Mitigating the Reader Collision Problem in RFID Networks with Mobile Readers

Dissertation

Submitted in partial fulfillment of the requirements
for the degree of

Masters of Technology

by

Shailesh M. Birari

Roll No: 03329028

under the guidance of

Prof. Sridhar Iyer

Kanwal Rekhi School of Information Technology
Indian Institute of Technology Bombay
2005

Dedicated to my family

Dissertation Approval Sheet

This is to certify that the dissertation entitled

Reader Collision Problem in RFID Networks with Mobile Readers

by

Shailesh M. Birari

(Roll no. 03329028)

is approved for the degree of **Master of Technology**.

____

Prof. Sridhar Iyer
(Supervisor)

____

Prof. Anirudha Sahoo
(Internal Examiner)

____

Dr. Pravin Bhagwat
(External Examiner)

____

Prof. Abhay Karandikar
(Chairperson)

Date: _______________

Place: ______________

Abstract

Radio Frequency Identification (RFID) is a means to identify and track objects using radio frequency transmission. An RFID system consists of readers and tags. Readers use radio signals to communicate with the tags. Tags may be *active* (battery powered) or *passive* (powered by the reader's signals). RFID is increasingly being used in many applications such as inventory management, object tracking, retail checkout etc. The reader collision problem occurs when the signal from one reader interferes with the signal from other readers. Such interference can result in lack of communication between the readers and some of the tags in the vicinity leading to incorrect and inefficient operation of an RFID system. This problem is further aggravated when mobile/hand-held readers are used in the system. Hence efforts are required to minimize this interference.

We describe Pulse, a distributed protocol to reduce these reader collisions in the RFID systems. The operation of the Pulse protocol is based on periodic beaconing on a separate control channel by the reader, while it is reading the tags. The protocol functions effectively not only with fixed RFID readers but also with mobile RFID readers. We show, using simulation in QualNet, that using Pulse protocol, the throughput (overall read rate) is increased by 98%(with 49 readers) as compared to "Listen Before Talk"(CSMA) and by 337% as compared to Colorwave(with 9 readers). We also present an analytical model for our protocol in a single hop scenario.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 RFID Networks

Automatic Identification is the process of identification of objects with minimum human intervention. In recent years, automatic identification procedures(Auto-ID) have become very popular in many service industries, purchasing and distribution logistics, industry, manufacturing companies and material flow system. Radio Frequency Indentification(RFID) is a technique of Auto-ID which uses radio frequency to automatically identify and track individual item through the supply chain.

An RFID system consists of an RFID reader, which is a transmitter/receiver module connected to an antenna, and a set of RFID tags, each of which is a low functionality microchip connected to an antenna[1]. A tag, which is generally attached to an object, typically stores information about the object. This information may range from static identification (serial number) to user written data(cost of the item) to sensory data(temperature of a boiler). The reader uses radio signals to communicate with the tag and access this information. A tag may be active(powered by an external battery) or passive(powered by energy in the reader's signals) [2][3].

- **Passive Tags:**
    - Uses the reader field as a source of energy for any on-chip computation and also for communication back to the reader.
    - As the communication back to the reader is a reflected signal, these tags can only be read from a short-range distance of approximately 5-10 feet.
    - These tags are cheaper and hence can be applied in high quantities to individual items.

- **Active Tags:**
    - Use external battery power for computation and for communication back to the reader. These can be read from a long-range distance of more than 100 feet.
    - Are ideal for tracking high-value items over long ranges, such as tracking shipping containers in transit.
    - Have high power and battery requirements, so they are heavier and can be costly.

1.1.1 RFID systems

Depending on the radio frequency used for communication, the RFID systems have been classified[2] as under

RF Systems	Frquency Range	Typical Read Range
LF System	< 135 KHz	<0.5m
HF System	< 13.56 MHz	1m
UHF System	< 860 - 930 MHz	4-5m
Microwave System	< 2.45 GHz	1m

Table 1.1: RFID System Classification

1.1.2 Operating Principle

Inorder to energy and communicate with a reader, passive tags use one of the two methods:

- **Near Field (Inductive Coupling):** This technique employs inductive coupling of the tag to the magnetic field circulating around the reader antenna(like a transformer). Near field is used by RFID systems operating in LF and HF frequency bands. Communication from reader to the tag happen by amplitude modulation whereas from the tag to the reader is achieved by changing the impedence in the secondary coil (tag antenna) which result in appropriate voltage change in the primary coil(reader side).

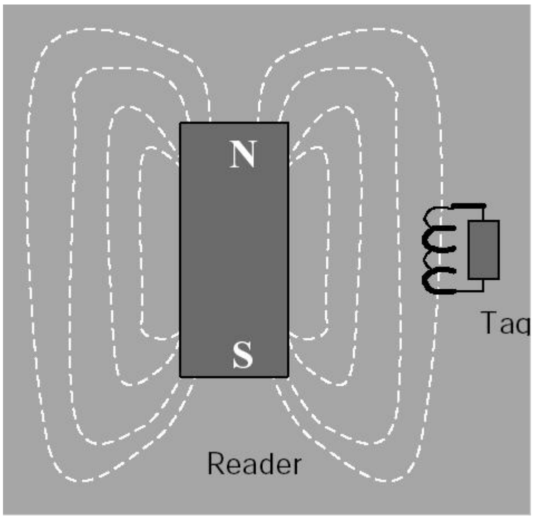

Figure 1.1: Near Field Coupling

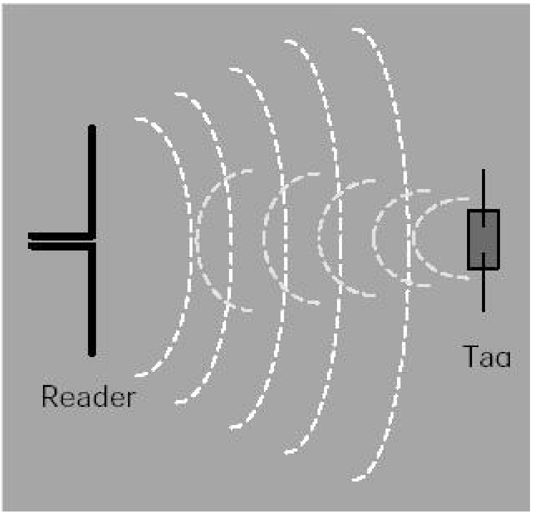

Figure 1.2: Far field Coupling

- **Far Field (Backscatter reflection):** This technique employs the radar technology and is used in UHF and microwave systems. When the propagating wave from the reader collides with a tag antenna, part of the energy is absorbed to power the tag and a small part is reflected back to the reader technique known as backscatter. Communication back to the reader is achieved by altering the antenna input impedance.

1.1.3 RFID Applications

Following are the common applications of RFID systems:

- Identification and Inventory Management: In number of applications related to inventory mangement like identifying the items at the point of sale, counting the number of items left in the shelf in a super market or searching a particular book in the library.

- Access Control: To automatically check the access authorisation of individuals to buildings, premises or individual rooms using “touch & go” RFID tags.

- Tracking : In tracking of large containers and trucks in the transport systems. Also RFID can be used in tracking of tagged animals.

- Theft Detection: RFID can be used in theft detection of items in super markets by keeping an “always on“ RFID reader in the shelves or at the exit point.

1.1.4 Advantages of RFID over other auto-identification techniques

RFID’s basic advantage over other identification techniques is the full automation of the data capture process where the optical identification systems fail. The most commonly used identification systems is the barcode system. Barcode systems typically require the laser gun to be shooted on the barcode to read it thus expecting an orientation between the two. The information in the barcode is fixed. The barcode system is sensitive to the clear optics, harsh environments and abrasion of the barcode on the item. RFID systems can work from a greater distance, even in harsh environments, without any need of the line of sight. The RFID systems read rate is about 50 tags/second in high frequency tags and upto 200 tags/second in ultra high frequency tags[2]which is very high compared to the barcode read rate. RFID systems can thus enable the tracking of items in real time.

1.2 Motivation for Mobile Readers

The advantages of having mobile readers can be summarised as follows

- **Cost:** Not all applications require “always-on”/real-time sensing of the item to be tracked. So a large deployment of fixed readers to cover the area is an overkill. For example, is it important to instantaneously sense the removal of a coke can in a retail store? Instead a periodic walk-through of mobile reader suffices in such situation. Also fewer mobile readers would suffice to cover the deployment area thus reducing the cost to a considerable extent.

- **Convenience:** Mobile readers require no wiring hassles or disruption of activities. Also mobile readers promote faster deployment of application and increases end user convenience.

- **Client Enabling:** The handheld readers can have customized client slide applications like searching of a particular book in the library, or counting the number of item on the shelf. Another interesting application in a super market can be with readers attached to the shopping cart and these readers would display the list of items in its read range so that the customer need not look through the shelves in search of the desired items.

1.3 The Reader Collision Problem

Many applications require readers to operate in close proximity of each other. Due to proximity, the signals from one reader might interfere with the signals from other readers. This interference is called reader collision[4].

- **Reader to Reader interference** arises when stronger signal from a reader interfere with the weak reflected signal from a tag. For example, in fig. 1.3, R_1 lies in interference region of reader R_2. The reflected signals reaching reader R_1 from tag T_1, can easily get distorted by signals from R_2. Note that such interference is possible even when the read range of the two readers do not overlap.

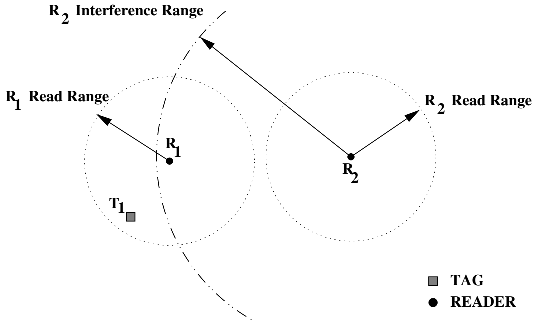

Figure 1.3: Reader to Reader Interference

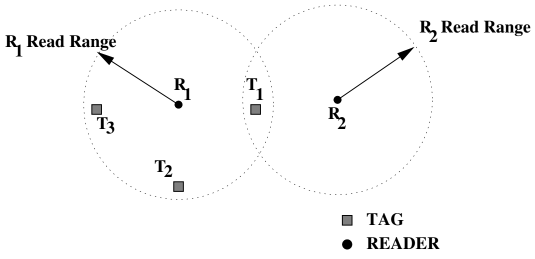

Figure 1.4: Reader to Tag Interference

- **Multiple reader to tag interference** arises when more than one reader try to read the same tag simultaneously. In fig. 1.4, the read range of the two readers overlap. Hence the signals from R_1 and R_2 might interfere at tag T_1. In such case, T_1 can not decipher any query and the tag is read neither by R_1 nor by R_2. Due to reader collisions, R_1 will be able to read T_2 and T_3 but it may not be able to read the tag T_1. In such case, R_1 will indicate presence of 2 tags instead of 3.

