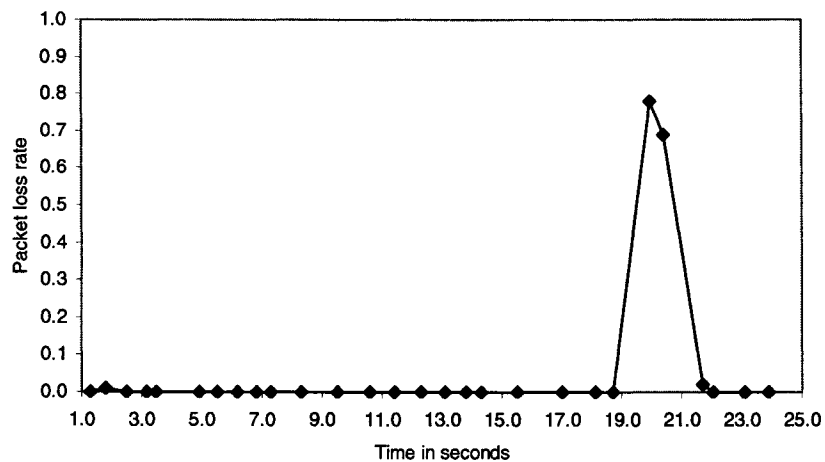

Figure 14: Effect of signal attenuation on packet loss rate of the RTP flow versus time (BS range=250m)

At 21.7s, the packet loss rate of MN2 reduces to 0.02 as it moves within the range of BS1. Table 2 shows the values of the distance between MN2 and BS1 along with packet loss experienced by the node during signal attenuation when the base station range is 250m.

53

Time	Distance (MN2 – BS1)	Packet loss rate
19.95	245	0.78
20.4s	244	0.69

Table 2: Packet loss rate of the RTP flow in case of signal attenuation and distance between MN2 and BS1 (BS range=250m)

We repeated the previous simulations. This time, we set the range of the base station to 100m and then to 40m to test SGWAS during signal attenuation with different base station ranges. Initially, MN2 is stationary at the location (20,30). Here, the base station range is set to 100m. At 6s, MN2 moves towards the location (120,50) with a speed of 10ms. Figure 15 shows the packet loss reported in RRs sent to the sink by MN2. There is no packet loss observed in the RTP flow received by MN2 till 17.9s because interfering UDP traffic is sent at low rate. At 17.9s, the packet loss rate incurred by MN2 increases to 0.84. When the sink receives RR with high packet loss, it checks the location (116, 49) of MN2 and calculates the distance between BS1 and MN2. Then, the sink finds that the distance (97m) is close to the range of BS1, i.e. 100m and detects that the reason of high packet loss is due to signal attenuation. At 18.3, packet loss of the RTP flow received by MN2 increases further to 0.9. Then, the sink uses the location (117, 49.4) information of MN2 and calculates the distance between BS1 and MN2 (98m). Since, the distance is close to the range of BS1, the sink detects that current high packet loss of the RTP flow is due to signal attenuation.
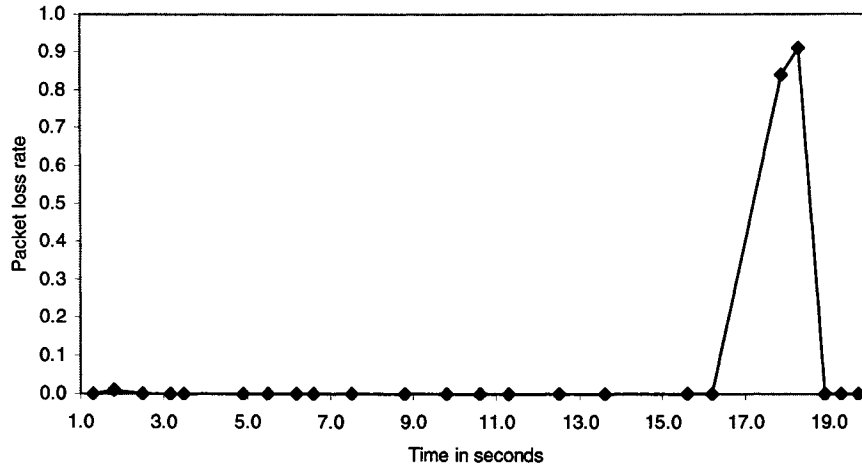
54