- Another case where reader collision can occur is shown in fig. 1.5. Here the read ranges of the two readers do not overlap. However, the signals from reader R_2

can interfere with the signals from reader R_1 at tag T. This case can also happen when the two readers are not in each other's sensing range making carrier sensing ineffective in RFID networks.

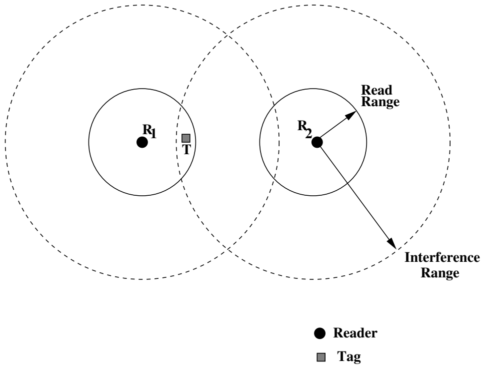

Figure 1.5: Reader Collision making carrier sensing ineffective

Apart from incorrect operations, reader collisions also result in reduction of the overall read rate of the RFID system. Morever this problem is aggravated in case of mobile/handheld readers. Hence reducing these reader collisions is essential.

1.4 Problem Statement

Traditionally most of the RFID system have been designed with only a single reader scenario in mind. With the increasing use of RFID in the industries and also huge scope for deploying mobile RFID readers, many scenarios would require readers to operate in close proximity of each other leading to interference which inturn would result in incorrect operation and/or slower tag read rates.

We propose a distributed MAC protocol, Pulse, for the RFID system which uses the concept of beaconing on a seperate control channel while it is communicating with the tags on the data channel. The scenario that we consider is of a super market or a library where each item in the inventory is tagged. All the tags are passive since they are cheaper and hence suitable for a large scale deployment like a super market. The readers form an ad hoc network with all the readers having unrestricted mobility. The readers frequnently join and leave the network. Possible applications in such a scenario could be inventory check by a number of mobile RFID readers. Another possible application is of searching of an item by a handheld reader taken around by a customer.

1.5 Thesis Outline

The major contributions of this work are

- An insight into the reader collision problem in RFID.
- A distributed protocol, Pulse, to mitigate this problem for static as well as mobile RFID networks. This protocol needs very less overhead at the readers and no modification at the tags.
- Extensive simulation results that prove the effectiveness of Pulse and also gives the optimal values of protocol parameters for the scenario under consideration.
- A theoretical model of Pulse with a single collision domain.

In this thesis, the next chapter dicusses the reasons why traditional multiple access mechanisms and collision avoidance techniques cannot be applied to RFID. It also discusses other proposals to avoid the reader collision problem and reasons why they are not effective in a scenario of mobile readers thus realising the need for a new protocol.

In chapter 3, we present our proposed protocol for a mobile scenario. Chapter 4 notes the implementation details of the protocol in the QualNet simulator. We then discuss the simulation setup and the results of simulations in chapter 5. Using simulations we also give an approximate optimal values for the protocol parameters. In chapter 6, we present the analytical model of our protocol along with a comparison of analytical and simulation results. Finally we present our conclusion and future work in chapter 7.

Chapter 2

Related Work

In this chapter, we present the salient features of the RCP and the reasons why the traditional multipe access mechanisms and collision avoidance protocols cannot be directly applied to RCP. We also present the existing work being done to avoid the RCP and its inability of cater to the mobility scenario.

2.1 Salient Features of RCP

- The well known hidden terminal problem is one aspect of the RCP. The readers that are not in each others sensing range might interfer at the tags. Thus normal carrier sensing will not work in this sceanrio.
- When queries/transmissions from multiple readers collide at a tag, signals get distorted and the tag will not be able to receive either query.
- We assume in our scenario that the tags are passive. Hence the tags cannot coordinate amongst themselves neither can they proactively communicate with the readers inorder to help in the collision avoidance. The tags can communicate only when they are activated by a reader field.

2.2 Existing Multiple Access Mechanisms

Standard multiple access mechanisms cannot be directly applied to RFID systems due to the following reasons.

- **FDMA:** With FDMA, the interfering readers can use different frequencies to communicate with the tags. However the tags do not have a frequency tuning circuitry.

Hence the tags cannot select a particular reader for communication. Also adding such a tuning circuitry will increase the cost of the RFID tags which will in turn hamper its large scale deployment. Hence FDMA is not a practical solution in RFID systems.

- **TDMA:** With TDMA, the interfering readers are alloted different time slots thus avoiding simultaneous transmissions. However this is similar to the well known coloring problem in graph theory[4] which is an NP-hard problem[4]. In a mobile scenario, non interfering readers may move closer and start interfering which will require reshuffling of time slots in a dynamic topology. Having such dynamically distributed time slots will reduce the read rate of the RFID system.

- **CSMA:** RFID networks, like other wireless networks, suffer from hidden terminal problem. Readers that are not in each other's sensing range may interfere at the tags. Hence carrier sensing alone is not sufficient to avoid collisions in RFID networks.

- **CDMA:** CDMA will require extra circuitry at the tag which will increase the cost of the tags. Also code assignment to all the tags at the deployment site may be a complicated job. Hence CDMA may not be a cost effective solution.

FDMA, TDMA and CSMA are discussed in more detail in section 2.4.

2.3 Existing Collision Avoidance Mechanism

Standard collision avoidance protocols like RTS-CTS[12] cannot be directly applied to RFID systems due to following reasons.

- In case of traditional wireless networks, only one node has to send a CTS back to the sender. However in RFID, if a reader broadcasts an RTS, all tags in the read range need to send back a CTS to the reader. This demands another collision avoidance mechanism for these CTS which will make the protocol more complicated.

- Also there are chances that a tag(say T_1) may not receive an RTS due to collision while other tag(say T_2) may receive it. In such case, a CTS from T_2 is not a guarantee that there is no collision in the read range of the reader. Some how the reader has to ensure that it has received a CTS from all the tags in the read range which is non-trivial.

2.4 Existing Approaches to avoid RCP

2.4.1 UHF Generation 2 Standard

The **Class 1 Generation 2 UHF standard**[5] ratified by **EPCGlobal**[6] uses spectral planning(FDMA). It seperates the reader transmissions and the tag transmissions spectrally such that tags collide with tags but not with readers and readers collide with readers but not with tags. Such seperation solves the reader to reader interference since the reader transmissions and tag transmissions are on seperate frequency channels. However the tags do not have frequency selectivity. Hence when two readers using separate frequency communicate with the tag simultaneously, the tag will not be able to tune to a particular frequency and hence it will lead to collision at the tags. Thus multiple reader to tag interference still exists in this standard.

2.4.2 Colorwave

Colorwave[7] is a distributed TDMA based algorithm, where each reader chooses a random time slot(color) from 0. . . maxColors to transmit. If it collides, it selects a new timeslot(color) and sends a kick (small control packet) to all its neighbours to indicate selection of new timeslot. If any neighbour has the same color, it chooses a new color and sends a kick and this continues. This switch and reservation action is refered to as the kick. Each reader keeps track of what color it believes the current timeslot to be.

In Colorwave, each reader monitors the percentage of successful transmissions. Five inputs to the algorithm determine when a reader changes its local value of max colors:

- **UpSafe**: The safe percentage at which to increase maxColors.
- **UpTrig**: The trigger percentage at which to increase max colors, if a neighboring reader is also switching to a maxColors higher than that of this reader.
- **DnSafe, DnTrig**: analogues of UpSafe, UpTrig, except decreasing max colors.

- **MinTimeInColor**: The minimum number of timeslots before the Colorwave algorithm will change max colors again after initialization or changing max colors.

When reader executing Colorwave reaches a Safe percentage to change its own value for max colors, it will send out a kick to all neighboring readers. If the phenomenon that is causing it to exceed a Safe percentage is local to that reader, other readers will not have passed their own Trig percentages and will not respond. However, if the phenomenon causing the collision value to exceed a Safe threshold is widespread, neighboring readers will most likely have exceeded their own Trig thresholds, and a kick wave will ensue. As kicks spread from the initiating reader throughout the entire system, large portion(or all) of the readers in a reader system may change their value of max colors.

Colorwave requires time synchronisation between readers. Also, Colorwave assumes that the readers are able to detect collisions in the RFID system. However it may not be practical for a reader alone to detect the collisions that happen at the tags unless the tags take part in the collision detection. Also mobility may lead to reshuffling of the time slots selected which may spread throughout the network leading to unavailability of the entire system.

2.4.3 ETSI EN 302 208 Standard

ETSI EN 302 208[8][9] is an evolving standard being developed for RFID readers. It has a CSMA based protocol called “Listen Before Talk”. The reader first listens on the data channel for any on-going communication for a specified minimum time. If the channel is idle for that time, it starts reading the tags. If the channel is not idle, it chooses a random backoff. However as described earlier in section 2.2, the readers may not be able to detect collision by carrier sensing alone.

2.4.4 Q Learning

Q-Learning[10] presents HiQ, a hierarchical, online learning algorithm that finds dynamic solutions to the Reader Collision Problem in RFID systems by learning the collision patterns of the readers and by effectively assigning frequencies over time to the readers. The hierarchical structure is as shown in fig. 2.1. The readers send the collision information to the the reader-level server (R-server) tier. An individual R-server then assigns

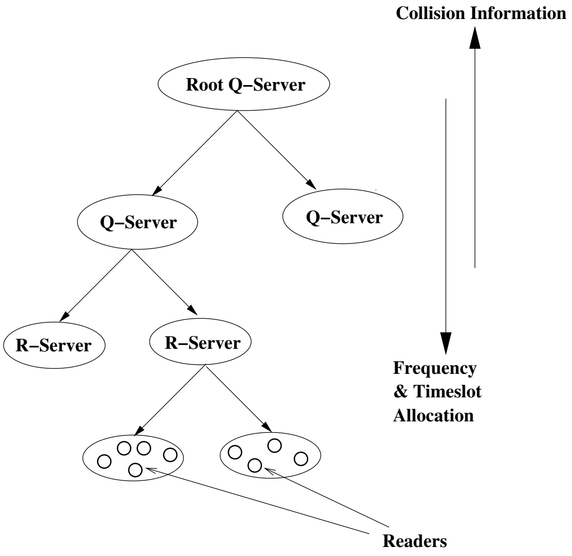

Figure 2.1: Hierarchical Structure of Q-Learning

resources to its readers in such a way that they do not interfere with each others communication. R-servers are allocated frequencies and time slots by the Q-learning servers, or Q-servers. The root Q-Server has global knowledge of all frequency and time slot resources, and is able to allocate them all. Unlike R-servers, Q-servers have no knowledge of constraints between individual readers. This information is inferred through interaction with the servers at the tier directly below.

This approach will have the following problems if applied to our scenario

- This protocol maintains a hierarchical structure which will require extra management overhead.

- For the case of mobile readers, the topology may change indefinitely which will change the hierarchical structure. This will require the distribution of the time slots to be reshuffled which will take time and make the system unavailable.

- Q-learning assumes collision detection for readers which are not in sensing range of each other. However not all collisions might be detected leading to incorrect operation of the protocol.

- The use of timeslots need all the readers to be synchronised. This synchronisation will be another overhead in the whole system.

As we see, the existing approaches cannot cater to the mobility scenario. They are either not practical or are inefficient. In the next chapter, we present our proposed protocol, Pulse, in detail which is practical and efficient.

Chapter 3

Pulse Protocol

The most important factor in designing a protocol to avoid the reader collision problem was that the tags were passive and hence could not participate in collision avoidance. Secondly adding any new functionality to the tags would increase the cost of the tags which would hamper large scale deployment of RFID systems. Hence we had to design a protocol that would not bring the tags in the picture. In this chapter we describe our proposed protocol in detail.

RFID networks suffer from the hidden terminal problem. As seen in figure 3.1, R_1 and R_2 are not in each other's sensing region, but signals from R_2 might interfere with signals from R_1 at tag T. For such a scenario, a notification mechanism is required between R_1 and R_2 such that, while R_1 is communicating with T, R_2 is informed of R_1's transmissions so that R_2 can withhold its communication with the tag. We propose to have this notification through a broadcast message called "beacon" that a reader will send periodically on a seperate control channel while it is communicating with the tags.

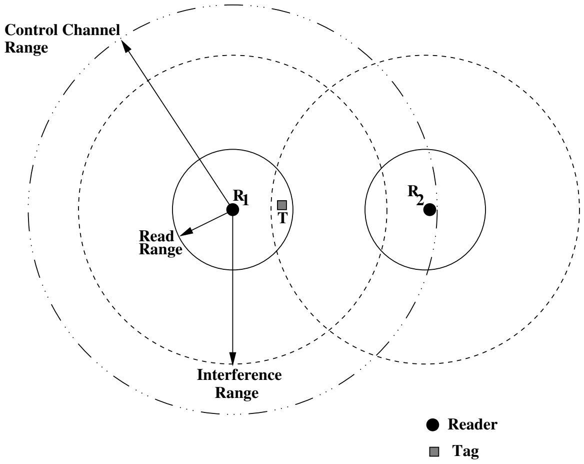

Figure 3.1: Control Channel Range for Pulse Protocol

The communication range in the control channel is such that, any two readers that can interfere with each other on the data channel (channel used to read the tags), are able to communicate on the control channel. Thus in fig 3.1, since R_1 and R_2 interfere with each other on the data channel, they will be able to communicate on the control channel. This can be achieved by making the readers transmit at a higher power on the control channel than the data channel. The control channel can simply be a sub-band in the RFID spectrum apart from those used for reader-tag communication. Hence transmission on the control channel will not affect any on-going communication on the data channel. The data channel is used for reader-tag communication whereas the control channel is used for reader-reader communication. We assume that the reader is able to simultaneously receive on both the control and the data channel.

3.1 Frame Format

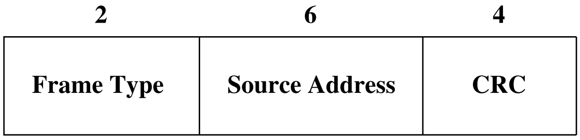

Figure 3.2: Frame format of a BEACON

Pulse protocol is present only at the reader since the tags do not take part in the collision avoidance. Fig. 3.2 shows the structure of a beacon. It has the following fields:

- **Frame Type:** This field indicates that the packet is a beacon. This is kept only for future use like it can be split into frame type and sequence number in which the sequence number will indicate the number of the beacon that is being transmitted.
- **Source Address:** This field contains the address of the reader that sent the beacon. The beacon does not have any destination address in its structure since it is a broadcast message on the control channel.
- **CRC:** This field is used to error detection and correction. This field is the cyclic redundancy check[11] of all the fields in the packet.

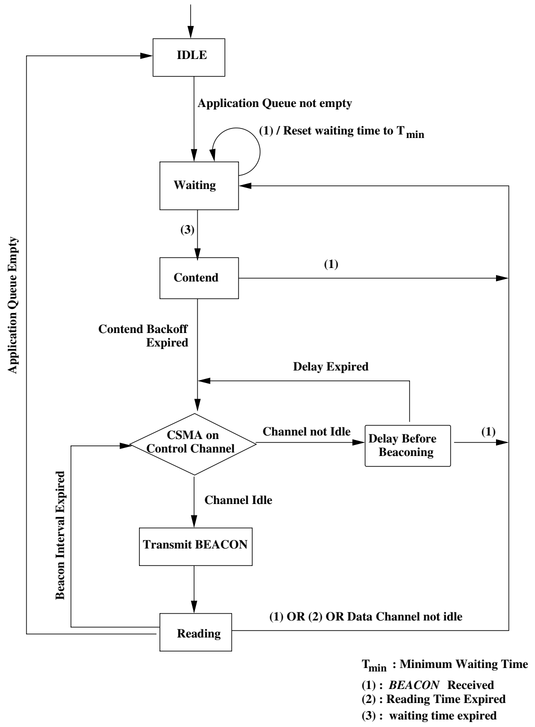

Figure 3.3: Flow Chart for Pulse

3.2 Description

Following is an overview of the Pulse protocol.

- Before communicating with the tags, a reader has to wait in the state *WAITING* for a minimum time T_{min} which is thrice the beacon interval. The time T_{min} is analogous to the DIFS time in 802.11 protocol[12]. Everytime it receives a beacon in this state, it resets its waiting time to T_{min}.

- After T_{min} time has elapsed and it did not receive any beacon for that time, the reader concludes that there is no other reader in the neighbourhood which is reading the tags. Hence it enters a contention phase and chooses a random backoff time ($contend\_backoff$) from the interval $[0 \ldots CW]$. If it chooses i, it waits for i beacon intervals in state *CONTEND*. If it now receives a beacon, it has lost this cycle and waits for the next cycle, i.e until it does not receive a beacon for atleast T_{min} time. If the randomized backoff time is over and the reader did not receive any beacon, the reader assumes that there is no other reader to compete and hence it sends a beacon on the control channel and starts communicating with the tags on the data channel. This randomized backoff helps to avoid collisions between readers, otherwise many readers would try to transmit the beacon simultaneously after waiting for T_{min} time. *contend_backoff* is a multiple of beacon intervals to improve fairness.

- While the reader is communicating with the tags, the reader sends a beacon on the control channel every beacon interval. This beacon acts as a notification to the neighbouring readers so that they can withhold their communication with the tags and thus avoid possible collisions. After the communication with the tags is over, the reader again waits in the *WAITING* state and the cycle continues.
- Everytime the reader sends a beacon, it first senses the control channel. If the control channel is busy, it continues to sense the control channel. As soon as the channel gets idle, the reader waits for a random delay(*delay_before_beaconing*) and senses the channel again to send the beacon. This random delay is a multiple of the beacon propagation delay and helps to avoid collisions - otherwise many readers would simultaneously send the beacon after the channel became idle.

Fig. 3.3 shows the detailed flowchart and fig. 3.4 and 3.5 shows the detailed algorithm for the Pulse protocol. The *contend_backoff* and the *delay_before_beaconing* in the protocol are similar to the backoffs in general wireless networks, they are decreased as long as the control channel is sensed idle, stopped when a transmission is detected, and reactivated when the control channel is sensed idle again. Also, if the reader receives a beacon during backoff (*contend_backoff*), in the contention phase, it stores the residual backoff timer and then waits for the next chance, i.e until it does not receive a beacon for atleast T_{min} time. It then uses this residual backoff time when it re-enter the *CONTEND* state. This is done only to improve fairness amongst readers.

Need for a Seperate Control Channel

The reason for a seperate control channel is that, a beacon transmission at a higher power on the data channel will interfere with any ongoing reader-tag communication in the interference region of this beacon transmission. To make situation worse, such interference will always occur periodically, at every beacon interval, in the interference region of the beacon transmission of all the readers in the network that are communicating with the tags. Hence we propose to have a seperate control channel which can be one of the sub bands of the RFID spectrum[8].

Optimisation

One optimisation in this protocol is that, when a reader is in the idle state and receives a query to be sent to the tags, it first checks the time elapsed since it has received any beacon on the control channel. If this time is already greater than T_{min}, then it directly moves to the *CONTEND* state instead of waiting in the *WAITING* state. This saves the extra T_{min} time that a reader would have to wait initially.

- **CASE:** Receive packet from application to send on the network

```
if state = IDLE then
    state = WAITING
    Set waiting_time_expired timer to $T_{min}$
end if
```

- **CASE:** Control channel becomes busy

```
if state = CONTEND then
    Pause contend_backoff_expired timer
end if
if state = DELAY_BEFORE_BEACONING then
    Pause delay_before_beaconing_expired timer
end if
```

- **CASE:** Control channel becomes idle

```
if state = CONTEND then
    Resume contend_backoff_expired timer
end if
if state = DELAY_BEFORE_BEACONING then
    Resume delay_before_beaconing_expired timer
end if
```

- **CASE:** *BEACON* Received

```
if state = READING OR state = CONTEND OR state = WAITING then
    Cancel all timers
    state = WAITING
    Set waiting_time_expired timer to $T_{min}$
end if
```

Figure 3.4: Pulse Protocol Algorithm(Part I)

- **CASE:** Timer Expired

```
if waiting_time_expired timer AND state = WAITING then
    state = CONTEND
    Set contend_backoff_expired timer to previous residual value if any else select a new random backoff
end if
if (beacon_interval_expired timer AND state = READING) OR (contend_backoff_expired timer AND state = CONTEND) then
    if Control channel is IDLE then
        transmit BEACON on control channel
        Set reading_time_expired timer to max allowed communication time, if not set
        Set beacon_interval_expired timer
        state = READING
        Start communication with the tags
    else
        state = DELAY_BEFORE_BEACONING
        Set delay_before_beaconing_expired timer to random delay
    end if
end if
if reading_time_expired timer AND (state = READING OR state = DELAY_BEFORE_BEACONING) then
    cancel all timers
    state = WAITING
    Set waiting_time_expired timer to $T_{min}$
end if
```

Figure 3.5: Pulse Protocol Algorithm

Chapter 4

Implementation Details

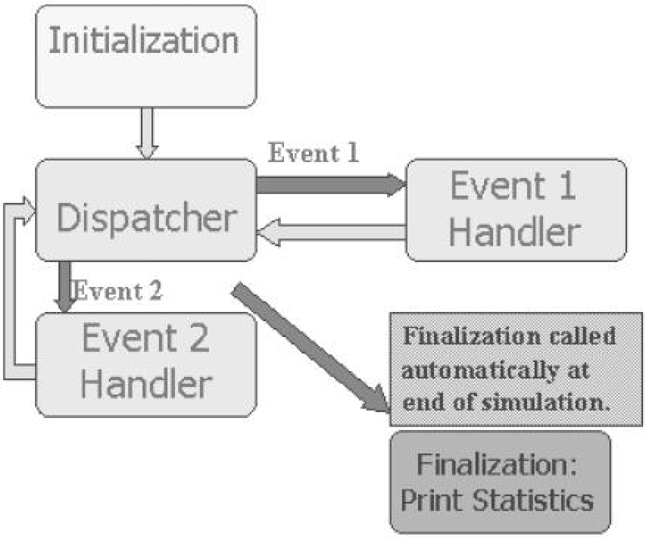

Figure 4.1: Protocol Overview in QualNet

In this chapter we discuss the implentation details of our protocol, and the changes that we made to QualNet simulator[13] for the simulation of RFID readers and tags.