Figure 15: Effect of signal attenuation on packet loss rate of the RTP flow versus time (BS range=100m)

Time	Distance (MN2 – BS1)	Packet loss rate
17.9s	97	0.84
18.3s	98	0.91

Table 3: Packet loss rate of the RTP flow in case of signal attenuation and distance between MN2 and BS1 (BS range=100m)

Then at 18.4s, MN2 moves towards the location (20,30) and its packet loss reduces to 0 at 18.9s as it moves within the range of BS1. Table 3 shows the values of the distance between MN2 and BS1 along with packet loss experienced by the node during signal attenuation when the base station range is 100m.

In the next experiment, we set the range of the base station to 40m. Initially, MN2 is stationary at the location (20,30). After 6s, MN2 starts to move towards the location (60,50) with a speed of 10ms. Figure 16 shows the packet loss reported in RRs sent to the sink by MN2 when the BS1 range is set to 40m.

In figure 16 no packet loss is incurred by the RTP flow received by MN2 until 12.5s because interfering UDP traffic is sent at a very low rate. At 12.5s, packet loss rate of MN2 increases to 0.89. When the sink receives RR with high packet loss, it checks the location (52, 46) of MN2 and calculates the distance between BS1 and MN2. Then, the

55

sink identifies that distance (35m) is close to the range of BS1, i.e. 40m and infers that the reason of high packet loss is due to signal attenuation. Then at 12.83s, the packet loss rate changes to 0.97 and the sink calculates the distance between MN2 and BS1 using the location information (53, 47) of MN2. Then, the sink identifies that the high packet loss is due to signal attenuation because the distance between MN2 and BS1 (37m) is close to radius (range) of BS1 which is 40m. Table 4 shows the values distance between MN2 and BS1 along with packet loss experienced by the node during signal attenuation when base station range is 40m.
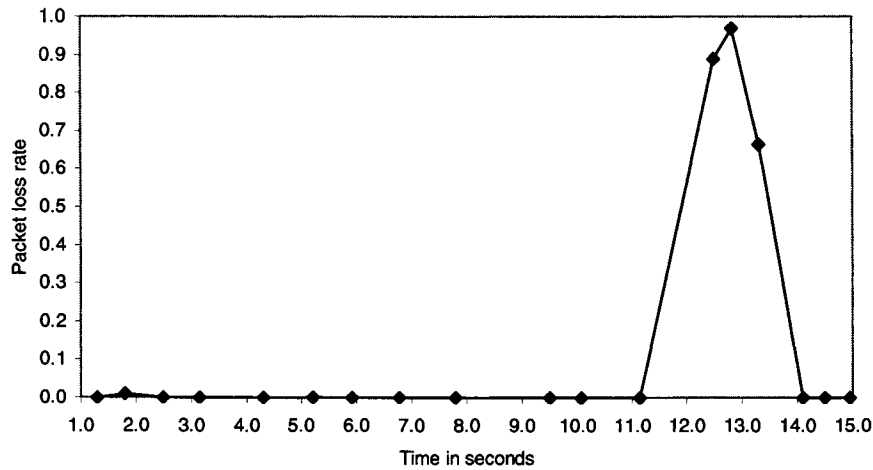
Figure 16: Effect of signal attenuation on packet loss rate of the RTP flow versus time
(BS range=40m)

Time	Distance (MN2 – BS1)	Packet loss rate
12.5s	35	0.89
12.83s	37	0.97

Table 4: Packet loss rate of the RTP flow in case of signal attenuation and distance between MN2 and BS1 (BS range=40m)

Then at 13.0s, MN2 moves towards the location (20,30) and its packet loss reduces to 0.66 at 13.3s as it starts to moves towards BS1. At 14.1s, the packet loss reduces to 0 as MN2 moves within the range of BS1.