4.1 QualNet Simulator

The QualNet Simulator is an event based simulator. In event based simulator, the time is viewed not as a constant flow but as a discrete points where the events occur. Events can be arrival of a packet, arrival of a signal, timer expire informing the mac protocol that the backoff period has expired etc. The simulator runs by single stepping through the events in an event scheduler and executing the next scheduled event. Protocols in

QualNet essentially run as a finite state machine that changes state only on the occurence of an event. Each protocol runs at a layer in its own state machine. To pass data to, or request a service from, an adjacent layer, the system schedules an event at that layer. Each protocol thus can either create events for itself (like the timer expire events) or events that are processed by another protocol operating at any layer in the protocol stack.

Each layer protocol is implemented as an event handler, that receives an event data structure, called a message, containing the type of event, and the associated data. Fig. 4.1 gives an overview of a typical protocol implementation in QualNet. Each time the event comes, the QualNet simulator determines which protocol this event is meant for and calls that protocol's event dispatcher which then further passes the event to the appropriate event handler depending on the type of event. Finally at the end of the simulation the protocol state changes to finalize state where the protocol's statistics are collected.

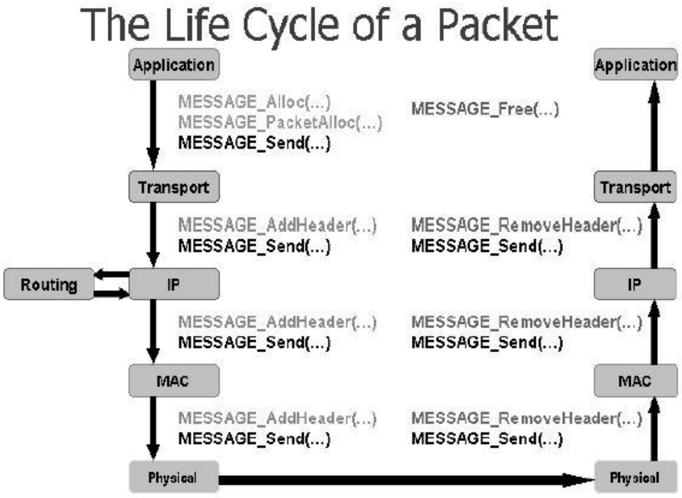

Figure 4.2: Packet Life Cycle in QualNet

When a layer needs to send a packet to an adjacent layer in the QualNet protocol stack, it schedules a packet event at the adjacent layer. The occurence of a packet event at the adjacent layer simulates the arrival of a packet. Fig.4.2 shows how the packet moves through the protocol stack in QualNet. MESSAGE_PacketAlloc, MESSAGE_Free, MESSAGE_AddHeader and MESSAGE_Send are the apis that are used to allocate packet, free packet, add header and send the packet to a protocol. Apart from the message apis, a layer can also send a packet by directly calling that protocol specific apis, if any for example function NetworkIpReceivePacketFromTransportLayer() is a network layer function that can be called by the transport layer if the transport layer has packet to be processed by the network layer.

4.2 Important Changes made to QualNet

Change in Protocol Stack

QualNet does not have any support for RFID and RFID nodes do not require any features of TCP/IP layer of the protocol stack in QualNet. Hence inorder to simulate RFID, we have changed the protocol stack of the QualNet simulator as shown in figure 4.3. We let the application layer in RFID reader bypass the TCP/IP layer and directly communicate with the RFID MAC layer. This is done by letting the application layer send the messages directly to the MAC layer and letting the MAC layer to call the application layer APIs directly. Thus the simulated RFID reader in QualNet does not have any IP address nor is any port number assigned to any application.

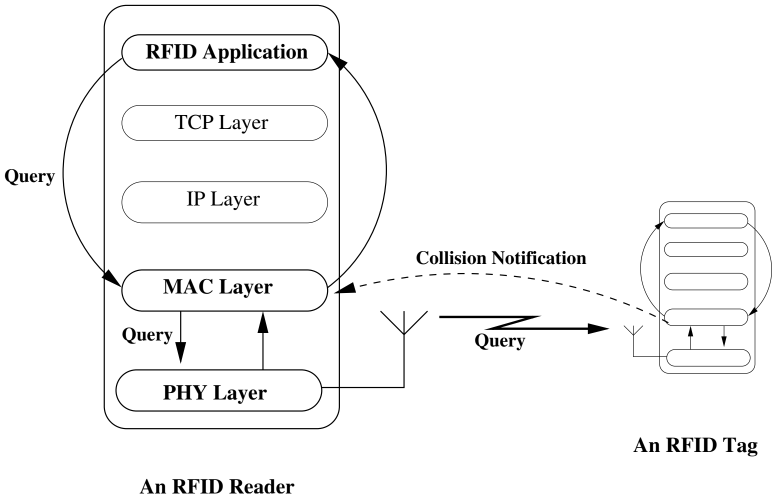

Figure 4.3: Communication between RFID reader and Tag in QualNet

Calculation of Queries Collided

As shown in fig. 4.3, at the reader, when the RFID application generates the query, it sends the query to the RFID MAC layer, which then broadcasts it on the wireless medium

2	6	4
Frame Type	**Source Address**	**CRC**

Figure 4.4: Frame format of a BEACON

as soon as the reader gets access to the medium. This query is then received by all the tags within the read range.

On the tag side, we make the tag to maintain a linked list of the readers from whom it is currently receiving the signals. We have changed the physical layer of the QualNet, so that when a packet is lost due to collision, the MAC layer of that node receives a notification. When the tag receives a collision notification, it sends an off-line notification message to all the readers in the linked list, that it is currently receiving signals from. We call this message as an offline message because it does not account for any bandwidth. It is sent from the MAC layer of the tag direcly to the MAC layer of the reader. At the reader side, these offline notification messages are only used for statistics purpose in calculating number of queries collided and do not take part in the MAC protocol. This offline message exist only in simulation and not in actual implementation.

Frame Format

The frame format of the beacon that we recommend is as shown in the fig. 4.4. However for simulation purpose, the tag had to indicate in the offline notification message which query had collided. Hence we kept an extra field in the Pulse protocol header which would indicate the sequence number of the query. This increased the size of the beacon by 8 bytes.

The format of the query that we used doesnot affect the operation of Pulse, however we used a query of 40 bytes in size.

Dual Channel Implementation

Our protocol assumed that the reader can receive signals simultaneously from both, data and control channels. However, in QualNet, if a node has a single physical layer and 2 channels, then at any given time, a node can listen to a single channel and hence can either only receive or transmit on that channel.

Hence inorder to have a reader simultaneously receive on both the data and control channel, we had 2 physical layers with one data and control channel each. We then made one physical layer to stop listening on data channel and the other physical layer on the control channel. Thus with this kind of setup, the reader could simultaneously transmit and receive on both the channels. However we did not use the feature of simultaneous transmissions.

Chapter 5

Simulation Experiments and Results

We discuss the simulation experiments that we performed in QualNet to check the performance of our protocol. We also present the results of our experiments later in this chapter.

5.1 Simulation Setup

In this section we discuss the simulation setup that we had for the experiments.

5.1.1 Simulation Model

We have simulated the UHF RFID network in QualNet with data channel frequency as 915MHz and the control channel frequency as 930MHz. Our simulation model has the following characteristics

- No inter channel interference between the data and the control channel
- Free space propagation path loss, no fading
- Packet collision is the only cause of packet loss.
- The reception is SNR based and SNR threshold is 10(QualNet default)
- The antenna of all the RFID readers are omni-directional.
- The data processing delay and the channel switching delay is considered negligible.
- 2 Mbps data rate, -91dBm Radio Rx sensitivity and -81dBm Rx threshold
- The transmission power of the RFID node is adjusted to -45dBm, to make the read range $\sim$ 5 feet as is the case with UHF RFID readers.

With these parameters the read range, sensing range and the interference range are 5.31 feet(1.62 meters), 17.71 feet(5.4 meters) and 23.29 feet(7.1 meters) respectively. Here the interference range is the maximum distance upto which a reader's transmission can interfere with another reader-tag communication. Thus the beacon range should be **atleast equal to** the interference range inorder to make this protocol effective.

We define the **Beacon Range Factor(BRF)** as the ratio of the control channel transmission power to the data channel transmission power. According to [14], with λ being the signal wavelength and r being the distance between the antennas, the relationship between the power P_t of the signal transmitted by an antenna with gain G_t, and the power P_r of the signal received by another antenna with gain G_r, is given by:

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi r}\right)^2 \alpha \frac{1}{r^2}$$

For Beacon range,

$$\frac{P_r}{P_{Beacon}} \quad \alpha \quad \frac{1}{r^2_{Beacon}}$$

For Data range,

$$\frac{P_r}{P_{Data}} \quad \alpha \quad \frac{1}{r^2_{Data}}$$

Thus,

$$BRF = \frac{P_{Beacon}}{P_{Data}} = \left(\frac{r_{Beacon}}{r_{data}}\right)^2$$

Thus with data range as 1.62 meters, inorder to have a beacon range of 7.1 meters, we require a BRF of *19.2*.

5.1.2 Performance metrics

A query is said to be successfully sent if it is sent by a reader and is successfully received by all the tags in the read range i.e. it does not collide with any other query in the network. Note that in QualNet implementation, a reader receives a offline collision notification from the tags if its query gets collided. Hence if the reader does not receive any offline message for a query, the query is considered as being sent successfully.

We define the system throughput and the percentage efficiency as follows.

$$\textbf{System Throughput} = \frac{\text{Total queries sent successfully(by all readers)}}{\text{Total time}}$$

$$\textbf{System Efficiency(\%)} = \frac{\text{Total queries sent successfully(by all readers)} \times 100}{\text{Total queries sent(successful + collided) by all readers}}$$

In general, the tag identification is through a query-response protocol where the reader sends a query and the tag responds with its unique identification number. Higher the number of queries sent successfully, higher the throughput, and hence higher would be the number of tags identified by the readers. Percentage efficiency reflects the ability of a protocol to detect a possibility of collision at the tags and hence avoid unnecessary transmissions. An improvement in throughput indicate an improvement in the read rate whereas an improvement in the efficiency indicate reduction in collisions. Thus throughput and efficiency together define the effectiveness of the protocol. Through simulations we show that Pulse protocol is effective in both the dimensions.

5.1.3 Simulation Scenarios

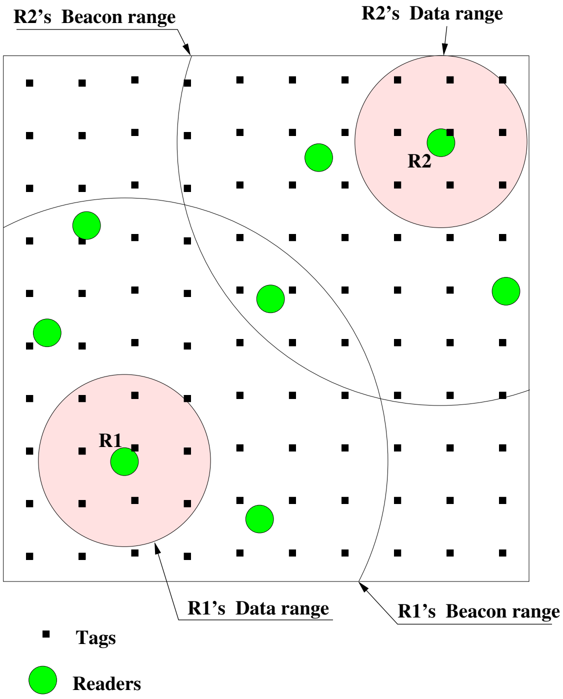

Figure 5.1: A typical scenario in the simulation setup

We used the following simulation setup for running the experiments.

- *Tag setup:* We used a field of 10 meter X 10 meter area, with 400 tags forming a grid of 20 X 20. The tags were placed throughout the simulation field with 0.5 meter interval so that most of the collisions in the field would be detected by these tags. Fig. 5.1 shows a typical simulation setup with tags placed uniformly and some readers placed randomly in the field. The figure shows an instance of the simulation where R_1 and R_2 are reading the tags and send beacon periodicallly. All other readers which receive a beacon withhold from reading the tags.
- *Fixed Readers:* For fixed reader simulation, all the readers were randomly placed in the field. We used 20 random topologies with 3 different seeds in each case giving a total of 60 simulations per protocol.
- *Mobile Readers:* For simulation of mobile readers, the initial placement of readers was a uniform grid of readers. We used a random way point mobility with low speed of 0.5 to 2 meters per second and 10 random seeds.

For simulation, the RFID application generated a packet(query) to be sent to the tags with exponential interarrival time of average 500 μsec throughout the simulation time of 60 seconds.

5.1.4 Compared Protocols

We compared our Pulse protocol with Aloha protocol, CSMA protocol[8][9] and Colorwave.

- A reader with Aloha protocol assumes that it is the only reader communicating with the tag. Hence when the reader wants to communicate with the tags, it simply starts its transmission without applying any collision avoidance.
- The CSMA protocol is similar to **ETSI EN 302 208**[8][9] with a listen time of 15msec and maximum reading time of 4sec.
- For Colorwave protocol, we used the time slot of 10 msec. Rest of the parameters for Colorwave are as given in [7]

We set the beacon interval of Pulse protocol as 5 msec and T_{min} same as the listen time in CSMA i.e 15msec. Using similar settings for both the protocols help us evaluate the MAC protocols in an unbiased manner.

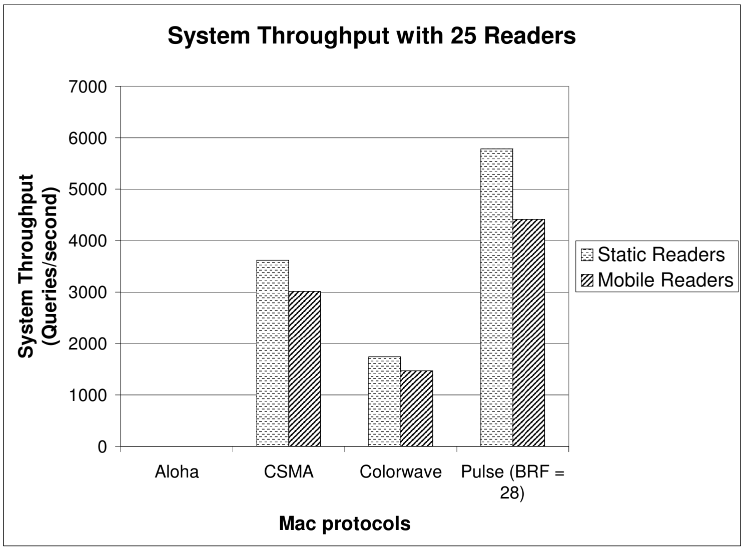

Figure 5.2: Throughput comparison with 25 readers

5.2 Results

We first did a throughput comparison of Pulse with other protocols considering BRF=28 and beacon interval = 5msec with a 25 reader topology. We then changed the number of readers(4. . . 64) and saw the effect on the system throughput. Similar experiments were performed for comparison of system efficiency. We also studied the effect of BRF and beaconing interval on throughput and efficiency of Pulse in subsequent subsections.

5.2.1 Throughput

25 Reader Topology:

Fig. 5.2 shows the comparison of Pulse with other protocols in 25 reader topology with static and mobile readers. As seen in the figure:

- With Aloha protocol, almost every transmission in the system collided because readers with aloha protocol do not apply any collision avoidance.
- CSMA has better throughput than Aloha because carrier sensing is succesful in avoiding collision with the readers within the sensing range. However the number of collisions using CSMA is still high because of the hidden terminal problem.
- In colorwave, because of the distributed timeslot mechanism, the timeslots are underutilised thus showing lower throughput.

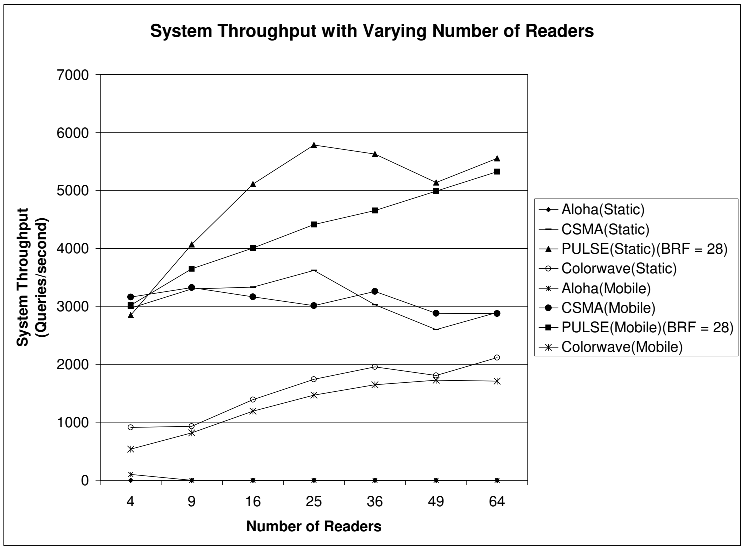

Figure 5.3: Throughput comparison with different number of readers

- In Pulse, these collisions are avoided because the beacon sent by a reader acts as a notification to the neighbouring readers(including hidden nodes), which then withhold their transmission thus avoiding collisions. Pulse shows throughput improvement of 60% as compared to CSMA and 232% as compared to Colorwave in static topology.

- In case of mobility, the system throughput drops as compared to their static counterpart. However, Pulse still remains to be effective with throughput improvement of about 46% as compared to CSMA and 200% as compared to Colorwave.

Varying Number of Readers: Fig. 5.3 shows the graph of throughput with varying number of readers in the system. Following are the observations:

- Aloha continues to show negligible throughput.

- As the number of readers in the system are increased, the throughput of CSMA protocol does not increase. Hence CSMA cannot cater to dense networks.

- Pulse protocol shows better throughput in all topologies as compared to both colorwave and CSMA protocol. It shows an improvement of as high as 98% (with 49 readers) over CSMA and 337% (with 9 readers) over colorwave protocol.

- Using Pulse protocol, the throughput of the system keeps on increasing as the number of readers in the system is increased upto a **saturation point** after which the throughput of the system stops increasing even if the number of readers is increased. For example according to the graph, for BRF=28, 25 readers is the saturation point for Pulse. Hence if the throughput of the system is of prime importance, no more than the saturation number of readers should be deployed.

- Note that Pulse remains to be effective even in a highly dense mobile network of 64 readers.

5.2.2 Efficiency

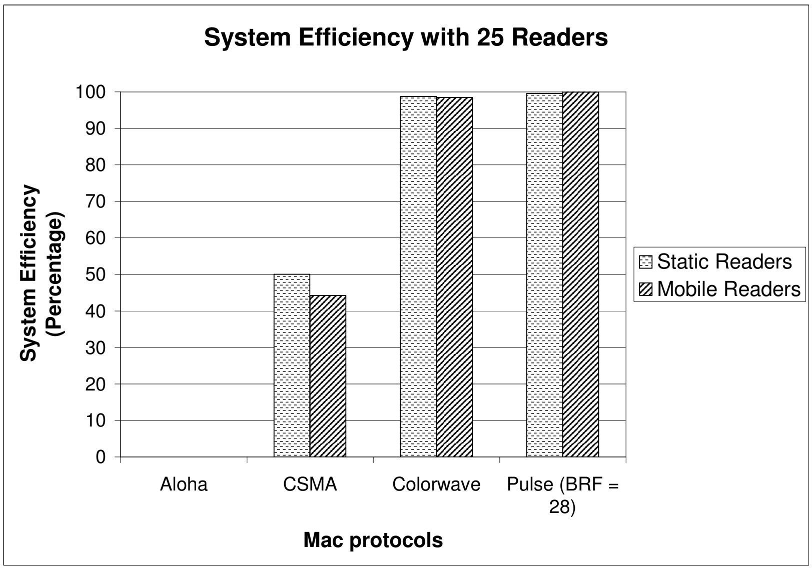

Figure 5.4: Efficiency with 25 Readers

25 Reader Topology: Figure. 5.4 shows the percentage efficiency of the system using different MAC protocols.

- The efficiency with CSMA barely crosses 50% which means that 50% of the transmissions in the network are wasted due to collision.

- Using Colorwave, the efficiency is almost 100% however, colorwave fails to give better throughput than Pulse.

- With Pulse, the efficiency is above 99% with both static and mobile reader network. Thus Pulse is successful in detecting possibility of collisions and thus avoid the same.

Varying Number of Readers: Fig. 5.5 shows the graph for the same.

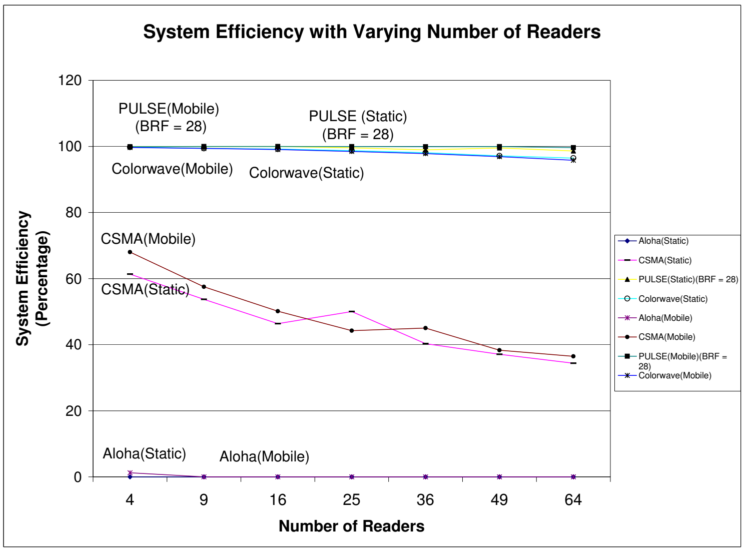

Figure 5.5: Efficiency with Varying Number of Readers

- With Aloha protocol, the efficiency is negligible in all the experiments.