56

These results show that SGWAS identifies the reason of high packet loss during signal attenuation, using different ranges for the base station.

5.3.4 Rate adaptation in wired network

High packet loss can occur due to congestion in the wired network. In SGWAS, the base station present at the intersection of wired/wireless network, detects if there is significant packet loss in the wired region. It intercepts RTP data packets and uses the sequence number in RTP header to identify the packet loss. It then sends a message to the mobile node asking it to send the RTCP RRs to the data sender present in the wired region. Then, this sender decreases its rate of data transmission to reduce the packet loss and to alleviate congestion.

In this experiment, at 1.2s, S1 sends RTP data to MN2 at a rate of 256Kbps. S2 sends interfering UDP traffic at a high rate (4800Kbps) to BS1 which starts at 2.2s and stops at 8s. At 8s, S1 sends interfering UDP flows at a rate of 4700Kbps to BS1 and stops at 15s. Figure 17 shows the change in sending rate of the RTP flow, performed by the data sender, in case of congestion in the wired network. Figure 18 shows the packet loss rate of the RTP flow reported in RRs received at the sender in case of wired network congestion. It shows also the packet loss reported at the sink before congestion in the wired network is detected and when congestion in the wired network ceases. At the beginning of the simulation, no packet loss is observed at BS1 and MN2, as there is not much traffic.

At 3.25, packet loss (0.14) is being detected at BS1 because the amount of traffic (i.e. RTP flow and interfering UDP traffic) increases at BS1. Initially, MN2 sends RRs to the sink. But, after BS1 detects high packet loss in the RTP flow, it sends a message to MN2 asking it to send RRs to the sender S1. Then, the sender checks if the packet loss incurred by the mobile node is greater than threshold. The sender sets the packet loss threshold to 0.13 to deal with wired network congestion.

57
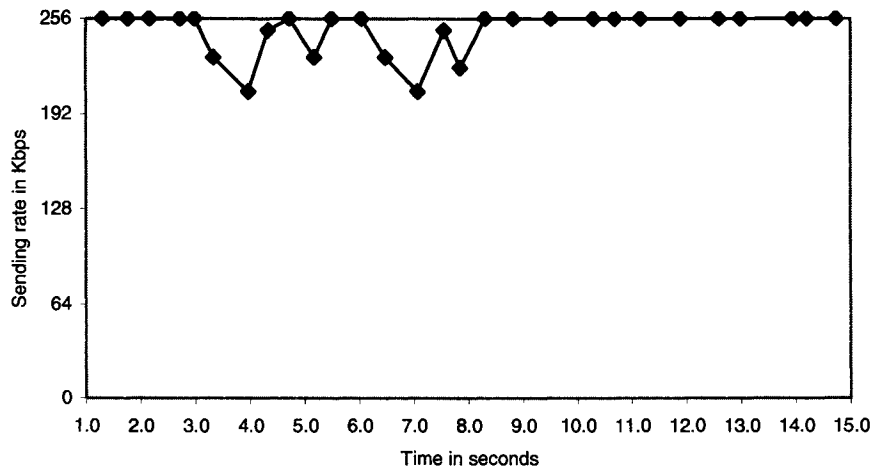
Figure 17: Sender rate adaptation versus time in case of congestion in the wired network
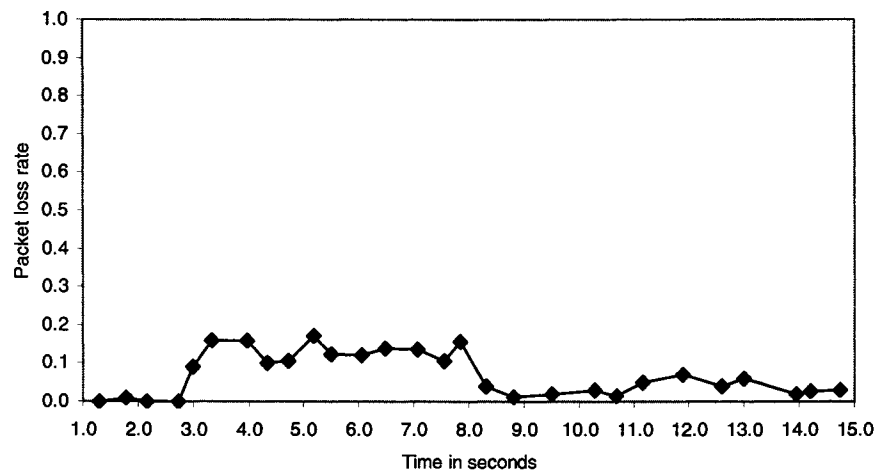
Figure 18: Packet loss of the RTP flow versus time in case of sender rate adaptation