- As seen, the efficiency of CSMA keeps on decreasing as the number of readers go on increasing. As the density of the network increases, the number of hidden terminals increase thus reducing the efficiency.

- Efficiency of Colorwave is ¿ 97%. However, as seen in section 5.2.1, the throughput of Colorwave is very less which means that using Colorwave, a reader gets lesser chance to transmit.

- Pulse protocol overcomes the hidden terminal problem through a beacon on the control channel and hence the efficiency of the system is above 95% in all topologies.

Thus Pulse is definitely an improvment over the existing solutions in both the dimensions of throughput and efficiency. It remains to be effective even in a highly dense mobile network.

We further test the effect of the protocol parameters, BRF and beaconing interval, on the system throughput and efficiency.

5.2.3 Optimal BRF

We initially used BRF as 20($>$ 19.2) to run the experiments on a 25 reader topology. We observed that even with BRF=20 i.e with beacon range almost same as the interference

BRF	Beacon Range(meters)
20	7.24
24	7.93
28	8.57
32	9.16
36	9.72

Table 5.1: Beacon Range for different BRF

range, there were lots of collisions in the network due to which the efficiency was low. The reason for the collision is that the signals from multiple readers outside the beacon range adds to the noise at the tags, so that the SNR gets reduced, leading to collision at the tags. Consequently we repeated the experiments with increasing BRF in step of 4. Beacon range for different BRF values are given in table 5.1.

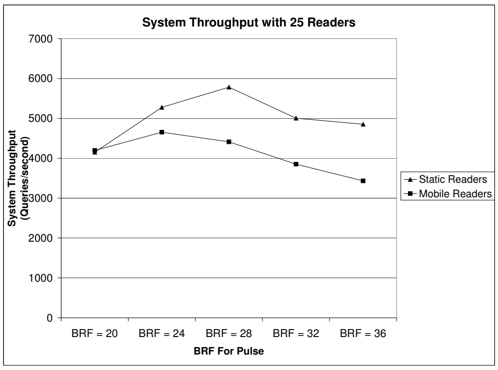

Figure 5.6: Throughput with different BRFs

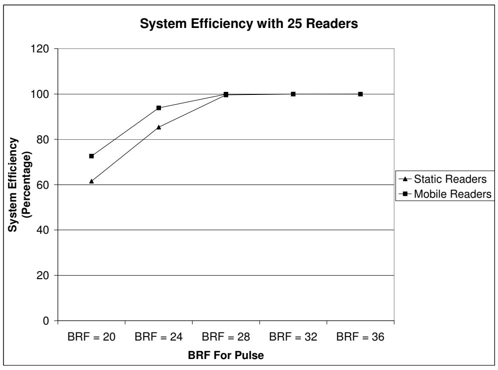

Figure 5.7: System Efficiency with different BRFs

Fig. 5.6 and fig. 5.7 show the throughput and efficiency of the system in 25 reader topology with different BRFs.

- *With increasing BRF, the throughput, efficiency of the system increases:* This is because, due to increase in the beacon range, more readers in the neighbourhood get notified and hence withhold their transmission which otherwise would have collided.

- *Throughput decreases beyond crossover point:* As the BRF is further increased, there is a **crossover point**(BRF=28 for the considered topology) upto which the throughput increases. If BRF is increased beyond this value, the throughput start decreasing and efficency remains at its peak. This is because with the increase in the

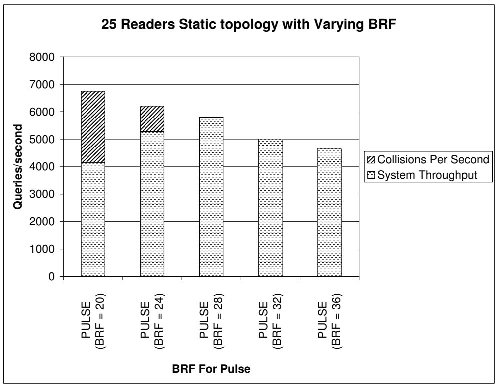

Figure 5.8: Queries sent in 25 reader static topology

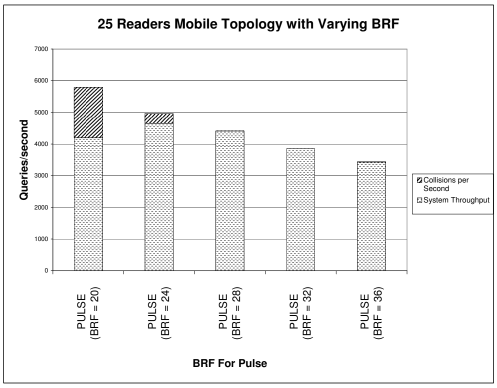

Figure 5.9: Queries sent in 25 reader mobile topology

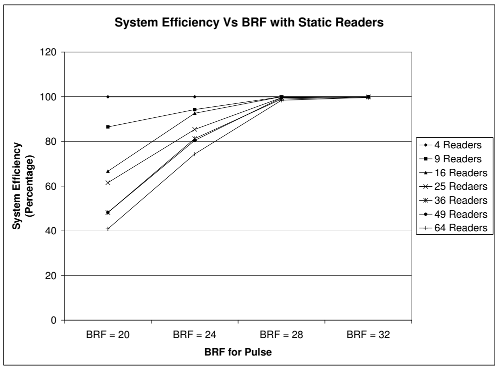

Figure 5.10: Queries sent in 25 reader static topology

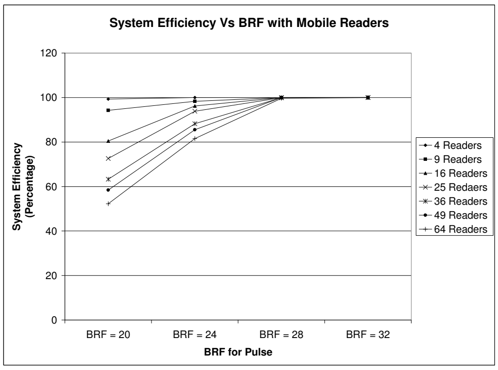

Figure 5.11: Queries sent in 25 reader mobile topology

beacon range, even the farther non-interfering readers start to receive the beacon and withhold their transmission which otherwise would have been successful. The case is similar with mobile reader scenario, except that the crossover point is BRF=24.

The height of the bars in fig. 5.8 and fig. 5.9 indicate the total number of queries(successful + collided) sent per second by all the readers. With increasing BRFs, the total queries sent keep decreasing. This observation too has the same reason that as BRF increases more number of readers withhold their transmissions inorder to avoid any collisions thus reducing the total queries sent.

Fig. 5.10 and Fig. 5.11 shows the system efficiency of the network with different BRF values. It shows that both in fixed(static) and mobile readers case, the efficiency is very low with BRF=20. However, as BRF increases, efficiency increases. It is almost 99% at BRF = 28 and above, in all the networks.

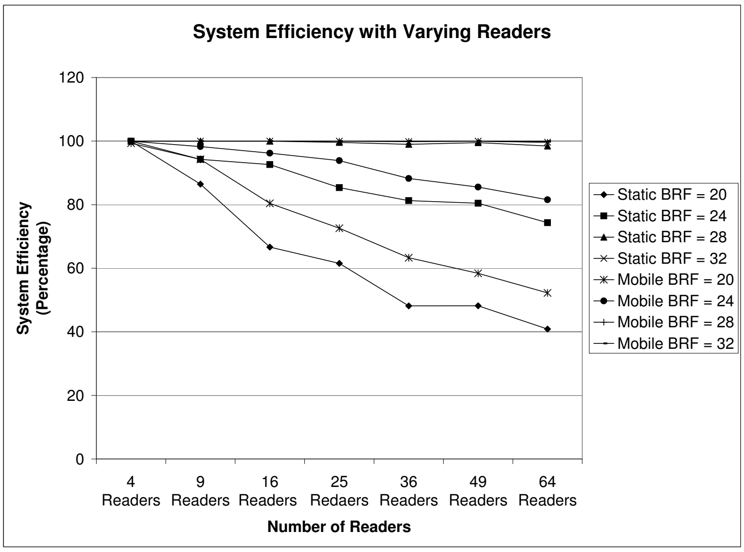

Figure 5.12: System Efficency with different BRFs with varying number of readers

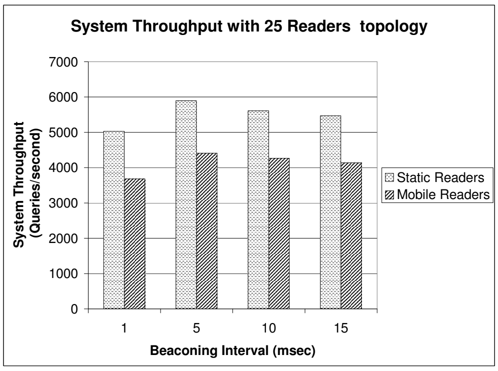

Figure 5.13: Effect of Beacon interval on system throughput

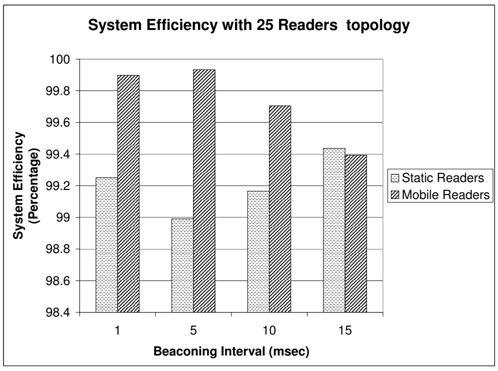

Figure 5.14: Effect of Beacon interval on system efficiency

Another interesting result is the impact of increasing density on efficiency of Pulse with differnt BRFs. We observe in Fig. 5.12 that with BRF of 20 and 24, the system efficiency decreases as the number of readers in the network increases. However with BRF of 28 and 32 the efficiency is as high as 97% even in dense network of 64 readers.

Thus keeping BRF too low will reduce the efficiency whereas keeping it too high will reduce the throughput of the RFID system.

5.2.4 Optimal Beacon Interval

We also tested the Pulse protocol with different beacon intervals. Fig. 5.13 shows the plot of throughput Vs beacon interval. In each case, T_{min} is 3 times the beacon interval.

As seen, the throughput initially increases till beacon interval of 5 msec and then starts decreasing. With low beacon interval, lot of time is wasted in sending beacons, thus reducing the overall system throughput. Whereas, with very high beacon interval, lot of time gets wasted by readers waiting for T_{min}(3 times the beacon interval) time in the *WAITING* state. However as seen in the figure, the change in throughput of the system is not so significant. Also as seen in figure 5.14, the change in the beaconing interval do not show any significant change in the system efficiency. Hence this protocol parameter is not very significant during the deployment of an RFID system with Pulse protocol.