After BS1 detects high packet loss of the RTP flow is greater than or equal to 0.13, it sends a message to MN2 asking it to send RRs directly to the sender S1 instead of the sink. After that, each time BS1 detects packet loss greater than or equal to 0.1 only (see explanation below), not 0.13, it asks MN2 to send its RRs to S1. The base station has two thresholds: maximum threshold (0.13) and minimum threshold (0.1)[5]. The first time it detects high packet loss, it uses the maximum threshold. Then, it uses the minimum

---

[5] Packet loss that exceeds 10-20% is not acceptable for audio flows [KR03].

58

threshold to keep on detecting the subsequent packet loss. This way, it can prevent high oscillations. If packet loss decreases below the minimum threshold, then BS1 recognizes that congestion in the wired network ceases and asks MN2 to reports its packet loss directly to the sink. At 3.34s, S1 receives an RR from MN2 reporting packet loss 0.16. Then, S1 decreases the sending rate of RTP flow to 230 Kbps (see figure 17) since the packet loss is greater than threshold. At 3.97s, MN2 reports high packet loss (0.166) and S1 reduces further the sending rate of the RTP flow to 207Kbps.

S1 receives another RR at 4.33s with packet loss 0.1. Since this value is less than threshold set by the sender (0.13), S1 increases the sending rate of RTP flow to 248Kbps. At 4.72s, the packet loss (0.105) remains under threshold (see Figure 18) and S1 increases the sending rate of the RTP flow to 256Kbps (original rate). S1 keeps on adapting the transmission rate of the RTP flow to alleviate congestion in the wired network.

At 8.25s, BS1 notices packet loss (0.04). The packet loss reduces because of decrease in the amount of interfering UDP traffic at BS1. That is to say, the amount of interfering traffic at BS1 decreases, as S2 stops sending interfering UDP traffic at 8s. But, packet loss still occurs at BS1 because of the UDP traffic sent from S1 to BS1 that starts at 8s and stops at 15s. When BS1 notices packet loss (0.04), it compares the packet loss with the threshold set at the base station, i.e. 0.1. Since the packet loss is less than threshold, BS1 detects that congestion in the wired network has reduced. Then, BS1 sends a message to MN2 to inform it to send RRs to the sink. The sink receives RRs from MN2 at 8.82s. The packet loss at BS1 remains under threshold for the rest of the simulation and MN2 keeps on sending its following RRs to the sink.

These results show that our scheme (SGWAS) identifies congestion in the wired region. Then, the sender performs transmission rate adaptation to decrease the packet loss and to alleviate congestion in the wired region.

5.4 Summary

This chapter explains the simulation topology, implementation and various simulation experiments and results. Our results show that SGWAS helps in identifying

59

the main reasons of packet loss when running real-multimedia application over the wireless network.

When the packet loss is due to handoff, the sink identifies the handoff location co-ordinates and informs the mobile node that it is currently experiencing packet loss because it is in the handoff region.

When the packet loss is due to signal attenuation, the sink calculates the distance between the mobile node and the base station. If the distance is approximately close to the range of the base station or greater than the range, the sink identifies that the current high packet loss is due to signal attenuation. It then informs the base station to increase its transmission power or change the direction of the antenna.

When the packet loss is due to wireless link congestion, the sink informs the base station. Then, the base station performs transmission rate adaptation to improve the QoS of the transmission.

When the packet loss is due to wired network congestion, the base station informs the mobile node to send RRs to the sender. Then, based on the feedback received from the mobile node, the sender performs rate adaptation to improve the QoS of the transmission.

60

CHAPTER VI

CONCLUSIONS AND RECOMMENDATIONS

This thesis proposes a Sensor Guided Wireless Adaptation Scheme (SGWAS) that helps identify the main reason of high packet loss when running real-time multimedia applications over wireless/wired networks. Consequently, it takes the appropriate action to improve the Quality of Service (QoS) of the real-time multimedia transmission.

When running multimedia applications over wired networks, the quality of the transmission gets affected if congestion occurs. To alleviate congestion, rate-based adaptation schemes are used and packet loss rate is used as the main indicator of congestion. However, when running multimedia applications over wireless networks, packet loss could be due to various reasons other than congestion. That is to say, packet loss could be due to handoff, signal attenuation or obstruction, or the low bandwidth of the wireless link that can cause local wireless congestion. So there is a need to identify the main reason of high packet loss and improve the QoS of the data transmission.

We designed and implemented a scheme called SGWAS that works in a micromobility domain and infers the main reason of high packet loss incurred by the mobile node in the wireless cell. The packet loss rate reported in the RTCP feedback receiver reports sent by the mobile node help in determining the current network state. But, to infer the main reason of high packet loss, we need to identify the location of the mobile node within the cell. We use the information obtained from the wireless sensors, specifically RFID devices scattered in the cell, to identify the location of the mobile node within the cell.

The simulation results show that SGWAS helps detect the reason of high packet loss during handoff, signal attenuation, local wireless link congestion, or congestion in the wired region. That is to say, if high packet loss is due to handoff, the mobile node is informed that the currently experienced packet loss is because of its current existence in the handoff region. Moreover, if high packet loss occurs because of signal attenuation, then the base station is informed to increase its transmission power or change the direction of its antenna. Furthermore, if high packet loss is due to local wireless link congestion, the base station performs rate adaptation. It decreases its forwarding rate of

61

the real-time multimedia flow, which is currently experiencing high packet loss, to alleviate congestion in the wireless cell. The base station does not perform rate adaptation if the cause for high packet loss in the wireless cell is not local congestion. This is important particularly when there are multiple nodes, in the same wireless cell, receiving the same real-time multimedia flow. In addition, if high packet loss is due to congestion in the wired region, the base station asks the mobile node to report the packet loss to the data sender. Then, the sender performs rate adaptation to alleviate congestion in the wired region.

Some enhancements can be added to SGWAS for further improvement. The main reason of packet loss incurred by the mobile node is detected by using the information sent by the RFID readers. This mainly depends on the range of RFID readers because they can detect the mobile node only if it is moving within their range. So, increasing the range of RFID readers can cover larger areas and reduce the number of RFID readers needed. But, increasing the range could also increase the cost of the readers. So, further research can investigate the trade off between cost and range of RFID readers.

In SGWAS, we assume that the sender is located in the wired region. It performs rate adaptation in case of congestion in the wired network. If the sender is present in another wireless cell, then high packet loss incurred by the receiving mobile node might occur when the sender is moving in the handoff region or when it is far away from its base station. Hence, the sender should not perform rate adaptation in case of handoff or signal attenuation. To handle this issue, some further improvements can be added to SGWAS. The sender can send a message to the sink, located in its cell, to find its location. If the sender receives a message from the sink informing it that its current location is the handoff region, then the sender will not perform rate adaptation. The same could happen if the sender is suffering from signal attenuation because it is far from base station. Otherwise, the sender assumes that packet loss is because of congestion and decreases its transmission rate to alleviate congestion.