Thus we have seen that Pulse shows considerable improvement in throughput and is successful in reducing the reader collisions as compared to the existing approaches.

5.3 Discussion

With the help of a beacon we notify all the possibly interfering readers about the transmission on the data channel so that they backoff and thus avoid collisions. With Pulse protocol, the throughput of the RFID system is increased by as high as 98% (with 49 readers) in static network and as high as 85% (with 64 readers) in mobile network as compared to CSMA protocol.

We did not account for any channel switching delay in our simulations. However we believe it to be negligible as compared to the beacon interval. Ofcourse, the Pulse protocol demands for some extra circuitry on the receiver end of a reader. If the control channel is within the coverage of the receiver antenna of the RFID reader, the reader will only need an extra isolation circuit that will seperate the signals received on the control and the data channel.

However Pulse protocol increases the throughput considerably. It also promotes the use of lesser number of readers by being effective in a mobile scenario. We believe this performance gain and reduction in number of readers required is high enough to offset the hardware modification required by this protocol. Also as compared to Colorwave, the readers with Pulse protocol do not require any time synchronisation which otherwise is an overhead for colorwave.

Chapter 6

Performance Modelling

In this chapter we give a theoretical analysis of our protocol with some assumptions to simplify the model. We then also compared the simulation results with the analytical results.

6.1 Theoretical Analysis

In this section we try to model our system inorder to find the average system throughput for a topology with static readers. We make the following assumption on the system to simplify the analysis.

- We assume a saturation case, i.e. all the readers always have to communicate with the tags.
- There are no hidden terminals on the control channel. Hence if a reader sends a beacon, all the readers receive the beacon. Note that even in such a case the readers might not be able to communicate with each other on the data channel since the range on the data channel is lesser than on the control channel.
- Since all the readers receive a beacon sent by a reader, normally there can be not more than one reader in the network communicating with the tags at any given point of time.
- We also assume that the time is slotted with the beacon interval(T_{BI}) as the slot size, although in reality the time may not be slotted and synchronised across all nodes.

Each reader starts communicating with the tags by sending a beacon on the control channel at the start of a time slot. When multiple readers send a beacon simultaneously, they collide and the slot is wasted. The readers then again choose the *contend_backoff* uniformly from $[0, CW]$ and waits for those many beacon intervals. It then decrements its *contend_backoff* at the end of every empty time slot (beacon interval) and transmit when *contend_backoff* counts down to 0. The reader always chooses its backoff value from $[0, CW]$. Thus the average backoff value chosen is $\overline{W} = CW/2$.

variable	meaning
CW	contention window size from which *contend_backoff* is chosen
N	number of readers in the system
$\overline{W}$	Average backoff window size
p	probability that a beacon transmission collides with another beacon
BDI	Backoff Decrement Interval
$E[T_{BDI}]$	average duration of a BDI
$E[BDI]$	average number of BDIs between two successful transmissions by a reader
T_e, T_s, T_c	duration of *BDI* that is empty, successful or contain collision respectively
P_e, P_s, P_c	probability that *BDI* is empty, successful or contain collision respectively
$E[T_{cycle}]$	average duration between two successful transmissions by a reader
T_{read}	maximum duration for which a reader is allowed to communicate with the tags at a time
$\tau_{query}, \tau_{beacon}$	propagation delay on data and control channel respectively
l_{query}, l_{beacon}	transmission time of a query and beacon respectively
$Q_{T_{read}}$	number of queries sent by a reader in T_{read}
S	System throughput, number of queries tranmitted by all the readers per unit time

Table 6.1: Notation of anaylsis variables

Backoff Decrement Interval(BDI): The basis of our analysis is similar to as given in [15]. We define a backoff decrement interval(BDI) to be the interval after which the backoff value is decremented. Fig.6.1 shows the time line of 4 readers in the system whereas Fig. 6.2 shows the transmission of other readers R_2, R_3, R_4 superimposed on the timeline of reader R_1. Fig. 6.2 shows the BDIs as dotted lines. When reader R_1, at time t_2, receives a beacon from reader R_4, R_1 stops the backoff counter and resumes when it has not received any beacon for T_{min} time i.e at time t_3. R_1 then decrements its backoff value at the end of the next empty time slot at time t_4. Thus the BDI duration is $T_s = T_{read} + T_{min} + 1$. Similarly, if there is a collision on the channel, (see R_3's time line at time t_0 in fig. 6.1) the duration of BDI will then be from, t_0 to t_1 and thus $T_c = 1(\text{collision}) + 1(\text{empty time slot})$. If the BDI contains neither a successful transmission neither a collision, then the duration of the BDI will be a single empty time slot. Now we find the probability of each of these cases.

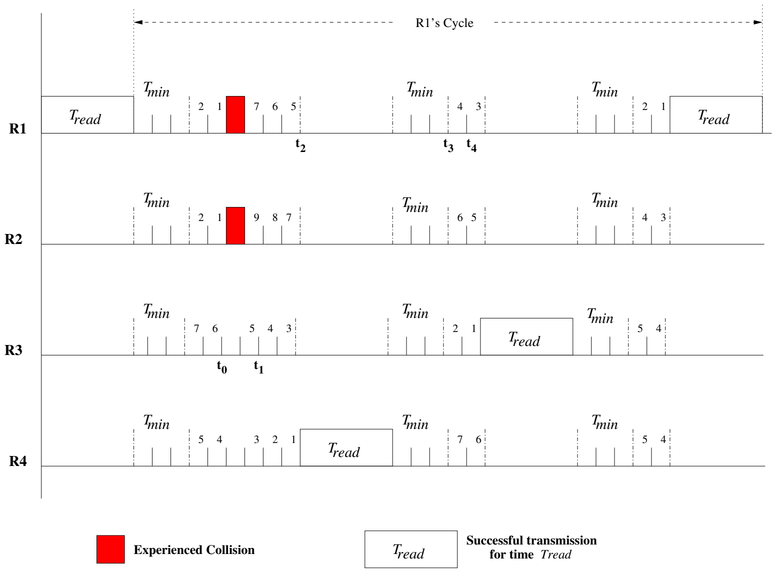

Figure 6.1: Effect of transmissions on BDIs of other readers

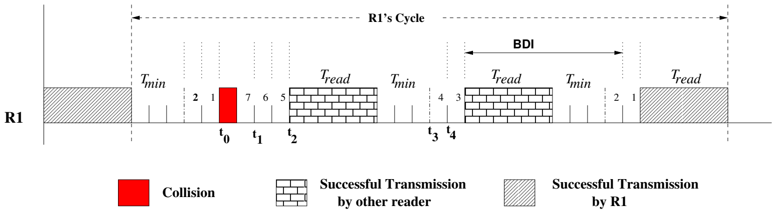

Figure 6.2: BDIs of a Reader

A BDI is said to be active if it contains transmission from atleast one reader. The probability that a given BDI is active is given by

$$P[\text{active}] \;=\; 1-\left(1-\frac{1}{\overline{W}}\right)^{N} \tag{6.1}$$

and the probability that the BDI contains a collision given that it is active is given by

$$P[\text{collision}|\text{active}] \;=\; \frac{1-\left(1-\frac{1}{\overline{W}}\right)^{N}-\frac{N}{\overline{W}}\left(1-\frac{1}{\overline{W}}\right)^{N-1}}{1-\left(1-\frac{1}{\overline{W}}\right)^{N}} \tag{6.2}$$

Thus, the probability that a given BDI contains a collision is

$$\begin{aligned} P_c &= P[\text{collision}|\text{active}] \times P[\text{active}] \\ &= 1-\left(1-\frac{1}{\overline{W}}\right)^{N}-\frac{N}{\overline{W}}\left(1-\frac{1}{\overline{W}}\right)^{N-1} \end{aligned} \tag{6.3}$$

Similarly, the probability that a given BDI contains a successful transmission by a reader is given by

$$\begin{aligned} P_s &= P[\text{success}|\text{active}] \times P[\text{active}] \\ &= \frac{N}{\overline{W}}\left(1-\frac{1}{\overline{W}}\right)^{N-1} \end{aligned} \tag{6.4}$$

The average duration of a BDI is calculated using the theorem of total probability [22] as

$$\begin{aligned} E[T_{BDI}] &= P_eT_e+P_sT_s+P_cT_c \\ &= T_c+\left(1-\frac{1}{\overline{W}}\right)^{N}(T_e-T_c)+\frac{N}{\overline{W}}\left(1-\frac{1}{\overline{W}}\right)^{N-1}(T_s-T_c) \end{aligned} \tag{6.5}$$

Cycle Duration: Consider two readers R_1 and R_2. Since R_1's backoff timer is suspended whenever R_2 is transmitting, it appears to R_1 that R_2 is transmitting for one slot after every $\overline{W}$ slots [16]. Thus the probability that R_1's transmission will collide with R_2's transmission is $1/\overline{W}$. And for a network of N nodes, the probability of $R1$'s transmission getting collided is given by,

$$p \;=\; 1-\left(1-\frac{1}{\overline{W}}\right)^{N-1} \tag{6.6}$$

We define the read cycle of a reader to be the time between two successful channel captures by a reader. Note that successful channel captures in this case is different from successful transmissions. A reader captures the data channel for a duration of T_{read}. During a capture, the reader transmits multiple queries successively for T_{read} time.

As discussed earlier, the reader might transmit and collide with probability p, after which it again chooses a backoff value from $[0, CW]$ and transmits when the backoff counts down to 0. This goes on until the beacon transmission is successful. Thus the number of transmission attempts can be modelled as a geometric distribution with probability of success as $(1-p)$. Thus the expected number of BDIs until a successful transmission is given by

$$\begin{aligned} E[BDI] &= (1-p)\frac{CW}{2} + p(1-p)2\frac{CW}{2} + p^2(1-p)2^2\frac{CW}{2} + \cdots \\ &= \frac{CW}{2(1-p)} \end{aligned} \tag{6.7}$$

The average duration of a cycle is given by

$$\begin{aligned} E[T_{cycle}] &= E[BDI] \times E[T_{BDI}] + T_{read} \\ &= \frac{CW}{2(1-p)} \times E[T_{BDI}] + T_{read} \end{aligned} \tag{6.8}$$

Throughput: Now, let us assume each reader is allowed to communicate with the tags for a maximum of x beacon intervals, i.e. $T_{read} = x$ time slots. Now, each time slot in a T_{read} will consist of one beacon transmission on the control channel and several transmissions(called queries) on the data channel by the reader. Thus each beacon interval $= (\tau_{query} + l_{query}) \times$ (no of queries in one beacon interval) $+ (\tau_{beacon} + l_{beacon})$. Thus,

$$T_{read} = \left[(\tau_{query} + l_{query}) \times Q_{T_{read}} \right] + x(\tau_{beacon} + l_{beacon}) \tag{6.9}$$

Thus,

$$Q_{T_{read}} = \left[\frac{T_{read} - x(\tau_{beacon} + l_{beacon})}{\tau_{query} + l_{query}} \right] \tag{6.10}$$

where $Q_{T_{read}}$ is the number of queries sent by a reader in T_{read}.

The average number of such successful periods(T_{read}) by all the readers in one cycle is $P_s \times E[BDI]$. Thus the average number of queries sent by all the readers in one second, which is essentially the system throughput as defined in chap. 5, will be

$$S = \frac{Q_{T_{read}} \times P_s \times E[BDI]}{E[T_{cycle}]} \tag{6.11}$$

Time to wait: The average time to wait for a reader before getting access to the channel is same as the average cycle duration $E[T_{cycle}]$ which is given by equation 6.8.

Utilisation: We define utilisation as the ratio of total time spent by all the readers in communicating with the tags during a cycle to the total duration of a cycle.

$$Utilisation = \frac{T_{read} \times P_s \times E[BDI]}{E[T_{cycle}]} \tag{6.12}$$

6.2 Numerical Validation

For validation of the model, we calculated the system throughput using eq. 6.11 for various number of readers. The simulations done earlier had hidden terminals on the control channel. Also the readers in the simulation were not in saturation. Hence we did new simulations for comparing with the analytical results. The readers in these new experiments always had a query to be sent to the tags and also the area used was small (8X8 meters). For the analytical modeling we assumed duration of collision to be exactly one beacon interval whereas, in simulation it might be much less than that depending on when the reader detects the data channel to be busy or receives beacon from the neighbour while it is itself communicating with the tags. We kept rest of the parameters same as in simulations. The parameter values used in the analysis are shown in table 6.2.

variable	value
x	800
CW	32
beacon interval(T_{BI})	5000μs
T_{min}	3 $\times T_{BI}$
T_{read}	4sec
T_c	$(1+1)\times T_{BI}$
T_s	$T_{read} + T_{min} + T_{BI}$
T_e	1 T_{BI}
beacon size	20 bytes
query size	40 bytes
l_{beacon}	265μs
l_{query}	341μs

Table 6.2: Analytical Modeling parameters

N	$\overline{W}$	p	$E[BDI]$	P_c	P_s	P_e	$E[T_{BDI}]$ μs	$E[T_{cycle}]$ μs	*Utilisation* (%)	*Throughput* (Queries/sec)
2	16	0.06	17.07	0.01	0.12	0.88	475527	12115667	66	1834
4	16	0.18	19.42	0.02	0.21	0.77	832172	20159181	79	2204
9	16	0.40	26.81	0.10	0.34	0.56	1353178	40283133	89	2482
16	16	0.62	42.13	0.26	0.38	0.36	1531267	68506261	93	2594
25	16	0.79	75.30	0.47	0.33	0.20	1340301	104928025	95	2647
36	16	0.90	153.15	0.67	0.24	0.10	952098	149816529	96	2669
49	16	0.95	354.40	0.82	0.14	0.04	564212	203959041	96	2669
64	16	0.98	933.10	0.92	0.07	0.02	284959	269896030	95	2634

Table 6.3: System Throughput of the network using analytical model

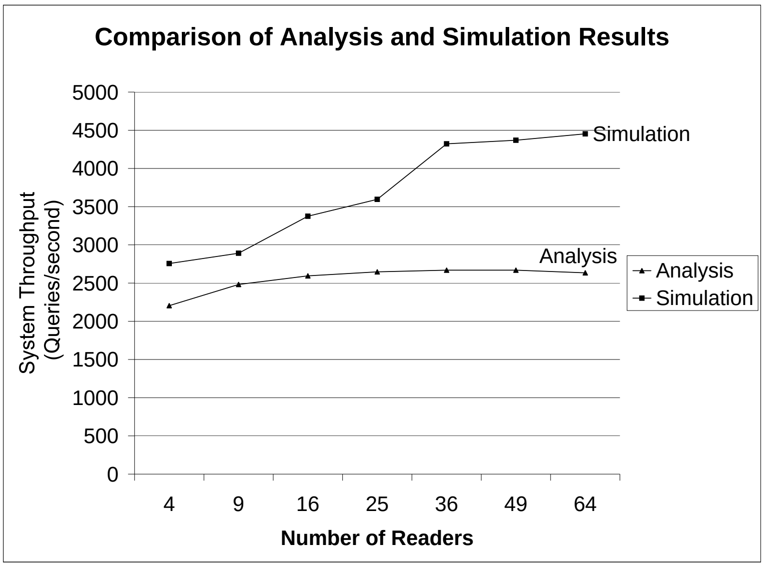

Figure 6.3: Throughput Comparison for analytical model and simulations

The values of l_{beacon}, l_{query} are taken from the simulation in QualNet whereas the values of T_c, T_s, T_e are explained in section 6.1.

Table. 6.3 show the analysis results and the fig. 6.3 shows the comparison of the system throughput obtained through simulation and analysis. We see a similar trend in the analytical results as in the simulation results despite its assumptions about collisions and *delay_before_beaconing*.

Observations:

- Initially, P_e is very high due to which many slots remain empty and without any collision.

- However as N increases, there are more number of nodes to transmit and hence Pe decreases and Ps goes on increasing. Thus the system throughput increases. However after some N, as there are large number of nodes, the probability of collision increases and that of success decreases.
- As seen in the table 6.3, the duration of the cycle keep on increasing as the number of nodes increases and hence each reader communicates less frequently with the tags.
- The utilisation goes as high as 95% in the analysis resutls.
- We have assumed that the entire beacon interval goes wasted in case of a collision and also we have not modeled the *delay_before_beaconing*. Hence the probability of collision in the analytical model increases faster than in simulations due to which the analytical model curve drifts away from the simulation curve as the number of nodes increases in the network. However the simulation results show a similar trend as the analytical model.

Chapter 7

Conclusion

Making the readers mobile have advantages of mainly convenience and reduction in cost. Large number of applications based on RFID system require the readers to operate in close proximity of each other. Due of the reader collision, the RFID system may operate incorrectly and see a reduction in read rate. This may hamper the proliferation of RFID systems.

We presented a distributed protocol for a RFID network which uses a beaconing mechanism by sending periodic beacon on the control channel. It mitigates the reader collision problem by reducing the reader collisions to 1-2% and also increasing the read rate of the system by as high as 98% as compared to CSMA. It requires very less overhead on the reader side and absolutely no support on the tag side. Our protocol is also very effective in a mobile scenario facilitating the use of mobile readers which is a cost effective solution for many applications.

Some possible extensions to this work are:

- Some RFID systems have multiple data channels to communicate with the tags. Our protocol did not take into consideration such a scenario. Future research of our protocol can involve porting it to such a scenario by having the information about the channels in the beacon.

- When two readers collide, not letting one of them to transmit is the general way of avoiding collision. However, by this way, we reduce the throughput of the entire system. Another way can be making the readers transmit at a lower transmission power such that the interference region is minimised. Future work of our protocol may involve making the Pulse work for such a scenario. This may require changing the control channel transmission power according to the change in data channel transmission power.

- We did not have any timing information in the beacon like the sequence number or the expected time a reader would need to communicate with the tags. Having such information in the beacon can let the other readers enter a power save mode by switching off their transmitters.
- The analytical model that we designed, had a few assumptions like the readers are in saturation and there are no hidden terminals on the control channel. Extending this model to a generic can also be a very interesting problem to solve in the theoretical domain.

Bibliography

[1] Klaus Finkenzeller. *RFID Handbook : fundamentals and applications in contactless smart cards and identification.* Chichester : John Wiley, Leipzig, dritte edition, 2003.

[2] A basic introduction to rfid technology and its use in supply chain. Technical report, Laran Technologies, January 2004.

[3] Microsoft and rfid. Technical report, Microsoft, January 2004.

[4] Daniel W. Engels. The reader collision problem. Technical report, epcglobal.org, 2002.

[5] Chris Diorio. Class 1 generation 2, uhf rfid. CTAN: `www.autoid.org/SC31/2004/dec/SG3_200411_430_Gen2Update.pdf`, December 2004.

[6] Electronic product code. `http://www.epcglobalinc.org`.

[7] J. Waldrop, D. W. Engels, and S. E. Sarma. Colorwave: An anticollison algorithm for the reader collision problem. In *IEEE Wireless Communications and Networking Conference (WCNC)*, 2003.

[8] *ETSI EN 302 208-1 v1.1.1*, September 2004. CTAN: `http://www.etsi.org`.

[9] *ETSI EN 302 208-2 v1.1.1*, September 2004. CTAN: `http://www.etsi.org`.

[10] Junius K. Ho. Solving the reader collision problem with a hierarchical q-learning algorithm. Master's thesis, Massachusetts Institute of Technology, February 2003.

[11] Andrew S. Tanenbaum. *Computer Networks.* Prentice Hall, India, 2002.

[12] IEEE Computer Society LAN MAN Standards Committee. Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications. In *ANSI/IEEE Std.*

802.11, 1999 Edition, The Institute of Electrical and Electronics Engineers. New York, 1999.

[13] Qualnet simulator 3.6. `http://www.qualnet.com`.

[14] Prashant Krishnamurthy Kaveh Pahlavan. *Principles of Wireless Networks.* Pearson Education, 2002.

[15] O. Tickoo and B. Sikdar. Queing Analysis and Delay Mitigation in IEEE 802.11 Random Access MAC based Wireless Networks. In *IEEE INFOCOM*, 2004.

[16] Y. C. Tay and K. C. Chua. A capacity analysis for the ieee 802.11 mac protocol. *Wireless Networks*, 7(2):159–171, 2001.

[17] Radio frequency identification - a basic primer. White Paper, AIM Inc WP-98/002R2, August 2001.

[18] Draft paper on characteristics of rfid-systems. White Paper, AIM Inc WP-98/002R2, July 2000.

[19] Auto-ID center. *860Mhz-960Mhz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification, Recommended Standard*, November 2002.

[20] Auto-ID center. *13.56Mhz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification, Recommended Standard*, November 2002.

[21] Roy Blake. *Wireless Communication Technology.* Delmar: Thomson Learning, 2001.

[22] Kishor Trivedi. *Probability & Statictics With Reliability, Queuing, And Computer Science Applications.* Prentice Hall India, fifteenth edition, 2003.

Acknowledgements

I take this opportunity to express my sincere gratitude for **Prof. Sridhar Iyer** for his constant support and encouragement. His excellent guidance has been instrumental in making this project work a success and also given a new dimension to my thinking process.

I would like to thank **Prof. Anirudha Sahoo** for reviewing my work in the intermediate stage. I would also like to thank my colleagues **S. Anusha** and **Nitin Salodkar** for helpful discussions in the initial part of my project, **Imran Mansuri** for being a supportive friend and the **KReSIT department** for providing me a world class computing infrastructure.

I would also like to thank my **family** and **friends** especially my entire **M.Tech Batch**, who have been a source of encouragement and inspiration throughout the duration of the project.

Last but not the least, I would like to thank the entire KReSIT family for making my stay at IIT Bombay a memorable one.

Shailesh M. Birari
I. I. T. Bombay
June 30^{th}, 2005