SGWAS helps also identify the reason of high packet loss incurred by the real-time multimedia flow received by the mobile node, in case of signal obstruction by an obstacle, such as a mountain. This is done using the information obtained from RFID sensors. After identifying the reason of high packet loss, the sink searches for another

62

node, receiving the same real-time multimedia flow and that doesn't suffer from high packet loss. The sink asks this node to forward the data packets it receives to the mobile node experiencing the obstruction problem. This relaying node has to be in a location free of obstacles and not in the handoff region or suffering from a weak signal. In the future, this module of our scheme can be implemented to detect the reason of high packet loss in case of signal obstruction and thus try to forward the data packets to the mobile node which is suffering from signal obstruction.

Moreover, in the future, we can use dynamic threshold. In our scheme, the sender sets the packet loss threshold which does not change during the lifetime of a session. This fixed threshold may not be suitable for different network states because packet loss, reported in feedback reports, may change due to changing network conditions and thus oscillations may occur. Also, this threshold may change for different media like audio and video. So, in the future, our scheme should be able to adjust the threshold dynamically for a real-time multimedia flow. To calculate the dynamic threshold, it is necessary to estimate the packet loss to be reported in the next feedback report. The estimated packet loss can be calculated using the exponential weighted average function. This estimated packet loss reflects the previous estimated packet loss values (past history of packet loss) for the flow and the currently observed packet loss. But, more weight is put on the current packet loss. Then, threshold can be adjusted according to this estimated packet loss. The threshold can be changed within a range, for example between 10% and 20% for audio flows [KR03]. Consequently, the adjusted threshold copes with the changes in the network state.

APPENDICES

APPENDIX A

TERMINOLOGY

Name	Definition
Bandwidth	Link Transmission rate. It is usually measured in bits/second
Base Station	The base station transmits data to and from the mobile nodes.
End-to-end Delay	The delay from source to destination including nodal processing delay, queuing delay, transmission delay, and propagation delay. [KR03]
Flow	A flow is defined as the stream of packets transmitted between sender and receiver during an application session.
Handoff	The process of movement of the mobile node from one base station to another is known as handoff. [KR03]
Interval	The time difference between sending the current RTCP receiver report and the previous one from the same node.
Jitter	"It is the mean deviation of the difference between the packet spacing at the receiver and the sender for a pair of consecutive packets." [SCF03]
Media Access Control (MAC) Address	A hardware address that uniquely identifies the adapter of each node of a network.
Micromobility	It is defined as the movement of a node between various sub networks within a single network domain, such as wide area network. [RVS02]
RTP Mixer	An RTP mixer usually collects RTP data from different sources within a RTP session, changes their encoding or combines them according to some technique and forwards as a new RTP data packet. [SCF03]
RTP Session	"The association among a set of participants communicating with RTP." [SCF03]
Signal Attenuation	Weakening of signal strength due to increase in distance between base station and mobile node.
Sink	Sink is a sensor node with more energy and processing capabilities than other sensor nodes.

64

Throughput	It is the observed rate at which data is sent through a channel. [PD00]

65

APPENDIX B

ABBREVIATIONS

Abbreviation	Full Name
ACK	Acknowledgement
ARP	Address Resolution Protocol
BS	Base Station
CIMS	Columbia IP Micro-Mobility Suite
CNAME	Canonical Name
CN	Correspondent Node
DLSR	Delay since last Sender Report
FA	Foreign Agent
FEC	Forward Error Control
FTP	File Transfer Protocol
GRCA	Gateway-based Rate Control Algorithm
HAWAII	Handoff-Aware Wireless Access Internet Infrastructure
HA	Home Agent
IFQ	Interface Priority Queue
IP	Internet Protocol
IPG	Inter-Packet Gap
LAN	Local Area Network
LEACH	Low-Energy Adaptive Clustering Hierarchy
LL	Link Layer
MAC	Media Access Control

66

MN	Mobile Node
MPEG	Moving Picture Experts Group
netIF	network Interface
NOAH	NO Ad-hoc Routing
NS	Network Simulator
PT	Packet Type
QoS	Quality of Service
RAM	Random Access Memory
RC	Reception Count
RFID	Radio Frequency Identification
ROM	Read-Only Memory
RR	Receiver Report
RTP	Real-time Transport Protocol
RTCP	Real-time Control Protocol
SDES	Source Description
SGWAS	Sensor Guided Wireless Adaptation Scheme
SID	Session Identification
SPIN	Sensor Protocols for Information via Negotiation
SR	Sender Report
SSRC	Synchronization Source
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
UDP	User Datagram Protocol

67

WSN	Wireless Sensor Network

REFERENCES

[AIM01] AIM Association, "Radio Frequency Identification (RFID) – A Basic Primer", AIM Inc. WP-98/002R2, White Paper version 1.2, 2001.

[AVA05] I.F. Akyildiz, M.C.Vuran, and O.B. Akan "Wireless Sensor Networks: A Survey Revisited," to appear in Computer Networks Journal (Elsevier), 2005.

[AYB05] K. Akkaya, M. Younis and M. Bangad, "Sink repositioning for enhanced performance in wireless sensor networks", Computer Networks, vol 49, issue 4, pp512-534, 2005.

[BT94] J. Bolot and T. Turletti, "A Rate Control Mechanism for Packet Video in the Internet", In Proceedings of IEEE Infocom'94, pp. 1216-1223, 1994.

[BDS96] I. Busse, B. Deffner, and H. Schulzrinne, "Dynamic QoS Control of Multimedia Applications Based on RTP", Computer Communications, vol. 19, no. 1, pp. 49-58, 1996.

[CG01] A.T. Campbell and J. Gomez "IP Micro-Mobility Protocols", ACM SIGMOBILE Mobile Computer and Communication Review (MC2R), Vol. 4, No. 4, pp 45-54, October 2001. http://comet.columbia.edu/micromobility/

[CMU01] CMU Monarch Project, "Monarch Project Extensions to ns-2. http://www.monarch.cs.cmu.edu/cmu-nshtml accessed November 2001.

[CRK05] B. Carbunar, R. M. Krishna, and M. Koyuturk, "Redundant Reader Elimination in RFID Systems", CERIAS Tech Report 2005-63, Purdue University, 2005.

[CTY02] G. Cheung, W. t. Tan, and T. Yoshimura, "Streaming agent for wired network / wireless link rate-mismatch environment," in MMSP, 2002.

[CY02] G. Cheung and T. Yoshimura, "Streaming agent: A network proxy for media streaming in 3g wireless networks", In Packet Video Workshop, 2002.

[EL01] R. El-Marakby, "NS Implementation of RTP/RTCP", In Proc. of IEEE International Symposium on Signal Processing and Information Technology, 2001.

[EH97] R. El-Marakby and D. Hutchison, "Towards Managed Real-time communications in the Internet Environment", In Proceedings of the Fourth IEEE Workshop on

the Architecture and Implementation of High Performance Communication Systems (HPCS'97), 1997.

[EH98] R. El-Marakby and D. Hutchison, "A Scalability Scheme for the Real-time Control Protocol", Proceedings of IFIP Eighth International Conference on High Performance Networking (HPN'98), pp. 153-168, 1998.

[FH98] P. Ferguson and G. Huston, "Quality of Service: Delivering QoS on the Internet and in Corporate Networks", Wiley & Sons, New York, USA, 1998.

[FV99] K. Fall and K. Varadhan, "Network Simulator (NS-2) The NS Manual", www.isi.edu/nsnam/ns, 1999.

[GRE00] M. Greis, "Tutorial for the Network Simulator NS", 2000. http://www.isi.edu/nsnam/ns/tutorial/index.html

[HCB00] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy-Efficient Communication Protocols for Wireless Microsensor Networks, Proc. Hawaaian Int'l Conf. on Systems Science, 2000.

[IGE00] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCOM '00), 2000.

[KDJ04] C. Kerer, S. Dustdar, and M. Jazayeri, , "Presence-Aware Infrastructure using Web services and RFID technologies", 2nd European Workshop on Object Orientation and Web Services, ECOOP Workshop, 2004.

[KR03] J. F. Kurose and K. W. Ross, "Computer Networking – A Top-Down Approach Featuring the Internet", second edition, Addison Wesley, 2003.

[LR05] K. Langendoen and N. Reijers, "Distributed Localization Algorithms", Embedded Systems Handbook, R. Zurawski (editor), CRC press, August 2005.

[PER02] C. Perkins, "IP Mobility Support for IPv4", RFC 3344, 2002.

[PD00] L. Peterson and B. Davie, "Computer Networks: A Systems Approach", Second Edition, Morgan Kaufman Publisher, 2000.

[PK00] G. J. Pottie and W. J. Kaiser, Wireless Integrated Network Sensors, Communications of ACM, vol.43, no.5, pp. 51-58, 2000.

[POS80] J. Postel, "User Datagram Protocol", IETF RFC 768, 1980.

[POS81] J. Postel, "Transmission Control Protocol", IETF RFC 793, 1981.

[RAP01] T. Rapport, "Wireless Communications: Principles and Practice", Prentice Hall PTR, 2001.

[RT05] S. Rinzivillo, F. Turini, "Extracting Spatial Association Rules from Spatial Transaction", Proceedings of the 13th annual ACM international workshop on Geographic information systems, pp. 79 – 86, 2005.

[RVS02] R. Ramjee, K. Varadhan, and L. Salgarelli, "HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks", IEEE/ACM Transactions on Networking Volume10, Issue3, 2002.

[SAB04] A. Sabetti, "Applications of Radio Frequency Identification (RFID)", AIM Global Network, 2004.

[SCF03] H. Schulzrinne, S. Casner, and R. Frederick, "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, 2003.

[SGW01] L. Schwiebert, S.K. Gupta and J. Weinmann, "Research Challenges in wireless networks of biomedical sensors" in Proc. ACM / IEEE MOBICOMM '01, pp 151-165, 2001.

[VAL99] A.G.Valko, "Cellular IP: A New Approach to Internet Host Mobility," ACM Computer Communications Review, pp. 50-65, 1999.

[WID00] J. Widmer, "Network Simulations for A Mobile Network Architecture for Vehicles", Joint project of ICSI and DaimlerChrysler Research, 2000. http://www.icsi.berkeley.edu/~widmer/mnav/

[YOK02] T. Yoshimura, T. Ohya, and T. Kawahara, "Rate and Robustness Control with RTP Monitoring Agent for Mobile Multimedia Streaming", In Proc. of IEEE International Conference on Communications (ICC), 2002.

[YYY00] L. Youngseok, Y. Yung, and W. Youjae, "GRCA: Gateway-based Rate Control Algorithm for the CBR Traffic over the Wireless Link", The 14th International Conference on Information Networking, 2000.

[ZK03] M. Zuniga and B. Krishnamachari, "Integrating Future Large-Scale Wireless Sensor Networks with the Internet," USC Computer Science Technical Report CS 03-792, 2003.

VITA AUCTORIS

NAME	Mythili Enugula
YEAR OF BIRTH	1981
PLACE OF BIRTH	Warangal, India
EDUCATION	M.Sc. Computer Science University Of Windsor Windsor, Ontario Canada 2006
	Post Graduate Diploma in Information Systems Osmania University Hyderabad India 2002
	Bachelors in Computer Applications Osmania University Hyderabad India 2001